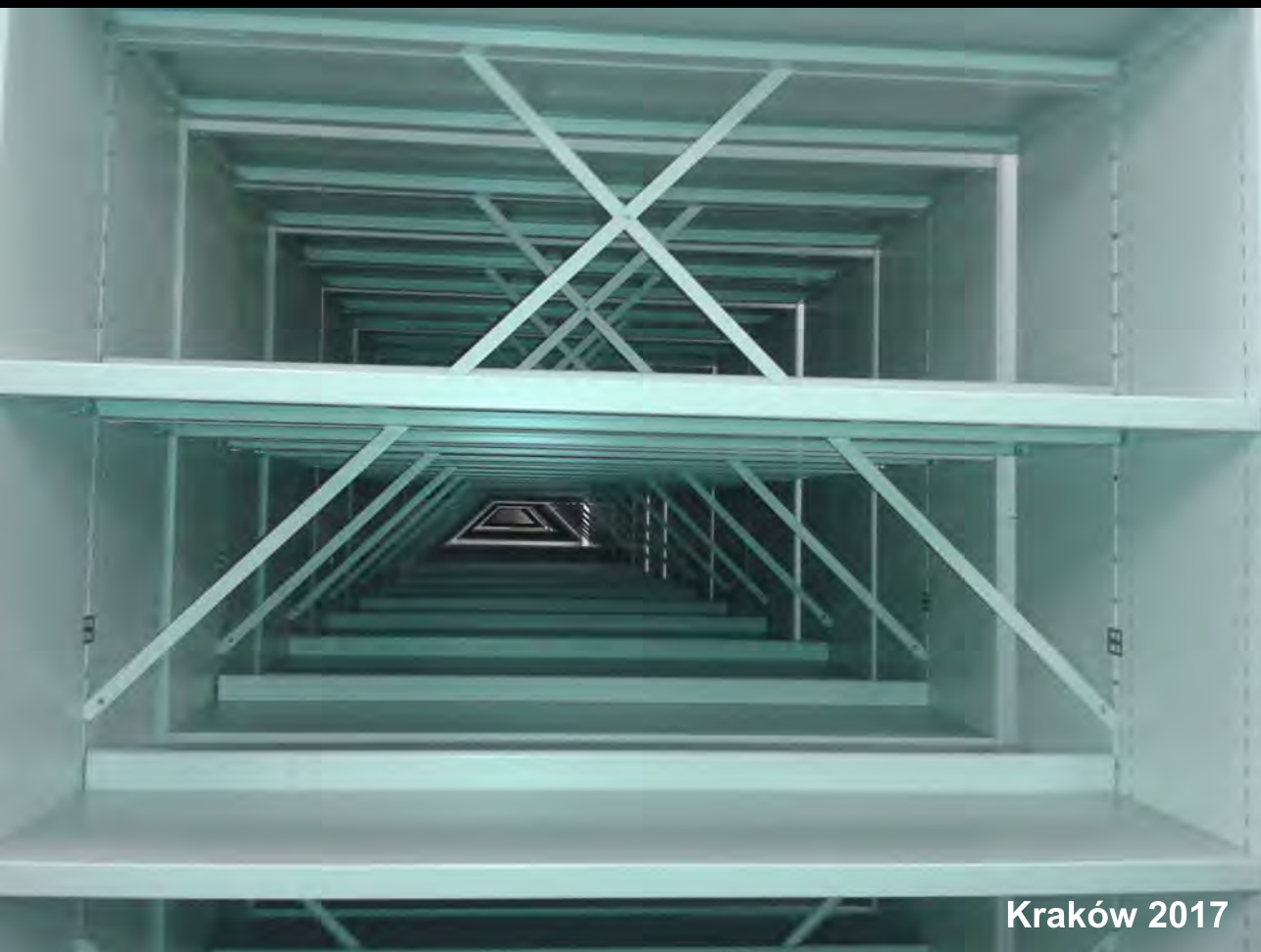
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie
Instytut Bezpieczeństwa i Edukacji Obywatelskiej
KATEDRA KULTURY INFORMACYJNEJ I ZARZĄDZANIA INFORMACJĄ

Walka informacyjna

Uwarunkowania - Incydenty - Wyzwania

Pod redakcją naukową
Hanny Batorowskiej



Kraków 2017

Walka informacyjna

Uwarunkowania
Incydenty
Wyzwania

Monografia poświęcona
Profesorowi Zbigniewowi Kwiasowskiemu
z okazji Jubileuszu 50-lecia pracy zawodowej

Walka informacyjna

Uwarunkowania – Incydenty – Wyzwania

pod redakcją naukową
Hanny Batorowskiej

Wydawca:

Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej
w Krakowie
Instytut Bezpieczeństwa i Edukacji Obywatelskiej
Katedra Kultury Informacyjnej i Zarządzania Informacją

Kraków 2017

Recenzenci:
prof. zw. dr hab. Michał Huzarski
dr hab. Tomasz Wieciech

Redakcja naukowa:
Hanna Batorowska

Korekta:
Emilia Musiał

Skład komputerowy:
Bożena Jarosz, Paulina Motylińska

Projekt okładki
i fotografia na okładce:
Hanna Batorowska

ISBN 978-83-8084-049-2

Wydawca:
Uniwersytet Pedagogiczny w Krakowie
Instytut Bezpieczeństwa i Edukacji Obywatelskiej
Katedra Kultury Informacyjnej i Zarządzania Informacją

Druk i oprawa:
Zespół Poligraficzny UP w Krakowie
30-084 Kraków, ul. Podchorążych 2

Słowo od redaktora

Niniejsza monografia ma charakter szczególny. Powstała z myślą o Panu Profesorze Zbigniewie Kwiasowskim, wieloletnim pracowniku Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie, który w 2017 roku obchodzi Jubileusz 50-lecia pracy zawodowej. Otwiera ją szkic biograficzny przygotowany przez redaktora tomu i *Słowo do Dostojnego Jubilata* autorstwa prof. zw. dr hab. Jerzego Kunikowskiego, uzupełnione bibliografią dorobku naukowego Profesora opracowaną przez Paulinę Motylińską.

Poza częścią jubileuszową, prezentowany tom obejmuje artykuły dotyczące wybranych aspektów walki informacyjnej, ze szczególnym uwzględnieniem charakterystyki środowiska bezpieczeństwa informacyjnego, uwarunkowań wpływających na wykorzystywanie informacji jako narzędzia walki informacyjnej, incydentów potwierdzających wyjątkową skuteczność zastosowania mediów w tej walce oraz refleksji nad możliwością obrony przed kształtowaniem świata w sposób korzystny wyłącznie dla niewielkiej grupy decydentów – ekspertów od manipulacji informacją oraz postawami i zachowaniami obranych przez siebie obiektów (człowieka, organizacji, narodów, całej ludzkości). Ze względu na specyfikę monografii, dwie główne jej części: *Walka informacyjna w kontekście przemian cywilizacyjnych* i *Środowisko bezpieczeństwa informacyjnego* wzbogaca tekst dedykowany Szacownemu Jubilatowi autorstwa Tomasza Jana Biedronia. Scharakteryzowano w nim pracę wydziałów Narodowej Organizacji Wojskowej odpowiedzialnych za pozyskiwanie informacji i jej przekazywanie, akcentując w ten sposób wagę informacji w strukturach obronności kraju, także w okresie historycznym.

Publikacja jest pokłosiem dyskursu naukowego, do którego włączyli się badacze problemów współczesnego świata z Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie: dr hab. Jerzy Świeca, prof. UP – politolog i autor książek z zakresu stosunków międzynarodowych; prof. dr hab. Olga Wasiuta – politolog; prof. dr hab. Sergiusz Wasiuta – specjalista w zakresie międzynarodowych stosunków gospodarczych i polityki społeczno-ekologicznej; dr hab. Andrzej Żebrowski, prof. UP – politolog i autor książek z zakresu walki i wojny informacyjnej; dr hab. Tomasz J. Biedroń, prof. UP – historyk, znawca problemów najnowszej historii Polski; dr hab. Hanna Batorowska, prof. UP – informatolog, badacz problemów kultury informacyjnej i kultury bezpieczeństwa informacyjnego, a także naukowcy z innych ośrodków akademickich: prof. dr hab. Jadwiga Stawnicka – lingwista w WSB w Dąbrowie Górniczej, specjalista od analizy kryminalnej; prof. dr hab. Marian Cieślarczyk – politolog z Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, badacz problemów kultury bezpieczeństwa i obronności; dr hab. Wiesław Babik – informatolog z Uniwersytetu Jagiellońskiego, specjalista w zakresie języków informacyjnych

oraz badacz infosfery, szczególnie z punktu widzenia ekologii informacji. Do dyskursu włączyli się także pracownicy naukowi, mający duże doświadczenie w zakresie edukacji dla bezpieczeństwa i roli mediów w kształtowaniu polityki światowej, do których zaliczyć można: dr Agnieszkę Filipek – politologa z WSP-H w Siedlcach, a z UP w Krakowie: dr Joannę Świątkowską, dr Rafała Klepkę – politologa i medioznawcę, dr Przemysława Mazura – politologa. W wymianie poglądów na temat środowiska bezpieczeństwa informacyjnego wzięli udział także młodzi pracownicy nauki: mgr Mirosław Milkowski, mgr Konrad Harasim, mgr Magdalena Rudnicka, mgr Paulina Polko.

Nie wszystkie dedykowane Panu Profesorowi artykułu zamieszczono w niniejszym tomie. Część z nich opublikowana została w monografii przygotowanej pod redakcją Hanny Batorowskiej i Emilii Musiał pt.: *Bezpieczeństwo informacyjne w dyskursie naukowym* (Kraków: Uniwersytet Pedagogiczny 2017). Tom ten zawiera teksty poświęcone głównie problemom ochrony informacji oraz polityce bezpieczeństwa informacyjnego i stanowi doskonałe uzupełnienie tematyki prezentowanej książki pt.: *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania.*

Przekazując publikację w ręce Czytelników, autorzy mają nadzieję, że zainspiruje ona do dalszych poszukiwań badawczych i własnych refleksji.

Natomiast Panu Profesorowi z okazji Jubileuszu składamy serdeczne podziękowania za wieloletnią współpracę, przyjaźń i wszystko, co zrobił dla dobra Instytutu Bezpieczeństwa i Edukacji Obywatelskiej oraz dla wspólnoty akademickiej i nauki polskiej. Jednocześnie przekazujemy życzenia dobrego zdrowia, sił twórczych i wszelkiej pomyślności.

Hanna Batorowska

SPIS TREŚCI

I
Walka informacyjna w kontekście przemian cywilizacyjnych

II
Środowisko bezpieczeństwa informacyjnego

*

Z historii wojskowości

TABLE OF CONTENTS

I
Information warfare in the context of civilizational changes

II
Information security environment

*

Military history

Hanna Batorowska

Pozostawić ślad

Jubileusz 50-lecia pracy zawodowej Profesora Zbigniewa Kwiasowskiego

Dr hab. prof. UP Zbigniew Kwiasowski większość swojego dorosłego życia poświęcił nauce, edukacji i wychowaniu młodzieży. Znamy go jako wspaniałego organizatora, oddanego nauczyciela i szanowanego członka społeczności akademickiej. Dlatego też dedykujemy książkę zatytułowaną *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania* Panu Profesorowi, który z szeroko pojętego problemu bezpieczeństwa uczynił przedmiot własnych dociekań badawczych oraz publikacji naukowych. Księga ukaże się w 2017 roku, w którym Pan Profesor obchodzi dwa jubileusze: 50-lecia pracy zawodowej oraz 15-lecia kierowania (do roku 2013 Katedrą) Instytutem Bezpieczeństwa i Edukacji Obywatelskiej na Wydziale Pedagogicznym UP w Krakowie.

Dr hab. Zbigniew Tadeusz Kwiasowski, profesor Uniwersytetu Pedagogicznego w Krakowie urodził się 23 lipca 1949 roku w Kaliszu. Tam także ukończył szkołę podstawową i męskie Liceum Ogólnokształcące im. Adama Asnyka. W tym okresie aktywnie działał w Związku Harcerstwa Polskiego oraz był członkiem Aeroklubu Ostrowskiego, gdzie uzyskał dyplom pilota szybowcowego. W latach 1967-1971 studiował w Wyższej Szkole Oficerskiej Wojsk Zmechanizowanych we Wrocławiu, uzyskując tytuł inżyniera-dowódcy. Pierwszym miejscem zawodowej służby wojskowej był 11 pułk 4 Dywizji Zmechanizowanej w Krośnie Odrzańskim, gdzie pełnił służbę na stanowiskach dowódcy plutonu i dowódcy kompanii. W 1973 roku został przeniesiony do Wojskowej Akademii Medycznej (WAM) w Łodzi, pełniąc tam służbę na stanowiskach dowódczych. W 1980 roku ukończył Wydział Filozoficzno-Historyczny Uniwersytetu Łódzkiego z tytułem *magistra pedagogiki*, a rok później, w drodze wyróżnienia, został skierowany do Akademii Sztabu Generalnego w Warszawie, po ukończeniu której w 1984 roku, z tytułem *oficera dyplomowanego*, wrócił do WAM na stanowisko nauczyciela akademickiego. W 1987 roku po obronie rozprawy doktorskiej Rada Wydziału Lekarskiego WAM nadała mu stopień *doktora nauk wojskowych*. W tym też roku ukończył dwuletni, podyplomowy kurs języka niemieckiego dla nauczycieli akademickich na Uniwersytecie Łódzkim.

W 1993 roku sfinalizował Podyplomowe Studium Operacyjno-Strategiczne w Wydziale Strategiczno-Obronnym Akademii Obrony Narodowej (AON). W 1997 roku ukończył Szkołę Praw i Wolności Człowieka oraz warsztaty *Sztuka Negocjacji*

w ramach Helsińskiej Fundacji Praw Człowieka w Warszawie. Rok później jako jeden z dwunastu oficerów Sił Zbrojnych RP uzyskał, po ukończeniu kursu zorganizowanego przez Międzynarodowy Komitet Czerwonego Krzyża z siedzibą w Genewie, uprawnienia instruktora Międzynarodowego Prawa Konfliktów Zbrojnych. W 1998 roku zdał kolokwium habilitacyjne na Wydziale Wojsk Lądowych Akademii Obrony Narodowej, uzyskując stopień naukowy *doktora habilitowanego nauk wojskowych* w specjalności *logistyka*. Od 1999 roku poszerzał swoje naukowe zainteresowania o problematykę bezpieczeństwa narodowego i międzynarodowego, podejmując badania w tym obszarze.

Zgodnie z uchwałą Senatu WAM i decyzją Ministra Obrony Narodowej w 2000 roku został wyznaczony na stanowisko służbowe profesora nadzwyczajnego. W tym samym roku podjął także dodatkowe zatrudnienie w Wyższej Szkole Studiów Międzynarodowych w Łodzi na etacie profesora nadzwyczajnego tej Uczelni, kierując przedmiotem i specjalnością bezpieczeństwo międzynarodowe.

W 2001 roku na wniosek Rektora Akademii Pedagogicznej w Krakowie, decyzją Ministra Obrony Narodowej Profesor Zbigniew Kwiasowski został skierowany do pełnienia służby poza resortem MON na stanowisku profesora nadzwyczajnego i Kierownika Katedry Edukacji Obronnej. Jednostka ta funkcjonuje w Uczelni od 1972 roku i przechodziła wiele zmian organizacyjnych. W momencie przejęcia kierownictwa w Katedrze zatrudnionych było dwanaście osób, w tym czterech samodzielnych pracowników nauki, czterech adiunktów, trzech wykładowców oraz jeden asystent. Jego staraniem w 2005 roku Katedra Edukacji Obronnej stała się samodzielną jednostką organizacyjną Wydziału Pedagogicznego. W jej skład weszły nowo powołane zakłady: Zakład Wychowania Obronnego oraz Zakład Bezpieczeństwa Narodowego. Dalsza aktywność organizacyjna Pana Profesora doprowadziła do rozszerzenia zakresu działań Katedry i stąd nastąpiła zmiana nazwy z Katedry Edukacji Obronnej na Katedrę Bezpieczeństwa i Edukacji Obywatelskiej. W styczniu 2014 roku Katedra przekształcona została w Instytut Bezpieczeństwa i Edukacji Obywatelskiej, którego dyrektorem został dr hab. Zbigniew Kwiasowski, prof. UP. W skład Instytutu weszło pięć katedr: Katedra Bezpieczeństwa Narodowego, Katedra Bezpieczeństwa Społecznego, Katedra Edukacji dla Bezpieczeństwa, Katedra Wychowania Obywatelskiego oraz Katedra Kultury Informacyjnej i Zarządzania Informacją. Przez piętnaście lat kierowania najpierw Katedrą, a następnie Instytutem, zespół pracowników naukowych rozrósł się z 12 do 27 osób, w tym 5 doktorów habilitowanych na etacie profesorów nadzwyczajnych, 20 doktorów na etacie adiunktów i 2 magistrów na etacie asystentów.

Profesor Zbigniew Kwiasowski sprawował także funkcję pełnomocnika Rektora AP ds. przysposobienia obronnego. Powołany zespół pracowników Katedry Edukacji Obronnej przez kilka lat prowadził szkolenia studentów

z piętnastu małopolskich uczelni w zakresie *przysposobienia obronnego*. W dniu 01.02.2007 roku decyzją Ministra Obrony Narodowej Profesor Zbigniew Kwiasowski został zwolniony z zawodowej służby wojskowej i przeniesiony do rezerwy w stopniu pułkownika.

Swoje zainteresowania badawcze Profesor Zbigniew Kwiasowski koncentrował na problematyce całożyciowej edukacji dla bezpieczeństwa nauczycieli, studentów, młodzieży i dzieci. Stąd też tematyka wykładów, publikacji i wystąpień naukowych Pana Profesora oscyluje wokół praw człowieka, międzynarodowego prawa humanitarnego i bezpieczeństwa szkolnego. Przykładem powiązania badań naukowych z praktyką było opracowanie mapy zagrożeń szkolnych na różnych etapach kształcenia. Przesłanie Św. Brata Alberta *Trzeba być dobrym jak chleb* jest mottem Jego postępowania oraz tworzenia kultury szacunku dla człowieka i jego godności. Stąd szczególna troska Pana Profesora o respektowanie zasad dobrego wychowania i używanie w życiu codziennym trzech magicznych słów: *proszę, dziękuję i przepraszam*.

Efektem Jego poszukiwań badawczych jest 166 prac naukowych, w tym 17 publikacji zwartych. Pod jego współredakcją ukazało się 6 numerów roczników *Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate et Educatione Civili.* Idee zawarte w swoim dorobku Profesor Zbigniew Kwiasowski prezentował na 73 międzynarodowych i krajowych konferencjach, zjazdach i sympozjach naukowych. W wielu przypadkach był ich organizatorem lub współorganizatorem.

Od wielu lat współpracował lub współpracuje z różnymi organizacjami i instytucjami naukowymi, wśród których należy wymienić: Komisję Nauk Pedagogicznych PAN Oddział w Krakowie, Komitet Naukowy Serii Wydawniczej *Biblioteka Edukacji dla Bezpieczeństwa* Fundacji AWF w Katowicach, Radę Wydziału Strategiczno-Obronnego Akademii Obrony Narodowej (AON) w Warszawie, Komitet Redakcyjny dwumiesięcznika *Edukacja dla Bezpieczeństwa*, Zespół ds. Upowszechniania Międzynarodowego Prawa Humanitarnego Małopolskiego Zarządu PCK w Krakowie (przewodniczący Zespołu). Od 2002 roku jest także rzeczoznawcą merytoryczno-dydaktycznym MEN w zakresie: kwalifikowania do użytku szkolnego podręczników do przysposobienia obronnego i edukacji dla bezpieczeństwa oraz opiniowania programów nauczania przysposobienia obronnego i edukacji dla bezpieczeństwa.

Pełnił lub nadal pełni wiele funkcji w organach Uniwersytetu Pedagogicznego w Krakowie. Od 2002 roku jest członkiem Rady Wydziału Pedagogicznego, w latach 2008 do 2016 był członkiem Senackiej Komisji ds. Nauki, a w latach 2012-2016 zasiadał w Senacie. Od roku 2012 do 2014 pełnił funkcję prodziekana Wydziału Pedagogicznego. Trzeba zaznaczyć, że każdemu realizowanemu zadaniu Profesor Zbigniew Kwiasowski oddaje się z wielkim zaangażowaniem i pasją, pozostając zawsze otwartym na drugiego człowieka.

Działalność naukowo-badawczą zawsze łączy ściśle z działalnością dydaktyczną i wychowawczą. Bardzo mocno angażuje się w rozwój młodszej kadry naukowej, nie szczędząc im wsparcia oraz organizacyjnej i merytorycznej pomocy. Stworzył klimat umożliwiający twórcze działania badawcze i edukacyjne zespołowi ludzi, którymi kierował i kieruje nadal. Pod jego kierownictwem powstały dwie rozprawy doktorskie, 420 prac magisterskich i 180 licencjackich. Pomimo stawiania wysokich wymagań cieszy się wśród studentów szacunkiem i uznaniem. Jest Autorem dwunastu recenzji doktorskich i habilitacyjnych oraz wielu opinii merytorycznych prac naukowych i podręczników. Koordynował współpracę z University of Chester z Wielkiej Brytanii w ramach badań na temat: *Bezpieczeństwo w edukacji młodzieży*. Prowadził także badania i wykłady na Litwie w ramach programu: *Uczenie się przez całe życie – Erasmus.*

Za swoją dotychczasową działalność Pan Profesor był wielokrotnie wyróżniany i nagradzany, m.in.: Krzyżem Kawalerskim Orderu Odrodzenia Polski, Złotym i Srebrnym Krzyżem Zasługi, Medalem Komisji Edukacji Narodowej, Złotym Medalem za Długoletnią Służbę, Medalami Wojskowej Akademii Medycznej i Uniwersytetu Pedagogicznego, Honorowymi odznakami Polskiego Czerwonego Krzyża II i III stopnia.

Jego pasją są bliskie i dalekie podróże, literatura historyczno-biograficzna, muzyka, a także najnowsze osiągnięcia motoryzacji. Często na wykładach daje przykłady z życia, odwołując się do doświadczeń własnych oraz dwóch córek i czwórki wnucząt. Nie sposób w tak krótkim adresie opisać wszystkie osiągnięcia Pana Profesora – zwłaszcza te w obszarze naukowym, dydaktycznym, jak i organizacyjnym. Życzymy sobie i innym, aby dane nam było jak najdłużej obcować ze wspaniałą osobowością Profesora Zbigniewa Kwiasowskiego oraz doświadczać Jego profesjonalizmu, szczerości w relacjach, otwartości i miłości do ludzi. Panu Profesorowi zaś życzymy długich lat życia w zdrowiu oraz wielu sukcesów w dalszej pracy zawodowej.

Słowo do Dostojnego Jubilata
Profesora dra hab. Zbigniewa KWIASOWSKIEGO

Wielce Szanowny Panie Profesorze

Z wielką radością pragnę złożyć serdeczne życzenia z okazji tak pięknego Jubileuszu Urodzin. Czynię to z wielką radością i satysfakcją, gdyż mam możliwość i szczęście znać osobiście Pana Profesora od wielu lat, gdy rozpocząłem pracę w szkolnictwie wyższym. Z przyjemnością wspominam dziś wielokrotne rozmowy i wymieniane poglądy w ramach wspólnie organizowanych konferencji naukowych, a także dyskusji naukowych na współczesne tematy społeczne, dydaktyczne i wychowawcze.

Pragnę też stwierdzić, że z wielkim zainteresowaniem studiuję, podobnie jak również i inni pracownicy naukowo-dydaktyczni, doktoranci oraz studiująca i ucząca się młodzież niezwykle wartościowe i cenione prace naukowe oraz pozycje książkowe, które poznawałem także wcześniej. Ze szczególnym zainteresowaniem studiuje się takie prace i książki Pana Profesora, związane ściśle z edukacją dla bezpieczeństwa, edukacją obywatelską oraz nowoczesnym a także efektywnym funkcjonowaniem szkoły, jak: *Edukacja wobec wyzwań współczesności (2012); Szkoła nowych czasów (2013); Edukacja dla bezpieczeństwa: teoria i praktyka (2014); Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka (2016); Bezpieczeństwo w nowych czasach (2016).*

Bogaty dorobek i olbrzymi wkład Pana Profesora w rozwój nauk społecznych, zwłaszcza pedagogiki ogólnej i nauk o bezpieczeństwie oraz doskonalenie kadr naukowo-dydaktycznych uznawany i ceniony jest zarówno w Pana Uczelni – Uniwersytecie Pedagogicznym im. Komisji Edukacji Narodowej w Krakowie, jak również i innych uczelniach w Polsce. Wszędzie tam, gdzie rozwijane są społecznie oczekiwane i wysokie wartości obywatelskie młodzieży, w tym umiejętność myślenia i działania w sposób twórczy.

W olbrzymi dorobek Pana Profesora wpisuje się na trwałe inicjowana i rozwijana współpraca z wieloma uczelniami wyższymi, jak też placówkami naukowo-badawczymi w Polsce. Moja uczelnia – Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach jest tego wymownym przykładem. Na trwale w pamięci zachowuję również te słowa, które wypowiadał Pan Profesor wielokrotnie na konferencjach naukowych, wyrażając radość i zadowolenie z rozwoju naszej Uczelni oraz Wydziału Humanistycznego, jak też z efektów kształcenia i rozwoju wspaniałej młodzieży Podlasia.

Chciałbym też podkreślić, że wieloletnie poczynania Pana Profesora zawsze zorientowane były na budowanie uczelnianej rzeczywistości w zakresie przygotowywania obywatelskiego i zawodowego młodzieży, także młodych kadr służących społecznemu bezpieczeństwu i gospodarce narodowej. Jest też Pan Profesor wzorem i autorytetem nie tylko dla młodzieży. Wspaniałym człowiekiem oraz wzorem niezwykłej skromności, pracowitości i wymagalności od siebie, a także niesienia pomocy innym, zwłaszcza młodej kadrze naukowo-dydaktycznej.

W dniu tak pięknego Jubileuszu pragnę życzyć Panu Profesorowi dużo dobra i wszelkiej pomyślności, radości ze wspólnego przebywania z wychowankami, współpracownikami, zwłaszcza z bliskimi, nade wszystko zaś dużo zdrowia i długich lat życia. Proszę również o przyjęcie gratulacji oraz wyrazów najwyższego szacunku i poważania.

Profesor Jerzy Kunikowski

Warszawa – Siedlce, 2017 rok

Paulina Motylińska

Działalność naukowo-badawcza Profesora Zbigniewa Kwiasowskiego

Profesor Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie, Zbigniew Kwiasowski, doktor habilitowany, jako nauczyciel akademicki i pracownik naukowy jest związany z Uniwersytetem Pedagogicznym od wielu lat. Od 2001 r. dr hab. Zbigniew Kwiasowski, prof. Akademii Pedagogicznej kierował działaniami Katedry Edukacji Obronnej na Wydziale Pedagogicznym tej Uczelni. Katedra Edukacji Obronnej, po kilkukrotnych zmianach w strukturze organizacyjnej Wydziału, przekształcona została w 2013 r. w Instytut Bezpieczeństwa i Edukacji Obywatelskiej, którego dyrektorem został dr hab. Zbigniew Kwiasowski, prof. UP. Profesor Kwiasowski pełnił także funkcję Prodziekana Wydziału Pedagogicznego Uniwersytetu Pedagogicznego w latach akademickich 2012/2013 i 2013/2014.

Zbigniew Kwiasowski w 1980 r. uzyskał tytuł magistra, broniąc pracy magisterskiej *Wyposażenie kulturalne domu rodzinnego, a poznawcza i kulturalna aktywność studentów WAM*, napisaną pod kierunkiem dr Janiny Tobery w Zakładzie Pedagogiki Społecznej na Wydziale Filozoficzno-Historycznym Uniwersytetu Łódzkiego. Kolejnym etapem rozwoju naukowego Zbigniewa Kwiasowskiego było opracowanie rozprawy doktorskiej *Zabezpieczenie bojowe. Ochrona i obrona bazy szpitalnej frontu w operacji zaczepnej*, której promotorem był płk doc. dr hab. med. Kazimierz Uglik oraz uzyskanie tytułu doktora nauk wojskowych w 1987 r. na nieistniejącej już obecnie Wojskowej Akademii Medycznej im. gen. dyw. Bolesława Szareckiego w Łodzi. W jedenaście lat po uzyskaniu tytułu doktora, Zbigniew Kwiasowski przedstawił rozprawę habilitacyjną *Obrona i ochrona jednostek i urządzeń logistycznych w operacji obronnej*, uzyskując 28 października 1998 stopień doktora habilitowanego nauk wojskowych ze specjalnością logistyka na Wydziale Wojsk Lądowych Akademii Obrony Narodowej w Warszawie.

Uzyskane tytuły w dziedzinie nauk wojskowych oraz tematyka podejmowana w rozprawach, zarówno doktorskiej, jak i habilitacyjnej, wskazują na zakres zainteresowań naukowo-badawczych dr hab. Zbigniewa Kwiasowskiego, prof. UP. Już od pierwszych publikacji widać konsekwencję w doborze tematyki badawczej. Pierwsze artykuły w karierze naukowej Profesora, m.in. *Wybrane problemy przechodzenia oddziału z natarcia do obrony* oraz *Specyfika prowadzenia działań przez OGN armii na północnonadmorskim kierunku operacyjnym* opublikowane zostały w czasopiśmie „Myśl Wojskowa" na kilka lat przed uzyskaniem tytułu naukowego doktora. W późniejszych pracach

opublikowanych na przełomie lat 80. i 90. XX w. można zauważyć zainteresowanie Profesora tematyką bezpieczeństwa w kontekście służby zdrowia i zabezpieczenia medycznego; wśród przykładów takich prac można wymienić m.in. artykuły *Rola i miejsce starszego lekarza pułku w czasie wypracowywania decyzji i pracy sztabu*, *Wybrane problemy ochrony prawnej służby zdrowia i personelu duchownego Sił Zbrojnych RP*, *Wybrane problemy zabezpieczenia medycznego działań obronnych na obszarze okręgu wojskowego (OW)*, *Zagrożenie punktów opatrunkowych i szpitali w warunkach działań wojennych* lub artykuł *Wpływ środowiska geograficznego na zabezpieczenie medyczne wojsk działających w warunkach szczególnych* napisany wspólnie *z* Wiktorem Żukocińskim.

Wraz z objęciem przez Profesora Kwiasowskiego funkcji kierownika Katedry Edukacji Obronnej na Uniwersytecie Pedagogicznym tematyka jego prac naukowo-badawczych zaczęła ewoluować w stronę edukacji dla bezpieczeństwa. Efektem pracy naukowej w tym zakresie były artykuły dotyczące m.in. kształcenia nauczycieli: *Bezpieczeństwo w kształceniu nauczycieli*, *Optymalizacja jakości kształcenia nauczycieli przysposobienia obronnego* lub *Kształcenie nauczycieli przysposobienia obronnego w zmieniającej się rzeczywistości edukacyjnej*. Wśród prac w nurcie pedagogicznym wyróżnić można także artykuły dotyczące bezpieczeństwa młodzieży (np. *Młodzież wobec wyzwań cywilizacji przełomu – wybrane problemy*) oraz bezpieczeństwa szkolnego (np. *Bezpieczeństwo szkolne – kontekst edukacyjny*). Tematyka edukacji dla bezpieczeństwa widoczna jest także w pracach Profesora opublikowanych w ciągu ostatnich kilku lat – m.in. w 2012 r. Zbigniew Kwiasowski, razem z Klaudią Cendą-Miedzińską zredagował tom monografii *Edukacja dla bezpieczeństwa wobec wyzwań współczesności*. Profesor Kwiasowski jest także kierownikiem zadania badawczego *Społeczny i edukacyjny wymiar bezpieczeństwa* realizowanego w Instytucie Bezpieczeństwa i Edukacji Obywatelskiej Uniwersytetu Pedagogicznego w Krakowie.

Zbigniew Kwiasowski był także promotorem rozpraw doktorskich w zakresie m.in. działań humanitarnych Polskich Kontyngentów Wojskowych oraz więziennictwa polskiego i jego znaczenia w polityce bezpieczeństwa. Wśród jego doktorantów znajdują się Bogdan Dobrowolski, Malina Kaszuba i Paweł Góra. Działalność Profesora obejmuje także recenzje kilkunastu prac doktorskich i habilitacyjnych dotyczących tematyki m.in. zabezpieczenia logistycznego, kompetencji interpersonalnych dowódców związków taktycznych i oddziałów, wojskowej służby zdrowia, wsparcia samoobrony w ochronie ludności oraz polityki bezpieczeństwa lokalnego. Profesor recenzował prace doktorskie Mirosława Zielony, Marka Kubińskiego, Zbigniewa Pietrasa, Janusza Ropskiego, Wojciecha Nowaka, Romana Krawczyńskiego, Józefa Jedynaka, Tadeusza Kurka, Doroty Łęgockiej-Bartczak, Anny Antczak i Marka Barć, a także rozprawy habilitacyjne Włodzimierza Wysockiego i Marka Kubińskiego.

W dorobku Zbigniewa Kwiasowskiego znajdują się także recenzje monografii (m.in. recenzja książki *Bezpieczeństwo lokalne w opiniach mieszkańców Tarnobrzega* pod redakcją Jana Dziubińskiego i in.; recenzja książki *Karta Praw Podstawowych UE: nowa szansa dla praw człowieka?* pod redakcją Wiesława Wacławczyka oraz artykułów opublikowanych w *Zeszytach Naukowych Małopolskiej Szkoły Wyższej w Brzesku* w 2010 r.). Profesor był również redaktorem czasopisma *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili* wydawanego przez Instytut Bezpieczeństwa i Edukacji Obywatelskiej Uniwersytetu Pedagogicznego we współpracy z Wydawnictwem Naukowym Uniwersytetu Pedagogicznego.

Profesor Zbigniew Kwiasowski brał także czynny udział w licznych konferencjach naukowych, zarówno krajowych, jak i międzynarodowych. Profesor aktywnie uczestniczył w konferencjach organizowanych m.in. przez Wojskową Akademię Medyczną w Łodzi, Akademię Obrony Narodowej w Warszawie, Politechnikę Łódzką, Kuratorium Oświaty w Krakowie i Urząd Miasta Krakowa, Akademię Podlaską w Siedlcach, Polską Akademię Nauk, a także konferencjach innych ośrodków naukowych m.in. z Warszawy, Bydgoszczy, Łodzi, Katowic, Nowego Sącza i Krakowa. Tematyka podejmowana przez Profesora w referatach konferencyjnych koncentruje się wokół edukacji dla bezpieczeństwa, bezpieczeństwa szkolnego, pracy nauczyciela przysposobienia obronnego oraz zagrożeń XXI wieku. Warto wspomnieć także o konferencjach naukowych i branżowych organizowanych lub współtworzonych przez Profesora Kwiasowskiego; wśród licznych przykładów można wyróżnić członkostwo Profesora w komitecie naukowym m.in. *Międzynarodowej Konferencji Naukowej: Edukacja dla bezpieczeństwa* zorganizowanej w 2003, przewodniczenie Komitetowi Naukowemu *V Ogólnopolskiej Konferencji Naukowej: Kształcenie nauczycieli przysposobienia obronnego w polskich uczelniach – stan obecny i perspektywy* w 2005 r. oraz współorganizowanie *Konferencji Naukowej z cyklu Człowiek w świecie informacji nt.: Kultura informacyjna w ujęciu interdyscyplinarnym* z 2015 r.

Profesor Kwiasowski aktywnie uczestniczy również w działalności organizacji i instytucji naukowych i edukacyjnych, angażując się w ich prace. Od 2011 r. jest członkiem Komisji Nauk Pedagogicznych Polskiej Akademii Nauk Oddział w Krakowie, od 2003 r. współpracuje z Małopolskim Oddziałem Okręgowym Polskiego Czerwonego Krzyża w Krakowie, przy czym od 2011 r. jest także przewodniczącym Zespołu ds. Upowszechniania Międzynarodowego Prawa Humanitarnego Małopolskiego Oddziału Okręgowego Polskiego Czerwonego Krzyża. W 2002 r. został także upoważniony do pełnienia roli rzeczoznawcy merytoryczno-dydaktycznego Ministerstwa Edukacji Narodowej do kwalifikowania do użytku szkolnego podręczników do przysposobienia obronnego i edukacji dla bezpieczeństwa oraz do opiniowania programów nauczania przysposobienia

obronnego i edukacji dla bezpieczeństwa oraz programów ścieżki edukacyjnej obrona cywilna. Wśród opiniowanych przez Profesora Kwiasowskiego podręczników można wymienić m.in. *Przysposobienie obronne: podręcznik dla liceum ogólnokształcącego, liceum profilowanego i technikum*, cz. 2 Mariusza Noniewicza, Anny Nowak i Zbigniewa Smutek z 2006 r., *Edukacja dla bezpieczeństwa: podręcznik dla gimnazjum* Mieczysława Borowieckiego, Zbigniewa Pytasz i Edwarda Rygała z 2009 r. oraz *Edukacja dla bezpieczeństwa. Podręcznik. Gimnazjum* Krzysztofa Izbickiego i Łukasza Wrycz-Rekowskiego z 2010 r. Profesor opracował także recenzje merytoryczne programów nauczania oraz recenzje podręczników. Do recenzowanych przez Profesora programów nauczania można włączyć *Program nauczania przysposobienia obronnego dla szkół ponadgimnazjalnych* autorstwa Mieczysława Borowieckiego, Zbigniewa Pytasz i Edwarda Rygała z 2003 r. oraz *Program szkolny „Klocki Autonomiczne"* opracowany przez zespół Gdańskiej Fundacji Oświatowej pod kierunkiem Katarzyny Hall z 2002 r.

Podsumowując Profesor Kwiasowski jest autorem kilkudziesięciu artykułów naukowych, redaktorem wielu monografii i czasopism naukowych, czynnie uczestniczył także w blisko 80 konferencjach i sympozjach. W dorobku Profesora znalazło się także kilkanaście skryptów i podręczników akademickich, promotorstwo trzech rozpraw doktorskich oraz liczne recenzje i opinie merytoryczne, w tym m.in. prac doktorskich i habilitacyjnych oraz podręczników i programów nauczania. Jubileusz 50-lecia pracy zawodowej dra hab. Zbigniewa Kwiasowskiego, prof. UP skłania do zaprezentowania wykazu Jego osiągnięć naukowo-dydaktycznych.

W Y K A Z

OSIĄGNIĘĆ W PRACY NAUKOWO–BADAWCZEJ

prof. nadzw. dra hab. Zbigniewa Kwiasowskiego

Rozprawa magisterska, doktorska, habilitacyjna

Praca magisterska: Kwiasowski Z. (1980). *Wyposażenie kulturalne domu rodzinnego, a poznawcza i kulturalna aktywność studentów WAM*. Praca napisana pod kierunkiem dr Janiny Tobery, Zakład Pedagogiki Społecznej, Wydział Filozoficzno-Historycznym Uniwersytetu Łódzkiego, Łódź 1980, 120 s.

Rozprawa doktorska: Kwiasowski Z. (1987) *Zabezpieczenie bojowe (ochrona i obrona) bazy szpitalnej frontu w operacji zaczepnej*. Praca napisana pod

kierunkiem płk doc. dra hab. med. Kazimierza Uglika, Wojskowa Akademia Medyczna w Łodzi, nr 08724.

Rozprawa habilitacyjna: Kwiasowski Z. (1998) *Obrona i ochrona jednostek i urządzeń logistycznych w operacji obronnej*, Akademia Obrony Narodowej w Warszawie.

Monografie (redakcja)

Kwiasowski Z. red. (2007) *Kształcenie nauczycieli przysposobienia obronnego w polskich uczelniach: stan obecny i perspektywy*. Kraków: Wydaw. Naukowe Akademii Pedagogicznej, 188 s. ISBN 978-83-7271-428-2.

Kwiasowski Z., Cenda-Miedzińska K. red. (2012) *Edukacja dla bezpieczeństwa wobec wyzwań współczesności*. Kraków: Wydaw. Naukowe Uniwersytetu Pedagogicznego, 244 s. ISBN 978-83-7271-711-5.

Kwiasowski Z., Campion. M. red. (2013) *Polska w Unii Europejskiej: wybrane aspekty polityki bezpieczeństwa w działalności edukacyjno-wychowawczej*. Kraków: Wydaw. Naukowe Uniwersytetu Pedagogicznego, 127 s. ISBN 978-83-7271-778-8.

Batorowska H., Kwiasowski Z. red. (2016) *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka. T.2*. Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Instytut Bezpieczeństwa i Edukacji Obywatelskiej, Katedra Kultury Informacyjnej i Zarządzania Informacją, 336 s. ISBN 978-83-7271-943-0.

Kwiasowski Z., Pabis-Cisowska K., Pietrzyk M. red. (2016) Bezpieczeństwo w nowych czasach. Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, 238 s. ISBN 978-83-8084-030-0.

Skrypty akademickie i podręczniki

Skrypt akademicki: Kwiasowski Z. (1992) *Charakterystyka zagrożenia oraz zasadnicze przedsięwzięcia militarnej obrony obszaru kraju*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Problemowy materiał studyjny: Kwiasowski Z. (1993) *Wybrane problemy realizacji zadań ochrony i obrony etapów ewakuacji medycznej w strategicznej operacji obronnej*. Warszawa: Wydaw. Akademii Obrony Narodowej.

Skrypt akademicki: Kwiasowski Z. (1994) *Geografia wojenna z elementami wojskowej geografii medycznej*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Skrypt akademicki: Kwiasowski Z. (1996) *Logistyka. Część I (pododdziały)*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Skrypt akademicki: Kwiasowski Z. (1996) *Logistyka. Część II (oddział, ZT)*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Skrypt akademicki: Kwiasowski Z. (1996) *Organizacja oraz ogólne zasady użycia BZ (BPanc) w walce*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Skrypt akademicki: Kwiasowski Z. (1996) *Zasady osiąganie wyższych stanów gotowości bojowej (WSGB) i mobilizacyjnego rozwinięcia J.W.* Łódź: Wydaw. Wojskowej Akademii Medycznej.

Problemowy materiał studyjny: Kwiasowski Z., Bieńkowski W. (1997) *Wybrane problemy zabezpieczenia inżynieryjnego Wojsk Lądowych SZ RP*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Kwiasowski Z. (1997) *Struktura organizacyjna oraz ogólne zasady użycia pododdziałów Wojsk Lądowych SZ RP w działaniach taktycznych*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Podręcznik akademicki: Kwiasowski Z. (1997) *Zabezpieczenie logistyczne pododdziałów, oddziałów i związków taktycznych Wojsk Lądowych w walce*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Studium: Kwiasowski Z. (1998) *Ochrona i obrona systemu medycznego korpusu w operacji obronnej*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Skrypt akademicki. Kwiasowski Z. (1998) *Podstawowy sprzęt łączności oraz wybrane problemy organizacji łączności Wojsk Lądowych SZ RP*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Studium: Kwiasowski Z., Szwedo J. (1998) *Wybrane problemy organizacji łączności Wojsk Lądowych SZ RP*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Studium: Kwiasowski Z. (1998) *Wybrane problemy organizacji i funkcjonowania Systemu Obronnego RP*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Problemowy materiał studyjny: Kwiasowski Z. (1998) *Charakterystyka zagrożeń obszaru Rzeczypospolitej Polskiej*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Podręcznik akademicki: Kwiasowski Z., Gaszyński W. (1999) *Medycyna katastrof*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Studium: Kwiasowski Z. (2000) *Wybrane problemy geografii wojennej Polski*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Studium: Kwiasowski Z. (2000). *Dywizja zmechanizowana w działaniach taktycznych – obrona*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Redakcja czasopisma

Kwiasowski Z., Biedroń T.J. red. (2010) *Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate et Educatione Civili I*, nr 76. ISSN 1689-9903.

Kwiasowski Z., Biedroń T.J. red. (2012) *Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate et Educatione Civili II*, nr 109. ISSN 2082-0917.

Kwiasowski Z., Biedroń T.J. red. (2013) *Annales Universitatis Paedagogicae Cracoviensis, Studia de Securitate et Educatione Civili III*, nr 144. ISSN 2082-0917.

Biedroń T.J., Kwiasowski Z. red. (2014) *Annales Universitas Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili IV*, nr 166, ISSN 2082-0917.

Artykuły w czasopismach

1984

Kwiasowski Z. (1984) *Wybrane problemy przechodzenia oddziału z natarcia do obrony*. „Myśl Wojskowa", nr 6/48.

1986

Kwiasowski Z. (1986) *Specyfika prowadzenia działań przez OGN armii na północno-nadmorskim kierunku operacyjnym*. „Myśl Wojskowa", nr 3/86.

1987

Kwiasowski Z. (1987) *Ochrona wojskowych obiektów sanitarnych i personelu sanitarnego w świetle postanowień międzynarodowego prawa konfliktów zbrojnych*. „Biuletyn Wojskowej Akademii Medycznej", nr 2/87, s. 149-165.

Kwiasowski Z. (1987) *Specyfikacja prowadzenia działań przez OGM Armii na północno-nadmorskim kierunku operacyjnym*. „Myśl Wojskowa" (tajna), nr 3, s. 23-38.

Kwiasowski Z. (1987) *Sposoby i możliwości niszczenia SD npla przez zgrupowanie wojsk działających w głębi operacyjnej*. „Myśl Wojskowa" (tajna).

Kwiasowski Z. (1987) *Rola i miejsce starszego lekarza pułku w czasie wypracowania decyzji i pracy sztabu*. „Biuletyn Wojskowej Akademii Medycznej".

1994

Kwiasowski Z. (1994) *Wybrane problemy ochrony prawnej służby zdrowia i personelu duchownego Sił Zbrojnych RP*. „Myśl Wojskowa", nr 2, s. 164-170.

1995

Kwiasowski Z., Lasota B. (1995) *Publiczna służba zdrowia jako element układu pozamilitarnego systemu obronnego państwa*. „Myśl Wojskowa", nr 2, s. 89-93.

1996

Kwiasowski Z., Dójczyński M. (1996) *Wybrane problemy zabezpieczenia medycznego działań obronnych na obszarze okręgu wojskowego (OW)*. „Myśl Wojskowa" (tajna), nr 2, s. 41–56.

Kwiasowski Z., Dójczyński M. (1996) *Straty sanitarne na współczesnym polu walki*. „Lekarz Wojskowy", nr 1, s. 14-20.

Kwiasowski Z. (1996) *Egzamin oficerski w korpusie osobowym Służby Zdrowia*. „Myśl Wojskowa", nr 1, s. 90-91.

Kwiasowski Z., Żukociński W. (1996) *Wpływ środowiska geograficznego na zabezpieczenie medyczne wojsk działających w warunkach szczególnych*. „Lekarz Wojskowy", nr 1, s. 6-13.

Kwiasowski Z., Kocur J. (1996) *Uwarunkowania zaburzeń psychicznych u żołnierzy*. „Myśl Wojskowa", nr 5, s. 120-124.

1997

Kwiasowski Z., Kuczmański Z. (1997) *Pole walki dziś i jutro*. „Myśl Wojskowa", nr 6, s. 8.

1998

Kuczmański Z., Kwiasowski Z. (1998) *Rozwój działań powietrzno-lądowych*. „Zeszyty Naukowe Akademii Obrony Narodowej", nr 1(30), s. 111-122.

Kuczmański Z., Kwiasowski Z. (1998) *Możliwości tworzenia zgrupowań (oddziałów) areomobilnych*. „Zeszyty Naukowe Akademii Obrony Narodowej", nr 1(30), s. 123-130.

Kwiasowski Z. (1998) *Zagrożenie punktów opatrunkowych i szpitali w warunkach działań wojennych*. „Kwartalnik Ortopedyczny", nr 3.

Kwiasowski Z. (1998) *Organizacja i zadania SZ RP w programie „Armia 2012"*. „Biuletyn 10 Wojskowego Szpitala Klinicznego w Bydgoszczy", nr 3, s. 43-48.

Kwiasowski Z., Kuczmański Z. (b.d.) *Piechota na przestrzeni wieków*. „Przegląd Wojsk Lądowych".

2000

Kwiasowski Z., Bąkowski K. (2000) *System zabezpieczenia logistycznego wojsk według zasad NATO*. „Myśl Wojskowa" (tajna), nr 2, s. 92-101.

2001

Kwiasowski Z. (2001) *Wybrane aspekty zagrożenia związane ze stosowaniem w działaniach militarnych broni zawierającej zubożony uran*. „VALETUDINARIA – Postępy Medycyny Klinicznej i Wojskowej, Kwartalnik Wojskowego Szpitala Klinicznego w Bydgoszczy", T. 6, nr 3–4.

2002

Kwiasowski Z., Leszczyński W. (2002) *Elementy geograficzne wpływające na funkcjonowanie wojskowej służby zdrowia*. „Przegląd Wojskowo–Medyczny, vol. 44, nr 3-4, s. 287-294.

2003

Kwiasowski Z. (2003) *Bezpieczeństwo w programie kształcenia Katedry Edukacji Obronnej Akademii Pedagogicznej w Krakowie*. „Edukacja dla Bezpieczeństwa", nr 2(13), s. 29-31.

2004

Kwiasowski Z., Durmała T. (2004) *Sesja naukowa Katedry Edukacji Obronnej Akademii Pedagogicznej w Krakowie*. „Edukacja dla Bezpieczeństwa", nr 1(17), s. 34-36.

Kwiasowski Z. (2004) *Problematyka bezpieczeństwa w edukacji nauczycielskiej*. „Podlaskie Zeszyty Pedagogiczne", nr 10, s. 235-242.

2005

Kwiasowski Z. (2005) *30 lat Katedry Edukacji Obronnej Akademii Pedagogicznej w Krakowie*. „Annales Academiae Paedagogicae Cracoviensis. Studia ad Educationem Defensorami Pertinentia", nr 24, z. 1, s. 5-7.

Kwiasowski Z. (2005) *Z doświadczeń Katedry Edukacji Obronnej Akademii Pedagogicznej im. KEN w Krakowie*. „Edukacja dla Bezpieczeństwa", nr 4(25), s. 24-26.

2006

Kwiasowski Z. (2006) *Optymalizacja jakości kształcenia nauczycieli przysposobienia obronnego*. „Edukacja dla Bezpieczeństwa", nr 1, s. 29-32.

Kwiasowski Z. (2006) *Organy samorządu terytorialnego w zarządzaniu kryzysowym*. „Roczniki Geomatyki", t. 4, z.1, s. 29-36.

2007

Kwiasowski Z. (2007) *Monitoring to nie sposób na ucznia*. „Polska Gazeta Krakowska", nr 250, 25.10.2007, s. 26.

Kwiasowski Z. (2007) *Problem bezpieczeństwa człowieka w edukacji nauczycielskiej*. „Konspekt" nr 2(29), s. 10-13.

2010

Kwiasowski Z. (2010) *Bezpieczeństwo szkoły w opinii szkolnych podmiotów wychowania*. „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civilil", nr 76, z. 1, strony 51-61.

Kwiasowski Z. (2010) *Nauczyciel wobec wyzwań współczesności*. „Hejnał Oświatowy", nr 12/98, s. 4-6.

Artykuły w monografiach

1995

Kwiasowski Z. (1995) *Godność stanu i zawodu lekarza wojskowego. Postulaty i rzeczywistość*. W: *Etos oficerski w procesie przemian. Materiały z sympozjum naukowego*. Warszawa: Wydaw. Wojskowej Akademii Technicznej.

1996

Kwiasowski Z. (1996) *Transformacja Sił Zbrojnych RP, a zmiany w procesie kształcenia ogólnowojskowego kadr Wojskowej Służby Zdrowia*. W: Kucharski M. (red.), *Przygotowanie studentów uczelni wojskowych i oficerów do pracy szkoleniowo-wychowawczej: Materiały z Sympozjum Naukowego, 11-12 kwietnia 1996 r*. Warszawa: Wydaw. Akademii Obrony Narodowej, s. 154-160.

2002

Kwiasowski Z., Mazur S. (2002) *Terroryzm na progu XXI wieku*. W: Budzowski K. (red.) *Administracja, zarządzanie i handel zagraniczny w warunkach integracji: materiały konferencyjne - zarządzanie bezpieczeństwem*. Kraków: na zlec.

Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego: Krakowskie Towarzystwo Edukacyjne, s. 190-200.

2003

Kwiasowski Z. (2003) *Bezpieczeństwo w edukacji*. „Biuletyn Pokonferencyjny Zarządu Głównego Towarzystwa Wiedzy Obronnej, ", nr 3-4.

2004

Kwiasowski Z. (2004) *Bezpieczeństwo w kształceniu nauczycieli*. W: Ożóg-Radew M., Rosa R. (red.), *Bezpieczeństwo i prawa człowieka, tom II Edukacja dla bezpieczeństwa i praw człowieka*. Siedlce: Wydaw. Akademii Podlaskiej.

Kwiasowski Z. (2004) *Definicja terroryzmu, jego narodziny, rozwój i podział. Skutki działalności terrorystycznej*. W: *Materiały z konferencji na temat: Współdziałanie organów administracji szczebla wojewódzkiego w zakresie przeciwdziałania zagrożeniom wynikających z aktu terroryzmu*. Kraków: Małopolski Urząd Wojewódzki, Komenda Wojewódzkiej Państwowej Straży Pożarnej, Towarzystwo Wiedzy Obronnej oddział przy Wojewódzkim Sztabie Wojskowym w Krakowie, 20.04.2004.

2005

Kwiasowski Z. (2005) *Wybrane aspekty bezpieczeństwa szkolnego*. W: Kuźma J., Morbitzer J. (red.), *Edukacja – szkoła – nauczyciel: promowanie rozwoju dziecka*. Kraków: Wydaw. Naukowe Akademii Pedagogicznej, s. 105-109.

Kwiasowski Z. (2005) *Wybrane aspekty zagrożeń na progu XXI wieku*. W: Rosa R. (red.), *Bezpieczeństwo i prawa człowieka w badaniach naukowych i edukacji, tom I Teoretyczne problemy bezpieczeństwa i praw człowieka*. Siedlce: Wydaw. Akademii Podlaskiej.

Kwiasowski Z., Durmała T. (2005) *Pozamilitarne zagrożenia u progu XXI wieku*. W: Maliszewski W.J. (red.), *Bezpieczeństwo człowieka i zbiorowości społecznych*. Bydgoszcz: Wydaw. Akademii Bydgoskiej im. Kazimierza Wielkiego, s. 25-34.

2006

Kwiasowski Z. (2006) *Bezpieczeństwo i pokój w edukacji szkolnej*. W: Leżańska W., Jałmużna T. (red.), *Pokój jako przedmiot badań społecznych i pedagogicznych*. Łódź : Wyższa Szkoła Informatyki, s. 187-196.

2007

Kwiasowski Z. (2007) *Kształcenie nauczycieli przysposobienia obronnego w zmieniającej się rzeczywistości edukacyjnej*. W: Kwiasowski Z. (red.), *Kształcenie*

nauczycieli przysposobienia obronnego w polskich uczelniach : stan obecny i perspektywy. Kraków: Wydaw. Naukowe Akademii Pedagogicznej, s. 67-75.

Kwiasowski Z. (2007) *Edukacja dla bezpieczeństwa wobec wyzwań cywilizacji przełomu*. W: Cudowska A., Kunikowski J. (red.), *Czynić świat bardziej bezpiecznym: księga jubileuszowa dedykowana profesorowi doktorowi habilitowanemu Ryszardowi Rosie. T. 2*. Siedlce: Wydaw. Akademii Podlaskiej, s. 23-29.

Kwiasowski Z. (2007) *Wybrane problemy bezpieczeństwa młodzieży*. W: Kowalczyk-Jamnicka M., Sołtysiak T. (red.), *Zjawiska patologiczne wśród młodzieży i możliwości przeciwdziałań*. Bydgoszcz: Wydaw. Uniwersytetu Kazimierza Wielkiego, s. 25-35.

Kwiasowski Z. (2007) *Młodzież wobec wyzwań cywilizacji przełomu: wybrane problemy*. W: Zacłona Z. (red.), *Nauczyciel w rzeczywistości globalnej i lokalnej*. Nowy Sącz: Państwowa Wyższa Szkoła Zawodowa, s. 49-57.

2008

Kwiasowski Z. (2008) *Przygotowanie nauczycieli Przysposobienia Obronnego do wykonywania zawodu*. W: Skrabacz A. (red.), *Takie będą Rzeczypospolite, jakie ich młodzieży chowanie: spuścizna korpusu kadetów w procesie kształcenia obronnego młodzieży - stan i perspektywy: materiał pokonferencyjny*. Warszawa: Centralna Biblioteka Wojskowa im. Józefa Piłsudskiego, s. 42-50.

2009

Kwiasowski Z. (2009) *Prawo do wolności i bezpieczeństwa osobistego*. W: Koba L., Wacławczyk W. (red.), *Prawa człowieka : wybrane zagadnienia i problemy*. Warszawa: Oficyna Wolters Kluwer Business, s. 199-211.

Kwiasowski Z. (2009) *Młodzież wobec edukacji dla bezpieczeństwa*. W: Rosa R., Bocian B. (red.), *Edukacja do demokracji, bezpieczeństwa i praw człowieka w początkach XXI wieku*. Siedlce: Wydaw. Akademii Podlaskiej, s. 207-216.

2010

Kwiasowski Z. (2010) *Wybrane problemy bezpieczeństwa szkolnego*. W: Kalinowski R. (red.), *Bezpieczeństwo i obronność w świetle współczesnych wyzwań i potrzeb: ujęcie ogólne*. Siedlce: Wydaw. Akademii Podlaskiej, s. 119-127.

Kwiasowski Z. (2010) *Bezpieczeństwo szkolne: kontekst edukacyjny*. W: Sołtysiak T., Nowakowska A. (red.), *Młode pokolenie: ofiary czy sprawcy przemocy?* . Bydgoszcz: Wydaw. Uniwersytetu Kazimierza Wielkiego, s. 133-142.

2011

Kwiasowski Z. (2011) *Wokół autorytetu nauczyciela*. W: Jarmoch E., Kunikowski J. (red.), *Filozofia życia: w poszukiwaniu mądrości, piękna i dobra: księga jubileuszowa Profesora Ryszarda Rosy w 70. rocznicę urodzin. T. 1*. Siedlce, Drohiczyn: Wydaw. Uniwersytetu Przyrodniczo-Humanistycznego, s. 373-382.

2012

Kwiasowski Z. (2012) *Nauczyciel wobec wyzwań współczesnej szkoły*. W: Kwiasowski Z., Cenda-Miedzińska K. (red.), *Edukacja dla bezpieczeństwa wobec wyzwań współczesności*. Kraków: Wydaw. Naukowe Uniwersytetu Pedagogicznego, s. 8-19.

2013

Kwiasowski Z. (2013) *Szkoła nowych czasów*. W: Kwiasowski Z., Campion M. (red.), *Polska w Unii Europejskiej: wybrane aspekty polityki bezpieczeństwa w działalności edukacyjno-wychowawczej*. Kraków: Wydaw. Naukowe Uniwersytetu Pedagogicznego, s. 116-126.

2014

Kwiasowski Z. (2014) *Znaczenie edukacji dla bezpieczeństwa w wychowaniu obywatelskim*. W: Skrabacz A., Kanarski L. (red.), *Edukacja dla bezpieczeństwa: teoria i praktyka*. Warszawa: Wojskowe Centrum Edukacji Obywatelskiej, s. 81-95.

2016

Kwiasowski Z. (2016) *Znaczenie Internetu w wychowaniu*. W: Batorowska H., Kwiasowski Z. (red.), *Kultura informacyjna w ujęciu interdyscyplinarnym: teoria i praktyka. T. 2.* Kraków: Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Instytut Bezpieczeństwa i Edukacji Obywatelskiej, Katedra Kultury Informacyjnej i Zarządzania Informacją, s. 176-187.

Prace nieprzeznaczone do druku

Kwiasowski Z. (1984) Praca dyplomowa: *Prowadzenie działań przez OGM Armii na nadmorskim kierunku operacyjnym*. Praca tajna, napisana pod kierunkiem ppłka dra Ryszarda Sachaja. Akademia Sztabu Generalnego Wojska Polskiego nr 042306. Warszawa 1984 (41 s. + 10 zał.).

Kwiasowski Z. (1985) *Natarcie pułku zmechanizowanego z rejonu położonego w bezpośredniej styczności z nieprzyjacielem*. Ćwiczenia dla IV RS. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Kwiasowski Z. (1986) *Ćwiczenie ogólnoakademickie pod kryptonimem „LANCET-86”*. Łódź: Wydaw. Wojskowej Akademii Medycznej.

Lasota B., Śmigielski J., Kwiasowski Z., Polański A. (1989) *Zadanie Badawcze Szefostwa Służby Zdrowia Sztabu Generalnego WP A.01.O1. Wykorzystanie stacjonarnych zakładów leczniczych i rozwijanie Baz Szpitalnych Frontu na ZTDW, ze szczególnym uwzględnieniem Środkowoeuropejskiego Rejonu Strategicznego. Kryptonim „Rusałka”*. Łódź: Wojskowa Akademia Medyczna, 112 s.

Kwiasowski Z. (1996) *Przygotowanie i prowadzenie operacji obronnej korpusu. Sprawozdanie z pracy badawczej pk.: „Eskulap - 96”*. Łódź: Wojskowa Akademia Medyczna 14.05.1996.

Kwiasowski Z. (1996) *Charakterystyka współczesnego pola walki. Wykład na odprawie kierowniczej kadry Służby Zdrowia WP*. Łódź: Wojskowa Akademia Medyczna, 15.05.1996.

Kwiasowski Z. (1997) *Zadania Badawcze MON pk.: „α - K”. Gospodarka obronna: Wykorzystanie zasobów służby zdrowia dla potrzeb obronnych RP*. Łódź: Wojskowa Akademia Medyczna.

Kwiasowski Z. (1998) *Zadanie badawcze: Logistyka armii wybranych państw NATO.* Warszawa: Zarząd Logistyki Sztabu Generalnego Wojska Polskiego.

Udział w kongresach, konferencjach i seminariach naukowych

1987

Referat: *Prowadzenie działań zaczepnych przez OGM Armii na nadmorskim kierunku operacyjnym*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1987.

Referat: *Zabezpieczenie bojowe (ochrona i obrona) Bazy Szpitalnej Frontu w operacji Zaczepnej i Obronnej*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1987.

1988

Referat: *Tendencje zmian w organizacji, wyposażeniu i zasadach prowadzenia walki na szczeblu taktycznym*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1988.

1989

Referat: *Koncepcje i możliwości prowadzenia działań wojennych przez siły zbrojne NATO na Środkowoeuropejskim Teatrze Działań Wojennych*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1989.

Referat: *Nowoczesne środki walki*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1989.

1991

Referat: *Konflikt w Zatoce Perskiej - doświadczenia i wnioski*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1991.

1994

Referat: *Zmiany w procesie kształcenia ogólnowojskowego w Wojskowej Akademii Medycznej*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1994.

Referat: *Organizacja Sił Zbrojnych RP*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1994.

1996

Referat: *Transformacja Sił Zbrojnych RP, a zmiany w procesie kształcenia ogólnowojskowego kadr Wojskowej Służby Zdrowia*,
Sympozjum naukowe Akademii Obrony Narodowej, Warszawa 1996.

1997

Referat: *Organizacja i zadania Sił Zbrojnych Rzeczypospolitej Polskiej w świetle programu "ARMIA - 2012"*,
Konferencja naukowa Zarządu Wojskowej Służby Zdrowia WP, Bydgoszcz 1997.

1998

Referat: *Międzynarodowe prawo humanitarne, a współczesne konflikty zbrojne*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 1998.

1999

Referat: *Procedury zabezpieczenia wojsk w myśl zasad logistycznych NATO*,
Konferencja naukowa Sztabu Generalnego Sił Zbrojnych Rzeczypospolitej Polskiej, Hel 1999.

2000

Referat: *Organizacja i zasady funkcjonowania zespołów dowodzenia logistyki*, Konferencja naukowa Zarządu Służby Zdrowia WP, Dęblin 2000.

Referat: *Środki rażenia współczesnego pola walki*,
XVII Konferencja Naukowo-Szkoleniowa Ortopedów Wojska Polskiego, Spała 25.05.2000.

2001

Referat: *Wsparcie logistyczne przez państwo gospodarza*,
Konferencja naukowa Wojskowej Akademii Medycznej, Łódź 2001.

2002

Referat: *Współczesny bioterroryzm*,
Ogólnopolska Studencka Konferencja Naukowa: Medycyna a bioterroryzm – zagrożenie i wyzwanie, Wojskowa Akademia Medyczna, Łódź 27.04.2002.

Referat: *Terroryzm na progu XXI wieku*,
Międzynarodowa Konferencja Naukowa: Administracja, zarządzanie i handel zagraniczny w warunkach integracji, Zakopane 02.06.2002.

Referat: *Rozwiązania edukacyjne Akademii Pedagogicznej w Krakowie w zakresie kształcenia nauczycieli przedmiotu przysposobienie obronnego*,
Konferencja Szkoleniowo-Metodyczna Ministerstwa Edukacji Narodowej i Sportu (starszych wizytatorów ds. obronnych kuratoriów oświaty), Warszawa 16.10.2002.

2003

Referat: *Pozamilitarne zagrożenia na progu XXI wieku*,
Ogólnopolska Konferencja Naukowa: Szanse i zagrożenia w socjalizacji, wychowaniu i edukacji, Bydgoszcz 17.03.2003.

Członek komitetu naukowego,
Międzynarodowa Konferencja Naukowa: Edukacja dla bezpieczeństwa (Akademia Wychowania Fizycznego Katowice, European Association for Security), Kraków 27.04.2003.

Referat: *Zagrożenia cywilizacyjne XXI wieku*,
II Ogólnopolska Konferencja Naukowa: Medycyna a zagrożenia cywilizacyjne XXI wieku, Łódź, Spała 17.05.2003

Referat: *Konflikty międzynarodowe, sposoby zapobiegania i rozwiązywania*,
Ogólnopolska Konferencja Naukowa: Dyplomacja a problemy bezpieczeństwa międzynarodowego, Łódź 19.05.2003.

Referat: *Bezpieczeństwo w kształceniu nauczycieli*,
Międzynarodowa Konferencja Naukowa: Bezpieczeństwo i prawa człowieka, Siedlce 26.05.2003.

Referat: *Bezpieczeństwo w kształceniu studentów*,
Konferencja: Zasady funkcjonowania struktur organów administracji publicznej i terenowych organów administracji wojskowej na obszarze województwa w warunkach kryzysu i wojny, Kraków 07.10.2003.

Referat: *Bezpieczeństwo w kształceniu nauczycieli Przysposobienia Obronnego*,
Organizator i przewodniczący Komitetu naukowego,
Sesja Naukowa: 30 lecie kształcenia nauczycieli przysposobienia obronnego w Akademii Pedagogicznej im. Komisji Edukacji Narodowej, Kraków 27.11.2003.

2004

Referat: *Wybrane aspekty bezpieczeństwa szkolnego*,
Ogólnopolska Konferencja Naukowa: Edukacja – Szkoła – Nauczyciele: Promowanie rozwoju dziecka, Kraków 16.01.2004.

Referat: *Bezpieczeństwo szkolne*,
Konferencja Szkoleniowa Zespołu Doradców Metodycznych Miasta Krakowa: Środowisko szkolne i jego bezpieczeństwo, Kraków 19.04.2004.

Referat: *Definicja terroryzmu, jego narodziny, rozwój i podział. Skutki działalności terrorystycznej*,
Konferencja Naukowa Szkoły Aspirantów Pożarnictwa Państwowej Straży Pożarnej: Współdziałania organów administracji szczebla wojewódzkiego w zakresie przeciwdziałania zagrożeniom wynikającym z aktów terroryzmu, 20.04.2004.

Referat: *Wybrane aspekty zagrożeń na progu XXI wieku*,
IV Międzynarodowa Konferencja Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego: Państwo i społeczeństwo w XXI wieku, Kraków 30.05.2004.

Referat: *Podnoszenie kwalifikacji nauczycieli z zakresu edukacji dla bezpieczeństwa*,
Ogólnopolska Konferencja Szkoleniowo-metodyczna starszych wizytatorów ds. obronnych kuratoriów oświaty Ministerstwa Edukacji Narodowej, Warszawa 06.10.2004.

Referat: *Przyszłość operacji humanitarnych*,
Konferencja Naukowa Akademii Obrony Narodowej: Charakter przyszłych operacji, Warszawa 20.10.2004.

Referat: *Wybrane problemy bezpieczeństwa szkolnego*,
Ogólnopolska Konferencja Naukowa: Problem współczesnych zagrożeń w edukacji obronnej młodzieży, Akademia Podlaska 17.12.2004.

2005

Referat: *Wybrane problemy bezpieczeństwa młodzieży*,
X Ogólnopolska Konferencja Naukowa: Zjawiska patologiczne wśród młodzieży ze szczególnym uwzględnieniem studentów – etiologia, fenomenologia, skutki, możliwości działań profilaktycznych i resocjalizacyjnych, Bydgoszcz 11.04.2005.

Komunikat: *Problematyka bezpieczeństwa w kształceniu przyszłych nauczycieli*,
Konferencja Popularnonaukowa: Patriotyzm, obronność i bezpieczeństwo obywateli, Warszawa 16.04.2005.

Komunikat: *Obszary współpracy i wymiana doświadczeń z badań nad bezpieczeństwem między placówkami naukowo-badawczymi*,
Sympozjum naukowe Akademii Obrony Narodowej: Ochrona terytorium polski w warunkach zagrożeń i wyzwań XXI wieku, Warszawa 28.04.2005.

Referat: *Wybrane aspekty zagrożeń na progu XXI wieku*,
Ogólnopolska Konferencja Naukowa: Bezpieczeństwo i prawa człowieka, Siedlce 24.10.2005.

Organizator i przewodniczący Komitetu naukowego,
Referat: *Interdyscyplinarność w kształceniu nauczycieli Przysposobienia obronnego*,
V Ogólnopolska Konferencja Naukowa: Kształcenie nauczycieli przysposobienia obronnego w polskich uczelniach – stan obecny i perspektywy, Kraków 17.12.2005.

Referat: *Zarządzanie bezpieczeństwem pracy*,
XI Międzynarodowa Konferencja Naukowa: Zarządzanie organizacjami gospodarczymi w wieku informacji, Łódź 01.12.2005.

2006

Referat: *Bezpieczeństwo i pokój w edukacji szkolnej*,
Ogólnopolska Konferencja Naukowa: Pokój jako przedmiot badań społecznych i pedagogicznych, Łódź 15.05.2006.

Członek Rady Programowej,
Referat: *Organy samorządu terytorialnego w zarządzaniu kryzysowym*,
II Ogólnopolskie Sympozjum „Krakowskie Spotkania z INSPIRE": Informacja przestrzenna w zarządzaniu kryzysowym, Kraków 08.06.2006.

Referat: *Wybrane aspekty edukacji dla bezpieczeństwa przyszłych nauczycieli – pedagogów*,
Międzynarodowa Konferencja Naukowa: Szkoła i nauczyciel w zmieniającym się społeczeństwie, Kraków 12.06.2006.

2007

Referat: *Edukacja dla bezpieczeństwa wobec wyzwań cywilizacji przełomu*,
Międzynarodowa Konferencja Naukowa: Czynić świat bardziej bezpiecznym, Siedlce 15.01.2007.

Referat: *Rodzina wobec zagrożeń*,
Konferencja Naukowa: Rodzina w kontekście współczesnych problemów wychowania, Kraków 21.06.2007.

Referat: *Młodzież wobec wyzwań cywilizacji przełomu – wybrane problemy*,
Międzynarodowa Konferencja Naukowa: Nauczyciel w dobie globalizacji i glokalizacji, Nowy Sącz 22.10.2007.

Referat: *Bezpieczeństwo szkolne wobec wyzwań cywilizacji XXI wieku*,
Konferencja Szkoleniowa Kuratorium Oświaty w Krakowie i Urzędu Miasta Krakowa: Dobra i bezpieczna szkoła – stan obecny i perspektywy, Kraków 24.10.2007.

Współorganizator,
Referat: *Czynić świat wolnym od min*,
Sympozjum Małopolskiego Zarządu Polskiego Czerwonego Krzyża i Katedry Edukacji Obronnej Akademii Pedagogicznej: 10 lat Konwencji Ottawskiej, Kraków 03.12.2007.

2008

Referat: *Prawo do wolności i bezpieczeństwa osobistego*,
I Konferencja Naukowa: Prawa Człowieka. 60 rocznica Powszechnej Deklaracji Praw Człowieka, Słupsk 25.09.2008.

Referat: *Przygotowanie nauczycieli Przysposobienia Obronnego do wykonywania zawodu*,
Konferencja Naukowa Ministerstwa Edukacji Narodowej i Ministerstwa Obrony Narodowej: Takie będą Rzeczypospolite jakie ich młodzieży chowanie, Warszawa 21.10.2008.

Referat: *Nauczyciel Przysposobienia Obronnego wczoraj – dziś – jutro*,
Konferencja Szkoleniowa Kuratorium Oświaty w Krakowie i Urzędu Miasta Krakowa: Bezpieczna szkoła oraz aktualne problemy wychowania dla bezpieczeństwa, Kraków 28.10.2008.

2009

Organizator i przewodniczący komitetu naukowego,
Referat: *Nauczyciel wobec wyzwań współczesności*,
VI Międzynarodowa Konferencja Naukowa: Edukacja Dla Bezpieczeństwa Wobec Wyzwań Współczesności, Kraków 08.10.2009.

Referat: *Młodzież wobec edukacji dla bezpieczeństwa*,
IV Międzynarodowa Konferencja Naukowa: Bezpieczeństwo i prawa człowieka w teoriach i praktyce społecznej początków XXI wieku, Siedlce 26.10.2009.

Referat: *Bezpieczeństwo szkolne - kontekst edukacyjny,*
Ogólnopolska Konferencja Naukowa: Młode pokolenie - sprawcy i ofiary przemocy, Szubin 22.10.2009.

Referat: *Biedne, głodne dzieci jako mniejszość*,
Ogólnopolska Konferencja: Mniejszości w ustroju demokratycznym, Tarnów 26.11.2009.

2010

Członek komitetu naukowego,
Referat: *Bezpieczeństwo szkolne w świecie pełnym zagrożeń*,
Międzynarodowa Konferencja Naukowa pod patronatem Komitetu Nauk Pedagogicznych Polskiej Akademii Nauk z cyklu Komunikowanie społeczne w edukacji – VIII spotkanie. Multidyscyplinarność bezpieczeństwa w szkole w perspektywie komunikowania międzyludzkiego – od komunikacji intrapersonalnej po komunikację masową. Komunikowanie a bezpieczeństwo personalne i strukturalne w wymiarze edukacyjnym, Lądek Zdrój 25.05.2010.

2011

Członek komitetu naukowego,
Referat: *Nauczyciel w (nie)bezpiecznej szkole*,
Międzynarodowa Konferencja Naukowa z cyklu Komunikowanie społeczne w edukacji – X Jubileuszowe Spotkanie. Multidyscyplinarność bezpieczeństwa podmiotowego i przedmiotowego w perspektywie komunikowania międzyludzkiego. Od komunikacji intrapersonalnej, interpersonalnej po komunikowanie globalne w perspektywie bezpieczeństwa człowieka i zbiorowości społecznych. Od komunikacji międzykulturowej do bezpieczeństwa wielu kultur, Lądek Zdrój 16.05.2011.

Referat: *Bezpieczeństwo szkolne w świecie pełnym zagrożeń*,
VIII Międzynarodowa Konferencja Naukowa: Bezpieczeństwo człowieka a rozwój naukowo-techniczny, Drohiczyn n/Bugiem 07.09.2011.

Członek komitetu naukowego,
Referat: *Edukacja obywatelska w szkole nowych czasów*.
Konferencja Szkoleniowa Kuratorium Oświaty w Krakowie i Urzędu Miasta Krakowa: Współczesny nauczyciel – ideał i rzeczywistość, Kraków 24.10.2011.

2012

Członek komitetu naukowego,
Referat: *Edukacja dla bezpieczeństwa w szkole nowych czasów*,
Konferencja Naukowa: Współczesne potrzeby i wymagania edukacji dla bezpieczeństwa, Siedlce 16.04.2012.

Członek komitetu naukowego,
Przewodniczący sekcji „Wartości środowiska rodzinnego",
Referat: *Rodzina jako wartość Małej Ojczyzny*,
Konferencja Naukowa: Wartości w teorii i praktyce pedagogicznej, Kraków 17.05.2012.

Organizator i przewodniczący komitetu naukowego,
Referat: *Wyzwania edukacji obywatelskiej XXI wieku*,
Ogólnopolska Konferencja Naukowa: Wyzwania edukacji obywatelskiej w dobie współczesności, Kraków 12.06.2012.

2013

Członek komitetu naukowego,
Referat: *Edukacja obywatelska szkoły XXI wieku*,
Konferencja Edukacyjno-Naukowa, połączona ze szkoleniem praktycznym: Rola i znaczenie zarządzania kryzysowego w systemie bezpieczeństwa państwa, Wierzchosławice 12.04.2013.

Członek komitetu naukowego,
Referat: *Znaczenie edukacji dla bezpieczeństwa w edukacji obywatelskiej,*
Seminarium Naukowe: Edukacja a bezpieczeństwo człowieka, Kujanki k./ Złotowa 14.05.2013.

Referat: *Zadania edukacji obywatelskiej w tworzeniu społeczeństwa demokratycznego*,
Międzynarodowa Konferencja Naukowa: Demokracja w XXI wieku z perspektywy jednostki – deklarowane wartości a rzeczywistość, Nałęczów 03.06.2013.

Wykład: *Znaczenie edukacji dla bezpieczeństwa w wychowaniu obywatelskim,*
Sympozjum Naukowe pt.: Bezpieczeństwo jako problem naukowy – od wartości do tożsamości edukacji dla bezpieczeństwa, Warszawa 05.12.2013.

2014

Referat: Bezpieczeństwo polskiej szkoły XXI wieku,
Seminarium Międzynarodowe pt.: Społeczne oblicza Europy XXI wieku, Piła 21.11.2014.

Współorganizator seminarium,
Ogólnopolskie Sympozjum Naukowe, Seminarium pt.: Bezpieczeństwo Polski w warunkach członkostwa w UE. Kraków 20.11.2014.

Współorganizator wernisażu wystawy,
Wykład: *95 lat Polskiego Czerwonego Krzyża*,
Wystawa pt.: Polskie organizacje czerwonokrzyskie w czasie Wielkiej Wojny, zorganizowana w 100-lecie wybuchu I Wojny Światowej i 95. rocznicy powstania Polskiego Czerwonego Krzyża, Kraków 06.11.2014.

2015

Współorganizator konferencji,
Referat: *Znaczenie Internetu w wychowaniu*,
Międzynarodowa Konferencja Naukowa z cyklu Człowiek w świecie informacji nt.: Kultura informacyjna w ujęciu interdyscyplinarnym, Kraków 09.10.2015.

2016

Współorganizator konferencji,
Wprowadzenie: *Bezpieczeństwo i prawa człowieka w kreowaniu nowych zawodów wobec potrzeb społecznych*,
Międzynarodowa Konferencja Naukowa: Teoria i praktyka pedagogiczna w zmieniającej się rzeczywistości, Kraków 24.05.2016.

Organizator konferencji,
Międzynarodowa Konferencja Naukowa: Współczesne wyzwania bezpieczeństwa europejskiego, Kraków 18-19.10.2016.

Promotorstwo rozpraw doktorskich

Dobrowolski B. (2004) Rozprawa doktorska: *Standaryzacja dozoru technicznego w Siłach Zbrojnych RP w aspekcie potrzeb funkcjonowania w NATO*. Warszawa: Wydział Wojsk Lądowych Akademii Obrony Narodowej.

Kaszuba M. (2009) Rozprawa doktorska: *Działania humanitarne Polskich Kontyngentów Wojskowych w operacjach pokojowych*. Warszawa: Wydział Strategiczno-Obronny Akademii Obrony Narodowej.

Góra P. (otwarcie przewodu 2012) Rozprawa doktorska: *Znaczenie więziennictwa polskiego w polityce bezpieczeństwa RP*. Siedlce: Wydział Humanistyczny Uniwersytetu Przyrodniczo-Humanistycznego.

Recenzje rozpraw doktorskich i habilitacyjnych

Zielony M. (24.01.2001) Rozprawa doktorska: *System logistyczny związku taktycznego w walce*. Warszawa: Rada Wydziału Wojsk Lądowych Akademii Obrony Narodowej.

Kubiński M. (20.11.2001) Rozprawa doktorska: *Działania batalionu desantowo-szturmowego sił natychmiastowego reagowania.* Warszawa: Rada Wydziału Wojsk Lądowych Akademii Obrony Narodowej.

Pietras Z. (24.04.2002) Rozprawa doktorska: *Zabezpieczenie logistyczne dywizji w przeciwuderzeniu*. Warszawa: Rada Wydziału Wojsk Lądowych Akademii Obrony Narodowej.

Ropski J. (01.07.2003) Rozprawa doktorska: *Kompetencje interpersonalne dowódców związków taktycznych i oddziałów a skuteczność dowodzenia.* Warszawa: Rada Wydziału Wojsk Lądowych Akademii Obrony Narodowej.

Nowak W. (25.11.2003) Rozprawa doktorska: *Modelowanie procesu informacyjno-decyzyjnego w Centrum Zabezpieczenia Działań Stanowiska Dowodzenia brygady zmechanizowanej (pancernej).* Warszawa: Rada Wydziału Strategiczno-Obronnego Akademii Obrony Narodowej.

Krawczyński R. (21.06.2004) Rozprawa doktorska: *Inspiracja tworzenia i wsparcie samoobrony w ochronie ludności i ratownictwie.* Warszawa: Rada Wydziału Strategiczno-Obronnego Akademii Obrony Narodowej.

Jedynak J. (13.07.2006) Rozprawa doktorska: *Społeczne i pedagogiczne uwarunkowania polityki bezpieczeństwa lokalnego w zakresie przeciwdziałania przestępczości nieletnich.* Kraków: Rada Wydziału Pedagogicznego Akademii Pedagogicznej im. Komisji Edukacji Narodowej w Krakowie.

Kurek T. (27.04.2010) Rozprawa doktorska: *Wojskowa służba zdrowia w systemie bezpieczeństwa Rzeczypospolitej Polskiej.* Warszawa: Rada Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej.

Łęgocka-Bartczak D. (05.10.2010) Rozprawa doktorska: *Efektywność procesu szkolenia z zakresu udzielania pierwszej pomocy w oparciu o bazę dydaktyczną Centrum Szkolenia Wojskowych Służb Medycznych w Łodzi.* Łódź: Wydział Wojskowo-Lekarski Uniwersytetu Medycznego.

Antczak A. (24.09.2013) Rozprawa doktorska: *Pozamilitarne aspekty konfliktów zbrojnych w ujęciu polemologicznym*. Warszawa: Wydział Zarządzania i Dowodzenia Akademii Obrony Narodowej.

Barć M. (24.06.2014) Rozprawa doktorska: *Działania 21 Brygady Strzelców Podhalańskich w sytuacjach kryzysowych na obszarze województwa podkarpackiego.* Warszawa: Wydział Zarządzania i Dowodzenia Akademii Obrony Narodowej.

Kubiński M. (26.10.2010) Rozprawa habilitacyjna: *Siły zadaniowe Wojsk Lądowych w działaniach taktycznych*. Warszawa: Rada Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej.

Wysocki W. (kolokwium 06.07.2012) Rozprawa habilitacyjna: *Korupcja zagrożeniem Systemu Obronności Polski*. Warszawa: Rada Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej.

Inne recenzje i opinie

Recenzja merytoryczna: Zespół Gdańskiej Fundacji Oświatowej pod kier. Hall K. (2002, 24.01.2003) *Program szkolny Klocki Autonomiczne dla liceum ogólnokształcącego, liceum profilowanego i technikum*". Warszawa: Wydaw. Nowa ERA.

Recenzja merytoryczna: Stebelski M. (2003, 10.03.2003) *Podręcznik przysposobienia obronnego dla uczniów szkół ponadgimnazjalnych część I pt.: Pierwsza pomoc*". Warszawa: Dom Wydawniczy ELIPSA.

Recenzja merytoryczna: Borowiecki M., Pytasz Z., Rygała E. (2003, 12.05.2003) *Program nauczania przysposobienia obronnego dla szkół ponadgimnazjalnych*. Warszawa, Łódź: Wydaw. Szkolne PWN.

Recenzja merytoryczna: Borowiecki M., Pytasz Z., Rygała E. (29.22.2004) *Podręcznik przysposobienia obronnego dla uczniów szkół ponadgimnazjalnych pt. Bądźmy bezpieczni. Przysposobienie obronne cz. I*. Warszawa, Łódź: Wydaw. Szkolne PWN.

Recenzja książki: Dziubiński J., Danielewski F., Moczuk E., Szulich P., Żak J. red. (2007) *Bezpieczeństwo lokalne w opiniach mieszkańców Tarnobrzega*. Tarnobrzeg: Państwowa Wyższa Szkoła Zawodowa (PWSZ) im. prof. S. Tarnowskiego.

Recenzja książki: Wacławczyk W. red. (2010). *Karta Praw Podstawowych Unii Europejskiej: nowa szansa dla praw człowieka?*. Warszawa: Wydaw. ERIDA.

Recenzja artykułów: *Zeszyty Naukowe Małopolskiej Szkoły Wyższej w Brzesku* (2010) nr 1(2)/2010, liczba recenzowanych artykułów 6.

Opinia merytoryczna: Goniewicz M., Nowak-Kowal, A.W., Smutek, Z. (2007, opinia 01.09.2006) *Przysposobienie obronne: podręcznik dla zasadniczej szkoły zawodowej*, wyd. 4 zm.Gdynia: Wydaw. Pedagogiczne Operon.

Opinia merytoryczna: Goniewicz M., Nowak-Kowal, A.W., Smutek, Z. (opinia 01.09.2006) *Przysposobienie obronne: podręcznik dla szkół ponadgimnazjalnych, cz. II.* Gdynia: Wydaw. Pedagogiczne Operon.

Opinia merytoryczna: Goniewicz M., Nowak-Kowal, A.W., Smutek, Z. (01.10.2006) *Przysposobienie obronne: podręcznik dla szkół ponadgimnazjalnych, cz. II,* wyd. 2 zm. Gdynia: Wydaw. Pedagogiczne Operon.

Opinia merytoryczno-dydaktyczna: Borowiecki M., Pytasz Z., Rygała E. (2009) *Edukacja dla bezpieczeństwa: podręcznik dla gimnazjum*. Warszawa, Łódź: Wydaw. Szkolne PWN.

Opinia merytoryczno-dydaktyczna: Izbicki K., Wrycz-Rekowski Ł. (2010) *Edukacja dla bezpieczeństwa: podręcznik dla gimnazjum*. Gdynia: Wydaw. Pedagogiczne Operon.

CZĘŚĆ I

Walka informacyjna
w kontekście przemian cywilizacyjnych

Jerzy Świeca
Uniwersytet Pedagogiczny w Krakowie

Interpolarność w globalnym systemie *jedno-wielobiegunowym*

Interpolarność w warunkach wzrastającej współzależności

Według Josepha S. Nye, Jr współczesna władza w stosunkach międzynarodowych jest rozdzielona według modelu trzech szachownic ułożonych warstwowo (Nye 2010, s. 3):

- amerykańskiej, jednobiegunowej władzy militarnej,
- niżej położonej (środkowej) szachownicy władzy gospodarczej o charakterze multipolarnym, utrzymującej się od kilku dekad (w rękach USA, UE, Japonii i Chin),
- dolnej szachownicy stanowiącej pas transnarodowy; ta ostatnia obejmuje aktorów niepaństwowych, instytucje finansowe, terrorystów, hackerów naruszających bezpieczeństwo cyberprzestrzeni oraz pandemiczne wyzwania czy też zjawiska obejmujące zmiany klimatyczne; dolna płaszczyzna władzy międzynarodowej jest poddawana dynamicznej dyfuzji i nie ma sensu jej charakteryzowanie jako jednobiegunowej, wielobiegunowej czy też ujmowanie w kategoriach systemu hegemonistycznego.

Do wyjaśniania mechanizmów współczesnego świata okazuje się bardzo przydatny wzorzec uregulowań sieciowych czy też globalnego systemu współzależności sieciowych. Globalna struktura współczesnego świata nie jest jedynie układem rywalizujących państw, ale skomplikowaną siecią współzależności[1]. Jest to świat uwikłany w zjawiska terroryzmu, narkotyków, handlu bronią, niekontrolowanego przemieszczania się ludzi, zmian klimatycznych i niszczenia bioróżnorodności, niebezpieczeństw wynikających z ograniczonych zasobów żywności oraz wody, korupcji, „prania brudnych" pieniędzy, niepłacenia podatków, chorób w wymiarze pandemicznym (zob. Slaughter 2016, s. 76). Większość polityków postrzega świat w wymiarze XVII wiecznym, w ujęciu postwestfalskim. Realizm świata i płynących zagrożeń sieciowych jest dobrze znany decydentom światowym, lecz nie wypracowali oni dotąd należytej strategii w celu ich konfrontowania. Administracja prezydenta Donalda Trumpa winna zbudować międzynarodowy porządek oparty na trzech filarach: 1) otwartych społeczeństwach, 2) otwartych rządach, 3) otwartym międzynarodowym systemie[2]. Linia podziału w świecie cyfrowym biegnie nie pomiędzy demokracją a autokracją, lecz pomiędzy tym co „zamknięte" i „otwarte". Systemy są otwarte ze względu na cechę partycypacji. Sieć energetyzuje się, uzyskując władzę poprzez proces partycypacji. Systemy są otwarte w sensie transparentności – udaremniają wysiłki zmierzające do kontrolowania informacji w taki sposób, by zaszkodzić

wolnościom. One są także otwarte w sensie autonomii bowiem w odróżnieniu od rządowych systemów zhierarchizowanych, sieć potęguje samoorganizację.

W 2011 roku prezydent Barack Obama ogłosił Otwarte Partnerstwo Rządowe (*Open Government Partnership*) najpierw z siedmioma innymi państwami, które w 2016 roku obejmowało już 70 państw, a w podpisanych deklaracjach zapisały one jak dotąd 2250 zobowiązań. Zawierają one trzy zasady: transparentność, obywatelską partycypację, odpowiedzialność[3]. Transparencja oznacza dostęp do informacji rządowych i uczynienie z nich obiektywnych standardów, co nie może oznaczać rezygnacji z tajności. Druga zasada pozwala na monitorowanie aktywności rządów i wdrożenie systemu ich oceniania. Trzecia zasada: odpowiedzialność – oznacza profesjonalną integralność co ułatwi walkę z korupcją. Zasady te ułatwią budowanie horyzontalnych powiązań sieciowych, które są zaprzeczeniem interakcji wertykalnych spotykanych w demokracjach i autokracjach.

Współczesny świat staje się coraz bardziej współzależny. Interpolarność – według Giovanniego Grevi jest zjawiskiem zupełnie nowym, nie występującym uprzednio w historii świata[4]. Redystrybucja władzy w skali globalnej oraz wzrastająca współzależność – są głównymi wymiarami transformacji pozimnowojennej. Procesy światowe z przełomu wieków odzwierciedlają ciągły i wznoszący się proces umiędzynarodowienia. Nie zawsze procesy te mają charakter globalny i są zjawiskami starszymi od procesów globalizacyjnych. Umiędzynarodowienie zjawisk i cech wewnętrznosystemowych nastąpiło z wielką siłą w drugiej połowie XX w. i trwa ze zdwojoną siłą na początku XXI w.

Asymetria rozdziału władzy na scenie światowej – która następuje w pierwszej dekadzie XXI w. – hamuje pokusę mocarstw by budować świat unipolarny z zarysowującą się hegemonią jednego z aktorów. Chęć zabezpieczenia sobie – przez podmioty międzynarodowe- dostępu do zasobów naturalnych i energetycznych – staje się centralną kwestią dla stosunków międzynarodowych nowego okresu. Opis analityczny systemu multipolarnego wymaga ujęcia wielu wymiarów środowiska. Pokazanie obrazu relatywnej władzy rywalizujących mocarstw daje tylko częściową diagnozę. Pogłębiająca się współzależność jest drugim, ważnym trendem kształtującym system międzynarodowy i wprowadza nowy kontekst do stosunków pomiędzy mocarstwami. Wzrost gospodarczy, bezpieczeństwo energetyczne i podtrzymywanie jakości środowiska naturalnego (zob. Levi 2009) są trzema współzależnymi problemami w rdzeniu kompleksowej współzależności (Grevi 2009, s. 5). Wszystkie mocarstwa są wystawione na bezprecedensowe połączenie gospodarczego, energetycznego i środowiskowego kryzysu i żadne z nich nie może z powodzeniem konfrontować tych wyzwań w pojedynkę. Zarówno istniejące, jak i wschodzące mocarstwa posiadają sprecyzowane interesy strategiczne w inwestowanie w kooperację, która powinna im zapewnić przyszłość oraz bezpieczeństwo na pewnym gruncie. Takie

zachowanie przyniesie korzystne warunki dla pojawiania się mechanizmów świata interpolarnego.

Interpolarność posiada kilka wymiarów. Jest ona po pierwsze, zbudowana na bazie przenikania się interesów mocarstw. Po drugie, ma wymiar systemu rozwiązywania problemów, gdyż jest zorientowana na wyzwania wymagające kooperatywnych działań. Jest także, po trzecie, zorientowana na tworzeniu systemu procesów międzynarodowych. Najważniejsze teoretyczne zagadnienie polega współcześnie na próbie rozstrzygnięcia kwestii – czy Unia Europejska dorosła do wyzwań sterowanych i kontrolowanych zmian powodujących wzrost mechanizmów interpolarnych i promujących efektywny multilateralizm? Prawdziwy test dla mocarstw i ugrupowań dopiero się zaczyna, gdyż w pierwszych dekadach XXI w. współzależność będzie się pogłębiać. Czy Unia stanie się centralnym podmiotem w interakcjach międzynarodowych, będzie decyzyjnym, przełomowym momentem dla jej przyszłości i dla kształtu systemu międzynarodowego, który dopiero się pojawi. Fareed Zakaria powątpiewa co do możliwości odegrania przez Unię i Japonię poważniejszej roli w nadchodzącej przyszłości[5]. Unia znajduje się w systemie zachodnim, ale także w globalnym środowisku *jedno-wielobiegunowym.* Stany Zjednoczone są najsilniejszym mocarstwem militarnym i politycznym[6], ale dystans między nimi a „resztą świata" (głównie Chinami i Indiami) wydatnie się zmniejsza. Europa powinna współpracować z USA w ich strategii współpracy, porozumienia, współdziałania, budowania szerokich koalicji (zob. Zakaria 2009, s. 13). Czy Europa może tak jak Stany Zjednoczone stać się mediatorem konfliktów i animatorem porozumień? Czy nowa struktura unijnej władzy (przewodniczący Rady Europejskiej i szef dyplomacji UE) będzie sprzyjać *quasi* państwowej aktywności na arenie międzynarodowej? Wybitny analityk amerykański, hinduskiego pochodzenia – Fareed Zakaria – negatywnie ocenia możliwości europejskie na scenie globalnej. Szanse gospodarcze Europy są faktycznie duże, ale nadzieje na poważny udział w stosunkach międzynarodowych, są raczej skromne. Zwłaszcza jeśli chodzi o kategorie polityczne i militarne. Żyjemy w czasach ogromnych przemian transformacyjnych w stosunkach międzynarodowych, które prawdopodobnie są spowodowane nie schyłkiem Ameryki, lecz rezultatem wzrostu „reszty świata" – jak twierdzi Fareed Zakaria (zob. Zakaria 2009). Powstaje nowy układ sił międzynarodowych, który można zdefiniować jako *jedno-wielubiegunowy.* USA są najsilniejszym państwem świata, ale dystans między nimi a pozostałymi aktorami, bardzo szybko się zmniejsza. Teoria Zakarii, nie jest zapewne tylko teorią dedukcyjną, lecz indukcyjną percepcją realistycznego obrazu świata w pierwszych dekadach XXI w. Jest to wizja optymistyczna. Strategia, którą USA powinny się posługiwać bazuje na takich kategoriach jak: współpraca, porozumienie, współdziałanie, budowanie szerokich koalicji. Czy faktycznie w nowym układzie sił zabraknie Europy[7].

W analizie świata interpolarnego ważne są dwa trendy zmian: redystrybucja władzy na poziomie globalnym, prowadząca do nowych form multipolarności, wzrastająca współzależność dotycząca bezpośrednio pomyślności oraz bezpieczeństwa wielkich mocarstw, a także społeczności międzynarodowej jednocześnie (Grevi 2009, s. 9). Wypracowanie modelu kooperatywnych działań jest naczelnym wyzwaniem, którego nie można zaniedbywać kosztem realizacji krótkotrwałych interesów. Multipolarność klasyczna, tradycyjna, zwykle kojarzyła się z modelem konfrontacyjnym. Interpolarność jest multipolarnością w epoce współzależności (Grevi 2009, s. 9). Interpolarność bazuje na interesach, przesuwaniu się dynamiki problemów, zorientowaniu na procesy zjawisk. Bieguny czy ośrodki władzy w systemie międzynarodowym są zwyczajowo definiowane jako państwa wyposażone w środki, wolę polityczną i instytucjonalne zdolności do projektowania i chronienia swoich interesów na poziomie globalnym, multiregionalnym i regionalnym, uzależnionym od rozmiarów mocarstw w danej kwestii. W takim rozumieniu UE nie spełnia tych kryteriów, ale ma wkład do procesu zarządzania i multilateralizmu.

Jeśli definiujemy system międzynarodowy w kategoriach interpolarności, nie musi to oznaczać, że lekceważmy znaczenie aktorów pozapaństwowych. Jest to raczej problem dobrego zdefiniowania zmiennych kształtujących ewolucję systemu globalnego. Aktorzy państwowi tworzą jednakże szkielet struktury bezpieczeństwa i w ogóle stabilizacji stosunków międzynarodowych. Poglądy oceniające rolę międzynarodową USA bardzo szybko zaczęły się zmieniać. Według R. Holbrooka „restauracja uszanowania wartości oraz przywództwa amerykańskiego jest podstawowa nie dlatego, że jest to bardzo przyjemne być popularnym, ale dlatego, że jest to uwarunkowanie przedwstępne dla legitymizowanego przywództwa i długotrwałych wpływów”[8]. Dynamiczna gospodarka, model socjalny oraz wdrażane innowacje technologiczne – imponowały całemu światu. Samodzielne zadawane szkody polityczne, tylko częściowo mogą tłumaczyć kres amerykańskiej hegemonii. Reszta świata – położona poza światem zachodnim – stworzyła nowy układ sił. Świat stawał się coraz bardziej heterogeniczny. Kompleksowość sceny międzynarodowej, nie da się sprowadzić do prostych dychotomii. Podział na państwa demokratyczne i autorytarne jest bardzo istotny, zwłaszcza gdy chodzi o ochronę praw człowieka i rolę prawa. Uwarunkowania socjoekonomiczne, które pozwoliły na Zachodzie wdrożyć systemy liberalne i konstytucyjne, stanowią najważniejsze uwarunkowanie wstępne tych procesów. Bardzo istotne w tych podziałach jest rozumienie suwerenności. USA stosowały w ostatnim czasie model zarówno strategii utrzymującej *status quo*, jak i mocarstwa rewizjonistycznego pragnącego narzucać demokrację siłą. Obok płaszczyzny bezpieczeństwa, bardzo ważną sferą wyzwań i regulacji jest handel międzynarodowy. Istnieje trudna do przebycia przepaść pomiędzy grupą państw kształtujących system handlu

międzynarodowego oraz tych, które dążą do jego zmiany i wyrażają niezadowolenie z przemian.

Jeśli chodzi o systemy gospodarcze, to kryzys zapoczątkowany w 2008 r. przytłumił znaczenie modelu anglosaskiego i zaczęto dyskutować kwestię koegzystencji i rywalizacji różnych modeli. Choć współcześnie wartości demokratyczne i gospodarki rynkowej nie są kwestionowane, to żywo dyskutuje się sposoby ich implementacji. Powróciły dyskusje nad znaczeniem historii wraz z wytworzeniem się przepaści pomiędzy obozem demokracji (USA i Europa) oraz stowarzyszeniem państw autorytarnych (głównie Rosja i Chiny), a także pomiędzy modernizacją i liberalizmem a radykalnym islamem (Grevi 2009, s. 14). Po trzywiekowej dominacji Zachodu, wraca heterogeniczny system sceny międzynarodowej. To podkopuje znaczenie unilateralnych działań. Czy faktycznie jednak, system międzynarodowy – biorąc pod uwagę poziom płaszczyzny interakcji – ewoluuje od jedno-wielopolarności do multipolarności[9]? Kryzys finansowy zapoczątkowany w 2008 r., przyspieszył ewolucję, choć cechy systemu unipolarnego i multipolarnego ciągle współwystępują.

Należy przeanalizować trzy cechy klasycznego systemu multipolarnego: 1) kwestię prymatu głównego mocarstwa; 2) problem równoważenia (przez inne podmioty państwowe); 3) zakres działań kolektywnych (Grevi 2009, s. 23). Na ogół władza była rozłożona pomiędzy kilka mocarstw, co nie przeszkadzało, że jedno z nich mogło posiadać przewagę. Co do zakresu równoważenia władzy międzynarodowej, państwa podejmują się w realizacji swoich interesów, różnych środków włącznie z wojną. W stosunku do akcji kolektywnych trzeba podkreślić, że są one potrzebne dla odpowiedzi związanych z wyzwaniami globalnymi i interregionalnymi. Opis analityczny systemu multipolarnego odzwierciedla nowe cechy jego środowiska. Podejście to zbytnio koncentruje się jednak na względnej władzy jednych mocarstw wobec drugich, a nie nad ewolucją aktualnego kontekstu (środowiska) ich wzajemnych interakcji. Innymi słowy, problem z podejściem metodologicznym określanym przez multipolarność, nie polega na tym, że jest złe, ale że jest to ujęcie fragmentaryczne.

Wraz z multipolarnością pojawia się problem akcentowania relatywnej władzy oraz zakresu równoważenia i rywalizacji pomiędzy biegunami systemu. Problem polega na tym, że władza nie może być mierzona relatywnie w stosunku do innej władzy, ale powinna być oceniana relatywnie do zmieniającego się szczebla (poziomu) pola interakcji. Współczesny system międzynarodowy cechuje pogłębiająca się egzystencjalna współzależność. Centralnym problemem władzy staje się adresowanie w stosunku do zaistniałych wyzwań, zarówno multiratelarnej kooperacji, jak i akcji kolektywnych. Wzrost ekonomiczny, bezpieczeństwo energetyczne (zob. Victor, Yueh 2010, s. 61-73; Ruhl 2010 s. 63-75) i środowiskowe zrównoważenie – są bardzo ze sobą związane. Ta współzależność trzech trendów wraz z walką z rozpowszechnianiem broni

masowego rażenia jest najpoważniejszym wyzwaniem dekad nadchodzących. Geopolityczny efekt kryzysu finansowego spowoduje przeniesienie gospodarczej władzy i politycznych wpływów z Zachodu na Wschód.

Świat prawdopodobnie wszedł w epokę konwergencji, w której podtrzymywana ekspansja demograficzna staje się równoległa do poziomu dochodu narodowego brutto *per capita*. Ten trend widoczny jest w krajach rozwijających się o wysokiej dynamice wzrostu. Rezultat gospodarczy takiej ekspansji powinien być tak zarządzany, by nie potęgował jeszcze większych nierówności, wzrostu ubóstwa oraz degradacji środowiska naturalnego. W zakresie środowiska naturalnego, dane są alarmistyczne (Bales, Duke 2008, s. 78-89). Kraje spoza OECD (*non-OECD countries*) mają udział w zapotrzebowaniu na energię na poziomie -87%, a w emisji CO_2 w -wysokości 97% (Grevi 2009, s. 25). Rezultat w postaci katastrofy ekologicznej – w tej sytuacji – może być bliski. Zmiany klimatyczne mogą działać jako „groźba zwielokrotniająca" i podkopująca stabilność i bezpieczeństwo słabszych państw. W porównaniu z innymi wyzwaniami dotyczącymi rozwoju i bezpieczeństwa, gospodarcza współzależność ewoluuje w kierunki egzystencjalnej współzależności. Analizując kryzys finansowy oraz zbliżający się ekologiczny kryzysy planetarny, niektórzy analitycy wychodzą z założenia, że ich prawdziwe przyczyny leżą w systemie zaniedbywania długoterminowych wyzwań wynikających z własnego funkcjonowania i koncentrowania się na bieżących kwestiach[10]. Oba kryzysy są groźne, ale kryzys planetrany będzie nieodwracalny i katastroficzny. Kooperacja multilateralna może okazać się mechanizmem odpowiednim do walki o lepszy byt ludzkości.

Kombinacja pojawiającej się multipolarności oraz pogłębiających się współzależności zmieni przebieg stosunków międzynarodowych. Głównym problemem pozostaje, czy pojawiający się system multipolarny, będzie miał charakter konfrontacyjny, rywalizujący czy też kooperatywny. Te trzy wymiary są bardzo współzależne, lecz jest krytycznym i najważniejszym zagadnieniem, by kooperacja dominowała nad konfrontacją, a rywalizacja nie była restryktywnie ograniczana. Głównym wyzwaniem pozostaje kwestia, w jaki sposób promować kooperatywną formę multipolarności w epoce współzależności. Innymi słowy wyzwanie to polega na tym, jak pogodzić efektywny multilateralny porządek z multipolarnym systemem międzynarodowym? Naczelnym ujęciem porządku międzynarodowego jest założenie, że główne mocarstwa uniwersalne i regionalne, pozostają nadal najważniejszymi decydentami w polityce międzynarodowej.

Powstający system multipolarny – według reguł kształtujących się w I poł. XXI w. – to realnie system interpolarny. Interpolarność ucieleśnia dwa wymiary wielkiej transformacji w stosunkach międzynarodowych: multipolarność oraz pogłębiającą się współzależność. Wymiar multipolarny powoduje progresywną redystrybucję władzy w skali globalnej w celu skonfrontowania największych wyzwań wspólnymi siłami.

Percepcja stosunków międzynarodowych oparta na interpolarności toruje drogę pod reformy oraz umocnienie porządku multilateralnego. Żaden multipolarny porządek nie będzie jednak trwały jeśli nie będzie połączony z transformacją systemu międzynarodowego i głównymi interesami mocarstw uniwersalnych. Świat jest obecnie dużo bardziej nasycony cechą rywalizacji, niż w dekadach poprzednich. Stabilizacja wymaga zastosowania woli politycznej, bez której nie utrzyma się homeostazy. Do identyfikacji stopnia konwergencji, dystansu czy konfliktów potrzebne jest respektowanie interesów mocarstw i ich ciągłej roli w urządzaniu świata. Interesy nigdy nie są stałe, lecz ewoluują jak każda stworzona przez człowieka idea. Interesy indywidualne podmiotów państwowych są oczywiście odmienne od interesów współdzielonych. Interpolarność zorientowana na analizę bazy interesów jest także interpolarnością dynamizowaną przez problemy, które pojawiają się jako wyzwania do wspólnej konfrontacji, jako że w trybie unilateralnym, żadne państwo nie może zagwarantować sobie prosperity, stabilności, bezpieczeństwa. Uznaje się, że zmiany klimatyczne (por. Flynn 2008, s. 2-8) mogą być wyzwaniem najpoważniejszym, gdyż mają kompleksowy charakter i dotyczą takich sfer jak: bezpieczeństwo energetyczne, rozwój, zabezpieczenie żywności, fale migracyjne. Skoncentrowanie się na tych wyzwaniach unaoczni korzyści z kooperacji, a świat interpolarny stanie się oczywistym, przynajmniej w percepcji.

Redystrybucja władzy oparta na nowych zasadach, z uwzględnieniem odmiennych tradycji różnych państw, może w pierwszej fazie nawet skomplikować kolektywne działania. To może także komplikować transformację. Trzeba dbać o stabilność zachodniej strategii normatywnej i nie stosować podwójnych standardów wobec różnych podmiotów państwowych. Wyjście polega na bezwzględnym stosowaniu wartości podstawowych transformacji: praworządności, przestrzegania praw człowieka, demokracji; wdrażaniu ich z wielką konsekwencją i w systemie spójności, tak aby korespondowały z koncepcją świata interpolarnego. Ponadto trzeba stosować spojrzenie analityczne oparte na bazie konwergencji interesów, rozwiązywania podzielonych problemów. System interpolarny jest także zorientowany na procesy (por. Flynn 2008, s. 30). Stąd ogromne znaczenie multilateralnego szkieletu i instrumentów dla kooperatywnych działań. Jeśli mają być przeprowadzone z sukcesem finalnym, reformy multilateralizmu muszą odzwierciedlać i towarzyszyć dwóm ważnym trendom: 1) zmianom w układzie sił, co nakłada problem legitymizacji i reprezentacji na forach multilateralnych; 2) pogłębiającej się współzależności, która skutkuje kwestią efektywności, koordynacji środków dla organizacji i mechanizmów międzynarodowych. W procesie reform ważnym będzie ustalanie reform – priorytetów. Dyplomacja szczytów staje się ważnym instrumentem mechanizmów multilateralnych.

System interpolarny jest układem analizującym interesy i zorientowanym na problemy, stąd coraz częściej uwzględnia takie struktury jak G-20, ugrupowanie zrzeszające kraje produkujące 90% PKB. Stany Zjednoczone powinny więc odłożyć plany budowy ugrupowania demokratycznego na arenie międzynarodowej, gdyż instytucja taka utrudniłaby tylko wpływy i legitymizację Zachodu w stosunkach międzynarodowych (Kupchan 2008, s. 96-109).

Słabnące mocarstwo uniwersalne w mechanice stosunków międzynarodowych

Potęgę państwa określają trzy czynniki: środowisko międzynarodowe, zasoby, działania zbiorowe. Polega ona na narzucaniu swej woli innym jednostkom politycznym (Aron 1995, s. 69-98). Amerykański analityk Joseph S. Nye, Jr , określa władzę zarówno jako zdolność do uzyskiwania celu zamierzonego, jak i umiejętność dysponowania środkami, które pozwalają na różnicowanie działań w niejednorodnych uwarunkowaniach międzynarodowych (Nye 2010, s. 2).

W końcowym okresie zimnej wojny historyk amerykański Paul Kennedy pisał, że zobowiązania amerykańskie przekraczają możliwości ich realizacji (Kennedy 2009, s. 21). Trzy lata później USA wysłały kontyngent złożony z 600 tys. żołnierzy do Iraku, nie podnosząc nawet wymiaru podatkowego. W części koszty zostały sfinansowane jednak przez naftowe kraje arabskie, w tym przez wahhabickie Królestwo Saudów.

Teoria schyłkowości USA wielokrotnie była kwestionowana przez fakty[11]. Wzrost gospodarczy USA trwał w zasadzie do 2008 r. W tym samym roku znany amerykański analityk Parag Khanna oceniał, że USA na rynku geopolitycznym schodzą ze sceny i są zastępowane przez nowe podmioty (Brzeziński 2013, s. 23). Khanna wskazuje na głównych rywali USA – Unię Europejską oraz Chiny. Fakty uderzają jednak mocno w teorię schyłkowości USA. Wartość amerykańskiej gospodarki wynosiła w 2015 roku prawie 18 bln USD i była tylko nieco mniej niż cztery połączone ekonomiki liczone razem: japońska, chińska, niemiecka i francuska. Nigdy w nowożytnym świecie przepaść dzieląca mocarstwa, nie była tak wyraźna. Współcześnie, w pewnym sensie jedynym wyzwaniem dla gospodarki USA jest ekonomika UE o sile 16 bln USD (Brzeziński 2013, s. 25; dane zaktualizowano na 2015 rok). Nie jest to jednakże żaden wskaźniki o sile porównawczej. Takim bez wątpienia będzie strefa Euro, na którą składają się ekonomiki 19 państw, która ma wspólną politykę monetarną oraz fiskalną, a PKB sumaryczne wynosi 13,5 bln Euro. Wspólnej waluty używa codziennie około 338,6 milionów ludzi w 19 z 28 krajów Unii Europejskiej. UE w pierwszym, pełnym zakresie oraz w drugim – ilościowo ograniczonym – nie jest żadnym graczem strategicznym. USA posiadają 7,5-krotnie większy dochód *per capita* niż Chiny, wyprzedzając kolejnego rywala w zakresie *soft power*.

Przewaga militarna USA nad resztą świata jest jeszcze bardziej niepodważalna. Budżet obronny na rok 2010 wynosił w USA 685 mld USD. Najwięksi rywale Ameryki: Chiny, Indie, Japonia i Rosja[12] – wydatkują 1/3 tej sumy, choć w drugiej dekadzie Kreml zwiększył wydatki modernizacyjne na armię. Budżet obronny CHRL stanowi mniej niż 1/7 amerykańskiego. Przewaga w sile i tonażu marynarki wojennej jest miażdżąca. Dzisiejsze mocarstwa: Chiny, Indie, Japonia, Rosja nie są w stanie przeprowadzać operacji wojennych 8000 mil od swoich wybrzeży. USA przeprowadzają takie operacje w Iraku i Afganistanie.

Stany Zjednoczone ciągle odnoszą – w analizach – swoją mocarstwowość jedynie do potencjału militarnego, a nie do wymiaru gospodarczego i to wbrew strategiom innych państw. Tylko dwaj powojenni prezydenci: Harry Truman i Dwight Eisenhower uwzględniali oba czynniki jako ważne i dopełniające się. Powstrzymując i odstraszając komunizm, oferowali oni pomoc wojskową i gospodarczą swoim sojusznikom (por. Gelb 2010, s. 35).

Podstawowym problemem współczesności jest kwestia ożywienia gospodarki. Powstaje jednak w tym przypadku luka pomiędzy gospodarczym potencjałem USA a jego przetworzeniem w realne wpływy. Wiele problemów wewnętrznych rodzi się poza granicami państwa. Dodatkowo ten efekt wzmacniany jest przez słabą wydajność i skuteczność zewnętrznych oddziaływań. Wewnętrzna strategia amerykańskiego bezpieczeństwa narodowego jest słaba i wykazuje niedociągnięcia. Dostosowanie amerykańskiej polityki do mechanizmów globalnych jest trudne, gdyż tam obowiązują akcenty gospodarcze, a nie militarne. W fazie do I wojny światowej zarówno Niemcy, jak i Japonia promowały swoje interesy ekonomiczne przy pomocy środków wojskowych. Okres ten uwidocznił się także w okresie II wojny światowej. Nie wydaje się słuszna idea, że Chiny będą kolejnym, funkcjonującym według powyższego, starego wzorca mocarstwem, które chce dominować przez handel i finanse, a jeśli to niemożliwe to przy pomocy środków wojskowych (Gelb 2010, s. 36). Stare Niemcy i Japonia umotywowane były przez mechanizmy wojenne i walczyły o potencjał wojskowy drogą militarnej ekspansji.

Komuniści chińscy rządzą krajem, w którym połowa ludności doświadcza ubóstwa jako dotkliwej formy przemocy strukturalnej, a więc partia musi walczyć o przetrwanie u władzy. Przewaga drugiej ery globalizacji zrodzonej w wyniku II wojny światowej, a zwłaszcza zimnej wojny, polega na integracji państw ustabilizowanych we wspólnej walce z terroryzmem. W przeszłości państwa walczyły praktycznie o nic (Gelb 2010, s. 37) (realnie jednak o nowy układ sił – J. Ś). W gruncie rzezy współczesne państwa w wielkiej rywalizacji są współzależne i jedno potrzebuje drugie, by rozwijać swój gospodarczy potencjał. To dotyczy zarówno relacji Chiny – Rosja, jak i Chiny – USA. Współcześnie państwa budują siłę gospodarczą, by używać ją do celów nie militarnych, a ekonomicznych. Ten proces walki o większy potencjał gospodarczy dotyczy w szczególności krajów z obszaru

BRICS (obejmującego Brazylię, Rosję, Indie, Chiny, Afrykę Południową). Choć państwa te mają wyraźne motywy, by budować strategię klasycznego bezpieczeństwa, to koncentrują się głównie wokół potęgowania PKB. Waszyngton z trudem uznaje tezę, że gospodarka jest w centrum geopolityki. Za Trumana i Eisenhowera budżet obronny nigdy nie był definiowany jako pierwszy, a dług zagraniczny traktowali obaj prezydenci jako największe zagrożenie (Gelb 2010, s. 38).

Warto jednakże czerpać wiedzą z historii. Truman i Eisenhower według emerytowanego prezydenta think tanku – *Council on Foreign Relations* – L. H. Gelba, odpowiedzieliby na atak z 9 września w następujący sposób: nawiązaliby bliskie więzi współpracy z sąsiadami Afganistanu, by powstrzymać Talibów, zastosowaliby wobec Talibów odstraszanie karząc ich w razie współpracy z Al-Ka'idą, dezintegrowaliby Talibów drogą środków dyplomatycznych, wspomagaliby tworzenie nowego rządu w Kabulu oraz wspomagaliby rząd i przywódców plemiennych pomocą gospodarczą i wojskową (Gelb 2010, s. 40-41). Strategia ostatnich prezydentów zastosowana wobec terrorystów przyniosła wiele strat. W listopadzie 2016 roku Talibowie kontrolowali 60% terytorium Afganistanu. Żeby wygrać z nimi wojnę w Afganistanie trzeba wygrać dla siebie Pakistan i uczynić go bliskim, regionalnym współpracownikiem w działaniach strategicznych, tak by przestał stanowić subsystem wspomagania dla Talibów. Współcześnie USA kontynuują politykę bycia regionalnym stabilizatorem w wyborach strategicznych odnoszących się do roli Chin w Azji, Rosji we wschodniej Europie i Iranu w regionie bliskiego i środkowego wschodu. Percepcja strategii USA w stolicach rywali jest trafna i dokładna, zgodna z amerykańskimi intencjami.

W złożonym środowisku globalnym, strategia USA powinna koncentrować się wokół następujących kwestii: budowania silnej gospodarki, która zwycięża w systemie rywalizacji jak najmniejszym kosztem; kontrowersyjny cel utrzymywania mocarstwowości militarnej dla protekcji handlu i innych celów gospodarczych (Gelb 2010, s. 42). Trzeba przemyśleć sposób używania środków związanych z wpływami międzynarodowymi, stosownie do realizowanych celów. Wektorem poprawności będą wartości wspólne dla całej społeczności globalnej.

Wielkim atutem USA jest zdolność wchłaniania do demograficznego systemu amerykańskiego ogromnej ilości imigrantów. Co prawda, w 1910 roku liczba rezydentów urodzonych poza granicami Stanów Zjednoczonych wynosiła 14,7%, a współcześnie 11,7% i ciągle spada, to i tak wskaźniki są relatywnie dobre. Imigracja powoduje problemy socjalne, ale w sumie wzmacnia amerykańską potęgę międzynarodową. Odnotowuje się pozytywną korelację pomiędzy ilości przyznawanych dla specjalistów wiz H-1B, a ilością uzyskiwanych patentów. Amerykańska *soft power* rośnie dzięki migracji (Nye 2010, s. 5).

USA wydawały także znaczne kwoty na *research&development*, bo w końcu pierwszej dekady XXI wieku rocznie 369 mld. USD w stosunku do 338

inwestowanych w Azji i 263 mld USD w Europie. Wydatki te stanowiły 2,7% PKB, czyli dwukrotnie więcej niż chińskie i nieco mniej niż prawie 3% wydawanych przez Japonię i Korę Płd. (Nye 2010, s. 6). Duże obawy budzi natomiast wzrastające zadłużenie publiczne, które według Fareeda Zakarii osiągnęło już katastroficzny pułap 107%[13].

USA są absolutnie unikalnym krajem w zakresie wydatków na oświatę. W dwudziestce najlepszych uniwersytetów światowych, aż 17 to amerykańskie. USA wydają więcej niż dwukrotnie na oświatę, mierzone jako procent PKB, niż Francja, Niemcy, Japonia i Wielka Brytania (Nye 2010, s. 7).

Problem amerykańskiej władzy nie polega na jej osłabieniu czy upadaniu, ale sprowadza się do pytania: co robić aby w wielkim kraju nie były możliwe sytuacje, że nie można uzyskać celu zaplanowanego, bez pomocy innych podmiotów państwowych. Oczywiście konieczne są rozwiązania sieciowe, na miejsce dotychczasowych zhierarchizowanych międzypaństwowych. Jeśli kraj posiada niewielkie zasoby surowcowo-energetyczne, to trudniej jest mu uzyskiwać planowane cele. Z drugiej strony nadmiar władzy w wymiarze zasobów surowców prowadzi często do przekalkulowania możliwości i wyboru błędnych strategii (Nye 2010, s. 12).

Smart-potęga w XXI w. nie może polegać na maksymalizacji władzy lub zachowaniu hegemonii. Jest to odnajdywanie drogi, w której nastąpi wkomponowanie środków w zwycięską strategię w nowym kontekście dyfuzji władzy międzynarodowej i wzrostu pozostałych państw. Według Jesepha S. Nye, Jr. potrzebne jest wypracowania strategii, która łączy hard- i soft-potęgę posiadanych zasobów, i która akcentuje sojusze i sieć, które są odpowiednie do nowego kontekstu globalnej ery informatycznej (Nye 2010, s. 12).

Prognoza nie jest więc pesymistyczna dla dotychczasowego lidera sceny globalnej. W motto do autorskiej książki, Fareed Zakaria, cytuje swojego wielkiego mentora: Arnolda. J. Toynbee, który pisze: *Wzrost występuje wszędzie tam, gdzie na wyzwanie odpowiada działanie uwieńczone sukcesem, co z kolei powoduje pojawienie się kolejnych wyzwań. Nie znaleźliśmy żadnej rzeczywistej przyczyny, dla której ten proces nie miałby powtarzać się w nieskończoność, nawet jeśli wziąć pod uwagę historyczny fakt, że większość cywilizacji upadła* (za: Zakaria 2009, motto).

Czyżby po spełnieniu warunków Arnolda J. Toynbeego, wbrew doświadczeniom historycznym, mocarstwa uniwersalne mogły trwać w nieskończoność, bez limitu czasowego? Byłby to bardzo swoisty eksperyment historyczny. Można jednak skonstatować, że spełnienie tego warunku może znacznie przedłużyć kondycję państw. Wielka Brytania była wielkim mocarstwem liberalnym przez dwa i pól wieku, od czasów elżbietańskich aż po Wielką Wojnę w 1914 roku.

Jednak, gdy świat wkroczy w 2025 roku w erę postamerykańską, może się okazać, że to nie Chiny będą dominującym liderem, lecz zapanuje niebezpieczny chaos (Brzeziński 2013).

Budowa Wielkich Chin. Nowy system jedno-wielobiegunowy

Władza nie wynika jednak ze wzrostu gospodarczego. Co zatem czyni dany kraj wielkim? (Joffe 2009, s. 29). Na ogół na potęgę współczesnego mocarstwa składa się według wielu analityków PKB. Czy można jednakże, aż tak uprościć proces osiągania mocarstwowości?

Problem Chin polega na dynamicznym wzroście ich gospodarki – w tempie trzy razy szybszym niż w USA (w ujęciu nominalnym, gospodarka chińska wysunęła się na drugie miejsce za amerykańską i przed japońską dopiero w 2010 roku). Po zastosowaniu ujęcia obliczeniowego tzw. parytetu siły nabywczej (*perchasing power parity* – PPP) okazało się, że chiński PKB w 2007 r. urósł z nominalnego wymiaru równego 3,3 bln do 8 bln USD – dzięki głównie niskim cenom oraz niskiemu poziomowi zarobków chińskiej siły roboczej (Joffe 2009, s. 27). Jeśli chińska gospodarka będzie się rozwijała w tempie 10% rocznie, to zo siedem lat zdubluje swój PKB. Życie jednakże nie rozwija się linearnie, a proste projekcje warunkowane są przez błędy ekstrapolacji.

Dublowanie się chińskiej gospodarki wskutek wysokiego tempa wzrostu, jest zjawiskiem nowym, występującym od 2003 r. Chińska gospodarka skrajnie zależy od eksportu, który stanowi 40% PKB. Jest więc niezwykle wrażliwa na trendy światowe. Tylko 35% PKB to konsumpcja indywidualna, podczas gdy w krajach zachodnich wskaźnik ten wynosi aż 60% (Joffe 2009, s. 28).

Problemem chińskim są cywilne, polityczne zamieszki, o których świat nie dowiaduje się prawie w ogóle, ze względu na autorytarny charakter państwa. Jeżeli Chiny nie przesuną znacznych środków z dziedziny aktywności służb socjalnych i wsparcia dla społeczeństwa, model społeczno-gospodarczy oparty na wzroście potęgowanym przez eksport, załamie się gwałtownie[14]. RFN posiada bardzo podobny wskaźnik udziału eksportu do PKB, ale udział w produkcie brutto kosztów państwa dobrobytu sięga aż 1/3 przy wzroście rocznym 1,5% przez okres dłuższy niż dekada (Joffe 2009, s. 28).

Chiny stoją przed wyzwaniem wyboru strategicznego: eksport lub model *welfare state.* Jeśli nawet Chiny unikną wyzwań klasycznych stojących przed władzą autorytarną i imperialną, takich jak wojny, rewolucje, niepokoje społeczne (jak w historycznej Rosji, Niemczech, Japonii), kolejnym groźnym wyzwaniem będzie pogorszenie się jakości zasobów demograficznych (Joffe 2009, s. 29). Ludność chińska starzeje się, zanim osiąga status bogactwa (por. Świeca 2008, s. 177 i nast). Do połowy stulecia średni wiek w USA będzie najniższy w zestawieniu ze wszystkimi mocarstwami z wyjątkiem Indii. Populacja pracująca w USA wzrośnie o 30%, a chińska spadnie o 3%. Starsza część chińskiego

społeczeństwa będzie wymagała przesunięcia środków z inwestycji do opieki społecznej. Będzie to zmiana rewolucyjna o dużych skutkach gospodarczych i strategicznych. W 2050 r. w Chinach będzie zamieszkiwało 329 mln emerytów. To musi obciąć środki przeznaczane na armię. Jeśli Chiny nie sprostają temu podwójnemu wyzwaniu, w jaki sposób zdeklasują USA jako światowego lidera?

Zagadką jest ekonomiczny proces podwajania gospodarki chińskiej, co przy rocznym wzroście 7% nastąpi w okresie pomiędzy 2007 a 2015 r. i w 2025 r. nastąpi kolejne podwojenie. Przyjmując wzrost amerykański na poziomie 3,5% (jest to historyczny wskaźnik długoterminowy), USA w roku 2025 powinny mieć PKB na poziomie dwukrotnie wyższym niż chiński (Świeca 2008, s. 29). Jest to kalkulacja bardziej realna, niż przyjmowanie tempa wzrostu w Chinach pochodzącego z ostatnich lat.

Choć atak chiński na USA jest nieprawdopodobny, to CHRL może zdynamizować sprzeczności wokół Tajwanu i na Morzu Południowochińskim, bardzo kłopotliwe dla funkcjonowania USA. Także koszty operacji w Afganistanie i Iraku są istotne, bo wynosiły aż 3 bln. USD. USA funkcjonują jako globalny stabilizator dokonywanych wyborów spośród zakresu różnych opcji.

USA stały się wielkim mocarstwem bez wątpienia dzięki wyrafinowanym technikom wojskowym finansowanym przez wielki budżet obronny. Należy w szczególności podkreślić rolę wyższego szkolnictwa oraz badań naukowych. W zasadzie projekty przejęcia pierwszeństwa przez Chiny na scenie globalnej w I poł. XXI w., pomijały te dwa fenomenalne czynniki[15].

Chińskie wydatki na edukację w ciągu ostatniego ćwierćwiecza, kształtowały się na poziomie 2,0-2,5% PKB, w środowisku 4-krotnie wyższej populacji niż ta w USA oraz gospodarki czterokrotnie mniejszej od amerykańskiej. W USA roczne wydatki na edukację bliskie są 6% PKB i jest to więcej niż w UE, Rosji, Indiach, Japonii. Podobny układ jest w zakresie wydatków na R&D – wskaźnik amerykański jest dwukrotnie wyższy niż chiński. Wskaźnik R&D jak i edukacja są przyszłościowe, bowiem warunkują możliwości narodów w dekadach, które nastąpią.

USA kierują się misją w świecie i wyborem roli na scenie globalnej, co je odróżnia od pozostałych mocarstw uniwersalnych. Ta samodefinicja amerykańskiego supermocarstwa, odróżnia je diametralnie od Rosji, która chce odzyskać wszystko to, co utraciła i od Chin, które chcą więcej niż miały i mają (Levin 2010, s. 31). Obaj rywale chcą więcej, ale dla siebie nie dla innych. Dlatego nie mogą one być takim podmiotem jak USA w XX w., państwem które realizując własne interesy, zarazem realizowało interesy innych i w ten sposób kreowało globalne zapotrzebowanie na dobra, które rozprowadzało. Takie działanie nie było ani altruizmem, ani też egoizmem, lecz oświeconym samo-interesem, który mnożył wpływy.

Co więc czyni USA mocarstwem niezastąpionym aktualnie? Współcześnie trudno sobie wyobrazić Chiny, Indie, Japonię, UE i Rosję jako strażników

realizujących szersze interesy. Najbliżej ideału jest UE, która nie ma ani środków, ani woli, by działać strategicznie. Rosja i Chiny funkcjonują w autorytarnym środowisku modernizacyjnym (Gat 2007, s. 59 i nast.). Okazuje się, że upadające mocarstwa – jeśli przyjąć tezę, że USA to właśnie taki przypadek – mogą dużo więcej niż państwa z dobrą prognozą rozwojową[16].

Prognozy linearne – konstruowane względem Chin – nie mogą być poprawne (Joffe 2009, s. 35). Okazuje się, że w XXI w. USA mają młodszą ludność i bardziej dynamiczną, innowacyjną gospodarkę niż ich rywale. Trzeba rozważyć jednakże dalsze możliwe sytuacje względem Chin, gdyż samo stwierdzenie, że procesy linearne rzadko zachodzą w świecie, nie wystarcza, by udowodnić stabilizację USA jako jedynego, wpływowego mocarstwa uniwersalnego o dużej przewadze nad rywalami.

Nawet jeśli według najnowszych prognoz Chiny zrównają się z USA pod kątem wielkości PKB w 2030 roku i tak będą słabe ze względu na głębokie zacofanie ogromnego terytorium, a uprzednio realizowana polityka jednego dziecka w rodzinie, przyniesie dewastację równowagi demograficzno-ekonomicznej (Nye 2010, s. 4). Ucierpi na tym jakość cywilizacji, gdyż zjawiska te uderzą w PKB *per capita*. Partycypacja obywateli w realizowanych aspiracjach ze względu na system autorytarny, nie będzie realizowana pomimo istotnych reform nowego lidera Xi Jinpinga[17]. Tak więc Chiny w nowym systemie globalnym, sieciowym nie posiadają pewnych szans bycia najsilniejszym biegunem w interpolarnym systemie jedno-wielobiegunowym.

Uwarunkowania geopolityczne roli Chin. Budowa nowego multipolarnego porządku w regionie azjatyckim

Możliwości przyszłościowe Pekinu wynikają w dużej mierze z chińskiego położenia geopolitycznego (zob. Kaplan 2010, s. 22 i nast.). Chiny aktualnie konsolidują swoje terytorium i zamierzają rozciągnąć wpływy znacznie dalej. Działania Pekinu związane są z koniecznością zagwarantowania bezpieczeństwa energetycznego, materiałów strategicznych, surowców naturalnych – tak, by zapewnić zaspokojenie potrzeb ogromnego narodu. W realizacji tych celów – Chiny natrafiają na bariery nacjonalizmów państw lokalnych. Szczególnie ważna dla Chin jest kontrola portów na Oceanie Indyjskim oraz Morzu Południowo-Chińskim. Są tu położone w większości państwa autorytarne.

Konflikt z USA na tle interakcji chińskich z tymi państwami jest pośredni, nie grozi wojną. Porty te zabezpieczają dostęp do arabsko-perskiego pasa hydrowodorowego. Opanowywanie tych obszarów przez Chiny, odbywa się według nowych technik bardziej związanych z globalizacją niż podbojami w XIX w. Projektowane wpływy chińskie rozciągają się od Centralnej Azji po Morze Południowochińskie, od rosyjskiego Dalekiego Wschodu po Ocean Indyjski. Każdy z tych subregionów jest bardzo ważny dla przyszłości Chin[18]. Wewnątrz obszaru

państwowego dwie prowincje na zachodzie: Xinjiang i Tybet sprawiają władzom najwięcej politycznych komplikacji. Ponad 45% Xinijangu to pochodzenia tureckiego Ujgurowie, nie uznający ekspansji rdzennych grup etnicznych większości chińskiej Han. Zarówno Xinjiang, jak i Tybet są bardzo istotnymi obszarami dla chińskiej terytorialnej tożsamości oraz dla strategii zewnętrznej Pekinu (Kaplan 2010, s. 26). Tybet jest zasobny w pokłady miedzi, rud żelaza i inne zasoby mineralne.

Indie z kolei – potężny sąsiad i rywal – leżą na skraju obszaru chińskich wpływów. Chiny i Indie z racji na uwarunkowania geograficzne są naturalnie predestynowane by być wielkimi rywalami. Ogromna w zasoby demograficzne, bogata kultura, sprzeczne roszczenia do pewnych terytoriów – to poważne węzły sprzeczności i napięć. Na północy rozciąga się Mongolia – obszar o bardzo słabej populacji – niezbędny Chinom ze względu na zasoby: miedzi, niklu, cynku, rud żelaza, drewna, złota. Trzy północno-wschodnie prowincje o zaludnieniu 100 mln. przylegają do rosyjskiego Dalekiego Wschodu, obszaru bardzo bogatego w surowce i zamieszkałego przez siedem mln ludności. Nie ma groźby wojskowej interwencji CHRL, ale jest intensywna imigracja ludności chińskiej i wzrastająca aktywność korporacji.

O przyszłości w budowie Wielkich Chin, zadecyduje kierunek południowo-wschodni. Wielkim krajem subregionu jest Myanmar (Birma). Chiny utrzymują aktywne, ale wyłącznie bilateralne stosunki z krajami ASEAN. Azja Centralna, rosyjski Daleki Wschód, Azja Południowo-Wschodnia – to naturalna strefa wpływów chińskich. Chiny budują także kosztem kilku bilionów dolarów dwa nowe, handlowe szlaki jedwabne do Europy i projekt ten zdaniem analityków nie powinien być negowany przez administrację amerykańską, gdyż chodzi w nim przecież o wyzwolenie zjawisk rozwojowych na ogromnej przestrzeni[19].

Według niektórych politologów, najbardziej niebezpieczne w stosunkach międzynarodowych są mocarstwa lądowe z wielkimi armiami. Chińska armia jest najliczniejsza w świecie (1,6 mln), lecz nie posiada oddziałów ekspedycyjnych i nie będzie nimi dysponowała w najbliższych dekadach. XXI w. będzie dla Chin okresem transformacji w kierunku mocarstwa morskiego.

Na morzach CHRL posiada wrogie środowisko. Punktami zapalnymi są takie miejsca jak: Półwysep Koreański, Wyspy Kurylskie, Japonia, Tajwan, Filipiny, Indonezja, Australia. System ten określa się mianem „pierwszego łańcucha wysp". *First Islands Chain* są według analityków „rewersem Wielkiego Muru"[20]: bardzo dobrze zorganizowaną linią sojuszników USA, którzy będą blokować dostęp Chin do Pacyfiku. Potęga morska uchodzi za łagodniejszą formę władzy międzynarodowej niż wojskowa siła lądowa. Ewolucja Chin w kierunku rozbudowy floty, dynamizowania handlu, jest bardzo prawdopodobnym kierunkiem rozwoju. Ponieważ Chiny wykazują mniejszy poziom samozaufania do obszarów kontrolowanych niż w przeszłości Wenecja, Wielka Brytania czy USA, jest bardzo

prawdopodobnym, że ekspansja dopiero się rozpocznie. Pojęcie *„first island chain" oraz „second island chain"* – jest bardzo pomocne przy rekonstrukcji przyszłych, chińskich strategii. Za tym drugim pojęciem kryją się obszary kluczowych wysp strategicznych: Guam i Wysp Marianów Północnych. Na wodach mórz chińskich i w ich pobliżu, w ostatnich latach okręty chińskie atakowały obce jednostki, w tym USA, bez większych sukcesów. CHRL brakuje silnej floty oceanicznej. Chiny, podobnie jak w przeszłości ZSRR, budują zręby silnej floty podwodnej. To może pokrzyżować łatwy dostęp USA do zachodnich wybrzeży Pacyfiku. Chiny nie zamierzają atakować jednostek amerykańskich, ale stwarzać dla nich ciągłe wyzwania. Podstawą władzy jest przecież wpływanie na zachowanie/działania adwersarza. Można się liczyć z tym, że idea Wielkich Chin będzie realizowana zarówno na lądzie, jak i na morzu.

Dla budowy Wielkich Chin niezbędne jest opanowanie Tajwanu, który gen. D. MacArthur nazywał: „niezatapialnym lotniskowcem", drogą do wybrzeża chińskiego. Dla oceanicznych strategów, takich jak Holmes i Yoshihara, Tajwan jest miejscem, z którego mocarstwo zewnętrzne (USA) może promieniować wpływami na wybrzeże chińskie. Jeśli Tajwan wróci do Chin, flota CHRL nie tylko ulepszy swoją rywalizacyjną pozycją stosunku do *„first island chain",* ale i rozwinie władzę do niespotykanego wcześniej stopnia.

Włączenie Tajwanu do Chin będzie oznaczało powstanie nowego multipolarnego porządku w regionie azjatyckim. Według studium RAND z 2009 r. (za: Luft 2016, s. 36), w roku 2020, USA nie będą w stanie zagwarantować bezpieczeństwa Tajwanowi przed ewentualnym atakiem Pekinu. Obrona Tajwanu przez USA dla Japonii, Filipin, Australii, a nawet Indii, oznacza rzetelność w wykonywaniu zobowiązań sojuszniczych. USA i Tajpej muszą znaleźć asymetryczne sposoby, by równoważyć CHRL. Tu już nie chodzi o militarne pokonanie Pekinu w Cieśnienie Tajwańskiej, ale uczynienie, by planowanie wojny przez CHRL stało się nieopłacalne. Walka o Morze Południowowchińskie będzie zacięta bo jest to azjatyckie Morze Śródziemne dla CHRL i serce geopolityczne w zbliżających się dekadach[21].

Chiny nie chcą konfrontacji wojennej z USA w sposób otwarty. W sytuacji jak spada relatywne znaczenie międzynarodowe USA i wzrasta chińskie, multipolarność będzie w sposób wzrastający definiowała interakcje w teatrze azjatyckim. Mocarstwa Azji Południowej i Wschodniej się zbroją. Chiny budują potężną bazę marynarki wojennej dla okrętów podwodnych na wyspie Hannan, Japonia, Płd. Korea modernizują swoje okręty, Indie są w trakcie rozbudowy potężnej floty. Wielostronne interakcje Chin muszą w minimalnym wymiarze przynieść kontakt z Indiami i Rosją.

Azja cierpi na kryzys przestrzeni. Czy Stany Zjednoczone mogą jednocześnie stabilizować region, wspierać sojuszników, utrudniać powstanie Wielkich Chin oraz omijać konflikty wojenne?

Indie, Japonia, Korea Południowa chcą, by Waszyngton zaistniał w przestrzeni azjatyckiej i na wodach kontynentu w sposób trwały, a nie doraźny. Przyszłość relacji amerykańsko-indyjskich nie jest wcale klarowna. Ta perspektywa będzie uzależniona od przyszłego wyboru USA jako trwałego sojusznika Delhi, i czy system podtrzyma pozytywne zmiany socjalne oraz gospodarcze, a także jaką politykę Waszyngton wybierze w tym subregionie, co musi zaważyć na indyjskich interesach (Feigenbaum 2010, s. 76-91). Jeden z planów – plan płk. Pata Garreta – zakłada wprowadzenie do regionu Euroazji znaczenia strategicznego – Oceanii (Kaplan 2010, s. 39).

Rola Oceanii będzie coraz większa, gdyż Chiny nie zakładają gorliwego utrudniania dostępu USA do tych obszarów. Guam, Karoliny, wyspy Marshalla, Płn. Mariany, wyspy Salomona – są bardzo korzystnie położone, blisko Korei, a bazy na nich mniej prowokują niż w Japonii. Według planu Garreta, amerykańska marynarka wojenna i siły powietrzne konstytuują „istotną obecność regionalną", ulokowaną zaraz „za horyzontem" od umownych, informacyjnych granic Wielkich Chin i od głównej linii oceanicznej Euroazji[22].

Umacnianie sił morskich i powietrznych w Oceanii, będzie kompromisowym podejściem pomiędzy oporem wobec utworzenia Wielkich Chin a przyzwoleniem na przyszłość, w której chińska flota będzie policyjnie nadzorowała „pierwszy łańcuch wysp" (Kaplan 2010, s. 40). To podejście będzie także oznaczało, że Chiny zapłacą wysoką cenę za agresję militarną przeciwko Tajwanowi. Plan Garreta przewiduje ekspansję amerykańską na Oceanie Indyjskim.

Wielkie Chiny mogą powstać w wymiarze politycznym, ekonomicznym lub militarnym w Azji Centralnej, na Oceanie Indyjskim, w Azji Południowo-Wschodniej i na Zachodnim Pacyfiku. Będzie temu towarzyszyła transformacja chińskiej floty od formacji przybrzeżnej do struktur w pełni oceanicznych. Sytuacja jest dużo lepsza dla Amerykanów teraz niż była w okresie zimnej wojny, kiedy to obok potrzeby równoważenia radzieckich sił morskich, trzeba było wysłać na kontynent europejski potężne siły lądowe. Takie siły na granicy Euroazji nie będą potrzebne, a przewaga amerykańskiej floty nad chińską pozostanie długo jako druzgocąca. Sygnalizacyjnym mechanizmem dramatu XXI w. będzie fakt, że supermocarstwo zachodniej hemisfery będzie próbowało uniemożliwić Chinom uzyskanie statusu hegemona na większej części wschodniej hemisfery.

Podejście Chin do problematyki rozwoju, uczyniło z Państwa Środka giganta finansowego, a jego symbolem stał się Ludowy Bank Chin i wzrastające znaczenie waluty – yuana (Miller 2010, s. 96). W system chińskiej finansowej strategii uzależniania suwerennych państw, wpada coraz większa ilość podmiotów międzynarodowych, włącznie ze Stanami Zjednoczonymi. Spojrzenie na amerykańskie finanse po 2020 r. jest krytyczne i pesymistyczne, nawet wstrząsające. USA są wielkim dłużnikiem, a jego wierzycielami są kraje rozwijające się, w tym głównie Chiny. Prawdopodobnie 50% zadłużenia amerykańskiego

resortu skarbu, spoczywa w rękach zagranicznych wierzycieli w tym 22% w CHRL. Wpływowa teza P. Kennedy`ego o „przestrzennym rozciągnięciu" imperium i „przeinwestowaniu" jest według niektórych analityków przesadzona , gdyż koszt wojen w Iraku i Afganistanie – to tylko 10-15% deficytu budżetowego USA. Łącznie wojny te kosztowały jednak aż 3 bln. USD.

To głównie niepowodzenia finansowe, gospodarcze i polityczne USA w kraju są prawdziwą przyczyną słabości w systemie globalnym (Miller 2010, s. 34).

Oczywiście relatywne zagrożenie „reszty świata", w tym głównie Chin istnieje. Chiny stają się mocarstwem finansowym w czasie, gdy USA przeżywają kryzys finansowy. O wpływach świadczą głównie zagraniczne inwestycje bezpośrednie, a one nie są najwyższe w przypadku CHRL. Większość chińskich FDI (*Foreign Direct Investment*) wychodziło z korporacji państwowych. Ilość inwestycji w ostatnich latach była zaskakująco niska (Miller 2010, s. 102).

Chińskie firmy napotykają opór obcych korporacji przy wielkokalibrowych próbach przejmowania ich udziałów. Wiele amerykańsko-chińskich ekonomicznych problemów zależy od polityki finansowej (walutowej), polityki zatrudnienia i zblokowanych z nimi finansowych braków równowagi. CHRL pojawiła się jako potęga finansowa na scenie globalnej dziesięć lat temu. Waszyngton musi lepiej zrozumieć imperatywy krajowe Chin, lepiej współuczestnicząc w projektowaniu globalnej aktywności Pekinu. W ten sposób USA intensywniej przyczynią się do budowy stabilnego bezpiecznego świata. Jest to wizja dość optymistyczna. Powstaje jednak pytanie, co będzie ze światem, gdy USA jako supermocarstwo upadną szybko i nagle (Fergusson 2010, s. 18-32). Taki model dynamicznej destrukcji ważnego podmiotu zdarzał się w historii dość często. Kryzys rozpoczęty w 2008 r. ciągle skutkuje słabnącą pozycja USA i Europy Zachodniej (Altman 2010, s. 2-14).

*

Musimy jednakże – jak zaznacza amerykański analityk Joseph S. Nye, Jr – unikać mylących metafor upadku właściwego strukturom organicznym, bowiem narody nie są istotami biologicznymi z zakreślonym życiorysem (Nye 2010, s. 2). Państwa są podmiotami działającymi w środowisku wytworzonym przez rewolucję informatyczną i procesy globalizacyjne. Większe zagrożenie niż ze strony nowych mocarstw – jak Chiny, Indie czy Brazylia – może przyjść ze strony nowych barbarzyńców i aktorów niepaństwowych. W świecie zdominowanym przez informatykę, dyfuzja władzy stanowi większe zagrożenie niż transformacja władzy (Nye 2010, s. 2).

Jeśli jednak współczesny system międzynarodowy okaże się mało elastyczny by ulec zmianie, po prostu rozpadnie się (Slaughter 2016, s. 83). W teorii systemów, poziomy organizacji systemów zamkniętych pozostają takie same przez dłuższy czas lub ulegają degradacji. W systemach otwartych jest odwrotnie –

w oparciu o nowe wyzwania mogą one omijać przeszkody wywołane zmianami relacji w płaszczyźnie oddziaływań pomiędzy mocarstwami i inkorporować nowe sieci. Dotychczasowy system międzynarodowy, który uosabia Bank Światowy, Międzynarodowy Fundusz Walutowy, a przed wszystkim ONZ, został utworzony dla zabezpieczenia interesów wielkich mocarstw (Slaughter 2016, s. 84).

Instytucje zbudowane po wojnie muszą zostać tak przebudowane, by stać się osią bardziej elastycznego i szybko działającego systemu. Ten nowy układ obok państw musi uwzględniać aktorów niepaństwowych oraz relacje obywateli z nimi. Wielka strategia amerykańska powinna koncentrować się na ustanowieniu otwartych społeczeństw, otwartych rządów i otwartego systemu międzynarodowego (Slaughter 2016, s. 87). Strona formalno-prawna tego porządku winna ochraniać państwa i obywateli. Sfera krajowa i międzynarodowa systemu muszą być rozdzielane granicami przepuszczalnymi. Ten podwójny porządek słabo jawi się jako wyraźna wizja, ale jest pewne, że stary nie wytrzyma próby czasu. Nowy porządek powinien zwielokrotnić wpływy i władzę obywateli. Dokonuje się to pod wpływem wstrząsu, który został wywołany transformacją globalną na przełomie XX i XXI w. i jak zaznacza Henry Kissinger, uprzednio realia te wystąpiły w obszarze niemieckim po wojnie 30-letniej, gdy na obszarze niemieckojęzycznym wyginęła 1/3 ludności. Faktycznie Traktat Westfalski stworzył taki system ochronny poprzez nowe struktury i orientacje religijne (Slaughter 2016, s. 89). Rozwiązania sieciowe dają obywatelom znacznie więcej władzy. Póki ich wizja nie przeistoczy się w konkretne strategie działań, mogą pozostać utraconą nadzieją.

Przypisy

[1] O interaktywności współczesnego świata szeroko pisze w całej monografii Z. Brzeziński (Brzeziński 2013).
[2] „Otwartość" została zdefiniowana w (Slaughter 2016, s. 77-78).
[3] Szersza analiza pojęć w (Slaughter 2016, s. 81).
[4] Autorem pojęcia system interpolarny jest Senior Research Fellow w Instytucie Studiów Strategicznych UE (zob. Grevi 2009).
[5] Ten klimat wnioskowania widoczny jest w całym tekście książki (zob. Zakaria 2009).
[6] Ciągle wielką mocarstwowość USA charakteryzuje optymistycznie: (Joffe 2009, s. 21-35).
[7] Priorytety Zakarii zlokalizowane są w rejonach „reszty świata" czyli w Chinach – określonych jako rywal i Indiach – zdefiniowanych jako sojusznik (zob. Zakaria 2009, s. 116-192).
[8] Opinię Richarda Holbrooka cytuje G. Grevi (Grevi 2009, s. 11).
[9] Terminu jedno-wielobiegunowy używa S. P. Huntington (Huntington 1999, s. 35-49).
[10] Takiego zdania jest Nicholas Stern.
[11] O „gasnącym" Zachodzie i zmierzchu amerykańskiego snu pisze także: Z. Brzeziński (Brzeziński 2013).
[12] Rosja posiada wielkie interesy, by współpracować z Zachodem (zob. Trenin 2009, s. 64-78).

[13] Zadłużenie publiczne może wyhamować dalszy rozwój kraju i jest dowodem na redukcję przyszłych możliwości. W Wielkiej Brytanii dług publiczny wynosi 88%, a w Niemczech ok. 80% (zob. Zakaria 2013, s. 26 i nast.).
[14] Ewolucja potęgi chińskiej od 1820 r. po rewolucję w 1949 r. jest ewidentna. Chiny były już wielką potęgą gospodarczą (zob. Lampton 2007, s. 117).
[15] Postęp edukacji w państwach azjatyckich jest wielki. Dla Zachodu wzrost rangi uniwersytetów azjatyckich jest szansą, a nie zagrożeniem (zob. Levin 2010, s. 63-75).
[16] Tą ryzykowna tezę uzasadnia J. Joffe (Joffe 2009, s. 34).
[17] Reformy Xi Jinpinga szeroko analizuje E. C. Economy (Economy 2014, s. 80-91).
[18] Niektórzy analitycy przewiązują szczególną wagę do obszaru Azji Południowo-Wschodniej (zob. Bond, Simons 2009, s. 52-63).
[19] Szerzej na temat nowego szlaku jedwabnego pisze G. Luft (Luft 2016, s. 68-75).
[20] Takiego zdania jest John Holmes i Toshi Yoshihara z U. S. Naval War College (Luft 2016, s. 33).
[21] Parafrazując wybitnego amerykańskiego geopolityka Spykmana (Luft 2016, s. 37).
[22] *„Region al presence in being"* to określenie stare historycznie, stworzone przez Sir Johna Corbettsa, dla którego *"fleet in being"* oznaczała rozproszone okręty, które mogły przejść bardzo szybko w grupę zdolną do zdecydowanego ataku (Kaplan 2010, s. 40).

Bibliografia

Aron, R. (1995) *Pokój i wojna między narodami (teoria*). Warszawa: Centrum im. A. Smitha.

Altman, R. C. (2010) *The Great Crash.* "Foreign Affairs", No 1, vol. 88.

Altman, R. C., Haass, R. N. (2010) *American Profligacy and Merican Power. The Cosequences of Fiscal Irresponsibility.* "Foreign Affairs", No 6, vol. 89, ss. 25-34.

Bales, C. F., Duke, R. D. (2008) *Containing Climate Change. "*Foreign Affairs", No 5, ss. 78-89.

Bond, Ch. S., Simons L. M. (2009) *The Forgotten Front.* "Foreign Affairs", No 6, vol. 88, ss. 52-63.

Brzeziński, Z. (2013) *Strategiczna wizja. Ameryka a kryzys globalnej potęgi*. Kraków: Wydawnictwo Literackie.

Eberstadt, N. (2010) *The Demographic Future. What Population Growth – and Decline – Merans for the Global Economy*. "Foreign Affairs", No 6, vol. 89, ss. 54-64.

Eberstad, N., Groth, H. (2007) *Healthy Old Europe.* „Foreign Affairs", No 3, vol. 86, ss. 55-68.

Eberstadt, N. (2010) *The Demographic Future. What Population Growth – and Decline – Merans for the Global Economy. "*Foreign Affairs", No 6, vol. 89, ss. 54-64.

Economy, E. C. (2014) *Chinaś Imperial President. Xi Jinping Tightens His Grip.* "Foreign Affairs", No 6, vol. 93, ss. 80-91.

Feigenbaum, E. A. (2010) *India`s Rise, America`s Interest*. „Foreign Affairs", No 2, vol. 89, ss. 76-91.

Fergusson, N. (2010) *Complexity and Collapse.* „Foreign Affairs", No 2, vol. 89, ss. 18-32.

Flynn, S. E. (2008) *America the Resilient.* „Foreign Affairs", No 2, vol. 87, ss. 2-8.

Gat, A. (2007) *The Return of Authoritarian Great Powers.* "Foreign Affairs", No 4, vol. 86.

Gelb, L. H. (2010) *GDP Now Matters More Than Force. A U.S. Foreign Policy for the Age of Economic Power.* „Foreign Affairs", No 6, vol. 89, ss. 35-43.

Goldstone, A. (2010) *The New Populations Bomb. The Four Magatrends That Will Change The World.* "Foreign Affairs", No. 1, vol. 89, ss. 31-43.

Grevi, G. (2009) *The interpolar World: a new scenario.* "Occasional Paper", No 79.

Haass, R.N. (2008) *The Age of Nonpolarity. What Will Follow U.S Dominance*. "Foreign Affairs", May/June, vol. 87, No 3.

Haass, R. N. (2006) *The New Middle East.* „Foreign Affairs", No 6, vol. 85, ss. 2-11.

Huntington, S. P. (1999) *The Lonely superopower*. „Foreign Affairs", No 2, vol. 78, ss. 35-49.

Joffe, J. (2009) *The Default Power*. „Foreign Affairs", No 5, vol. 88, ss. 21-35.

Kaplan, R. D. (2010) *The Geography of Chinese Power. How far can Bejing Reach on land and at sea.* „Foreign Affairs", No 3, vol. 89, ss. 22-41.

Kennedy, P. (2009) *The Rise and Fall of GreatPowers.* Za: Joffe, J. (2009) *The Default Power. The False Prophecy of America`s Decline*. „Foreign Affairs", No 5, vol. 88, ss. 21-35.

Kupchan, Ch. A. (2008) *Minor League. "*Foreign Affairs", No 6, vol. 87, ss. 96-109.

Lampton, D. M. (2007) *The Faces of China Power*. „Foreign Affairs", No 1, vol. 86, ss. 115-127.

Levi, M. A. (2009) *Copenhagen`s Incovenient Truth.* „Foreign Affairs", No 5, vol. 88, ss. 93-104.

Levi, M. A. (2009) *Copenhagen`s Incovenient Truth*. „Foreign Affairs", No 5, vol. 88, ss. 92-104.

Levin, R. C. (2010) *Top of the Class. The Rise of Asia`s Universities*. „Foreign Affairs", No 3, vol. 89, ss. 63-75.

Luft, G. (2016) *China`s Infrastructure Play. Why Washington Should Accept the New Silk Road.* „Foreign Affairs", No 5, vol. 95, ss. 68-75.

Miller, K. (2010) *Coping z China`Financial Power.Beiiing`s Financial Foreign Policy.* "ForeignAffairs", No 4, vol. 89, ss. 96-109.

Nye, J. S., JR. (2010) *The Future of American Power. Dominance and Decline in Perspective*. "Foreign Affairs", No 6, vol. 89, ss. 2-12.

Ruhl, Ch. (2010) *Global Energy After the Crisis.* „Foreign Affairs", No 2, vol. 89.

Slaughter, A. M. (2016) *How to Succedin the Networked World. A Grand Strategyforthe Digital Age*. "Foreign Affairs", No 6, vol. 95, ss. 76-89.

Świeca, J. (2008) *Światowy układ sił oraz transnarodowy system bezpieczeństwa w pierwszych dekadach XXI w. Analiza potencjałów głównych podmiotów światowych.* W: Panecki, T. (red. nauk.), *Polityka bezpieczeństwa Polski w XX wieku i na początku XXI w wieku. (Wybrane problemy)*. Częstochowa: AJD.

Trenin, D. (2009) *Russia Reburn.* „Foreign Affairs", No 6, vol. 88, ss. 64-78.

Victor, D. G., Yueh, L. (2010) *The New Energy Order.* „Foreign Affairs", No 1, vol. 89, ss. 61-73.

Zakaria, F. (2009) *Koniec Hegemonii Ameryki*. Warszawa: NADIR. Media Lazar.

Zakaria, F. (2013) *Can America Be Fixed/The New Crisisa of Democracy*. „Foreign Affairs", No 1, vol. 92, ss. 22-33.

Streszczenie

W artykule przeanalizowano globalną scenę w pierwszych dekadach XXI w. Autor ocenia, że świat opisywany za pomocą teorii interpolarnej jest strukturą realnie istniejącą, a nie programem na przyszłość, nie jest także jedynie podejściem metodologicznym. W przeciwieństwie do wielobiegunowości – która koncentruje się na wielu biegunach i ogniskach siły – międzynarodowy system interpolarny można scharakteryzować poprzez wielość centrów wyposażonych w znaczącą władzę. Na pierwszy rzut oka współczesny system jest multipolarny. Interpolarność – opisana przez G. Greviego – akcentuje dwa istotne trendy rozwojowe: asymetryczną redystrybucję władzy na scenie globalnej prowadzącą do nowych form multipolarności oraz pogłębiające się współzależności . Ta wizja dająca realny obraz dzisiejszego świata, nie udziela odpowiedzi na pytanie: – kto

zastąpi USA jako lidera światowego?, ponieważ nowy świat nie będzie miał lidera opisanego według tradycyjnych poglądów, a USA są nadal mocarstwem w dobrej kondycji, a nie mocarstwem upadającym. Oczywiście jako pojedyncze mocarstwo, Chiny stanowią wielkie wyzwanie dla USA. Prezydent Donald Trumph winien zatwierdzić wielką strategię budowy otwartego międzynarodowego porządku bazującego na trzech filarach: otwartych społeczeństwach, otwartych rządach oraz otwartym międzynarodowym systemie.

Słowa kluczowe: system interpolarny, system jedno-wielobiegunowy, struktura sieciowa

Interpolarity In The Global Uni – Multipolar System

Summary

The article is analysing the global scene in the first decade of XXI c. The author estimated that the world described by the theory of interpolarity is real structure, not a program for future, is not only as well, the methodological approach. In contrast to multipolarity –which involves several distinct poles or concentrations of power – a interpolar international system is characterized by numerous centers with meaningful power. At first glance, the world today may appear to be multipolar. Interpolarity-described by G.Grevi- underlined two main trends of development: asymmetric redistribution of power on the global scene leading to a new form of multipolarity, and deepening interdependences. These vision give real picture of today's world is not answering to main question: who will replace U.S. as the leader? – since a new world will not have a leader known from the traditional point of view and the U.S is the superpower in good condition and not a descent, default power. Of course – as a single superstate – the China creating the main challenge to Washington. President Donald Trump should adopt a grand strategy of building an open international order based on three pillars: open societes, open governments, an open international system.

Keywords: interpolarity system, uni-/multpolar system, networked structure

Olga Wasiuta
Sergiusz Wasiuta
Uniwersytet Pedagogiczny w Krakowie

Wojna informacyjna zagrożeniem dla bezpieczeństwa ludzkości

Wstęp

Jedną z form ochrony jakiegokolwiek państwa jest bezpieczeństwo jego przestrzeni informacyjnej. Kto kontroluje przestrzeń informacyjną, ten kontroluje państwo. Ten aksjomat jest tak stary jak ludzkość. Dlatego władze różnych państw wykorzystują mass media dla wpływów informacyjnych na społeczeństwo, w tym na społeczność międzynarodową dla obrony swoich interesów narodowych.

Z początkiem aneksji Krymu i konfliktu rosyjsko-ukraińskiego na wschodzie Ukrainy rośnie zainteresowanie problemami wojny informacyjnej, która jest bezpośrednim zagrożeniem dla ludzkości. Przedmiotem tej wojny jest świadomość ludzi, próba zmiany odpowiedniego postrzegania rzeczywistości i życia w świecie iluzji. Opiera się ona na zdolności do zarządzania i manipulacji świadomością publiczną w celu podporządkowania woli człowieka. Najczęściej osoba manipulowana jest nieświadoma manipulacji i informacyjno-psychologicznego działania (11, s. 184).

Konieczne jest zatem, aby zrozumieć naturę i technologię władzy informatycznej nad ludźmi, ponieważ brak kontroli może prowadzić nie tylko do masowej eksterminacji odrębnych narodów, ale także do zniszczenia współczesnej cywilizacji jako całości (30, s. 6)

Wojna informacyjna – to wpływ na ludność cywilną i/lub wojskową innego kraju poprzez rozpowszechnianie odpowiednio dobranych informacji. Obiektem wojny informacyjnej jest zarówno zbiorowa świadomość, jak i indywidualna. A wpływ informacyjny może odbywać się zarówno w tle szumu informacyjnego i w próżni informacyjnej. Wprowadzenie w życie obcych celów sprawia, że wojna informacyjna staje się wojną i odróżnia ją od zwykłej propagandy. Zasobami wojny informacyjnej są różne narzędzia komunikacji – od mediów do poczty i plotek. Informacje te obejmują przeinaczenia faktów lub narzucanie obywatelom emocjonalnego postrzegania, wygodnego agresorowi.

Cyberprzestrzeń odgrywa coraz ważniejszą rolę w strategicznej komunikacji jako nasze uzależnienie od nowoczesnych technologii, sieci komputerowych i Internetu. Uzależnienie to rośnie z dnia na dzień. Wykorzystujemy cyberprzestrzeń do odbierania i przekazywania informacji, w celu koordynacji naszych działań, a także do analizy otoczenia wokół siebie w celu wykrywania i oceny potencjalnych zagrożeń. Cyberprzestrzeń jest często wykorzystywana w konfliktach. Jednak konflikt w Ukrainie pokazał, że cyberprzestrzeń może

również odgrywać rolę w prowadzeniu operacji, gdzie głównymi celami nie są maszyny lub sieci, ale umysły ludzi. Internet i media społecznościowe, ze względu na ich zdolność do upowszechniania informacji w szybkim tempie i niewielkim kosztem, są coraz częściej wykorzystywane przez propagandę rosyjską i wojnę informacyjną. Dzięki nim można zmienić zarówno percepcję podmiotu oddziaływania, jak i śledzić początkowe źródło informacji, sprawdzać jego autentyczność, oddzielić fakty od fikcji. Wraz ze wzrostem popularności platform społecznościowych, rozszerza się koncepcja społecznego cyberataku. Jej realizację umożliwiają niskie koszty i szybki sposób manipulowania społeczeństwem w celu spowodowania niepożądanego zachowania w prawdziwym życiu. Cyberataki na media społecznościowe obserwowane podczas konfliktu rosyjsko-ukraińskiego doprowadziły do wniosku, że większość z nich była realizowana w sposób zorganizowany jako część większej strategii wpływu (3, s. 104).

Wojna hybrydowa a wojna informacyjna

Wojna hybrydowa jest często interpretowana jako coś nowego, ale większość jej części składowych spotykało się wcześniej i były one używane prawie we wszystkich wojnach w przeszłości. Wyjątkowa jest spójność i konsolidacja tych elementów, dynamizm i elastyczność ich stosowania. Dodatkowo szczególną rolę zaczął w niej pełnić element informacyjny, który stał się niezależną częścią, nie mniej ważną niż komponent wojskowy, w celu tworzenia warunków do uznania przez własne społeczeństwo wojny sprawiedliwą. Właśnie dlatego rosyjska aneksja Krymu i agresja we wschodniej Ukrainie stały się nowym impulsem do analizy i oceny zjawiska współczesnej „wojny hybrydowej".

Jednak osobliwością tego konfliktu jest propaganda informacyjno-psychologiczna, którą można traktować jako wojnę informacyjną.

Rosja przygotowywała się do wojny hybrydowej przeciwko Ukrainie na długo przed rozpoczęciem Rewolucji Godności. Teoria, strategia i taktyka nowoczesnej hybrydowej wojny, którą Rosja postrzega jako totalną wojnę na wszystkich poziomach, rozpoczęto w ZSRR od 1987 roku. Od tego czasu do chwili obecnej Rosja wykorzystuje nie tylko badania i doświadczenia ZSRR, ale również doświadczenia USA, NATO i UE. Przykładem może być koncepcja bezpieczeństwa publicznego pod nazwą „Martwa woda" (wydanie pierwsze – koniec 1994 r., drugie – 1996 r.), którą zaczęto przygotowywać w 1987 roku dzięki inicjatywie grupy publicznej „Wewnętrzny Predictor ZSRR" (18).

W ramach teorii koncepcji bezpieczeństwa publicznego wojna została przedstawiona w postaci sześciu poziomów (priorytetów kontroli ludzkości). Z 6 priorytetów tylko jeden był wojskowym, pozostałe 5 są metodami wojny informacyjnej (jednocześnie potężnymi środkami broni informacyjnej) (54). Są to poziomy:

- ideologiczny: poglądy społeczeństwa na kluczowe pojęcia dobra i zła, życia i wszechświata;
- chronologiczny: „przepisz historię narodu, i ty podbijesz go"; Rosja wykorzystuje mity historyczne, aby uzasadnić swoje roszczenia do „post-sowieckiej" przestrzeni i Europy Wschodniej;
- faktologiczny: dogmaty, ideologia, kulty religijne, technologia, nawiązywanie do norm kultury, ideologii, sposobu życia (alkoholizm, łapówkarstwo, kult władzy państwowej); Rosyjski Kościół Prawosławny jest aktywnie zaangażowany w konflikt w Ukrainie i w pełni popiera politykę Władimira Putina; zdarza się, że kapłani Kościoła Prawosławnego Patriarchatu Moskiewskiego błogosławią terrorystów, którzy walczą przeciwko Ukrainie (13; 39; 49).
- gospodarczy jako środek wpływu przez finanse; na przykład, próby gwałtownego upadku hrywny związane nie tylko z czynnikami wewnętrznymi, (chociaż ich wpływ jest wielki), ale także z działaniami niektórych rosyjskich banków, które działają na terytorium Ukrainy;
- broń genetyczna (ludobójstwo) lub ekologiczna, która wpływa nie tylko na dane pokolenie (zły stan zdrowia, aż do śmierci), ale także przyszłe pokolenia (zmiany w genach następnych pokoleń); narkotyki, alkohol;
- broń wojskowa, narzędzia destrukcji – broń w tradycyjnym tego słowa znaczeniu, która zabija i kaleczy ludzi, niszczy materiały i obiekty techniczne cywilizacji; od początku 2014 roku w czasie rozpętanej przez Rosję wojny w Ukrainie zginęło już około 10 tysięcy Ukraińców, w tym ponad 2,5 tys. wojskowych z Sił Zbrojnych innych służb mundurowych (7), 22431 zostało rannych, ponad 2 mln. osób zostało wewnętrznymi migrantami (19; 20; 34; 52); samo rozminowanie Donbasu zajmie Ukrainie 10-15 lat (30).

Wśród niekonwencjonalnych („innowacyjnych") szkół wojskowo-strategicznej myśli można wydzielić cztery główne kierunki: „miatieżwojna" (31; 12), bezkontaktowa zdalnie sterowana wojna (53), cyberwojna (25; 35; 36; 37) i wojna „na pokonanie świadomości" („świadomościowa", w języku ros. *консциентальная война* – od łac. *conscientia*) (29; 24). U podstaw koncepcji wojny „na pokonanie świadomości" leży zniszczenie ludzkiej zdolności do identyfikacji, czyli do samostanowienia tego, kim dana osoba próbuje być i w ramach jakiej tradycji kulturowej i historycznej. Po zniszczeniu tej zdolności, podmiotowi może być nadawana lub indukowana jakaś inna identyfikacja, która z jakiegoś powodu jest potrzebna od zewnątrz. Identyfikacja jest oparta na podstawie wyobraźni – umiejętności wytwarzania obrazów i zasadniczych symboli. Właśnie symboliczne rządy i sama wyobraźnia ulegają rozwarstwieniu lub załamaniu w pierwszej kolejności (24, s. 86).

W 1997 roku jako dodatek do czasopisma „Rosja – 2010" została opublikowana książka „Kto będzie właścicielem konscijentalnej

(świadomościowej) broni w XXI wieku?" (27). Pomimo faktu, że minęło prawie dwadzieścia lat, wiele pomysłów renomowanych autorów jest nadal aktualnych. Główną tezę książki, która definiuje istotę wojny świadomościowej, charakteryzuje Jurij Gromyko (15), który pisze: *Wojna świadomościowa sugeruje, że świat wszedł w nową fazę walki – konkurencji form organizacji świadomości, gdzie przedmiotem klęski i zniszczenia są pewne rodzaje świadomości. Oznacza to, że w wyniku wojny świadomościowej niektóre rodzaje świadomości trzeba zniszczyć, żeby one przestały istnieć.* […] *Rodzaje świadomości – przedmioty porażki w wojnie świadomościowej – muszą być wypchnięte poza cywilizacyjno-dopuszczalne formy. To działo się i wcześniej, gdy jeden rodzaj organizacji świadomości wypierał drugi, jak na przykład chrześcijaństwo zastąpiło pogaństwo* […] *Bardzo ważne jest, aby uświadomić sobie, że zniszczenie niektórych rodzajów świadomości polega na niszczeniu i reorganizacji społeczności, które tworzą ten rodzaj świadomości* (15).

J. Gromyko opisał również pięć głównych sposobów niszczenia świadomości w walce świadomościowej:

1. uraz mózgowego podłoża, który zmniejsza poziom działania świadomości; może być oparty na bazie działania substancji chemicznych, zatrutego przez dłuższy czas powietrza, żywności, skierowanych radiacyjnych wpływów,
2. zmniejszenie poziomu organizacji informacyjno-komunikatywnego środowiska na podstawie jego dezintegracji i prymitywizacji, w której funkcjonuje i „żyje" świadomość,
3. wpływ okultyzmu na świadomość na podstawie skierowanego przesłania myślowych form przedmiotom oddziaływania;
4. specjalna organizacja i dystrybucja przez kanały komunikacji obrazów i tekstów, które niszczą pracę świadomości (warunkowo może być wyznaczona jako broń psychotropowa),
5. zniszczenie sposobów i form identyfikacji osoby w odniesieniu do trwałych społeczności, co prowadzi do zmiany formy samostanowienia i do depersonalizacji (15; 28; 40, s. 32).

Najwyższym osiągnięciem właściwie zorganizowanej wojny świadomościowej – wojny na pokonanie świadomości i jej zdolności do swobodnej identyfikacji – jest stworzenie takiej sytuacji, w której w środku działań wojennych oraz w warunkach katastroficznych dla społeczeństwa (w tym i zawodowych polityków i wojskowych, włączając elitę) staje się absolutnie oczywiste i znaczące uczucie największego spokoju i przekonania, że wojna jest gdzieś bardzo daleko (24, s. 87).

Inny rosyjski badacz W. Potekhin stwierdza, że wojna świadomościowa – to jest *wojna psychologiczna za kształtem, cywilizacyjna według treści i informacyjna według funduszy, w której przedmiotem zniszczenia i transformacji są kierunki moralności i wartości społeczeństwa wroga, w wyniku czego pierwotne cele są zastąpione drugorzędnymi, trzeciorzędnymi i bardziej przyziemnymi, ze*

zwiększonym prawdopodobieństwem do ich realizacji, „osiągnięcie zastępujących celów jest postrzegane jako jego błogosławieństwo". Ze względu na bezpośredni związek z wartością i moralnością człowieka do kultury swego narodu, autor podkreśla, że celem zniszczenia w wojnie świadomościowej jest powłoka kulturowa wroga, a tak jak kultura jest rdzeniem cywilizacji, jest to kwestią zniszczenia cywilizacji (44, s. 73).

Jeden z badaczy rosyjskich – Sergiej Anchukov (12) – jeszcze w 2002 r. napisał, że postindustrialne społeczeństwo informacyjne doprowadziło do depersonalizacji wojny i do przejścia od „doktryny wojny totalnej E. Ludendorffa" do doktryny globalnej „wojny informacyjnej". Podkreśla on, że wojna na naszych oczach zmienia się w „wojnę sieciową" i walkę w przestrzeni globalnej komunikacji, gdzie polem bitwy jest cały glob, ale dla realizacji strategii działań pośrednich, korzystnych tylko dla jednej ze stron. Dalej stwierdza, że najbardziej narażone na atak sieciowy są Stany Zjednoczone z ich masową komputeryzacją. A kiedy wojna toczy się na monitorach – to haker jest jedną z kluczowych postaci „przyszłości zawodowej armii". Kiedy komputerami w wojsku manipulują głównie utalentowani ludzie dobrze zorientowani w strategii, linia między działaniami wojskowymi i pozamilitarnych jest bardzo umowna i niejasna (12).

Arsenał wojny informacyjnej

Głębokiej analizy teorii powstania i rozwoju **wojny informacyjnej** we współczesnym świecie dokonał amerykański profesor Philip Taylor, który w swojej książce „Globalne komunikacje, stosunki międzynarodowe i media po 1945 r." (6) udowadnia, że szybki rozwój cywilizacji, nowe technologie komunikacji masowej mają decydujący wpływ na rozwój stosunków międzynarodowych we współczesnym świecie. „Zaczynając od XX w. media realnie wpływają na rozwój nowej historii świata" – podkreśla Philip Taylor (5). Szczegółowej analizie Taylor poddaje wpływ mediów na rozwój wydarzeń międzynarodowych w czasie tak zwanej „zimnej wojny", wojny w Wietnamie i Zatoce Perskiej. Właśnie rewolucja w technologii komunikacji doprowadziła do powstania tak zwanych supermocarstw. Taylor twierdzi, że podczas II wojny światowej globalnego wpływu mass mediów jeszcze nie odczuwało się, a nawet w czasie konfliktu o Falklandy w 1982 roku. Ale w czasie wojny w Zatoce Perskiej pojawiła się radykalna i niebezpieczna jednocześnie rola mediów. Media same stały się przedmiotem konfliktu, a nie świadkiem. Często media świadomie działały jako nośniki dezinformacji. Na przykład, media wielokrotnie podawały informację, że atak na Irak zacznie się od strony morza, podczas gdy w rzeczywistości armia Husajna była atakowana z lądu.

Stwierdzenie Mao Zedonga, iż aby obalić jakąś władzę polityczną, należy zacząć od przygotowania opinii publicznej i od pracy ideologicznej, zarówno w przypadku klasy rewolucyjnej, jak i klasy nierewolucyjnej (4, s. 110),

odzwierciedla trafnie zastosowanie wojny informacyjnej w konfliktach międzynarodowych, gdzie polem walki są przede wszystkim umysł i mentalność człowieka, jako nie posiadające w dobie społeczeństwa informacyjnego, naturalnej bariery przed manipulacją, dezinformacją czy konsekwentną i zmasowaną propagandą. Wojnę informacyjną należy definiować z punktu widzenia mocarstw konkurujących o zdobycie lub utrzymanie przewagi w polityce globalnej bądź regionalnej (38).

Prawdziwa informacja obecnie nie ma już znaczenia. Człowiek, który był demoralizowany przez długi czas, nie jest w stanie ocenić wiarygodności informacji. Fakty nie przemawiają do niego. „Nawet gdyby takiej osobie dać informację rzetelną, zgodną z rzeczywistością, z dowodami dokumentalnymi, ze zdjęciami, nawet jeśli pokazać jej prawdziwy obóz koncentracyjny – on nie uwierzy, dopóki nie otrzyma „ciosu w tyłek rosyjskim wojskowym butem". Tylko wtedy zrozumie. Ale nie wcześniej i to jest tragedią – podkreślał Jurij Bezmienow w wywiadzie dla amerykańskiego czasopisma (14). Jurij Bezmienow (ros. *Юрий Александрович Безменов*, znany też pod nazwiskiem Tomas David Schuman oraz Jurij Makiejew, ros. Юрий Александрович Макеев) urodził się w 1939 r. w Mytiszczi, koło Moskwy, w rodzinie wysoko postawionego oficera sowieckiego, członka sztabu generalnego ZSRR, inspektora oddziałów w krajach satelickich. Zmarł 7 stycznia 1993 r. w Windsor, Kanada). Był radzieckim tajnym współpracownikiem działającym pod przykryciem dziennikarza na zlecenie Pierwszego Zarządu Głównego Komitetu Bezpieczeństwa Państwowego, w 1970 zbiegł do Kanady z Indii, gdzie pracował jako oficer prasowy ambasady sowieckiej w New Delhi. Był członkiem elitarnego zespołu, głównego oręża propagandy KGB znanego pod nazwą Agencja Prasowa Nowosti. Od 1967 roku z polecenia KGB pracował dla „Russia Today". Należał do grona światowej klasy wybitnych ekspertów w dziedzinie technik dezinformacyjnych, sowieckiej propagandy, dezinformacji, dywersji ideologicznej i tak zwanej strategii małych kroków. Przekazywał USA wiele cennych informacji na temat działalności Związku Radzieckiego, a następnie Rosji w zakresie dezinformacji, przewrotu ideologicznego oraz technik wykorzystywanych do przejęcia kontroli nad kolejnym państwem.

Informacja jest dziś prawdziwą potęgą w rękach władzy. To dlatego rządy państw totalitarnych starają się kontrolować media w celu wpływu na świadomość i działalność ludzi. Te zjawiska we współczesnym świecie nazywają się nowym typem propagandy, która wykorzystuje przede wszystkim wpływ psychologiczny. Kampania medialna Moskwy w wojnie przeciwko Ukrainie była zaskakująco skuteczna – nie tylko dla samej Rosji, ale także i dla zachodniej opinii publicznej. Ten sukces propagandowy był efektem długotrwałych wysiłków, które obejmowały znaczne inwestycje i umiejętne korzystanie z telewizji i mediów społecznościowych. Nie zauważalnie dla innych Rosja stworzyła wysoko rozwinięty

arsenał wojny informacyjnej, z którym nie tylko Ukraina, ale NATO i UE nie były w stanie w początkowym okresie wojny hybrydowej konkurować.

J. Bērziņš z Akademii Obrony Narodowej Łotwy w swojej pracy „Wojna nowej generacji w Ukrainie: implikacje dla polityki obronnej Łotwy" podaje osiem kluczowych działań świadczących o stanie wojny hybrydowej, wśród których ważne miejsce zajmuje zarządzanie oddziałami wojskowymi w sferze informacji i informowania (1).

Zazwyczaj skuteczną metodą wojny informacyjnej jest uwolnienie dezinformacji lub podanie informacji w korzystny sposób dla agresora. Metody te pozwalają na zniekształcenie oceny tego, co się dzieje, demoralizację obywateli i potencjalnie zapewniają przejście na stronę agresora informacyjnego. Opierając się na dotychczasowych osiągnięciach ukraińskich i rosyjskich naukowców (45; 22; 42; 43; 46; 47; 51, s.15-21; 56; 48) można wydzielić kilka rodzajów dezinformacji:

1. Oszustwo konkretnej grupy osób przez przekazanie świadomie wadliwej informacji (nieaktualnej, niekompletnej, zniekształconej, błędnie zinterpretowanej) jako podstawy do podjęcia odpowiedniej decyzji. W zależności od ilości wiarygodnych informacji wykorzystywanych przy przygotowywaniu wsparcia informacyjnego, wydziela się tzw. „szarą" (synteza polega na wykorzystaniu prawdziwej i fałszywej informacji) i „czarną" (zdominowane przez fałszywą informację) dezinformację (41, s. 73);
2. Modyfikacja przepływu informacji. Polega ona na selektywnym dostarczaniu informacji (niekompletna, półprawdziwa, dozowana, pominięcie niektórych informacji) lub tendencyjna i stronnicza prezentacja na temat wydarzeń z wykorzystaniem wybranych prawdziwych danych. Zwykle specjalnie spreparowaną informację przekazuje się obiektowi w wyznaczonych dawkach w celu utrzymania stale rosnącego napięcia. Przewiduje się systematyczne „podrzucanie" nowych porcji odpowiednio ograniczonych i odmierzonych danych w środowisko deficytu informacyjnego;
3. „Biały szum" jest technologią otoczenia prawdziwej informacji jej fałszywymi wersjami, które również są potwierdzone pewnymi dowodami, faktami, świadkami. Te wersje zmieniają i deformują prawdziwą wersję, w związku z czym percepcja osoby atakowanej łączy się w jeden „biały szum", a podmiot szybko traci zainteresowanie taką informacją (55, s. 80);
4. Dezinformowanie „od odwrotnego" odbywa się przez zapewnienie prawdziwych wiadomości w zniekształconej formie lub w takiej sytuacji, gdy są one postrzegane jako fałszywe. W rezultacie wykorzystania takich środków pojawia się sytuacja, kiedy obiekt zna prawdziwą informacje o zamiarach lub konkretnych działaniach innej strony, ale spostrzega je nieadekwatnie i nie jest odpowiednio przygotowany, aby oprzeć się negatywnemu wpływowi przekazywanych treści (41, s. 73);

5. Terminologiczne „podkładanie min”, które polega na zniekształceniu początkowej prawdziwej istoty ważnych pojęć, terminów i interpretacji ogólno-światopoglądowego i operacyjno-stosowanego charakteru.

Niektórzy badacze (50, s. 15-21) zaliczają do gatunków dezinformacji również manipulowanie działaniami osoby (grupy osób), mające na celu zmianę kierunki jej działalności lub poziomu aktywności w tej działalności.

Rosyjska kampania propagandowa przeciwko Ukrainie

XXI wiek nie tylko ułatwił dostęp do informacji, ale także ułatwił pracę rosyjskiej propagandzie państwowej. Wojna informacyjno-psychologiczna przyniosła ze sobą wojnę jakościowo nowego typu, w której bronią jest informacja, a walkę prowadzi się w celu zmiany świadomości społecznej. Wyzwaniem rosyjskich propagandystów było wprowadzenie do świadomości społecznej takich wyobrażeń o wydarzeniach, które pozwoliłyby w przyszłości manipulować całym społeczeństwem danego państwa, a także rządzącą elitą.

Współczesne elementy rosyjskiej propagandy:

- emocjonalizacja: niektóre narody są bardziej sentymentalne albo emocjonalne, niektóre mają problemy z przeszłością, co wykorzystuje się w propagandzie,
- demonizacja wroga,
- wojna, która zakończy wszystkie wojny,
- nieuczciwość, która jest zawsze obecna w propagandzie w czasie wojny.

Obecna praktyka rosyjskiej wojny informacyjnej łączy w sobie szereg sprawdzonych narzędzi, wpływów z nowoczesną technologią i możliwościami. Niektóre narzędzia są rozpoznawalne jako elementy kampanii wywrotowej z czasów zimnej wojny. Ale uznanie tego faktu przez zachodnie społeczeństwa, rządy państw demokratycznych jest powolne. Wynika to z dwóch głównych czynników. Po pierwsze, nie ma zbiorowej pamięci instytucjonalnej wśród odbiorców – znaczna część społeczeństw zachodnich jest młoda i nie pamięta problemów związanych ze Związkiem Radzieckim. Po drugie, Rosja zainwestowała znaczące środki w rozwój propagandy i manipulacji internetowej. Te nowe inwestycje rosyjskie obejmowały trzy główne obszary:

- wewnętrzne i zewnętrzne media odgrywające istotne znaczenie w działalności *online*, z których „*Russia Today*” jest najbardziej znanym;
- wykorzystanie mediów społecznościowych i forów internetowych jako siły dla zapewnienia rosyjskiej narracji i osiągnięcia szerokiego zasięgu i penetracji;
- wykorzystanie różnorodnych języków w celu zaangażowania odbiorców z różnych państw świata (2, s. 1).

W przypadku kampanii informacyjnej Rosji, to ona wykorzystuje wszystkie możliwe techniki i chwyty w Internecie. Z jednej strony uczestniczą w niej osoby działające na zlecenie, otrzymujące wynagrodzenia za wykonaną pracę, co

w przypadku zorganizowanego trollingu polega na zamieszczaniu wiadomości i komentarzy, pokazywaniu pewnych ludzi i zdarzeń z punktu widzenia Kremla, rozpowszechnianiu wybranych, zmodyfikowanych faktów w odpowiednim kontekście. Wykorzystywani są również tak zwani „pożyteczni idioci", którzy regularnie i nieświadomie komentują wydarzenia, rozmnażają dezinformację na różnych profilach, w serwisach społecznościowym i/lub osobistych blogach, w których publikują teksty „pożądane" z punktu widzenia prorosyjskiej perspektywy. Jest niezwykle trudno odróżnić te dwie kategorie komentujących, ponieważ wykorzystują oni dokładnie te same techniki komunikacji i odnoszą się do tych samych źródeł.

Analiza rosyjsko-ukraińskiego konfliktu w mediach społecznościowych ujawniła, że Kreml wykorzystuje również wszystkie możliwe techniki wpływania na opinię publiczną. Trolle (zarówno rosyjskie i ukraińskie) nieustannie starają się wpływać na odbiorców poprzez zamieszczanie różnego rodzaju informacji, jak również przez manipulowanie, naznaczanie, wprowadzanie w błąd, poniżanie, promowanie oszustwa, odstraszanie i mobilizowanie swoich współpracowników. Oprócz powyższych technik istnieje jeszcze kilka ważnych strategii komunikacyjnych, które zwiększają skuteczność rosyjskich trolli. Są to zaprzeczenie, budowanie chaosu informacji (w tym dezinformacji i plotek), zaostrzenie konfliktu wewnętrznego (poprzez podkreślenie niekompetencji, korupcji i sporów politycznych władz), groźby i zniechęcania, budowanie wizerunku wroga (Ukraińców, Amerykanów, Turków), podżeganie narodowej, etnicznej i religijnej nienawiści, niezgoda i budowanie teorii spiskowych (9, p. 64). Najczęściej trolle zaprzeczają oczywistym faktom, wydarzeniom i opiniom innych, niezgodnym z ich myślą.

Chociaż powyższe techniki i strategie komunikacyjne były stosowane w sposób ciągły, trudno jest określić, w jakim stopniu na przebieg dyskusji w rzeczywistości mają wpływ przekonania, wartości i postawy czytelników. Nie ma wątpliwości, że działania komentujących są organizowane, a nie są przypadkowe. Są zlecane i kontrolowane z Kremla, a to oznacza, że mamy obecnie do czynienia z wojną w Internecie (9, s. 69). Jednak trudno jest stwierdzić jednoznacznie stopień oddziaływania społeczno-medialnego i jego skuteczność.

Wojna, jaką toczy Rosja w Ukrainie pełna jest przykładów cyberataków na media społeczne służące do wzbudzania paniki. Dla przykładu, 4 czerwca 2014 na Instagramie Pawła Astakhova, Rzecznika Praw Dziecka przy Prezydencie Federacji Rosyjskiej była zamieszczona informacja o tym, że w ciągu jednej doby do obwodu rostowskiego przybyło ponad 7000 ukraińskich uchodźców. 5 czerwca media pisały już o 8386 nowych uchodźcach z Ukrainy. Tegoż 5 czerwca 2014 roku na oficjalnym portalu obwodu rostowskiego została zamieszczona informacja o 437 osobach z Ukrainy. Tymczasem tylko 7 osób zwróciło się o przyznanie statusu uchodźca, a 5 osób o nadanie tymczasowego azylu (21).

Zachodnie organizacje medialne były całkowicie nieprzygotowane do ukierunkowanej i spójnej wrogiej kampanii informacyjnej zorganizowanej na szczeblu państwowym. Wynik był zaskakujący: początkowy sukces Rosji na Krymie (23, s. 8), kiedy wszędzie: w stosunku do obywateli, dziennikarzy i rządów innych państw, zaobserwować można było niewytłumaczalne zaprzeczenie obecności rosyjskiej na Ukrainie, zmienił się na rozumienie tego, że Kreml i jego dziennikarze dezinformują cały świat. Pozytywną zmianą było odnotowanie, że rosyjskie kampanie informacyjne zawodzą, są niezdarne, nieproduktywne i można je łatwo obalić. Niestety towarzyszyło temu znaczne ryzyko błędnej interpretacji ich celów w wyniku mirroringu. Jednakże niektóre rosyjskie cele kampanii informacyjnej osiągnęły sukces. Można to zaobserwować w przypadku dwóch kluczowych obszarów: kontrolowania rosyjskiego środowiska medialnego i podważania obiektywizmu zachodnich mediów.

Rosji udało się „zabezpieczyć jej przestrzeń informacyjną" i „zapobiedz naruszeniom" w niej. Innymi słowy, społeczeństwo zostało skutecznie odizolowane od innych źródeł informacji, niż te, które podawał Kreml. Taka izolacja nie jest całkowita i hermetyczna – wciąż jest możliwe, że Rosjanie mogą uzyskać dostęp do zagranicznych mediów, jeśli chcą albo mogą. Jednak ostatnie wydarzenia w Rosji powiązane ze ściślejszą kontrolą nad korzystaniem z Internetu w kraju, w połączeniu z wycofaniem licencji, znacznie utrudniają ten proces. Innymi słowy, mieszkańcom Rosji coraz trudniej jest znaleźć alternatywne źródła wiadomości. Konsekwencją takiego stanu rzeczy stała się szeroka akceptacja alternatywnej rzeczywistości propagowanej przez rosyjskie media państwowe.

Wyjątkiem potwierdzającym regułę jest Internet, w tym media społecznościowe. Jak już wielokrotnie zostało powiedziane, informacje na temat aneksji Krymu i operacji we wschodniej części Ukrainy były pobieranez Internetu, co znacznie osłabia lub zaprzecza oficjalnej linii Kremla i stwarza największe wyzwanie dla rosyjskich kampanii informacyjnych. Rezultatem takiej działalności mediów społecznościowych stała się próba ich kontrolowania przez rosyjskie służby specjalne.

Rosja próbowała również przedstawić swoją alternatywną rzeczywistość za granicami państwa. Ale liberalne media zachodnie nie uwierzyły wiadomościom pochodzącym z Rosji. Świat zachodni przedstawił prawdziwą spójną wersję wydarzeń w Ukrainie a potem i w Syrii. Tutaj swoją własną, odrębną rolę odegrały Internet i media społecznościowe. Armia trolli Kremla oddziaływująca bezpośrednio na wielu forach internetowych, dyskusyjnych, w tym na Twitterze, działała jako siła, która miała za zadanie dostarczyć potrzebne stronie rosyjskiej komunikaty – szczególnie poprzez inicjowanie lub tłumienie debaty wydarzeń niespójnych z wersją Moskwy.

Podczas gdy prawda jest podstawowym wymogiem zachodnich strategii komunikacyjnych, rosyjskie mass media nie muszą nawet zastanawiać się nad

przedstawieniem prawdziwych wydarzeń, by odnieść sukces. W Rosji praktycznie nie istnieją niezależne media. Zostały one skutecznie usunięte z rynku. Za granicą rosyjska alternatywa rzeczywistości nie musi być wiarygodna w celu zapewnienia alternatywy dla prawdy, ponieważ zadaniem armii trolli Kremla jest penetracja wśród grupy docelowej, niezależnie od wiarygodności komunikatów przez nich preparowanych. Wystarczy, powodując zamieszanie i wątpliwości, podważyć zaufanie do obiektywnych wiadomości, a zwłaszcza do oficjalnych wypowiedzi przeciwników Rosji. Kluczowym przykładem takiego podejścia było zestrzelenie Malaysia Airlines Flight MH17. Cztery dni po katastrofie rosyjskie Ministerstwo Obrony Narodowej przeprowadziło konferencję prasową, na której wyjaśniono przyczyny tej tragedii. Prezentowane scenariusze były różnorodne i wzajemnie sprzeczne.

Rosyjska dezinformacja działa w taki sposób, aby osiągnąć swoje cele, siejąc zamieszanie i wątpliwości za granicą i ukrywając prawdę. Nieoczekiwane zaprzeczenia prawdy są formą manipulacji, na którą zachodnie media są szczególnie źle przygotowane. Tak więc, gdy Władimir Putin zaprzeczał, że wojska rosyjskie są na Krymie i we wschodniej Ukrainie, to nie było ważne, co mówi, ale że było skuteczne nie tylko podczas konferencji prasowych, ale również wśród elity politycznej. Jednocześnie sprawia to, że zachodni politycy uświadamiają sobie, że nie można liczyć ani na konfrontację, ani na współpracę z prezydentem Putinem. Świat rozumie, że rosyjskie kampanie dezinformacyjne są samobójcze, ponieważ prowadzą swoich twórców do „pułapki" – ograniczającej ich możliwości poprzez zmuszanie ich do subskrypcji własnych narracji i działania w zgodzie z własną propagandą.

W Rosji nie ma takich dylematów, ponieważ obraz świata dostarczany przez rosyjskie media jest całkowicie pod kontrolą Kremla i można go regulować tak długo, aby uzasadnić wszelkie działania lidera. Niebezpieczeństwo pojawia się wtedy, gdy proces opiniotwórczy Rosji na Zachodzie zaczyna wpływać na sam proces tworzenia polityki. Rosyjskie kampanie informacyjne przygotowują grunt dla przyszłych działań Kremla, które bezpośrednio sprzeczne są z interesami Europy i Zachodu. Rosja dopasowuje kluczowe zmienne dotyczące bezpieczeństwa, określa ryzyko związane z przyszłymi działaniami asertywnymi wobec swoich sąsiadów. Mało prawdopodobne jest, że Ukraina i Gruzja są ostatnimi ofiarami polityki imperialnej Rosji. Obecne rosyjskie ambicje prowadzą do bardziej bezpośredniej konfrontacji z Zachodem. Rosja wykorzystuje wszystkie elementy wojny informacyjnej w stosunku do swoich sąsiadów i do Europy, co w przyszłości będzie kluczowym czynnikiem dalszych działań (2, p. 5).

Międzynarodowy zespół wolontariuszy dziennikarzy, politologów, ekspertów wojskowych, osób publicznych i tłumaczy InformNapalm, których celem jest informowanie społeczności międzynarodowej o rozwoju wydarzeń w Ukrainie, w 2016 roku przedstawił interesujący materiał analityczny eksperta

bezpieczeństwa informacyjnego Wiaczesława Husarowa pt. „Sprzeciw Informacyjny". Autor przeanalizował, ile Federacja Rosyjska corocznie wydaje na wojnę informacyjną przeciwko Ukrainie i ustalił, że „FR co rok wydaje na kampanię informacyjną nie mniej niż $ 3,5 mld, a rosyjska maszyna informacyjna działa w tak pełnym trybie przez ostatnie trzy lata". Autor podkreśla, że wojna, wywołana przez Rosję przeciwko Ukrainie, tylko częściowo była prowadzona za pomocą tradycyjnej broni – karabinów, czołgów i armat. Za kurtyną walk pozostaje czynnik informacyjny rosyjskiej agresji: wojskowe systemy radio-wywiadu (podsłuch radiowy) i zakłócania radiowego, typografia służąca drukowaniu ulotek i sprzęt symulujący pracę mobilnych nadajników, które rozsyłały na telefony ukraińskich żołnierzy SMS-y o prowokacyjnej treści etc. (16). Oprócz tego Rosja w 2014 roku według kongresmena Senatu USA Dana Mike wydała na kampanię propagandową przeciwko Ukrainie ponad 9 mld USD (33).

Zestaw instrumentów wpływu informacyjnego Rosji jest szeroki. Należą do niego:

- środki walki radio-elektronicznej,
- środki wywiadu radiowego,
- system bezpilotowy,
- środki walki psychologicznej, w tym produkcja ulotek i gazet,
- wsparcie prorosyjskich ruchów ideologicznych w okupowanym Donbasie („Wolny Donbas", „Doniecka Republika", „Opłot", „Pokój Ługańszczyźnie", „Noworosja", „Południowy Wschód", „Ługański Sojusz Ekonomiczny" i inne)
- wsparcie regionalnych prorosyjskich mediów**:**
  a) Telewizja („Ługańsk-24", „Noworosja TV", „1 Kanał Republikański", „Opłot TV", „Junion DNR", „AR-TV") – rocznie ok. 180 mln rubli;
  b) internetowe kanały online „Pierwszy Republikański – DNR TV", „Informbiuro", „Patriotyczne Siły Donbasu", „News-Front" i inne – rocznie ok. 5 mln rubli,
  c) FM-radio („Radio Noworosji", „Radio DNR") – rocznie ok. 5 mln rubli;
  d) retransmisja pakietu federalnych kanałów telewizyjnych i radiowych – rocznie 2 mln rubli,
  e) prasa drukowana („XXI wiek", „Gazeta Municypalna", „Głos Ludu" i inne) – rocznie ok. 1 mln rubli;
  f) wsparcie mediów elektronicznych (lugansk-online.info, novorosinform.org, komitet.net.ua, dnr.today, rusvesna.su i inne) – rocznie ok. 1 mln rubli.

Coroczne wydatki z budżetu Federacji Rosyjskiej na działalność informacyjną z propagandy separatyzmu w okupowanym Donbasie wynosi około 274 mln rubli na rok ($ 5,5 mln). Przy tym wartość sprzętu bojowego przetransportowanego na terytorium Ukrainy przez Rosję wynosi 1,4 mld rubli ($25 mln) (16).

W 2015 roku Rosja zajęła pierwsze miejsce na świecie w rządowych wydatkach na propagandę. Rządowe wsparcie prorządowych mediów w Rosji wyniosło 48,65 mld rubli (1,6 mld dolarów) (26).

Zachodni eksperci uważają, że Rosja w ostatnich latach znacznie rozszerzyła swoje kampanie propagandowe przeciwko Zachodowi, w tym przeciwko Niemcom. Stanowią one próbę Kremla manipulowania opinią publiczną na Zachodzie, tworzenie konfliktów wewnątrz państw i destabilizacji społeczeństw zachodnich. Do prowadzenia polityki zagranicznej Kreml wykorzystuje „stare metody" KGB: dezinformację i destabilizację. Metody te widoczne są w Ukrainie i w państwach zachodnich. Rosja przez swoje kanały telewizyjne oraz trolle masowo szerzy propagandę. Rosyjska propaganda pada na podatny grunt na Zachodzie, gdzie brak zaufania do polityków i mediów jest powszechne, co wzbudza niechęć wobec uchodźców i migrantów oraz podważa zaufanie do instytucji demokratycznych i mediów. To wszystko jest częścią strategii dyskredytacji i osłabienia Zachodu. Rosja uważa to za konieczne w celu ochrony swoich interesów. Od czasu upadku Związku Radzieckiego Kreml był w defensywie. W oczach Moskwy, Zachód zyskał przewagę w 1990 roku zarówno militarnie przez rozszerzenie NATO na Wschodzie, jak i pod względem propagandowym, przedstawiając zachodnią demokrację jako jedyną atrakcyjną formę rządu. Aby przeciwdziałać prymatowi Zachodu, Moskwa wykorzystuje taktyki partyzanckie, próbując podważyć zachodnie wartości. Obejmuje to: cyberataki, „małe zielone ludziki", uzbrojonych mężczyzn w nieoznakowanych mundurach wojskowych (8, s.79-92). Zamiast broni walka odbywa się za pomocą słów, a Internet stał się najważniejszym polem bitwy (10).

Bieżący informacyjny, agresywny atak rosyjskich mediów jest skierowany nie tylko na swoich obywateli, ale na zapobieganie negatywnej ocenie ze strony społeczności międzynarodowej. Skuteczności maszyny propagandowej Putina w interpretacji wydarzeń, mógłby pozazdrościć każdy propagandysta, szczególnie w zakresie zniekształcania faktów, jednostronnej i tendencyjnie przedstawionej informacji, tworzenia i wykorzystania wizerunku „wroga Rosji" na początku agresji FR Ukraińców, a od października 2015 roku – Turków.

Niezaprzeczalne osiągnięcie Putina – to uczynienie z Rosji agresora w erze informacyjnej. Zbrodnie wszystkich agresorów przeszłości trzeba badać poprzez dokumenty. Agresję reżimu Putina można obserwować w czasie rzeczywistym. To wyjątkowy „sukces", który nie ma sobie równych.

Podsumowując, wojna informacyjna jest prowadzona cały czas, tylko na to zjawisko nikt nie zwracał uwagi, dopóki w Ukrainie nie zaczęły się rosyjskie działania wojenne. Głównym celem rosyjskiej wojny psychologicznej jest świadomość zwykłych obywateli Ukrainy. Donbas, Krym są owocami właśnie wojny informacyjno-psychologicznej. Jeżeli dziś niezwłocznie nie będą podejmowane niezbędne działania, skierowane na masową edukację ludności,

„dojrzeją" następne owoce tej wojny: społeczeństwo depresyjne, niewolnicza świadomość, kompletny brak zrozumienia procesów zachodzących na poziomie państwowym, apatia, agresja, brak zaufania do wszystkich i do wszystkiego. Dziś główny ciężar polityki informacyjnej Rosji jest skierowany na manipulowanie świadomością Ukraińców i destabilizację wewnątrz państwa. W związku z czym przed Ukrainą stoi ważne zadanie: jak najszybciej zmienić koncepcję bezpieczeństwa informacyjnego. Opóźnienie w przygotowaniu do informacyjno-psychologicznej wojny stanowi poważną lukę w obronie Ukrainy.

Tymczasem w niektórych państwach europejskich szerzy się przekonanie, że trzeba współpracować a nie izolować Rosję. Ale niestety, jakakolwiek próba włączenia jej w proces demokratyczny jest polityczną iluzją. Markiz Astolphe-Louis-Léonor de Custine jeszcze w 1839 roku słusznie zauważył: *Ten naród (rosyjski), pozbawiony przyjemności i własnej woli – nie co innego jak tłum ciał bez duszy. Niemożliwe bez niepokoju myśleć o tym, że na tak ogromną liczbę rąk i nóg jest tylko jedna jedyna głowa. Despotyzm jest mieszanką niecierpliwości i lenistwa* […] *Tyrania jest urojoną chorobą ludzi. Tyran przebrany lekarzem mówi im, że cywilizowany człowiek nigdy nie jest zdrowy i że czym większe zagrażające jemu niebezpieczeństwo, tym bardziej zdecydowanie należy go leczyć: tak pod pretekstem walki ze złem tyran tylko zaostrza ją* (17, s.118). W związku z powyższym należy postawić pytanie nie tylko o współistnienie Ukrainy i Rosji, ale również o współistnienie świata i Rosji. Z cywilizowanego punktu widzenia taka koegzystencja musi być pokojowa. Tymczasem Ukraina samotnie walczy z rosyjskim imperializmem w czystej postaci i jest to walka różnych ideologii i światopoglądów.

Bibliografia

1. Bērziņš, J., *Russia's new generation warfare in Ukraine: implications for Latvian defense policy*. National Defense Academy of Latvia Center for Security and Strategic Research. Dostęp: 10.03.2016. Tryb dostępu: http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.
2. Giles, K. (2015) *Russia's Hybrid Warfare: A Success in Propaganda*. "Arbeitspapier Sicherheitspolitik", nr 1.
3. Lange-Ionatamishvili, E., Svetoka, S. (2015) *Strategic Communications and Social Media in the Russia Ukraine Conflict.* W: Geers, K. (Ed.), *NATO Strategic Communications Centre of Excellence. Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications.

4. Loubier, A. (2006) *Grupy redukcyjne, techniki sterowania i manipulacji wewnątrz stowarzyszeń*. Komorów: Wydawnictwo Antyk Marcin Dybowski.
5. Taylor, P. M., *Global Communications, International Affairs and the Media Since 1945.* Dostęp: 10.03.2016. Tryb dostępu: https://networks.h-net.org/node/9997/reviews/10434/killen-taylor-global-communications-international-affairs-and-media.
6. Taylor, P. M. (1997) *Global Communications, International Affairs and the Media Since 1945 (The New International History).* New York and London: Routledge.
7. *Prezydent: W czasie wojny, którą rozpętała Rosja, zginęło 10 tysięcy Ukraińców.* Dostęp: 07.12.2016. Tryb dostępu: http://zik.ua/pl/news/2016/12/06/prezydent_w_czasie_wojny_ktr_rozptaa_rosja_zgino_10_tysicy_ukraicw_1004123.
8. Srogosz, T. (2015) *Status prawny nieoznakowanych żołnierzy w wojnie hybrydowej.* „Sprawy Międzynarodowe", nr 4.
9. Szwed, R. (2016) *Framing of the Ukraine–Russia conflict in online and social media.* Riga: NATO StratCom COE.
10. *The Hybrid War: Russia's Propaganda Campaign Against Germany.* Dostęp: 21.02.2016. Tryb dostępu: http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html.
11. Żuk-Łapińska, L. (1991) *Problem tolerancji*. Warszawa: Wydawnictwo Uniwersytetu Warszawskiego.
12. Анчуков, С. В., Суслов, А. И. *Война и военная стратегия: реквием современности (постмодернистский взгляд и посильные размышления о будущем).* Dostęp: 11.01.2016. Tryb dostępu: http://www.whiteworld.ru/rubriki/000101/001/02073004.htm.
13. Гавриш, С. *Русская православная церковь не содействует примирению и участвует в информационной войне против Украины.* Dostęp: 23.02.2016. Tryb dostępu: http://ukrreal.info/ua/intervyu/91202-stepan-gavrish-russkaya-pravoslavnaya-tserkov-ne-sodeystvuet-preniyu-i-uchastvuet-v-informatsionnoy-voyne-protiv-ukrainy.

14. Гриффин, Э. (1984) *Фрагменты интервью с Юрием Безменовым.* Dostęp: 19.10.2016. Tryb dostępu: http://aillarionov.livejournal.com/891034.html.

15. Громыко, Ю. *Оружие, поражающие сознание, – что это такое*? Dostęp: 13.02.2016. Tryb dostępu: http://www.pereplet.ru/text/grom0.html.

16. Гусаров, В. *Русские пришли-2. Сколько стоит российская информационная война?* Dostęp: 17.06.2016. Tryb dostępu: http://sprotyv.info/ru/news/kiev/russkie-prishli-2-skolko-stoit-rossiyskaya-informacionnaya-voyna.

17. де Кюстин, А. (2008) *Россия в 1839 году*. Пер. с фр. О. Гринберг, С. Зенкина, В. Мильчиной, И. Стаф. Издательство Крига, Санкт-Петербург.

18. Жук, Н. *Концепция общественной безопасности Мёртвая вода*. Dostęp: dostęp 23.02.2016. Tryb dostępu: https://www.proza.ru/2010/05/12/564.

19. З *початку АТО загинули 2673 військових, з них 831 – не в боях.* Dostęp: 13.03.2016. Tryb dostępu: http://www.pravda.com.ua/news/2015/11/20/7089604/ .

20. *За час АТО в Донбасі загинули дев'ять тисяч осіб – МЗС.* Dostęp: 13.03.2016. Tryb dostępu: https://ukr.media/ukrain/255821/.

21. *Информацию о тысячах украинских беженцев опровергли ростовские чиновники.* Dostęp: 16.05.2016. Tryb dostępu: http://www.stopfake.org/informatsiyu-o-tysyachah-ukrainskih-bezhentsev-oprovergli-rostovskie-chinovniki/.

22. Петрик, В. М., Остроухов, В.,В., Присяжнюк та, М.,М. (ред.) (2010) *Інформаційна безпека (соціально-правові аспек*ти): підруч., Київ: Видавництво КНТ.

23. Баровської, А. (ред.) (2016) *Інформаційні виклики гібридної війни: контент, канали, механізми протидії*. Київ: Видавництво НІСД.

24. Калашников, М., Крупнов, Ю. (2003) *Гнев орка: (Америка против России*). Москва: Издательство Астрель.

25. Кемаль, А. (2015) *Кибервойна. Как Россия манипулирует миром*. Москва: Издательство Litres.

26. Колотій, Н., *Ляльководи свідомості.* Dostęp: 21.10.2016. Tryb dostępu: http://gazeta.dt.ua/technologies/lyalkovodi-svidomosti-_.html.

27. Крупнов, Ю. В. (red.) (1997) *Кому будет принадлежать консиентальное оружие в XXI веке*? (1997). Москва: Издательство Россия.

28. *Консиентальные войны: реальность и фантастика.* Dostęp: 13.02.2016. Tryb dostępu: http://ot-a-do-ya.org/Articles/Global/Cons_war.aspx#.Vt_0z16soUM.

29. Крупнов, Ю. В. (2004) *Россия между Западом и Востоком. Курс Норд-Ост.* Москва; ОЛМА Медиа Групп.

30. Лисичкин, В., Шелепин, Л. (2000) *Третья мировая информационно-психологическая война.* Москва: Академия социальных наук.

31. Маначинский, А. (2006) *Асимметричные войны – одна из реалий современности*. „Независимое Военное Обозрение", nr 47;

32. Анчуков, С. В., *Тайны мятеж-войны – Россия на рубеже столетий.* Dostęp: 10.03.2016. Tryb dostępu: http://www.pseudology.org/Anchukov/Anchukov_TaynyMyatezhVoiny2.pdf.

33. *Міноборони: Для розмінування Донбасу потрібно не менше 10 років.* Dostęp: 23.02.2016. Tryb dostępu: http://www.pravda.com.ua/news/2016/02/29/7100593/.

34. *На антиукраинскую пропаганду Россия потратила более 9 миллиардов долларов.* Dostęp: 17.06.2016. Tryb dostępu: http://onpress.info/na-antiukrainskuyu-propagandu-rossiya-potratila-bolee-9-milliardov-dollarov-13036.

35. На *Донбасі від початку АТО загинули 2 тисячі 269 українських військових – Порошенко.* Dostęp: 13.03.2016. Tryb dostępu: http://www.unian.ua/war/1249761-na-donbasi-vid-pochatku-ato-zaginuli-2-tisyachi-269-ukrajinskih-viyskovih-poroshenko.html.

36. Овчинский, В., Ларина, Е. (2016) *Кибервойны XXI века. О чем умолчал Эдвард Сноуден*. Москва: Издательство Litres.

37. Панарин, И. Н. (2003) *Информационная война и выборы.* Москва: Издательский дом „Городец".

38. Панарин, И. Н. (2006) *Информационная война и геополитика*. Москва: Издательство Поколение.

39. Панарин, И. Н. (2012) *СМИ, пропаганда и информационные войны*. Москва: Издательство Поколение.

40. *Паралелі. Чи стане РПЦ другим ІГІЛ?* Dostęp: 23.02.2016. Tryb dostępu: http://www.ukrop-ua.net/publications/society/1275-paralel-chi-stane-rpc-drugim-gl.html.

41. Паршакова, Е. Д. (2012) *Информационные войны;* Краматорск: Донбасская государственная машиностроительная академия.

42. Петрик, В. М. (2009) *Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу. „*Сучасні інформаційні технології у сфері безпеки та оборони", nr 3.

43. Петрик, В. М. (2008) *Информационно-психологическая безопасность в эпоху глобализации*, под ред. В.В. Остроухова. Київ.

44. Петрик, В. М. (2007) *Соціально-правові основи інформаційної безпеки,* за ред. В.В.Остроухова. Київ: Видавництво Росава.

45. Потехин, В. К.,*Современные войны и национальная безопасность России*. В: *Кому будет принадлежать консиентальное оружие в XXI веке?* Издательство Россия 2010, Москва 1997.

46. Почепцов, Г. Г. (2015) *Информационные войны. Новый инструментарий политики*. Москва: Издательство Эксмо.

47. Почепцов, Г. Г. (2001) *Информация & дезинформация*. Київ: Видавництво Ника-Центр, Эльга.

48. Почепцов, Г.Г., *Психологические войны*. Издательство Рефл-бук, Москва 2000; Видавництво Ваклер, Київ 1999.

49. Присяжнюк, М.М., *Дезінформація та її роль у інформаційно-психологічних операціях*. Dostęp: 22.05.2016. Tryb dostępu: http://defpol.org.ua/site/index.php/en/arhiv/kolonkaavtora/106-2009-09-09-18-06-14.

50. *Русская православная церковь активно усиливает террористические группировки на Донбассе – З.Шкиряк.* Dostęp: 23.02.2016. Tryb dostępu: http://www.unn.com.ua/ru/news/1391643-rosiyska-pravoslavna-tserkva-aktivno-posilyuye-teroristichni-ugrupuvannya-na-donbasi-z-shkiryak.

51. Серов, А. (2011) *О роли дезинформации в современных конфликтах и войнах*. „Зарубежное военное обозрение", nr 7, Ч. 1.

52. Серов, А. (2011) *О роли дезинформации в современных конфликтах и войнах*. „Зарубежное военное обозрение”, nr 8. Ч. 2.

53. Сірук, М., *Чи здатна ООН зупинити війну в Україні?* Dostęp: 10.11.2016. Tryb dostępu: https://day.kyiv.ua/uk/article/den-planety/chy-zdatna-oon-zupynyty-viynu-v-ukrayin.

54. Слипченко, В. (2004) *Войны нового поколения: дистанционные бесконтактные*. Москва: ОЛМА-ПРЕСС Образование.

55. Усенко, В., *Многоуровневый характер гибридной войны.* Dostęp: 23.02.2016. Tryb dostępu: http://sprotyv.info/ru/news/13956-mnogourovnevyy-harakter-gibridnoy-voyny.

56. Шлапаченко, В. М. (2013) *Дезінформація як спосіб інформаційно-психологічного впливу*. *„Інформаційна безпека людини, суспільства, держави”*, Nr 2.

57. Юдін, О. К. (2005) *Інформаційна безпека держави*. Харків: Видавництво Консум.

Streszczenie

W artykule autorzy podjęli próbę analizy bezpieczeństwa państwa i jego przestrzeni informacyjnej. Z początkiem aneksji Krymu i konfliktu rosyjsko-ukraińskiego na wschodzie Ukrainy rośnie zainteresowanie problemami wojny informacyjnej, która jest głównym bezpośrednim zagrożeniem dla ludzkości. Autorzy zwracają uwagę na konieczność zrozumienia natury i technologii władzy informatycznej nad ludźmi, ponieważ brak kontroli może prowadzić nie tylko do masowej eksterminacji odrębnych narodów, ale także do zniszczenia współczesnej cywilizacji jako całości. Cyberprzestrzeń odgrywa coraz ważniejszą rolę w strategicznej komunikacji jako nasze uzależnienie od nowoczesnych technologii, sieci komputerowych i Internetu. Wraz ze wzrostem popularności platform społecznościowych, rozszerzają się koncepcje społecznych cyberataków.

Słowa kluczowe: wojna informacyjna, wojna hybrydowa, miatieżowojna (wojna-chaos), konscijentalna wojna (świadomościowa), cyberprzestrzeń, cyberataki, media społecznościowe

Informational warfare – threat to for safety of mankind

Abstract

The authors attempted to analyze the security of the state and its information space. At the beginning of the annexation of Crimea and Russian-Ukrainian conflict, in eastern Ukrainian regions is growing interest in the problems of informational war, which is the main and direct threat to humanity. The authors draw attention to the need of understanding the nature of technology and computing power over the people, because the lack of control can lead not only to mass extermination of separate nations, but also to the destruction of modern civilization as a whole. Cyberspace is playing an increasingly important role in strategic communication as our dependence on modern technology, computer networks and Internet. With the increasing popularity of social networking platforms, we have also experienced extending of social cyber-attacks.

Keywords: Information warfare, hybrid warfare, war-chaos, awareness war, cyberspace, cyber-attacks, social media

Andrzej Żebrowski
Uniwersytet Pedagogiczny w Krakowie

Determinanty walki informacyjnej

Wprowadzenie

Walka informacyjna jest obecna w naszym codziennym życiu. Jest uprawiana przez wszystkie podmioty, bez względu na ich usytuowanie w otoczeniu wewnętrznym i zewnętrznym państwa. Pozwala na podejmowanie decyzji, którą każdy uczestnik kooperacji negatywnej będzie zakłócał. Właściwości walki informacyjnej (np. niejawny charakter, brak możliwości wykrycia strony ofensywnej) i towarzyszące jej rozwój teleinformatyki usytuowanej w globalnej przestrzeni informacyjnej, czyni z niej szczególnie niebezpieczny oręż. W materiale przedstawione zostały cechy walki informacyjnej i jej wpływ na możliwości strony ofensywnej.

Zjawisko walki informacyjnej

Walka informacyjna jest prowadzona przez wszystkie podmioty, tak państwowe, jaki pozapaństwowe. Trudno jest wskazać jej początek, a tym bardziej koniec. *Historia walki informacyjnej jest tak samo długa, jak historia ludzkich dziejów. Nikt jej jednak nie spisał. Co więcej – nigdy nawet nie używano takiego pojęcia. Nie oznacza to jednak, że kojarzone z nią dziś funkcje zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej zaistniały dopiero u schyłku XX wieku. Istniały zawsze. Teraz unaoczniają się tylko z niewspółmiernie większą wyrazistością. Postępująca politechnizacja życia i szybki rozwój szeroko rozumianej komunikacji spowodowały, że samo słowo informacja stało się dziś pojęciem powszechnie używanym. Zawsze jednak walczące ze sobą strony rozpoznawały się wzajemnie. Zawsze starały się wzajemnie oszukiwać i wprowadzać w błąd. Zawsze też posiadały sekrety, które z wielką skrupulatnością ukrywały przed wrogiem* (Szpyra 2003, s. 91-92).

W początkowym okresie walka informacyjna przebiegała jedynie w osobowej przestrzeni informacyjnej, gdzie podstawowym źródłem informacji był człowiek, a także zjawiska zachodzące w jego bliższym i dalszym otoczeniu. W tym czasie tylko bezpośrednia obserwacja i uczestnictwo w prowadzonych rozmowach, czy dostęp do przekazów pisemnych pozwalało na poznanie przeciwnika i wypracowania decyzji, które przekładały się na praktyczne działania. Dokonujące się przemiany cywilizacyjne, którym towarzyszy intensywny rozwój nauki i techniki, sprawiają, że walka informacyjna prowadzona jest również w technicznej przestrzeni informacyjnej. Istnienie globalnej sieci informacyjnej pozwala na zwiększanie możliwości w zakresie oddziaływania informacyjnego na ściśle określony obiekt (obiekty). Tzw. usieciowienie, powszechny dostęp

i zależność od teleinformatyki to większe możliwości strony ofensywnej w zakresie ataku informacyjnego i zakłócania informacyjnego. Ponadto coraz trudniejsze, a nawet niemożliwe wskazanie strony (stron) atakującej.

Aktualnie zjawisko walki informacyjnej można rozpatrywać z perspektywy cybernetyki, co wynika z następujących przesłanek (Sienkiewicz, Świeboda 2009, s. 83-84):

1. sterowanie i informowanie na potencjalnym polu walki stanowi istotę działania systemów dowodzenia i systemów informacyjnych,
2. obiekty zaangażowane w procesy walki informacyjnej charakteryzowane są za pomocą określonych wejść i wyjść informacyjnych zarówno pozytywnych, jak i negatywnych (destrukcyjnych),
3. każdy rozpatrywany obiekt cechuje określony potencjał i efektywność, zaś ich zasoby mają wartość, ocenianą z różnych punktów widzenia (np. ich dysponenta i przeciwnika),
4. każdy obiekt (proces, system) rozpatrywany jest w określonym kontekście i relacjach z otoczeniem (zarówno w sensie pozytywnym, jak i negatywnym),
5. informowanie może mieć charakter:
   - transinformowania (informowania wiarygodnego),
   - pseudoinformowania (np. informowania pozornego),
   - dezinformowania (informowania fałszywego, zmierzającego do wprowadzania w błąd przeciwnika),
   - metainformowania (informowania o informowaniu).

Tabela 1. Przykładowe pojęcia walki informacyjne

Lp.	Źródło	Treść
1.	*AFDD 2-5 Information Operations* (1989), USAF.	Walka informacyjna to działania informacyjne prowadzone dla obrony własnej informacji i systemów informacyjnych lub dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika; jest toczona głównie w czasie kryzysu lub konfliktu; defensywny komponent tej walki, podobnie jak obrona powietrzna, realizuje się w każdej fazie działań militarnych, od pokoju do wojny.
2.	J. L. (1998) *Amerykańska koncepcja walki informacyjne*, „Wojskowy Przegląd Zagraniczny", nr 4, s. 16.	W walce informacyjnej, informacja jest zarówno bronią, jak i celem ataku. Oznacza najczęściej użycie informacji dla osiągnięcia ważnych celów państwowych i narodowych w wymiarze wojskowym, społecznym i gospodarczym.

3.	Ciborowski, L. (1999) *Walka informacyjna.* Toruń: Europejskie Centrum Edukacyjne, s. 187.	Walka informacyjna to kooperacja negatywna, wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej.
4.	J. L. (1999) *Rosyjska koncepcja walki informacyjnej.,* „Wojskowy Przegląd Zagraniczny", nr 1, s. 80.	Walka informacyjna to kompleks przedsięwzięć obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzenia działań bojowych.
5.	Szpyra, R. (2002) *Operacje informacyjne państwa w działaniach sił powietrznych.* Warszawa: AON, s. 149.	Walka informacyjna (w znaczeniu wojskowym) to zorganizowana w formie przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłania przez nie informacji przed podobnym działaniem przeciwnika.
6.	Denning, D. E. (2002) *Wojna informacyjna i bezpieczeństwo informacji.* Warszawa: Wydawnictwa Naukowo-Techniczne, s. 23.	Wojna informacyjna to działania, których celem jest zdobycie lub wykorzystanie zasobów informacyjnych.
7.	Gawliczek, P., Pawłowski, J. (2003) *Zagrożenia asymetryczne.* Warszawa: AON, s. 42.	Walka informacyjna to działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego z zamiarem promowania określonego celu politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników.

Źródło. opracowano na podstawie dostępnej literatury.

*

Mając na uwadze trwającą walkę informacyjną, która jest ściśle powiązana z cyberprzestrzenią, można wskazać następujące jej cechy:

1. przeciwnik (przeciwnicy) jest anonimowy, niewidzialny, tzn. funkcjonuje w strukturze wirtualnej, jest trudny do wskazania i zidentyfikowania; praktycznie nie wiemy kto siedzi przy klawiaturze komputera, prowadzi atak informacyjny i zakłócanie informacyjne,
2. terenem działań jest przestrzeń cybernetyczna, czyli globalna sieć informacyjna,
3. brak przestrzennych granic,
4. brak geograficznych i politycznych granic,
5. wielość obiektów ataku; szczególnie zagrożona jest tzw. infrastruktura krytyczna sektora państwowego i prywatnego, ich poszczególne elementy i podsystemy, oraz elementy infrastruktury kierowania bezpieczeństwem państwa, systemy dowodzenia, rozpoznania, łączności i kierowania uzbrojeniem,
6. proste technologie, zależność i powszechny dostęp do nowoczesnych rozwiązań związanych z technikami teleinformatyczną i komunikacyjną,
7. niejasne prawo, niejasna odpowiedzialność,
8. akt kryminalny,
9. akt wojny,
10. słabo określone przedsięwzięcia zaradcze,
11. czas, w tym zdolność do wykonania cybernetycznych uderzeń wyprzedzających, prowadzących do dezorganizacji i utraty zdolności sterowania przez podstawowe systemy przeciwnika,
12. ponadto walka informacyjna może:
    - stanowić element operacji politycznej, gospodarczej, a także operacji innej niż wojna,
    - mieć zasięg ograniczony (np. dany rejon lub region),
    - mieć zasięg nieograniczony, czyli może być prowadzona w dowolnym miejscu i w dowolnym czasie,
    - może mieć zasięg globalny, czego skutkiem może być dezorganizacja globalnej sieci informacyjnej,
    - może przynieść korzyści o charakterze strategicznym.

Należy wyraźnie zaznaczyć, że celem strategicznym walki informacyjnej jest uzyskanie przewagi informacyjnej nad przeciwnikiem.

Właściwości walki informacyjnej i cyberprzestrzeni pozwalają na prowadzenie wojny w cyberprzestrzeni w jakościowo innych warunkach z pominięciem tradycyjnego pola walki, gdzie wykorzystuje się środki ogniowe o zróżnicowanej sile rażenia. Tym polem konfrontacji będzie cyberprzestrzeń, gdzie zaangażowane strony będą korzystały z szerokiego spektrum środków

informacyjnych, ukierunkowanych na systemy i zasoby informacyjne uczestników kooperacji negatywnej. Stanowi to ogół środków komunikacji do użytku cywilnego i/lub wojskowego, kierowanych drogą cyfrową poprzez zautomatyzowane, połączone między sobą systemy (Harrel 2015, s. 160).

Istotne jest to, że walka informacyjna nie jest przypisana wyłącznie do sił zbrojnych, jest ona również prowadzona przez podmioty pozamilitarne w czasie pokoju i w stanie kryzysu. Możliwości prowadzenia działań ofensywnych na sieci komputerowe stają się nieodłącznym elementem arsenałów walki każdego państwa. Wymusza to na państwach podejmowanie rozwiązań organizacyjno-prawnych, wspieranych przez wyszkolony personel, środki materiałowe (w tym (sprzętowe) i finansowe, które pozwolą na prowadzenie skutecznych informacyjnych działań ofensywnych i defensywnych.

Podstawę tych działań powinna jednak stanowić cyberstrategia państwa, a także doktryna walki informacyjnej, będące częścią strategii bezpieczeństwa narodowego i doktryny militarnej.

Działania informacyjne można traktować w kategoriach broni masowego rażenia. Za takim stanowiskiem przemawia m.in. to, że wybuchowi broni atomowej towarzyszy impuls elektromagnetyczny, który niszczy urządzenia pracujące z wykorzystaniem promieniowania elektromagnetycznego. Dlatego właściwie zidentyfikowana, oceniona infrastruktura krytyczna państwa (obiektu) wytypowanego do ataku informacyjnego i zakłócania informacyjnego, połączona z informacją rozpoznawczą (wywiadowczą) i wsparta programami symulacyjnymi i wspomagającymi proces decyzyjny, może doprowadzić do zniszczenia narodu, a tym samym osiągnięcia celu strategicznego strony ofensywnej bez użycia sił zbrojnych w klasycznym rozumieniu.

*

Z uwagi na jej specyficzne cechy walka informacyjna jest prowadzona zawsze w informacyjnej przestrzeni osobowej i informacyjnej przestrzeni technicznej. Należy podkreślić, że nie jest ona czymś nowym, zawsze towarzyszy człowiekowi i na przestrzeni wieków ewoluowała wraz z pojawianiem się nowych środków komunikacji i technologii (Żebrowski 2015, s. 105). Informacja, system jej pozyskiwania, gromadzenia, przetwarzania, dystrybucji i jej ochrona, w każdym okresie historycznym decydowała o sukcesie, a nawet porażce. Wraz z rozwojem cywilizacyjnym ludzkość wchodziła w posiadanie coraz to nowych narzędzi, które pozwalały na doskonalenie form i metod pozyskiwania informacji. W tym wzmożonym procesie obecny był atak informacyjny, zakłócanie informacyjne i obrona informacyjna. Były one na przestrzeni wieków doskonalone i dostosowywane do potrzeb podmiotów będących uczestnikami kooperacji negatywnej i pozytywnej.

Podstawy zainteresowania walką informacyjną

Mając na uwadze cechy walki informacyjnej, warto wskazać przyczyny zainteresowania się tak skutecznym oddziaływaniem informacyjnym na osobową i techniczną przestrzeń informacyjną uczestników kooperacji negatywnej. Do przyczyn zainteresowania walką informacyjną zalicza się m.in. (Żebrowski 2015, s. 110):

1. powstanie i rozwój globalnej sieci informacyjnej,
2. istnienie licznych baz danych o zróżnicowanym przeznaczeniu i powszechny dostęp do komputerów osobistych,
3. upowszechnienie systemów łączności elektronicznej,
4. komputeryzacja wszystkich obszarów działalności państwa,
5. powszechne wykorzystywanie komputerów przez podmioty pozapaństwowe,
6. informatyzacja podmiotów właściwych w sferze bezpieczeństwa wewnętrznego i obronności państwa,
7. informatyzacja sił zbrojnych:
   - wzrost możliwości systemów łączności wszystkich szczebli dowodzenia, wysokie nasycenie wojsk nowoczesnymi środkami rozpoznania (w tym pochodzenia od optycznych do optoelektronicznych urządzeń rozpoznania obrazowego) i stosunkowo szerokie stosowanie środków precyzyjnego rażenia,
   - rosnące uzależnienie sił zbrojnych od cywilnej infrastruktury łączności naziemnej i satelitarnej, a także od komercyjnej techniki informatycznej,
8. wzmożona penetracja systemów informacyjnych i systemów informatycznych przez podmioty państwowe i niepaństwowe do tego nieuprawnione.

Cechy walki informacyjnej i globalna sieć informacyjna stanowią podstawy do poszukiwania paradygmatu bezpieczeństwa i obronności państwa, w tym prowadzenia wojny. W tych jakościowo nowych warunkach, cyberprzestrzeń jest piątym wymiarem prowadzenia konfrontacji militarnej obok przestrzeni powietrznej, kosmicznej, lądu i morza. Jest systematycznie rozpoznawana pod kątem jej wykorzystania z uwzględnieniem aktualnych osiągnięć w nauce i technice, czemu towarzyszy intensywny proces badawczy.

Obecnie wielu specjalistów przyjmuje, iż należy odejść od liniowego postrzegania sytuacji w aspekcie istnienia możliwość prowadzenia tzw. wojny cybernetycznej i przyjęcia sieciowego myślenia i działania, przyjmując za uzasadnione postrzeganie sytuacji jako sieci nieliniowych sprzężeń zwrotnych. Wojna cybernetyczna może w przyszłości stworzyć warunki do osiągania politycznych celów wojny nie na tradycyjnym polu walki, z wykorzystaniem materialnych, niszczących środków, lecz w przestrzeni cybernetycznej za pomocą środków informacyjnych, skierowanych przeciw systemom i zasobom informacyjnym (Sienkiewicz, Świeboda 2009, s. 85).

*

Warto mieć na uwadze to, że prowadzący walkę informacyjną porusza się na dwóch płaszczyznach, rzeczywistej i wirtualnej. Tym samym istotą tej złożonej sytuacji są: dyskrecja (niewykrywalność), zmienność, wiralność, odtwarzalność, wszechobecność, szkodliwość, możliwość przypisania, zwodniczość, interaktywność, ulotność i nieprzewidywalność. I tak (Harrel 2015, s. 35-36):

1. dyskrecja jest czynnikiem niezbędnym w przypadku pozycji ofensywnej: większość ważnych działań wymaga przede wszystkim braku detekcji; im bardziej słaba wykrywalność rozciąga się w czasie (łącznie z okresem po zakończeniu operacji w przypadku cyberbroni nieuchwytnej, która pozostaje w systemie na celowniku), tym bardziej odnalezienie źródła staje się sprawą skomplikowaną i wręcz niemożliwą,
2. zmienność jest właściwa głównie w warstwie programowej oraz informacyjnej, wskazuje na permanentny rozwój narzędzi, broni, ale też i samej cyberprzestrzeni, która nie zna rzeczywistych granic i która przystosowuje się do nowych okoliczności i przeszkód niczym żywy organizm,
3. wiralność jest takim rodzajem oddziaływania na informacje bądź oprogramowanie, który powoduje ich bardzo szybkie rozprzestrzenianie, skutkiem czego jest trudny do skontrolowania przez władze,
4. odtwarzalność jest pojęciem zakładającym, zależnie od przypadku, możliwość bądź nawet przymus klonowania w celu zabezpieczenia lub szkodzenia,
5. wszechobecność jest aspektem oferującym jakimś danym bądź oprogramowaniom możliwość znalezienia się w kilku miejscach cyberprzestrzeni w tym samym czasie, zasadniczo jest to powiązane z odtwarzalnością i wiralnością,
6. szkodliwość pociąga za sobą mniejsze lub większe zagrożenie wobec jednej z warstw cyberprzestrzeni; jedną z trudności w dziedzinie cyberstrategia jest poznanie dokładnego skutku niektórych działań,
7. możliwość przypisania,
8. zwodniczość jest maską Janusa cyberprzestrzeni, której każdy element, z jakiego się składa, ma drugie oblicze; przykładowo, P2P (*Peer to Peer*), pozwala rozładować sieci i znacznie przyspieszyć szybkość transmisji danych, jest również procederem, który może służyć cyfrowym fałszerstwom na dużą skalę,
9. interaktywność jest właściwa systemowi komunikacji maszyna – maszyna bądź człowiek – maszyna w tym sensie, iż zmusza do wymiany, jako że pasywność jest nie do zaakceptowania, nawet jeżeli ta interakcja jest zmienna, mniej lub bardziej szeroka,
10. ulotność jest elementem odnoszącym się do sieci cyfrowych w tym sensie, iż przepływ wykładniczy transferu danych doprowadza do działań, które mogą

być bardziej ograniczone w czasie aniżeli infrastruktury umożliwiające je fizycznie,

11. nieprzewidywalność jest najbardziej złożonym elementem do brania pod uwagę, ponieważ polega na przypadkowości działania, które może wystąpić w nieokreślonym miejscu (warstwy sprzętowe i softwarowe) w dążeniu do efektów nieokreślonych, o grawitacji trudnej do skwantyfikowania (przykładem intruzja, która nie zostaje szybko wykryta), a wszystko to – moment, w jakim występuje oraz długość trwania, jest równie niezdeterminowane (przed ofensywą cybernetyczną z reguły nie występuje wystrzał ostrzegawczy).

Warto mieć na uwadze to, że w cyberprzestrzeni uwzględnia się znaną od dawna walkę miecza i tarczy. Oznacza to, że uczestnicy kooperacji negatywnej w cyberprzestrzeni nie dysponują jednakowymi siłami i środkami, gdzie istnieją różnice w poziomie technicznego zaawansowania. Występuje tzw. asymetria nie tylko w wielkości posiadanych sił, ale także w istnieniu odmiennych problemów z tym związanych. *W przypadku tarczy – jest to ochrona systemu i zachowanie zdobyczy nawet za pomocą środków finansowych i ludzkich, a miecza – maksymalizacja ciosów zadanych po najmniejszych kosztach, łącząca dyskrecję, inwencję i szybkość. W ostatecznym wyniku miecz, jako bardziej mobilny, stale posiadający inicjatywę i natchniony ideą zdobywczą, zawsze będzie mieć przewagę nad tarczą, która wskutek nagromadzenia elementów osłaniających, siłą rzeczy cięższa, mniej mobilna, a zatem ogranicza się do oczekiwania przyszłych ataków. Cyberprzestrzeń reprodukuje ów schemat z nieprzewidywalnymi atakami i ochroną o coraz mniejszym zakresie, zwłaszcza, że aktorzy cyberofensywy niekoniecznie uderzają w te same miejsca wzmocnionego pancerza* (Harrel 2015, s. 37-38).

Walka informacyjna bronią XXI wieku

Bezpieczeństwo każdego państwa jest coraz bardziej uzależnione od sprawności funkcjonowania jego infrastruktury technicznej. Jej załamanie mogłoby spowodować katastrofę, której rozmiar jest z każdym rokiem coraz większy. Groźbę takiego rozwoju wydarzeń stwarzają zarówno skomplikowany charakter powiązań funkcjonalnych i sprzężeń wewnętrznych infrastruktury technicznej państwa, jak i lawinowy rozwój techniki informacyjnej. [...] *Załamanie funkcjonowania infrastruktury technicznej państwa może doprowadzić do dezorganizacji jego funkcjonowania i zagrożenia jego interesów na świecie* (J. L. 1999, s. 5).

Aktywność państw i podmiotów pozapaństwowych w otoczeniu wewnętrznym i środowisku bezpieczeństwa międzynarodowego, w tym w sferach militarnej i pozamilitarnej, poddawana jest intensywnemu oddziaływaniu informacyjnemu. Ma to miejsce w kooperacji negatywnej i pozytywnej. Szczególnie jest widoczna w tej pierwszej, która dominuje w naszym codziennym

życiu, nie tylko w skali państwa, czy regionu, ale także w skali globalnej. Skala tego oddziaływania zależy od wielu czynników, m.in. historycznych, ideologicznych, politycznych, kulturowych, religijnych, położenia geopolitycznego, stosunku do mniejszości narodowych i etnicznych, sojuszy polityczno-wojskowych i finansowo-gospodarczych, relacji z państwami graniczącymi i charakteru prowadzonej przez nie polityki, stanu demokracji, stabilnych regulacji prawnych i sprawnego wymiaru sprawiedliwości, rozwoju przestępczości pospolitej i zorganizowanej, arogancji władzy, uprzedmiotowienia społeczeństwa itp.

*

Podejmowanym decyzjom związanym z realizacją funkcji zewnętrznej i wewnętrznej państwa, bardzo często towarzyszą zjawiska destrukcyjne. *Ich objawy występują z różnym nasileniem, są bowiem funkcją impulsów sprawczych, najczęściej wywoływanych niepopularnymi decyzjami władz lub brakiem skutecznej decyzji. W pierwszym przypadku społeczeństwo odnosi wrażenie, iż jest traktowane instrumentalnie, w drugim irytują go przejawy niemocy i postępującego bezprawia (anarchizacji)* (Dworecki 1996, s. 33). Należy podkreślić, że podmioty prowadzące walkę informacyjną w sferze politycznej, gospodarczej, czy militarnej, ukierunkowaną na społeczeństwo własne, czy społeczność międzynarodową muszą mieć świadomość tego, że mogą pojawić się reakcje na wszelakiego rodzaju nieprawidłowości w takim stopniu, w jakim je one dotykają i zmieniają dotychczasowy stan rzeczy (Dworecki 1996, s. 33). Ich eskalacja stanowi poważne zagrożenie dla bezpieczeństwa wewnętrznego i zewnętrznego państwa. Związane jest to m.in. z determinacją, stopniem zorganizowania, zasięgiem, formą prowadzonych działań przez podmioty będące obiektem oddziaływania informacyjnego.

*

Walka informacyjna ma ścisły związek z wiadomością, która stanowi podstawę procesu decyzyjnego i działania każdego podmiotu. Informacje były i są zawsze pożądane, a jednostki czy też organizacje zawsze dążą do posiadania dostępu do szerokiego spektrum informacji użytecznych z ich punktu widzenia (Żebrowski 2005, s. 24).

Fundamenty współczesnego społeczeństwa oparte są na dostępności do informacji, która zabezpiecza prosperującej ekonomii wzrost lub spycha słabą w uzależnienie od silniejszej. Takie uzależnienie widoczne jest szczególnie w sferze politycznej, która zdominowała działalność wewnętrzną i zewnętrzną państwa. W dzisiejszym elektronicznie wzajemnie połączonym świecie, informacja przemieszcza się z prędkością światła, jest nieuchwytna i niezmiernie wartościowa. Dzisiejsza informacja jest ekwiwalentem wczorajszych fabryk, lecz jest dużo bardziej wrażliwa (Schwartau 1996, [za:] Szpyra 2003, s. 88).

Walka o informację jest prowadzona w każdym obszarze ze szczególnym wskazaniem na polityczny, ideologiczny, kulturowy, gospodarczy, wojskowy.Toczy się o dostęp do wyników opracowań naukowych, technicznych i nowoczesnych technologii produkcji, jest częścią walki z przestępczością zorganizowaną, terroryzmem itp. Jej celem jest wejście w posiadanie takich informacji, które pozwolą na uzyskanie przewagi informacyjnej nad przeciwnikiem wewnętrznym i zewnętrznym, co pozwala na wprowadzenie go w błąd, uzyskanie zaskoczenia, a tym samym na realizację celów strategicznych.

Przyjmuje się, że informacja staje się decydującym elementem pozwalającym na stymulację rozwoju i postępu. Zacznie odgrywać kluczową rolę w formach i metodach prowadzenia konfliktów zbrojnych, który będzie prowadzony nie na polu walki, ale w sferze informacji.

Konieczność walki o informację prowadzi do kształtowania nowych form konfliktów i sposobów ich rozgrywania, tj. walki w obszarze informacji.

Przykładowo, wyobraźmy sobie świat, gdzie informacja jest medium wymiany, a pieniądze używane są jedynie do zakupów podręcznych (ma to już miejsce – przyp. Autora) – świat, gdzie informacja, a nie język angielski, niemiecki, japoński czy rosyjski jest wspólnym językiem; świat, gdzie potęga wiedzy i informacji może uzurpować sobie siłę równą militarnej; świat całkowicie uzależniony od nowych narzędzi wyrafinowanych technologii, które czynią informację dostępną permanentnie dla każdego, gdziekolwiek, w każdym czasie; świat, gdzie ten, kto kontroluje informację, kontroluje ludzi; świat, gdzie elektryczna prywatność już nie istnieje (Szpyra 2003, s. 89).

Kolejne przykłady (Szpyra 2003, s. 89):

1. wyobraźmy sobie konflikt między przeciwnikami, w którym informacja jest wygraną, wojennym łupem – konflikt ze zwycięzcą i pokonanym; konflikt, który określa komputery i systemy komunikacyjne (łączności) jako podstawowe cele zmuszone do samoobrony przeciwko zabójczym, niewidzialnym kulom i bombom,
2. wyobraźmy sobie rywalizującą ekonomię, która walczy o poszerzenie strefy globalnego wpływu na elektroniczne, finansowe infostrady, nie poświęcając żadnych wydatków dla zapewnienia zwycięstwa; następnie wyobraźmy sobie świat złożony z firm, które rywalizują i rozwiązują spory za pomocą regularnych, wzajemnych najazdów – blitzkriegów na informacyjne infrastruktury; świat, gdzie elektroniczne i rywalizacyjne szpiegostwo jest oczekiwaną manierą prowadzenia biznesu,
3. wyobraźmy sobie świat, w którym osobisty rewanż i odwet są w zasięgu uderzenia klawisza; jakiego rodzaju jest to świat? to jest świat walki informacyjnej, a my jako jednostki i jako kraj nie jesteśmy przygotowania na przyszłość, którą sobie tworzymy.

*

Walka informacyjna wspierająca inne rodzaje walk, wobec wysokiej dynamiki negatywnych zjawisk zachodzących w informacyjnej sferze praktyki, jest szczególnie niebezpieczna dla obiektów objętych ofensywnymi działaniami informacyjnymi, tj.:

1. atakiem informacyjnym,
2. zakłócaniem informacyjnym.

Walka informacyjna zawsze jest istotnym elementem walki zbrojnej, dotyczy to również walki niezbrojnej. Z kolei postęp w technologii informacyjnej stanowi źródło jakościowych zmian w prowadzeniu walki informacyjnej, m.in. takie jak (Sienkiewicz, Świeboda 2009, s. 81):

1. wzrost różnorodności rodzajów i typu zagrożeń informacyjnych,
2. wzrost kompleksowości zagrożeń, tj. wzrost liczby typów i rodzajów obiektów zagrożeń informacyjnych,
3. wzrost autonomiczności informacyjnych oddziaływań destrukcyjnych,
4. wzrost autonomiczności niektórych form walki informacyjnej, tj. uzyskanie statusu samodzielnego środka osiągania celów militarnych,
5. globalizacja systemów informacyjnych,
6. powstanie przestrzeni cybernetycznej i nadanie jej rangi jednego z wymiarów walki.

*

Walka informacyjna jest bronią, która w zasadniczy sposób zmienia obszary konfliktów. Powoli zamienia bomby i naboje na informację. Informacja i takie narzędzia, jak technika teleinformatyczna i komunikacyjna usytuowane w globalnej sieci informacyjnej stanowią skuteczną broń o charakterze ofensywnym. Jest ona dostępna w katalogach, specjalistycznych sklepach ogólnie dostępnych. Jest to broń, do której dostęp jest powszechny tak dla pojedynczego człowieka, grupy zawodowej, narodu, mniejszości narodowych, etnicznych i religijnych, wyspecjalizowanych podmiotów sektora państwowego i prywatnego (np. służby specjalne, policyjne), sił zbrojnych, jak i organizacji przestępczych, organizacji terrorystycznych, najemników itp.

Walka informacyjna traktowana jako broń XXI wieku dotyczy m.in.:

1. polityki, która ukierunkowana jest na realizację funkcji wewnętrznej i zewnętrznej państwa; bardzo często towarzyszy jej walka ideologiczna,
2. pieniędzy; odnosi się do dystrybucji dóbr i polega na niedopuszczeniu ich do oponenta. Walka ta rodzi informacyjnych wojowników, którzy toczą walki na wskroś globalnej sieci w grze cyberyzyka,
3. przeżycia, wiele państw rozwija swoją gospodarkę m.in. w oparciu o kradzież technologii, nowoczesnych technik, patentów, receptur itp.,
4. strachu, ten kto kontroluje informację, może zaszczepić strach tym, którzy chcą trzymać swoje sekrety w ukryciu; np. obawa, że bank o kluczowym

znaczeniu upadnie, gdy tylko na jeden dzień powstanie w nim deficyt 23 miliardów dolarów i zostanie to ujawnione,

5. arogancji władzy, organizacji terrorystycznych, zorganizowanych grup przestępczych,
6. kontroli informacji; jako społeczeństwo posiadamy coraz mniejszą kontrolę nad rozszerzaniem rozprzestrzenianiem się elektronicznej anarchii w cyberprzestrzeni; dzisiejsza planeta oferuje dojrzałe warunki do walki informacyjnej, warunki, które nie były przewidywane nawet kilka lat temu,
7. wyzwań; z zaniedbanych dzielnic cyberprzestrzeni zjawią się hakerzy marginesu społecznego nie mający nic do stracenia; część z nich zorganizuje się w działające w cyberprzestrzeni gangi, zorganizowaną przestępczość cyberprzestrzeni. Uznają oni i docenią korzyści ekonomiczne płynące z prowadzenia walki informacyjnej.

*

Świat ***z***dominowany przez teleinformatykę, globalna sieć informacyjna (Internet) sprawiają, że informacje stają się powszechnie dostępne. Ta sytuacja generuje określone zagrożenia nie tylko dla jednostki czy narodu, ale dla bezpieczeństwa wewnętrznego i zewnętrznego państwa. Jednym z kluczowych zagrożeń to niekontrolowany wyciek informacji charakteru niejawnego, co przekłada się m.in. na bezpieczeństwo państwa. Przeciwnik wykorzystuje te informacje stosując zróżnicowane formy i metody ataku informacyjnego na systemy informacyjne (w tym systemy informatyczne), które najczęściej nie są skutecznie zabezpieczone.

Kolejne zagrożenie to możliwość wpływania jednostek, państw, a także podmiotów pozapaństwowych (np. naruszających prawo międzynarodowe i krajowe) na innych poprzez wysyłanie informacji fałszywych, czyli dezinformację.

Każda wojna (w tym i o charakterze pozamilitarnym) to droga kłamstwa, dlatego jeśli coś możesz – pokazuj, że nie możesz; jeśli korzystasz z czegoś – pokazuj, że nie korzystasz; jeśli jesteś blisko – pokazuj, że daleko; jeśli znajdujesz się daleko – pokazuj, że jesteś blisko; zwabiaj przeciwnika korzyściami, spowoduj u niego dezorganizację i bierz go: przyjąwszy pokorny wygląd, wzbudź w nim pewność siebie; napadaj przeciwnika kiedy nie jest przygotowany; pojawiaj się tam, gdzie on ciebie nie oczekuje (Sun Tsu 1994).

Powyższe oznacza, że państwo dążące do utrzymania zdolności konkurencyjnej, realizacji funkcji zewnętrznej i wewnętrznej jest zmuszone do poszukiwania możliwości zastosowania nowoczesnych technologii teleinformatycznych i komunikacyjnych, a także do zabezpieczania swoich potrzeb informacyjnych.

Należy zwrócić uwagę, że w sferze militarnej systemy informacyjne łączone przez sensory z centrum decyzyjnym, w coraz większym stopniu zależne są od cywilnych technologii, do których dostęp posiadają wyłącznie państwa wysoko

rozwinięte. Oznacza to, że będą bardziej podatne na globalne oddziaływanie informacyjne, w tym na ataki informacyjne i zakłócanie informacyjne, ze szczególnym wskazaniem na infrastrukturę krytyczną. Podatność ta może być tak duża, że może zakłócić funkcjonowanie podstawowych organów państwa, w tym właściwych w sferze bezpieczeństwa i obronności państwa. Z uwagi na powszechny dostęp do technologii informatycznych i komunikacyjnych szczególne zagrożenie stanowią państwa słabe, które za pośrednictwem posiadanych narzędzi mogą atakować przeciwnika silnego, uderzając w jego czułe miejsce jakim jest infrastruktura krytyczne, np. systemy: finansowe, energetyczne, dystrybucji ropy i gazu, żywności, lekarstw, łączności.

Cyberprzestrzeń obok państw (ich wyspecjalizowanych instytucji) jest również wykorzystywana przez organizacje przestępcze i terrorystyczne, a także pojedynczych hakerów.

Rodzące się z tego powodu konflikty będą rozstrzygane bez konieczności angażowania sił zbrojnych, które w wyniku blokady informacji niezbędnej do ich funkcjonowania staną się niezdolne do sprawnego działania. […] *Walka w sferze informacji obejmuje nie tylko obszar militarny, ale całe społeczeństwo, gdyż będzie ona przebiegać nie tylko między polityczno-militarnymi przeciwnikami, ale w każdej dziedzinie rywalizacji* (S. P. 1997, s. 37).

Walka ta przebiega między systemami zarzadzania bezpieczeństwem państwa, systemami dowodzenia i kierowania, w ramach których biorą udział podmioty zdobywania, gromadzenia, przetwarzania, ochrony, przesyłania i wykorzystania informacji, a także te, które aktywnie uczestniczą w prowadzeniu dezinformacji, zakłócaniu systemów dowodzenia, rozpoznania, łączności, kierowania uzbrojeniem. Tak więc, w aktualnych i przyszłych konfliktach nie systemy walki zbrojnej potencjalnego przeciwnika, lecz jego system nerwowy jest (będzie) niszczony w pierwszej kolejności (S. P. 1997, s. 37).

Rozwój nauki, techniki, a przede wszystkim nowoczesnych technologii produkcji (Dworecki 1996, s. 150), prowadzi do zwiększenia możliwości uczestników walki informacyjnej w sferze zdobywania, zakłócania i obrony informacyjnej. To techniki teleinformatyczna i komunikacyjna, skala i dynamika ich rozwoju sprawiają, że walka informacyjna na początku XXI wieku jest uniwersalna i nabiera szczególnego znaczenia. Przy braku skutecznej polityki bezpieczeństwa sieci i systemów informacyjnych walka informacyjne (atak informacyjny) pozwala na nieograniczony dostęp do zasobów informacyjnych w sferach: politycznej, wojskowej, gospodarczej, finansowej, marketingowej, naukowej, organów ścigania i wymiaru sprawiedliwości, wyspecjalizowanych agend rządowych (np. wywiadu, kontrwywiadu), mediów tradycyjnych i elektronicznych, organizacji terrorystycznych, zorganizowanych grup przestępczych, najemników itp.

Warto mieć na uwadze to, że cechy przypisywane walce informacyjnej oznaczają, że jest ona prowadzona nie tylko z udziałem komputerów, sieci

komputerowych i globalnej sieci informacyjnej. *Obejmuje ona informacje we wszelkiej postaci i przesyłane wszystkimi środkami, począwszy od ludzi i ich fizycznego środowiska do druków, telefonów, radia i telewizji, do komputerów i sieci komputerowych. Wojna taka to operacje ukierunkowane przeciw treści informacji i operacje przeciw związanym z nimi systemami, włącznie z oprzyrządowaniem, oprogramowaniem i pracą człowieka* (Denning 2002, s. 14).

O sile uczestników walki informacyjnej decyduje m.in. bezpieczny przepływ informacji, co pozwala na realizację celów strategicznych we wszystkich przestrzeniach jej prowadzenia. Rozwijając się infosfera pozwala na pokonanie bariery czasu i przestrzeni, która w trwającej kooperacji negatywnej nabiera szczególnego znaczenia, dla każdego uczestnika walki informacyjnej.

Walka informacyjna a siły zbrojne

Siły zbrojne są na stałe wpisane w jakościowo nowy wymiar prowadzenia operacji wojskowych jakim jest cyberprzestrzeń. Można nawet postawić tezę, że na stałe wpisują się w ten obszar prowadzenia działań i są od niej zależne. Wyizolowanie prowadzi do klęski.

Cyberprzestrzeń jest w rozmaitym stopniu nieodłączna od globalizacji: działania prowadzone w danym miejscu globu mogą mieć reperkusje na jego drugim końcu. O ile ludzie pozostają więźniami swojej fizyczności, o tyle ich wirtualni awatarzy mogą się symultanicznie projektować w kilku miejscach przestrzeni dysponującej właściwymi receptorami (Harrel 2015, s. 41).

Cyberprzestrzeń jest obszarem konfliktowym, gdzie trwa kooperacja negatywna zarówno w sferze pozamilitarnej, jak i militarnej. *Jest to miejsce konfrontacji aktorów i wizji, gdzie wyzwania zwiększają się wraz z możliwościami, które świat oferuje, a użytkownicy sami stają się źródłem zainteresowania, czasem nawet pożądania. Według zasady wykrytej przez duńskiego badacza Jakoba Nielsena, w cyberprzestrzeni panuje reguła 90 – 9 – 1, gdzie tylko 1% jednostek tworzy zawartość uzupełnioną przez 9% współpracowników dla 90% użytkowników* (Harrel 2015, s. 42).

Globalna wioska zdominowana przez mobilne cyfrowe terminale pozwala na realizacje zadań na poziomie strategicznym. Ta właściwość i cechy walki informacyjnej są adoptowane przez siły zbrojne (poszczególne komponenty), jednostki walki elektronicznej, wywiad i kontrwywiad, służby policyjne, prywatny sektor gospodarczy, a także organizacje przestępcze, terrorystyczne.

Na szczególną uwagę zasługują jednak siły zbrojne i jego wyspecjalizowane komponenty.

We wszystkich koncepcjach prowadzenia walki informacyjnej w działaniach militarnych o charakterze ofensywnym, jak i defensywnym, główną rolę przypisuje się zasobom informacyjnym. Zasoby te stanowią kluczowy wyznacznik potencjałów militarnych uczestników kooperacji negatywnej. Oznacza to, że

warunkiem uzyskania powodzenia w działaniach bojowych jest uzyskanie przewagi informacyjnej nad przeciwnikiem. Stanowi ona zdolność do zdobywania, gromadzenia, przetwarzania i dystrybucji informacji dla uprawnionych odbiorców, a także ochrony przed analogicznymi działaniami przeciwnika. Uzyskanie przewagi informacji skutkuje dominacją informacyjną, która obejmuje zarówno wysiłki ofensywne, jak i defensywne, których celem jest stworzenie dystansu między tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni bojowej (Darilek 2001, s. 17, [za:] Sienkiewicz, Świeboda 2009, s. 85-86).

Tzw. cyberwojna oznacza prowadzenie operacji militarnych zgodnie z zasadami dotyczącymi informacji i przygotowywanie się do tych operacji. To oznacza przerywanie lub niszczenie szeroko pojętych systemów informacji i komunikacji, uwzględniających nawet kulturę militarną przeciwnika, aby poznać samemu: kto jest, gdzie jest, co i kiedy może zrobić, dlaczego walczy, z jakimi groźbami liczyć się najpierw i tak dalej. Inaczej mówiąc, trzeba dowiedzieć się wszystkiego o przeciwniku, jednocześnie nie pozwalając przeciwnikowi dowiedzieć się wiele o nas (Denning 2002, s. 77). Działania tego charakteru mają wpływ na uzyskanie omawianej dominacji informacyjnej nad przeciwnikiem.

Przyjmując koncepcję prowadzenia operacji informacyjnych poprzedzających prowadzenie działań militarnych, wymaga się poszukiwania nowych kryteriów oceny efektywności. Jedną z nich jest tzw. stosunek wiedzy, wyrażający dominację informacyjną, określony dla następujących założeń (Sienkiewicz, Świeboda 2009, s. 86):

1. dowolna jednostka kontroluje dowolny obszar, gdy jest ona zdolna do działania wewnątrz tego obszaru w sposób swobodny,
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).

Dla potrzeb działań militarnych XXI wieku walka informacyjna obejmuje (Szpyra 2003, s. 96):

1. walkę o przewagę w dowodzeniu,
2. walkę bazującą na wiedzy rozpoznawczej,
3. walkę elektroniczną,
4. działania psychologiczne,
5. wojnę hackerską,
6. informacyjną walkę ekonomiczna,

7. cyberwojnę (walkę w wirtualnej rzeczywistości),
8. dezinformację militarną (wprowadzanie w błąd co do możliwości i zamiarów),
9. fizyczne niszczenie (użycie spektrum broni od konwencjonalnej do impulsu elektromagnetycznego),
10. przedsięwzięcia bezpieczeństwa.

*

Militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działonem przeciwnika (Szpyra 2003, s. 106).

Elementami militarnej walki informacyjnej są:

1. atak informacyjny, który obejmuje:
   - atak informatyczny (w sferze przetwarzania danych cyfrowych),
   - atak elektroniczny,
   - atak ogniowy,
   - działania psychologiczne,
   - dezinformacja,
2. zakłócanie informacyjne,
3. obrona informacyjna, która przybiera formy:
   - przeciwdziałania aktywności rozpoznawczej, polegającego na odstraszaniu i obezwładnianiu,
   - ochrony informacji, polegającej na prowadzeniu: kontrwywiadu, ochrony technicznej, ochrony informatycznej, ochrony psychologicznej, kontrdezinformacji, inżynieryjnej rozbudowy.

Warto mieć na uwadze to, że wykorzystywanie systemów informacyjnych przez dowódców i sztaby pozwala na monitorowanie sytuacji na polu walki, wprowadzanie zmian w zależności od przebiegu działań, optymalne wykorzystywanie posiadanych sił i środków rażenia, zapewniając interoperacyjność i spójność działań.

Tabela 2. Oczekiwane skutki walki informacyjnej

Lp.	**Siły własne**	**Siły przeciwnika**
1.	Ochrona systemów dowodzenia, łączności i rozpoznania	Zakłócanie procesów informacyjno-decyzyjnych w systemach dowodzenia
2.	Minimalizacja wpływu walki elektronicznej	Minimalizacja efektywności systemów dowodzenia, kierowania środkami walki, teleinformatyki,

		rozpoznania i walki elektronicznej
3.	Minimalizacja zagrożeń informacyjnych bezpieczeństwa systemów dowodzenia i kierowania	Uniemożliwienie wykorzystania pełnej siły rażenia oraz obniżanie tempa działań
4.	Minimalizacja wpływu działań psychologicznych	Zwiększenie podatności na działania psychologiczne

Źródło: (Sienkiewicz, Świeboda 2009, s. 88).

Realizacja przyjętych celów walki informacyjnej jest osiągana następującymi sposobami:

1. w czasie pokoju, poprzez elektroniczne zastraszanie,
2. w czasie narastania kryzysu, poprzez selektywne i zmasowane użycie środków elektronicznych przeciwko wojskowym i cywilnym strukturom, kierowania państwem, dowodzenia wojskami i strukturom informacyjnym,
3. w czasie trwania konfliktu zbrojnego, poprzez zmasowane użycie zarówno środków elektronicznych, jak i ogniowych przeciwko wojskom i cywilnym strukturom dowódczym i informacyjnym przeciwnika.

Przyjmuje się, że współczesne konflikty zbrojne powinny być traktowane jako synergizm dwóch elementów, tj.:

1. sprzężenia ognia i elektroniki – polega na wykorzystaniu potencjału bojowego do bezpośredniego oddziaływania na technikę bojową i siłę żywą,
2. informacji, mieszczą się tu możliwości zdobywania informacji i ich wykorzystanie w celu zwiększenia potencjału bojowego środków bezpośredniego oddziaływania bojowego na przeciwnika (środków ogniowych i walki elektronicznej).

*

Kierujący bezpieczeństwem państwa, dowodzący wojskami na poziomie strategicznym, operacyjnym i taktycznym w celu pokonywania różnych trudności, związanych zwłaszcza z ryzykiem działania, pomyślnym kształtowaniem swojej pozycji wobec przeciwnika, muszą dysponować odpowiednimi informacjami i systemami ich zdobywania oraz przetwarzania. Muszą uwzględniać tzw. infosferę, która z jednej strony pozwala na likwidację tzw. luki informacyjnej, a z drugiej stanowi źródło szumu informacyjnego. Informacje są konieczne dla prawidłowego sterowania procesami w ramach prowadzonych działań militarnych, a także właściwego wykorzystania posiadanych sił i środków ogniowych. To walka informacyjna i jej specyficzne cechy pozwalają na zabezpieczenie własnych potrzeb informacyjnych, co niekiedy przekłada się na uzyskanie przewagi informacyjnej nad uczestnikiem kooperacji negatywnej w sferze militarnej.

Zakończenie

Unikatowy charakter walki informacyjnej sprawia, że wspiera ona działania różnych podmiotów w działaniach ofensywnych i defensywnych, ukierunkowanych na otoczenie wewnętrzne i zewnętrzne państwa. Brak świadomości jej prowadzenia przez przeciwnika, to lekceważenie własnego bezpieczeństwa. Jej nieograniczony zasięg, a także wszechobecność, pozwala ingerować w nasze codzienne życie. To broń informacyjna XXI wieku, która pozwala na realizację celu (celów) bez użycia sił zbrojnych w tradycyjnym rozumieniu. Na jej negatywne skutki najczęściej narażone są państwa wysoko usieciowione, co pozwala stronie słabej na zadanie dotkliwych strat przeciwnikowi. Na sukces (lub porażkę) obok cech walki informacyjnej, mają wpływ: systemy komunikacyjne i komputery, a także wiedza i umiejętności. Dlatego blitzkrig informacyjny może towarzyszyć jednostkom, państwom w procesie realizacji funkcji wewnętrznej i zewnętrznej państwa.

Bibliografia

Darilek, R. (2001) *Measures of Effectiveness for the Information – Age Army*. Santa Monica, CA: Rand.

Denning, D. E. (2002) *Wojna informacyjna i bezpieczeństwo informacji.* Warszawa: Wydawnictwa Naukowo-Techniczne.

Dworecki, S. (1996) *Od konfliktu do wojny*. Warszawa: BUWIK.

J. L. (1999) *Bezpieczeństwo Stanów Zjednoczonych w świetle walki informacyjnej*. „Wojskowy Przegląd Zagraniczny", nr 3.

Sienkiewicz, P., Świeboda, H. (2009) *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej.* W: Madej, M., Terlikowski, M. (red.), *Bezpieczeństwo teleinformatyczne państw*. Warszawa: Polski Instytut Spraw Międzynarodowych, s. 75-94.

S. P. (1997) *Informacja jako decydujący czynnik sukcesu w przyszłych konfliktach zbrojnych*. „Wojskowy Przegląd Zagraniczny", nr 1.

Schwartau, W. (1996) *Information Warfare. Cyberterrorism: Protectinq Your Personal Security in the Electronic Age.* New York: Thunder's Mouth Press.

Sun Tsu (1994) *Sztuka wojny*. Warszawa: Wydaw. Przedświt.

Szpyra, R. (2003) *Militarne operacje informacyjne*. Warszawa: Wydaw. AON.

Harrel, Y. (2015) *Rosyjska cyberstrategia*. Warszawa: Wydaw. DiG.

Żebrowski, A. (2005) *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej (Wywiad i kontrwywiad w latach 1989 – 2003).* Kraków: Wydaw. ABRYS.

Żebrowski, A. (2015) *Walka informacyjna zagrożeniem dla jednostki, narodu, państwa*. W: Wiśniewska-Paź, B. (red.), *Edukacja a bezpieczeństwo w różnych wymiarach i kontekstach: formacje militarne i paramilitarne wobec wyzwań edukacyjnych*. Wrocław: Wydaw. Uniwersytetu Wrocławskiego, s. 105-123.

Streszczenie

Walka informacyjna wspierająca uczestników kooperacji pozytywnej i negatywnej, zajmuje znaczącą pozycję wśród innych walk. Na szczególną uwagę zasługują jej cechy, co czyni ją szczególnie niebezpieczną. Jest prowadzona w sposób skryty, przeciwnik jest anonimowy, brak granic przestrzennych, geograficznych i doraźnych, istnieje wielość obiektów ataku. Ponadto wykorzystuje proste technologie, niejasne prawo, słabo określone przedsięwzięcia zaradcze, a także niejasną odpowiedzialność. Jest zarówno aktem kryminalnym i aktem wojny. Uczestnicy każdej kooperacji prowadzą walkę informacyjną, gdzie ma miejsce atak informacyjny, zakłócanie informacyjne i obrona informacyjna. Jej celem strategicznym jest zawsze uzyskanie przewagi informacyjnej nad przeciwnikiem, co pozwala na podejmowanie właściwych decyzji i działań.

Słowa kluczowe: walka informacyjna, elementy walki informacyjnej

Determinants of information warfare

Abstract

Information warfare supports participants of positive and negative cooperations, and holds the significant position among other warfare. Its characteristics deserve special attention because they make it dangerous. Information warfare is waged in an implicid way and the opponent is anonymous. Furthermore, there is no spatial, geographical and ad hoc borders. There is a multiplicity of targets. Moreover, information warfare uses simple technologies, a vague law, undefined procedures and unclear responsibility. It is both a criminal act and an act of war. Participants of each cooperations wage information warfare, where is an information attack, distortion of information and information security. The strategic goal of information warfare is to achieve information adventage over the enemy, which allows to make a right decisions and activities.

Keywords: information warfare, elements of information warfare

Kacper Mirosław Milkowski
Uniwersytet Warmińsko-Mazurski w Olsztynie

Wojna informacyjna w Donbasie w ujęciu prawa międzynarodowego

Wstęp

Konflikt we wschodniej Ukrainie jest bardzo ważny dla przyszłości nie tylko Ukrainy, ale także kształtowania się ładu międzynarodowego. W trakcie zajęcia półwyspu krymskiego Rosja zaprezentowała światu, jak doniosłą rolę odgrywa przekazywanie „właściwych" wiadomości określonej lokalnej społeczności. Prowadzenie wojny informacyjnej pozwala podporządkowanie sobie ludzi bez rozlewu krwi. Celem prowadzenia takich działań jest oddziaływanie na emocje, motywy, obiektywne rozumowanie. To powoduje, że w dalszej kolejności będzie to miało wpływ na zachowania rządów innych państw, organizacji, grup i jednostek. Przejawami wojny informacyjnej będzie stosowanie: presji psychologicznej, podważanie zaufania i wiarygodności w oczach partnerów zagranicznych, wzmacnianie paniki lub poczucia zagrożenia, kompromitowanie władz i elit itp. (Lelonek 2016). Wobec tego to mass media stają się podstawowym czynnikiem, za pomocą którego Federacja Rosyjska, lokalne władze, czy Ukraina wpływać będą na kształtowanie się opinii w regionie, jak i na świecie na temat Ukrainy oraz postrzegania obecnej sytuacji w Donbasie[1] (Chernyak 2015). Media realizując jedną ze swoich najważniejszych funkcji, czyli informacyjną, przedstawiają wydarzenia w tym czy innym świetle, co powoduje kształtowanie opinii społecznej na pewien temat. Dla wielu osób na świecie media są jedynym źródłem informacji, dlatego ich zawartość oraz sposób przedstawiania treści jest bardzo ważny. Sprawnie wykorzystał i wykorzystuje to prezydent Rosji Władimir Putin, który to podejmuje wiele działań wchodzących w zakres tzw. wojny informacyjnej. Instrumentem wykorzystywanym w wojnie informacyjnej na Ukrainie jest także Internet. Celem ataków są przede wszystkim sieci komputerowe, a w szczególności witryny internetowe rządu, wojska, czy strony koncernów prywatnych należących do oligarchów angażujących się w konflikt. Zaangażowani w wojnę internetową hakerzy wykorzystują Internet do szerzenia propagandy, czy dezinformacji, stosują narzędzia poswalające na wprowadzenie szkodliwego oprogramowania, włamania, blokowanie, jak również przeciążanie serwerów.

Wojna informacyjna

Wojna informacyjna, zgodnie z definicją przedstawioną przez J. Darczewską, jest to podporządkowanie sobie elit i społeczeństw innych państw w sposób niezauważalny, przy wykorzystaniu różnych tajnych i jawnych kanałów (służb

specjalnych, dyplomatycznych, medialnych), oddziaływania psychologicznego, dywersji ideologicznej i politycznej (Darczewska 2014). Głównym celem prowadzenia wojny informacyjnej jest zgodnie z twierdzeniem Messnera: „zdobycie duszy wrogiego narodu" (Месснер 2004). Rosyjska koncepcja prowadzenia wojen informacyjnych nawiązuje do wojen psychologicznych i specpropagandy stosowanej w ZSRR (Darczewska 2014). Bohdan Pac wskazuje, że *strona rosyjska definiuje wojnę informacyjną jako oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, które mogą być stosowane jako swoista broń informacyjna. Działania te skierowane są nie tylko przeciw siłom zbrojnym, ale przede wszystkim ukierunkowane są na całe społeczeństwo oraz jego świadomość, a także na aparat administracyjny, świat nauki i kultury oraz przemysł i ekonomikę danego państwa* (Pac 2016).

Władze Federacji Rosyjskiej zdały sobie sprawę z tego, jak doniosłą rolę odgrywa informacja w prowadzeniu działań destabilizujących dane państwo. Jak wskazuje Tomasz Aleksandrowicz: *uznanie informacji za zasób strategiczny – zarówno w wymiarze militarnym, jak i pozamilitarnym – spowodowało powstanie kategorii walki informacyjnej, a więc takiej, w której informacja traktowana jest zarówno jako broń, jak i cel ataku*. Podstawowymi narzędziami wojny informacyjnej są: dyplomacja, propaganda, kampanie psychologiczne, działania na poziomie wpływania na procesy polityczne lub kulturowe, dezinformacja, manipulacja lokalnymi mediami, czy infiltracja sieci komputerowych i baz danych (Aleksandrowicz 2015).

Już w trakcie trwania „rewolucji godności" na Placu Niepodległości w Kijowie Rosja rozpoczęła zintensyfikowaną działalność propagandową. Była do tego w pełni przygotowana. Działania okazały się na tyle skuteczne, że Krym udało się odseparować bez większego rozlewu krwi. Rosyjskie media, w szczególności te państwowe zaczęły publikować materiały, których celem było podburzenie nastrojów obywateli Ukrainy wobec krajów zachodnich i Stanów Zjednoczonych. Cała kampania została przeprowadzona w sposób konsekwentny. Od początku prowadzenia ww działań w Donbasie pracowali dziennikarze zarówno z Rosji, Polski, Ukrainy, jak i państw zachodnich oraz Stanów Zjednoczonych. Relacje z miejsc zdarzeń systematycznie zamieszczane były w serwisach informacyjnych oraz prezentowane w przekazach telewizyjnych. Dla Rosji Donbas okazał się sprzyjającym środowiskiem z powodu bliskości kulturowej, braku bariery językowej, a przede wszystkim dużej liczby etnicznych Rosjan i rosyjskojęzycznych Ukraińców zamieszkujcych ten teren. Te same zdarzenia były w różny sposób interpretowane i przedstawiane przez dziennikarzy określonych serwisów i telewizji. Mieszkańcy regionu mając dostęp do telewizji ukraińskiej oraz rosyjskiej wybierali tę drugą. Wiązało się to z faktem, że duża część osób na wschodzie

Ukrainy nie zna języka ukraińskiego, a przekazy rosyjskie miały dla nich dogodniejszą formę. Nie ulega wątpliwości, że określone informacje odbierane przez społeczeństwo mają silny wpływ na kształtowanie się opinii publicznej. Świadoma skuteczności mass mediów Rosja posługuje się w Donbasie i na Krymie rozbudowaną rosyjskojęzyczną propagandą.

Mass media, zgodnie z definicją zawartą w encyklopedii Państwowego Wydawnictwa Naukowego, są środkami masowego przekazu (prasa, radio, telewizja) (PWN 2016). Zazwyczaj komunikaty przez nie tworzone są krytyczne wobec władzy, natomiast gdy są w jej posiadaniu, to stają się instrumentem za pomocą, którego można skutecznie manipulować społeczeństwem. Natomiast propaganda ma za zadanie w sposób świadomy oddziaływać na odbiorcę poprzez systematyczne rozpowszechnianie określonych haseł, sloganów, idei, jak również symboli, gestów w celu pozyskania zwolenników i nakłonienie ich do zachowań pożądanych z punktu widzenia nadawcy, który ją rozpowszechnia. Osłabienie propagandy grozi osłabieniem mobilizacji społeczeństwa, pojawieniem się wątpliwości i dostrzeżeniem problemów rosyjskiej rzeczywistości, na którą ma wpływ konflikt we wschodniej Ukrainie, natomiast dla władzy będzie oznaczać początek kłopotów (Stępniewski 2014). Propaganda stosowana w ramach wojny informacyjnej przejawia się etykietowaniem i stygmatyzowaniem przeciwnika, czy budowaniem przejaskrawionego obrazu wroga zarówno wewnętrznego („zdrajca narodu"), jak i zewnętrznego („zgniły Zachód", „faszystowski Zachód"). Zazwyczaj prezentowany jest on za pomocą mowy nienawiści. W rosyjskich mass mediach używa się określeń takich jak „faszystowska junta" i informuje się o „oddziałach karnych", które w rzeczywistości nie istnieją. W Donbasie wspierane są wszelkie przejawy postaw, które cechują się poczuciem odrębności narodowej wobec Ukrainy. Ma to na celu pokazanie społeczeństwu w regionie, że walczą o swój głos – mass media nawołują do zmiany zasad gry, rezygnacji z ukraińskich planów eurointegracji. Należy zatem zauważyć, że w tej sytuacji mass media dotykają aspektów ideologicznych, jakimi jest ich wpływ na tworzenie i podtrzymywanie narodowej tożsamości odbiorców. Chcą one wykreować obywatela Donieckiej, czy Ługańskiej Republiki Ludowej i pokazać, że jedynym przyjacielem – sojusznikiem jest Rosja (Darczewska 2015).

Obraz konfliktu w Donbasie, który został zaprezentowany rosyjskojęzycznym obywatelom Ukrainy w Donbasie, nie był prawdziwy, ale dzięki kontroli mediów i ich dyscyplinie – spójny i jednoznaczny. Siła propagandy zdecydowała o tym, że oni uwierzyli w kremlowskie informacje, często wbrew faktom i własnym doświadczeniom. Poddana propagandzie ludność gotowa była i jest zakceptować sprzeczności. Jako przykład można odnieść się do sposobu prezentowania faktów. Wypowiedzi prezydenta Władimira Putina dotyczące wojsk przebywających na Krymie zawierały sprzeczne dane. W marcu 2014 roku prezydent stwierdził, że uzbrojeni ludzie na terytorium Krymu to „samoobrona"

złożona z mieszkańców. W późniejszych wypowiedziach stwierdził, częściowo przyznając się, że w czasie przeprowadzanego referendum wojsko rosyjskie „zabezpieczało swobodne wyrażenie woli mieszkańców Krymu" (kremlin.ru 2014). Natomiast w marcu 2015 r. w swojej wypowiedzi przyznał, że to on osobiście dowodził wojskiem, które zdobyło Krym (Prus 2015).

Wojna informacyjna prowadzona przez Federacje Rosyjską w Donbasie ma na celu zdestabilizowanie sytuacji w regionie. Ludności zamieszkałej na terenie Donieckiej i Ługańskiej Republiki Ludowej prezentuje się treści mające na celu wzbudzanie negatywnych emocji wobec rządu Ukrainy oraz mieszkańców zachodnich obszarów. Prezentując ich jako „faszystów" czy „banderowców" wpływa się na kwestionowanie przez obywateli ukraińskich faktów. Działania skoncentrowane są na odwoływaniu się do „historycznej wrażliwości" sporów granicznych, rosyjskich obywateli mieszkających w innych państwach (i pragnących samostanowienia w kraju zamieszkania) czy sprzeciwów wobec nazizmu i faszyzmu itd. Mieszkańcy tego regionu pod wpływem takich przekazów nie chcą się utożsamiać z osobami z zachodniej Ukrainy (Thomas 2015). Wskazuje się lokalnej ludności, że tylko mają dualny wybór pomiędzy „dobrą Rosją", która cały czas pomaga i wspiera (np. misje humanitarne) a „złym Kijowem", gdzie panuje chaos wywołany przez wpływy zachodnich służb specjalnych, faszystów i oligarchów (Lipman 2015). Federacja Rosyjska realizując działania wynikające z wojny informacyjnej prezentowała za pomocą mass mediów protesty na Placu Niepodległości w Kijowie, jako spisek państw zachodnich, sterowany przez władze USA mający na celu przejęcie władzy w kraju. Starały się one udowadniać, że USA dąży do osłabienia Rosji, bo nie chce, aby odzyskała ona należną jej silną pozycję na arenie międzynarodowej. Pokazują one, że inicjatorem antyrosyjskiej polityki jest Waszyngton, który obecnie cieszy się pozycją najsilniejszego państwa na świecie, a w razie wzmocnienia Rosji może ją utracić.

Zwrócić należy także uwagę, że propaganda stosowana w Donbasie zostaje także przeniesiona na terytorium Federacji Rosyjskiej. Władza stanęła przed wyzwaniem jakim jest wytłumaczenie obywatelom Federacji Rosyjskiej, dlaczego ich sytuacja życiowa z dnia na dzień się pogarsza. Właśnie stąd sytuację w Rosji od 2014 r. oddaje określenie „między lodówką a telewizorem" (Prus 2015). Umiejętnie prowadzona propaganda powoduje to, że obywatele stają się skorzy do poświęceń.

Przykładem pokazującym w jaki sposób media w Donbasie nastawione są do obywateli Ukrainy prezentuje obraz ukrzyżowanego chłopca. 12 lipca 2014 r. w *prime timie* transmisji głównego kanału Rosji ORT w wiadomościach był pokazany fragment wywiadu z panią Haliną Pyszniak. W rozmowie z dziennikarką Julią Czumakową kobieta mówiła: *Centrum miasta, to plac Lenina, jedyne miejsce, gdzie można zebrać razem tyle ludzi. Zebrali wszystkie kobiety, dzieciaków, starszych ludzi* [...] *Nazywa się to „pozorna śmierć" – wzięli chłopczyka, małego,*

w koszulce i majteczkach... Jak Jezusa, przybili do deski. [...] *I to na oczach matki, żeby patrzyła. Krzyki były* [...]. *Ludzie mdleli. Półtorej godziny dziecko się męczyło aż zmarło. A potem matkę przywiązali do czołgu i wozili tak po placu* [...]. Wskazane zdarzenie miało pokazać, jak okrutni są żołnierze ukraińscy. Zaprezentowanie takiej zbrodni powoduje strach wśród lokalnej społeczności przed wojskiem z zachodu, a żołnierze Donieckiej i Ługańskiej Republiki Ludowej uchodzą za bohaterów, którzy bronią ich przed tymi ludźmi. Później okazało się, że cała ta historia nagłaśniana w mediach lokalnych, a później w europejskich, okazała się wyreżyserowana. Brali w niej udział aktorzy, którzy na potrzeby telewizji przygotowali takie działania. 18 grudnia 2014 r., kiedy odbyła się otwarta konferencja z Władimirem Putinem i gdzie został poruszony problem prawdziwości podobnych wiadomości na stronie internetowej ORT pojawił się komunikat o następującej treści: faktów potwierdzających prawdziwość tej historii kanał nie posiada. Przed zaprezentowaniem wywiadu powiedziane było: [...] *nie da się zrozumieć, jak takie coś jest możliwe w centrum Europy, a serce w ogóle nie wierzy, że jest to możliwe. Z drugie strony mamy tu opowieść* [...]. Według autorów programu, taki wstęp nie zapowiadał stuprocentowej wiarygodności wypowiedzi Pani Haliny (Чумакова 2014).

W prowadzeniu wojny informacyjnej coraz większą rolę odgrywa Internet, w którym tzw. trolle publikują wpisy, memy, artykuły i komentarze mogące wywołać wrażenie, że poparcie czy przynajmniej zrozumienie dla Moskwy jest wszechobecne. Są w stanie w komentarzach do artykułu, za pomocą jednego wpisu sprowokować masową publikaję innych komentarzy. Właściwie umieszczony i dobrany komentarz może spowodować wywołanie całej fali komentarzy autorstwa osób, które w tej grze się nie orientują, ale nieświadomie biorą w niej udział. Skala tego zjawiska rośnie. W przypadku wojny informacyjnej ważne jest wypracowanie właściwych mechanizmów działania. Opierają się one na rozpoznaniu socjologicznym i psychologicznym. Celem propagandy w sieci jest skierowanie jej do niezadowolonych, sfrustrowanych, zdezorientowanych ludzi, tych których można „przeciągnąć" na swoją stronę. Przestrzeń Internetu, która zdaniem wielu miała być przestrzenią nieograniczonej wolności słowa, niemal realizacją ideału demokracji bezpośredniej, zostaje wykorzystywana jako przestrzeń do manipulacji i prowokacji. Mass media ukraińskie również muszą walczyć, żeby przeciwstawić się wschodniej propagandzie. Przywódcy zdają sobie sprawę, że mogą one mieć duży wpływ na lokalne społeczności i doprowadzić do dalszych eskalacji konfliktu w innych regionach kraju. Ukraina musi bronić swojego państwa nie tylko za pomocą karabinów i armat, ale również walki z dezinformacją. Nie bez powodu Napoleon Bonaparte stwierdził, iż *trzech wrogich gazet należy bardziej się obawiać niż tysiąca żołnierzy z bagnetami* (Kochańczyk 2012).

Prezentowane w ukraińskich mass mediach filmy pokazujące, jak okrutnie zachowują się „separatyści" wywołują dwa rodzaje skutków. Pierwszym jest przedstawienie, w jaki sposób traktowani są na wschodzie jeńcy ukraińscy, gdzie strona rosyjska nie przestrzega norm prawa humanitarnego. Drugim skutkiem, którego Ukraina nie chciała osiągnąć jest przestraszenie potencjalnych ochotników. Prezentowane filmy spowodowały obniżenie społecznych morali. Taki sam negatywny efekt wywarło prezentowanie dużej ilości materiałów przedstawiających zwłoki żołnierzy i cywilów obu stron konfliktu, a także rannych i poszkodowanych w wyniku konfliktu (Pieńkowski 2015).

Prawo międzynarodowe

W związku z prowadzonymi działaniami w ramach wojny informacyjnej trudnio jest udowodnić, że dane państwo jest agresorem. Zgodnie z Kartą Narodów Zjednoczonych w aspekcie wojny informacyjnej państwo, które posługuje się tego typu działaniami nie będzie traktowane jako państwo – agresor. Zgromadzenie Ogólne ONZ przyjęło 14 grudnia 1974 r. na 29 posiedzeniu rezolucję Nr 3314 (XXIX) zawierającą definicję agresji, wzorowaną na Konwencji z 1933 r. wprowadzając pewne uzupełnienia. Określa ona agresję jako użycie siły zbrojnej przez państwo lub grupę państw przeciw suwerenności terytorialnej lub niezawisłości politycznej innego państwa. W rezolucji nie zostały wymienione żadne działania, które traktowałby jako agresję posługiwanie się wojną informacyjną (Ochmann i in. 2016).

Wymienić należy także Traktat Ligi Narodów z 1936 r., a mianowicie Międzynarodową Konwencję dotyczącą Używania Nadawania w Służbie Pokoju, która zobowiązywała państwa do „ograniczenia wszelkich form wypowiedzi, które zagrażałyby pokojowi między narodami i bezpieczeństwu". Sygnatariuszem nadal pozostaje formalnie Federacja Rosyjska. Celem jej jest zapobieganie i powstrzymanie się od nadawania na swoich terytoriach przekazów, które *mają taki charakter, że podburzają ludność jakiegokolwiek terytorium do działań godzących w porządek wewnętrzny lub bezpieczeństwo tego terytorium*. Konwencja zabrania nadawania fałszywych informacji. Jest to użyteczne przypomnienie o potrzebie utrzymywania równowagi między wolnością wypowiedzi a obowiązkiem powstrzymania się od propagandy i nienawiści (Mijatovic 2014).

Ważne znaczenie odgrywa Międzynarodowy Pakt Praw Obywatelskich i Politycznych, a dokładniej jego art. 20, w którym zostało stwierdzone, iż: *wszelka propaganda wojenna powinna być ustawowo zakazana* oraz *popieranie w jakikolwiek sposób nienawiści narodowej, rasowej lub religijnej, stanowiące podżeganie do dyskryminacji, wrogości lub stosowania przemocy, powinno być ustawowo zakazane*. Posługiwanie się w przekazach mową nienawiści powodować będzie, że zostaną złamane przepisy powyższej umowy międzynarodowej. Mass

media działające z ramienia władzy rosyjskiej stosując taką, a nie inną retorykę dokonują naruszania standardów międzynarodowych (Mijatovic 2014). Jak obrazuje to obecny konflikt w Donbasie, propaganda i ograniczenie wolności mediów (rządowe rosyjskie) często idą w parze i stają się motorem konfliktu, który z kolei przyczynia się do dalszej, zintensyfikowanej eskalacji propagandy. W czasach ZSRR na porządku dziennym było stosowanie działań w ramach wojen psychologicznych i wypróbowanych wówczas technik wywierania wpływu i sterowania społecznego. Aktualna władza wykorzystała wcześniej wypracowaną metodologię i rozwinęła ją, tworząc skuteczną „broń". Federacja Rosyjska nie respektuje w tym aspekcie prawa międzynarodowego, a ponadto stale modyfikuje i doskonali techniki przekazu propagandowego, uwzględnia nowe narzędzia medialne, wprowadza innowacje dotyczące działania w sieciach społecznościowych itp.

Podsumowanie

Konflikt w Donbasie i towarzysząca mu wojna informacyjna jest efektem konsekwentnie realizowanej od lat polityki umacniania państwa i odbudowy stref wpływów Federacji Rosyjskiej, a także mobilizacji społeczeństwa. Należy wnioskować, że rosyjskie działania informacyjne będą dalej kontynuowane. Władze dostrzegły skuteczność spójnych działań propagandowych w destabilizacji wybranych regionów kraju. Zatem przemawiać będzie za korzystaniem z tego typu strategii to, że wojna informacyjna może okazać się skuteczniejsza niż konwencjonalna – co społeczności międzynarodowej zaprezentowała Federacja Rosyjska w stosunku do Krymu (Darczewska 2014).

Tym bardziej, że rosyjska propaganda uczy nas, że:

- nie ma ukraińskiego narodu, ale wszyscy Ukraińcy to nacjonaliści,
- nie ma państwa ukraińskiego, ale jednocześnie jego organy są opresyjne,
- nie ma języka ukraińskiego, ale Rosjanie są zmuszani do jego używania.

Wskazuje się również, że Ukraińcy są „bratnim" narodem, a jednocześnie prezentuje się ich jako „faszystów i banderowców", a rosyjskie wojska są na Ukrainie i jednocześnie ich tam nie ma. Sytuacja na Ukrainie pokazuje również, jak niebezpieczne może być niejawne finansowanie mediów i organizacji pozarządowych, nawet tylko tych skupiających się na aktywności na portalach społecznościowych.

Przypisy

[1] Donbas (ukr. Донбас) inaczej Donieckie Zagłębie Węglowe (ukr. Донецький вугільний басейн) jest to obwód przemysłowy, który swoim obszarem obejmuje obwód doniecki (ukr. Донецька область) i ługański (ukr. Луганська область), jak również obwód rostowski (ros. Ростовская область) – znajdujący się na terenie Federacji Rosyjskiej. Donbas leży nad Dońcem, w krainie geograficznej o licznych tradycjach historycznych i kulturowych.

Bibliografia

Aleksandrowicz, T. (2015) *Wojna Informacyjna. Dlaczego Zachód przegrywa z Rosją?*. Dostęp: 07.01.2017 r. Tryb dostępu: https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-wojna-informacyjna-dlaczego-zachod-przegrywa-z-rosja/ .

Darczewska, J. (2014) *Anatomia rosyjskiej wojny informacyjnej Operacja Krymska – studium przypadku*. „Punkt Widzenia", nr 42.

Darczewska, J. (2015) *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?* „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne.

Kochańczyk, J. (2012) *Napoleon*. Będzin: E-bookowo.

Lelonek, A. (2016) *Rosyjska wojna informacyjna na Ukrainie*. Dostęp: 07.01.2017 r. Tryb dostępu: http://www.defence24.pl/361059,rosyjska-wojna-informacyjna-na-ukrainie.

Lipman, M. (2015) *How Russia has come to loathe the West*. Dostęp: 07.01.2017 r. Tryb dostępu: http://www.ecfr.eu/article/commentary_how_russia_has_come_to_loathe_the_west311346.

Месснер, Е. (2004) *Всемирная мятежевойна*. Москва: Кучково поле.

Mijatović, D. (2015) *Propaganda i wolność mediów*. Wiedeń: OBWE.

Ochmann, P., Wojas, J. (2016) *Zagadnienia prawne rosyjskiej interwencji na Krymie*. „Sprawy Międzynarodowe", nr 1.

Oficjalna strona Państwowego Wydawnictwa Naukowego. Dostęp: 07.01.2017 r. Tryb dostępu: http://sjp.pwn.pl/sjp/mass_media;2567152.

Pac, B. (2016) *Wojna informacyjna jako skuteczne narzędzie destabilizacji państw i rządów*. Dostęp: 07.01.2017 r. Tryb dostępu: http://www.defence24.pl/299734,wojna-informacyjna-jako-skuteczne-narzedzie-destabilizacji-panstw-i-rzadow-raport.

Pieńkowski, P. (2015) *Europejskie społeczeństwo ryzyka wobec kryzysu na Ukrainie*. „Władza Sądzenia", nr 5.

Prus, J. (2015) *Rosja między lodówką a telewizorem*. „Sprawy międzynarodowe", nr 1.

Stępniewski, T. (2014) *Cele rosyjskiej inwazji i okupacji na Ukrainie oraz reakcja Zachodu i Europy Środkowej*. „Rocznik Instytutu Europy Środkowo-Wschodniej", nr 5.

Thomas, T. (2015) *Russia's 21st Century Information War: Working To Undermine And Destabilize Populations*. „Defence Strategic Communications", nr 1.

Чумакова, Ю. (2014) *Беженка из Славянска вспоминает, как при ней казнили маленького сына и жену ополченца*. Dostęp: 07.01.2017 r. Tryb dostępu: https://www.1tv.ru/news/2014/07/12/37175bezhenka_iz_slavyanska_vspominaet_kak_pri_ney_kaznili_malenkogo_syna_i_zhenu_opolchentsa.

Официальная страница президента РФ Владимира Путина, Владимир Путин ответил на вопросы журналистов о ситуации на Украине. Dostęp: 07.01.2017 r. Tryb dostępu: http://kremlin.ru/events/president/news/20366.

Официальная страница президента РФ Владимира Путина, Прямая линия с Владимиром Путиным. Dostęp: 07.01.2017 r. Tryb dostępu: http://kremlin.ru/events/president/news/20796.

Streszczenie

Prowadzenie wojny informacyjnej pozwala na podporządkowanie sobie ludzi bez rozlewu krwi. Celem prowadzenia takich działań jest oddziaływanie na emocje, motywy oraz obiektywne rozumowanie danej społeczność. W publikacji odwołano się do problematyki wojny informacyjnej w Donbasie. Autor przedstawia podstawowe definicje pojęcia, prezentuje przykłady posługiwania się działaniami kwalifikowanymi jako wojna informacyjna, a także nawiązuje do prawa międzynarodowego w ww zakresie.

Słowa kluczowe: wojna informacyjna, Donbas, Ukraina, informacja, konflikt, prawo międzynarodowe

Information war in Donbas in terms of international law

Summary

Conduct information warfare allows the subjugation of people without bloodshed. The aim of the measures is to influence the emotions, motives, and objective reasoning of the community. The publication is made analysis of the issues of information war in Donbas. The author presents the basic definitions of the term. In the article are presented as examples of the use of actions qualified as a war information. Made it is also analysis of issues in terms of international law.

Keywords: war, information, international law, Donbas, Ukraine, information war

Konrad Harasim
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Panika moralna narzędziem terrorystów

Wprowadzenie

Architekci zamachów terrorystycznych wykorzystują media, nie tylko do komunikacji w obrębie własnej organizacji, ale też do zwiększenia efektywności operacyjnej, zbierania informacji, rekrutacji, pozyskiwania funduszy czy realizacji programów propagandowych (Nacos 2003, s. 13-19). Media w zamian skupiają uwagę odbiorców – co perspektywicznie przekłada się na zwiększenie zysków. Ta relacja jest nie tylko nie etyczna, ale przede wszystkim zagrażająca bezpieczeństwu tak ontologicznemu, jak i globalnemu. Tak jak akt terrorystyczny musi być nagłośniony (żeby grupa terrorystyczna w pełni wykorzystała jego potencjał), tak media muszą zdawać relacje z takich incydentów, żeby zainteresować odbiorców. Nie przeprowadzając pogłębionej analizy, można stwierdzić, że pomiędzy terroryzmem a mediami istnieje symbioza. W zasadzie nie da się temu zaprzeczyć, nie mniej media (w swojej misyjności) szczególny nacisk powinny położyć na przekazy o charakterze informacyjno-weryfikacyjnym, a nie wartościująco-emotywnym (Laskowska 2004, s. 56-61). W niniejszym artykule, spróbuję syntetycznie przedstawić koncepcje teoretyczne, egzemplifikacje i rekomendacje dotyczące korespondencji pomiędzy polityką mass mediów a polityką grup terrorystycznych.

Panika moralna

Teoria *paniki moralnej* jest narzędziem socjologii dewiacji, która poszukuje źródeł reakcji społecznej na sytuacje naruszające określoną normę i jest silnie powiązana z teorią naznaczania. Stanley Cohen (2002, s. 17-96), który w latach 70. XX w., jako pierwszy szeroko opisał mechanizm paniki moralnej, nie sformułował jednoznacznej definicji tego zjawiska. W literaturze przedmiotu odnaleźć można kilka propozycji. Jedna z nich określa panikę moralną jako *nagłą, wyolbrzymioną i wzmacnianą przez media reakcję społeczną, potępiającą początkowo niewielkie akty dewiacji. Taka nadreakcja mediow, policji, przedstawicieli władzy oraz odbiorców medialnych, zamiast zamierzonej eliminacji niepożądanego zachowania, doprowadza raczej do jego wzmocnienia*. Należy zaznaczyć, że choć zjawisko paniki moralnej jest nieodłącznym elementem konstytuowania się wszelakich struktur społecznych, to największy dynamizm rozwoju zawdzięcza rozwojowi mass mediów (Thompson 1999, s. 11). W ostatnich latach XX wieku, koncepcja ta była narzędziem do określania i definiowania problemów społecznych (Cohen 2002, s. 67-84; Goode, Ben-Yehuda 2010). Obecnie ma dużo szersze zastosowanie, a bywa też narzędziem do propagowania określonych treści

czy ukierunkowania interpretacji zdarzeń (Cohen 2002, s. 19). Wyróżnia on trzy etapy zjawiska: podjęcie przez media sensacyjnie brzmiącego przekazu; spirala (wzmocnienie przekazu) oraz próba wygaszania zjawiska. Podaje on też trzy cechy charakterystyczne dla paniki moralnej: przesada i zniekształcenie, przewidywanie oraz symbolizację (Cohen 2002, s. 26).

Według Goode'a i Ben-Yehudy (Goode, Ben-Yehuda 2010, s. 37-43) charakterystycznymi cechami, które różnicują klasyczny niepokój społeczny od paniki moralnej są:

zwiększony niepokój (*heightened concern*) – związany jest z określonymi grupami oraz ich negatywnym wpływem na trwałość ładu społecznego, jak również na poziom pocucia bezpieczeństwa ontologicznego (Giddens 2002, s. 51-4);

wrogość (*hostility*) – segregacja społeczeństwa na „my" oraz „oni" – „oni" wyróżniają się czymś na tle pozostałych, co odczytywane jest jako zagrożenie porządku;

konsensus (*consensus*) – uznanie danej grupy za zagrażającej społeczeństwu, opiera się na jednomyślności obywateli w tej materii;

nieproporcjonalność (*disproportionality*) – rozumiana jest, jako dysproporcja pomiędzy konkretnymi działaniami a realnym zagrożeniem; nieproporcjonalność powiązana jest z wyolbrzymioną reakcją wobec zastanej sytuacji;

niestabilność (*volatility*) – spadek zainteresowania danym zdarzeniem jest równoznaczny z wygaśnięciem paniki moralnej jaką wzbudziło.

Koncepcja paniki moralnej jest tworem abstrakcyjnym (Berger 1983, s. 145-149), niemniej występuje w niej kilku aktorów społecznych, a interakcje między nimi stanowią rdzeń zjawiska. Należą do nich:

środki masowego przekazu – ich działalność skupia się wokół identyfikacji określonego wydarzenia jako zagrażającego lub nie;

grupy wpływu – ich celem jest wprowadzenie zmiany społecznej (często legislacyjnej) – ukrywają prawdziwe intencje, ale podsycają niepokój społeczny, żeby zrealizować cele polityczne (Goode, Ben-Yehuda 2010);

dysydenci – mają za zadanie wprowadzanie zmian w celu zachowania ładu społecznego; każdy ewentualny sprzeciw wobec ich planów traktowany jest jako zagrożenie dla interesów społeczeństwa – choć wielokrotnie realizują interesy grup wpływu a nie ogółu;

opinia publiczna – determinuje „powodzenie" w aranżowaniu zjawiska paniki moralnej przez mass media i osiągnięcie „sukcesu";

folk devils – *diabeł ludowy* (diabeł w oczach ludu) – to jednostki, którym przypisuje się odpowiedzialność za kreowanie zagrożeń – to społeczni dewianci, uosobienie zła (Berger 1983, s. 145-149).

Polityka strachu

Opierając się na taksonomii Goode'a i Ben-Yehuda (Goode, Ben-Yehuda 2010, s. 68-79) oraz modelu Cohena spróbuję przestawić zależność pomiędzy zamachem terrorystycznym a reakcją mediów na taki incydent. Hoffman (Hoffman 2006, s. 65) twierdzi, że bez „wsparcia" mediów, „rażenie" zamachem terrorystycznym ograniczone jest tylko do bezpośrednich ofiar – a celem terrorystów jest dotarcie do możliwie szerokiej „grupy docelowej", czyli wykorzystanie w pełni potencjału zamachu m.in. w celu wywołania lęku wśród obserwatorów. Podobne stanowisko prezentuje Thomson (Thomson 1999, s. 11) twierdzi, że terroryści są zainteresowani przede wszystkim publicznością, a nie ofiarą – i podkreśla, że reakcja publiczności jest równie ważne jak sam czyn. Terroryści uznają zamach za efektywny, gdy skupia on uwagę mediów. W tym celu, terroryści starannie dobierają miejsca, w których przeprowadzają ataki, tak, aby zapewnić najlepszą „obsługę medialną". W rzeczywistości, cele terrorystów nie są wyłącznie ograniczone do skupienia uwagi mass mediów. Za ich pośrednictwem przedstawiają swoją ideologię – podają przyczyny i oczekiwania polityczne (Nacos 2003, s. 13-19).

Mass media to kolejne **narzędzie w strategii działania grup terrorystycznych** (obok funduszy, ochotników, broni). Narzędzie stosowane w celu zniwelowania asymetrii sił pomiędzy nimi a podmiotem ich oddziaływania. Media – niejako „przy okazji" – propagują ideologię, wzmagają atmosferę strachu – obniżają poczucie bezpieczeństwa i dają okazję do legitymizowania swoich czynów przez grupy terrorystyczne. Jednocześnie poszerza się grono obserwatorów, a tym samym powiększa się społeczność, na którą można oddziaływać. Znakomitą egzemplifikacją wydają się być słowa Ajman'a az-Zawahiri (obecny przywódca al-Kaidy): *w walce, a ponad połowa z tej bitwy odbywa się na polu bitwy mediów – w sercu i umysłach niewiernych* (Seib 2011, s. 64). Postęp technologii informacyjnych, został przez terrorystów w pełni wykorzystany – pozwoliły one na rozpowszechnianie komunikatów terrorystycznych i dotarcie do szerszej publiczności (Baran 2008, s. 24). Internet wyraźnie zwiększył zakres propagandy i działalności terrorystycznej i stał się doskonałym narzędziem dla terrorystów pod względem realizacji celów operacyjnych, niskich kosztów oraz niwielkiego ryzyka identyfikacji nadawcy wiadomości.

Należy zauważyć, że terroryzm jest atrakcyjny dla mediów, głównie dlatego, że ataki terrorystyczne są atrakcyjne dla widza. W zjawisku terroryzmu jest wiele aspektów, które czynią go ważkim tematem dla mediów, ma on w sobie elementy dramatu, niebezpieczeństwa, ludzkiej tragedii, bohaterów, szokującego materiału i działania przeciwterrorystycznego (Baudrillard 2005, s. 24-9).

Nadrzędnym czynnikiem popularyzatorskim terroryzmu jest to, że przemoc zajmuje centralne miejsce we współczesnej kulturze i ma kluczowe znaczenie

w aspekcie semiotycznym i finansowym dla współczesnych organizacji medialnych (Lewis, 2005, s. 32-48). Jedną z przyczyn takiego stanu rzeczy, jest profil kadry zarządzającej mediami – większość to managerowie, a nie dziennikarze. Problem nie leży w tym, dlaczego media zajmują się terroryzmem, ale jak go pozycjonują. Media ograniczają się do relacji z miejsca zdarzania i wypowiedzi eksperta, pomijając kontekst historyczny i nie zwracając uwagi na kontekst traumatyzacyjny. Aspekt traumatyzacyjny wzmaga cykliczna projekcja scen z miejsca zdarzenia – wyolbrzymia to zagrożenie (Lewis 2005, s. 32-48). Tak częsta ekspozycja odbiorców mediów na informacje o zagrożeniu to **narracja oparta na witymizacji** (Altheide 2009, s. 49-56) – narracje te tworzą atmosferę zagrożenia lub bezpośredniego traktowanie siebie jako ofiarę.

Wywołanie niepokojów społecznych czy stanów zagrożenia w związku z doniesieniami o zamachu terrorystycznym oparte jest zarówno na gwałtownym i nieprzewidywalnym jego charakterze jak i intensywności przekazów medialnych. Terroryzm generuje „kulturę strachu" (Fured 2006, s. 51-57), rozpatrywaną nie tylko jako wywołanie strat w konkretnym miejscu, ale też poprzez manifestowanie sposobów kontrolowania czy przeciwdziałania zagrożeniom (Savitch 2014, s. 74-79). Uzbrojeni żołnierze podczas uroczystości lokalnych, zasieki lub wzmożone kontrole w portach lotniczych – czy inne środki i działania podejmowane w celu zwiększenia bezpieczeństwa, to bezpośrednie czynniki wzmagające lęk i strach w społeczeństwie. Media w kooperatywie z dysydentami przedstawiają innowacyjne metody przeciwdziałania terroryzmowi, a jednocześnie podsycają napięcia związane z – bardziej lub mniej prawdopodobnym – zagrożeniem (Savitch 2014, s. 74-79). Wzmożona kontrola coraz to nowych sfer życia jednostki ogranicza jej wolność. Niemniej ludzie godzą się na to w imię zachowania ładu, a postawy takie wyzwalają przypływy patriotyzmu i jedności społecznej.

Nie pozostaje to jednak bez znaczenia dla rozumienia bezpieczeństwa ontologicznego przez Giddensa: *ufność pokładana w egzystencjalnych punktach zaczepienia, w sensie emocjonalnym i w pewnym stopniu poznawczym, opiera się na nabytej we wczesnych doświadczeniach dziecka pewności co do tego, że na innych można polegać* (Giddens 2002, s. 51-4). Ograniczenie zaufania do innych okazuje się być wymogiem, a w zasadzie podstawowym elementem odpowiedzialności wobec siebie i innych.

Doniesienia medialne wywołują intensywną wrogość tak wobec sprawców aktów terrorystycznych, jak i całych nacji, z którymi owych zamachowców identyfikują media. Semantyka wypowiedzi narracyjnej (Żurek 2015, s. 109-13) („terroryzm fanatyczny", „terroryzm nihilistyczny", „ultra terroryzm") buduje fabułę, ukierunkowuje wypowiedź, a przez to przypisuje jej jednoznaczne znaczenie. Taka dynamika dyskursu, wzbudza lęk przed konkretnymi grupami narodowościowymi, etnicznymi czy religijnymi. Arthur Goldberg charakteryzuje terroryzm, jako *wyraźne i aktualne zagrożenie dla cywilizacji samego istnienia*

(Sheldon 2008, s. 607). Terroryzm określony przez Prezydenta Bucha, jako „nowy rodzaj zła" (Hoffman 2006, s. 39), rozumiany jest jako zagrożenie dla moralności. Narracja traktująca terroryzm w aspekcie moralności (odwoływanie się do podstawowych wartości) była też oficjalnym wyjaśnieniem wydarzeń z 9 września 2001 roku. Taka retoryka, to czysta inżynieria paniki moralnej – odwołuje się do praw podstawowych, ma za zadanie jednoczyć obywateli przy jednoczesnym ukierunkowywaniu interpretacji wydarzeń zgodnie z polityką rządzących. Odwraca to uwagę od innych aspektów wydarzeń przy jednoczesnym obniżeniu poziomu poczucia bezpieczeństwa. Niejednokrotnie „diabły ludowe" są wyczarowane wyłącznie poprzez kampanie medialne i polityczne, terroryści aktywnie wzniecają niepewności, a tym samym przeświadczenie o powszechności przemocy.

Niemniej jednak, podczas gdy ugrupowania terrorystyczne starają się wpisać zamachy w życie codzienne, badania sugerują, że reakcje mediów są nieuzasadnione w porównaniu do bardziej szkodliwych problemów (Hoffman 2006, s. 39). Oficjalne reakcje na terroryzm często pociągają za sobą represyjną retorykę i polityki, które prowokują irracjonalny lęk. Kategoryczne reakcje dysydentów nie zawsze swoje źródło biorą z prawdziwej troski o bezpieczeństwo społeczeństwa – częstokroć są podyktowane priorytetami politycznymi czy zawartymi sojuszami. Retoryka taka pozwala na usankcjonowanie celów politycznych, wzmocnienie legitymizacji działań (czy zaprzestania działania) np. interwencje wojskowe, represje polityczne, wzmożenie nadzoru (Walsh 2015, s. 212).

Panika moralna wywołana przez ataki terrorystyczne inspiruje instytucje poszczególnych państw i agendy międzynarodowe do eskalacji społecznej dyscypliny i kontroli, a nie rzadko represji ze strony służb mundurowych. Uchylenie, zawieszenie czy obejście praw człowieka to najczęstsze techniki wykorzystywane do obrony społeczeństwa (Cohen 2002, s. 67-84). Odwołania do społecznej sprawiedliwości czy globalnego konfliktu (bez wyraźnego zidentyfikowania przeciwnika) dostarcza niejako alibi dla użycia wszelkich sposobów zaprowadzenia porządku (Walsh 2015, s. 212). Reżyserowany przez polityków, a komentowany (nie recenzowany) spektakl „walki z globalnym terroryzmem" wzmacnia kulturę strachu i tym samym obniża poziom bezpieczeństwa (Jarecka 2012, s. 181).

Takie tendencje są wyjątkowo jaskrawe w przypadku współczesnego klimatu islamofobii. W szczególności, interpretacja terroryzmu poprzez rejestry różnicy rasowej i religijnej prowadzi do identyfikowania całych zbiorowości jako „ludowych diabłów". W połączeniu z globalnym wzrostem masowego przekazu w 24-godzinnym cyklu wiadomości, doniesienia o aktach terroru cyklicznie wzmagają stan niepokoju i niepewność (Garland 2008, s. 14). Długotrwałe poczucie bezbronności z jednej strony generuje autoizolację jednostki, a z drugiej może wzniecać – na drodze paniki moralnej – ustawiczny lęk.

Wykorzystywanie paniki moralnej przez ugrupowania terrorystyczne, może przyjmować różne oblicza, od afektywnej przemocy przez prowokację do wzmocnienia (poszerzenia) rażenia. Zarządzanie przekazem medialnym jest gałęzią terroryzmu, który propaguje swoje idee, maksymalizuje grono odbiorców czy zachęca do współpracy. Terroryści w wyrafinowany sposób korzystają z mass mediów – mając na uwadze, że media *to nie są lustra, które odbijają obiektywnie „rzeczywistości", ale odbijają obraz o wiele ostrzej niż rzeczywistość* (Cohen 2002, s. 43).

Spektakularność ataków terrorystycznych jest atrakcyjna dla mediów, ponieważ w epoce szumu informacyjnego istnieje wzmożone „zapotrzebowanie" na panikę moralną. Terroryści wykorzystali to zapotrzebowanie – według podręcznika szkoleniowego Al-Ka'idy: *cele dobierać należy tak, aby pozyskać intensywną reklamę i wzbudzić wszechobecny strach* (Nacos 2003, s. 16). Ataki terrorystyczne (zazwyczaj) swym zakresem ograniczają się do wąskiej grupy ofiar a za sprawą przekazów medialnych, ich skala wydaje się nieporównywalnie większa, a zasięg powszechny (Lewis 2005, s. 32-48).

Uwagi końcowe

W literaturze przedmiotu, związek mediów z terroryzmem jest szeroko opisywany. W aspekcie paniki moralnej znajdujemy też wiele opracowań – skupiają się one jednak na wykazywaniu związków terroryzmu z wzniecaniem lęków. Postawiłem sobie za cel zaprezentowanie możliwych technik niwelowania czy ograniczania destrukcyjnego wpływu mediów na poczucie bezpieczeństwa. Wieloaspektowość organizacji i funkcjonowania – tak mediów jak i organizacji terrorystycznych – nie ułatwiają zadania. Niemniej, wspierając się propozycjami ekspertów (Adamski 2007; Nacos 2002) zestawiłem katalog wytycznych, dzięki którym zminimalizować można negatywne skutki przekazu medialnego na temat aktów terroru. Należy do nich:

obiektywizm – powinien być kluczem podczas raportowania historii, wtedy odbiorca może wyrobić sobie własne zdanie na temat wiadomości;

przejrzystość – jednym z narzędzi terrorystów jest zarządzanie informacją poprzez szerzenie dezinformacji; dlatego też media powinny dostarczać najbardziej rzeczowe i najbardziej wyważone informacje, tak, aby zapobiec błędnej interpretacji zdarzeń związanych z terroryzmem;

zróżnicowanie – media powinny odróżniać rodzaje terroryzmu i grup terrorystycznych, aby nie kierować negatywnych uczuć opinii publicznej przeciwko mniejszościom etnicznym czy religijnych;

selektywne stosowanie propagandy – stosowanie narzędzi multimedialnych przeciwko terrorystom, zwłaszcza w wojnie narracyjnej z radykalnym ekstremizmem, jest na ogół bezowocne, biorąc pod uwagę, że media mają szereg ograniczeń, natomiast terroryści nie;

desekurytyzacja – nie ma wątpliwości, że o aktach terrorystycznych społeczeństwo musi być informowane, ale narracja ma tu kluczowe znaczenie; desekurytyzacja polega na przedstawieniu wydarzeń w sposób stonowany i mniej „sensacyjny"; taka retoryka uniemożliwi terrorystom traktowanie mediów jako narzędzia promocyjnego i rekrutacyjnego, przez co zapobiegnie eskalacji strachu na poziomie publicznym.

Nadrzędną powinności rządzących, ale także przedstawicieli tzw. czwartej władzy powinno być skupianie się wokół dążenia do zachowania lub przywracania ładu społecznego. Ataki terrorystyczne zmieniają profil współczesnych społeczeństw – z otwartych na zamknięte. Społeczeństwo przestaje się rozwijać i dążyć do postępu, ponieważ skupia się na otaczających go *quasi* zagrożeniach.

Bibliografia

Adamski, J. (2007) *Nowe technologie w służbie terrorystów.* Warszawa: Wydawnictwo Trio.

Altheide, L. (2009) *Terror Post 9/11 and the Media.* New York: Peter Lang.

Baran, J. (2008) *Terrorism and the Mass Media after Al Qaeda: A Change of Course?* „The Peace and Conflict Review", March, pp. 21-46.

Baudrillard, J. (2005) *Duch terroryzmu. Requiem dla Twin Towers.* Warszawa: Sic!.

Berger, P. Luckmann, T. (1983) *Społeczne tworzenie rzeczywistości.* Warszawa: PIW.

Cohen, S. (2002) *Folk Devils and Moral Panics.* London: Routledge.

Fured, F. (2006) *Furedi F (2006) Culture of Fear Revisitedy.* London: B9loomsbur.

Garland, D. (2008) *On the concept of moral panic*. „Crime, Media, Culture", No 4(1), April, pp. 9-30.

Giddens, A. (2002) *Nowoczesność i tożsamość. „Ja" i społeczeństwo.* Warszawa: PWN.

Goode, E., Ben-Yehuda, N. (2010) *Moral Panics: The Social Construction of Deviance.* Worldcat: Oxford.

Hoffman, B. (2006) *Inside Terrorism.* New York: Columbia University Press: Columbia University Press.

Jarecka, U. (2012) *Retoryka wizualności. Pokazać katastrofę.* W: Wasilewski, J., Nita, A. (red.) *Instrukcja obsługi tekstów. Metody retoryki.* Sopot: Gdańskie Wydawnictwo Psychologiczne, s. 177-196.

Jary, D., Jary, J. (1999) *Dictionary of Sociology.* Glasgow: HarperCollins.

Laskowska, E. (2004) *Dyskurs parlamentarny w ujęciu komunikacyjnym.* Bydgoszcz: Wydawn. Akademii Bydgoskiej im. Kazimierza Wielkiego.

Lewis, J. (2005) *Language Wars: The Role of Media and Culture in Global Terror and Political Violence.* London: Pluto Press.

Nacos, B. (2003) *The terrorist calculus behind*. „Studies in Conflict and Terrorism", No 26(1), January, pp. 9-36.

Savitch, H. (2014) *Cities in a Time of Terror.* London: Routledge.

Seib, P., Janbek, D. (2011) *Global Terrorism and New Media: The Post-Al Qaeda Generation.* New York: Routledge.

Sheldon, U. (2008) *Panika moralna vs. Społeczeństwo ryzyka: konsekwencje zmian w sferze niepokojów społecznych*. W: Sztompka, P., Bogunia-Borowska, M. (red.), *Socjologia codzienności.* Kraków: Znak. s. 507-734.

Thompson, K. (1999) *Moral Panics.* London, New York: Routledge.

Walsh, J. (2015) *Border theatre and security spectacles: Surveillance, mobility, and reality-based television*. "Crime, Media, Culture", No 11(2), p. 201-221.

Żurek Ł. (2015) *Postrukturalizm i teoria Stefana Szymutki*. W: Błaszkowska, M., Kuster, M., Pisarek, I. (red.), *Literatura – kultura – lektura. Dzisiejsze spojrzenie na teorie i praktyki badań literackich i kulturowych.* Kraków: Uniwersytet Jagielloński.

Streszczenie

Celem artykułu jest przestawienie zależności pomiędzy przekazem medialnym a terroryzmem. Współczesne ugrupowania terrorystyczne wpisują przekaz medialny w strategię swojego działania (obok pozyskiwania funduszy, organizacji zamachów czy prowadzenia rekrutacji). Mass media przekazując informacje związane z aktami terroru, wzniecają w społeczeństwach tzw. *panikę moralną,* czyli wyolbrzymioną społeczną reakcję na prezentowane treści. Retoryka i etykietowanie stosowane przez media wpływają degradująco na odczuwany poziom bezpieczeństwa społeczeństw, a tym samym stają się narzędziem współczesnego terroryzmu. Skala rażenia atakiem terrorystycznym poszerza się poza grono bezpośrednich ofiar.

Słowa kluczowe: panika moralna, terroryzm, polityka strachu

Moral panic as a tool of terrorism

Abstract

The purpose of the article is to show the relationship between media coverage and terrorism. Modern terrorist groups use the strategy of media coverage in its activities (in addition to fundraising, organization of terrorist attacks or recruiting). Mass media providing information related to acts of terror raise in societies so called “moral panic”, exaggerated reaction to the presented content. Rhetoric and labeling used by media have a degrading effect on the perceived level of safety in population and thus become a tool of modern terrorism. The scale of destruction arise from terrorist attack extends beyond the circle of direct victims.

Keywords: moral panic, terrorism, politics of fear

Wojciech Cendrowski
Uniwersytet Pedagogiczny w Krakowie

Cyberwojna i jej znaczenie dla bezpieczeństwa NATO w kontekście przypadków i dokumentów strategicznych

Wstęp

Wydarzenia z początku XXI wieku pokazały, że zagrożenie dla bezpieczeństwa narodowego związane z jego funkcjonowaniem w cyberprzestrzeni jest realne – przykładem był atak DDoS (*Distributed Denial of Service*) na Estonię w 2007 roku – państwo, które jest członkiem NATO nie potrafiło sobie poradzić z nim i musiało odłączyć punkty przesyłowe łączące kraj z resztą świata. Miało to ustabilizować sytuację oraz zneutralizować zagrożenie, ale w konsekwencji gospodarka kraju została sparaliżowana ze względu na uniemożliwienie wykonywania elektronicznych transakcji bankowych, cała administracja państwowa (z racji specyfiki jej prowadzenia przy użyciu Internetu) przestała funkcjonować, istniało rzeczywiste wysokie ryzyko wycieku danych poufnych klientów i ich środków z krajowych banków.

To był wstrząs dla całej areny międzynarodowej, w reakcji bardzo szybko zaczęły powstawać nowe strategie w sojuszach i organizacjach międzynarodowych dotyczące cyberprzestrzeni oraz ośrodki, których celem byłoby zapobieganie i zwalczanie tego typu ataków w przyszłości.

W artykule podjęto próbę przedstawienia aktualnego stosunku NATO do zagrożenia cyberwojen, poprzedzonego terminologicznymi rozważaniami na temat tego zjawiska oraz ustosunowano się do kwestii przygotowania Sojuszu Północnoatlantyckiego do obrony przed atakiem cyberwojny.

Terminologia i problemy teoretyczne – cyberprzestrzeń, cyberwojna, cyberatak, cyberkonflikt i jego rodzaje

Prowadząc rozważania nad cyberwojną należy wyjść od określenia jej pola walki. Istnieje wiele definicji cyberprzestrzeni, jednakże warto pozostać przy użytkowej definicji, używanej w prawie polskim, dokładnie w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, art. 2. ust. 1b. Przez *cyberprzestrzeń* […] *rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. Nr 64, poz. 565, z późn. zm.) *wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*.

Natomiast definicja z *Tallin Manual on the International Law Applicable to CyberWarfare* nie uwzględnia czynnika ludzkiego. Według tego dokumentu cyberprzestrzeń to *środowisko tworzone przez składniki fizyczne i niefizyczne charakteryzujące się wykorzystaniem komputerów i widma elektromagnetycznego do przechowywania, modyfikowania i wymiany danych z wykorzystaniem sieci komputerowych* (Schmitt 2013).

Warto przypomnieć, że większość państw ma swoje własne doktryny i strategie dotyczące bezpieczeństwa w cyberprzestrzeni, co implikuje wiele rozbieżności pod kątem nazewnictwa i kryteriów znamion, które miałyby charakteryzować konkretne zjawiska. Ciągły rozwój technologiczny tylko pogłębia przepaść w postrzeganiu tych zjawisk.

Jedną z podstawowych definicji ujęcia zjawiska cyberwojny jest definicja Krzysztofa Liedela i Pauliny Piaseckiej zamieszczona w publikacji *Wojna cybernetyczna – wyzwanie XXI w.,* którą sformułowano następująco – to *zorganizowana w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika, lub przepływających przez nie informacji oraz ochronę własnych systemów informacyjnych przed podobnym działaniem przeciwnika* (Lidel, Piasecka 2011, s. 23).

Wspomniani autorzy oparli swoją definicję na publikacji RAND Corporation, w której wyodrębniono dwa rodzaje cyberwojny – „cyberwar" określaną przez nich jako *sposób prowadzenia operacji wojskowych zgodnie z zasadami związanymi z informacją jako zasobem strategicznym. Jego głównym celem jest zakłócenie funkcjonowania lub zniszczenie systemów komunikacyjnych i informacyjnych przeciwnika oraz osiągnięcie przewagi poprzez zgromadzenie maksymalnej wiedzy na temat przeciwnika przy jednoczesnym zapobieganiu uzyskania przez przeciwnika informacji na temat własnych stron – słabych i mocnych* (Tamże, s. 23). Warto tutaj zwrócić uwagę na nacisk przy zachowaniu anonimowości przez agresora w stosunku do ofiary.

Na zjawisko cyberwojny można także popatrzeć poprzez pryzmat definicji wojny konwencjonalnej. Odwołując się do najsłynniejszego teoretyka wojennego – Carla von Clausewitza i jego *opus magnum O wojnie,* możemy zauważyć wiele zbieżności z powyższymi definicjami jak np.: celem ma być zniwelowanie oporu przeciwnika, doprowadzenie do jego bezbronności, spowodowanie jak największych zniszczeń, czy realizacja celów politycznych (Clausevitz 2010, s. 19). Jednakże, formowanie definicji cyberwojny poprzez wspomniany pryzmat tez Clausevitza jest dosyć ryzykowne.

Jedną z głównych tez Clausewitza jest założenie, że stronami wojny muszą być państwa, i Liedel wraz z Piasecką definiując cyberwojnę, analogicznie wychodzą z tej samej tezy – uznają, że w momencie, w którym państwo definiuje

atak na swoje struktury informatyczne jako cyberwojnę, miałoby dopiero czynić ten akt cyberwojną. Problem w tym, że w definicji cyberwojny RAND Corporation, jest położony wyraźny nacisk na ukrywanie tożsamości atakującego. Omówione w dalszej części artykułu *case studies*, wykazują, że wykrycie atakującego (a nawet metody jakiej użył do ataku) jest bardzo często technicznie niemożliwe, natomiast bezpośrednie wypowiedzenie cyberwojny znacznie zatraca sens jej użycia, jak i skuteczność. Liedel i Piasecka także ograniczyli działania ofensywne podczas cyberwojny do trzech funkcji: 1) oślepianie przeciwników; 2) inflitracja systemów komputerowych; 3) przeciążanie systemów (Liedel, Piasecka 2011, s. 10).

W tym kontekście należy ponownie odwołać się do raportu RAND Corporation z 1993 roku (Arquilla, Ronfeldt 1993). Obecnie, 13 lat później, kiedy technologia znacznie się rozwinęła i miało miejsce kilka wydarzeń określanych przez naukowców cyberwojnami (Shakarian 2013, s. 2) warto podchodzić do tego typu tez z większym dystansem.

Temat ten rozwija jeden ze współautorów wspomnianego raportu RAND Corporation (chodzi o *cyberwar is coming*) z 1993, Paul K. Davis, który w 2014 roku wydał artykuł pt.: *Deterrence, Influence, Cyberattack, and cyberwar.* W tej publikacji cyberwojna jest już definiowana jako akcja aktora państwowego lub bezpaństwowego mająca na celu spenetrowanie komputerów lub sieci danego państwa, by spowodować znaczące zniszczenia lub wprowadzić zamęt, chaos (Davies 2014, s. 328). Davies jednakże zaznacza, że w tej definicji nie zawiera się robienie żartów, działania wywiadowcze, przestępczość czy przygotowywanie do ataku w kontekście *sensu stricto* militarnym, ale zaznacza, że cyberwojna jak najbardziej może być częścią większego konfliktu (Tamże).

W 2013 roku została wydana książka *Introduction to Cyber-Warfare* pod redakcją Paulo Shakariana. Do dziś jest jedną z ważniejszych pozycji światowych dotyczących cyberwojen. Shakarian polemizuje z faktem, czy stronami cyberwojny muszą koniecznie być państwa, przywołując przykłady ataków ze strony Hamasu, Anonymous, Lulzsec, etc. Z drugiej strony nie można uznać wskazuje on, że istniały przypadki, gdzie operacje cybernetyczne prowadziła garstka osób (Shakarian 2013, s. 2). Z drugiej strony nie można powiedzieć, by np. nieletni, którzy rozsyłają spam na większą skalę, toczyli własną cyberwojnę.

Ostatecznie, mając świadomość, że dyskusja na temat definicji cyberwojny jest cały czas otwarta, przyjmuję definicję Shakariana, w której *cyberwojna jest przedłużeniem polityki poprzez działania podejmowane w cyberprzestrzeni przez państwowe lub niepaństwowe podmioty, które albo stanowią poważne zagrożenie dla bezpieczeństwa narodowego lub są prowadzone w odpowiedzi na postrzegane zagrożenie przeciwko bezpieczeństwu narodowemu* (Tamże). Biorąc pod uwagę analizę przypadków można śmiało powiedzieć, że powyższa definicja prawdopodobnie najbardziej, w chwili obecnej, wyczerpuje opis zjawiska cyberwojny.

Podsumowaniem dla wywodu o terminologii cyberwojen, powinno być odwołanie się do definicji aprobowanej przez Sojusz Północnoatlantycki – bowiem właśnie ta definicja będzie precyzować konkretne znamiona jakie dany cyberkonflikt musi wyczerpywać, by zostać uznany za cyberwojnę i co powoduje podjęcie konkretnych działań. Jednakże postrzeganie tego zjawiska przez NATO nie jest proste, by można go było sprowadzić tylko do kilkuzdaniowej definicji, wyrwanej z kontekstu działalności CCDCOE (*Cooperative Cyber Defence Centre of Excellence*) oraz wydanych przez tę instytucję dokumentów prawno-naukowych.

Najbardziej klarowne podejście do zagadnienia cyberwojen przedstawia reguła 22 z *Tallin Manual on the International Law Applicable to CyberWarfare*, która odwołuje się bezpośrednio do art. 2 z konwencji Genewskiej z 1949 roku. W dosłownym przekładzie z języka angielskiego brzmi: *Międzynarodowy konflikt zbrojny istnieje w każdej sytuacji działań wojennych, które mogą obejmować lub ograniczać się do działań cyberoperacyjnych pomiędzy dwoma państwami lub ich większą liczbą* (Schmitt 2013, s. 79).

Obecnie w NATO istnieje trend, który zakłada odejście od interpretowania cyberwojny przez pryzmat teorii Clausevitza (*Atak w wirtualu* 2016).

W środowisku naukowym istnieje także przeciwny nurt zakładający, że cyberwojny nie ma, nie było i nie będzie (Rid 2011, s. 5-32) opisany w publikacji o tytule *Cyber War Will not take place*. Jego autor nawiązuje do definicji Clausevitza i w swoich analizach stawia hipotezę, że wszystkie dotychczasowe incydenty określane przez np. Skakariana jako akty cyberwojny, można zakwalifikować najwyżej do trzech przejawów aktywności, takich jak wywrotowość, szpiegostwo i sabotaż. Nie można odmówić logiki w tym wywodzie, mocno i głęboko opartej na tezach Clausevitza. Rid wskazuje konkretnie trzy kryteria, które Clausevitz określał jako indykatory aktu wojny: 1. musi być śmiertelny, śmiercionośny – chodzi tu o *sensu largo* charakter przemocy – jako sposobu zmuszenia wroga do wykonania naszej woli; 2. jest instrumentalny – pojmowanie wojny jako procesu – przemoc jest elementem środkowym, ugięcie się przeciwnika pod wolą zwycięzcy jest ostatnim etapem; wojna jako taka jest tylko tym środkowym elementem; 3. ma cechy polityczne – wojna nie jest jednorazowym podjęciem decyzji, a całym szeregiem, który jest motywowany dojściem do realizacji swoich większych celów politycznych (Tamże s. 6).

Rid mocno akcentuje występującą w teoriach Clausvitza potrzebę „fizycznego" ataku, by można było w ogóle kontynuować rozważania, czy dany cyberatak może być uważany za cyberwojnę. Akt cyberwojny określa jako coś bardziej pośredniego, jako działanie, w wyniku którego dopiero na końcu mogą wystąpić straty fizyczne w sprzęcie i ludziach. Dalej Rid w swoim artykule toczy mniej lub bardziej racjonalny wywód, w którym stara się obronić postawioną tezę, że wszystkie dotychczasowe incydenty spełniały najwyżej jeden z trzech obowiązkowych cech wojny (Tamże).

Rid bardzo ogólnie podchodzi do problemu prawa międzynarodowego, ponieważ definiowanie cyberwojny jako 'siły' rozumianej w kontekście dokumentów międzynarodowych, a zwłaszcza Karty Narodów Zjednoczonych, jest kluczowe dla jej definiowania. Rid przywołuje w swoich rozważaniach stanowisko Matthwa C. Waxmana, zawarte w jego artykule *Cyber-Attack and the Use of Forcje: Back to the Fufuter of Article 2(4)*. Waxman dokładnie rozpatrzył kontekst definicji siły w odniesieniu do art. 2 pkt. 4 Karty Narodów Zjednoczonych. Przepis ten stanowi, że *wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od groźby użycia siły lub użycia jej przeciwko integralności terytorialnej lub niezawisłości politycznej któregokolwiek państwa, bądź w jakikolwiek inny sposób niezgodny z celami Organizacji Narodów Zjednoczonych.* Zgodnie z art. 51 Karty *żadne postanowienie niniejszej Karty nie narusza naturalnego prawa każdego członka Organizacji Narodów Zjednoczonych, przeciwko któremu dokonano zbrojnej napaści, do indywidualnej lub zbiorowej samoobrony.* Chociaż zakres prawa do samoobrony przy zastosowaniu sił zbrojnych wciąż wzbudza wiele kontrowersji, powszechnie uznaje się, że postanowienia art. 51 ustanawiają wyjątek od art. 2 pkt. 4 dotyczącego surowego zakazu użycia siły w innym przypadku (Franck 2002, s. 45-52), a nadto powszechnie uważa się, że „atak zbrojny" jest, mimo iż ściśle powiązany, węższą kategorią „groźby użycia siły" lub jej „użycia". W odniesieniu do ofensywnych możliwości cybernetycznych i Karty Narodów Zjednoczonych, wspomniane przepisy poruszają dwie istotne kwestie. Po pierwsze, w odniesieniu do art. 2 pkt. 4, można zadać pytanie, czy niektóre rodzaje cyberataków można uznać za zabronione „użycie siły"? Pytanie to porusza zagadnienie, czy obecne regulacje prawne nakładają wyraźne ograniczenia w zakresie wrogich działań cybernetycznych. Druga kwestia, dotycząca wykładni art. 51, dotyczy pytania, czy w odpowiedzi na ataki cybernetyczne powstaje prawo do użycia sił zbrojnych? Pytanie to porusza aspekt dostępnego wachlarza środków zaradczych dla państw, które ucierpiały z powodu gróźb cyberataków lub ich rzeczywistego przeprowadzenia (Waxman 2011, s. 421-459).

Uczestnicy cyberwojen i ich prawa

Ogólnie są określani jako „hakerzy" lub „cyberżołnierze". *Tallin Manual on the International Law Applicable to CyberWarfare* określa, że jest uzasadnione (choć opinie w samym dokumencie są podzielone) stosowanie wobec cyberżołnierzy broni konwencjonalnej i ich fizyczna eliminacja (stosowanie tego samego prawa humanitarnego jak wobec żołnierzy walczących na froncie). Jest to dosyć kontrowersyjne zalecenie, bo pod te same reguły tallińska instrukcja podciąga także aktywistów (Schmitt 2013, s. 169). Aspekt stosowania art. 4 Konwencji Haskiej jest bardzo szeroki i odnosi się w głównej mierze do tworzenia korpusów żołnierzy i rekrutacji. Ale według ekspertów, którzy opracowali *Tallin*

Manual on the International Law Applicable z pewnością nie zawierałyby się w niej osoby nieświadomie uczestniczące w strukturach botnetów atakujących na zasadzie DDoS (Tamże s. 120). Teoretycznie, państwo neutralne, na mocy art. 5 Konwencji Haskiej, na którego terenie by się znajdowały jednostki atakujące, miałoby obowiązek je wyeliminować. Z drugiej strony w takiej sytuacji, państwo neutralne nie ma obowiązku zapobiegania procesowi dołączania „wolontariuszy", „ochotników", do atakujących (w pewnym sensie niedobrowolni uczestnicy botnetów są traktowani jak jeńcy), co dokładnie precyzuje art. 6 wspomnianej konwencji – *Państwo może używać jako pracowników jeńców wojennych, za wyjątkiem oficerów, odpowiednio do ich rangi i zdolności. Prace te nie powinny być nadmierne i nie będą w żadnym związku z działaniami wojennymi.* Choć w przypadku, gdy mówimy o „ochotnikach", grupach hakerów w cyberwojnie, nie mają zastosowania zasady prawa międzynarodowego (Roscini 2014, s. 45). Ale to samo prawo jasno określa chronione kategorie osób i dóbr w trakcie wojny, a atak na nie, stanowi zbrodnię wojenną i jest ścigane przez odpowiednie instytucje międzynarodowe, w tym między innymi Międzynarodowy Trybunał Karny (Tamże).

Przykad ataku na Estonię w 2007 r.

Przy analizie tak skomplikowanego zjawiska jakim jest cyberwojna konieczne jest odwołanie się do wydarzeń, które przez badaczy oraz w świetle wspomnianej już kilkakrotnie *Tallin Manual on the International Law Applicable to CyberWarfare*, miały cechy cyberwojen lub są określane cyberwojnami. Incydentów tego typu było dużo, w tym dokumencie jest opisany najbardziej znany przypadek – Atak na Estonię. Warto także zapoznać się z innymi wydarzeniami określanymi jako cyberwojny, jak operacja Orchard w 2007 roku, ataki podczas wojny w Gruzji w 2008, przypadek wirusa Stuxnet oraz działania podczas konfliktu na Ukrainie w 2008 roku.

W sierpniu 1944 Estonia została zajęta przez wojska radzieckie i włączona w skład ZSRR, gdzie pozostała aż do 20 sierpnia 1991 roku. Estończycy określają ten okres jako pięćdziesięcioletnią okupację ich kraju. Wtedy też skolonizowano kraj ludnością rosyjską (*Rozrachunek z dzieciństwa*… 2016). To w konsekwencji doprowadziło do dosyć kuriozalnej sytuacji po odzyskaniu niepodległości: Litwa, Łotwa i Estonia podjęły wspólną decyzję o nieprzyznaniu obywatelstwa osiedleńcom rosyjskim oraz ich potomstwu urodzonemu na terenie swoich państw. Nagle okazało się, że ok. ¼ mieszkańców Estonii to tzw. „bezpaństwowcy" (Fjuk 1997, s. 7). Jednakże warto zaznaczyć, że status bezpaństwowca w Estonii jest dosyć symboliczny, bowiem taka osoba ma niemalże pełen zakres praw publicznych z wyjątkiem biernego prawa wyborczego (*Rozrachunek z dzieciństwa*… 2016). Całokształt tej sytuacji do dziś implikuje

tendencje wśród ludności etnicznej do obrony swojej kultury i tożsamości narodowej.

Dzień 27 kwietnia 2007 roku był punktem kulminacyjnym. Chęć relokacji z centrum Tallina monumentu upamiętniającego żołnierzy Armii Czerwonej doprowadziła do walk ulicznych i protestów, które trwały do 29 kwietnia. Następnie walka przeniosła się w cyberprzestrzeń.

Estonia pod względem ekonomicznym i technologicznym jest krajem, który wykorzystał doskonale szansę jaką stanowił upadek ZSRR. Mimo wyniszczającej eksploatacji przez Sowietów oraz dzięki wielu mądrym posunięciom i zdecydowanemu działaniu polityków, Estonii udało się wyjść z grupy krajów rozwijających się i przejść do grupy krajów rozwiniętych. Przyczyniło się do tego między innymi postawienie na rozwiązania teleinformatyczne – Estonia bardzo szybko stała się liderem jeśli chodzi o e-administrację – zwłaszcza w kontekście systemu podatkowego, prowadzenia działalności gospodarczej, bankowości elektronicznej, oraz nauki i edukacji (*Liderzy czy*… 2015).

Kraj ten zaatakowano na zasadzie ataku DDoS, ale można było wyróżnić kilka rodzajów konkretnych działań, np.: zalew informacji dużymi ilościami pakietów danych, tzw. *Web site defecement* oraz przesyłanie spamu (Shakarian 2013, s. 16). Powyższa metoda była zastosowana na ogromną skalę i przerosła możliwości mocy systemu telekomunikacyjnego. Pierwszym celem były strony rządowe oraz adresy e-mail ważniejszych państwowych urzędów i oficjeli, co spowodowało wyłączenie rządowych serwerów na 12 godzin (Tamże, s. 17).

Rząd estoński z początku nie miał możliwości podjęcia żadnych przeciwdziałań. Atakujący cyberzłożołnierze mogli być wszędzie, nie było możliwości fizycznej identyfikacji sprawców (Tamże, s. 18). Od strony informatycznej, też nie było możliwości rozwiązania problemu. Wprawdzie dostawcy usług internetowych (z ang. ISP) oferują usługę ochrony przeciw DDoS, ale jej działanie nie zawsze jest skuteczne. Największym problemem była kwestia rozproszonego ataku – gdyby prośby o wysłanie pakietu pochodziły z jednego lub kilka hostów, można ręcznie zablokować adres IP nadawcy. Trzeba też wziąć pod uwagę, że część zapytań pochodziła prawdopodobnie ze sfałszowanych numerów IP. Zespół estońskiego CERT-u (*Computer Emergency Response Team*) podszedł do sprawy bardzo poważnie i natychmiast skontaktował się z CERT-ami z Niemiec, Finlandii i Słowacji. Współpraca pozwoliła określić źródło ataku jako zagraniczne. W celu ratowania dostępu do danych zastrzeżonych podmiotów handlowych, banków etc. podjęto decyzję o odcięciu całego ruchu z sieci spoza Estonii, co ostatecznie rozwiązało problem. Kilka lat później ustalono, że za atakiem stała młodzieżówka rosyjskiej parii *Jedna Rosja* (Tamże, s. 18-20).

Aktualne podejście do cyberwojny w raportach i dokumentach sojuszu NATO

Na szczycie w Walii we wrześniu 2014 roku, członkowie państw NATO zatwierdzili nowy plan działań, który skierował politykę tej organizacji na zupełnie nowe tory oraz uznali za priorytet rozwój współpracy z sektorem prywatnym w zakresie analizy nowych cyberzagrożeń. W związku z tym powstał specjalny program *The NATO Industry CyberPartnership* (NICP), który został zaprezentowany podczas dwudniowej konferencji w Mons w Belgii, w której wzięło ok. 1500 przedstawicieli ze świata informatyki (*NATO opens*… 2016). Można powiedzieć, że ta współpraca okazała się jednym z największych sukcesów NATO przy tworzeniu obrony na wypadek zaistnienia cyberwojny.

Obecnie, głównym sposobem przeciwdziałania zagrożeniom teleinformatycznym jest ogólnie pojęta obrona oraz wzajemne wspieranie się – aczkolwiek, każde państwo jest indywidualnie odpowiedzialne za ochronę swojej strukturach (*Atak w wirtualu* 2016). Dla realizacji tych celów NATO w swoich strukturach powołało kilka instytucji na kilku poziomach. Poziom ekspercki reprezentuje *The Cyber Defence Committee*, który jest jednostką podporządkowaną Radzie Północnoatlantyckiej i ma na celu konsolidację polityki i cyberobrony; realizuje je poprzez nadzór i doradztwo dla krajów członkowskich. Poziom wykonawczy reprezentuje *CyberDefence Management Board* (CDMB) – które jest odpowiedzialne za koordynację całej cyberobrony, zwłaszcza w aspekcie współpracy pomiędzy instytucjami cywilnymi i militarnymi; CDMB składa się głównie z liderów politycznych, wojskowych oraz jednostek operacyjnych i technicznych. Poziom doradczy reprezentuje *The NATO Consultation, Control and Command* (NC3) – jest to jednostka pełniąca funkcję konsultacyjne dotyczące aspektów technicznych i implementacji obrony przed cyberatakami. Na kolejnych poziomach reprezentują: *The NATO Military Authorities* (NMA) oraz *NATO Communications and Information Agency* (NCIA) ponoszące odpowiedzialność za identyfikację konkretnych wymagań operacyjnych, a ponadto nabywanie, wdrażanie i eksploatację zdolności cyberobronnych NATO; NCIA ponadto świadczy usługi techniczne. Następnie *Allied Dowództwo Transformacji* (ACT), które jest odpowiedzialne za planowanie i prowadzenie corocznych ćwiczeń cyberkoalicji; *The NATO Computer Incident Response Capability* (NCIRC), które chroni sieci NATO poprzez zapewnienie ciągłej i scentralizowanej pomocy dla technicznej dla wszelkich miejsc działania NATO; odgrywa kluczową rolę w reagowaniu na dowolne cyberataki wobec państw Sojuszu; zajmuje się incydentami, ich zgłaszaniem i rozpowszechnianiem istotnych informacji z nimi związanymi do systemu zarządzania bezpieczeństwem (*Cyber*… 2016).

Ważną datą dla NATO był marzec 2015 roku, kiedy sekretarz generalny, Jens Stoltenberg oficjalnie uznał możliwość zastosowania art. V Traktatu

Północnoatlantyckiego w przypadku cyberataku na państwo należącego do Sojuszu Północnoatlantyckiego (*Cyberprzestrzeń zostanie*… 2016). Mogłoby się wydawać, że jest to kamień milowy dla NATO, jeśli chodzi o cały aspekt cyberwojen, jednakże trzeba pamiętać, że art. V nie precyzuje konkretnie, jaką pomoc mają udzielić inni członkowie sojuszu.

Tallin Manual on the International Law Applicable to CyberWarfare

Tallinn Manual on the International Law Applicable to CyberWarfare, który powstał z inicjatywy NATO CCDCOE, jest w chwili obecnej jedynym w skali międzynarodowej zbiorem sugerowanych postępowań w przypadku szeroko pojętego zagrożenia związanego z cyberatakami czy cyberwojnami. Został on opracowany przez międzynarodowych ekspertów, jednakże nie stanowi obowiązującego prawa, jest dokumentem, na który można się powoływać, gdyby rzeczywiście zaistniała taka potrzeba. Nie może być też uznany za dokument reprezentujący doktrynę NATO w temacie prowadzenia cyberwojen, a w wielu przypadkach tezy w nim zawarte nie są jednoznaczne.

Nie jest możliwe przedstawienie w artykule wszystkich zagadnień prawnych *Tallin Manual on the International Law Applicable* ze względu na bardzo szerokie spektrum problemów dotyczących cyberprzestrzeni. Analizy powyższego dokumentu już istnieją (choć nie w języku polskim), a NATO CDCCOE zapowiedziało wydanie kolejnej, poprawionej wersji tego dokumentu (*Looking*… 2016). Warto jednak przyjrzeć się jednemu, prawdopodobnie najbardziej kontrowersyjnemu zagadnieniu z tej publikacji określanej jako „biblia" cyberwojny.

Art. 51 Karty Narodów zjednoczonych zakłada, że *żadne postanowienie niniejszej Karty nie narusza naturalnego prawa każdego członka Organizacji Narodów Zjednoczonych, przeciwko któremu dokonano zbrojnej napaści, do indywidualnej lub zbiorowej samoobrony, zanim Rada Bezpieczeństwa zastosuje środki, konieczne dla utrzymania międzynarodowego pokoju i bezpieczeństwa. Środki podjęte przez członków w wykonaniu tego prawa do samoobrony powinny być natychmiast podane do wiadomości Radzie Bezpieczeństwa i w niczym nie powinny naruszać wynikającej z niniejszej Karty kompetencji i odpowiedzialności Rady do podjęcia w każdym czasie akcji, jaką uzna ona za konieczną dla utrzymania albo przywrócenia międzynarodowego pokoju i bezpieczeństwa.* Zgodnie z nim, każde państwo ma prawo do samoobrony, przynajmniej do czasu spełniania określonych warunków wymienionych w powyższym artykule. Jednakże autorzy *Tallin Manual on the International Law Applicable* sugerują, że jeśli formą tego ataku miałby być cyberatak, to forma obrony miałaby się sprowadzać przede wszystkim do ograniczenia skutków. Głównym uzasadnieniem dla takiego postępowania jest odwołanie się do zasady konieczności i proporcjonalności w odniesieniu do rozmiaru cyberataku. Jeśli jednak taki atak byłby wymierzony w

infrastrukturę krytyczną, jest to przesłanka za określeniem takiego ataku jako aktu agresji, który usprawiedliwia użycie środków konwencjonalnych w akcji odwetowej. W całej tej sytuacji, bez względu na cel atakującego, autorzy zaznaczają, że nadal obowiązuje strony konfliktu międzynarodowe prawo humanitarne, zwłaszcza konwencje genewskie – nawet jeśli nie można byłoby wskazać znamion wyczerpujących definicję wojny (Tarnogórski 2013).

Zakończenie

Trudno jednoznacznie określić, czy w chwili obecnej sojusz jest rzeczywiście przygotowany do odparcia cyberataków. Nie ma też żadnej wymiernej skali, która pozwoliłaby określić, czy NATO w tym momencie ma przewagę na tej płaszczyźnie, a jedynymi źródłami na ten temat są informacje z publicznych wywiadów z dowódcami wojskowymi, mniej lub bardziej powiązanymi z bezpieczeństwem sieci, które sprowadzają się np. do określeń, że w razie ataku sojusz bez wątpliwości by wygrał (*Atak*… 2016). Ale czy tak jest rzeczywiście? W 2010 roku były wiceadmirał i szef *National Intelligence* Michael McConnell, stwierdził podczas przesłuchania przed Komitetem ds. Handlu i Transportu Senatu USA, że Stany Zjednoczone nie wygrałyby cyberwojny, gdyby zostały zaatakowane w ten sposób, zwłaszcza że jednym z podstawowych filarów tego państwa jest szeroka infrastruktura sieciowa, na której opiera się jego funkcjonowanie (*Atak*… 2016). Nasuwa się w związku z tym pytanie, czy rzeczywiście udało się w tak krótkim czasie nadrobić zaległości na polu tworzenia podstaw cyberbezpieczeństwa.

Można zaobserwować progres w odchodzeniu od lekceważenia zagrożeń związanych z cyberprzestrzenią i tworzenie nowych komórek organizacyjnych (idea powstawania CERTów) zajmujących się ochroną cyberbezpieczeństwa w aspekcie bezpieczeństwa narodowego. Drugą pozytywną zmianą jest określanie konkretnych strategii bezpieczeństwa w kontekście zagrożeń cyberprzestrzeni. Także coraz więcej państw traktuje zagrożenia cyberatakami poważnie i dołącza do inicjatywy oraz wsparcia (głównie finansowego) CCDCOE. W kwietniu 2016 roku było to już 16 państw (*NATO opens*… 2008).

Warto zwrócić uwagę, że USA w 2011 roku uznały cyberprzestrzeń jako *operacyjną sferę wojny i zapowiedziały reagowanie na ataki w cyberprzestrzeni, tak jak na wszelkie inne zagrożenia* (Tamże). Powołano nawet specjalny organ dowodzenia – *US CyberCommand*. Amerykańska doktryna pozwala nawet na przeprowadzenie kampanii ofensywnej (*Atak*… 2016). Istnieją w NATO także plany na powołanie odrębnego cyberdowództwa (Tamże). Pytanie tylko czy nie będzie to mnożeniem biurokracji przy tak dużej ilości powstałych w ramach Sojuszu instytucji zajmujących się cyberzagrożeniami.

Podsumowując, NATO w bardzo krótkim czasie podjęło istotne działania zapewniające swoim członkom bezpieczeństwo. Zapewne powiodłaby się również

obrona przed poważniejszym cyberatakiem. Ale mimo to, wciąż istnieje potrzeba opracowania szczegółowych dokumentów strategicznych w tym zakresie.

Bibliografia

AAP-06 Edition 2014. NATO Glossary of terms and Definitions. Dostęp 14.06.2016. Tryb dostępu: http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf.

All about ARPAnet. Dostęp 05.12.2016. Dostępny Tryb dostępu: https://www.prairiehill.org/technology/web_projects/CV_ARPANET.html.

Arquilla, J., Ronfeldt, D., *Cyberwar is coming!* W: *In Athena's Camp: Preparing for conflict in the information age, RAND Corporation* 1993. Tryb dostępu: http://www.rand.org.

Atak w wirtualu. Dostęp 12.05.2016 r. Tryb dostępu: http://polska-zbrojna.pl/home/articleinmagazineshow/10171?t=ATAK-W-WIRTUALU.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2013). Warszawa: Biuro Bezpieczeństwa Narodowego.

Clausewitz, C. (2010) *O wojnie*. Warszawa: Wydaw. MUZA.

Cyber defence. *NorthAtlanticTreaty Organization.* Dostęp: 16.05.2016. Tryb dostępu: http://www.nato.int/cps/en/natohq/topics_78170.htm.

Cyberprzestrzeń zostanie uznana za sferę działań wojskowych. Dostęp 16.02.2016. Tryb dostępu: http://www.cyberdefence24.pl/378951,cyberprzestrzen-zostanie-uznana-za-sfere-dzialan-wojskowych .

Cyberwojna – wielkie wyzwanie dla NATO. Czy uda się wypracować jednolitą strategię Sojuszu. Dostęp 23.06.2016. Tryb dostępu: http://konflikty.wp.pl/kat,106090,title,Cyberwojna-wielkie-wyzwanie-dla-NATO-Czy-uda-sie-wypracowac-jednolita-strategie-Sojuszu,wid,16219495,wiadomosc.html.

Darczewska, J. (2014) *Anatomia rosyjskiej wojny informacyjnej – studium przypadku.* „Punkt Widzenia", nr 42. Dostęp 21.06.2016. Tryb dostępu: http://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf.

Davies, P. K. (2014) *Deterrence, Influence, Cyber Attack, and Cyberwar*. "New York Uniwersity Journal of International Law and Politics", v. 47, no. 2, s. 327-355.

Fjuk, I. (1997) *Estonia:Emerging and Dynamic.* USA: Wydaw. Wonder Book.

Górka-Winter B. (2002) *Praski szczyt NATO (21-22 listopada 2002 r.).* „Biuletyn Polskiego Instytutu Spraw Międzynarodowych”*, nr 102.* Dostęp 23.06.2016. Tryb dostępu: http://www.pism.pl/index/?id=afdec7005cc9f14302cd0474fd0f3c96.

Hakerzy na pierwszej linii frontu. Dostęp 14.04.2016. Tryb dostępu: http://argumenty.net/netsociety/techsoc/1669-hacker-wars.

Jemioło, T., Sienkiewicz, P. (red.) (2004) *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka).* Tom I. Raport z badań. Warszawa.

Karta Narodów Zjednoczonych. Dostęp 05.05.2016. Tryb dostępu: http://libr.sejm.gov.pl/tek01/txt/onz/1945.html.

Koncepcja Strategiczna NATO Z 2010 r. Dostęp 14.06.2016*.* Tryb dostępu: https://www.bbn.gov.pl/download/1/15758/KoncepcjastrategicznaNATO.pdf.

Konwencja haska IV (1907). Dostęp 30.06.2016. Tryb dostępu: https://pl.wikisource.org/wiki/Konwencja_haska_IV_(1907).

Liderzy czy naśladowcy. Dostęp 27.112015. Tryb dostępu: http://www.pi.gov.pl/parp/chapter_86196.asp?soid=D4C9F0B3CD20486D8B5C3F497251AE47.

Liedel, K., Piasecka. P. (2011) *Wojna cybernetyczna – wyzwanie XXI wieku*. „Pozamilitarne aspekty bezpieczeństwa. Biuro Bezpieczeństwa Narodowego”, nr 1. s. 15-28. Dostęp 04.11.2015. Tryb dostępu: https://www.bbn.gov.pl/download/1/7008/1Wojnacybernetyczna.pdf.

Looking forward to 2017. Dostęp 26.12.2016. Tryb dostępu: https://ccdcoe.org/looking-forward-2017.html.

Marne szanse USA w wypadku cyberwojny. Dostęp 18.06.2016. Tryb dostępu: http://tech.wp.pl/kat,1009785,title,Marne-szanse-USA-w-wypadku-cyberwojny,wid,12018933,wiadomosc.html?ticaid=1173ab&_ticrsn=3.

NATO i UE podpisały porozumienie w sprawie cyberobrony. Dostęp 16.02.2016. Tryb dostępu: http://www.cyberdefence24.pl/306205,nato-i-ue-podpisaly-porozumienie-w-sprawie-cyberobrony.

NATO opens new centre of excellence on cyber defence (2008). Dostęp 15.03.2016. Tryb dostępu: http://www.nato.int/docu/update/2008/05-may/e0514a.html.

Rid, T. (2011) *Cyber War Will Not Take Place.* “Journal of Strategic Studies”, No 35:1, s. 5-32.

Roscini, M. (2014) *Cyber Operations and the Use of Force in International Law*. United Kingdom: Oxford University Press.

Rozrachunek z dziedzictwem epoki radzieckiej w Estonii. Dostęp 14.05.2016. Tryb dostępu: http://www.goethe.de/ges/pok/prj/usv/svg/pl7578017.htm.

Schmitt, M.N. (red.) (2013) *Tallin Manual on the International Law Applicable to CyberWarfare*. USA: Cambridge University Press.

Shakarian, P. (red) (2013) *Introduction to Cyber-warfare. A multidisciplinary approach.* Waltham.

Smart Defence. *NATO Review Magazine.* Dostęp 21.05.2016. Tryb dostępu: http://www.nato.int/docu/review/topics/en/Smart-Defence.htm.

Tarnogórski, R. (2013) *Prawo konfliktów zbrojnych a cyberprzestrzeń*. „Biuletyn PISM", nr 31.

Terms and definition. *NATO Cooperative Cyber Defence of Excellence.* Dostęp 17.05.2016. Tryb dostępu: https://ccdcoe.org/cyber-definitions.html.

Toffler, A., Toffler, H. (2006) *Wojna i Antywojna. Jak przetrwać na progu XX wieku?* Poznań: Wydaw. KURPISZ S.A.

Waxman, M. C. (2011) *Cyber-Attacks and the Use of Force.* Dostęp 14.06.2016. Tryb dostępu: https://yalejournalofintllaw.files.wordpress.com/2016/02/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf.

Wojna hybrydowa. Dostęp 17.02.2016. Tryb dostępu: http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.

Streszczenie

Rozwój Internetu, technologii i szeroko pojętej cyberprzestrzeni, implikuje infromatyzację społeczeństw w każdej dziedzinie. W artykule podjęto próbę przedstawienia aktualnego stosunku NATO do zagrożenia cyberwojen, poprzedzonego terminologicznymi rozważaniami na temat tego zjawiska oraz ustosunowano się do kwestii przygotowania Sojuszu Północnoatlantyckiego do obrony przed atakiem cyberwojny.

Słowa kluczowe: cyberwojna, NATO, Tallin Manual, CCDCOE

Cyberwar and its importance for the security of NATO in the context of cases and strategic documents

Summary

Development of the Internet, technology and broader cyberspace implies improvmenet in societies in every field. This phenomenon occurs in an uncontrolled manner, which was established some kind of a security flaw which the state and other political actors another option for achieving its goals, not necessarily in a legal way. The purpose of this article is the importance of cyberwar in the international arena as well as the operation and institutions in response to NATO appointed for the defense of its members in the context of the threat.

Key-words: Cyberwar, NATO, Tallin Manual, CCDCOE

CZĘŚĆ II

Środowisko bezpieczeństwa informacyjnego

Marian Cieślarczyk
Wydział Humanistyczny UPH w Siedlcach

Ekologia informacji, kultura informacyjna i kultura bezpieczeństwa informacyjnego w teorii i w praktyce

Kontury sytuacji problemowej

Podejmując próbę syntetycznego nakreślenia sytuacji problemowej, stanowiącej swoiste tło do dalszych rozważań, zacznijmy od krótkiej refleksji dotyczącej znaczenia *środowiska informacyjnego* Człowieka i Jego *kultury informacyjnej* dla różnych sfer życia i bezpieczeństwa osób, grup społecznych i zawodowych, dla społeczności lokalnych oraz dla całych społeczeństw. Mówiąc o szeroko rozumianym *bezpieczeństwie* mamy na myśli nie tylko *brak zagrożeń* dla wyżej wymienionych *podmiotów,* ale także możliwość ich *rozwoju* w bliższej i dalszej perspektywie oraz – co ma szczególne znaczenie dla społeczeństw wysoko rozwiniętych – godną *jakość* ich *życia*. W rozważaniach na temat *kultury informacyjnej* i *kultury bezpieczeństwa informacyjnego* warto brać pod uwagę wpływ tych dwu fenomenów na różne, przedmiotowe obszary bezpieczeństwa, takie jak: bezpieczeństwo ekologiczne i zdrowotne, bezpieczeństwo ekonomiczne, polityczne i społeczne, bezpieczeństwo publiczne i militarne oraz inne, nie nazwane jeszcze wymiary bezpieczeństwa. Życie dostarcza wielu przykładów na to, że taki związek istnieje.

Nie zawsze jednak pamięta się o tym, że kultura informacyjna i kultura bezpieczeństwa – także informacyjnego – mają dla człowieka szczególne znaczenie w sytuacjach kryzysowych w każdym z przedstawionych wyżej obszarów bezpieczeństwa. Z dużym prawdopodobieństwem można przyjąć, że skuteczne radzenie sobie z kryzysami wymaga wysokiego poziomu kultury informacyjnej i kultury bezpieczeństwa informacyjnego. Łatwiej jest to wyobrazić sobie wtedy, kiedy przywołujemy w pamięci różnorodne sytuacje kryzysowe, jakich doświadczaliśmy np. w domu, w miejscu zamieszkania czy w pracy, ale także patrząc na ten problem szerzej przez pryzmat kryzysów globalnych np. ekonomicznych, politycznych czy militarnych. Przyjęcie takiej perspektywy otwiera, jak się wydaje, wiele ciekawych poznawczo i praktycznie znaczących obszarów badawczych, szczególnie wtedy, kiedy kulturę informacyjną będziemy traktować jako jeden z podstawowych elementów kultury bezpieczeństwa (Cieślarczyk 2015).

Wysoki poziom kultury bezpieczeństwa człowieka i grup społecznych, w tym przede wszystkim kultury informacyjnej i kultury bezpieczeństwa informacyjnego, sprzyja osiąganiu *poczucia podmiotowości*. Dobrze służy także kształtowaniu się przekonania o wpływie tego czynnika na *jakość życia* tych podmiotów oraz na wyższy poziom ich bezpieczeństwa w wymiarze *obiektywnym* i *subiektywnym*.

Można przypuszczać, że odpowiedni poziom kultury informacyjnej i kultury bezpieczeństwa informacyjnego danego podmiotu jest jednym z głównych warunków kształtowania względnej równowagi między bezpieczeństwem *obiektywnym* i *subiektywnym* (Frei 1997). Bez tego zaś nie ma bezpieczeństwa w dłuższym wymiarze czasu. Jeśli tak, to ewentualne upowszechnianie się „cywilizacji post prawdy" może budzić uzasadniony niepokój. Taka sytuacja z jednej strony utrudnia funkcjonowanie człowieka i grup społecznych w coraz bardziej złożonej rzeczywistości XXI wieku, a tym samym ogranicza ich rozwój i bezpieczeństwo. Z drugiej zaś strony, może to niekorzystnie wpływać na różne rodzaje środowisk bezpieczeństwa, w tym także na środowisko informacyjne, niosąc z sobą wiele negatywnych skutków, np. zalew informacji, jej niską jakość, smog informacyjny itp. (Babik 2016, s. 46).

Chociaż znaczenie informacji i „zdrowego" środowiska informacyjnego dla bezpieczeństwa człowieka doceniano od zarania dziejów, to jednak w ostatnich dekadach, nazywanych cywilizacją informacyjną i cywilizacją wiedzy, nabierają one szczególnego znaczenia. Świadomość tego faktu nie jest jednak powszechna, a wynikające z tej sytuacji wnioski nie są jeszcze w stopniu zadowalającym wykorzystywane w różnych sferach życia i działalności człowieka, w różnych obszarach jego bezpieczeństwa. Nie mniej jednak, niektórzy ludzie i grupy społeczne, a być może nawet całe społeczeństwa, lepiej niż inne radzą sobie w tej sytuacji. Warto o tym wspomnieć dlatego, że różnice poziomu kultury informacyjnej między podmiotami fizycznymi i prawnymi były i są nierzadko wykorzystywane jako rodzaj przewagi konkurencyjnej, stosowanej także do osiągania nie zawsze godnych i egoistycznych celów. Najwyraźniej widać to na przykładzie zjawiska walki i wojny informacyjnej, której zakres i złożoność w ostatnich latach wyraźnie wzrasta. A może wzrasta nasza wrażliwość i świadomość tego rodzaju zagrożeń? Tak czy inaczej można przyjąć, że wyższy poziom kultury informacyjnej i kultury bezpieczeństwa informacyjnego osób, instytucji i organizacji może spełniać rolę „tarczy i miecza" jednocześnie. Ryzykownym byłoby jednak stwierdzenie, że w tym zakresie w naszym kraju niewiele już mamy do zrobienia.

Biorąc pod uwagę fakt, że jednym z istotnych wyznaczników kultury informacyjnej jest jednoznaczność rozumienia przez różne podmioty podstawowych terminów, jakimi posługują się one w rozwiązywaniu problemów o charakterze teoretycznym i praktycznym, w dalszej części artykułu zatrzymamy się przy kilku z nich.

Sposoby rozumienia podstawowych pojęć i relacji między nimi

Zacznijmy od pojęć: *ekologia informacji, kultura informacyjna, kultura bezpieczeństwa* – także *informacyjnego oraz bezpieczeństwo informacyjne,* z myślą o wykorzystaniu uzyskanej w ten sposób wiedzy przy interpretacji

niektórych wyników badań empirycznych. Przedstawione zostaną dane dotyczące elementów *kultury bezpieczeństwa,* a w niej *kultury informacyjnej* podmiotów fizycznych i prawnych (diagram 1 i tabela 1), funkcjonujących w strukturach zarządzania kryzysowego na szczeblu podstawowym w różnych regionach Polski.

Termin *ekologia informacji* do obiegu naukowego został wprowadzony w 1997 r. przez Thomasa Davenporta (za: K. Materska 2007, s. 243). W Polsce problematyką tą zajmują się: W. Babik, H. Batorowska, E. Głowacka, M. Hetmański i inni. Zdaniem W. Babika (2016, s. 48) *ekologia informacji to metafora traktująca przestrzeń informacyjną jako ekosystem/infosystem. Termin ten wyraża związek między ideami ekologii środowiska przyrodniczego a dynamiką rozwoju i cechami cyfrowej przestrzeni informacji. W opisie i analizie środowiska informacyjnego, w tym systemów informacyjnych, ekologia informacji posługuje się językiem ekologii jako nauki przyrodniczej, której przedmiotem jest środowisko przyrodnicze (przyroda).* Autor ten podkreśla, że *ekologia informacji* umożliwia człowiekowi dowiedzenie się czegoś więcej o sobie podczas eksploracji problemów infoekologicznych dzięki temu, że wnosi antropocentryczne podejście do informacji. Zwraca się więc uwagę na potrzebę ochrony człowieka przed nadmiarem informacji z myślą o jego zrównoważonym rozwoju. Może temu sprzyjać m.in. przechodzenie od alfabetyzacji informacyjnej do kultury informacyjnej, na co zwraca uwagę H. Batorowska. Autorka ta analizuje kulturę informacyjną z różnych perspektyw. Z jednej strony z punktu widzenia: socjologii kultury, psychologii i historii; z drugiej strony zaś zwraca uwagę na definicje normatywne i strukturalne. *Z punktu widzenia socjologii kultury ważne jest nie tylko określenie grupy osób, które się bada, ale także wybór określonych aspektów tej kultury poddawanych badaniom. W przypadku kultury informacyjnej obszarem tym jest świadomość informacyjna grupy, wartości, postawy wobec informacji, zachowania użytkowników, etyka korzystania z informacji, a także wytwory wynikające z uczestnictwa w procesie informacyjnym.* […] *W stosunku do kultury informacyjnej praktycznym wydaje się zastosowanie sposobu definiowania polegającego na wyliczeniu jej części składowych (głównie zachowań informacyjnych i czynników oddziałujących na te zachowania) oraz na ujmowaniu jej jako zespołu norm obowiązujących użytkowników informacji*. Zdaniem tej autorki […] *w kulturze informacyjnej występują różne kategorie elementów tej kultury, takie jak: materialno-techniczne (infrastruktura informacyjna), społeczne (relacje między użytkownikami informacji), ideologiczne (informacja jako towar, wartość) i psychiczne (proces percepcji informacji, dojrzałość informacyjna) oraz powiązania występujące między tymi elementami* (Batorowska 2013, s. 59-60).

Ten sposób rozumienia *kultury informacyjnej* stanowi dobry pomost między nią a *kulturą bezpieczeństwa* w znaczeniu, jakie nadaje temu terminowi M. Cieślarczyk. Autor ten pod pojęciem kultura bezpieczeństwa rozumie *zbiór podstawowych założeń, wartości, norm, reguł, symboli i przekonań*

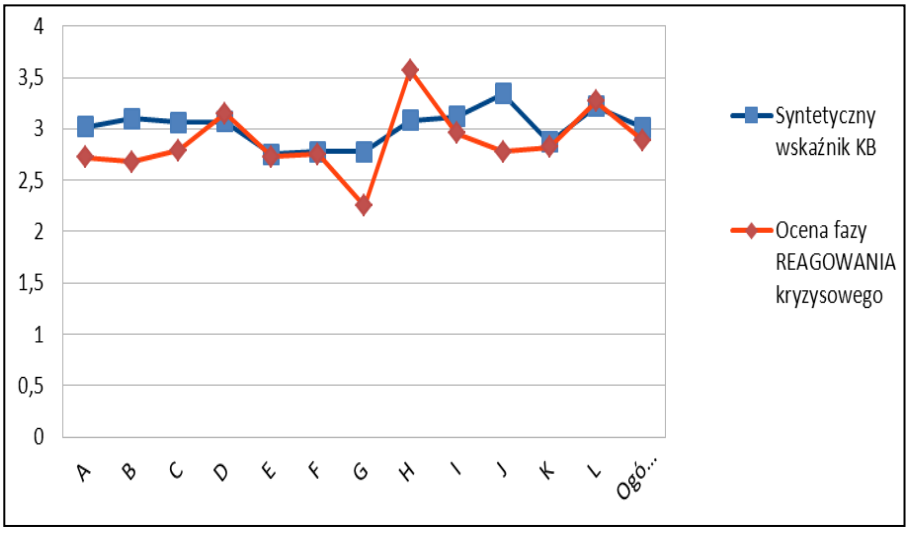
charakterystycznych dla danego podmiotu, wpływających na sposób postrzegania przez niego wyzwań, szans i zagrożeń w bliższym i dalszym otoczeniu, sposób odczuwania bezpieczeństwa i myślenia o nim oraz związany z tym sposób zachowania i działania, wyuczony przez podmiot w procesach edukacji i tworzenia infrastruktury, np. informatycznej i informacyjnej, służącej osiąganiu […] *najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie i dla otoczenia* (Cieślarczyk 2006, s. 210). Tak rozumiana *kultura bezpieczeństwa,* a w jej ramach *kultura bezpieczeństwa informacyjnego*, odnosząca się także do *bezpieczeństwa informacyjnego* spełnia niezmiernie ważną rolę w cywilizacji informacyjnej i cywilizacji wiedzy. Może być ona traktowana jako czynnik służący zharmonizowanemu rozwojowi i bezpieczeństwu podmiotów w dłuższym wymiarze czasu, a w sytuacjach ekstremalnych np. w walce i wojnie informacyjnej może ona pełnić wspomnianą już funkcję „tarczy" i „miecza" jednocześnie. Tym samym może dobrze służyć zapewnianiu bezpieczeństwa podmiotów fizycznych i prawnych w zasadniczych sferach ich życia i działalności, w różnych obszarach bezpieczeństwa – także informacyjnego. Na rysunku 2 bezpieczeństwo informacyjne zostało przedstawione jako swoisty fundament dla innych obszarów bezpieczeństwa. Zaś kultura bezpieczeństwa, a w niej kultura bezpieczeństwa informacyjnego może być traktowana jako struktura, spajająca przedmiotowe obszary bezpieczeństwa, a zarazem decydująca o ich poziomie i o harmonijnym rozwoju danego podmiotu oraz jego środowiska. W ten sposób zbliżyliśmy się do zagadnień *ekologii informacji.* Badania w tym zakresie mogą mieć także wartość praktyczną w strategicznym podejściu do badania *bezpieczeństwa informacyjnego* i podnoszenia jego poziomu m.in. poprzez doskonalenie kultury bezpieczeństwa i jej podstawowego elementu – kultury informacyjnej.

Czym więc jest *bezpieczeństwo informacyjne?* Nie ulega wątpliwości, że *staje się* ono coraz bardziej cenioną *wartością.* Jednak aktualnie stwierdzenie to dotyczy prawdopodobnie stosunkowo niewielkiej grupy osób. Jeśli tak, to w społeczeństwie demokratycznym powinno to stanowić powód do niepokoju. Czy bezpieczeństwo informacyjne można traktować jako jeden z przedmiotowych obszarów bezpieczeństwa? Czasami tak jest ono rozumiane. Jeśli tak, to warto je postrzegać jako podstawę dla innych obszarów bezpieczeństwa (patrz rys. 2). Deficyt badań w tym zakresie jest jednak odczuwalny. W związku z tym na obecnym etapie rozwoju wiedzy o tym *fenomenie* praktycznie użyteczne wydaje się przyjęcie, że *bezpieczeństwo informacyjne można rozumieć jako wypadkową bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego* […] (Łuczak 2004, s. 80) *oraz,* że […] *jest to kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska informacyjnego, a także jego formowanie, wykorzystanie i rozwój w interesie obywateli, organizacji i państwa. Ogólnie obejmuje trzy składowe: ludzi, technologie i procesy, które są obiektem badań, oraz oceny* (Janczak, Nowak 2013, s. 17).

Próba interpretacji wyników badań empirycznych w świetle przyjętych założeń teoretycznych

W tej części artykułu zostaną przedstawione niektóre wyniki badań empirycznych przeprowadzonych w 2013 roku w kilkunastu miejscowościach w różnych regionach Polski (Filipek i zespół 2013). W badaniach tych poszukiwano, m.in., odpowiedzi na pytanie: *czy istnieje zależność między poziomem i charakterem kultury bezpieczeństwa różnych podmiotów a jakością funkcjonowania Systemu Zarządzania Kryzysowego (SZK) w wymiarze lokalnym?* Wyniki badań potwierdziły istnienie zależności między poziomem kultury bezpieczeństwa osób wchodzących w skład SZK a jakością funkcjonowania tego systemu w wymiarze lokalnym. W graficznej formie związek ten zaprezentowano w postaci następującego wykresu.

Wykres 1. Zależności między kulturą bezpieczeństwa obywateli w danej miejscowości (A-L) a oceną *reagowania* na zagrożenia i sytuacje kryzysowe. N=1001



Źródło: „Kultura bezpieczeństwa", nr 3-4/2015, Siedlce: Wydaw. UPH, s. 236.

Wśród elementów kultury bezpieczeństwa znalazły się również *dane świadczące o poziomie kultury informacyjnej* badanych osób i grup społeczno-zawodowych (tabela 1 i diagramy 1-4). Ich omawianie zaczniemy od tabeli 1. Widać w niej stosunkowo niski poziom kultury bezpieczeństwa objętych badaniami osób (wys. wskaźnika 3,01 w skali 2-5). W tabeli tej można także zauważyć różnice ocen kultury bezpieczeństwa w poszczególnych miejscowościach oznaczonych symbolami A-L; najwyższe w miejscowości J – 3,34; zdecydowanie niższe w miejscowościach E, F i G – 2,75-2,78.

Różnice ocen dotyczą także tych elementów kultury bezpieczeństwa, które świadczą o poziomie kultury informacyjnej respondentów. Były to: *zakres wiedzy* niezbędnej badanym w sytuacjach kryzysowych (ocena 2,94), przydatność *sposobów myślenia* w sytuacjach kryzysowych (2,93), *„kompetencje" emocjonalne* niezbędne badanym w sytuacjach kryzysowych (2,92) oraz poziom ich *kultury prawnej* (2,90).

Tabela 1. Ocena niektórych elementów kultury informacyjnej badanych osób (N=1001) wśród innych elementów kultury bezpieczeństwa (Dane wg średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe).

SYMBOLE MIEJSCOWOŚCI													
Kategorie	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**Ogółem**
1.**Wartości i normy** w odniesieniu do bezpieczeństwa	3,47	3,35	3,27	3,30	3,34	3,28	3,16	3,22	3,44	3,57	3,39	3,41	**3,35**
2. **Zakres wiedzy** niezbędnej w sytuacjach kryzysowych	**2,90**	**2,98**	**2,95**	**2,99**	**2,56**	**2,59**	**2,71**	**2,87**	**2,92**	**3,08**	**2,69**	**3,10**	**2,94**
3. Przydatność **sposobów myślenia** w sytuacjach kryzysowych **(poziom kwalifikacji mentalnych)**	**2,94**	**3,16**	**3,03**	**3,05**	**2,65**	**2,61**	**2,79**	**2,96**	**3,05**	**3,12**	**2,74**	**3,12**	**2,93**
4. **„Kompetencje" emocjonalne** niezbędne w sytuacjach kryzysowych	**2,88**	**3,09**	**3,02**	**3,0**	**2,54**	**2,60**	**2,75**	**3,12**	**3,03**	**3,05**	**2,77**	**3,15**	**2,92**
5. **Sprawność działania** w sytuacjach kryzysowych	3,01	3,05	3,05	3,04	2,82	2,80	2,67	3,17	3,13	3,14	2,93	3,31	**3,01**
6. **Poziom współpracy,**	2,97	3,02	3,10	3,02	2,85	2,86	2,77	3,32	3,21	3,23	2,86	3,32	**3,04**

współdziałania w sytuacjach kryzysowych													
7. **Poziom kultury prawnej** przydatnej w sytuacjach kryzysowych	**2,90**	**3,05**	**3,01**	**3,09**	**2,54**	**2,75**	**2,61**	**2,90**	**3,08**	**3,06**	**2,73**	**3,16**	**2,90**
SYNTETYCZNY wskaźnik kultury bezpieczeń-stwa	**3,02**	**3,10**	**3,06**	**3,07**	**2,75**	**2,78**	**2,78**	**3,08**	**3,12**	**3,34**	**2,87**	**3,22**	**3,01**

Źródło: „Kultura bezpieczeństwa”, nr 3-4/2015, Siedlce: Wyd. UPH, s. 176.

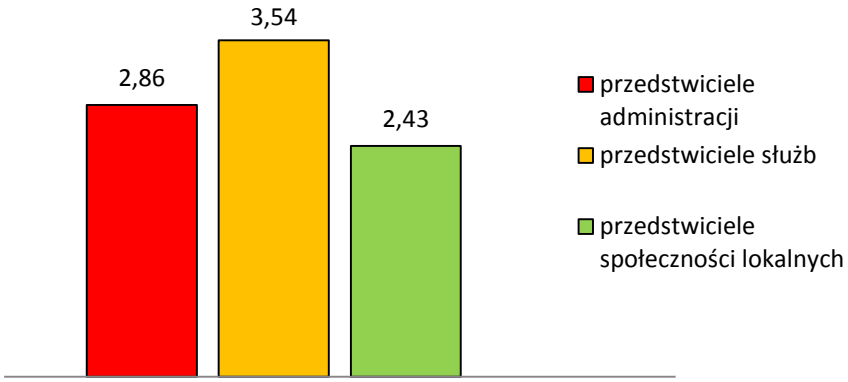
Przedstawione wyżej dane mogą wskazywać, że elementy kultury informacyjnej i kultury bezpieczeństwa informacyjnego badanych oceniane są najniżej (2,90-2,94) wśród innych elementów kultury bezpieczeństwa (3,01-3,35). Widać to szczególnie wyraźnie w miejscowościach E i F, w których oceny elementów kultury informacyjnej zbliżone są do niezadawalających i w większości oscylują między oceną 2,54 a 2,65. W miejscowościach tych stwierdzono jednocześnie najniższy poziom innych elementów kultury bezpieczeństwa (2,75-2,78), a zarazem najniższe oceny jakości funkcjonowania „systemu” zarządzania kryzysowego (2,73-2,75). Wyraz „system” celowo zapisano w cudzysłowie, jako że deficyt kultury informacyjnej osób, instytucji i organizacji wchodzących w skład tego „systemu” mógł wyraźnie utrudniać osiąganie cech systemowych i efektu dodanego, bez których trudno wyobrazić sobie rozwój SZK i doskonalenie jakości jego funkcjonowania.

Interesująco, a zarazem niepokojąco przedstawia się ocena elementów kultury informacyjnej dwóch grup społeczno-zawodowych wchodzących w skład szeroko rozumianego SZK. Chodzi o objętych badaniami przedstawicieli administracji terenowej i tzw. zwykłych obywateli. Ogólnie niski poziom kultury bezpieczeństwa tej ostatniej grupy, w tym także niski poziom kultury informacyjnej przyczyniały się do tego, że obywatele nie czuli się podmiotowo w systemie zarządzania kryzysowego. Warto również wspomnieć, że nie byli oni podmiotowo traktowani przez objętych badaniami przedstawicieli administracji terenowej, której poziom kultury bezpieczeństwa, a w niej kultury informacyjnej był niewiele wyższy od „zwykłych obywateli”. W ten sposób powstawała sytuacja „błędnego koła”, nie sprzyjająca doskonaleniu kultury informacyjnej i – szerzej biorąc – doskonaleniu kultury bezpieczeństwa obu tych grup. Bez tego zaś podnoszenie sprawności funkcjonowania SZK nie przynosi oczekiwanych efektów.

Niektóre elementy kultury informacyjnej objętych badaniami grup przedstawiono na diagramach 1-4, a wynikające z tego skutki zaprezentowano

na diagramie 5. Na diagramie 1 widać, że zbliżony do dobrego poziom *wiedzy przydatnej* w sytuacjach kryzysowych deklarują jedynie przedstawiciele służb funkcjonujących w ramach systemu zarządzania kryzysowego (3,54).

Diagram 1. Poziom wiedzy przydatnej badanym w sytuacjach kryzysowych (na podstawie średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe). N=1001



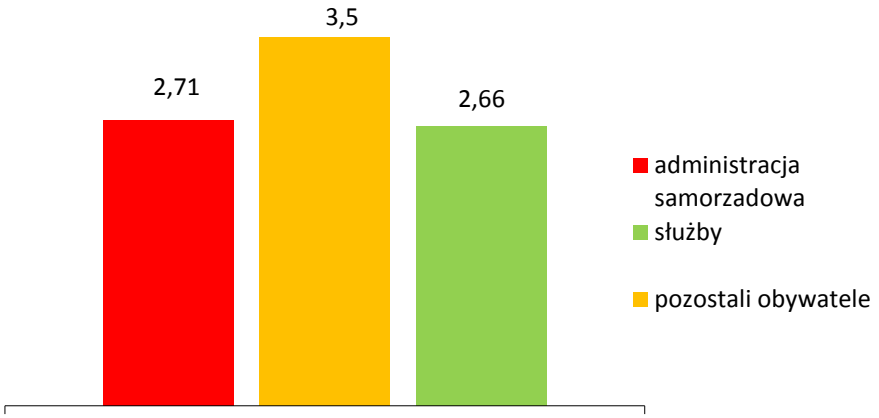
Źródło: „Kultura bezpieczeństwa”, nr 3-4/2015, Siedlce: Wydaw. UPH, s. 160.

Zaś przedstawiciele administracji terenowej oceniają swój poziom wiedzy przydatnej w sytuacjach kryzysowych poniżej oceny dostatecznej (2,86). Najbardziej krytyczne oceny swoich kompetencji w tym zakresie wyrażali objęci badaniami „zwykli obywatele” – 2,43.

Podobnie oceniano poziom kwalifikacji mentalnych badanych, przydatnych im w sytuacjach kryzysowych (diagram 2), chociaż – jak się wydaje – tzw. „zwykli obywatele” wykazywali w tym zakresie przesadny optymizm (ocena 2,66), podobnie jak objęci badaniami przedstawiciele administracji terenowej (2,71).

Chociaż przedstawiciele służb wyróżniali się na tym tle *in plus* (ocena 3,50), jeśli chodzi o poziom kwalifikacji mentalnych przydatnych im w sytuacjach kryzysowych, to jednak trudno byłoby powiedzieć, że osiągnęli oni poziom mistrzowski w tym zakresie.

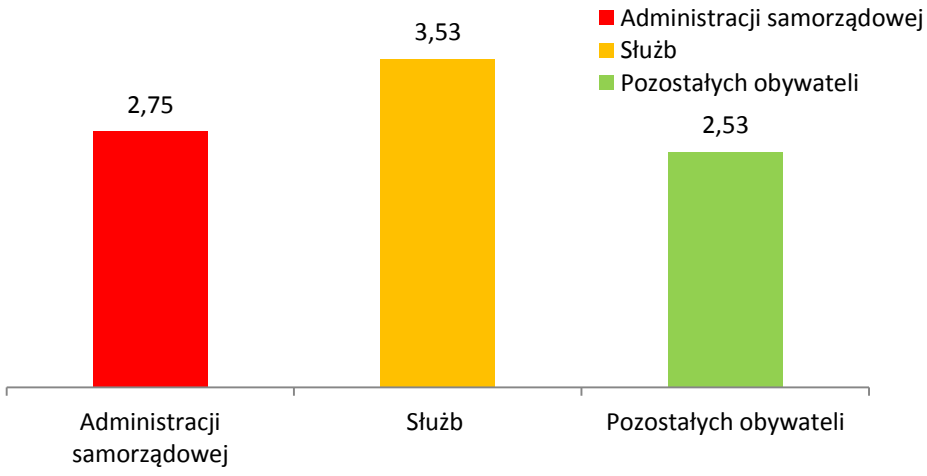
Diagram 2. Poziom kwalifikacji mentalnych badanych przydatnych im w sytuacjach kryzysowych (na podstawie średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe). N=1001



Źródło: „Kultura bezpieczeństwa”, nr 3-4/2015, Siedlce: Wyd. UPH, s. 162.

Badania wykazały także stosunkowo niski poziom „kompetencji” emocjonalnych niezbędnych tym grupom w sytuacjach kryzysowych (diagram 3). Nie pozostawało to bez wpływu na jakość funkcjonowania SZK.

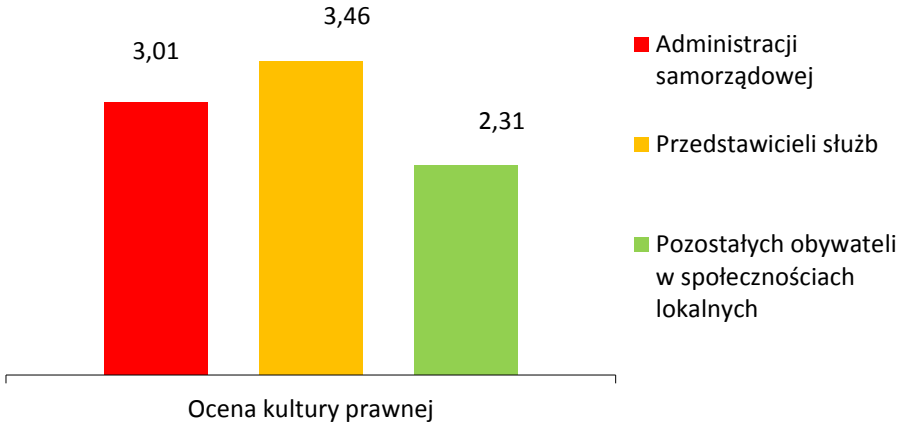
Diagram 3. Ocena emocjonalnej warstwy postaw jako elementu kultury bezpieczeństwa (na podstawie średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe). N=1001.



Źródło: „Kultura bezpieczeństwa”, nr 3-4/2015, Siedlce: Wydaw. UPH, s. 165.

Najniżej oceniono *poziom kultury prawnej* objętych badaniami grup społeczno-zawodowych (diagram 4). Chociaż poziom kompetencji administracji w tym zakresie przedstawiał się zadowalająco (ocena 3,01), to trudno byłoby przyjąć, że jest to ocena satysfakcjonująca. Szczególny niepokój może budzić widoczny na diagramie 4 wyjątkowo niski poziom kultury prawnej tzw. „zwykłych obywateli" (2,31), niezbędnej im nie tylko w trakcie trwania sytuacji kryzysowych, ale także przed ich wystąpieniem (chodzi o działania zapobiegawcze) oraz w fazie „odbudowy" np. po powodzi.

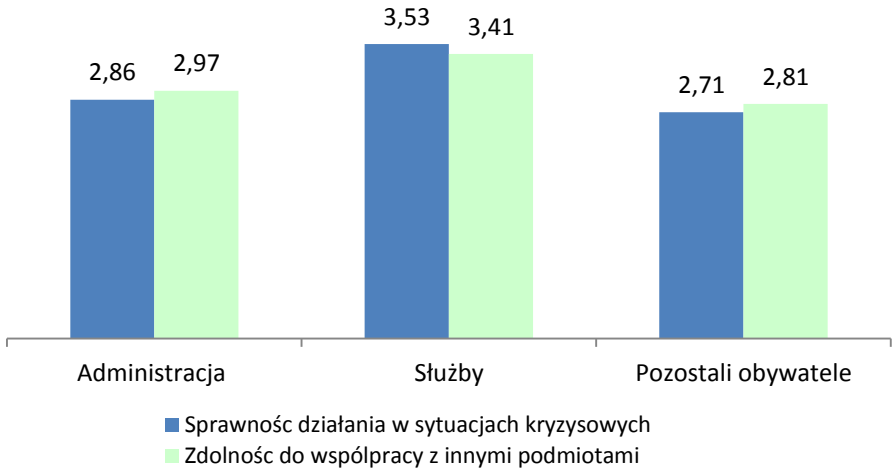
Diagram 4. Ocena kultury prawnej objętych badaniami podmiotów (na podstawie średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe). N=1001



Źródło: „Kultura bezpieczeństwa", nr 3-4/2015, Siedlce: Wydaw. UPH, s. 174.

Jak można się było spodziewać tak niskie, jak wyżej przedstawiono, wskaźniki kultury informacyjnej i kultury bezpieczeństwa nie sprzyjały *sprawności działania* i *zdolności do współpracy* w sytuacjach kryzysowych objętych badaniami osób i grup społeczno-zawodowych (diagram 5). Jedynie przedstawiciele służb pozytywnie oceniali swoją sprawność działania i współdziałania podczas sytuacji kryzysowych. Natomiast ocena kompetencji w tym zakresie administracji i pozostałych obywateli nie przekraczała 3,0. Tak duże, jak widać to na diagramach 2-4, dysproporcje między ocenami kultury informacyjnej administracji terenowej i tzw. „zwykłych obywateli" a służbami zarządzania kryzysowego nie sprzyja sprawności, skuteczności i efektywności funkcjonowania tego „systemu". Świadczą o tym zarówno wyniki badań empirycznych, jak również doświadczenia z różnych sytuacji kryzysowych. Problem ten był najbardziej odczuwalny w miejscowościach, które w ostatnich latach kilkakrotnie doświadczały powodzi.

Diagram 5. Ocena *sprawności działania* w sytuacjach kryzysowych i *zdolności do współpracy* z innymi podmiotami (na podstawie średnich arytmetycznych w skali: 5 – oceny najwyższe, 2 – oceny najniższe). N=1001

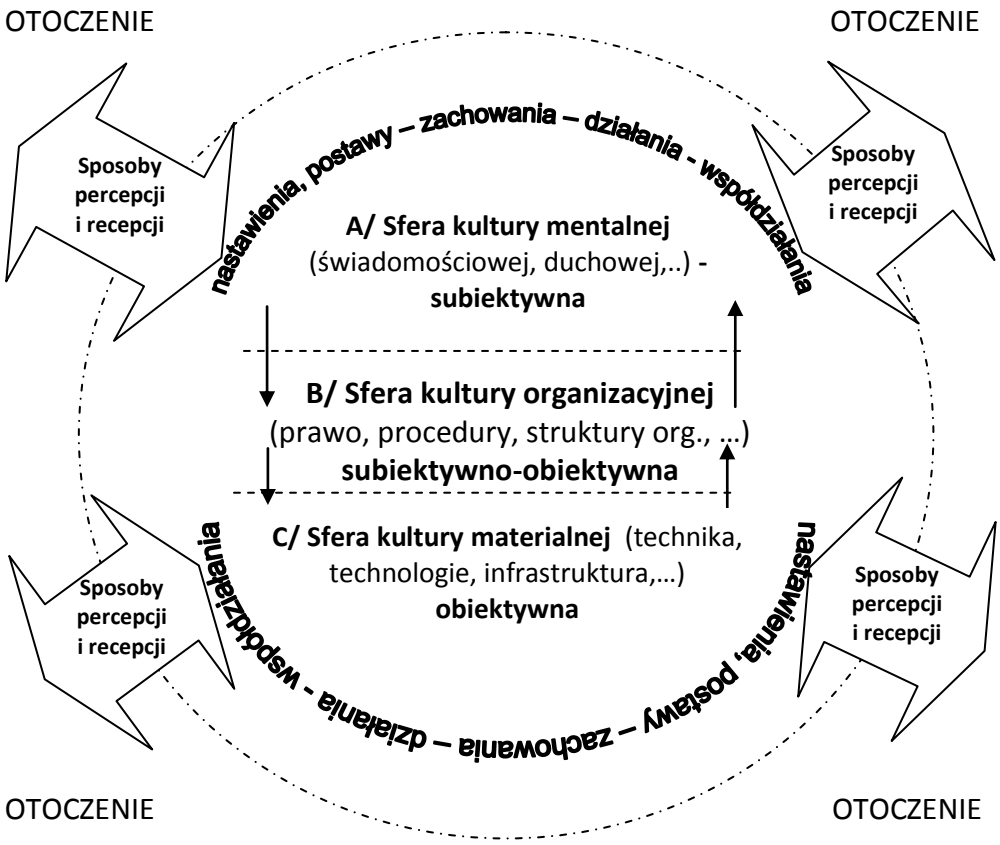


Źródło: „Kultura bezpieczeństwa”, nr 3-4/2015, Siedlce: Wydaw. UPH, s. 171.

Zamiast podsumowania – kilka wniosków o charakterze teoretycznym i praktycznym

Przedstawione wyżej dane empiryczne ukazują tylko niektóre elementy kultury bezpieczeństwa, a w niej kultury informacyjnej badanych osób i grup społeczno-zawodowych przydatne im w sytuacjach kryzysowych. Korzystając z modelu prezentowanego na rysunku 1 możemy przyjąć, że dane na diagramach 1-3 dotyczą głównie sfery A/, czyli elementów kultury mentalnej, świadomościowej; zaś dane na diagramie 4 ukazują tylko jeden z elementów kultury organizacyjnej (sfera B/), czyli ocenę poziomu kultury prawnej badanych osób.

Rysunek 1. Podmiot i elementy jego kultury informacyjnej i kultury bezpieczeństwa w relacjach z otoczeniem



Źródło: opracowanie własne na podstawie: Cieślarczyk, M. (2006) *Kultura bezpieczeństwa i obronności*. Siedlce: Wydaw. AP, s. 196-200.

Dane na diagramach 1-5 oraz w tabeli 1 wykorzystano jedynie jako przykłady ukazujące możliwości empirycznego badania kultury bezpieczeństwa i jej ważnego elementu – kultury informacyjnej w odniesieniu do systemu zarządzania kryzysowego. Prezentowane na tych diagramach dane nie uwzględniają innych elementów kultury bezpieczeństwa, takich jak np. znajomość i stosowanie procedur obowiązujących w poszczególnych etapach zarządzania kryzysowego (sfera B/), a także sposobów i zakresu wykorzystania techniki informatycznej, zaliczanej do kultury materialnej (sfera C/ na rys. 1). Należy

podkreślić, że badając kulturę informacyjną warto uwzględniać także wektory symbolizujące *relacje wewnętrzne* między sferami A/, B/ i C/, ale także *relacje zewnętrzne* między danym podmiotem a jego otoczeniem. W relacjach tych ważną rolę odgrywają *sposoby percepcji i recepcji* bliższego i dalszego otoczenia podmiotu oraz środowiska informacyjnego, postrzeganego przez pryzmat *ekologii informacji*. Być może prowadzone w przyszłości badania empiryczne powinny brać pod uwagę wyżej wymienione kwestie.

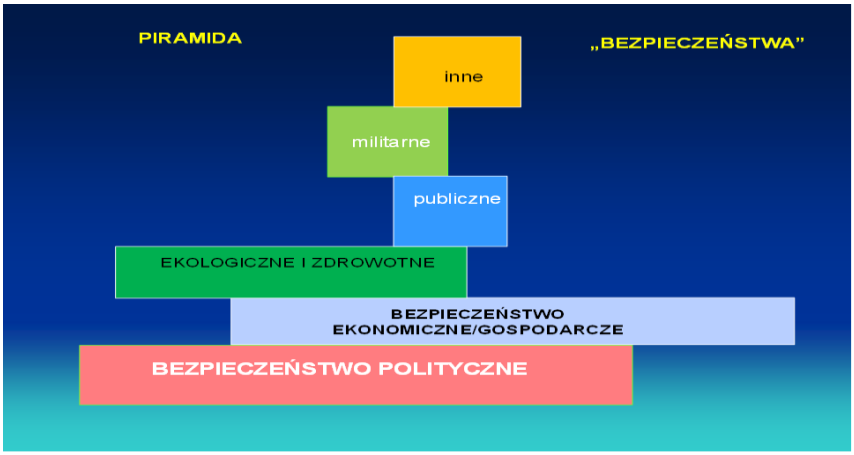
Inspiracją do kolejnych badań empirycznych mogą być także modele „piramidy bezpieczeństwa", prezentowane na rysunkach 2 i 3. Ukazują one usytuowanie względem siebie różnych przedmiotowych obszarów bezpieczeństwa, na co może mieć duży wpływ poziom kultury informacyjnej i kultury bezpieczeństwa informacyjnego podmiotów, których to dotyczy.

Rysunek 2. Bezpieczeństwo informacyjne w „piramidzie bezpieczeństwa" – model idealny

Źródło: opracowanie własne.

Prezentowany na rys. 2 model charakteryzuje podmiot(y) o wysokim poziomie kultury bezpieczeństwa, w tym także kultury informacyjnej i kultury bezpieczeństwa informacyjnego. *U podstaw* tego modelu znajduje się *bezpieczeństwo informacyjne*, na bazie którego mogą rozwijać się kolejne, przedmiotowe obszary bezpieczeństwa, zaczynając od ekologicznego i zdrowotnego, przez bezpieczeństwo ekonomiczne i polityczne oraz inne, ważne obszary bezpieczeństwa. Natomiast w sytuacji niskiego poziomu kultury informacyjnej i kultury bezpieczeństwa jakiegoś „podmiotu" model jego piramidy bezpieczeństwa może wyglądać tak, jak na rysunku 3.

Rysunek 3. Bezpieczeństwo informacyjne w „piramidzie bezpieczeństwa” – model realny



Źródło: opracowanie własne.

Porównując rysunki 2 i 3 nie trudno zauważyć, który z tych modeli charakteryzuje się większą stabilnością, trwałością i szeroko rozumianym bezpieczeństwem analizowanego podmiotu. Należy jednak zaznaczyć, że oba te modele opisują przypadki skrajne. Prawdopodobnie różne podmioty fizyczne i prawne będą bardziej realistycznie charakteryzowane przez modele pośrednie, lokujące się gdzieś między tymi, które przedstawiono na obu rysunkach. Ich usytuowanie na skali między ww. modelami będzie w dużym stopniu zależało od poziomu kultury informacyjnej i kultury bezpieczeństwa tych podmiotów. Do retorycznych należy więc pytanie, czy model przedstawiony na rysunku 3 charakteryzuje li tylko np. Koreę Północną, a model na rysunku 2 np. społeczeństwo szwajcarskie? W tym drugim społeczeństwie – obywatelskim – na edukację przeznacza się średnio około 20% PKB. W kraju tym dużą wagę przywiązuje się do procesu doskonalenia kultury bezpieczeństwa obywateli, szczególnie zaś kultury informacyjnej.

Wspomniano już wcześniej, że w procesie edukacji w Polsce problematyka kultury bezpieczeństwa dzieci i młodzieży, a w niej kultury informacyjnej, nie należą jeszcze do priorytetów. Być może zmieni się to w sytuacji, kiedy wiedza i konkretne fakty dotyczące *walki* i *wojny informacyjnej* szerzej dotrą do świadomości obywateli. Tymczasem zaś, nierzadko można mieć wrażenie, że informacje o tym, iż na początku stycznia 2017 roku Stany Zjednoczone wydaliły z USA 35 dyplomatów rosyjskich pod zarzutem wpływania przez nich na przebieg i wynik wyborów prezydenckich w tym kraju, traktuje się jako ciekawostkę. Jednocześnie duże zainteresowanie i wysoki poziom emocji budzą niezbyt ambitne seriale telewizyjne przeplatane informacjami o tym, że tzw. Państwo

Islamskie przyznało się do kolejnego aktu terrorystycznego, tym razem nad Bosforem, a sprawca tej tragedii zniknął jak „kamień w wodzie".

Bibliografia

Babik, W. (2016*) Kultura informacyjna a ekologia informacji współczesnego człowieka. Studium porównawcze*. W: Batorowska, H., Kwiasowski, Z. (red. nauk.), *Kultura informacyjna w ujęciu interdyscyplinarnym – teoria i praktyka*. T. 2. Kraków: Wydaw. UP im. KEN w Krakowie.

Batorowska, H. (2013) *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dorosłości informacyjnej.* Warszawa: Wydaw. SBP.

Beck, U. (2002) *Społeczeństwo ryzyka. W drodze do innej nowoczesności.* Warszawa: Wydawnictwo Naukowe Scholar.

Cieślarczyk, M. (2006) *Kultura bezpieczeństwa i obronności.* Siedlce: Wydaw. AP.

Cieślarczyk, M. (2015) *Kultura informacyjno-komunikacyjna jako element kultury bezpieczeństwa.* W: Batorowska, H. (red. nauk.), *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka.* T. 1. Kraków: Wydaw. UP w Krakowie.

Filipek, A. (2013) Kier. podzad. bad. nr 1.5. *Kultura bezpieczeństwa podmiotów jako element integrujący system bezpieczeństwa narodowego oraz regulujący jego funkcjonowanie i rozwój,* w ramach Projektu: *System Bezpieczeństwa Narodowego RP,* Projekt w zakresie obronności i bezpieczeństwa państwa finansowany ze środków Narodowego Centrum Badań i Rozwoju – umowa Nr DOBR/0076/R/ID1/2012/03, z dnia 18.12.2012 r., numer rejestracyjny projektu: O ROB/0076/03/001, Kierownik Projektu: prof. dr hab. inż. Waldemar Kitler, AON.

Frei, D. (1997) *Sichercheit. Grundfragen der Weltpolitik.* Stuttgard: verlag W. Kohlhammer.

Janczak, J., Nowak, A. (2013) *Bezpieczeństwo informacyjne. Wybrane problemy.* Warszawa: Wydaw. AON.

„Kultura bezpieczeństwa"*,* nr 3-4/2015, Siedlce: Wydaw. UPH.

Łuczak, J. (red.) (2004) *Zarządzanie bezpieczeństwem informacji.* Poznań: Oficyna Współczesna.

Materska, K. (2007) *Informacja w organizacjach społeczeństwa wiedzy.* Warszawa.

Streszczenie

Korzystając z założeń teoretycznych dotyczących ekologii informacji i kultury informacyjnej, a także kultury bezpieczeństwa i kultury bezpieczeństwa informacyjnego, autor artykułu podjął próbę wykorzystania tej wiedzy do interpretacji wybranych wyników badań empirycznych, ukazujących elementy kultury bezpieczeństwa i kultury informacyjnej podmiotów fizycznych i prawnych funkcjonujących w strukturach zarządzania kryzysowego na szczeblu podstawowym w różnych regionach Polski.

Słowa kluczowe: bezpieczeństwo, zarządzanie kryzysowe, ekologia informacji, kultura informacyjna, bezpieczeństwo informacyjne, kultura bezpieczeństwa informacyjnego.

Ecology of information, information culture and information security culture in theory and in practice

Abstract

Making use of a theoretical framework concerning *ecology of information* and *information culture* as well as *security culture* and *information security culture,* the author of the paper made an attempt to use such knowledge to interpret chosen results of empirical research presenting elements of *security culture* and *information culture* of natural and legal entities functioning in the structures of the crisis management at the basic level in various regions of Poland.

Keywords: security, the crisis management, ecology of information, information culture, security culture, information security culture.

Wiesław Babik
Uniwersytet Jagielloński w Krakowie

Ekologia informacji a bezpieczeństwo człowieka i informacji we współczesnym świecie

Bezpieczeństwo informacyjne i związane z nim zarządzanie należą do ważnych problemów współczesności. Bezpieczeństwo jest naszym podstawowym pragnieniem, które każdy z nas nosi w swoim sercu. Zdając sobie sprawę z wartości informacji we współczesnym świecie i uznając ją za zasób strategiczny państwa i każdej organizacji podjęcie się infoekologicznej refleksji nad zasygnalizowanym problemem bezpieczeństwa informacji w kontekście obecnej sytuacji człowieka funkcjonującego w cywilizacji informacyjno-technologicznej stanowi nie lada wyzwanie (Zawistowski 2011).

Ekologia informacji to nowe interdyscyplinarne pole (domena) badawcze dotyczące wzajemnych oddziaływań człowieka na informacje i odwrotnie, a także relacji informacyjnych między ludźmi w publicznej i prywatnej przestrzeni informacyjnej oraz wpływu na nie środowiska informacyjnego. Jej przedmiotem jest struktura i funkcjonowanie środowiska informacyjnego człowieka (Babik 2014). Ponieważ istnieje wiele zagrożeń środowiska informacyjnego, dlatego wymaga ono szczególnej ochrony. W granicach tej domeny badawczej znajduje się także bezpieczeństwo informacji, stąd szczególna uwaga zostanie skierowana na infoekologiczne aspekty bezpieczeństwa człowieka i informacji we współczesnym świecie oraz na potrzebę ich szczególnej ochrony.

Podejście infoekologiczne, które przyjęto w artykule za punkt widzenia na bezpieczeństwo informacji to podejście, które bazuje na relacjach człowieka z jego środowiskiem informacyjnym (Babik 2015). Ekologia informacji akcentuje wpływ na człowieka środowiskowych czynników informacyjnych i odwrotnie, a więc dotyczy relacji między człowiekiem a jego środowiskiem informacyjnym. Ekologiczne spojrzenie w nauce o informacji oznacza poszukiwanie w środowisku informacyjnym człowieka tych elementów i związków pomiędzy nimi, które dotyczą oddziaływania informacji na człowieka oraz odwrotnie, a także ochronę człowieka przed niekorzystnym oddziaływaniem informacji oraz ochronę samej informacji przed niszczycielskim działaniem człowieka (Babik 2012).

Zakres ekologii informacji określają m.in. następujące jej kluczowe zagadnienia: środowisko informacyjne człowieka, ekologiczne zarządzanie informacją, potrzeby informacyjne, bariery informacyjne, zachowania informacyjne, kultura informacyjna, etyka informacyjna, konsumpcja informacji, profilaktyka informacyjna, higiena informacyjna, ***bezpieczeństwo informacji,*** polityka informacyjna (Babik 2014, s. 110).

1. Bezpieczeństwo informacji – istota i cechy

Bezpieczeństwo informacyjne traktuję, za badaczami tego problemu, jako kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska informacyjnego, a także jego formowanie, wykorzystywanie i rozwój w interesie obywateli, organizacji i państwa. Obszarem dociekań naukowych i wymiany doświadczeń w zakresie bezpieczeństwa informacyjnego są nie tylko ludzie, informacja, procesy i technologie informacyjno-komunikacyjne, ale i sama infosfera narażona na ataki zarówno zamierzone, jak i nieświadome, infosfera w której toczy się nieustanna walka informacyjna. Jej obrona jest prowadzona także w przestrzeni permanentnej edukacji całego społeczeństwa.

Bezpieczeństwo informacji dotyczy w zasadzie wszystkich cech informacji, w tym takich, jak: relewantność, dokładność, aktualność, terminowość, kompletność, spójność, odpowiedniość formy, dostępność, jednoznaczność, wiarygodność, komunikatywność, rzetelność, elastyczność, nadmiarowość/ redundantność, użyteczność, złożoność, naturalność, zgodność semantyczna, zgodność strukturalna, weryfikowalność, zmienność, reputacja (Czerwiński, Krzesaj 2014, s. 49-50). Dotyczy też pełnionych przez informacje funkcji. Informacja to przecież towar, i to często o charakterze strategicznym, podstawowy element procesów biznesowych, narzędzie sterowania procesami w zautomatyzowanych systemach informacyjno-wyszukiwawczych (Hetmański 2015). Nic więc dziwnego, że informacja najczęściej bywa chroniona na mocy prawa lub zawartych umów (Klimek 2016).

Bezpieczeństwu informacji przypisuje się następujące atrybuty: poufność, autentyczność, dostępność, integralność (danych, systemu), rozliczalność, niezawodność (Białas 2007, s. 34). Składowymi bezpieczeństwa informacji są więc bezpieczeństwo fizyczne, bezpieczeństwo osobowo-organizacyjne, bezpieczeństwo teleinformatyczne i bezpieczeństwo prawne.

Informacja jest bardzo podatna na zniekształcenia. Ich przyczyny zwykle mają charakter:

- techniczno-organizacyjny (filtrowanie, selekcja, hamowanie, multiplikacja, kwantyfikacja, dyspersja informacji);
- socjologiczny i/lub psychologiczny (są związane z subiektywizacją informacji);
- strukturalny, tkwiący w infrastrukturze systemów informacyjnych (wzrost i rozmieszczenie źródeł informacji, rozproszenie i zróżnicowanie wartości informacji, ograniczenie możliwości przyswajania informacji, bariery informacyjne) (Górski 1997, s. 67-82).

Źródłem zagrożeń dla bezpieczeństwa informacji mogą być m. in.:

- mikrospołeczności z własnymi wizjami i porządkami;
- sytuacje typu „Jak podskoczysz, to wyskoczysz”;
- anonimowe, nieautoryzowane źródła informacji dostępne w sieci WWW;

- kłamstwo;
- negowanie wartości moralnych;
- zniekształcenia informacji;
- manipulowanie informacją;
- imputacja informacji;
- rynek informacyjny.

Zagrożenia dla bezpieczeństwa informacji następują m.in. na skutek:

- tworzenia/nadawania informacji przez osoby niekompetentne, nieobiektywne, nierzetelne;
- kierowania informacji do niewłaściwych odbiorców;
- manipulowania informacją;
- spowolnienia procesu docierania informacji do odbiorcy;
- niszczenia zaufania do informacji;
- relatywizacji prawdy i tzw. post-prawdy[1];
- deprecjacji postaw obywatelskich;
- ograniczania wolności i cenzury informacji;
- niedbałości o jakość informacji;
- populizmu;
- promowania konkretnej ideologii;
- obłudy nadawcy;
- emocjonalnego a nie racjonalnego traktowania informacji.

Szczególnie niebezpieczna jest manipulacja informacją nastawiona przede wszystkim na przekaz podprogowy. Często nawet, jeżeli nie zdajemy sobie z tego sprawy jesteśmy manipulowani, czy nam się to podoba, czy nie. Komunikat perswazyjny odbierany przez jego adresata u progu, a nawet poniżej progu świadomości ma na celu wywarcie ukrytego wpływu informacji na odbiorcę. W związku z tym niezbędne są: ostrożność w podchodzeniu do funkcjonowania istniejących systemów informacyjnych oraz stosowanie zasady ograniczonego zaufania.

W sytuacji jej zagrożeń, które mogą być spowodowane zarówno przez czynniki wewnętrzne (zjawiska językowe, zmiany funkcji i znaczenia), jak i czynniki zewnętrzne (zjawiska pozajęzykowe, starzenie się informacji) szczególnie ważna jest ochrona informacji. Ochrona informacji jako taka dotyczy przede wszystkim jej atrybutów: tajności, integralności, dostępności, rozliczalności, niezaprzeczalności, autentyczności (Liderman 2012, s. 19). Informacja niebezpieczna to informacja nieprawdziwa, która uprzedmiotawia człowieka. Informacja bezpieczna (zielona, green information), to informacja „czysta" (rzetelna), prawdziwa, obiektywna, kompletna.

2. Bezpieczeństwo człowieka funkcjonującego w cywilizacji informacyjno-technologicznej

Rozwój technologii sieci informacyjnych, w tym drastyczne zwiększenie szybkości przesyłania informacji oraz szerokie rozpowszechnianie usług sieciowych, głównie za sprawą Internetu, umożliwiły tworzenie się na bazie wymiany informacji różnego rodzaju społeczności oraz coraz powszechniejsze wykorzystywanie mechanizmów i działań związanych z manipulacją informacji za pomocą manipulacji językowych, manipulacji faktami i emocjami a także rodzenie się różnego rodzaju patologii informacyjnych. Zagrożenia bezpieczeństwa człowieka dotyczą zarówno zdrowia psychicznego i fizycznego, jak i sfery poznawczo-intelektualnej oraz moralnej (Bednarek 2014).

Poza Internetem to człowiek jest największym generatorem i depozytariuszem informacji i wiedzy. Niezbędna jest więc ciągła troska i ochrona znajdujących się w jego środowisku informacyjnym/otoczeniu informacji i wiedzy jako dobra ogólnoludzkiego. Informacja jest bowiem dobrem bardzo wrażliwym, o czym świadczą jej liczne cechy. Właśnie głównie ze względu na obecną sytuację człowieka w społeczeństwie informacyjnym bezpieczeństwo informacji staje się wyzwaniem współczesności. Szerokie i wieloaspektowe rozumienie bezpieczeństwa informacji w świecie obejmuje zarówno samych ludzi, jak i zbiory/zasoby informacji oraz dane/metadane a także usługi informacyjne.

W przedmiocie bezpieczeństwa informacji warto zwrócić uwagę na nadmiar informacji, który negatywnie wpływa na jakość i szybkość jej obiegu, a także na jakość tworzonych metainformacji oraz jakość i szybkość udostępniania i rozpowszechniania jej. Innym niebezpieczeństwem jest fragmentaryzacja informacji i wiedzy będąca skutkiem niepoprawnej lub opartej na jakiejś ideologii selekcji informacji, dezaktualizacja informacji w wyniku jej nieuaktualniania, czy deficyt informacji i wiedzy będący skutkiem zbyt wąskiej specjalizacji nadawcy/generatora informacji[2].

Działania w dziedzinie bezpieczeństwa i ochrony informacji powinny polegać na jej ochronie przed:

- nieuprawnionymi działaniami ludzi;
- błędami ludzkimi i organizacyjnymi;
- awariami sprzętu i wadami oprogramowania;
- skutkami katastrof i działań terrorystycznych.

Wśród środków zaradczych można wymienić:

- dbanie o równowagę informacyjną i zrównoważony rozwój środowiska informacyjnego;
- indywidualne zarządzanie informacją jako narzędzie obrony przed zagrożeniami w Sieci;
- duplikację informacji, ale bez nachalnej propagandy i reklamy.

Nadużyciom w tym przedmiocie przeciwdziała: etyka informacyjna, prawo informacyjne, etykieta informacyjna, edukacja informacyjna, kultura informacyjna, ekologia informacji. Niezbędnym czynnikiem i fundamentem bezpieczeństwa informacji w codziennym życiu jest kultura informacji (Kisilowska 2016), wzajemne zaufanie między ludźmi oraz zaufanie do informacji (Sztompka 2007).

3. Ekologia informacji narzędziem ochrony bezpieczeństwa informacji i człowieka

Ekologia informacji wychodzi naprzeciw współczesnym bolączkom szeroko pojętego procesu komunikowania się i oferuje rozwiązania sprzyjające optymalizacji tego procesu stosownie do potrzeb i możliwości użytkowników informacji (nadawców, pośredników i odbiorców). Za niezbędne uważa się stosowanie zasad profilaktyki, higieny i swoistego rodzaju diety informacyjnej oraz konieczność przewidywania skutków własnych decyzji w zakresie wpływania na homeostazę informacyjną swojego organizmu oraz innych. Kluczowym w działaniach na rzecz ekologii informacji jest zmiana mentalności/postaw i budowanie świadomości społecznej w tym przedmiocie.

Informacja z punktu widzenia teorii informacji jest bezpieczna, gdy:

- twórcami informacji są osoby kompetentne, obiektywne, rzetelne;
- jest „odporna" na różnego rodzaju zróżnicowane interpretacje;
- jest trudno podatna na zniekształcenia (np. informacja naukowa);
- nie jest „rozwlekła";
- jest zaopatrzona w kontekst;
- nie jest zbytnio nadmiarowa;
- jest odpowiednio zabezpieczona jej treść i forma;
- jest udostępniania/rozpowszechniana w odpowiedni sposób (na odpowiednim kanale);
- dociera do właściwego odbiorcy.

Ekologia informacji proponuje w tym zakresie działalność praktyczną polegającą na:

- oparciu polityki informacyjnej na odpowiednim/właściwym i jej szerokim rozumieniu;
- dbaniu o świadomość informacyjną człowieka jako istotnego elementu w procesach informacyjnych,
- ochronie człowieka przed jego uprzedmiotawianiem za pomocą informacji (manipulowanie);
- rozwijaniu kompetencji informacyjnych człowieka;
- wychowaniu/edukacji do odpowiedzialności za tworzenie/generowanie, przetwarzanie, rozpowszechnianie i wykorzystywanie informacji;
- równoważeniu rozwoju człowieka w świecie techniki, technologii i informacji;

- umiejętnym wykorzystywaniu informacji do budowania indywidualnej i zbiorowej wiedzy dla indywidualnego i wspólnego dobra ludzkości (Babik 2014, s. 138);
- zarządzaniu bezpieczeństwem informacji w środowisku informacyjnym człowieka.

Zarządzanie bezpieczeństwem informacji dotyczy w szczególności bezpiecznej realizacji procesów informacyjnych takich, jak:

- generowanie i pozyskiwanie informacji;
- gromadzenie i przechowywanie informacji;
- przetwarzanie informacji;
- udostępnianie, dystrybucja i rozpowszechnianie informacji.

Zarządzanie bezpieczeństwem informacji to przede wszystkim odpowiednie sterowanie przebiegiem wymienionych procesów informacyjnych mające na celu ich optymalizację.

4. Edukacja infoekologiczna w zakresie bezpieczeństwa informacji i człowieka we współczesnym świecie

W sytuacji występowania we współczesnym świecie takich tendencji, jak przechodzenie od cyfryzacji zasobów informacji do cyfryzacji społeczeństwa, zmiany paradygmatów edukacyjnych z ilościowych na jakościowe, ewolucji infrastruktury informatycznej społeczeństwa, nienadążania naszych możliwości za postępem naukowo-technicznym, budowanie społeczeństwa informacyjnego opartego na bezpiecznej informacji staje się ogólnoludzkim wyzwaniem XXI wieku. Analiza pojawiających się zagrożeń informacji skłania do tworzenia nowych programów edukacyjnych oraz profilaktycznych.

Odpowiednia edukacja i pielęgnowanie humanistycznych wartości to najskuteczniejsze sposoby przeciwdziałania zagrożeniom bezpieczeństwa informacji. Brak ładu moralnego i społecznego oraz napięcia powodowane przez wolny rynek i globalizację kapitału a nie wartości wymuszają ochronę informacji jako towaru. Informacja to przecież towar/produkt/wartość podlegający szczególnej ochronie. Niepokojącym zjawiskiem staje się fragmentaryzacja informacji i wiedzy. Niezbędnym jest więc wprowadzenie do edukacji takich wartości, jak poczucie, że jednostka jest częścią ludzkości, a nie tylko narodu, odejście od europocentryzmu, propagowanie tolerancji, chociaż jest to sprzeczne z neoliberalnym modelem ekonomicznym (Kwieciński 2010).

Ten nowy obszar edukacyjny pozwala na kształtowanie i doskonalenie kompetencji informacyjnych, kształtowanie świadomości społecznej nowych szans i zagrożeń dotyczących informacji oraz technologii jej generowania, rozpowszechniania i odbioru, co jest szczególnie ważne w związku z dynamicznym rozwojem technologicznych możliwości mediów cyfrowych i tworzeniem się zupełnie nowej jakości środowiska informacyjnego człowieka (Batorowska 2013).

Debata nad bezpieczeństwem informacji jest zjawiskiem stosunkowo nowym w polskiej edukacji i mediach. Jej celem powinno być m.in. pogłębione rozpoznanie i kompleksowy opis specyfiki współczesnych zagrożeń w dziedzinie informacji, co może mieć pozytywny wpływ na zaufanie i poczucie bezpieczeństwa dotyczącego cennych, wartościowych i użytecznych dla człowieka zasobów informacji i wiedzy (Materska 2007).

Podsumowanie

Zasygnalizowane w artykule wybrane problemy bezpieczeństwa informacyjnego wskazują m.in. na nową rolę i miejsce zachodzących obecnie przemian w świecie informacji, mających duży wpływ zarówno na samą informację, jak i funkcjonowanie człowieka w świecie informacji.

Bezpieczeństwo informacji to dla człowieka i współczesnego świata informacji ważny problem nie tylko o charakterze epistemologicznym (teoretyczny), ale też praktycznym. Nic więc dziwnego, że stał się on również jednym z ważnych problemów ekologii informacji. Bardzo pożytecznym byłoby więc wykorzystanie w działaniach na rzecz bezpieczeństwa informacji i człowieka we współczesnym świecie myśli teoretycznej i działań proponowanych przez ekologię informacji. Jej wymowa jest ponadczasowa i ma wymiar uniwersalny. Na drodze poszukiwania nowych sposobów funkcjonowania człowieka we współczesnym świecie informacja powinna stanowić swoistego rodzaju zwornik tworząc bezpieczne środowisko informacyjne będące miejscem spotkań dla ludzi, zbiorów danych i usług informacyjnych. Bezpieczeństwo informacji mogą zapewnić nie tylko konsekwentne i odważne decyzji dotyczące odpowiedniej ochrony danych i przestrzegania praw autorskich, lecz przede wszystkim świadomość odpowiedzialności za informacje i budowana na niej ekokultura informacji (Babik 2012), która pozwala unikać tzw. głupoty informacyjnej i powinna stanowić trwały punkt odniesienia dla działań informacyjnych człowieka i instytucji/organizacji. Powinniśmy być producentem bezpieczeństwa informacji a nie tylko jego konsumentem.

Przypisy

[1] Post-prawda to okoliczności, w których obiektywne fakty mają mniejszy wpływ na kształtowanie opinii publicznej niż odniesienia do emocji lub osobistych przekonań.

[2] Przykład zagrożenia bezpieczeństwa informacji (informacji w niebezpieczeństwie) o tym, że smog stanowi zagrożenie dla zdrowia człowieka może stanowić informacja/wypowiedź Ministra Zdrowia Konstantego Radziwiłła, że w Polsce smog to problem teoretyczny.

Bibliografia

Babik, W. (2015) *Bezpieczeństwo informacji w bibliotece w świetle ekologii informacji*. „Bibliotheca Nostra. Śląski Kwartalnik Naukowy", nr 4(42), s. 10-16.

Babik, W. (2014) *Ekologia informacji.* Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Babik, W. (2012) *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*. „Bibliotheca Nostra. Śląski Kwartalnik Naukowy", nr 2(28), s. 31-40.

Batorowska, H. (2013) *Od alfabetyzacji informacyjnej do kultury informacyjnej.* Warszawa: Wydawnictwo SBP.

Bednarek, J. (2014) *Społeczne kompetencje medialno-informacyjne w kontekście bezpieczeństwa w cyberprzestrzeni i świata wirtualnego.* W: Bednarek, J. (red. nauk.), *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*. Warszawa: Difin, s. 13-37.

Białas, A. (2007) *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie.* Warszawa: Wydawnictwo Naukowo-Techniczne.

Czerwiński, A., Krzesaj, M. (2014) *Wybrane zagadnienia oceny jakości systemu informacyjnego w sieci WWW*. Opole: Uniwersytet Opolski.

Górski, A. (1997) *Informacja naukowa na tle przeobrażeń procesów komunikacji społecznej i jako wyzwanie gospodarki rynkowej.* Szczecin: Uniwersytet Szczeciński.

Hetmański, M. (2015) *Świat informacji*. Warszawa: Difin.

Kisilowska, M. (2016) *Kultura informacji.* Warszawa: Wydawnictwo SBP.

Klimek, G. (2016) *Bezpieczeństwo informacji w perspektywie rozwoju Internetu rzeczy.* [W:] Czerwiński, A., Jańdziak, A., Krzesaj, M. (red. nauk), *Informacja – dobro publiczne czy prywatne?* Opole: Wydawnictwo Uniwersytetu Opolskiego, s. 153-162.

Kwieciński, M. (2010) *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane.* Kraków: Krakowskie Towarzystwo Edukacyjne. Oficyna Wydawnicza AFM.

Liderman, K. (2012) *Bezpieczeństwo informacyjne.* Warszawa: Wydawnictwo Naukowe PWN.

Materska, K. (2007) *Informacja w organizacjach społeczeństwa wiedzy.* Warszawa: Wydawnictwo SBP.

Sztompka, P. (2007) *Zaufanie fundament społeczeństwa*. Kraków: Wydawnictwo Znak.

Zawistowski, T. (2011) *Bezpieczeństwo informacji. Suplement.* Warszawa: Fundacja Rozwoju Demokracji Lokalnej.

Streszczenie

Zdając sobie sprawę z wartości informacji we współczesnym świecie i traktując ją jako zasób strategiczny państwa i każdej organizacji, wyeksponowano potrzebę zarządzania jej bezpieczeństwem, także w wymiarze bezpieczeństwa człowieka funkcjonującego w cywilizacji informacyjno-technologicznej.

Bezpieczeństwo informacyjne potraktowano, za badaczami tych problemów, jako kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska informacyjnego, a także jego formowanie, wykorzystywanie i rozwój w interesie obywateli, organizacji i państwa. Obszarem dociekań naukowych i wymiany doświadczeń w zakresie bezpieczeństwa informacyjnego należy uczynić nie tylko ludzi, procesy i technologie, ale i samą infosferę narażoną na ataki zarówno zamierzone, jak i nieświadome, infosferę w której toczy się nieustanna walka informacyjna. Obrona jej powinna być prowadzona także w przestrzeni permanentnej edukacji całego społeczeństwa.

Słowa kluczowe: bezpieczeństwo informacji, ekologia informacji, bezpieczeństwo człowieka

Information Ecology and the Security of Man and Information In the Present-Day World

Abstract

While realizing the value of information in the present-day world and recognizing information as a strategic resource of the state and each organization, has been stressed the need of information security management, also in the dimension of the security of man operating within information and technology civilisation.

Information security has been treated here, following the researchers of that issue, as a set of actions assuring the security of the information environment, as well as its building, use, and development in the interest of citizens, organization, and state. The area of research and exchange of experience on information security should include not only people, processes, and technologies, but also the infosphere exposed to both intended and involuntary attacks, the infosphere in which an incessant information battle continues. The

defence of infosphere should also be conducted in the area of permanent education involving the society at large.

Keywords: information security, information ecology, security of man

Agnieszka Filipek
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Rola edukacji w kształtowaniu kultury bezpieczeństwa informacyjnego

Edukacja to dziedzina społecznego funkcjonowania, która w sposób profesjonalny przygotowuje do życia zarówno młodsze, jak i starsze pokolenia. Celem istnienia systemu edukacyjnego jest dostarczanie wiedzy i umiejętności dzieciom, młodzieży oraz dorosłym, służących ich aktywnemu funkcjonowaniu w społeczeństwie. Wydaje się, iż współczesny świat rysuje potrzebę, aby wśród zadań edukacyjnych pojawiły się także, chociaż podstawowe aspekty kultury informacyjnej, a także kultury bezpieczeństwa informacyjnego.

Informacje i korzystnie z nich w XXI wieku

Informacje są elementami rzeczywistości, które warunkują sprawne i efektywne funkcjonowanie różnorodnych podmiotów. Dotyczy to zarówno tych podmiotów, które informacje publikują, jak i tych, które ich poszukują, a także tych, które je wykorzystują. Współczesny świat generuje niespotykaną dotychczas ilość informacji. Każdy podmiot mający związek z informacją, zazwyczaj liczy na osiąganie dzięki niej pozytywnych zmian. Sytuacja taka powinna sprzyjać pozytywnym przeobrażeniom i rozwojowi zaangażowanych podmiotów. Nie zawsze jednak wszystkie włączone podmioty korzyści takie osiągają. Zdarza się bowiem i tak, że jeśli jeden z nich osiąga „profity", to dla innego bądź dla innych rysuje się strata. Można przypuszczać, że do rzadkości należą sytuacje, których konsekwencją jest uszczerbek dla wszystkich stron uczestniczących w pojawiających się przekazach. Umiejętność klasyfikowania nadawanych i napływających informacji w kontekście wartościowania ich jest złożonym procesem dla wszystkich uczestników procesów komunikacyjnych. Selekcjonowanie różnego rodzaju przekazów jest niezbędne w sytuacji ich systematycznego napływu. Koncentrowanie się na wszelkiego rodzaju danych nie jest możliwe, a pominięcie wartościowych komunikatów może przynosić niebagatelne straty. Edukacja ma w tym zakresie aktualnie wiele do zrobienia. Przygotowanie do kompetentnego korzystania z mnogości napływających informacji jest ważną kwestią we współczesnym świecie. Najprawdopodobniej, nawet jeśli takie zagadnienia są realizowane, to nie poświęca się im zbyt dużo czasu. A wydaje się, że ten typ edukacji, który warto traktować jako ważny aspekt kultury bezpieczeństwa informacyjnego, może ułatwić funkcjonowanie młodego człowieka, a także całych grup społecznych w coraz bardziej złożonej rzeczywistości XXI wieku. Dlatego też poważnym wyzwaniem dla współczesnej szkoły może być systematyczne kształtowanie kultury informacyjnej oraz kultury

bezpieczeństwa informacyjnego, której ważnym elementem będzie kwalifikowanie napływających informacji jako istotnych bądź nieistotnych, prawdziwych bądź nieprawdziwych, sprzyjających lub nie rozwojowi podmiotu wraz z jego środowiskami: społecznym, naturalnym, kulturowym i informacyjnym (Cieślarczyk 2009, s. 74-79). Należy w tym miejscu nadmienić, że kulturę bezpieczeństwa informacyjnego traktuję jako składnik kultury bezpieczeństwa.

Kultura bezpieczeństwa jako wyzwanie

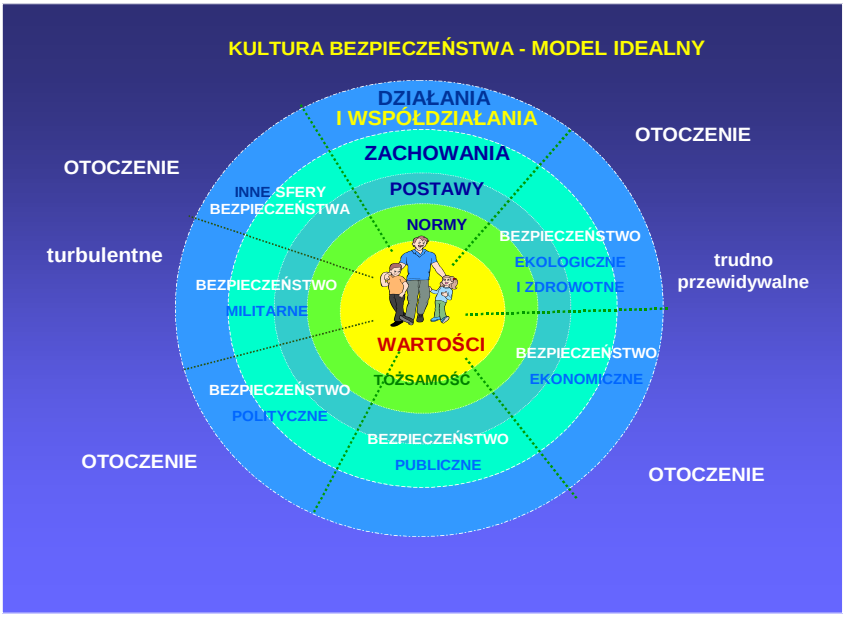
Określenie „wyzwanie" jest w literaturze interpretowane w sposób dość spójny. Michał Huzarski określa wyzwanie jako *sytuację nową i trudną, wymagającą określonego odzewu i podjęcia stosownych działań.* […] *Wyzwanie jest bowiem sygnałem do podjęcia stosownych działań* […] (Huzarski 2009, s. 22). J. Wojnarowski, uważa, że *wyzwania z natury swojej nie są ani dobre, ani złe. Dobrze spożytkowane stanowią szansę dla dalszego rozwoju, a źle wykorzystane lub niepodjęte mogą powodować zagrożenia i doprowadzić do kryzysu w rozwoju czy działaniu człowieka, systemu* (Wojnarowski 2005, s. 11). M. Cieślarczyk także twierdzi, iż: *„wyzwanie" jest pojęciem najszerszym, kryje w sobie zarówno szanse jak i zagrożenia.* Uzasadnia, że: *wyzwanie to określona sytuacja lub informacja o tej sytuacji, która właściwie odczytana i zinterpretowana może stać się szansą. Oczywiście tylko wtedy, kiedy dzieje się to w odpowiednim miejscu i we właściwym czasie. W przeciwnym razie wyzwanie może stać się zagrożeniem.* […] *Chodzi również o to, aby po rozpoznaniu i odczytaniu wyzwania podjąć odpowiednie działania i współdziałania. Odpowiednie – to znaczy adekwatne do potrzeb, we właściwym miejscu i we właściwym czasie oraz we właściwy sposób. Wyzwanie może stać się zagrożeniem wtedy, kiedy nie zostało zauważone (i) lub niewłaściwie odczytane, zinterpretowane. Również wtedy, kiedy związane z wyzwaniem działania nie zostały w ogóle podjęte (jest to tzw. grzech zaniechania) albo podjęto je zbyt późno, czy też nieadekwatnie do potrzeb* (Cieślarczyk 2006, s. 119-120). Powyższe wyjaśnienia pozwalają stwierdzić, że wyzwania to niełatwe sytuacje, które w porę dostrzeżone, właściwie zinterpretowane i powodujące mobilizację do właściwych działań w odpowiednim czasie, mogą doprowadzić do korzystnych zmian – szans. Brak zrealizowania choćby jednej z wymienionych przesłanek, kształtujących daną szansę, może powodować, że ostatecznie wyzwanie przeobrazi się w zagrożenie.

Przybliżenie wyjaśnienia kategorii „wyzwanie", pozwala na odniesienie tego sformułowania do kultury bezpieczeństwa, a także do aspektów związanych z edukacją w sferze informacyjnej. Te w pewien sposób wiążące się ze sobą elementy nie są najwyżej ocenianymi płaszczyznami funkcjonowania społeczeństwa (Filipek 2008, 2013). Ciągle zatem jest wiele do zrobienia w tych kwestiach.

Kulturę bezpieczeństwa postrzegam w sposób zaproponowany przez M. Cieślarczyka. Uczony konstruując wyjaśnienie sensu tego zagadnienia, w centrum modelu opisującego je umieścił wątek „wartości", które stanowią rdzeń i sedno dla pozostałych elementów kultury bezpieczeństwa. Badacz stwierdza, że *dla przybliżenia zagadnienia kultury bezpieczeństwa, a właściwie ukazania relacji między bezpieczeństwem, obronnością i kulturą bezpieczeństwa można skorzystać z metafory drzewa. Jeśli bezpieczeństwo porównamy do owoców drzewa, to obronność może przypominać konary, na których te owoce rosną. Zaś kulturę bezpieczeństwa moglibyśmy wyobrazić sobie jako korzenie i pień drzewa"* (Cieślarczyk 2004, s. 145). *Jakość tych „owoców" zależy w dużym stopniu od pnia drzewa i jego korzeni, ale także od podłoża, z którego drzewo wyrasta i w którym jest ukorzenione. „Podłoże" to składa się z takich składników, jak: kultura ekologiczna i zdrowotna, kultura ekonomiczna i polityczna, kultura życia publicznego, kultura organizacyjna i kultura prawna, kultura informacyjno-komunikacyjna i wiele innych. Ich nie najwyższą jakość można zauważyć w różnych sferach życia, w różnych obszarach bezpieczeństwa* (Cieślarczyk i in. 2014, s. 23-24).

Rysunek 1 przedstawia model idealny kultury bezpieczeństwa podmiotu wraz z jego elementami. Można go porównać do wnętrza struktury pnia drzewa – układu jego słojów – z którego wyrastają konary i owoce.

Rysunek 1. Podmiot i jego elementy kultury bezpieczeństwa w modelu idealnym



Źródło: (Cieślarczyk 2009, s. 160).

Kultura bezpieczeństwa *to wzór podstawowych założeń, wartości, norm, reguł, symboli i przekonań charakterystycznych dla danego* ***podmiotu****, wpływających na sposób postrzegania przez niego wyzwań, szans i (lub) zagrożeń w bliższym i dalszym otoczeniu, a także sposób odczuwania bezpieczeństwa i myślenia o nim* […] *oraz związany z tym sposób zachowania i działania (współdziałania), w różny sposób przez ten podmiot „wyuczonych" i wyartykułowanych, w procesach szeroko rozumianej edukacji, w tym również w naturalnych procesach wewnętrznej integracji i zewnętrznej adaptacji oraz w innych procesach organizacyjnych* […]*, a także w procesie umacniania szeroko (nie tylko militarnie) rozumianej obronności* […]*, służących w miarę harmonijnemu rozwojowi tego podmiotu i osiąganiu przez niego najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie, ale i dla otoczenia* (Cieślarczyk 2009, s. 157).

Zarówno rysunek jak i wyjaśnienie opisowe pozwalają dostrzec, że w modelu idealnym kultura bezpieczeństwa opiera swe istnienie na holistycznym postrzeganiu różnych przedmiotowych wymiarów bezpieczeństwa i hierarchicznym ich klasyfikowaniu w konkretnych wymagających tego sytuacjach w oparciu o uznawany układ wartości. Kultura bezpieczeństwa pomaga zatem odnaleźć słuszną drogę rozwoju, biorącą pod uwagę wszystkie przedmiotowe wymiary bezpieczeństwa. Kierowanie się takim całościowym spojrzeniem, niepomijającym wymiaru informacji, może przyczyniać się do formowania wyższego poziomu kultury bezpieczeństwa informacyjnego oraz korzystniejszego standardu bezpieczeństwa w ogóle.

Kultura informacyjna, kultura bezpieczeństwa informacyjnego i bezpieczeństwo informacyjne

Kultura informacyjna to zagadnienie interdyscyplinarne. Kultura jest pojęciem, które dotyczy człowieka, a różnego rodzaju komunikaty z kolei odnoszą się do różnych sfer życia człowieka. Literatura prezentuje odrębne wyjaśnienia pojęcia „kultura informacyjna". W. Babik opisuje, kulturę informacyjną jako *przejaw wiedzy dotyczący istoty informacji i jej funkcji, świadomości roli i znaczenia informacji, jako poprawne posługiwanie się terminologią z zakresu informacji, właściwe interpretowanie i wykorzystanie informacji, poszanowanie jej, odpowiednie gromadzenie, przechowywanie i udostępnianie informacji* (Babik 2016, s. 48). H. Batorowska z kolei wyjaśnia, że *kultura informacyjna jest zawsze ściśle związana z użytkownikiem informacji. Odnoszą się do niej także cechy wspólne, które przypisują kulturze badacze reprezentujący różne dyscypliny wiedzy, np. bycie zbiorem zjawisk wyuczonych przekazywanych w procesie wychowania i uczenia się, a nie na drodze biologicznego dziedziczenia; bycie zjawiskiem społecznym, bycie aparatem adaptacyjnym człowieka i pełnienie*

funkcji pośrednika między nim a środowiskiem, w którym żyje (Batorowska 2013, s. 59).

Kultura informacyjna jest więc zagadnieniem, które w dużej mierze dotyczy sposobów posługiwania się informacją w celu komunikacji z innym jej użytkownikiem. Różny poziom kultury informacyjnej będzie miał istotne znaczenie dla sposobów konstruowania informacji, jej przekazywania, przechowywania i odbierania docierających oznajmień. Może on również wpływać na postrzeganie wielu innych cech osoby zaangażowanej w konkretny obieg informacyjny. Sposób konstruowania jakiejkolwiek informacji, a także posługiwanie się nią, zawsze jest wizytówką autora bądź pośrednika. Problematyka ta jest istotna z punktu widzenia wszystkich dziedzin życia, gdyż każda z nich zawiera w sobie specyficzny obieg informacji. Można wręcz stwierdzić, że kultura informacyjna jest elementem spajającym różne wymiary życia, poprzez przenikanie ich jakby „w poprzek", dzięki czemu łączy je w całość. Taki status kultury informacyjnej powoduje, że wpływa ona w sposób znaczący na poziom rozwoju podmiotu, który daną kulturę reprezentuje oraz na jego innowacyjność funkcjonowania. Użyte sformułowania takie jak rozwój i innowacyjność kierunkują naszą uwagę w stronę przemyśleń dotyczących spostrzeżenia, iż kultura informacyjna może mieć znaczenie dla bezpieczeństwa informacyjnego danego podmiotu, może nawet stanowić o kształcie jego obronności w tym wymiarze.

Same umiejętności dotyczące konstruowania informacji, interpretowania ich, przekazywania, gromadzenia i przechowywania mogą być niewystarczające, aby w pełni zagościło bezpieczeństwo informacyjne. Na pewno ważnym elementem uzupełniającym w tym zakresie kulturę informacyjną jest zagadnienie „wychowania informacyjnego" zaproponowane przez W. Furmanka (Furmanek, 2004, s. 145). Ważnym uzupełnieniem wymienionych kwestii, mających znaczenie dla osiągania bezpieczeństwa, może być także kultura bezpieczeństwa informacyjnego, stanowiąca komponent kultury bezpieczeństwa.

Ogólnie rzecz biorąc o kulturze bezpieczeństwa informacyjnego danego podmiotu prawdopodobnie będzie świadczyła umiejętność odróżniania informacji fałszywych od prawdziwych oraz korzystania z tych informacji pod względem pożyteczności i przydatności w oparciu o wartości będące treścią życia. Ważne będzie, aby po kontakcie z daną informacją, jak najwcześniejszej doprowadzić do jej selekcji pod względem przedstawiania prawdy, a także wiarygodności źródła, z którego pochodzi, jak również istotne będzie ustalenie aktualności danych i kategoryzowanie podanych „newsów" pod względem akceptowanych wartości. Odniesienie do wartości może polegać na tym, aby skonfrontować, czy posługiwanie się daną informacją i korzystanie z jej treści służy ogólnie pojętemu dobru w oparciu o uznawane wartości i sprzyja osiąganiu szeroko rozumianego bezpieczeństwa przez zaangażowane podmioty oraz ich środowiska. Spójnik „oraz" w tym ostatnim stwierdzeniu jest użyty w sposób nieprzypadkowy. Tego

typu koniunkcja jest niezbędna, aby podmiot mógł funkcjonować w sposób „prawidłowy". Najbardziej prawdopodobne jest bowiem, że w zdrowych środowiskach kształtują się zdrowe podmioty. Nieprostym zadaniem jest jednak, szczególnie we współczesnym świecie, formowanie takich osobowości. Zwracał na to już uwagę Andrzej Targowski, pisząc iż *współczesne plagi cywilizacji zachodniej, takie jak samobójstwa młodych osób, nadużywanie narkotyków oraz przestępczość są zwykle tłumaczone w kategoriach personalnych, społecznych oraz ekonomicznych. Mówi się o braku pracy, biedzie, wykorzystywaniu nieletnich, rozpadzie rodzin itp. Jednakże autor sugeruje, że trendy tylko do pewnego stopnia zależą od tych czynników. Wynikają raczej z braku sensu znaczenia celu życia oraz konstrukcji systemu wartości. Ludzie muszą w coś wierzyć i dla czegoś żyć. Czując, że są częścią społeczności, systemu wartości, mają poczucie duchowego spełnienia się – to jest sens relacji i istnienia na świecie oraz wartości uniwersalnych, w których istnieją. Społeczeństwo samoutrzymujące się powinno zrobić następny krok w kierunku rozwoju społecznego i zorientować się na wartości, takie jak rodzina, normy oraz życie duchowe. Innymi słowy, musimy wymyślić kulturę, w której takie działania mogą być realizowane* (Targowski 2004, s. 40). Powyższa wytyczna skłania do przemyśleń związanych z praktycznym odniesieniem do kultury bezpieczeństwa w ujęciu M. Cieślarczyka, koncentrującej się wokół wartości. Wartości przy wykorzystywaniu informacji mogą odgrywać bowiem bardzo znaczącą rolę. Być może bez kultury bezpieczeństwa informacyjnego trudne będzie dążenie do bezpieczeństwa informacyjnego.

Przechodząc do interpretacji określenia bezpieczeństwo informacyjne warto skorzystać z dotychczas opracowanych wyjaśnień. Zdaniem K. Liedla, *na przełomie XX i XXI wieku obserwujemy wzrost wagi kolejnej, informacyjnej płaszczyzny bezpieczeństwa narodowego – bezpieczeństwa informacyjnego, które razem z bezpieczeństwem ekonomicznym staje się priorytetowym aspektem bezpieczeństwa narodowego*" (Liedel 2006, s. 17). Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej wyjaśnia, że *bezpieczeństwo informacyjne państwa staje się nową dziedziną całościowego systemu bezpieczeństwa narodowego. Wprowadza standardy ochrony danych i informacji oraz dobór środków i parametrów technicznych procesu przetwarzania w zależności od wymaganego stopnia poufności. Dotyczy to także bezpieczeństwa informacji przetwarzanych w strategicznych gałęziach życia kraju, takich jak przemysł, bankowość, telekomunikacja, energetyka oraz ochrona zdrowia.* (*Biała Księga BN RP* 2013, s. 71). Powyższe wyjaśnienia zagadnienia „bezpieczeństwo informacyjne" wskazują, że jest ono, podobnie jak kultura informacyjna, istotne z punktu widzenia różnych wymiarów życia i wiąże się z problematyką zaufania. Bezpieczeństwu informacyjnemu nieobojętne są zarówno informacje mające obieg w postaci dokumentów papierowych, elektronicznych, czy też np. w formie filmów lub innych nośników. Bardzo prawdopodobne zatem jest, że

bezpieczeństwo informacyjne danego podmiotu, jest konsekwencją charakterystycznej dla niego kultury bezpieczeństwa informacyjnego, stanowiącej ważny składnik bezpieczeństwa.

Poszukiwanie, znajdowanie i realizowanie wspólnych wartości może stanowić mocny fundament dla budowania społeczności pełnych wzajemnych więzi, jedności i integracji. Takie zespolenie z kolei może pomagać we współpracy, współdziałaniu i realizowaniu założeń synergii. Reintegracja współczesnych społeczeństw wokół elementów niematerialnych np. akceptowanych wartości, jest czynnikiem, który stwarza szansę ukazania sensu życia tym, którym go brakuje. Analizowanie napływających informacji pod kątem znaczenia dla podmiotu w kontekście wartości i na podstawie tego konstruowanie własnych działań może pozytywnie wpływać na bezpieczeństwo nie tylko danego podmiotu, ale także na bezpieczeństwo jego środowisk. Takie postępowanie będzie świadczyło o korzystnej kulturze bezpieczeństwa informacyjnego tegoż podmiotu.

Kultura bezpieczeństwa informacyjnego może być zatem postrzegana jako umiejętność skupiania się i poszukiwania odpowiedzi na pytania dotyczące tego, czy wykorzystywanie i posługiwanie się daną informacją, opieranie się na niej, będzie służyło bezpieczeństwu tego podmiotu i innych podmiotów: czy będzie pozytywnie oddziaływało na ich otoczenie, czy też będzie mogło powodować jego degradację. Istotne wsparcie dla tego typu analiz stanowić może właśnie odniesienie do wartości, norm i zasad. Wartościowanie znaczenia poszczególnych aspektów otrzymanej informacji w kontekście posiadanej hierarchii wartości, np. opierającej się na piramidzie bezpieczeństwa (Cieślarczyk 2009 s. 151), będzie wyznacznikiem dla korzystania z niej i konstruowania w oparciu o nią przyszłości bądź posłuży zignorowaniu tejże informacji. O charakterze kultury bezpieczeństwa informacyjnego będą świadczyły konkretne wybory sposobów postępowania, w oparciu o docierające informacje, realizowane przez podmiot zgodnie z porządkiem wartości bądź sprzecznie z nim. Są to zatem kwestie w dużej mierze związane z wychowywaniem. Z kolei poziom kultury bezpieczeństwa informacyjnego będzie przejawiał się w zdolności precyzyjnego i szybkiego selekcjonowania pojawiających się informacji pod względem przedstawiania prawdy, wiarygodności źródła, z którego pochodzi, poprzez np. potwierdzanie w innych źródłach, jak również istotne będzie ustalenie aktualności danych. Poziom kultury bezpieczeństwa informacyjnego zatem wiąże się z kwestiami technicznymi, stanowiącymi efekt nauczania. Ogólnie rzecz biorąc wysoko ocenianej kulturze bezpieczeństwa informacyjnego powinna towarzyszyć nieobojętność na inne wymiary przedmiotowych kultur bezpieczeństwa, jak np. kultura bezpieczeństwa zdrowotnego, czy kultura bezpieczeństwa ekologicznego itd. Dostrzeganie rangi i znaczenia przedmiotowych wymiarów bezpieczeństwa, w kontekście pojawiających się informacji i uwzględnianie ich wartości może tylko pozytywnie służyć dążeniu do zrównoważonego rozwoju i bezpieczeństwa.

Oznacza to, że wykorzystywaniu otrzymywanych informacji nie powinna towarzyszyć próżność i snobizm w kwestii korzyści dla jednego podmiotu czy jednego wymiaru bezpieczeństwa. Ujawnianie się takich cech będzie świadczyło o zuchwałości podmiotu i jego zarozumiałości. Własności te nie są charakterystyczne dla podmiotów skłaniających się ku wartościom uniwersalnym, o potrzebie których pisał A. Targowski. Warto zatem przypomnieć, że korzystanie z otrzymywanych informacji, przy wysokiej kulturze bezpieczeństwa informacyjnego, nie może odbywać się kosztem szkód w sferze szeroko rozumianego bezpieczeństwa i poszczególnych jego wymiarów. Atrakcyjność wykorzystania informacji powinna być czytelna nie tylko dla jednego wymiaru bezpieczeństwa, podmiotowego czy też przedmiotowego, ale powinna być także analizowana pod kątem jej znaczenia dla innych płaszczyzn bezpieczeństwa zarówno nadawców informacji, jak i jej odbiorców. Najkorzystniejszą byłaby sytuacja, gdyby bilans rozpowszechnianych informacji mógł wyrażać się bez wyróżniania przegranych i wygranych, a każdy uczestnik procesu komunikacyjnego mógłby czerpać profity. Dużą przysługę w kwestii pojawiania się tego rodzaju sytuacji może oddać system edukacyjny poprzez uwzględnianie istotnych elementów kultury informacyjnej i kultury bezpieczeństwa informacyjnego.

Edukacja w kształtowaniu kultury bezpieczeństwa informacyjnego

Systematyczne kształtowanie kultury bezpieczeństwa nie jest w szkolnictwie aktualnie zbyt popularnym sposobem edukowania. Kultura bezpieczeństwa informacyjnego dopiero rozpoczyna swoje teoretyczne funkcjonowanie. Krzewienie tego typu treści i umiejętności w społeczeństwie nie jest sprawą łatwą. Konieczne jest przede wszystkim wypracowanie chęci do współpracy i kooperacji w tym zakresie. Gdyby formalnie takie możliwości zaistniały niezbędne byłoby oddziaływanie zarówno na sferę kierunkową, jak i instrumentalną osobowości ucznia, człowieka (Więckowski 1998, s. 37). Sfera kierunkowa odpowiada za to, że wybieramy i konsekwentnie realizujemy postawy wobec przyjętej hierarchii wartości. Tu mieszczą się cechy, które powodują, że chcemy tak, a nie inaczej działać i podtrzymywać to działanie. Bez chęci trudno jest realizować jakiekolwiek założenia. Potrzebna jest motywacja i wytrwałość. Oddziaływanie na tę sferę będzie przejawiało się przede wszystkim w wychowywaniu. Sfera instrumentalna z kolei ma w swoim zakresie wpływanie na wiedzę, umiejętności, nawyki sprawnościowe, czyli zawiera się w niej to wszystko, co możemy zrobić, aby uczeń potrafił, umiał dane zadanie wykonać. Ten typ oddziaływań należy zakwalifikować jako nauczanie.

Dzięki przybliżeniu powyższych założeń teoretycznych zarysowano sposób kształtowania zarówno charakteru, jak i poziomu kultury bezpieczeństwa, także informacyjnego. Ważnymi wyznacznikami kultury bezpieczeństwa informacyjnego

mogą zatem być: opieranie się na utrwalonym, akceptowanym, ogólnoludzkim systemie wartości w kwestii przekształcania rzeczywistości w oparciu o otrzymywane informacje. Takie postępowanie pomoże osiągać stan równowagi poszczególnym jednostkom i może przysłużyć się także do osiągania zrównoważonego rozwoju przez podmioty wieloosobowe. Edukacja w kwestii poziomu kultury bezpieczeństwa informacyjnego może koncentrować się na podwyższaniu kwalifikacji dotyczących zdolności precyzyjnego i szybkiego selekcjonowania pojawiających się informacji pod względem przedstawiania prawdy i wiarygodności źródła, z którego one pochodzą. Służyć temu będzie np. potwierdzanie w innych źródłach, podobnie jak również istotne będzie ustalenie aktualności danych.

Najpełniejsze oddziaływanie na sfery osobowości człowieka istotne z punktu widzenia wychowania i nauczania ma środowisko rodzinne. Środowisko to najsilniej wpływa na człowieka w wieku dziecięcym. Okres ten jest równocześnie czasem, kiedy kształtuje się podstawowy zarys później utrwalanego poziomu i charakteru kultury bezpieczeństwa. Oprócz domu rodzinnego znaczący wpływ na kształt osobowości dziecka ma wypełnianie obowiązku szkolnego. Dobrze byłoby, aby w coraz bardziej świadomy sposób podczas realizowania edukacji szkolnej, była formowana kultura bezpieczeństwa dzieci i młodzieży, a także jej ważny element: kultura bezpieczeństwa informacyjnego. W społeczeństwie niezbędni są reprezentanci przejawiający wysoką kulturę informacyjną i kulturę bezpieczeństwa informacyjnego, aby mogli swą wiedzę i umiejętności wykorzystywać w celu realizowania założeń zrównoważonego rozwoju i podnoszenia poziomu bezpieczeństwa.

Bibliografia

Babik, W. (2016) *Kultura informacyjna a ekologia informacji współczesnego człowieka.* W: Batorowska, H., Kwiasowski, Z. (red. nauk.), *Kultura informacyjna w ujęciu interdyscyplinarnym*. *Teoria i praktyka*. T. II. Kraków: UP, IBiEO, KKIiZI.

Batorowska, H. (2013) *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*. Warszawa: Wydaw. SBP.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2013). Warszawa: Biuro Bezpieczeństwa Narodowego.

Cieślarczyk, M. (2004) *Kultura bezpieczeństwa – kilka refleksji o charakterze teoretyczno-metodologicznymi edukacyjnym*. W: Ożóg-Radew, M., Rosa, R. (red. nauk.), *Bezpieczeństwo i prawa człowieka*. T. 1. *Teoretyczne aspekty bezpieczeństwa i praw człowieka*. Siedlce: Wydaw. Akademii Podlaskiej.

Cieślarczyk, M. (2006) *Kultura bezpieczeństwa i* obronności. Siedlce: Wydaw. Akademii Podlaskiej.

Cieślarczyk, M. (2009) *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa.* Siedlce: Wydaw. Akademii Podlaskiej.

Cieślarczyk, M., Filipek, A., Świderski, A. W., Ważniewska, J. (2014) *Istota kultury bezpieczeństwa i jej znaczenie dla człowieka i grup społecznych.* „Kultura Bezpieczeństwa", nr 1/2, s. 17-57.

Filipek, A. (2008) *Poziom i charakter kultury bezpieczeństwa młodzieży akademickiej*. Siedlce: Wydaw. Akademii Podlaskiej.

Filipek, A. (2013) Raport z badań w realizacji zadania 1.5 w ramach Projektu „System Bezpieczeństwa Narodowego RP", projekt w zakresie obronności i bezpieczeństwa państwa finansowany ze środków Narodowego Centrum Badań i Rozwoju – umowa Nr DOBR/0076/R/ID1/2012/03 z dnia 18.12.2012 r., numer rejestracyjny projektu: O B/0076/03/001, Kierownik Projektu: prof. dr hab. inż. Waldemar KITLER, Warszawa AON.

Furmanek, W. (2004) *Wybrane problemy teleologii edukacji informacyjnej.* W: Furmanek, W., Piecuch, A. (red.), *Dydaktyka informatyki. Problemy teorii*. Rzeszów: Wydaw. Uniwersytetu Rzeszowskiego, s. 143-154.

Huzarski, M. (2009) *Zmienne podstawy bezpieczeństwa i obronności państwa*. Warszawa: Wydaw. Akademii Obrony Narodowej.

Liedel, K. (2006) *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Toruń: Adam Marszałek.

Targowski, A. (2004) *Społeczeństwo informacyjne. Właściwości i klasyfikacje.* „Zeszyty Naukowe AON", nr 1 (54), s. 23-64.

Wojnarowski, J. (2005) *System obronności państwa. Materiały do studiowania*. Warszawa: Akademia Obrony Narodowej.

Więckowski, R. (1998) *Pedagogika wczesnoszkolna.* Warszawa: Wydawnictwa Szkolne i Pedagogiczne.

Streszczenie

Bezpieczeństwu informacyjnemu sprzyja korzystne oddziaływanie kultury informacyjnej oraz kultury bezpieczeństwa informacyjnego. Dążenie do osiągania tych ważnych kwestii nie jest zadaniem łatwym. Tekst zawiera przemyślenia

dotyczące możliwości korzystnego wpływania na wspomniane czynniki w oparciu o edukację. Kształtowanie ich będzie sprzyjać także zrównoważonemu rozwojowi.

Słowa kluczowe: kultura informacyjna, kultura bezpieczeństwa informacyjnego, edukacja

The role of education in shaping information security culture

Abstract

Information security benefits from the influence of information culture and information security culture. The endeavour to achieve such important matters is not an easy task. The paper contains the reflections on the possibilities of the influence of education over the abovementioned factors. Their shaping will be also beneficial to sustainable development.

Keywords: information culture, information security culture, education

Hanna Batorowska
Uniwersytet Pedagogiczny w Krakowie

Analityk w środowisku walki o dominację i przetrwanie

Analityk informacji – profesja w czasach permanentnej walki informacyjnej

Analityk jest zawodem, na który – w czasach nadmiarowości informacji i przyspieszenia technologicznego, w czasach traktowania informacji jako zasobu strategicznego oraz narzędzia walki informacyjnej – będzie coraz większe zapotrzebowanie nie tylko decydentów z sektora polityki, obronności, gospodarki, biznesu, służb specjalnych i policji, nauki i kultury, ale i zwykłych obywateli stojących przed problemem wyboru i podjęcia decyzji w sprawach bankowych, zdrowotnych, edukacyjnych, konsumpcyjnych, a nawet rozrywki i wypoczynku. I oni w sytuacji stresu informacyjnego spowodowanego pośpiechem i nadmiarowością produktów, usług, parametrów, faktów oraz niemożnością podjęcia samodzielnego wyboru odwoływać się będą do opinii doradców, konsultantów, specjalistów, fachowców i „mądrości tłumu" korzystając z portali społecznościowych i wyszukiwarek internetowych pozycjonujących interesujące ich strony według nieznanych i najczęściej niezrozumiałych dla nich kryteriów.

Zapotrzebowanie na profesjonalistów od analizy informacyjnej i decyzyjnej będzie coraz częściej zamieniać się w uzależnienie od ich zdania, sugestii, sposobu interpretacji, a nawet propozycji podjęcia konkretnej decyzji. To sprawia, że analitycy informacji stanowią jeden z filarów procesu zarządzania bezpieczeństwem zewnętrznym i wewnętrznym państwa włączając się do walki informacyjnej zarówno w czasie pokoju, narastania kryzysu, jak i ewentualnego konfliktu zbrojnego. Jak pisze Andrzej Żebrowski, powołując się na rosyjską koncepcję walki informacyjnej *każdy konflikt zbrojny i niezbrojny musi być poprzedzony walką informacyjną i nie jest możliwe odniesienie zwycięstwa bez wcześniejszego pokonania systemów informacyjnych przeciwnika* (Żebrowski 2013, s. 85). Koncepcja walki informacyjnej, jak nadmieniają autorzy teoretycznych i praktycznych problemów analizy informacyjnej, znajduje swoje zastosowanie także poza sferą militarną np. w polityce, gospodarce, nauce, kulturze i niekoniecznie musi być związana z walką w cyberprzestrzeni (Liedel, Piasecka, Aleksandrowicz 2012a, s. 21). Dlatego takie działania jak dezinformacja, manipulacja, parainformowanie i wszelkie inne techniki zniekształcania informacji pozwalające na stworzenie fałszywego obrazu obiektu w celu ukierunkowania procesu decyzyjnego i zarządczego zgodnie z wolą atakującego, doskonale charakteryzują pole walki informacyjnej. Narzędzia te perfekcyjnie są wykorzystywane przez media np. w podczas walki wyborczej i kształtowania opinii publicznej, jak również przez organizacje w celu pozyskania informacji

o konkurencyjnych firmach i ochrony własnych danych strategicznych. Walka informacyjna na gruncie społeczno-gospodarczym związana jest także z podejmowaniem działań wyprzedzających, za skuteczność których odpowiadają zespoły analityków zajmujących się wywiadem gospodarczym.

W epoce dominacji społeczeństw opartych na informacji i wiedzy zachowanie bezpieczeństwa światowego staje się nowym wyzwaniem. Ponieważ za najważniejszą sprawę w społeczeństwie globalnym uznaje się rozwój technologiczny, organizacyjny, swobodny przepływ informacji i naukę, więc osiągnięcie sukcesu i dominacji w tych obszarach ściśle łączy się z walką informacyjną, która wspiera działania podejmowane przez różne podmioty. Organizacje generujące nową wiedzę pozyskiwaną z otoczenia i przetwarzające wiedzę indywidualną w zbiorową, poprzez jej transfer są w stanie podejmować racjonalne decyzje. Dlatego chętnie korzystają z narzędzi, metod i środków walki informacyjnej, wykorzystując je do pozyskania wiedzy strategicznej dla procesu zarządzania firmą. Łączy się to z koniecznością zatrudniania wysokiej klasy specjalistów, których różnorodne kwalifikacje i uzdolnienia sprzyjają tworzeniu wiedzy w organizacji. Wymaga się od nich innowacyjności i funkcjonowania w warunkach ciągłej zmiany, której tempo nakłada obowiązek bycia elastycznym i kreatywnym. Wymaga się także biegłości w wykorzystywaniu nowoczesnych, mobilnych technologii informatyczno-komunikacyjnych, które wspomagają tworzenie i wykorzystywanie nowej wiedzy. Dlatego, aby być profesjonalistą w organizacji wiedzy, niezbędna jest znajomość reguł operowania, porządkowania i interpretacji zarówno informacji, jak i wiedzy (Batorowska 2016b, s. 202). Wykorzystując najnowocześniejsze technologie informatyczne do identyfikacji, analizy, rozwiązywania problemów i podejmowania decyzji postrzegani są przez Jeremy Rifkina nie tylko jako dostawcy informacji, ale także twórcy i manipulatorzy (Rifkin 2001, s. 224). Alexander Bard i Jan Söderqvist dodają, że eksperci od zarządzania informacją zyskują miano kapłanów, przewodników, pośredników i komentatorów najnowszych informacji, a stosowana przez nich *statystyka to język nowej wyroczni, informacja, którą przedstawia się jako fakty naukowe* (Bard, Söderqvist 2006, s. 97, 99).

Kim zatem jest analityk informacji i czym charakteryzuje się jego zawód? W piśmiennictwie funkcjonują rożne definicje. Słownik języka polskiego PWN określa analityka jako specjalistę zajmującego się analizą danych i prognozowaniem lub naukowca stosującego w badaniach metodę analizy. To jednak zbyt duże uproszczenia, gdyż analityk zazwyczaj związany jest z określoną grupą polityczną, organizacją, branżą, firmą, środowiskiem i ze względu na ich specyfikę definiowane są cechy analityka, jego osobowość, kompetencje, obowiązki, funkcje, zadania i wymogi stawiane wytworom jego pracy. Dlatego oczekiwania wobec analityków ze strony decydentów różnią się w zależności od

tego dla kogo i w jakim celu monitorują infosferę, zbierają dane, przetwarzają informacje, interpretują je, tworzą wiedzę, sugerują wybory i prognozują.

W monografii na temat analizy informacji w zarządzaniu bezpieczeństwem analityk definiowany jest jako osoba, której zadaniem jest *prezentowanie decydentowi materiałów (w rożnej postaci), udzielanie odpowiedzi na dwa podstawowe pytania „co" i „co z tego", a więc jakie zaistniały nowe fakty, jak wzajemnie na siebie oddziaływują, jakie jest ich znaczenie i konsekwencje ich zaistnienia dla decydenta. Taki materiał stanowi podstawę do podjęcia decyzji – jego zasadniczym celem jest wyposażenie decydenta w optymalny zasób wiedzy pozwalający mu na podjęcie racjonalnej, opartej na rzeczowych przesłankach decyzji* (Liedel, Piasecka, Aleksandrowicz 2013, s. 19-20).

Analityk służb specjalnych, zgodnie z definicją J. Lareckiego, to *pracownik pionu informacyjnego, którego zadaniem jest dokładne studiowanie zdobytych i uzyskanych materiałów i informacji, zarówno agenturalnych, jak i oficjalnych, opracowywanie na tej bazie syntetycznych informacji oceniających zagrożenie lub wskazujących cele, jakimi służba powinna się zająć w toku pracy operacyjnej, oraz postulowanie pogłębienia informacji lub uzyskanie nowych, potwierdzających lub negujących konkluzje wynikające z takiej analizy materiałów* (Chlebowicz, Kamińska 2015, s. 43).

Analityk w wywiadzie, dyplomacji, polityce zagranicznej określany jest jako ekspert wykorzystujący na użytek polityki zagranicznej źródła otwarte (tzw. „biały wywiad") i prognozujący na ich podstawie rozwój wydarzeń oraz przewidujący powstawanie problemów i napięć międzynarodowych (Zajączkowski 2011, s. 10; Dahl 2007).

Analityk kryminalny to *funkcjonariusz lub pracownik służby policyjnej, którego zadaniem jest analiza materiałów sprawy karnej lub operacyjnej w celach wykrywczych, jak i procesowych. Wnioski analityka kryminalnego zawarte w raporcie analitycznym posiadają lub mogą posiadać walory dowodowe* (Chlebowicz, Kamińska 2015, s. 44; Chlebowicz, Filipkowski 2011; Ignaczak 2005).

Analityk w administracji rządowej jest elementem procesu zarządzania w strukturach biurokratycznych, czyli jest urzędnikiem. Na temat wynikających z tego faktu konsekwencji dla jakości procesu analitycznego pisał Tomasz Aleksandrowicz (Liedel, Piasecka, Aleksandrowicz 2013, s. 15-19). Analityk o takim profilu to *osoba, która w swojej pracy wykorzystuje nie rzadziej niż kilka razy w miesiącu wyniki badań, ekspertyz, analiz, diagnoz itp. (np. raporty Komisji Europejskiej, analizy OECD, dane GUS, raporty z ewaluacji funduszy europejskich, badania wykonywane przez krajowe ośrodki naukowe) oraz używa nie rzadziej niż kilka razy w miesiącu podstawowych metod analizy danych ilościowych (np. analiza wybranych parametrów statystycznych, takich jak średnia, mediana czy wariancja, analiza korelacji, podstawowe testy statystyczne, analiza szeregów czasowych itp.) lub która wykonuje nie rzadziej niż kilka razy w miesiącu, w całości*

lub w części badania (analizy, ekspertyzy) diagnozy z wykorzystaniem metod badań społeczno-ekonomicznych (Ledzion, Olejniczak 2014, s. 19).

Analista (abstractor, referent) to pracownik informacji, dokumentalista zatrudniony w bibliotekach naukowych, fachowych i ośrodkach informacji naukowej, technicznej i ekonomicznej (inte). Jest specjalistą opracowującym analizy dokumentacyjne, *czyli metainformacje o treści dokumentu, zwykle będące tekstem języka naturalnego, stanowiące streszczenie dokumentu dokonane zgodnie z kryteriami przyjętymi w danym systemie informacyjno-wyszukiwawczym* (Dembowska 1979, s. 24; Bojar 2002, s. 20; Majzell, Smith, Zinger 1975). Przygotowywane przez niego opracowania analityczno-syntetyczne nie mają tylko charakteru przeglądowego, ale bardzo często przygotowywane były dla kadry kierowniczej prawie wszystkich resortów gospodarki narodowej i zawierały informacje faktograficzne pochodzące z najbardziej aktualnych źródeł informacji, takich jak raporty, protokoły, sprawozdania, syntezy, normy, patenty, literatura firmowa, instrukcje. Zapotrzebowanie na systematycznie redagowane (zazwyczaj jako dwutygodniki, miesięczniki, kwartalniki) przez służby analityczne raporty, opracowania informacyjno-prognostyczne, sytuacyjne, syntezy dokumentacyjne, informacje prognostyczne, produkcyjno-technologiczne, informacje syntetyczne, sygnalne, faktograficzne, zestawienia tematyczne itp. było duże[1] (Terajewicz 1974). Na ich podstawie decydenci podejmowali decyzje gospodarce, nawiązywali współpracę ze wskazanymi w raportach analitycznych ośrodkami, podejmowali decyzje w sprawie uruchomienia nowych linii produkcyjnych, rozbudowy infrastruktury, likwidacji stanowisk pracy, zakupu sprzętu itp.

Współczesny analista to tzw. infobroker lub broker informacji. Definiuje się go jako *pośrednika pomiędzy zasobami informacyjnymi a ich użytkownikami, który za opłatą służy pomocą w fachowym wyszukiwaniu informacji, wzbogaconym o jej analizę i opracowanie* (Kowalska 2015, s. 165, 166). Sednem pracy infobrokerskiej jest akredytacja informacji wykorzystanej do realizacji zlecenia wyszukiwawczego na zadany temat. Oceniając jakość uzyskanej informacji infobroker ponosi odpowiedzialność za jej użyteczność. W literaturze występuje też często określenie specjalisty ds. informacji, który może być zarówno pracownikiem firmy infobrokerskiej, jak i bibliotekarzem zatrudnionym głownie w bibliotekach naukowych i fachowych. Nie należy go mylić z infobrokerem systemowym, który jest *specjalistą wytwarzającym specyficzny produkt, jakim jest wiedza odpowiadająca na pytanie o to, jak rozwiązać konkretny problem. Jego zadaniem jest dostarczenie przesłanek do podjęcia decyzji* (Kowalska 2015, s. 167). Będąc najczęściej pełnomocnikiem kierownika jednostki organizacyjnej lub zastępcą ds. wiedzy, procesów informacyjnych ponosi odpowiedzialność za *adekwatność stanu wiedzy organizacji ze stanem wiedzy w dziedzinie statutowego funkcjonowania danej organizacji* (Tamże).

Czy definicja analityka – pracownika służb analitycznych (zaplecza analitycznego) jest jednoznaczna i w podobny sposób rozumiana przez przedstawicieli różnych dziedzin? Liedel, Pasecka i Aleksandrowicz wymieniają dwie grupy analityków: akademickich i politycznych (analizy decyzyjne) przedstawiając różnice dzielące wytwory ich pracy, którymi są m.in. analizy naukowe lub decyzyjne (Liedel, Piasecka, Aleksandrowicz 2012a, s. 73). Pominięta w tych rozważaniach została grupa analityków ze służb dokumentacyjnych zatrudnianych w bibliotekach naukowych, fachowych, a niegdyś prawie we wszystkich branżowych i resortowych, a nawet zakładowych ośrodkach informacji naukowej, technicznej i ekonomicznej. Analizy przez nich opracowywane w stosunku do analiz akademickich różniły się tym, że dotyczyły zarówno przeszłości, jak i spraw aktualnych, przygotowywane były dla ekspertów, pracowników nauki, ale także dla kadry kierowniczej i biznesu i zgodnie z zapotrzebowaniem mogły mieć charakter przeglądowy, zawierać roczne lub krótsze raporty z analizy stanu badań, ale także ze względu na ich syntetyczny i faktograficzny charakter służyły decydentom do podejmowania decyzji gospodarczych, oświatowych, badawczych itp. Podobnie jak analizy akademickie zawierały dużą ilość szczegółów i były zaopatrzone w relewantne do analizowanego tematu dane bibliograficzne i opisy źródeł. Ich struktura jest szczegółowo opisana w normach polskich i zgodnie z nią redagowane były zawsze opracowania dokumentacyjne i wydawnictwa informacyjne ośrodków inte. Zazwyczaj kończyły się one wnioskami i podsumowaniem, chociaż niektóre z nich na wstępie zaopatrzone były w abstrakty, a nawet streszczenia owych abstraktów (np. w syntezach informacyjnych, informacjach sygnalnych lub zestawieniach tematycznych). Działalność służb analitycznych ośrodków inte można umieścić w szerokiej sieci społecznej, która otacza zespół analityczny realizujący zadania dla sektora bezpieczeństwa, porządku publicznego, służb specjalnych, o którym pisze Krzysztof Liedel i Paulina Piasecka (Liedel, Piasecka, Aleksandrowicz 2012b, s. 17). Autorzy podkreślają, że zespół analityczny powinien uwzględniać w swoim składzie osoby, które wcześniej pracowały w takich obszarach, jak dziennikarstwo, badania naukowe, nauki społeczne lub inne powiązane z nimi. Ponieważ dla analityka bardzo cenne jest metodologiczne przygotowanie z zakresu analizy informacji, dlatego wsparcie w tym obszarze doświadczeniem, wiedzą i umiejętnościami brokerów lub infobrokerów informacji mogłoby przynieść wymierne efekty, aby *80% czasu pracy analityka nie było poświęcanego na uzupełnianie baz danych* (Tamże, s. 16).

Typologię analityków najłatwiej przeprowadzić biorąc pod uwagę profil wykonywanej przez nich pracy, stąd wyróżnia się analityków specjalizujących się w finansach, biznesie, marketingu, związanych głównie z sektorem gospodarczym (np. analitycy finansowi, administracji rządowej), analityków zatrudnionych w służbach bezpieczeństwa (np. analityków kryminalnych, wywiadowczych,

kontrwywiadowczych), analityków informacji związanych z placówkami naukowymi (analitycy akademiccy, analitycy dokumentacyjni). Można wyróżnić inne jeszcze typy analityków związanych z analizą wybranych źródeł informacji, np. prasowych, stron internetowych, portali społecznościowych, otwartych źródeł informacji (Filipkowski, Mądrzejowski 2012; Liedel, Serafin 2011). W praktyce jednak trudno w procesie analitycznym ograniczać się do jednego typu źródeł, weryfikacja danych wymaga zawsze rozszerzenia obszaru poszukiwań.

Kompetencje analityków informacji

Na ten temat wypowiadają się autorzy prawie wszystkich publikacji poświęconych analizie i służbom analitycznym, odwołując się do światowej literatury oraz dokumentów opracowanych przez różne departamenty w zakresie obowiązujących standardów kompetencji tej grupy zawodowej. W przytoczonym przez Krzysztofa Liedla i Paulinę Piasecka „Law Enforcement Analytic Standards" z 2007 roku wyróżnia się następujące grupy kompetencji: wiedzę w odpowiednim zakresie przedmiotowym; opanowanie warsztatu analitycznego (metodologia analityczna, znajomość źródeł informacji i ich przetwarzanie, znajomość technologii informacyjnych, krytyczne myślenie, kreatywność, dyscyplina pracy umysłowej); umiejętności komunikacyjne (praca w zespole); etykę pracy (etyka w stosunku do „klienta informacyjnego", uczciwość, wysokie standardy etyczne) (Liedel, Piasecka, Aleksandrowicz 2012b, s. 15).

Natomiast w rozporządzeniu Prezesa Rady Ministrów z dnia 8 maja 2009 roku w sprawie warunków i sposobu przeprowadzania ocen okresowych członków korpusu służby cywilnej, w tym wszystkich stanowisk o charakterze analitycznym w administracji rządowej, stwierdza się, że analitycy powinni dysponować umiejętnościami analitycznymi rozumianymi jako umiejętne stawianie hipotez, wyciąganie wniosków przez analizowanie i interpretowanie danych, w tym: *rozróżnianie informacji istotnych od nieistotnych; dokonywanie systematycznych porównań różnych aspektów; interpretowanie danych pochodzących z dokumentów, opracowań, raportów; samodzielne wyszukiwanie potrzebnych informacji; dostrzeganie na jakim etapie jest wymagane wsparcie; zastosowanie logicznego podejścia do analizy przez rozbicie problemu na części, którymi można zarządzać; dostrzeganie relacji i powiązań między informacjami, umiejętne wyciąganie wniosków z posiadanych informacji; stosowanie procedur prowadzenia badań odpowiadających stawianym problemom; prezentowanie w optymalny sposób danych i wniosków z przeprowadzonej analizy; dobieranie odpowiednich narzędzi i technologii w celu rozwiązania problemu* (*Zasady tworzenia indywidualnych programów…*. 2014, s. 9). Wyżej wymienione kompetencje wpisują się w „Kanon Wiedzy" wymagany od analityka administracji rządowej, obejmujący pięć pól: teorię interwencji publicznych, metodykę badań, podejścia

i metody ilościowe, wykorzystanie wiedzy w procesach decyzyjnych oraz nowe trendy w zakresie analiz polityk publicznych (Ledzion, Olejniczak 2014, s. 98).

Standardy kompetencji analityka nawiązują w większości punktów do kompetencji infobrokerskich określonych w „Krajowym Standardzie Kompetencji Zawodowych. Broker informacji" i dotyczą takich obszarów, jak: informatyczny, społeczny, metodologiczny, komunikacyjny, analityczno-synteteyczny, biurowo-dokumentacyjny, prawny, ekonomiczny, infobrokerski. Od osoby wykonującej zawód brokera informacji (researchera) wymaga się w zakresie wiedzy, aby znała *w pogłębionym stopniu teorie i metody związane z wyszukiwaniem, weryfikowaniem, analizowaniem oraz udostępnianiem informacji, aby znała przepisy prawa, związane z dostępem do informacji publicznej, informacji gospodarczej, informacji niejawnych oraz inne przepisy prawa związane z informacją, Internetem oraz mediami i prawem autorskim; znała różne metody przeprowadzania analizy informacji; mała pogłębioną wiedzę o potrzebach i zachowaniach odbiorców usług brokera informacji; znała w stopniu zaawansowanym technologie informacyjne wykorzystywane w pracy brokera informacji; rozróżniała złożone uwarunkowania prowadzonej działalności; znała mechanizmy rynkowe oraz uwarunkowania związane z prowadzeniem działalności gospodarczej. Natomiast w zakresie umiejętności od przedstawicieli tego zawodu wymaga się stosowania metod, technik i środków związanych z wyszukiwaniem, pozyskiwaniem, analizowaniem i udostępnianiem relewantnych do zapytania informacji z różnych obszarów życia społecznego i gospodarczego; dobierania odpowiednich rozwiązań i metod realizacji zadań w zależności od sytuacji i dziedziny informacji; wykonywania zadań oraz formułowania i rozwiązywania problemów z wykorzystaniem nowej wiedzy; analizowania, dostosowywania do potrzeb i wdrażania nowych technologii informacyjnych; planowania procesu samokształcenia; umiejętności komunikowania się z osobami potrzebującymi i dostarczającymi informacje oraz stosowania i wykorzystywania mechanizmów rynkowych i gospodarczych* (*Krajowy Standard*…, s. 9). Zgodnie ze standardami kompetencji broker informacji odgrywa ważną role w procesie podejmowania decyzji zarządczych. Mateusz Bonecki i Anna Malitowska dodają, że *infobroker funkcjonujący w systemie podejmowania decyzji zarządczych jest aktorem uczącym się, tzn. przyswajającym i generującym wiedzę w sensie reguł przetwarzania informacji w celu jej późniejszego stosowania przy przeformułowywaniu i dekompozycji problemu infobrokerskiego*" (Bonecki, Malitowska 2015, s. 121). Zatem kompetencje brokera informacji powinny stanowić nieodzowny człon kompetencji analityka informacji, szczególnie w warunkach funkcjonowania w środowisku nadmiarowości informacji i trudności z jej weryfikacją.

Zastanawiając się w dalszej części artykułu nad kwestią, czy analizy informacji można się nauczyć, czy trzeba mieć wrodzone predyspozycje do

postrzegania rzeczywistości, faktów i informacji w sposób analityczno-syntetyczny, należy zwrócić szczególną uwagę na umiejętności wynikające z indywidualnych cech analityka i jego osobowości, które przyczyniają się w dużym stopniu do unikania błędów popełnianych w cyklu analitycznym, w tym pułapek myślowych związanych z interpretacją informacji. Wojciech Zajączkowski analizując cykl wywiadowczy w polityce zagranicznej, stwierdza, że popełniane przez analityka błędy trudno usystematyzować, niemniej spróbował pogrupować je ze względu na sprawcę pomyłki, tj. osobę analityka i środowisko instytucjonalne. Do błędów indywidualnych zaliczył: syndrom zwierciadła (przenoszenie na analizowaną obcą rzeczywistość schematów interpretacyjnych zapożyczonych z własnej rzeczywistości analityka), niedostateczną krytykę „wewnętrzną" i „zewnętrzną" źródeł informacji, dążenie do spójności narracyjnej za wszelką cenę (spójności nieudokumentowanej materiałem źródłowym), forsowanie hipotezy niepopartej dowodami, przekonanie o logiczności rzeczywistości społeczno-politycznej (pomijając czynniki nie mieszczące się w racjonalnej analizie politologicznej), przeświadczenie, ze „świat się kręci wokół nas" (podejmowanie głównie tematów analitycznych dotyczących własnego kraju), dryf w stronę obfitszej informacji (wykorzystywanie w raportach analitycznych informacji nierelewantnych zastępujących niedostateczny materiał dotyczący zadania analitycznego), autocenzura (obawy przed reakcją decydenta na treść raportu lub przed skutkami dotarcia opinii analityka do niepożądanych odbiorców). Natomiast do błędów wynikających z grupowych ograniczeń poznawczych autor „Metody analitycznej w polityce zagranicznej" zaliczył: źle dobrany skład osobowy zespołu analitycznego, w którym brak specjalistów o różnym wykształceniu i poglądach, dążenie za wszelką cenę do uzgodnienia stanowiska zespołu analitycznego, pomijając intuicję pojedynczych członków zespołu, akceptację rozwiązań standardowych, nadmierną różnorodność i rozproszenie tematyczne zadań analitycznych sprzyjające powierzchowności raportów analitycznych, odmienne kalibrowanie prawdopodobieństwa wystąpienia prognozowanych wydarzeń przez analityków z różnych zespołów pracujących dla tego samego decydenta (Zajączkowski 2011, s. 76-88). Niewątpliwie ważnym narzędziem pracy każdego analityka jest sprawna pamięć podręczna umożliwiająca wieloaspektowe przetwarzanie informacji, uogólnianie faktów, abstrahowanie, tworzenie struktur wiedzy, generowanie różnych hipotez, prognoz i interpretacji faktów. Sprawności te zależą od indywidualnych zdolności analityka oraz od praktyki i treningu w sztuce analitycznej. Dlatego ważne jest dla niego otoczenie intelektualne, w którym pracuje i kontakt z ośrodkami akademickimi i naukowo-badawczymi.

Analiza informacji – sztuka czy wyuczona umiejętność?

Czy każdy może zostać analitykiem? Czy kompetencje nieodzowne w pracy analitycznej można pozyskać w trakcie studiów i innych form kształcenia, czy

wystarczy wytężona praca, aby osiągnąć w tym obszarze doskonałość i uznanie w oczach decydentów podejmujących trafne decyzje na podstawie opracowanych przez analityków raportów? Czy każdy ekspert jest w stanie przygotować taki raport i być przekonanym, że decyzje zarządcze podjęte na ich podstawie są słuszne i zapewnią rozwój, sukces i bezpieczeństwo podmiotom, dla których były przeznaczone? Umiejętność analizy i syntetycznego oglądu problemu nie jest umiejętnością powszechną ani łatwą. Nie wszyscy posiadają predyspozycje psychiczne, fizyczne i intelektualne, aby móc zredagować spójny, relewantny, obiektywny, oparty na trafnie dobranych źródłach informacji i metodach analitycznych, a nade wszystko zrozumiały dla adresata dokument analityczny. Wojciech Zajączkowski powołując się na publikacje Richarda J. Heuera, byłego pracownika CIA, cytuje – *błędnie przyjmuje się założenie, że analitycy wiedzą jak analizować. Potrzebne są szkolenia, żeby podnieść samoświadomość odnoszącą się do organicznych problemów związanych z postrzeganiem i wydawaniem sądów analitycznych* […] (Zajączkowski 2011, s. 25).

Aby móc opanować sztukę tworzenia trafnych raportów analitycznych trzeba posiadać na wejściu tzw. potencjał analityczny, czyli zdolność, nie podlegającą rozwojowi w trakcie kariery zawodowej, w przeciwieństwie do wiedzy i umiejętności, które ciągle muszą być rozwijane (Ledzion, Olejniczak 2014, s. 45). Potencjał ten mierzony jest za pomocą znormalizowanych i wystandaryzowanych narzędzi, takich jak np. *Test Potencjału Analitycznego* (Test Kompetencji Analitycznych) i *Test Matryc Ravena*. Pozwalają one na wybór spośród osób ubiegających się na stanowiska analityków w urzędach administracji rządowej tylko tych, których potencjał analityczny okaże się wysoki. Uznaje się, że osoby o potencjale średnim i niskim będą zawsze mniej skuteczniej i efektywniej nabywały wiedzę i umiejętności specjalistyczne, bez względu na włożony przez nie wysiłek oraz koszty przeznaczone na środki i metody ich kształcenia. Natomiast osoby o wysokim potencjale analitycznym w sytuacji, w której ze względu na brak danych i jasnych kryteriów nie jest możliwe opracowanie jednoznacznej analizy parametrycznej, wykorzystują w procesie analitycznym intuicję, odgrywającą w wielu sytuacjach decyzyjnych niezwykle istotną rolę (Liedel, Piasecka Aleksandrowicz 2012a, s. 201-202).

Test Potencjału Analitycznego obejmuje zarówno wiedzę, umiejętności jak i zdolności analityczne. Założono, że aby poprawnie zidentyfikować pracownika o dużym potencjale analitycznym musi on zaliczyć *Test*… obejmujący pięć wymiarów pracy analityka, tj. wykorzystywanie wiedzy pochodzącej z już istniejących opracowań, np. badań, ekspertyz, analiz, diagnoz, raportów naukowych, statystyk; generowanie wiedzy poprzez tworzenie założeń metodycznych do badań, analiz, ekspertyz, diagnoz oraz współpracę z ekspertami zewnętrznymi przy opracowywaniu dokumentów analitycznych; wykorzystywanie metod ilościowej analizy danych i tworzenie na ich podstawie rozmaitych

opracowań; zaangażowanie w proces oceny interwencji publicznych (przygotowanie testów regulacyjnych, ocena skutków regulacji, udział w ewaluacji analiz, ekspertyz, weryfikacja badań ewaluacyjnych); zaangażowanie w proces stanowienia prawa (udział w tworzeniu rozporządzeń, ustaw, programów publicznych, projektów, strategii, założeń) (Ledzion, Olejniczak 2014, s. 16). Test pozwolił na wyłonienie trzech grup analityków, z których najwyżej oceniono analityków typu III, stosujących w pracy podstawowe i zaawansowane metody ilościowej analizy danych, uczestniczących w tworzeniu rozporządzeń i ustaw oraz biorących udział w procesie przygotowywania ocen wpływu, czyli uczestniczących w całym procesie analitycznym tworząc prawo oraz je oceniając. W pozostałych typach odnotowano brak elementu uczestnictwa w tworzeniu prawa lub/i elementu oceny wpływu. Analiza danych, które dostarczył *Test Potencjału Analitycznego* pozwoliła na sformułowanie wniosku, że *dotychczas nie brano pod uwagę potencjału analitycznego przy selekcji osób wykonujących prace analityczne w administracji publicznej*, ponieważ w grupie osób badanych 59% stanowiły osoby o potencjale analitycznym niskim i średnim, które *mogą popełniać błędy zarówno w zakresie opracowywania i wykonywania badań, jak i interpretacji ich wyników* (Tamże, s. 25, 45).

Można zatem przyjąć, że nie każdy posiada predyspozycje do postrzegania rzeczywistości w sposób analityczny i syntetyczny oraz do prowadzenia procesu analizy decyzyjnej. Trzeba mieć do tego talent, inteligencję i intuicję. Odwołując się do stanowiska Franka Boulinga, Wojciech Zajączkowski podkreśla, że analiza *jest stanem ducha, opartym na pewnej filozofii inteligencji i rozwoju zdolności indywidualnych w ramach kolektywu*, a jej opracowanie nie jest tylko efektem opanowania formułek i technik analitycznych (Zajączkowski 2011, s. 63). Potwierdzają to także wyniki badań prowadzone wśród studentów dotyczące ich skuteczności w zakresie uogólniania, abstrahowania, analizowania, syntezowania, wnioskowania, etykietowania, strukturyzowania, klasyfikowania, indeksowania pozyskiwanych informacji i przekształcania ich w wiedzę, które zebrano w tabelach zamieszczonych w publikacji pt. *Perceived self-efficacy vs. actual level of training in personal information and knowledge management. A research report (Poczucie własnej skuteczności a rzeczywiste przygotowanie do indywidualnego zarządzania informacja i wiedzą. Raport z badań)* (Batorowska 2016a, s. 67-81) oraz w tabelach ilustrujących artykuł pt. *Rozważania nad przetwarzaniem informacji w środowisku jej nadmiarowości i przyspieszenia technologicznego* (Batorowska 2017a). Stwierdzono, że analizowanie jest procesem wymagającym predyspozycji do segmentacji tekstu, czyli wyłaniania z niego wyrażeń składowych. Polega ono na pojęciowym wyodrębnianiu cech, części lub składników badanego zjawiska lub przedmiotu i jest nieodzowne w ocenianiu przydatności informacji. Wymaga także biegłości w zakresie uogólniania, dostrzegania związków pomiędzy komponentami rozpoznanymi

w procesie analizy i łączenia ich w całość. W ten sposób proces analizy przechodzi w proces syntezy i nie można ich traktować oddzielnie, jeżeli celem jest podjęcie trafnych i efektywnych decyzji (Batorowska 2015b, s. 173).

Umiejętność analizowania można wyćwiczyć, ale wymaga ona dużego zaangażowania ze strony podmiotu uczącego się i pracowitości. I chociaż w efekcie kształcenia wykonywana jest ona poprawnie, to na podstawie ww badań stwierdzono, że w większości analiz stwierdzono brak twórczego podejścia do opracowywanego tematu (Batorowska 2017b). Słusznie stwierdza Jerzy Konieczny, że efekt pracy analityka w dużej mierze nosi znamiona sztuki (Konieczny 2012, s. 21). Wyniki prowadzonych przeze mnie badań nie potwierdziły skuteczności studentów w zakresie tworzenia struktur wiedzy, kategoryzacji, indeksowania, klasyfikowania, analizowania, uogólniania, syntezy, etykietowania itp. Uznano, że na ten stan wpływa w decydującym stopniu funkcjonowanie młodzieży w świecie, w którym dominuje fragmentaryzacja, szybkość, natychmiastowość, powierzchowność, kult nowości, płynność, wielozadaniowość. Zaobserwowane deficyty w zakresie sprawnego zarządzania informacją wynikają między innymi z braku umiejętności radzenia sobie z problemami nadmiarowości informacji i z konsekwencjami przyspieszenia technologicznego (Batorowska 2017a). Z takiej młodzieży wywodzić się będą przyszli kandydaci do pracy na stanowiskach analityków w urzędach państwowych i firmach. Poza ponadprzeciętnym potencjałem analitycznym będą oni potrzebowali permanentnego szkolenia specjalistycznego.

Instytut Rozwoju Biznesu przygotował w 2014 roku dla Kancelarii Prezesa Rady Ministrów zestaw ekspertyz, raportów i komunikatów, w których przedstawiono diagnozę, wnioski i zalecenia odnoszące się do procesu kształcenia analityków dla administracji rządowej, zwracając szczególną uwagę na zasady tworzenia indywidualnych programów rozwoju zawodowego dla przedstawicieli tej profesji, wdrażania specjalistycznej ścieżki ich rozwoju oraz zwracania szczególnej uwagi podczas rekrutowania kadr na potencjał analityczny kandydatów do zawodu (*Optymalne*… 2014; *Zasady tworzenia*… 2014). Szkoleniem kadry analityków dla różnych gałęzi gospodarki narodowej i resortów zajmują się różne ośrodki. Jednym z nich jest Collegium Civitas niepubliczna uczelnia akademicka w Warszawie prowadząca studia między innymi z zakresu analizy informacji w zarządzaniu bezpieczeństwem[2]. Studia te umożliwiają zapoznanie się z metodami i technikami analizy informacji, ze szczególnym uwzględnieniem analizy, planowania i decydowania w obszarze zarządzania bezpieczeństwem (*Analiza informacji w zarządzaniu*…). Natomiast wiodącym ośrodkiem szkolenia analityków kryminalnych jest Wyższa Szkoła Policji w Szczytnie, w której realizowane są szkolenia z zakresu operacyjnej analizy kryminalnej dla kadr analityków specjalizujących się w międzynarodowej współpracy i wymianie informacji (wykorzystujących zunifikowane metody,

techniki analitycznych i narzędzia informatyczne stosowane przez służby specjalne na świecie, np. *Analyst's Notebook*, *iBase*) (zob. http://www.wspol.edu.pl/ibpkt/images/stories/ dokumenty/ofertaszkoleniowa.pdf). Także Centrum Doskonalenia Kursowego Oficerów Akademii Sztuki Wojennej w Warszawie ma w swojej ofercie edukacyjnej kursy w zakresie analizy informacji (http://www.akademia.mil.pl/kandydat/ informacje-dla-kandydatow.html). Z teorią i praktyką analizy kryminalnej, policyjnej, politycznej, wywiadowczej, kontrwywiadowczej itp. zapoznaje swoich studentów także większość uczelni prywatnych i państwowych prowadzących studia z zakresu bezpieczeństwa wewnętrznego i narodowego.

Bez względu czy szkolone będą kadry dla potrzeb ekonomii, biznesu, bezpieczeństwa narodowego lub wewnętrznego, nauki, należy przyjąć, że podstawą pracy analityka jest jego gruntowna wiedza i umiejętności w zakresie analizy informacji w ogóle. Stąd każdy z nich powinien oprócz wiedzy eksperckiej (wojskowej, ekonomicznej, prawniczej, technicznej, medycznej, biznesowej, marketingowej lub z innej dziedziny) posiadać podstawowe przygotowanie infobrokerskie, obejmujące kompetentne identyfikowanie rzeczywistych potrzeb klientów, oparte na przemyślanej strategii wyszukiwawczej, pozyskiwanie informacji z różnych źródeł, monitorowanie źródeł informacji, filtrację pozyskanej informacji, przetwarzanie jej w formie analiz, syntez, raportów, streszczeń, zestawień statystycznych, baz danych, akredytację dostarczonej w dokumentach analitycznych informacji (Bałos, Cisek, Januszko-Szakiel 2016, s. 20-21). Poza kompetencjami informacyjnymi infobroker musi legitymować się umiejętnościami komunikacyjnymi, językowymi i technologicznymi. Znajduje on zatrudnienie nie tylko w zawodzie broker informacji, ale także jako analityk w firmach badających rynek, w agencjach public relations, w firmach konsultingowych, w wywiadowniach gospodarczych. Tadeusz Wojewódzki zaznacza, że we współczesnym świecie *jakość życia społecznego uzależniona jest od jakości decyzji politycznych, gospodarczych, społecznych. Decyzji podejmowanych na różnych szczeblach, różnych organizacji*, a *jakość decyzji uzależniona jest od kompetencji infobrokerskich oraz poziomu kultury infobrokerskiej organizacji* (Wojewódzki 2016, s. 147). Dlatego analityk w firmie to zarazem infobroker systemowy, którego rola w organizacji związana jest z organizacją procesów informacyjnych nakierowanych na powstawanie zasobów wiedzy adekwatnych do potrzeb organizacji. Infobroker systemowy jest specjalistą w zakresie technologii procesów informacyjnych, dysponuje kompetencjami menadżerskimi wyższego stopnia umożliwiającymi wykonywanie nierutynowych zadań opartych na praktycznym wykorzystaniu znacznych zasobów wiedzy, posiada umiejętności komunikacyjne i poznawcze oparte na samodzielności myślenia i asocjacyjności problemowej. Dzięki tym kompetencjom jest w stanie dostarczyć odpowiedź na zidentyfikowane potrzeby informacyjne aktualnie rozwiązywanych problemów, sporządzać drzewa

problemów, drzewa wiedzy, raporty o stanie wiedzy w dziedzinie problemowej, drzewa wartości, drzewa argumentów decyzyjnych itp. (Wojewódzki 2016, s. 158-159).

Infobroker systemowy nie jest jednak obarczony odpowiedzialnością za błędne decyzje decydentów wynikające ze złej interpretacji faktów zamieszczonych w raportach analitycznych. Podobnie jak pracownik służb analitycznych w bibliotekach i ośrodkach informacji dbać musi głównie o obiektywizm, relewancję danych, dokładność, aktualność, kompletność, koherencję, dostępność, kompatybilność, bezpieczeństwo, ważność, wiarygodność danych i informacji gromadzonych i przetworzonych. Podczas gdy, analityk przygotowujący analizę polityczną, gospodarczą, kryminalną, śledczą, wywiadowczą, kontrwywiadowczą itp. poza analizą i oceną danych, interpretuje także fakty, proponuje rozwiązania problemu, przedstawia projekty decyzji, przewiduje możliwe scenariusze, prognozuje, przepowiada przyszłość, musi się liczyć z konsekwencjami złej asocjacji zebranych informacji, uwzględnieniem błędnych danych, sugerowaniem wniosków, które mogą prowadzić do stanów zagrożenia i konfliktów. Jak słusznie piszą autorzy książki *Analiza informacji…*, że chociaż *w ostateczności odpowiedzialność spada zawsze na decydenta, a analityk z reguły pozostaje w cieniu, to jednak zawsze trzeba pamiętać, że decyzje podejmuje się na podstawie analizy*, także tej zawierającej błędy, a więc odpowiedzialność analityka za jakość jego pracy nie może być umniejszana (Liedel, Piasecka, Aleksandrowicz 2012a, s. 76).

Podsumowując, w zglobalizowanej i usieciowionej gospodarce, w społeczeństwie ryzyka, konfliktów i katastrof, w środowisku zdominowanym przez informację decydenci będą zmuszeni w coraz większym stopniu korzystać z zaplecza analitycznego i doradczego. Zespół specjalistów tam pracujących musi mieć świadomość współodpowiedzialności za podejmowane na podstawie efektów swojej pracy decyzje, które coraz częściej będą miały charakter strategiczny dla firmy, organizacji, narodu, ludzkości. Można zaryzykować stwierdzenie, że to w rękach analityków, ekspertów od zarządzania informacją i wiedzą, netoktatów zatrudnionych w służbach analitycznych leży bezpieczeństwo poszczególnych państw oraz bezpieczeństwo międzynarodowe. Ich rola będzie wzrastać, wraz ze wzrostem ilości nieuporządkowanej informacji dopływającej różnymi kanałami, wraz z coraz większymi problemami zapanowania nad zalewem informacji, trudnościami w jej filtrowaniu i weryfikacji danych oraz odróżniania informacji od jej interpretacji, wraz z wykorzystywaniem informacji do manipulowania zachowaniami i postawami ludzi, wraz z powstawaniem nowych metod i narzędzi walki informacyjnej oraz z powstawaniem nowych zagrożeń w cyberprzestrzeni i bardziej wyrafinowanych technologii informatyczno-komunikacyjnych zagrażających bezpieczeństwu świata (Goodman 2016, s. 353).

Przypisy

[1] W 1990 roku nastąpił upadek instytucji centralnych, w tym CINTE – Centrum Informacji Naukowej Technicznej i Ekonomicznej odpowiedzialnego za koordynowanie działalności informacyjno-dokumentacyjnej w kraju, w tym działalności związanej z wydawaniem i rejestrowaniem wydawnictw informacyjnych przygotowywanych przez centralne, branżowe, zakładowe ośrodki inte. Stopniowej likwidacji ulegały także wymienione ośrodki inte.

[2] Prowadzone są także studia na kierunku: Bezpieczeństwo i analiza informacji przeznaczone dla osób planujących pracę na stanowisku analityka informacji w administracji publicznej, służbie cywilnej, ośrodkach analitycznych i biznesie. Program studiów obejmuje następujące przedmioty: metodologia i techniki analizy informacji, cyberbezpieczeństwo, planowanie i organizacja pracy zespołów analitycznych, analiza systemowa sytuacji kryzysowych i konfliktowych, analiza ryzyka, studia strategiczne. Podczas zajęć studenci uczą się używania narzędzi analitycznych oraz uzyskują praktyczną wiedzę umożliwiającą ocenę zagrożeń w skali mikro i makro. Dzięki temu są w stanie analizować zjawiska wpływające na stabilność i bezpieczeństwo organizacji i firm z różnych sektorów gospodarki, a także na funkcjonowanie państwa. Przy Collegium Civitas działa Instytut Analizy Informacji.

Bibliografia

Analiza informacji w zarządzaniu bezpieczeństwem. Dostęp: 1.02.2017. Tryb dostępu: https://www.civitas.edu.pl/collegium/oferta-edukacyjna/po-polsku/studia-podyplomowe-po-polsku/kierunki-studiow-podyplomowych/.

kierunki-studiow-podyplomowych-obszar-analiza-informacji-i-bezpieczenstwo/analiza-informacji-w-zarzadzaniu-bezpieczenstwem. Także: https://www.civitas.edu.pl/collegium/uczelnia/nauka-i-badania/centra-badawcze/instytut-analizy-informacji.

Bard, A., Söderqvist, J. (2006) *Netokracja. Nowa elita władzy i życie po kapitalizmie.* Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Bałos I., Cisek S., Januszko-Szakiel A. (2016) *Wprowadzenie do infobrokeringu. Wybrane aspekty*. W: Cisek, S., Januszko-Szakiel, A. (red.), *Zawód infobroker. Polski rynek* informacji. Piaseczno: Wydawnictwo Nieoczywiste GAB Media, s. 13-28.

Batorowska, H. (2015a) *Konsumpcja informacji a sztuka jej przetwarzania.* W: Morbitzer, J., Morańska, D., Musiał, E. (red.), *Człowiek – Media – Edukacja.* Dąbrowa Górnicza: Wyższa Szkoła Biznesu, s. 16-24.

Batorowska, H. (2015b) *Zanik umiejętności dostrzegania problemu w ujęciu całościowym i w interdyscyplinarnej refleksji.* W: Batorowska, H. (red.), *Kultura informacyjna w ujęciu interdyscyplinarnym – teoria i praktyka.* T. 1. Kraków: Uniwersytet Pedagogiczny w Krakowie, s. 170-179.

Batorowska, H. (2016a) *Perceived self-efficacy vs. actual level of training in personal information and knowledge management. A research report*. "Bibliotheca Nostra", nr 2, s. 61-89.

Batorowska, H. (2016b) *Wybrane aspekty kultury bezpieczeństwa w społeczeństwie informacji i wiedzy.* „Studia Politologia Ukraino-Polona", nr 6, s. 200-208.

Batorowska, H. (2017a), *Przetwarzanie informacji w środowisku jej nadmiarowości i przyspieszenia technologicznego w świetle badań własnych*. „Edukacja-Technika-Informatyka", nr 1 [w druku].

Batorowska, H. (2017b), *Umiejętność strukturalizacji treści przez podmiot uczący się.* W: Kamińska-Czubała, B., Skórka, S. (red.), *Projektowanie informacji w przestrzeni biblioteki*. Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego[w druku].

Bojar, B. (red.) (2002) *Słownik encyklopedyczny informacji, języków i systemów informacyjno-wyszukiwawczych*. Warszawa: Wydawnictwo SBP.

Bonecki M., Malitowska A. (2015), *Rola infobrokera w procesie podejmowania decyzji zarządczych.* W: Kowalska, M., Wojewódzki, T. (red.), *Infobrokerstwo. Idee, koncepcje, rozwiązania praktyczne*. Gdańsk: ATENEUM Szkoła Wyższa w Gdańsku, s. 121-142.

Chlebowicz, P., Filipkowski, W. (2011) *Analiza kryminalna. Aspekty kryminalistyczne i prawnodowodowe*. Warszawa.

Chlebowicz, P., Kamińska, J. (2015) *Operacyjna analiza kryminalna w służbach policyjnych*. Warszawa: Difin.

Dahl, R. (2007) *Współczesna analiza polityczna*. Warszawa: Wydawnictwo Naukowe Scholar.

Dembowska, M. (red) (1979) *Słownik terminologiczny informacji naukowej*. Wrocław: Ossolineum.

Filipkowski, W., Mądrzejowski, W. (red.) (2012) *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*. Warszawa: Wydawnictwo C. H. Beck.

Goodman, M. (2016) *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko tobie*. Gliwice: Wydawnictwo Helion.

Ignaczak, W. (2005) *Wybrane zagadnienia analizy kryminalnej*. Szczytno: Wyższa Szkoła Policyjna.

Konieczny, J. (red.) (2012) *Analiza informacji w służbach policyjnych i specjalnych*. Warszawa: Wydawnictwo C. H. Beck.

Kowalska, M. (2015) *Infobroker – definicja misji, zadania, kompetencje*. W: Kowalska, M., Wojewódzki, T. (red.), *Infobrokerstwo. Idee, koncepcje, rozwiązania praktyczne*. Gdańsk: ATENEUM Szkoła Wyższa w Gdańsku, s. 161-193.

Krajowy Standard Kompetencji Zawodowych. Broker informacji (researcher) (2013). Dostęp: 1.02.2017. Tryb dostępu: ftp://kwalifikacje.praca.gov.pl/STANDARDY%20KOMPETENCJI%20ZAWODOWYCH/77_262204_broker_informacji_researcher.pdf.

Ledzion, B., Olejniczak, K. (red.) (2014) *Potencjał analityczny kadr administracji rządowej. Ekspertyza*. Warszawa: Instytut Rozwoju Biznesu sp. Z o.o.

Liedel, K., Piasecka, P., Aleksandrowicz, T. R. (red.) (2013) *Analiza informacji w zarządzaniu bezpieczeństwem*. Warszawa: Difin.

Liedel, K., Piasecka, P., Aleksandrowicz, T. R. (2012a) *Analiza informacji: teoria i praktyka*. Warszawa: Difin.

Liedel, K., Piasecka, P., Aleksandrowicz, T. R. (2012b) *Analiza informacji w działaniu.* Warszawa: Difin.

Liedel, K., Serafin, T. (2011) *Otwarte źródła informacji w działalności wywiadowczej*. Warszawa: Difin.

Maizell, R. E., Smith, J., Zinger, T. E. R. (1975) *Analizy dokumentacyjne piśmiennictwa naukowo-technicznego*. Warszawa: Wydawnictwo Naukowo-Techniczne.

Optymalne wdrożenie specjalistycznej ścieżki rozwoju zawodowego dla analityków. *Raport* (2014). Warszawa: Instytut Rozwoju Biznesu sp. Z o.o.

Rifkin, J. (2001) *Koniec pracy. Schyłek Siły roboczej na świecie i początek ery postrynkowej*. Wrocław: Wydawnictwo Dolnośląskie.

Terajewicz, M. (1974) *Zasady sporządzania informacyjnych opracowań analityczno-syntetycznych.* Warszawa: CINTE. Prace Studia Przyczynki nr 6.

Wojewódzki, T. (2016) *Infobrokerstwo systemowe – kontekst niezbędności infobrokerskiej roboty*. W: Cisek, S., Januszko-Szakiel, A. (red.), *Zawód infobroker. Polski rynek* informacji. Piaseczno: Wydawnictwo Nieoczywiste GAB Media, s. 147-187.

Zajączkowski, W. (2011) *Zrozumieć innych. Metoda analityczna w polityce zagranicznej.* Warszawa: Krajowa Szkoła Administracji Publicznej.

Zasady tworzenia indywidualnych programów rozwoju zawodowego dla analityków (2014). Warszawa: Instytut Rozwoju Biznesu sp. Z o.o.

Żebrowski, A. (2016) *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego.* Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego w Krakowie.

Streszczenie

Przedstawiono rolę analityka informacji w czasach traktowania informacji jako zasobu strategicznego oraz narzędzia walki informacyjnej. Wyodrębniono różne typy analityków i scharakteryzowano ich cechy oraz kompetencje. Stwierdzono, że jest to zawód, który wymaga oprócz pracowitości, wiedzy i kompetencji analitycznych także talentu i wrodzonej intuicji do prognozowania na podstawie dostępnych faktów i danych. Analizowanie jest sztuką i tylko osoby z potencjałem analitycznym będą w stanie osiągnąć w pracy analityka sukces. Zwrócono uwagę na kontekst etyczny profesji, wskazując na odpowiedzialność za produkty analityczne i konsekwencje decyzji podejmowanych na ich podstawie.

Słowa kluczowe: walka informacyjna, analityk, analiza informacji, kompetencje analityczne, kompetencje informacyjne, zarządzanie informacją, *Test Potencjału Analitycznego*, kształcenie analityków informacji

Analyst in the environment of warfare for domination and survival

Abstract

Nowadays, information is perceived as a strategic resource and a weapon in information warfare. The role of the information analyst at this time is presented. Different types of information analysts are shown, and theirs attributes and competences are described. It was claimed that the profession of the information analyst required a diligence, knowledge, analytical skills, talent and natural ability for analysis of facts and data. The information analysis could be considered as an art, so only people with the analytical potential could be successful in this profession. The ethical aspect of the information analysis is also pointed out.

Keywords: information warfare, analyst, information analysis, analytical skills, information literacy, information management, information analysts' education

Jadwiga Stawnicka
Wyższa Szkoła Biznesu w Dąbrowie Górniczej

Manipulacja w cyberprzestrzeni. Mity i prawdy o anonimowości

Wstęp

Celem niniejszego artykułu jest prezentacja wybranych zagrożeń związanych z użytkowaniem Internetu, w których dokonuje się manipulacji użytkownikiem w oparciu o funkcjonujący mit anonimowości manipulatora w cyberprzestrzeni. Manipulator, przekonany o swojej anonimowości, stosuje różnorodne formy wpływu na ofiary. Co więcej, manipulator jest przekonany, iż jeśli internautę można wyśledzić wyłącznie, mając do dyspozycji jego numer IP i pseudonim, jakim podpisuje się np. na forum internetowym, to może się czuć bezkarny i publikować w Internecie teksty o różnej treści, szczególnie deprecjonujące i znieważające, nie będąc zidentyfikowanym. Wiele zależy od sposobu połączenia z siecią komputera oraz operatora, dostarczającego usługę dostępu do Internetu szukanej osobie. Adres IP może nie identyfikować jednoznacznie danego urządzenia, a może równie dobrze wskazywać operatora. Użytkownik sieci ujawnia przy tym swoje dane w sposób świadomy i nieświadomy. W sposób świadomy użytkownik ujawnia swój adres poczty elektronicznej, profile w komunikatorach, identyfikatory w portalach społecznościowych, wiadomości na forach, grupach dyskusyjnych i w portalach informacyjnych. Natomiast w sposób nieświadomy użytkownik udostępnia także część swoich danych np. adresy elektroniczne odwiedzanych serwisów (banków, sklepów internetowych), informacje o odwiedzanych stronach, pytania zadawane w wyszukiwarkach, informacje o kolejności wykonywanych czynności (np. z jakiej strony na jaką kolejną stronę wchodzi), informacje zawarte w plikach cookie, identyfikatory dostępu do usług i serwisów (*loginy, nicki*).

Użytkownik pozostawia również inne dane w sposób nieświadomy – dane językowe – ślad językowy, wpisy (teksty), których jest autorem. Na podstawie tekstów „pozostawionych" w Internecie można określić cechy językowe stylu autora. Autorka niniejszego artykułu, jedyna w Polsce biegła z lingwistyki kryminalistycznej, wykonuje od lat ekspertyzy na użytek wymiaru sprawiedliwości w celu zidentyfikowania sprawcy właśnie na podstawie jego cech językowych.

Pojęcie manipulacji w cyberprzestrzeni

Pojęcie manipulacji zostaje w niniejszym artykule uściślone do wpływu na sposób postrzegania świata. W cyberprzestrzeni internauci stają się obiektami oddziaływania sterowanego między innymi poprzez personalizację, marketing

behawioralny, sponsoring, gry komputerowe, autokreację sieciową, cyberterroryzm, psychomanipulację na stronach WWW, czatach, komunikatorach, upowszechnianie patologii w Internecie. Personalizowanie w Internecie związane jest np. z zapisywaniem każdej aktywności użytkownika związanej z użyciem usług Google, a także umożliwieniem tworzenia indywidualnych wyników wyszukiwania użytkownika oraz osobistej strony głównej wyszukiwarki Google. W kontekście marketingu behawioralnego można mówić o analizowaniu zwyczajów w odniesieniu do poczty elektronicznej oraz o analizie treści w darmowych skrzynkach pocztowych. Manipulacja poprzez sponsoring odbywa się poprzez pozycjonowanie, polegające na umieszczaniu na liście rezultatów wyszukiwania wyszukiwarki adresów tych stron, których właściciele wnieśli stosowne opłaty. Liczba wskazanych linków na innych stronach może również prowadzić do zwiększenia popularności określonej witryny. Z kolei wykupywanie słów kluczowych strategicznych dla konkurencji prowadzi do blokady tych słów w wyszukiwarce. W przypadku gier komputerowych można mówić o ich wpływie na wirtualną tożsamość graczy i wykorzystywaniu siły perswazyjnej gier. Użytkownik Internetu poruszając się w cyberprzestrzeni pozostawia ślad informatyczny[1]. Np. za każdym razem, gdy użytkownik odwiedza stronę internetową, wysyłane jest żądanie kodu HTML, który jest następnie przetwarzany w przeglądarce zainstalowanej na komputerze. Kod ten może zawierać zewnętrzne odnośniki, które również zostaną objęte tym samym żądaniem (Misztal, Czapla bd.). Jak wskazano powyżej, oprócz śladów, internauta pozostawia jeszcze jeden typ śladów, po których można go identyfikować, jest nim ślad językowy.

Pojęcie lingwistyki kryminalistycznej

Lingwistyka kryminalistyczna (językoznawstwo kryminalistyczne), ang. *forensic linguistics*, niem. *forensische Linguistik* zajmuje się wykorzystaniem wiedzy językowej dla celów wykonywania czynności śledczych i prawnych i jest **częścią lingwistyki stosowanej, funkcjonuje zatem na pograniczu językoznawstwa i kryminalistyki. Samo zaś językoznawstwo jest dyscypliną otwartą, co prowadzi do zintegrowania wielu dyscyplin przy uwzględnieniu wykorzystania we współczesnych badaniach języka narzędzi różnych dyscyplin naukowych.**

Badacz-lingwista poszukuje dowodu wykonawstwa bądź autorstwa tekstu oraz uzyskiwania dowodu zrozumienia tekstu. Ekspertyzy lingwistyczne opierają się zarówno na właściwościach leksykalnych, ortograficznych i fonetycznych, jak i składniowych analizowanych tekstów i dotyczą między innymi: ustalania intencji nadawcy komunikatu np. w sprawach o groźbę karalną, pomówienie czy zniewagę, oceny formy i charakteru wypowiedzi uważanych za obraźliwe, uwłaczające godności, ustalania autorstwa wypowiedzi (np. groźby, listy

samobójcze, żądania okupu); możliwości ustalania autorstwa anonimowych tekstów w Internecie, identyfikacji nadawcy ze względu na kraj pochodzenia, badania treści wpisów stalkerów, cyberstalkerów, wskazywania cech językowych stalkerów i cyberstalkerów, które mogą zidentyfikować nadawcę komunikatu, analizy treści sms, wpisów na blogach, forach – wskazywanie autorów/wykonawców, określania wieku, wykształcenia, pochodzenia na podstawie analizy językowej nadawcy.

W niniejszym artykule zostaną wskazane jedynie niektóre możliwości wykorzystania analizy lingwistycznej w kwestii ustalania autorstwa tekstów zamieszczanych w Internecie.

Ustalenia autorstwa anonimowych wpisów w sieci

Językoznawca ustala autorstwo wpisów w Internecie poprzez cechy idiolektu osobniczego. Idiolekt jest językiem pojedynczego użytkownika języka w danym okresie jego życia. Cechy idiolektu możliwe są do wyróżnienia dzięki temu, iż jednostka posiada pewne skłonności lub stałe cechy swojej aktywności językowej (Witosz 2009, s. 250). Na kształt idiolektu wpływają czynniki biologiczne (wiek, płeć, stan zdrowia), społeczne (rodzina, wykształcenie, zawód, zainteresowania, pochodzenie geograficzne, narodowość), interakcyjne (kontekst społeczny, tematyka, charakterystyka współuczestników kontaktu językowego, doświadczenia jednostki wynikające z historii jej życia) (Johnston 2009). Ślady obecności wymienionych czynników dają informacje o idiolekcie nadawcy. Najlepszym materiałem do opisu idiolektu są tzw. dokumenty osobiste, teksty prywatne, o swobodnej formie, przede wszystkim listy prywatne. Cechy idiolektu przejawiają się poprzez stopień znajomości słownictwa i gramatyki języka ogólnego, jak również przez indywidualne skłonności do używania w określonych sytuacjach określonych wyrazów i do łączenia ich ze sobą w określony sposób. Pojęcie idiolektu powinno uwzględniać czynnik temporalny i społeczny oraz kontekst sytuacyjny, a więc zróżnicowanie zmian w życiu człowieka, zróżnicowanie społeczne i sytuacyjne (np. dyskurs administracyjny, specjalistyczny, potoczny). Natomiast idiostyl jest stylem samego tekstu i obejmuje użycie określonych środków językowych, ich organizację, określenie intencji nadawcy i celu komunikacyjnego (Kudra 2011). Idiolekt jest determinowany przez stopień znajomości słownictwa, stopień znajomości gramatyki, jak również indywidualne skłonności używania w określonych sytuacjach określonych wyrazów. Mowę jednostkową osoby poznajemy z tekstów wytwarzanych przez tą osobę. Należy jednak uwzględnić zróżnicowanie cech osobniczych ze względu na wiek człowieka i jego ciągły rozwój, a także zróżnicowanie stylu tekstów. **A zatem na podstawie indywidualnego użycia środków językowych na poziomie leksykalnym i gramatyczno-syntaktycznym można z dużym prawdopodobieństwem identyfikować nadawcę**, a nawet – jeśli cechy językowa są wyraziste – można

udzielić odpowiedzi w sposób kategoryczny. W czasach „hejtu" i walki z tzw. mową nienawiści, biegły językoznawca może wskazać, czy konkretne wypowiedzi noszą takie znamiona. Pojęcie „anonimowego cyberstalkera" w ujęciu lingwistycznym (językoznawczym) jest oksymoronem, tj. metaforycznym zestawieniem wyrazów o przeciwstawnym, wykluczającym się wzajemnie znaczeniu, np. *gorzkie szczęście, wymowne milczenie,* gdyż anonimowość cyberstalkera w sieci zostaje podważona.

Stalker ma na celu zdobycie kontroli i zdominowanie ofiary i coraz częściej wykorzystuje do dręczenia ofiary Internet. Cyberstalking jest używaniem Internetu oraz wszelkiego rodzaju mediów elektronicznych do nękania drugiej osoby i manipulowania drugą osobą poprzez komentarze na forach internetowych, przesyłanie informacji za pomocą komunikatorów, wysyłanie niechcianych wiadomości e-mail, poprzez umieszczanie obraźliwych i obelżywych uwag na stronach internetowych czy też zdjęć mających kogoś upokorzyć.

Pozorna anonimowość w Internecie. Studium przypadku

Wśród ekspertyz, które wykonuję dla Wymiaru Sprawiedliwości, znajdują się także ekspertyzy dotyczące ustalenia autorstwa wpisów zamieszczanych na forach internetowych, w tym wpisów obraźliwych. Żeby dokonać takiej analizy i móc wskazać autora wpisu, trzeba dysponować materiałem porównawczym. Jeśli typowana jest jedna osoba, która mogłaby być autorem wpisów, wówczas analizowany jest materiał porównawczy autorstwa tej osoby. Jeśli typowanych jest kilka osób, to wówczas na podstawie analizy materiału dowodowego i porównawczego można przynajmniej wyeliminować jedną z nich, czy wyeliminować kilka osób lub wskazać osobę właściwą. Oto omówienie studium przypadku:

Anonimowy stalker nękał w sieci swoją byłą przyjaciółkę, która nie życzyła sobie utrzymywać z nim kontaktu. Zamieszczał wpisy w sieci, w których autorami – pozornie były różne osoby, posługujące się różnymi nickami (np. *teczowybigos, Samksiaze, seagull, egipcjanin, bondzio3 i diabel9777*). We wpisach deprecjonował ofiarę oraz firmę, której była właścicielką. Nękał także swoją ofiarę SMS-ami, pisał anonimy do instytucji, zawierające treści deprecjonujące firmę i jej właścicielkę. Analiza materiału językowego wskazała, że była to ta sama osoba, Marek S., były przyjaciel ofiary. W ekspertyzie językoznawczej poszukiwałam odpowiedzi na pytanie:

Czy idiolekt wyodrębniony z przedłożonego do badań materiału kwestionowanego w postaci anonimowych i maskowanych zapisów, jest idiolektem Marka S. wyodrębnionym z przedłożonego do badań materiału porównawczego?

Badania przeprowadzono w oparciu o metodę lingwistyczną, polegającą na analizie jakościowej tekstów. Na podstawie analizy cech językowych, leksykalnych,

słowotwórczych i składniowych zawartych w materiale porównawczym, wyodrębniono cechy idiolektu Marka S., po czym poszukiwano cech idiolektu Marka S. w materiale dowodowym, w którym sprawca posługiwał się 16 Nickami. **W pierwszym etapie badań** ustalono cechy idiolektu (języka osobniczego, języka indywidualnego) czyli zespołu indywidualnych cech językowych Marka S. Wszystkie te cechy sklasyfikowano i opisano, podając do każdej cechy przykład lub przykłady pochodzące z materiału porównawczego. **W drugim etapie** poszukiwano cech idiolektu wyodrębnionych z materiału porównawczego w materiale dowodowym.

Kierunek postępowania badawczego może być różnorodny. Można najpierw ustalić cechy idiolektu w materiale dowodowym, a później wyodrębnić cechu idiolektu w materiale porównawczym, po czy porównać cechy materiału dowodowego oraz porównawczego. Można również ustalić cechy idiolektu w materiale dowodowym, po czym poszukiwać tych cech w materiale porównawczym. Ta ostatnia możliwość, związana z wyodrębnieniem cech idiolektalnych materiału dowodowego jest stosowana, kiedy materiał dowodowy stanowi jeden dokument. W przypadku postawienia hipotezy, iż autorem wpisów może być Marek S., materiał dowodowy był bardzo zróżnicowany: były to komentarze i wpisy na blogach, Facebooku, pisma kierowane do różnych instytucji oraz korespondencja mailowa. A zatem, po wyodrębnieniu cech idiolektu Marka S., w każdym z dokumentów stanowiących materiał dowodowy poszukiwano cech idiolektu Marka S. Po przeprowadzeniu analiz materiału porównawczego oraz materiału dowodowego sformułowano wnioski dotyczące ustalenia, czy autorem zapisów anonimów oraz zapisów podpisanych, a rzekomo pochodzących od innych osób przedłożonych do badań jako materiał porównawczy, jest Marek S.

W ramach analizy komparatystycznej wyłoniono cechy językowe wspólne cechom idiolektalnym Marka S. oraz każdemu z dokumentów. Dokumentów było 27, a zatem analiza komparatystyczna składała się z 27 komponentów. Poniżej przytaczam fragmenty analizy[2]:

Na podstawie przeprowadzonej analizy materiału porównawczego, można wymienić cechy idiolektu Marka S. Nie wyklucza się przy tym występowania innych cech, które mogłyby zostać wyeksponowane i omówione przy analizie materiału dowodowego. Każda z cech została w opinii scharakteryzowana z podaniem i omówieniem przykładów. Wyróżniono między innymi następujące cechy idiolektu Marka S.: tendencja do hiperbolizacji („***żenujący temat***", „***stronniczy*** *wybór*", „***luksusowy*** *samochód*", "***rewelacyjny*** *temat*"), użycie parentezy jako przejaw tendencji do precyzji zawartości treściowej komunikatu, użycie cudzysłowu apostrofowego, użycie synonimów (*Widzę, że został Pan* ***przygotowany/ zmanipulowany, nakierowany*** *do odróżniania prawdy*[3]); użycie imiesłowów przysłówkowych współczesnych (*irytowalby mnie Pan* ***relacjonując*** *swoje kolejne działania; chwyta pan głodne kawałki,* ***niepotrafiac*** *się*

zdystansować od przerosnietego ego swojej szefowej", *„postanowiłem zawiadomić również Państwa jednocześnie* ***nakłaniając*** *do podjęcia natychmiastowych działań dbających o zapewnienie bezpieczeństwa dzieci*", błędna pisownia wyrażeń przyimkowych (połączenie przyimka z przysłówkiem **„napewno"*[4]; połączenie przyimka z rzeczownikiem **nadwyraz*: pisane jest łącznie: *traktować* ***nadwyraz*** *poważnie sytuacje*", pisownia rozdzielna formy trybu przypuszczającego czasownika *móc,* użycie rzeczowników kategorii *nomina actionis* (*zaproponowałem* ***pojechanie*** *i* ***przywiezienie*** *monitora; chciałem napisania tego listu*). Cech idiolektu Marka S. poszukiwano w każdym z 27-miu dokumentów. Przy tym, jeśli np. w dokumencie nr 1, stanowiącym materiał dowodowy wystąpiły cechy idiolektalne Marka S. i przypisano temu dokumentowi autorstwo Marka S., to pojawiające się cechy idiolektalne Marka S., które wystąpiły w dokumencie nr 1, a nie było ich w materiale porównawczym, uzupełniły listę cech, charakterystycznych dla idiolektu Marka S.

W zapisach osoby posługującej się nickiem *teczowybigos* wystąpiły między innymi cechy: tendencja do hiperbolizacji przejawiająca się poprzez użycie kontrastowego zestawienia *„dżentelmeni – stażyści*", przeciwstawienie *„być rozproszonym atrakcjami*", wyraziste i obrazowe metafory (*eksplodujące doznania*, *konsumować doznania*, *kuluary zaplecza*). Nickiem tym posługiwał się zatem Marek S.

Autorstwo treści zamieszczanych w Internecie

Oto wybrane przykłady wykorzystania opinii biegłego językoznawcy w kwestii ustalania autorstwa teksów. Dariusz P. – oskarżony o podpalenie domu w dniu 10 maja 2013 r. w Jastrzębiu Zdroju, w którym znajdowała się jego żona i dzieci, co spowodowało ich śmierć – został zatrzymany m.in. na podstawie analizy SMS-ów z pogróżkami, które – jak twierdził – otrzymywał. Ekspert potwierdził, że autorem SMS-sów z pogróżkami jest ta sama osoba, która udzielała wypowiedzi prasie.

Zbigniew P. używając Nicka *„macho777"* zamieszczał na stronach internetowych poradniki, jak zrobić bombę z niczego tj. mając do dyspozycji osiedlowy sklep ogrodniczy i drogerię. Zachęcał do wypróbowania tak skonstruowanych bomb. Marian P. proponował sprzedaż amfetaminy, a jego kolega Arkadiusz Z. uczył, jak otrzymać siarczan amfetaminy. Inny internauta groził, iż pozbawi życia jednego z prezydentów miast. Różnego rodzaju grupy nazistowskie czy antysemickie zamieszczają hasła propagujące brak tolerancji do innych kultur, sympatię z nacjonalistami z RPA, wymierzania sprawiedliwości na własną rękę. Symbolika takich tekstów ma charakter hybrydowy i wyrażana jest zarówno przez środki należące do kodu językowego, jak i wizualnego (np. rysunki szubienicy, symbol „Krzyża celtyckiego"). Nadmienić należy, iż ustalenia intencji nadawcy poprzez semantyczną i pragmatyczną interpretację tekstów, symboli

i wizerunków znajdujących się na materiale dowodowym dokonuje również biegły językoznawca.

Pojmujemy Internet jako globalną społeczno-kulturową wioskę, wirtualne forum, na którym można eksperymentować poprzez manipulację władzą, tożsamością i płcią. W tym miejscu należy podkreślić możliwości stosowania technik uwodzenia przez Internet, kiedy manipulator oferuje przyjaźń, zaprasza do udziału we wspólnych przedsięwzięciach, przyciąga potencjalną ofiarę, w tym dziecko i manipuluje ofiarą w celu doprowadzenia do bezpośredniego kontaktu poza Internetem. Ponieważ Internet jest anonimowy, sprawcy mogą udawać osobę o dowolnej charakterystyce, a nawet udawać, iż mają tyle samo lat, ile ich rozmówca, aby dziecko było przekonane, iż je rozumie. Jeden ze sprawców mówił, iż ma tyle samo lat, co ofiara, że jego rodzice się rozwiedli, że bardzo to przeżywa i że ma młodszą siostrę. Inny po jakimś czasie rozmowy przyznał, iż rodzice zabronili mu korzystania z Internetu i kontakt z ofiarą będzie utrzymywał jego starszy brat. Dziecko nie tylko zaakceptowało najpierw swego rozmówcę rówieśnika, ale i później osobę starszą, do której również miało całkowite zaufanie. Aby jednak udawać nastolatka, trzeba używać odpowiednich wyrażeń językowych, używanych przez młodzież. Oto fragment rozmowy na Facebooku dwóch nastolatków. Aby być jednym z nich, grać rolę jednego z nich, trzeba posługiwać się ich specyficznym socjolektem:

- *Siema, wpadne po obiedzie, pasi*
- *Sorniaczek, dzisiaj nie mogę, chujowo się czuje, ledwo mowie, jeszcze raz sorx*
- *Okejoza robaczanych snow*
- *Ah będziesz jutro?*
- *Nie wiem wszystko takie jekies wyjebane ostatnie 2 dni siedzialem na fejsie i nikogo ani nigdzie*
- *No to dobranocka*
- *Elo melo piec dwa zero idx spac penero bo nie wstaniesz na melo*
- *EEEv przespoko mega progres*

A zatem, żeby w Internecie grać rolę nastolatka, trzeba przygotować się do tej roli od strony językowej. A zmieniając perspektywę można byłoby zapytać o możliwość wykorzystania umiejętności językoznawcy w celu manipulowania odbiorcą – osobą dorosła, udającą dziecko w korespondencji internetowej, aby była przekonana, że rozmawia z dzieckiem, podczas gdy rozmowa poprzez komunikator internetowy będzie prowadzona np. z funkcjonariuszem Policji.

Na zakończenie jedna z wielu spraw, w których autorka tekstu – jako biegły językoznawca – wydawała opinię w kwestii ustalenia autorstwa wpisów anonimowych na blogu. Sprawa została nazwana kryptonimem *Leśny duszek*. Osoba używająca Nicka „lesnyduszek” dokonywała przez bardzo długi czas (około 2 lat) wpisów na blogu, oczerniających jedną z firm oraz poszczególnych pracowników firmy, podając tym samym do publicznej wiadomości fakty z życia

prywatnego poszczególnych pracowników. Podejrzewano, iż osobą dokonującą wpisów i używającą Nicka może być Janina Kowalska, pracownica firmy. Dokonano analizy korpusu dowodowego (liczne wpisy na blogu) i porównawczego (pisma autorstwa Janiny Kowalskiej) z punktu widzenia: błędów językowych, form gramatycznych, interpunkcji i ortografii, użycia parentez, podkreślanie elementów w kontekście, użycie pytań retorycznych, skonwencjonalizowanych zwrotów, substytutów komponentów niewerbalnych w kontekście i w jakich miejscach się pojawiają, użycie cudzysłowu apostrofowego, użycie powtórzeń, pojawienia się w tekstach synonimów. Osoba używająca Nicku „lesnyduszek" stosowała np. tzw. cudzysłów apostorofowy: *„zapomnial" nr telefonu do pogotowia, To on „zapomnial" numeru telefonu do pogotowia*; również dla wyodrębnienia wyrazów użytych ironicznie: *„kupiła" od developera ten lokal; odziedziczył „ten spadek"; co to za „wielka" osoba*. Ta sama cech językowa pojawiła się u Janiny Kowalskiej (to było ich „wspólne życie", „zapomniał" o swoich obowiązkach). Osoba posługująca się Nickiem „lesnyduszek" używała synonimów przy opisie sytuacji, co służyło również wyrażaniu emocji negatywnych, np. *serce (zimne, podłe*); *sumienie, prawość i uczciwość*; *chorowity, kapryśny, zdyzelowany (samochód*), ale i synonimów o zabarwieniu neutralnym: *Odstąpić/sprzedać lokal* (s. 63), najczęściej jednak rzeczownikowe: *zgodnie z wyrysem / szkicem*, *domek/altanka*, *po trudach całego dnia/tygodnia*. Janina Kowalska również używała synonimów, np. *ten domek / siedlisko; to był akt bezprawia, wandalizmu i okrucieństwa*. Osoba posługująca się Nickiem „lesnyduszek" używała parentez (wtrąceń) przy opisach różnych sytuacji, np. *Znacznie trudniej byłoby mi podjęć decyzję, gdybym nie odkrył (tak jak w przypadku innych działań), jakie nakłady zostały poczynione na rzecz tego oszusta / gawędziarza*, podobnie czyniła Janina Kowalska, np. *Przebywający w tym czasie w budynku ludzie (wraz z 4 letnim dzieckiem) narażeni są na niebezpieczeństwo.* Zaobserwowano również podobny układ kompozycyjny wypowiedzi w postaci początkowowej tezy (pierwsze wypowiedzenie tekstu), rozwijanej zwykle w ciągach skojarzeniowych oraz finalizowanej przez krótką puentę, np. *Kłamstwo króluje! Już nie pierwszy raz mieliśmy okazję, żeby to zaobserwować* („lesnyduszek") oraz *Głupota górą! W dzisiejszych czasach (początku XI wieku, kiedy oszuści / szarlatani dochodzą do glosu trudno o uczciwość, a wszyscy mają w dupie potrzebujących. Uważajmy na zakretach (gdzie pelno poszustow i krętaczy*) (u Janiny Kowalskiej). Zarówno „lesnyduszek" jak Janina Kowalska stosowali pytania retoryczne, np. Nie wolno i co z tego? *No bo jakie mieszkanie nie ma „czynszu"? I taka osoba twierdzi, że pomaga ludziom?* („lesnyduszek") i *Czego możemy spodziewać się po takiej osobie?* (Janina Kowalska). Zanalizowano również błędy językowe, w tym interpunkcyjne, stylistyczne popełniane przez osobę, używającą Nicka „lesnyduszek" i porównano je z tekstami, których autorem była Janina Kowalska. Na podstawie dokonanej analizy komparatystycznej materiału dowodowego oraz porównawczego

stwierdzono, iż osoba posługująca się Nickiem „lesnyduszek” i Janina Kowalska to ta sama osoba.

Zakończenie

Na zakończenie stwierdzić należy, iż nasza anonimowość w Internecie jest pozorna nie tylko ze względu na ślady o charakterze informatycznym, które pozostawia użytkownik w sieci, ale i ze względu na cechy językowe nadawcy komunikatów zamieszczanych w sieci. Rola językoznawcy dokonującego analizy cech językowych nadawcy jest nieoceniona. Zaznaczyć należy, iż przy dokonywaniu analizy lingwistycznej niebagatelne znaczenie ma obszerność materiału porównawczego, z którego wyłania się cechy językowe autora. Z dotychczasowych obserwacji wynika, iż im krótszy jest materiał kwestionowany, tym dłuższy powinien być materiał porównawczy. W przypadku badań materiału dowodowego, który jest tekstem długim tekstu długiego, materiał porównawczy powinien być co najmniej dwa razy dłuższy, w przypadku tekstu krótkiego stanowiącego materiał dowodowy, materiał porównawczy powinien być kilkanaście razy dłuższy. Poza tym materiał porównawczy powinien być podobny pod względem formy do materiału zakwestionowanego. Szczególną trudność dla językoznawcy może stanowić dokonanie analizy w przypadku posiadania materiału porównawczego, należącego do dyskursu urzędowego oraz wpisów na blogu, należących do dyskursu potocznego. Poza tym materiał porównawczy powinien pochodzić z okresu sporządzenia materiału dowodowego.

Przypisy

[1] Nie poruszam tutaj kwestii wykorzystania narzędzi służących do anonimizacji aktywności w Internecie, np. The Onion Router (TOR) – projekt zapobiegający analizie ruchu sieciowego System Linux TAILS, system The Amnesic Incognito Live System, znany jako TAILS Serwer proxy (przekaźnikowy), pośredniczący w przesyłaniu informacji czy generatory fałszywych tożsamości oraz anonimowe skrzynki e-mail.

[2] Cechy językowe przytaczanych przykładów zostały zmodyfikowane, aby uniemożliwić identyfikację sprawcy.

[3] W przykładach zachowano oryginalną pisownię.

[4] Przy pomocy znaku graficznego (*) oznaczono błędną pisownię.

Bibliografia

Kudra, A. (2011) *Idiolektostylem w mur, czyli o idiolekcie, idiostylu i krytycznej analizie dyskursu – na przykładzie felietonów Krzysztofa Skiby w tygodniku „Wprost”*. „Folia Litteraria Polonica”, nr 14, s. 27-34.

Gogołek, W. (2007) *Manipulacja w sieci*. W: Siemieniecki, B. (red.), *Manipulacja. Media. Edukacja.* Toruń: Wydaw. Adam Marszałek.

Johnston, B. (2009) *Stance, Style, and the Linguistic Individual*. W: Jaffe, A. (red.). *Sociolinguistic Perpectives on Stance*. New York: Oxford, s. 29-52.

Misztal, K., Czapla, P., *Jak namierzyć i obserwować czyjąś działalność w Internecie i jakie są tego skutki.* Data dostępu: 03.02.2016. Tryb dostępu: https://pikbloog90.wordpress.com/2012/11/08/jak-namierzyc-i-obserwowac-czyjas-dzialalnosc-w-internecie-i-jakie-sa-tego-skutki/.

Stawnicka, J. (2015) *Lingwistyka w służbie kryminalistyki. Diagnozy i prognozy.* W: Hołyst, B., Stawnicka, J., Potejko, P. (red.), *Optymalizacja procesów przepływu informacji w sytuacjach zagrożenia bezpieczeństwa państwa*. Szczytno: Wydawnictwo WSPol, s. 9-28.

Stawnicka, J. (2014) *Twój język Cię zdradza?* „Iustitia”, nr 4.

Stawnicka, J. (2015) *Językoznawstwo w służbie wymiaru sprawiedliwości*. „Kwartalnik Policyjny”, nr 2, s. 40-42.

Suchodolska, M. (2016) *Język zdradza jak odciski palców.* „Gazeta Prawna”, 20.05.2016, s. 4-6.

Witosz, B. (2009) *Dyskurs i stylistyka*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Streszczenie

W artykule opisano, czym jest kryminalistyczne językoznawstwo, zajmujące przestrzeń pomiędzy lingwistyką (nauką języka) i prawem, w tym organów ścigania. Wskazano możliwości wykorzystania badań w zakresie lingwistyki kryminalistycznej w aspekcie teoretycznym i praktycznym. Artykuł wskazuje ogromne możliwości otwierające się przed lingwistyką kryminalistyczną w kontekście możliwości wykorzystania językoznawcy, jego wiedzy i kwalifikacji w celu pracy na rzecz wymiaru sprawiedliwości.

Słowa kluczowe: lingwistyka kryminalistyczna, mowa nienawiści, anonim

Manipulation in cyberspace. Myths and truths about anonymity

Abstract

This paper begins by describing what forensic linguistics is, namely the interface between linguistics (the science of language) and the law, including law enforcement. This paper discusses forensic linguistics research from theoretical aspects and practical aspets. The article suggests that the future of Forensic Linguistics will be bright if linguists work on these issues, and also on acquiring skills, knowledge and qualifications in other disciplines in order to better prepare them for working in and with courts.

Keywords: forensic linguistic, hatespeech, anonym

Przemysław Mazur
Uniwersytet Pedagogiczny w Krakowie

E-dżihad, *soft power* radykalizmu islamskiego

Joseph S. Nye zauważył, że zdobywanie ludzkich serc i umysłów zawsze było ważne, ale w epoce globalnej informacji jest to jeszcze ważniejsze. *Informacja to władza, a nowoczesna technologia informatyczna rozpowszechnia informację znacznie szerzej niż kiedykolwiek w historii* (Nye 2007, s. 30). Wielu polityków nie jest jednak w stanie zrozumieć fenomenu zmiany w obrębie pojęcia władzy we współczesnym globalizującym się świecie. Najlepszym tego przykładem była administracja Georga W. Busha z Donaldem Ramsfeldem na czele. To oni wypowiedzieli wojnę terroryzmowi, a tak naprawdę, światu islamskiemu, a jedyną metodą jaką znali była przemoc, czyli twarda siła (z ang. *hard power*). Nye wyraźnie pokazuje, że tym samym Ameryka zaprzeczyła swoim ideom i przekreśliła swoje dotychczasowe sukcesy osiągnięte dzięki temu, co nazywa *soft power*. Wygrana z ZSRR w większym stopniu była możliwa dzięki atrakcyjności „American dream", niż faktycznej rywalizacji zbrojnej. Nie rozumienie tego, połączone z kulturową arogancją spowodowały konfrontacje ze światem islamskim.

Klasyczna teoria zderzenia cywilizacji Samuela Huntingtona (Huntington 1995), okazała się urzeczywistniać przy wydatnej pomocy polityków Zachodu. Igranie z radykalnymi postawami rodzącymi się w świecie muzułmańskim dla doraźnych celów politycznych, spowodowało, że w krótkim czasie tacy ludzie, jak Osama bin Laden z mudżahedina walczącego wspólnie z Amerykanami przeciwko radzieckim najeźdźcom Afganistanu, stał się ich śmiertelnym wrogiem. Nałożenie się na siebie bardzo wielu czynników, takich jak dysproporcje ekonomiczne, ubóstwo, podporządkowanie gospodarcze, problemy natury tożsamościowej okazało się bardzo dobrym gruntem do rozwoju radykalnych ruchów, głównie związanych z nurtem sallafiji (Jamsheer 1995; Danecki 1997). Jest to ruch religijny odrzucający postęp w zachodnim rozumieniu, nawołujący do powrotu do korzeni islamu i oparcia rzeczywistości społecznej i politycznej o prawo koraniczne (*szariat*) i wartości wynikające z Koranu i Sunny. Militarna i ekonomiczna obecność Zachodu w świecie arabskim tylko potęgowały antagonizm, który dał swój upust w postaci terroryzmu i powstawania kolejnych organizacji ekstremistycznych, z Al-Kaidą na czele.

W 2008 roku doszło na łamach prasy amerykańskiej, jak i w środowisku akademickim, do poważnego sporu teoretyków terroryzmu islamskiego. W związku ze znacznym rozbiciem Al-Kaidy część naukowców i analityków z Brucem Hoffmanem na czele, uznało, że terroryzm już nie będzie większym zagrożeniem, chyba że uda się odbudować struktury organizacyjne. Uważano, że

terroryzm islamski może się rozwijać jedynie dzięki posiadaniu określonych struktur, było to stanowisko zbliżone do teorii instytucjonalnej. Inną opinię przedstawił, urodzony w Polsce, socjolog Marc Sageman. Uznał on, że terroryzm jest zjawiskiem oddolnym, opartym na przesłankach społecznych. Zatem może on znów powrócić i nie potrzebuje do tego struktur. Wynika to ponadto z dostosowania się zarówno do amerykańskiej strategii walki, jak i zmieniających się realiów społecznych, technologicznych – po prostu globalizmu. Szczególną rolę może odegrać tutaj Internet i zjawisko samoradykalizacji. Internauci mający problemy natury tożsamościowej, mogą sami zradykalizować się i przystąpić do zbrojnego dżihadu, a rozbudowane struktury nie są do tego potrzebne (Sciolino, Schmitta 2016). Obie opcje sprawdziły się, ponieważ powstało tzw. Państwo Islamskie, a zatem instytucja. Jednocześnie występują coraz liczniejsze przypadki samoradykalizacji i działań samorzutnych.

Internet drogą do radykalizacji, mit czy prawda?

2 marca 2011 roku we Frankfurcie w wyniku zamachu zginęło dwóch amerykańskich żołnierzy, a dwóch kolejnych zostało rannych. Zamachu dokonał Arid Uka, dwudziestojednoletni Kosowianin. W zeznaniach przyznał, że nie jest członkiem żadnej organizacji terrorystycznej, nigdy też nie był w żadnym obozie szkoleniowym. To, co pchnęło go do zamachu, to film opublikowany przez Islamski Ruch Uzbekistanu (Ўзбекистон исломий ҳаракати/O'zbekiston islomiy harakati), ukazujący amerykańskich żołnierzy gwałcących dziewczynę. To wydarzenie miało mieć miejsce w Afganistanie, ale w rzeczywistości byli to Irakijczycy w amerykańskich mundurach. Film sprowokował Arid Uka do ataku na amerykańskich żołnierzy, którzy we Frankfurcie nad Menem, mieli lotnisko przesiadkowe do Afganistanu (Steinberg 2012b, s. 7).

Hoda Muthana to młoda dziewczyna pochodzenia jemeńskiego z Hoover, w stanie Alabama, USA. W wieku 17 lat zainteresowała się fundamentalizmem islamskim, korzystając z materiałów internetowych (jej rodzina nie praktykowała islamu, nie mogła zatem zostać zwerbowana w meczecie). Doskonale orientując się w skutecznym sposobie korzystania z mediów społecznościowych bardzo szybko zdobyła tysiące zwolenników. Tak zwerbowała Aqsa Mahmood, pierwszą kobietę ze Szkocji, która wyjechała do Syrii (19 lat). Sama też wyjechała do Raqqi i wstąpiła w szeregi ISIS (Islamskie Państwo Iraku i Syrii), poślubiła australijskiego dżihadystę Suhan al Rahman (*vel* Abu Jihad al Australi). Będąc już na miejscu Muthana kontynuowała werbunek i działania propagandowe na Twitterze, tak pozyskała 24-letniego nowojorczyka Sammyego i 42-letniego Ahmed Mohammed El Gammal'a z Arizony. Jej posty na Twitterze były bardzo radykalne, wzywała np. do zmasakrowania weteranów armii amerykańskiej podczas ich parady (Vidino, Hughes 2016). Jej życiorys ukazuje drogę od samodzielnej radykalizacji wynikającej głównie z problemów tożsamościowych i nieodnajdywania się w społeczeństwie

zachodnim do wejścia w struktury organizacji terrorystycznej i wykorzystania Internetu jako narzędzia do pozyskiwania nowych członków. Takich przykładów udanych werbunków, jak i samoradykalizacji można odnotować wiele.

Rozwój wykorzystania Internetu przez terroryzm islamski

Sposób wykorzystania Internetu dla ruchów radykalnego islamu zmieniał się w zależności od rozwoju technologicznego i sekwencji kolejnych zdarzeń natury politycznej i militarnej. E-dżihad to wykorzystanie technologii informatycznych w tym Internetu do walki dżihadu. Pojęcie to pochodzi z Koranu i ma dwa znaczenia, tzw. dżihad daleki i bliski. Ten pierwszy oznacza *de facto* dżihad wewnętrzny, czyli drogę do wyzwolenia się ze swoich słabości, dążenie do samodoskonalenia. Dżihad bliski to zbrojna obrona swoich idei, religii, wspólnoty (*ummy*) i terytorium danego od Boga (*dar al-islam*). Zasadniczo ten dżihad to walka obronna. Taką interpretację użył szejk Abd Allah Jusuf (Abdallah) Azzam wzywając wyznawców islamu do obrony Afganistanu przed najazdem radzieckim. Okazało się to skutecznym narzędziem, gdyż Koran nakłada w takiej sytuacji obowiązek walki (militarnej lub przez wsparcie walczących innymi metodami) i to bez względu na obowiązki wobec władzy państwowej, plemiennej czy rodzinnej. Wraz z upadkiem ZSRR dżihad przestał być już potrzebny, do czasu agresji USA na Irak, wówczas znów można było sięgnąć do tej idei. Pewną zmianą było wezwanie ucznia Azzama, czyli bin Ladena, który w fatwie z 1998 r. (Sageman 2008, s. 21) wezwał do zabijania Amerykanów, gdzie tylko się znajdują, także poza *dar al-islam*. Stworzono zatem nową interpretację wojny obronnej. W tym wymiarze e-dżihad wpisuje się w oba rozumienia dżihadu – dalekiego czyli formy wykorzystania Internetu jako narzędzia „kaznodziejskiego" oraz bliskiego jako narzędzia dla organizacji islamistycznych do walki, werbunku, logistyki etc. Co ciekawe, o ile ruch sallafiji to powrót do tradycji, to nie widzi nic złego w sięgnięciu po nowoczesną technologię. Sayyit Qutba, główny ideolog tego ruchu, w swoich *Kamieniach milowych* tak pisze: *Aby objąć przywództwo ludzkości, musimy mieć do zaoferowania coś więcej niż tyko rozwój materialny, a tą inną jakością może być jedynie wiara i sposób życia, które z jednej strony zachowują korzyści związane z nowoczesną nauką i techniką, a z drugiej zaspokajają podstawowe ludzkie potrzeby na tym samym poziomie, na jakim technika zaspokaja je w sferze materialnego komfortu życia* (za: Sageman 2008, s. 12).

Pierwszy etap wykorzystania Internetu można łączyć z atakiem na *World Trade Center* (11 września 2001 roku). Przykładem może być strona azzam.com, której nazwa pochodził od nazwiska Abdullaha Azzama, jednego z przywódców sallafickiej organizacji Braci Muzułmanów (Zdanowski 1986; Jamsheer 1995, s. 102-103). Strona założona została w Wielkiej Brytanii i poświęcona była głównie walkom w Czeczeni. W 1998 roku powstała strona alneda.com w języku arabskim, a jej redaktorem był członek Al-Kaidy Yusufa al-Uyairi.

Drugim etapem wykorzystania Internetu przez dżihad były zmiany wywołane wypowiedzeniem wojny terroryzmowi. Interwencja w Iraku, ale przede wszystkim w Pakistanie spowodowała duże problemy ruchów dżihadystycznych. USA walczyło z propagandą przy pomocy dronów. Zaczęto fizycznie eliminować przeciwników, w tym w Pakistanie. W efekcie propagandyści musieli opuścić tereny zagrożone, udali się między innymi do Jemenu i na Bliski Wschód. Ponieważ Internet nie ma ograniczeń terytorialnych zwolennicy radykalizmu islamskiego zaczęli działać w różnych rejonach świata. Charakterystyczne dla tego okresu jest też pojawianie się zapisów wideo oraz stron internetowych i mediów społeczenościowych, takich jak Twitter czy Facebook oraz różnego typu forów. To znacznie utrudniło kontrolę i zwalczanie terroryzmu przy pomocy tradycyjnych środków. W tym czasie powstała także organizacja Islamski Globalny Front Medialny (GIMF) (Steinberg 2012a, s. 23-31), która w sposób systematyczny pracowała nad propagandą w Internecie. Rozdzielała zadania i koordynowała formy przekazu. Warunkiem sprzyjającym był postęp technologiczny, szerokopasmowy Internet i częsty sprzeciw muzułmanów wobec interwencji w Iraku. Ta niechęć ułatwiała werbunek i przeradzała się w nienawiść wykorzystywaną przez ruchy dżihadystyczne. W 2007 r. Instytut Badania Mediów Bliskiego Wschodu (*Middle East Media Research Institute*) opublikował informację, że GIMF miał udostępnić aplikację o nazwie „Sekrety Mudżahedinów". Program miał służyć do szyfrowania danych z wykorzystaniem pięciu algorytmów szyfrowania z kluczami symetrycznymi o wielkości 256 bitów i asymetrycznymi o wielkości 2048 bitów (Bigo). Organizacja ta umiała wykorzystać potencjał dispory i zaczęła publikować w wielu językach, prowadziła fora, publikowała filmy Al-Kaidy, a nawet blokowała strony, czy też publikowała groźby kierowane przeciwko władzom państwowym (Musharbash 2016).

Ogromne znaczenie w szerzeniu ruchu muzułmańskiego spełniał portal As-Sahab, czyli „chmura". Powstał on najprawdopodobniej już w 2001 roku. Jego twórcy odpowiedzialni byli za kolportaż filmów, w tym tych z Osamą bin Ladenem. W ramach tego projektu wyprodukowano przynajmniej kilkadziesiąt filmów, aplikacje na telefony komórkowe. Dysponowali także technologią zbliżoną do tzw. „greenscrean", dającą możliwość dowolnej zmiany tła (Kraewetz 2007, s. 29-31). W 2008 roku doszło do wydarzenia bez precedensu, Ayman al-Zawahiri faktyczny przywódca Al-Kaidy, którego głowa warta była 25 milionów dolarów, wziął udział w czacie, który śledziło prawie 1900 osób z całego świata (Whitlock 2016). Taka sytuacja musiała spotkać się oporem ze strony internautów. W 2007 roku zablokowali oni szereg stron WWW mudżahedinów. 10 września 2007 r. udało się odciąć od sieci malezyjskie serwery, które miały posłużyć Al-Kaidzie do ataków cybernetycznych w rocznicę zamachów w USA. Wreszcie służby wywiadowcze zaczęły doceniać potęgę tego medium. Jedną z taktyk było wystawianie tzw. „honey pots", specjalnie preparowanych stron, czy postów dzięki którym udawało

się zwabić radykałów (Steinberg 2012b, s. 13). Stracili oni też dostęp do mediów tradycyjnych, a od 2005 roku zaprzestała z nimi współpracy telewizja Al Jazeera. Coraz trudniejsze okazało się przekazywanie materiałów przez fizyczną eliminację kurierów itd.

Trzecim etapem e-dżihadu jest obecna sytuacja, która zmieniła się w wyniku powstania Państwa Islamskiego. Postawiono nowe cele (powstanie kalifatu), doszło do dalszej radykalizacji postaw, ale przede wszystkim siły ISIS w dużej mierze oparto na zwolennikach z diaspory muzułmańskiej. Doszło zatem do połączenia kilku czynników, które dotychczas nie zawsze miały okazję współistnieć. Mamy zatem wsparcie finansowe, ISIS jest wspierana zarówno przez bogatych sponsorów (ważnym zapleczem finansowym Al-Kaidy były majątki rodziny bin Ladena i sponsorzy, głównie z Arabii Saudyjskiej) między innymi z Półwyspu Arabskiego (Katar, Arabia Saudyjska) oraz dochody własne (handel ropą naftową, dziełami sztuki, ludźmi, narkotykami czy podatki). Sama lokalizacja zapewnia bezpieczeństwo podejmowanych przez e-dżihad działań. Są też wykorzystywane umiejętności pozyskane z drugiego etapu rozwoju e-dżihadu, czyli rozproszenie, sieciowość organizacyjna, wykorzystanie diaspory z jej znajomością języków, kultury i zdobyczy technologicznych. Połączenie tych czynników daje możliwość stworzenia potężnej maszyny propagandowej. Kolejnym czynnikiem wspierającym jest postęp technologiczny, powszechność bezprzewodowego Internetu, miniaturyzacja i mobilność urządzeń, relatywne niskie koszty zakupu profesjonalnego sprzętu i co ważniejsze, coraz większe „uzależnienie" się ludzkości od informacji i wirtualnego świata.

Wirtualna *umma*

Państwo Islamskie postanowiło wykorzystać zdobycze Zachodu do walki z nim, wychodząc z jednego z założeń, że rozproszeni w zachodnim świecie muzułmanie nie odnajdują się w nim, a jednocześnie są wychowani w jego kulturze. Postanowiło zatem, aby ich potrzeby zaspokoić w taki sposób, do jakiego są przyzwyczajeni. Zdecydowano się na zachowanie formy przekazu charakterystycznego dla świata popkultury. Wykorzystywano zatem media społecznościowe, kanały streamingowe, a nawet zaczęto tworzyć gry komputerowe. Jednocześnie dbano o jakość przekazu, czyli jego profesjonalizm. Podświadomie też przekazywane przez media obrazy miały być spójne z realiami świata zachodniego. Dlatego też na zdjęciach widzimy ludzi ubranych często w markowe produkty, jeżdżących dobrymi samochodami, używających najnowsze modele smartfonów itd. Obraz ten jest dla odbiorcy atrakcyjny i dostosowany do jego konsumpcjonistycznych przyzwyczajeń. Przekaz treści jednak jest już zupełnie inny, ma on na celu wywołanie potrzeby poczucia się częścią większej wspólnoty, czyli *ummy*. Interpretacja islamu zostaje bardzo spłycona, ogranicza się tak

naprawdę tylko do pewnych ogólników, mających niewiele wspólnego z rzeczywistością i tradycją tej wiary.

Podsumowując, Internet może być wykorzystywany przez trzy kategorie podmiotów. Pierwszy to organizacje terrorystyczne. Wykorzystują go jako narzędzie do komunikacji wewnętrznej i zewnętrznej. Pierwsza obejmuje takie narzędzia jak telefony, tyle że tańsze, co jest szczególnie ważne dla organizacji o charakterze ponadlokalnym. Wykorzystywanie Internetu do komunikacji zewnętrznej pełni rolę tzw. „zamrażarki postaw", czyli propagandy wewnętrznej i utrzymywania morale. Drugą grupą podmiotów wykorzystujących Internet są tzw. „wirtualni mudżahedini", czyli osoby wspierające dżihad poprzez pracę z wykorzystaniem Internetu. Osoby takie odpowiedzialne są za werbunek, prowadzenie polityki medialnej, popularyzowanie ruchu, aktywną działalność na forach w celu eliminowania wrogich komentarzy i zbierania informacji. Ta ostatnia rola jest bardzo ważna, gdyż obejmuje „biały wywiad". Dzięki nim przywódcy ruchu wiedzą jak są postrzegani na Zachodzie, jaki skutek odnoszą ich działania, jakie działania planują rządy poszczególnych państw, a nawet jakie są słabe strony ich przecinków? Natomiast trzecią grupę podmiotów stanowią sympatycy, zwani też *followersami*, którzy podzielają ideologię, albo nią przynajmniej się interesują, czasami są wykorzystywani przez e-dżihad w sposób dla nich nieświadomy, choćby przez powielanie postów, czy ich akceptowanie w mediach społecznościowych.

„Fabryka snów" kontra „fabryka śmierci"

Propagandyści radykalnego islamu sięgnęli do przekazów wideo bardzo wcześnie, a od czasów popularyzacji takich kanałów jak YouTube, narzędzie to stało się jeszcze łatwiej dostępne. Medium to okazało się najlepsze, bo oddziałuje na wiele zmysłów, a jednocześnie poprzez media społecznościowe łatwo można je rozpowszechniać. Jednym z głównych inicjatorów wykorzystania tego medium był Amerykanin (co ciekawe pochodzenia żydowskiego) Adam Gadahn, *vel* Azzam al-Amriki. Pracując w Hollywood, podczas kręcenia jednego z filmów wyśmiewających Al-Kaidę zainteresował się islamem i ostatecznie został jego wyznawcą. Początkowo działał sam, potem został zwerbowany, szybko stał się swego rodzaju rzecznikiem prasowym bin Ladena, a następnie wstąpił w szeregi ISIS, gdzie kierował specjalną komórką propagandową. Al-Amriki wniósł swoiste „know-how". Chociaż pierwsze jego filmy były raczej proste, to on wprowadził do filmu *greescrean*, zadbał także o takie detale, jak logo, scenografia etc. Propaganda przez niego uprawiana była oparta na swoistym odwróceniu ról, przykładowo w filmie *Legitimate Demands*, cechy przypisywane Al-Kaidzie przypisuje on Zachodowi, a konkretnie prezydentowi Bushowi (*Legitimate Demands* 2016), nazywa go „ekstremistą", „rządnym krwi" przywódcą „imperium zła" na „globalnej krucjacie" zła etc. Jego filmy mają bardzo duży wpływ na młodych ekstremistów, brytyjska policja przyznaje, że często znajduje je

w komputerach osób aresztowanych pod zarzutem udziału w organizacjach terrorystycznych (Whitlock 2016). Jego slogany trafiają zwłaszcza do młodych ludzi, a jego bezczelne grożenie prezydentowi tego czy innego państwa, czyni z niego bohatera w ich oczach.

Z czasem filmy ISIS zaczęły nabierać nową formę, nagrywane były profesjonalnym sprzętem, według scenariusza, stosowano montaż, a nawet efekty specjalne. Swoistym szokiem był film wyreżyserowany przez am-Amriki wyemitowany 13 lutego 2015 roku. *Healing the believers chest* (*Healing the believers chest* 2016)*,* który przedstawia egzekucję przez spalenie jordańskiego pilota zestrzelonego nad Raqqą Muath al-Kasaesbeh'a. W filmie wykorzystano grafikę komputerową 3D, sceny z gier wideo, liczne fragmenty programów informacyjnych, głównie dla zobrazowania dlaczego Jordańczycy są postrzegani za zdrajców islamu. Jeniec opowiada o swoim szkoleniu, misjach w jakich brał udział, samolocie (F-16) i rodzajach przenoszonej broni, a także o islamskich państwach biorących udział w walkach z ISIS. Ciekawym zabiegiem było ubranie go w pomarańczowy strój więzienny, w takich strojach filmowanych było też wielu innych jeńców, na których dokonywano mordu. Ten strój nawiązuje do amerykańskich ubrań stosowanych w Guantanamo, jest to zatem swoiste odwrócenie ról. Ten sam zabieg jest stosowany także podczas egzekucji. Jeniec prowadzony jest przez zgliszcza, by zobaczył do czego doprowadził, dość nienaturalnie rozgląda się, co świadczy, że został do tego przymuszony. Następnie wmontowany jest fragment pokazujący spalonych, zabitych cywili w wyniku nalotów. Jest to zatem zabieg mający zapobiec współczuciu ofierze, która zostanie zgładzona w taki sam sposób. Jeniec idąc w stronę klatki mija oddział dżihadystów. To co rzuca się w oczy jest kolejną manipulacją na poziomie wizualnym. Film przedstawia doborową jednostkę, rosłych bojowników (wyższych od jeńca, lub stojących wyżej niż on), ubranych w nowe mundury z wypolerowaną bronią. Zamknięty w klatce pilot zostaje oblany benzyną i podpalony przez przywódcę społeczności lokalnej, która została przez niego pokrzywdzona. Był to Abu Muhammad al-Adnani (wł. Taha Subhi Falahi) „rzecznik prasowy" ISIS w Syrii. Na koniec zwłoki zostają zasypane gruzem, wystaje tylko zwęglona ręka, co nawiązuje do wcześniejszych zdjęć ofiar bombardowań zasypanych gruzem. W filmie zastosowano wiele efektów komputerowych (np. „podkręcony" kolor płomieni). Momentami wygląda to jak gra komputerowa lub film z Hollywood. W filmie wziął udział król Jordanii, emerytowany pilot wojskowy.

Filmy z egzekucji stały się niemal codziennością, dlatego coraz trudniej ich autorom było utrzymać uwagę widza (np. film z masowej egzekucji Koptów na plaży, zatapianie w basenie klatki z pojmanymi, brutalność tzw. Jihadi John'a – Mohammed Emwazi), obywatela Wielkiej Brytanii odpowiedzialnego za liczne egzekucje pojmanych obcokrajowców).

Od drugiej połowy 2015 roku wprowadzono zmiany w przesłaniu kierowanym przez ISIS. Coraz częściej w ich „produkcjach" pojawiają się dzieci. Zabieg ten ma z jednej strony ukazać stabilność kalifatu, z drugiej świadczy o uwzględnieniu „planu B" (w razie porażki obecnego kalifatu, pozostawi on po sobie następców, będących dzisiaj dziećmi). Dzieci stają się ważnym ogniwem propagandy kalifatu (Winter 2016b), stają się bohaterami i celebruje się ich męczeńską śmieć (Winter 2016a).

Przykładem takiego filmu jest *To the Sons of Jews* (*To the Sons of Jews* 2016). Film przedstawia trening dzieci (wyglądają na około 10 lat). Po nauce Koranu, sześciu chłopców zostaje wytypowanych do gry. Celem jest odnalezienie w opuszczonej twierdzy ukrytego szpiega, a następnie zabicie go. Scenariusz jest oparty na kanwie programu przygodowego *Fort Boyard* (emitowanego również w Polsce przez stację TVN), sposób realizacji podobny jak w poprzednim opisywanym filmie. Kręcony jest kilkoma kamerami HD, wykorzystano grafikę komputerową, a ofiary przedstawiają się w wywiadach i przyznają do winy. Film poprzedzony jest też politycznym uzasadnieniem, tym razem skierowanym przeciwko Izraelowi. Liczne są efekty specjalne, zwolnione ujęcia, zwielokrotnione efekty dźwiękowe (np. wystrzału), dobrana muzyka do tempa i wydarzeń etc.

W kwietniu 2015 roku Azzam al-Amriki został zabity przez amerykańskiego drona (*Al-Qaeda* 2016), a w styczniu 2016 roku życie stracił Jihadi John (Ford 2016).

Soft power

Ideologia Państwa Islamskiego wydaje nam się wręcz odrzucająca, ale mimo to okazuje się dla innych interesująca. Zależy to od punktu widzenia, gdyż ruch salaficki obiecuje muzułmanom sukces w postaci nie tylko kalifatu od Maroka po Malezję, ale i kontrolę nad światem. Nic zatem dziwnego, że trafia to do muzułmanów na całym świcie. Do tego wizja ta nie wymaga wyrzeczenia się wszystkich zdobyczy nowoczesności, zwłaszcza w kontekście wygody życia współczesnego. Ideologia Qutby i jego następców daje więc alternatywę, na jaką nie jest gotowy świat Zachodu. Bo z jednej strony daje gwarancje życia wygodnego z całym zapleczem technicznym, a jednocześnie na pierwszy plan wysuwa tożsamość, społeczność, wartości etyczne, przeciwstawiane indywidualizmowi, materializmowi, konsumpcjonizmowi, powiązane z ekonomizacją życia Zachodu. Taka wizja islamskiego świata jest zatem bardzo atrakcyjna i potrafi skusić nowych adeptów e-dżihadu. Świadomi tego są zarówno przywódcy Al-Kaidy, jak i spadkobiercy spod znaku Daesz. Ten sposób oddziaływania na ludzi jest wspierany przez nowoczesne technologie, które są do tego wręcz stworzone. Forma komunikatów i ich treść są bardzo podobne do tych, którą stosują przeciwnicy. Występuje jedynie odwróceniu ról. W amerykańskich filmach to Arabowie są: zdrajcami, słabeuszami, przegranymi, dzieciobójcami,

ignorantami, terrorystami. W przekazie ISIS jest dokładnie odwrotnie, ich miejsce zajmują Amerykanie. Świat propagandy Daesz jest swoistym lustrem naszego świata, różnica jest jednak zasadnicza. Śmierć na filmach Hollywood jest udawana, zaś na filmach dżihadystów jest prawdziwa, nawet na tym poziomie udowadniają, że za nimi stoi prawda. *Soft power* zdobywa dusze, które często potem używane są do *hard power*, czyli do bezwzględnej walki na śmierć i życie.

Metody walki

Powstaje pytanie, jak przeciwdziałać takiemu wykorzystaniu Internetu? Możemy zaproponować kilka opcji. Pierwsza to fizyczna eliminacja zarówno ludzi, jak i sprzętu. W ten sposób zlikwidowano większą cześć pracowników portalu as-Sabah, ważniejszych propagandystów, jak choćby am-Amriki. Efekty są jednak niezadowalające, po pierwsze śmierć czyni z nich męczenników sprawy, co tylko mobilizuje nowych terrorystów. Po drugie, prowadzi to do przystosowania się struktur, poprzez rozproszenie, kodowanie przekazów itd. Również niszczenie infrastruktury nie jest szczególnie skuteczne, ze względu na korzystanie z serwerów komercyjnych, systemu tzw. „chmur", które zapewniają bezpieczeństwo informacjom. Również prewencyjne blokowanie czy usuwanie okazuje się niewystarczające. Tak należy ocenić akcję przeprowadzoną przez właścicieli portalu Skype, który w 2014 roku zablokował blisko 1000 kont zwolenników radykalnych ruchów islamskich. W efekcie okazało się, że konta zostały odbudowane w ciągu zaledwie miesiąca, a ocenia się, że do odtworzenia treści zaangażowano zaledwie ok. 13% aktywnych zwolenników (Berger, Morgan 2016, s. 55). Jednocześnie doświadczenie to nauczyło lepszego stosowania kamuflażu przez e-dżihad, lepszej selekcji uczestników grup dyskusyjnych, wreszcie doprowadziło do radykalizacji postaw.

Kolejną próbą siły jest walka w sieci, to forma nowej wojny toczonej pomiędzy terrorystami a informatykami służb państw Zachodu. Choć o wiele ciekawsze są przypadki akcji prowadzonych przez zachodnich hakerów w sposób niezależny od rządów, takim przykładem był opisany wyżej *blackout* z 2007 roku, ale również wypowiedzona e-dżihadowi wojna przez tzw. grupę Anonymous z grudnia 2015 roku (Gilbert 2016) i po atakach w Brukseli (Millis 2016).

Jeszcze inną metodą jest monitoring i precyzyjna cenzura, połączone ze współpracą z organami ściągania. Takim projektem był „Clean IT Project" (http://www.cleanitproject.eu/) wspierany przez Komisję Europejską, którego zadaniem było połączenie potencjału władz, środowisk akademickich i biznesu w celu walki z propagowaniem terroryzmu w sieci. Jak jednak przyznaje jeden z członków tego projektu Asiem El Difraoui, natrafiono na bardzo duże problemy natury prawnej, założenie filtrów prewencyjnych godzi w wolność słowa, a jednocześnie przyczynia się do zwiększania poczucia ekskluzywności tych, którzy

mają dostęp do treści po ich usunięciu z ogólnodostępnych portali internetowych (*Wir solten…* 2016).

W maju 2016 Twitter, Facebook, Google, YouTube i Microsoft podpisały z Komisją Europejską kodeks postępowania, w którym zobowiązali się do usuwania wiadomości, zawierającychh tzw. „mowę nienawiści" (Guillén 2016). Akcja ma być podjęta do 24 godzin od wykrycia publikacji. Zobowiązano się również do szkolenia swoich pracowników w „szybkim i skutecznym" rozpoznawaniu treści uznawanych za niebezpieczne.

Taka współpraca korporacji z branży IT nie zawsze jest oczywista. Przykładem może być spór pomiędzy FBI i firmą Apple, która odmówiła odblokowania telefonu terrorysty. W grudniu 2015 roku Syed Rizwan Farook wraz z żoną dokonali masakry w San Bernardino, gdzie znaleziono jego telefon. Firma odmówiła dostępu do zapisanych w nim informacji, uważając, że będzie to złamaniem praw ich klienta (Szewczyk 2016). To też stało się przyczynkiem do rozmów pomiędzy władzami USA i przedstawicielami tzw. Doliny Krzemowej (*Carter Heads…* 2016), w celu uzyskania pomocy w walce z terrorystami.

Pewnym paradoksem jest to, że im bardziej opresyjna polityka wobec e-dżihadu, tym ten staje się silniejszy. Okazało się, że prewencyjne zamknięcie kont przez Twittera, spowodowało większe straty dla zachodnich służb specjalnych. Utracono kontrolę nad wieloma śledzonymi osobami, jednocześnie sami dżihadyści stali się bardziej ostrożni. Wprowadzenie agentów w to środowisko jest bardzo trudne, za to śledzenie ich online, pomijając skalę, jest dość proste. Pozostaje poza tym zasadnicze pytanie, czy walkę z przeciwnikami wolności słowa, można toczyć przez ograniczenie wolności słowa?

Bibliografia

Wir sollten den Zugang erschweren (2016) Dostęp: 15.12.2016. Tryb dostępu: http://www.golem.de/news/extremismus-im-netz-wir-sollten-den-zugang-erschweren-1210-95438.html.

Al-Qaeda spokesman with Jewish roots killed in US drone strike (2016) Dostęp: 15.12.2016. Tryb dostępu: http://www.timesofisrael.com/al-qaeda-leader-with-jewish-roots-killed-in-us-drone-strike/.

Berger J. M., Morgan J. (2015) *The ISIS Twitter Census. Defining and describing the population of ISIS supporters on Twitter*. "The Brookings Project on U.S. Relations with the Islamic World Analysis Paper", No. 20, March 2015, Dostęp: 15.12.2016. Tryb dostępu: http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

Bigo, Ł. (2016) *Al-Kaida i mudżahedini będą szyfrować dane*. Dostęp: 15.12.2016. Tryb dostępu: http://www.pcworld.pl/news/Al.Kaida.i.mudzahedini.beda.szyfrowac.dane,105270.html.

Carter Heads to Silicon Valley as ISIS Cyberwar Expands (2016). Dostęp: 15.12.2016. Tryb dostępu: http://newsmilitary.com/pages/70392237-carter-heads-to-silicon-valley-as-isis-cyberwar-expands.

Danecki, J. (1997) *Podstawowe wiadomości o islamie*. T. 1., T. 2. Warszawa: Dialog.

Ford, D., Almasy, S. (2016) *ISIS confirms death of 'Jihadi John'*. Dostęp: 15.12.2016. Tryb dostępu: http://edition.cnn.com/2016/01/19/middleeast/jihadi-john-dead/.

Gilbert, D. (2016) *Anonymous Is Hacking ISIS, But Warns Collaborating With US Government Is 'Deeply Stupid'*. Dostęp: 15.12.2016. Tryb dostępu: http://www.ibtimes.com/anonymous-hacking-isis-warns-collaborating-us-government-deeply-stupid-2226066.

Guillén, B. (2016) *Twitter y Facebook vetarán los mensajes que inciten al odio un día después de detectarlos.* Dostęp: 15.12.2016. Tryb dostępu: http://tecnologia.elpais.com/tecnologia/2016/05/31/actualidad/1464711881_734190.html.

Healing the believers chest (2016). Dostęp: 15.12.2016. Tryb dostępu: https://charlescarrollsociety.com/2015/02/03/healing-the-believers-heart-full-video-of-jordan-pilot-muath-al-kasaesbeh-being-burnt-alive-isis-jordanianpilot/.

Huntington, S. P. (2003) *Zderzenie cywilizacji i nowy kształt ładu światowego.* Warszawa: Wydawnictwo Literackie Muza.

Jamsheer, H. A. (1995) *Jedność arabska. Geneza idei tradycji wczesnego islamu*. Warszawa: Wydawnictwo Naukowe Semper.

Kraewetz, N. (2007) *A Picture's Worth..., Digital Image Analysys and Forensicis*. USA. Dostęp: 15.12.2016. Tryb dostępu: http://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf.

Legitimate Demands (2016). Dostęp: 15.12.2016. Tryb dostępu: https://www.youtube.com/watch?v=_A4ah-OI5pI.

Mills, K. A. (2016) *Brussels attacks: Anonymous declares war on ISIS in chilling video vowing 'we will find you'.* Dostęp: 15.12.2016. Tryb dostępu: http://www.mirror.co.uk/news/world-news/brussels-attacks-anonymous-declares-isis--7615029.

Musharbash, Y. (2016) *Neues Drohvideo gegen Deutschland und Österreich,* Dostęp: 15.12.2016. Tryb dostępu: http://www.spiegel.de/politik/deutschland/globale-islamische-medienfront-neues-drohvideo-gegen-deutschland-und-oesterreich-a-517533.html.

Nye, J. S. (2007) *Soft Power. Jak osiągnąć sukces w polityce światowej*. Warszawa: Wydawnictwo Akademickie i Profesjonalne.

Sageman, M. (2008) *Sieci terror*u. Kraków: Wydawnictwo UJ.

Sciolino, E., Schmitta, E. (2016) *Not Very Private Feud Over Terrorism*. Dostęp: 15.12.2016. Tryb dostępu: http://www.nytimes.com/2008/06/08/weekinreview/08sciolino.html.

Steinberg, G. (2012a) *Die Globale Islamische Medienfront (GIMF) und ihre Nachfolger*. W: Steinberg, G. (red.), *Jihadismus und Internet: Eine deutsche Perspektive*. Berlin: SWP.

Steinberg, G. (2012b) *Jihadismus und Internet. Eine Einführung*. W: Steinberg, G. (red.), *Jihadismus und Internet: Eine deutsche Perspektive*. Berlin: SWP.

Szewczyk, O. (2016) *FBI żąda odblokowania iPhone'a islamisty, Apple odmawia. Kto ma rację?* Dostęp: 15.12.2016. Tryb dostępu: http://www.polityka.pl/tygodnikpolityka/swiat/1651420,1,fbi-zada-odblokowania-iphonea-islamisty-apple-odmawia-kto-ma-racje.read.

To the Sons of Jews (2016). Dostęp: 15.12.2016. Tryb dostępu: http://heavy.com/news/2015/12/new-isis-islamic-state-news-videos-pictures-to-sons-of-jews-wilayat-al-khayr-child-boy-soldiers-executing-shooting-spies-jewish-ancient-ruins-obstacle-course-full-uncensored-youtube/.

Vidino, L., Hughes, S. (2016) *ISIS in America: From Retweets to Raqqa*. Dostęp: 15.12.2016. Tryb dostępu: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/ISIS%20in%20America%20-%20Full%20Report_0.pdf.

Whitlock, C. (2016) *Al-Qaeda's Growing Online Offensive*. Dostęp: 15.12.2016. Tryb dostępu: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/23/AR2008062302135.html.

Winter, Ch. (2016a) #*Syria: #IS celebrates death of another teen suicider, Abu Dujana al-Ansari, who died in #Raqqa Province (21-10-15)*. Dostęp: 15.12.2016. Tryb dostępu: https://twitter.com/charliewinter/status/681529758065229825.

Winter, Ch. (2016b) *Shocked by the 'cubs of the caliphate'? Of course you are – that's Isis's plan*. Dostęp: 15.12.2016. Tryb dostępu:

https://www.theguardian.com/commentisfree/2016/jan/05/cubs-of-caliphate-isis-children-videos-propaganda.

Zdanowski, J. (1986) *Bracia Muzułmanie i inni*. Szczecin: Wydawnictwo „Glob".

Streszczenie

Zgodnie z teorią J. S. Nye, *soft power* to forma kontrolowania ludzkich poczynań, postaw, opinii, czy nawet rządzenia nimi poprzez atrakcyjność przekazu. Radykalne ruchy islamskie, w tym organizacje terrorystyczne, skutecznie używają Internetu, jako narzędzia do propagowania swojej ideologii wśród muzułmanów. Okazuje się on być świetnym narzędziem propagandowym, ale i służacym do radykalizacji postaw. W artykule ukazano sposoby wykorzystania Internetu przez takie organizacje jak Al-Kaida czy ISIS oraz skalę problemu.

Słowa kluczowe: Dżihad, Internet, Muzułmanie, ISIS

E-jihad, *soft power* of Islamic radicalism

Abstract

"Soft power" due to J.S. Nye theory is a kind of souls rule by controlling *via* attracting messages. Radical Islamic movements, including terrorist organizations, are using internet to raise support among Muslims worldwide. It turns out that this is an excellent tool for conducting propaganda and radicalization. The article shows, what are the propaganda techniques using by organizations such as Al-Qaeda or ISIS, and how serious the problem is.

Key words: Jihad, Internet, Muslims, ISIS

Paulina Polko
Wyższa Szkoła Biznesu w Dąbrowie Górniczej

Media społecznościowe w służbie armii – analiza wybranych przypadków

Wprowadzenie

Służby mundurowe z zasady niechętnie dzielą się informacjami o swoich działaniach uznając tajność i skrytość za klucz do sukcesu prowadzonych operacji i gwarancję bezpieczeństwa ich realizatorów. Niemniej jednak wypracowane przez lata zasady polityki medialnej i kodeksy dobrych praktyk dotyczące relacji z dziennikarzami, pozwalają formacjom mundurowym korzystać z pośrednictwa mediów w kontaktach ze społeczeństwem, objaśniać swoją rolę w zapewnianiu bezpieczeństwa państwa, tłumaczyć swoje racje, czy nawet rozwiązywać sytuacje kryzysowe, przy jednoczesnym zachowaniu wspomnianej tajności i skrytości tam, gdzie to jest niezbędne.

Sytuacja ta była w miarę przejrzysta do momentu pojawienia się i umasowienia mediów społecznościowych (*Social Media*, Web 2.0), które diametralnie zmieniły komunikację w Internecie. Jak zauważa rzecznik prasowy *Israel Defence Forces*: *natura Social Media stoi w całkowitej sprzeczności z istotą armii, która jest organizacją zamkniętą, skłonną do ukrywania swoich sekretów i technik działania.* […] *Kluczowa jest zwłaszcza różnica w używanym języku – wojskowy jest bardzo precyzyjny, chłodny, pełen specjalistycznego słownictwa. Język mediów społecznościowych pełen jest natomiast emocji, pytań, skrótów myślowych. Ma wybitnie „nieformalny" charakter* (Stein 2012).

Media społecznościowe, często utożsamiane – nie do końca poprawnie – z Web 2.0, to działania członków różnych grup pozostających ze sobą w kontakcie za pośrednictwem Internetu, pozwalającym im na wymianę informacji, wiedzy i opinii dzięki popularnym mediom, umożliwiającym tworzenie oraz łatwy przekaz treści w formie tekstów, obrazów, nagrań wideo i audio (Safko, Brake 2009, s. 6-7). Ich cechą charakterystyczną jest szybki i łatwy dostęp do dużych i zróżnicowanych grup odbiorców, ale również wymóg, aby prowadzona za ich pośrednictwem działalność była nie jednokierunkowym pasem transmisyjnym, a komunikacją z informacją zwrotną, reaktywną, dającą w tym masowym wymiarze indywidualną odpowiedź (reakcję) na komentarze, pytania, działania odbiorców komunikatów. Na potrzeby niniejszego artykułu przyjęta zostanie typologia dokonana przez Arthura Weissa (Weiss 2010). Zawiera ją tabela nr 1.

Tab. 1. Typologia mediów społecznościowych

strony udostępniające treści – YouTube (nagrania wideo), Flickr, Instagram (zdjęcia), Slideshare.com (serwis do zamieszczania i przeglądania prezentacji multimedialnych)
serwisy społecznościowe – ich użytkownicy mają możliwość wymiany informacji z innymi użytkownikami, zaakceptowanymi jako ich znajomi (np. Facebook, My Space, LinkedIn, Xing czy Google+)
blogi i mikroblogi (np. Twitter lub Blip)
strony poświęcone współpracy użytkowników przy gromadzeniu informacji (Zoho, Google Docs)
fora internetowe i strony do umieszczania recenzji
strony umożliwiające interakcję i współpracę użytkowników (Wikipedia), strony umożliwiające zamieszczanie opinii (Yahoo Answers), serwisy internetowe służące gromadzeniu i ocenianiu linków do potencjalnie interesujących treści (SecondLife, Digg lub Delicious)

Źródło: Weiss, A. (2010) *Using social media to support marketing and computer research.* London, s. 101; Farin, K. (2011) *Media społecznościowe i ich wpływ na komunikację w obszarze bhp.* „Bezpieczeństwo Pracy", nr 9, s. 22.

Social media jako nowe narzędzie w zarządzaniu kryzysowym i komunikacji kryzysowej

Media społecznościowe otworzyły nowy rozdział w tej komunikacji, dając służbom narzędzie, które pozwala na kontakt z szerokimi grupami społecznymi bez konieczności korzystania z pośrednictwa tradycyjnych mediów i dziennikarzy. Wojsko – jako dysponent informacji – może ją przekazać w formie i zakresie przez siebie wybranym bez narażania się na zakłócenia wynikające z użycia pośredników (Goban-Klas 2009; Mrozowski 2001). Mimo tych ewidentnych zalet, media społecznościowe wzbudzają w armii obawy, ale jak zauważa Chondra Perry: *liderzy wojskowi widzą, jakie znaczenie zyskuje ten sposób komunikacji i starają się go adaptować do swoich instytucji. Nie mogą lekceważyć liczby ludzi, do których może ona dotrzeć i pomóc armii „opowiedzieć jej historię (wersję wydarzeń)* (Perry 2010, s. 63).

Analiza przypadków kryzysów, w których skorzystano z pomocy mediów społecznościowych, potwierdza słuszność takiej strategii. Podczas ataku terrorystycznego na mecie maratonu w Bostonie w 2012 roku jedna czwarta Amerykanów szukających informacji na temat tego zdarzenia używała mediów społecznościowych (Twittera i Facebooka), używając hashtagów i specjalnie dla tego wydarzenia tworzonych stron. Gdy bostońska policja na swoim profilu zamieściła informację: „złapany" (o zamachowcu, który przeżył atak), to w ciągu kilku minut podało tę informacje dalej 140 tys. osób. Mieszkańcy Bostonu zaś,

poprzez społecznościowe narzędzia Google oferowali maratończykom uwięzionym na trasie biegu schronienie, miejsce do wykąpania i gorące napoje (Maron 2013). Podczas huraganu Sandy w USA zanotowano 20 mln tweedów osób, będących w sferze działania zjawiska, pomimo, że wiele ofiar straciło swoje telefony komórkowe. W pewnym momencie używali oni mediów społecznościowych tak intensywnie, że zarząd spółki będącej właścicielem Twittera musiał ograniczyć ilość twittów na dzień (Palen 2013). Natomiast podczas ataku terrorystycznego na metro i lotnisko w Brukseli aplikacja *safety check* uruchomiona przez Facebooka pozwalała jego użytkownikom będącym w okolicy zdarzeń, na oznaczanie się jako osoby bezpiecznej.

Mając na uwadze powyższe, można stwierdzić, że media społecznościowe mogą być w różny sposób wykorzystane do zarządzania kryzysowego. Prezentuje je tabela nr 2.

Tab. 2. Wykorzystanie mediów społecznościowych do zarządzania kryzysowego

Typ social media:	**Przykład;**	**Zastosowanie:**
społeczność sieciowa	Facebook Myspace Friendster	○ koordynacja poszukiwań i działań potencjalnych wolontariuszy, ○ informowanie o tym, co się dzieje i odsyłanie do specjalistycznych serwisów,
dzielenie, udostępnianie, upowszechnianie treści	YouTube Flickr Vimeo	○ zamieszczanie lokalnych ostrzeżeń w czasie rzeczywistym, ○ wymiana zdjeć, filmów z miejsca zdarzenia, będących również informacją dla służb, ○ identyfikacja zagubionych i ofiar,
współpraca, wymiana wiedzy	Wikis Forums Message boards Podcasts	○ prowadzenie dialogu (czatów) pomiędzy ofiarami i służbami,
blogi i mikroblogi	Blogger Worldpress Tumblr Twitter	○ publikowanie ostrzeżeń, ○ dzielenie się ważnymi informacjami,
specjalistyczne	OpenStreetMap	○ mapowanie zagrożeń,

platformy	Crisis mappers Google map maker Ushahidi Crisis commons	○ platforma do komunikacji służb ratunkowych.

Źródło: Wendling, C., Radisch, J., Jacobzone, S. (2013) *The Use of Social Media in Risk and Crisis Communication.* „OECD Working Papers on Public Governance", nr 24, s. 12.

Dobrą ilustracją wykorzystania mediów społecznościowych do komunikacji w sytuacji kryzysowej jest przykład działań policji na przełomie 20015 i 2016 roku, w czasie zamieszek w Monachium, wywołanych molestowaniem kobiet świętujących Sylwestra przez imigrantów. Kierownictwo lokalnej policji użyło Twittera do komunikacji z mieszkańcami i turystami, ostrzegając ich o rejonach niebezpiecznych i informując o funkcjonowaniu komunikacji publicznej oraz zamknięciu (a następnie otwarciu) niektórych obiektów w mieście. Komunikacja odbywała się w kilku językach, a twitterowy profil monachijskiej policji był źródłem informacji nie tylko dla mieszkańców, ale również dla tradycyjnych mediów, które nie były w stanie tak szybko i z taką częstotliwością zdobywać wiedzy o wydarzeniach w mieście. Prowadzący profil byli w stanie nie tylko informować odbiorców, ale również odpowiadać na ich pytania. Spełniali zatem wszystkie kryteria kampanii w mediach społecznościowych określone przez K. Foot i S. Schneider w książce *Web Campaigning* (Foot, Schneider 2006, s. 56-67) jako: informowanie, łączenie, angażowanie i mobilizowanie.

Współcześnie nie można być nieobecnym w mediach społecznościowych. Lukę wypełniają źródła nieoficjalne, które używając nazw instytucji oficjalnych pretendują do wyrażania opinii w ich mieniu. Wpisanie w wyszukiwarkę Google słowa *army* powoduje uzyskanie ponad 230 milionów rekordów (stron). Większość z nich jest nieoficjalna, podobnie jak konta na Twitterze czy strony na Facebooku. Gdy kierownictwo US Army postanowiło ujednolicić politykę komunikacyjną i założyć oficjalne profile jednostek i instytucji wojskowych odkryło, że wiele nazw jest już używanych przez osoby do tego nieuprawnione.

To między innymi było powodem stworzenia w US Army w 2009 roku *Online and Social Media Division at the Office of the Chief of Public Affairs*. Komórka ta została odpowiedzialna za całą politykę komunikacyjną amerykańskich sił zbrojnych w mediach społecznościowych. Amerykanie byli jednymi z pierwszych, którzy zauważyli nie tylko rolę tychże w kreowaniu wizerunku wojska, ale również docenili je jako narzędzie własnej bezpośredniej komunikacji ze społeczeństwem. Ich śladem poszli inni, tworząc jeśli nie osobne piony, to przynajmniej zatrudniając osoby odpowiedzialne za prowadzenie stron i profili swoich instytucji i ich jednostek organizacyjnych w *social media*. US Army komunikując się z odbiorcami, w tym ze swoimi żołnierzami, poprzez różne media, zawsze za ich pośrednictwem odsyła użytkowników do swojego portalu, na którym znajduje się właściwa,

poszerzona informacja na dany temat. Ostateczny przekaz jest więc jednolity, choć oczywiście poprzez komentarze, formy udostępniania, aktywność odbiorców, będzie mógł być różnie odbierany w zależności od medium pośredniczącego.

Polityka armii wobec mediów społecznościowych i wybrane dobre praktyki z tego zakresu

W budowaniu polityki formacji mundurowej wobec mediów społecznościowych kluczowe jest zrozumienie trzech podstawowych elementów, które są istotne dla stworzenia strategii medialnej organizacji. Prezentuje je tabela nr 3. US Army swoje cele definiuje jako: komunikowanie i edukowanie. Cel pierwszy można nazwać celem bieżącym, cel drugi – długofalowym. Oba są istotne i wzajemnie się uzupełniające *(*Brown 2012, s. 4).

Tab. 3. Budowanie strategii używania mediów społecznościowych

Obecność (presence)	Nieobecni pozwalają, by w ich imieniu komunikację dotycząca organizacji prowadziły osoby nieuprawnione.
Jakość obecności (relevance)	Obecność w mediach społecznościowych i podejmowane działania muszą być spójne ze strategią całej organizacji i realizować jej cele. Aby zachęcić użytkowników do komunikacji z organizacją, musi ona dostarczać im informację wartościową, unikalną, wysokiej jakości, aktualną, prospektywną.
Wpływowość (prominence)	Sukcesem w mediach społecznościowych jest nie tylko liczba użytkowników, którzy wchodzą w interakcje, ale ich „jakość”, tj. zgodność ich zainteresowań lub zawodu z profilem organizacji, dzięki czemu mogą wpływać na opinię innych użytkowników.

Źródło: opracowanie własne na podstawie: *Social Media Best Practices*. Dostęp: 04.12.2016. Tryb dostępu: www.carlisle.Army.mil/banner/uploads/files/U.S.%20Army%20Social%20Media%20Best%20Practices.pdf.

Pamiętać należy, iż obecność i wizerunek wojska w mediach społecznościowych związane są nie tylko z działaniami podejmowanymi instytucjonalnie. Duże znaczenie odgrywa aktywność samych żołnierzy podejmujących indywidualne decyzje o używaniu (bądź nie) *social media* oraz o zakresie dzielenia się w nich sprawami zawodowymi. Na tym polu można wskazać najwięcej zagrożeń dla bezpieczeństwa instytucji. Należą do nich:

- niedostateczne bezpieczeństwo prowadzonych operacji (opsec),
- fałszywe konta (tożsamości, profile),
- nieoficjalne konta,
- szybkość rozprzestrzeniania się informacji o organizacji.

Żołnierzom i cywilnym pracownikom wojska oraz ich rodzinom zaleca się nie oznaczanie swojej lokalizacjami zdjęciami zamieszczanymi na portalach społecznościowych, aby uniknąć możliwości zlokalizowania wojsk realizujących

operacje poza granicami kraju. Zaleca się również niepodawanie szczegółowych informacji odnośnie miejsca pełnienia służby (wystarczy samo US Army) ani zakresu zadań, jakie się realizuje. W przypadku zmiany miejsca stacjonowania, wyjazdu na misję etc. można jedynie enigmatycznie wskazać, że w życiu danej jednostki nastąpiła taka zmiana bez podania szczegółów, mogących dawać odbiorcom informację w zakresie wskazanym powyżej. US Army opracowała specjalny poradnik dla żołnierzy i ich rodzin wskazujący, w jaki sposób zachowywać się w mediach społecznościowych, aby udostępniane informacje nie były wykorzystywane w walce informacyjnej przeciwnika.

Tab. 4. Poradnik US Army na temat zachowań w mediach społecznościowych (tłumaczenie dosłowne)

Formy wpisów – niebezpieczne	Formy wpisów – bezpieczniejsze
Mój żołnierz (mąż, chłopak, brat, syn) jest w bazie XYZ w mieście ABC w Afganistanie.	Mój żołnierz służy w Afganistanie.
Mój żołnierz wyjeżdża z Kuwejtu do Iraku za trzy dni.	Mój żołnierz w tym tygodniu zmienia miejsce stacjonowania.
Mój żołnierz wraca do domu we wtorek o godz. 11.	Mój żołnierz będzie w domu na wakacje
Mieszkamy w mieście XY w stanie ZW.	Jestem ze wschodniego wybrzeża.

Źródło: *6 Social Media Considerations for Deployed Soldiers and Their Families*. Social Media Roundup. Dostęp: 04.12.2016. Tryb dostępu: https://www.army.mil/.

W ślad za poradami publikowane są tematy zatwierdzone jako bezpieczne do poruszania w mediach społecznościowych. Należą do nich:

- wyrażanie dumy z pełnionej służby i przynależności do USArmy,
- generalne uwagi dotyczące służby, obowiązku obrony ojczyzny,
- generalne informacje o realizowanych zadaniach, bez szczegółów operacyjnych i lokalizacyjnych,
- udostępnianie informacji podanych przez oficjalne wojskowe źródła (*6 Social Media…*).

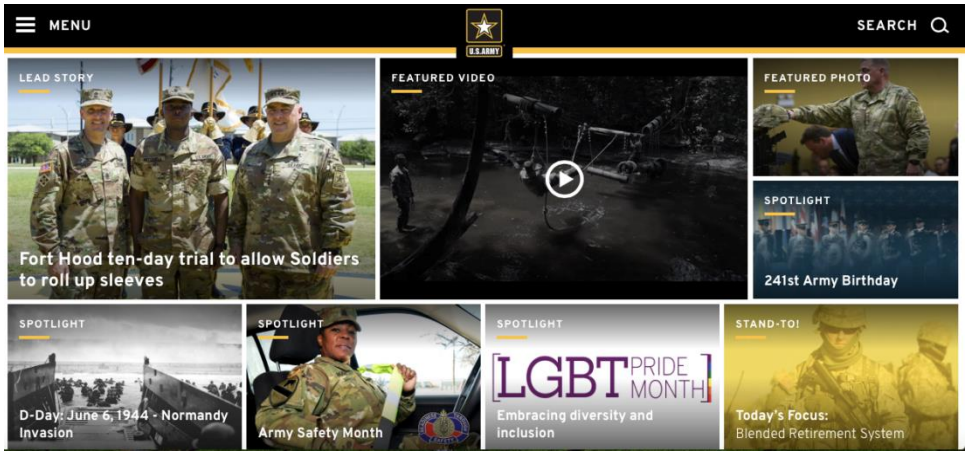
Pomimo wskazywania zagrożeń wynikających z braku świadomości konsekwencji umieszczania określonych komunikatów w mediach społecznościowych, US Army zachęca swoich żołnierzy do korzystania z nich wskazując, że autentyczne strony, profile i wpisy konkretnych osób są wiarygodniejsze dla odbiorców niż przekazy instytucjonalne.

Jedna treść, wiele form – *case study* USArmy

Zasady funkcjonowania US Army i jej członków w mediach społecznościowych opisują następujące dokumenty: *Directive Type Memorandum*

09-026 wydany przez Deputy Secretary of Defence z 25 lutego 2010 roku (nowelizowany 9 stycznia 2010 roku) i *Standard Operating Procedure* z 1 listopada 2010 roku przygotowany przez Department for the Army, Office of the Chief of Public Affairs, Online and Social Media Division. Trzecim istotnym dokumentem jest *US Army Social Media Strategy* zatwierdzona 6 października 2010 roku. Kompleksowa polityka armii Stanów Zjednoczonych wobec mediów społecznościowych powstała 6 lat temu, a więc w momencie, gdy zaczynały one zdobywać masową popularność. Były to pierwsze tego typu dokumenty w siłach zbrojnych na całym świecie. Są to dokumenty jawne, dostępne w różnych serwisach internetowych US Army.

Rys. 1. Strona internetowa US Army



Źródło: Dostęp: 08.02.2017. Tryb dostępu: https://www.army.mil.

Tylko na Facebooku znajduje się ponad 2 tysiące stron oficjalnie założonych czy to przez kierownictwo całej armii, czy poszczególne jednostki i dowództwa, setki stron Flickr, kont na Twitterze i kanałów YouTube. Standardowo temat wojskowości i obronności poruszany jest w każdym z popularnych mediów w sposób dla niego najbardziej atrakcyjny i jak już wspomniano, z odesłaniem do portalu prowadzonego przez wojsko. Działanie takie jest możliwe dzięki uruchomieniu w 2016 roku nowej wersji oficjalnej strony US Army w pełni zintegrowanej z narzędziami nawigacyjnymi mediów społecznościowych.

Rys. 2. Sposób prezentacji przyznania Medalu Honoru w różnych mediach społecznościowych

Źródło: *Army Live*, *the official blog of the US Army*. Dostęp: 04.12.2016. Tryb dostępu: http://armylive.dodlive.mil.

Oprócz przekazywania bieżących informacji na temat wydarzeń istotnych dla US Army, media społecznościowe używane są do:

- budowania szacunku wobec weteranów, zarówno wojen z XX wieku, jak i współczesnych,
- budowania pozytywnego wizerunku przełożonych,
- czczenia rocznic i świąt państwowych i wojskowych,
- akcji społecznościowych związanych z walką z nietolerancją, zachęcaniem do bezpiecznych zachowań, przypominaniem o świętach niezwiązanych z wojskiem (np. Dzień Dziecka, Dzień Pączka),
- opowiadania o armii poprzez historie zwykłych ludzi,
- edukowania w zakresie finansów, bezpieczeństwa w sieci,
- pokazywania codziennych treningów wojska,
- informowania o przełomowych wydarzeniach (wysłanie wojsk poza granice kraju, śmierć żołnierzy na misji),
- transmitowania na żywo wybranych elementów prowadzonych operacji wojskowych.

Wojna na Twitterze – case study Israel Defence Forces

14 listopada 2012 roku o godz. 6.29 na Twitterowym koncie rzecznika prasowego Israel Defence Forces (IDF) pojawił się wpis: *IDF rozpoczęły szeroko zakrojoną kampanię skierowaną na kryjówki terrorystów w #StrefaGazy, w tym na liderów #Hamas.* Był to pierwszy w historii przypadek ogłoszenia wojny poprzez medium społecznościowe. Wieczorem tego samego dnia rzecznik dopisał: *Ahmed Jabari: wyeliminowany*. Przez cały czas trwania operacji rzecznik zagrzewał

społeczeństwo do popierania prowadzonych działań wpisami: *Co byście zrobili, gdyby rakiety uderzały w wasze domy? Podaj dalej, jeśli się zgadzasz, że Izrael ma prawo do samoobrony*. Obserwatorzy profili w mediach społecznościowych IDF mogli się czuć jak na prawdziwej wojnie, szczególnie, gdy na tym samym polu ataki odpierała i swoje komentarze wyprowadzała druga strona.

Rys. 3. Twitterowa aktywność rzecznika prasowego IDF

Źródło: Dostęp: 04.12.2016. Tryb dostępu: https://twitter.com/IDFSpokesperson/status/268795866784075776.

W tym samym czasie, na kanałach YouTube należących do obu stron konfliktu, można było na żywo śledzić poszczególne ataki, które administrator co prawda usuwał, ale natychmiast pojawiały się nowe. Jak zauważa Natalie Sambhi, analityk Australian Strategic Policy Institute, *w tym przypadku mamy nie tylko do czynienia z pokazywaniem przemocy, co czynią przecież również te tradycyjne środki przekazu, ale z ich kreacją, co jest zjawiskiem nowym, trudnym do ujęcia w ramy prawne, karne, organizacyjne* (Sambhi 2012).

IDF ma długie tradycje używania mediów społecznościowych do upowszechniania własnej interpretacji sytuacji politycznej w Strefie Gazy oraz innych konfliktów, w które jest zaangażowana. Na przełomie 2008/2009 roku, dla potrzeb operacji *Cast Lead*, IDF uruchomiła własny kanał na YouTube, na którym na żywo prezentowała naloty własne i skutki działań przeciwnika. Pomimo międzynarodowego potępienia udostępniania nagrań, nie zaprzestano tej działalności. Najpopularniejsze z nich zostały wyświetlone ponad 2 miliony razy. Mimo to, decyzja o użyciu innych mediów społecznościowych nie była oczywista. Twittera, z pewnymi oporami, IDF zaczął oficjalnie używać w 2009 roku. W przypadku Facebooka obawiano się opcji komentowania prezentowanych treści (przy kanałach na YouTube opcja zamieszczania komentarza była wyłączona). Dlatego też oficjalna strona IDF na Facebooku pojawiła się dopiero w sierpniu

2011 roku z hasłem: *kliknij, jeśli popierasz sposób, w jaki IDF broni Izraela* (Stein, 2012).

W czasie pokoju IDF wykorzystuje media społecznościowe do „ocieplania" swojego wizerunku i przedstawiania swoich racji w mniej brutalny i bezpośredni sposób niż w okresie konfrontacji w realnym świecie. Zbiera zwolenników medialnych, jak też rekrutuje żołnierzy do swojej armii walczącej w realnym świecie. Pokazuje siłę i różnorodność armii poprzez konkretnych żołnierzy, opisuje specyfikę poszczególnych rodzajów sił zbrojnych, nie zapomina o złożeniu życzeń z okazji Szabasu. Historie opowiadane są przez konkretne postacie, duże znaczenie ma odwołanie się do pozytywnych skojarzeń (psy, rzucanie palenia, sport, zdrowy styl życia). W podtekście cały czas jest jednak gotowość do obrony ojczyzny, nawet gdy składane są muzułmanom życzenia dobrego Ramadanu.

Za przygotowanie i realizację strategii działań w mediach społecznościowych odpowiada *New Interactive Media Branch*, w którym całe zespoły pracują nad zbieraniem informacji, produkcją materiałów i ich dystrybucją w różnych *social media* oraz zarządzaniem tym, co się z nimi po udostępnieniu dzieje. Ludzie pracujący nad angażowaniem odbiorców w treści, które zamieszczane są pod logo IDF (w tym obecnych, byłych, przyszłych i potencjalnych żołnierzy), wykorzystują nawet grywalizację, co wywołuje oskarżenie o trywializację i popularyzację wojny wśród młodych ludzi (Ungerleider 2012).

Polityka kierownictwa IDF wobec mediów społecznościowych jest jedną z bardziej restrykcyjnych na świecie. Wprowadzone w październiku 2014 roku przepisy zakazują żołnierzom publikowania nawet na prywatnych profilach opinii sprzecznych z oficjalną linią armii. Posty są dozwolone dopiero po analizie, czy nie naruszają bezpieczeństwa jednostki i jej zespołu, nie zdradzają tajemnic obcym wywiadom oraz czy promują wartości IDF. Każdy żołnierz ma obowiązek informowania przełożonych o niewłaściwych zachowaniach kolegów w sieci. Do takich zaliczyć można nawet polubienie opinii sprzecznej z oficjalną linią armii. Mają zakaz oznaczania lokalizacji, w których się znajdują podczas służby, zamieszczania zdjęć, baz, sprzętu, realizowanych operacji i bezwzględnie muszą przestrzegać zasad w zakresie seksualności i pornografii (zakaz publikowania zdjęć nagich osób czy treści o charakterze seksualnym). Poszanowanie ludzkiej godności obejmuje również pokazywanie wziętych do niewoli jeńców czy więźniów oraz sposób pokazywania zwłok przeciwników (Zitun 2014; Yeoshua 2015).

Mimo tych restrykcji, kierownictwo IDF ma duży problem z ich egzekucją – żołnierze udostępniają coraz więcej wrażliwych treści, nierzadko w postaci relacji na żywo, a związane z tym skandale, takie jak nago tańczący spadochroniarze czy *selfie* żołnierza na tle związanych Palestyńczyków podejrzanych o terroryzm, są na porządku dziennym.

Konkluzje

1. Media społecznościowe są ważnym polem działania dla wojska, choć jest to teren trudny, wymagający od zespołów analityków medialnych ogromnego zaangażowania i czujności.

2. Przykład US Army i IDF wskazuje, że liczące się organizacje militarne mają świadomość, że podejmując to wezwanie coraz bardziej profesjonalnie muszą się do niego przygotowywać. Budują całe zespoły do prowadzenia komunikacji przy użyciu tego narzędzia, łączą różne strony i konta tak, by zdywersyfikowany przekaz był różnorodny w formie, ale jednolity w treści.

3. W przypadku armii – bardziej niż w przypadku cywili – istotne są zagrożenia związane z ujawnieniem niewłaściwych informacji na temat pojedynczych żołnierzy oraz armii, czy jej jednostek jako instytucji. Konsekwencje niewłaściwego korzystania z mediów społecznościowych implikują opracowywanie przez zwierzchników żołnierzy wytycznych ściśle określających zasady obecności na platformach społecznościowych zarówno dla żołnierzy, jak i ich bliskich.

4. Świadomość zagrożeń, jakie może nieść ze sobą używanie *social media* nie zniechęca jednak armii do korzystania z tego narzędzia. Wojskowi liderzy mają świadomość, że wielu żołnierzy, zwłaszcza młodych, i tak z mediów społecznościach korzysta. Kluczowe jest, by robili to w sposób bezpieczny i z korzyścią dla budowania wizerunku całych sił zbrojnych.

Bibliografia

6 Social Media Considerations for Deployed Soldiers and Their Families, Social Media Roundup. Dostęp: 04.12.2016. Tryb dostępu: www.army.mil.

Brown, B. (2012) *U.S. Army Social Media*. *U.S. Army Online and Social Media Division, HQDA, April.* Dostęp: 04.12.2016. Tryb dostępu: http://www.forthoodpresscenter.com/external/content/document/3439/1416855/1/1-Army%20Social%20Media%20Brief.pdf.

Farin, K. (2011) *Media społecznościowe i ich wpływ na komunikację w obszarze bhp*. „Bezpieczeństwo Pracy", nr 9, s. 22-24.

Fine, D. (2013) *Disaster Response*. Dostęp: 04.12.2016. Tryb dostępu: https://www.scientificamerican.com/article/how-social-media-is-changing-disaster-response/.

Foot, K., Schneider, S. (2006) *Web Campaigning*. Cambridge: MIT Press.

Goban-Klas, T. (2009) *Media i komunikowanie masowe. Teorie i analizy prasy, radia, telewizji i Internetu*. Warszawa: PWN.

Mrozowski, M. (2001) *Media masowe. Władza, rozrywka i biznes*. Warszawa: Aspra-Jr.

Palen, L. (2008) *Online Social Media in Crisis Events*. „Educause Quaterly", No 3, s. 76-78.

Perry, Ch. (2010) *Social Media and the Army*. „Military Review", No. 2, vol. 90.

Safko, L., Brake, D. K. (2009) *The Social Media Bible. Tactics, Tools and Strategies for Business Success*. Hoboken, N. J.: John Wiley & Sons.

Sambhi, N. (2012) *Social media and the military: the Israel Defense Forces and Hamas*. Dostęp: 04.12.2016. Tryb dostępu: http://www.aspistrategist.org.au/social-media-and-the-military-the-israel-defense-forces-and-hamas-2/.

Stein, R. L. (2012) *Inside Israel's Twitter War Room. History of a Social Media Arsenal*. Dostęp: 04.12.2016. Tryb dostępu: .http://www.merip.org/mero/mero112412.

Ungerleider, N. (2012) *Inside The Israeli Military's Social Media Squad*. Dostęp: 04.12.2016. Tryb dostępu: http://www.fastcompany.com/3003305/inside-israeli-militarys-social-media-squad.

Weiss, A. (2010) *Using social media to support marketing and computer research*. Dostęp: 04.12.2016. Tryb dostępu: http://www.online-information.co.uk/online2010/conference/conference-programme_live.html.

Wendling, C., Radisch, J., Jacobzone, S. (2013) *The Use of Social Media in Risk and Crisis Communication.* "OECD Working Papers on Public Governance"*, No. 24.*

Yehoshua, Y. (2015) *IDF combats social media mishaps among troops.* Dostęp: 04.12.2016. Tryb dostępu: http://www.ynetnews.com/articles/0,7340,L-4663623,00.html.

Zitun, Y. (2014) *IDF announces new restrictions on social media use.* Dostęp: 04.12.2016. Tryb dostępu: http://www.ynetnews.com/articles/0,7340,L-4528589,00.html.

Streszczenie

Media społecznościowe mają szerokie zastosowanie w działalności biznesowej czy komunikacji społecznej, ale są wciąż rzadko używane w zarządzaniu kryzysowym, w tym w komunikacji kryzysowej. Decydenci wojskowi na całym świecie odnoszą się dość sceptycznie do tego środka komunikacji,

szczególnie jeśli chodzi o tłumaczenie swoich decyzji, czy działań formacji im podległych. Przymuszeni do transparentności mimo wszystko wolą tradycyjne środki komunikacji. Jednakże, w ostatnich latach obserwujemy przypadki dobrych praktyk w zakresie wykorzystania *social media* przez wojsko, w tym w szczególności US Army i Israel Defense Forces. Niniejszy artykuł jest próbą usystematyzowania takich działań oraz wskazania możliwych trendów rozwoju tej dziedziny w przyszłości.

Słowa kluczowe: media społecznościowe, Facebook, Twitter, wojsko, zarządzanie kryzysowe, komunikacja kryzysowa, Izrael Defence Forces, US Army

Social media on duty for the army – case study of chosen examples of military defence forces

Abstract

Social media has a vide and variety application in business and social communication but still is rarely used in emergency management, especially in crisis communication. Military decision-makers all over the world are still more to avoid communication with society about their operations than to clarify their decisions, motivations and circumstanes of action. Forced to be more transparent and open they prefer to use traditional means of communication than the new one. However, there are few good examples of use social media by the army, particularly from Israel Defense Forces and USArmy. The article aims to present good practices in the discussed subject and possible trends of use of social media by the army in the future.

Keywords: social media, Facebook, Twitter, army, emergency management, crisis communication, Izrael Defence Forces (IDF), USArmy

Magdalena Rudnicka
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Wykorzystanie Internetu przez organizacje terrorystyczne jako komponent manipulacji w cyberprzestrzeni

Wstęp

W sferze publicznej coraz częściej podnosi się kwestię cyberbezpieczeństwa. Jednak w tym obszarze zdecydowanie brakuje rzetelnej analizy, a dominację przejmuje strach. Owa panika stanowi główne zamierzenie terrorystów, paraliżuje wolność lub w zupełności komprymuje prawa osobiste oraz prywatność jednostki. W wielu państwach o demokratycznym ustroju, walka z cyberzagrożeniami przybiera charakter polityczny, często staje się przedmiotem rentownych interesów. Nawet, jeśli owe zagrożenia nie są współmierne z rzeczywistością, to należy podkreślić, że istnieją, a ich przesadzony charakter jest konsekwencją manipulacji mediów. Celem artykułu jest ocena aktualnego stanu zagrożeń bezpieczeństwa, jakie niesie ze sobą cyberprzestrzeń. W walce o medialność terroryści zdobyli nowe narzędzie, jakie stanowi Internet. W wielu płaszczyznach sieć internetowa staje się bardziej skutecznym środkiem przekazu niż tradycyjna telewizja czy prasa. Za główną tezę przyjęto, że organizacje terrorystyczne w oczywisty sposób wykorzystują Internet do reklamy, werbowania nowych członków, a przede wszystkim do manipulowania społecznościami. Wraz z rozwojem technologii informacyjnych, przenosi się ich oddziaływanie na wszystkie sfery aktywności człowieka. Globalizacja oraz dynamicznie rozwijające się sektory gospodarki kształtują nowe wzorce zachowań, jak też style życia. Wraz z wysokim poziomem rozwoju technologicznego powstał cyberterroryzm – terroryzm wymierzony w kluczowe dla państwa systemy, sieci i usługi teleinformatyczne.

Cyberterroryzm jako jedna z postaci terroryzmu

Po raz pierwszy termin „cyberterroryzm" pojawił się w Szwecji w 1979 roku. Został zawarty w raporcie o zagrożeniach komputerowych. Dotyczył wszelkiej działalności z użyciem komputerów, mającej na celu destruowanie systemów nadzoru i kontroli, systemów teleinformatycznych, danych bankowych posiadanych przez instytucje państwowe, a w następstwie zastraszanie rządów państw oraz społeczeństw, stosowanie szantażu psychologicznego, doprowadzanie do znacznych strat materialnych, a nawet zagrożenia życia. Stosowanie ataków cybernetycznych przez zamachowców wzrosło po wydarzeniach w Nowym Jorku – zamachach na Word Trade Center. Po tych zajściach zwrócono uwagę na prawdopodobieństwo wystąpienia ataków o podobnym charakterze na całym świecie (Sienkiewicz i in. 2006, s. 11-20).

Dostrzeżono również realność ataków na systemy teleinformatyczne USA oraz państw koalicyjnych, które brały udział w walce z globalnym terroryzmem. Wówczas amerykańska ustawa antyterrorystyczna została poszerzona o nową definicję terroru, jaką stanowił cyberterroryzm. W raporcie noszącym nazwę „Cyberataki podczas wojny z terroryzmem", który został opracowany przez Instytut Technologii Bezpieczeństwa (z ang. *Institute for Security Technology*) wyodrębniono cztery podstawowe źródła cybertrroryzmu, do których zaliczono: klasyczne grupy terrorystyczne, do których mogłyby partycypować takie kraje, jak Rosja, Kuba czy Chiny; fanatycy grup terrorystycznych i amerykańscy hakerzy; osoby charakteryzujące się poszukiwaniem silnych wrażeń, które nie mają w tym interesu politycznego ani ideologicznego.

Biorąc pod uwagę swoistość cyberprzestrzeni, zjawisko cyberterroryzmu należy rozpatrywać w kilku wymiarach, a mianowicie:

- narzędzia propagandowego, zawierającego w sobie element informacyjny lub dezinformacyjny (priorytetem jest zastraszanie oraz popularność),
- skutków dezorganizacyjnych.

Można skonstatować, że wąskie ujęcie cyberterroryzmu to aktywność terrorystyczna w systemach teleinformatycznych, zorientowana na modyfikację lub zniszczenie danych w tych systemach, prowadząca do zniszczenia mienia w dużym stopniu, a nawet przynosząca ofiary śmiertelne (Górka 2014, s. 283).

Należy podkreślić, że aktywność organizacji terrorystycznych w sieciach teleinformatycznych daje możliwość:

- bezpiecznego kontaktowania się między sobą, przesyłania danych i rotacji informacji, realizowania programów propagandowych,
- prowadzenia działalności terrorystycznej w ścisłym znaczeniu,
- zdobywanie informacji zawartych w różnych portalach, w tym przeszukiwanie stron WWW.

Cyberprzestrzeń stała się dobrze prosperującym centrum szkoleniowym, które jest trudne do zlokalizowania z uwagi na szybkość oraz łatwość zacierania śladów działalności w sieci. Specjaliści przewidują, że istnieje ryzyko progresu takich działań, w szczególności przez islamskie ugrupowania terrorystyczne. Od kiedy w sieci zaczęły pojawiać się karykatury Mahometa, rozpoczęła się swoista cyberwojna. Rezultatem były zintensyfikowane ataki hakerów, wymierzone na strony internetowe oraz strony instytucji państwowych w całej Europie Zachodniej (Górka 2014, s. 284).

Aby chronić państwo przed atakami cybernetycznymi konieczne było stworzenie bardziej zaawansowanych systemów zabezpieczeń. Najbardziej narażone stały się rządowe strony internetowe, infrastruktura krytyczna oraz infrastruktura bankowa (Bógdoł-Brzezińska, Gawrycki 2003, s. 103). Do najbardziej spektakularnych zamachów cybernetycznych doszło w maju 2007 roku na Estonię, na przełomie czerwca i lipca w 2008 roku na Litwę, jak też w sierpniu 2008 roku na

Gruzję. Podczas szczytu NATO, który miał miejsce z Pradze w 2002 roku zdecydowano o wdrożeniu *Programu Ochrony Cybernetycznej* (z ang. *Cyber Defense Program)* oraz rozwoju Zdolności Reagowania na Incydenty Komputerowe (z ang. *Computer Incident Response Capability*). Atak cybernetyczny wymierzony w Estonię, spowodował paraliż całego państwa, doszło do zablokowania sieci komórkowych i dostępu do systemu bankowego. Za sprawcę ataku uznano Rosję, jednak nie udało się zgromadzić dowodów obciążających, które formalnie potwierdziłyby wrogie działanie władz tego kraju (Bukalska 2009). Natężone ataki cybernetyczne zmusiły państwa członkowskie NATO do podjęcia efektywnych działań, zmierzających do przeciwdziałania tego typu zagrożeniom.

Styczeń 2008 roku był miesiącem, w którym przyjęto Strategię Obrony Cybernetycznej (z ang. *Policy on Cyber Defence*). Natomiast w maju 2008 roku szefowie sztabów generalnych Estonii, Łotwy, Litwy, Hiszpanii, Włoch, Niemiec i Słowacji oraz Sojusznicze Dowództwo Transformacji (z ang. *Allied Command Transformation – ACT*) podpisali Memorandum o utworzeniu w Tallinie Centrum Kompetencyjnego ds. Ochrony Teleinformatycznej (z ang. *Concept for Cooperative Cyber Defense Centre of Excellence – CCD COE*). Polska do CCD COE przystąpiła w listopadzie 2011 roku, razem z USA. Zapisy odnoszące się do bezpieczeństwa w cyberprzestrzeni znalazły również swoje miejsce w Koncepcji Strategicznej NATO, powstałej w listopadzie w 2010 roku. W czerwcu 2011 roku ministrowie obrony państw NATO podpisali dokument o nazwie Polityka NATO w obszarze cyberobrony (z ang. *NATO Policy on Cyber Defense*), jak też Plan działania (z ang. *Cyber Defence Action Plan*).

Cyberterroryzm – wyzwanie dla ochrony cyberprzestrzeni

Co powoduje, że cyberterroryzm staje się jednym z najważniejszych wyzwań XXI wieku? Naukowcy, wojskowi oraz politycy ciągle starają się odpowiedzieć na to pytanie. Glenn Buchan wytypował sześć głównych powodów, które niemal zachęcają cyberterrorystów do przeprowadzania ataków w sieci:

- obniżony nakład pieniężny takiej działalności, porównując je z kosztami działalności zbrojnej. Obecnie do przeprowadzenia ataku cyberterrorystycznego wystarczy przeciętnej jakości sprzęt komputerowy, dostęp do Internetu oraz umiejętności;
- zanikanie suwerennych granic państw; cyberterroryzym ma charakter globalny, atak na dany kraj można dokonać niemal z każdego miejsca na ziemi, w którym jest dostęp do Internetu; granice wyznaczające strefy prywatne od stref międzypaństwowych ulegają zatarciu; zanikanie barier wszelkiej kategorii może skutkować tym, że zaatakowane państwo, nie będzie tego świadome;
- Internet daje możliwość dokonywania nagłych oraz nieprzewidzianych akcji, ofiary znajdują się w pełnej nieświadomości, nie są przygotowane do ich odparcia;

- zupełna anonimowość – daje to sposobność do manipulowania informacjami, komplikuje nawiązywanie międzypaństwowych koalicji oraz stawia państwa w bezsilności w odpieraniu ataków;
- zminimalizowane ryzyko wykrycia planowanego ataku;
- największe straty ponosi system zaatakowanego państwa; ofiary nie są najważniejszym celem ataku; liczy się siła wpływania na opinię publiczną oraz efekt popularyzacji terrorystycznego czynu(Buchan 1996, s. 108).

Można skonkludować, że istnieje wiele innych powodów, dla których terroryści przenieśli swoją działalność do cyberprzestrzeni. Pospolite metody działania terrorystów przynoszą ryzyko im samym. Sieć internetowa umożliwia przeprowadzenie ataku bez narażania swojej własnej osoby. Kolejnym predykatorem jest to, że nie trzeba do tego posiadać konkretnego wykwalifikowania, wystarczy trochę umiejętności. Równie dobrze, można się posłużyć wynajętymi hakerami, którzy za odpłatność finansową są w stanie przeprowadzić cyberatak np. dla zabawy, łamiąc systemy zabezpieczeń bez świadomości, jak ogromne szkody może wywołać ich działanie. Podejmowanie walki z cyberterroryzmem wymaga skoordynowanych, dobrze zaplanowanych działań. Biorąc pod uwagę szybkość w rozwoju technologii i powstawaniu nowych metod szyfrowania informacji, steganografii czy kryptografii, terroryści odczuwają beztroskę pod względem bezpieczeństwa w działaniu (Collin 1998, s. 76). Kolejnym powodem jest zmiana postrzegania zagrożenia, trudno wyłowić te groźby, które są realne, a które pozostają tylko w świecie wirtualnym. Należy również zauważyć, że państwa mają ograniczenia pod względem możliwości zastosowania sankcji. O wiele łatwiej jest bronić się przed fizycznym zagrożeniem aniżeli przez niewidzialnym przeciwnikiem, stąd powstanie dezintegracji w odpowiedzi zaatakowanego kraju wobec cyberterrorystów.

Następnym powodem jest ogólna dostępność do komputerów. W czasach, kiedy Windows nie był zintegrowanym systemem operacyjnym, wykonanie jakiejkolwiek pracy na komputerze wymagało posiadania odpowiednich umiejętności. Aktualnie wystarczy wiedzieć, gdzie włącza się komputer, aby móc sprawnie z niego korzystać. W analogiczny sposób można postrzegać narzędzia potrzebne do przeprowadzenia ataku cybernetycznego. W sieci można znaleźć wiele programów, które dają możliwość odszyfrowania kodu dostępu do bazy danych, czy włamania się do systemu. Współmiernie, ze zmniejszaniem się posiadania niezbędnych umiejętności do przeprowadzenia cyberataku, wzrasta skuteczność i jakość programów, dających taką możliwość. Mając na uwadze powyższe, każdy z nas może zostać cyberterrorystą (Collin 1998, s. 78).

Ochrona cyberprzestrzeni jest jednym z kluczowych elementów, dotyczących bezpieczeństwa państwa. Organizacje międzynarodowe czy inne podmioty niepaństwowe są świadome, że stabilizacja w funkcjonowaniu oraz powszechny rozwój globalnego społeczeństwa informacyjnego, są zależne od

otwartej, sprawnej, a przede wszystkim bezpiecznej cyberprzestrzeni. Gwałtowny wzrost ataków przeprowadzanych w sieci powinien wiązać się ze zwiększaniem świadomości w tym zakresie. Polska również jest krajem narażonym na tego typu zagrożenia. Porównywalnie z innymi państwami, stoimy przed wyzwaniem, jakie stanowi wypracowanie nowych dyrektyw prawnych i organizacyjnych, zapewniających właściwy poziom bezpieczeństwa w cyberprzestrzeni, a co za tym idzie, bezpieczeństwa funkcjonujących w nim ludzi.

Terroryzm w wirtualnym świecie

Wydarzenia, które miały miejsce 11 września 2001 roku w Nowym Jorku spowodowały, że wielu specjalistów zajmujących się bezpieczeństwem państwa, spodziewało się kolejnego ataku w cyberprzestrzeni. Niezwłocznie podjęto działania zmierzające do odseparowania terrorystów od informacji o istotnym wpływie na bezpieczeństwo kraju. Ze stron internetowych usunięto plany zarządzania kryzysowego, które były opublikowane przez Agencję Ochrony Środowiska (z ang. *The Environmental Protection Agency*). Plany dotyczyły postępowania na wypadek katastrof chemicznych. Departament Transportu (z ang. *The Departament of Transportation*) zminimalizował dostęp do informacji o schematach i położeniach geograficznych amerykańskich rurociągów. Z Internetu wycofano raport o brakach w przygotowaniu na wypadek chemicznego ataku terrorystycznego, który został opublikowany przez Centrum Kontroli i Zapobiegania Chorobom (z ang. *The Center fot Disease Control and Prevention*). Działań o takim charakterze, podjęto o wiele więcej. Wytworzono nawet projekt, dotyczący powstania równoległej sieci informacyjnej – Govnet. Miała ona stanowić bezpieczny kanał łączności dla wszystkich federalnych instytucji Stanów Zjednoczonych. Govnet miał być w zupełności odizolowany od Internetu, jego koszt oszacowano na miliardy dolarów (Dębek 2002, s. 18). Jednak specjaliści w dziedzinie informatyki jasno stwierdzili, że powstanie bezpiecznej sieci to fikcja. Podejście do cyberterroryzmu miało bardzo poważny wymiar.

Uświadomienie sobie zagrożenia, jakie może wynikać z ataku cyberterrorystycznego, wysuwa się na pierwszy plan w aspekcie podjęcia niezbędnych działań w celu zapobieżenia tej groźbie. Kolejny etap stanowi określenie konkretnych obiektów, które mogłyby być w zainteresowaniu cyberterrorystów. Idąc za W. Schwartau, można stwierdzić, że na ataki cyberterrorystyczne najbardziej narażone są system bankowy Wall Street, centrala elektroniki medycznej, system kontroli lotów, publiczne systemy ratownictwa oraz sieci energetyczne (Schwartau 1999, s. 64).

Na postawie literatury dotyczącej ataków cyberterroryzmu, możemy wyróżnić dwa rodzaje tego typu działań:

- mających miejsce wyłącznie w cyberprzestrzeni;
- ataki na systemy informacyjne przy użyciu siły fizycznej.

Oba rodzaje działalności mogą się obopólnie uzupełniać. Jeśli cyberatak występuje w towarzystwie jakiejś większej kampanii, terroryści dokonują działań pozorujących czy też ułatwiających faktyczne uderzenie w rzeczywistym świecie (Górka 2014, s. 139). Atak fizyczny na systemy informacyjne to walka uskuteczniana przy pomocy znanych metod, zmieniają się jedynie cele tych działań. Członkowie ugrupowań terrorystycznych wiedzą, jak duże znaczenie w obecnym świcie ma informacja i są świadomi, że atak paraliżujący infrastrukturę informacyjną może poczynić większe szkody, niż zwykły, fizyczny akt terrorystyczny. Jednak nie wszystkie organizacje terrorystyczne dysponują możliwościami, finansami czy umiejętnościami w wykorzystaniu nowoczesnych technologii do realizacji zamierzonych celów. Stąd też pojawiła się tendencja do łączenia starych i nowych technik działania. A. Rathmell dokonał podziału organizacji terrorystycznych, które posługują się nowymi technikami. Wyróżnił trzy kategorie, takie jak:

- kategoria I – nowe techniki są wykorzystywane do prowadzenia rutynowej działalności; używa się ich do gromadzenia informacji, komunikacji oraz pozyskiwania środków finansowych;
- kategoria II – wykorzystanie starych technik do nowych działalności, dewastacja systemu informacyjnego przy pomocy siły fizycznej;
- kategoria III – zastosowanie nowych technik do nowych działań, cyberatak na system informacyjny (Rathmell 1997, s. 3-4).

Instytucje zajmujące się nadzorowaniem cyberprzestrzeni ostrzegają, że liczba ataków dokonywanych w świecie wirtualnym sukcesywnie wzrasta. Z badania, które zostało przeprowadzone na potrzeby raportu „W obronie cyfrowych granic" wynika, że w 2015 roku niemal połowa firm w Polsce zanotowała ok. 6 cyberataków w ciągu roku (Urban, Krasoń 2016). Wiąże się to z ponoszeniem ogromnych strat finansowych.

Wykorzystanie Internetu do działań terrorystycznych

Lata dziewięćdziesiąte były czasem, w którym ugrupowania terrorystyczne zaczęły dostrzegać rolę Internetu (Adamski 2007, s. 44). Niewątpliwie Internet to narzędzie łatwo dostępne, tanie, szybkie. Członkowie organizacji terrorystycznych dostrzegli jego przydatność, chociażby pod względem nieograniczonej możliwości przekazu, wpływu na postawy społeczne czy siły oddziaływania (Lenarcik 2006, s. 18). Anonimowość, jaką zapewnia, sprawia, że terroryści bardzo chętnie z niego korzystają. Działalność ugrupowań terrorystycznych w cyberprzestrzeni może przybrać wiele kierunków. Służy im m.in. do rozpowszechniana propagandy prowadzącej do mobilizacji, rekrutacji nowych członków oraz zrzeszania sympatyków, zamieszczania ekstremistycznych treści, jak też do komunikowania się, publikowania instrukcji dotyczących przeprowadzania ataków (Lenarcik 2006, s. 23). Terroryści wykorzystują eksterytorialny charakter Internetu przede

wszystkim do prowadzenia wojny psychologicznej, akcji związanych z rozpowszechnianiem nieprawdziwych bądź zniekształconych informacji, promowania wyznawanej ideologii. Wszystko to ma silny związek z prowadzeniem propagandowej kampanii internetowej, której priorytet stanowi dotarcie do jak największej liczby odbiorców z zamiarem przekonania ich do swojej ideologii, w tym również do szerzenia nienawiści. Inną, równie popularną formą wykorzystania Internetu przez organizacje terrorystyczne jest szerzenie agitacji politycznej oraz manipulowanie założeniami ideowo-religijnymi. Fachowość w tym zakresie osiągnęła Al-Ka'ida, która założyła swoje własne przedsiębiorstwo PR-owsko-informacyjne Al-Sahab (Jihad Intel b. d.). Al-Sahab zajmuje się głównie publikowaniem w Internecie nagrań z odezwami, komunikatami oraz publicznymi oświadczeniami przywódców ugrupowania.

Internet wykorzystywany jest także w fazie planowania ewentualnych ataków, jako środek łączności służący do przeprowadzenia rozpoznania operacyjnego terenu planowanego uderzenia. Nieograniczona dostępność do map czy nawet zdjęć służy nie tylko do zdobywania informacji, ale także daje możliwość przygotowania konwencjonalnego ataku przy użyciu legalnych, ogólnodostępnych środków.

Internet stanowi narzędzie, przy pomocy którego, terroryści zastraszają społeczeństwo. Treści w nim publikowane nie podlegają cenzurze, a więc jest to doskonałe miejsce do udostępniania informacji o przeprowadzonych przez terrorystów akcjach. W telewizji nie znajdziemy nagrania na żywo z egzekucji. Natomiast w Internecie istnieją strony i fora internetowe, które w całości poświęcone są emitowaniu obrazów nienawiści np. serwis OGRISH.COM (obecnie LiveLeak.com). Kilka miesięcy po rozpropagowaniu obrazów z egzekucji, wykonanej na irackich zakładnikach, na OGRISH.COM powstała specjalna sekcja, nazwana Beheading/Hostage/Execution Videos emitująca filmy z egzekucji obywateli amerykańskich np. dziennikarza Daniela Pearl.

Podsumowanie

Medialny charakter terroryzmu znajduje swoje odbicie zarówno w naukach politycznych, jak też prawnych. Terroryści dążą do swoich celów, wykorzystując mass media oraz Internet jako kanały informacyjne. Stało się oczywistym, że terroryści wykorzystują podstawowe wartości demokratyczne, jakimi bezspornie są wolność słowa oraz wolność rozpowszechniania informacji. Z przedstawionych konstatacji można wyciągnąć bardzo ważny wniosek – terroryzm jest nieodłącznie związany ze światem wirtualnym, stanowią niemal symbiotyczną relację. Zatem jeśli Internet działa na korzyść organizacji terrorystycznych, powinien też być ważnym elementem walki z nim. W konflikcie pomiędzy terrorystami a demokracją, środki masowego przekazu opowiadają się po stronie demokracji. Punktem wyjścia musi być pogodzenie się z tym, że dobry

terroryzm nie istnieje, co najwyżej mogą istnieć szczytne cele, do osiągnięcia których, wykorzystuje się niegodne sposoby. Ocena metod stosowanych przez terrorystów jednoznacznie musi być negatywna. Cyberterroryzm zdecydowanie stanowi realne zagrożenie dla bezpieczeństwa narodowego oraz międzynarodowego, a przy tak szybkim rozwoju, ma szansę stać się jednym z największych wyzwań współczesnego świata.

Bibliografia

Adamski, J. (2007) *Nowe technologie w służbie terrorystów.* Warszawa: Collegium Civitas, Wydawnictwo TRIO.

Bógdoł-Brzezińska, A., Gawrycki, M. (2003) *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa: Fundacja Studiów Międzynarodowych, Oficyna Wydawnicza ASPRA-JR.

Buchan, G. (1996) *Information Warfare and the Air Force: Wave of Future? Current Fad?* Santa Monica, Calif.: Rand.

Bukalska, P. (2009) *Eesti.pl.* Dostęp: 12.05.2009. Tryb dostępu: http://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html.

Collin, B. C. (1998) *Cyberterrorism. From Virtual Darkness: New Weapons in a Timeless Battle.* San Luis: Obispo.

Dębek, S. (2002). *Niewidzialne uderzenie*. „Chip", nr 12, s. 18.

Górka, M. (red.) (2014) *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXi wieku.* Warszawa: Difin.

Database: Identifiers of Designated Islamic Terrorist Organizations, Al-Qaeda: Al-Sahab Media. Dostęp: 01.12.2014. Tryb dostępu: http://jihadintel.meforum.org/identifier/298/al-qaeda-al-sahab-media.

Lenarcik, M. (2006) *Terroryzm w erze informacji. Internet jako narzędzie w rękach terrorystów.* Warszawa.

Urban, P., Krasoń, A. (2016) *W obronie cyfrowych granic czyli 5 rad, aby realnie wzmocnić ochronę firmy przed CYBER ryzykiem.* Dostęp: 12.01.2016, Tryb dostępu: http://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagrozenia-2016.pdf.

Streszczenie

Artykuł został poświęcony aspektowi wykorzystania Internetu przez organizacje terrorystyczne. Zawiera opis cyberterroryzmu jako jednej z postaci terroryzmu. Poruszono w nim kwestię motywów, jakimi kierują się organizacje terrorystyczne przy wykorzystaniu sieci internetowych.

Słowa kluczowe: cyberterroryzm, sieć informacyjna, atak cybernetyczny; cyberterrorism, information network, cyberatack

Use of the Internet by terrorist organizations as a component of manipulation in cyberspace

Abstract

The article was devoted to the aspect of the use of the Internet by terrorist organizations. It contains a description of cyber-terrorism as one of the forms of terrorism. It addresses the question of motives guided by terrorist organizations using online networks.

Keywords: cyberterrorism, information network, cyber attack

Rafał Klepka
Uniwersytet Pedagogiczny w Krakowie

Ewolucja Wiadomości TVP1: od medialnej stronniczości do propagandy politycznej

Wprowadzenie

Problematyka bezpieczeństwa informacyjnego w państwie demokratycznym bez wątpienia obejmuje także zagadnienia odnoszące się do sposobu, w jaki media informują obywateli o wydarzeniach politycznych. Badacze zarówno demokracji, jak i mediów zgodnie podkreślają, że obiektywne media stanowią jeden z istotniejszych warunków funkcjonowania tego systemu politycznego (Dahl 2015; Sartori 1987; Norris 2000, s. 3 i n.; McNair 2012, s. 1 i n.; Curran 2002, s. 217 i n.; Strömbäck 2005, s. 331-345). Brian McNair wskazuje pięć funkcji, jakie media pełnią w społeczeństwie demokratycznym:

- informują obywateli o tym, co dzieje się wokół nich,
- edukują obywateli o znaczeniu przekazywanych informacji, tłumaczą ich sens i konsekwencje,
- stanowią platformę publicznego dyskursu politycznego, sprzyjają formowaniu opinii publicznej, stając się także naturalnym forum wyrażania sprzeciwu,
- pilnują rządzących, przedstawiając rządzonym także niewygodne dla sprawujących władzę informacje, ujawniają nieprawidłowości i przypadki nadużyć,
- są kanałem prezentacji różnych punktów widzenia, sprzyjają artykulacji rozmaitych poglądów i programów działania i ich prezentacji masowej publiczności (McNair 2011, s. 18 i n.).

Żeby funkcje te mogły być w należyty sposób realizowane postuluje się, aby media były obiektywne, co najczęściej definiuje się jako przeciwieństwo stronniczości (Hopmann Van Aelst, Legnante 2011, s. 240 i n.). Mając na względzie powyższe uwarunkowania poddano analizie wybrane zmiany, jakie dokonały się w formie, treści i sposobie jej przekazu w przypadku programu informacyjnego „Wiadomości" nadawanego w pierwszym programie polskiej telewizji publicznej. Wybór tego właśnie programu do analizy podyktowany jest szeroką dyskusją na temat zmian, jakie dokonały się w „Wiadomościach" po wygranej Prawa i Sprawiedliwości w wyborach parlamentarnych w 2015 roku. Celem opracowania jest charakterystyka i ocena zmian w kontekście zarysowanej koncepcji dotyczącej roli mediów w systemie demokratycznym.

Media: obiektywne czy stronnicze?

Mimo wskazanych postulatów dotyczących obiektywizmu mediów jako warunku sprzyjającego demokracji, podnieść należy, że obiektywizm pozostaje

ideą nie zaś stanem, który da się w pełni osiągnąć. Istnieje zatem możliwość prowadzenia porównawczych badań empirycznych, które pozwolą wykazać, który z analizowanych programów czy tytułów pozostaje bardziej obiektywny, który zaś jest w większym stopniu stronniczy, premiuje określone racje polityczne, w lepszym świetle ukazuje wybraną partię polityczną, czy częściej cytuje opinie opowiadające się za jedną z racji. Podkreślić należy jednak, że relacjonowanie polityki przez media – niezależnie od przyjętej optyki badawczej – zawsze uznać można za stronnicze do pewnego stopnia. Telewizyjny program informacyjny nie może przedstawić całego kilkugodzinnego wydarzenia. Konieczne staje się dokonanie skrótu, a więc wyboru części – fragmentów, które zostaną zaprezentowane. Proces selekcji, którego ogólne założenia tłumaczy koncepcja *gate-keepingu*, uznać należy za pierwsze nieuniknione źródło przyczyny, dla której medialne obrazy świata mają charakter subiektywny (Shoemaker, Vos 2009, s. 11 i n.; Soroka 2012, s. 514 i n.).

Poza tą niezamierzoną w istocie rzeczy formą stronniczości (*structural bias)*, istnieje także szereg działań, które określić można jako zamierzoną stronniczość polityczną (*intended political bias*). Dotyczy ona sytuacji planowanego doboru treści, polegającego na przemilczeniu wybranych wydarzeń, uwypukleniu innych, zestawianiu rzeczy nieporównywalnych czy niedających się porównać, nadawaniu określonego kontekstu poprzez wydźwięk lub kolejność prezentowanych treści, wreszcie uzupełnieniu treści przez stosowny komentarz do prezentowanych wydarzeń (Groseclose, Milyo 2005, s. 308 i n.; Toggle 1998, s. 65 i n.). Pomiędzy niedostępnym w mediach, ale możliwym do wyobrażenia pełnym obiektywizmem, a skrajnie nieobiektywnym, stronniczym prezentowaniem rzeczywistości, rozciąga się więc kontinuum, które wraz ze zmniejszającą się skalą obiektywizmu przechodzi w stronę medialnej propagandy politycznej.

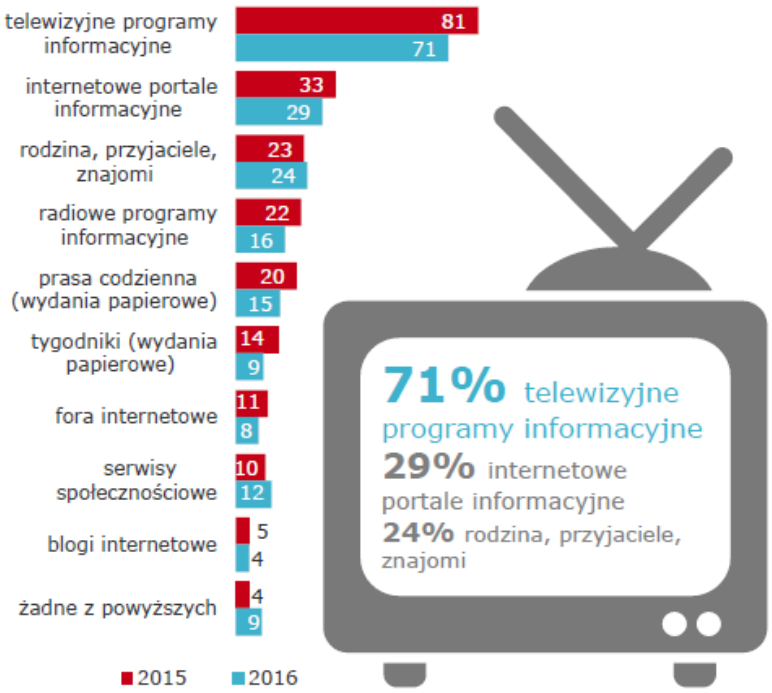
Samo pojęcie propagandy od dawna jest przedmiotem badań i analiz naukowych (Bernays 1928; Pratkanis, Aronson 2001; Cull, Culbert, Welch 2003; Jowett, O'Donnell 2012). Jego znaczenie zmieniało się, zaś szczególnie negatywny wydźwięk uzyskało w związku z totalitaryzmami XX wieku, których istotną częścią była wszechobecna propaganda (Wilke 2015, s. 492 i n.). Medialną propagandę polityczną należy rozumieć jako taką metodę kształtowania przekazu medialnego, aby w sposób celowy i zamierzony wpływać na poglądy, postawy i działania poprzez podawanie tylko części informacji, prezentowanie ich w korzystnym stale dla tego samego podmiotu kontekście lub komentowanie ich zawsze w sposób tendencyjny, właściwy tylko dla jednego punktu widzenia.

„Wiadomości" TVP: pierwszy program informacyjny Polaków

Rozważania na temat obiektywizmu głównego wydania Wiadomości TVP w kontekście bezpieczeństwa informacyjnego oraz znaczenia mediów w państwie demokratycznym wynikają z kilku zasadniczych przesłanek. Po pierwsze, badania

sondażowe przeprowadzone w Polsce w 2016 roku dowodzą, że mimo rosnącego znaczenia Internetu, telewizja wciąż pozostaje głównym źródłem informacji o polityce. W przeprowadzonym na ogólnopolskiej, reprezentatywnej próbie 1011 mieszkańców Polski w wieku 15 i więcej lat przez TNS OBOP badaniu 71% respondentów wskazało, że głównym źródłem informacji na temat polityki są dla nich telewizyjne programy informacyjne (TNS OBOP 2016, s. 5).

Rys. 1. Wyniki badania sondażowego dotyczącego źródeł, z których ludzie czerpią informacje na temat polityki



Źródło: *Wiarygodne informacje – czy są dziś w cenie?* TNS OBOP (2016), s. 5. Dostęp: 01.02.2017. Tryb dostępu: http://www.tnsglobal.pl/wp-content/blogs.dir/9/files/2016/05/K.023_Wiarygodne_informacje_O03a-16.pdf.

Po drugie, „Wiadomości" TVP są historycznie pierwszym po okresie transformacji ustrojowej programem informacyjnym w Polsce, który emitowany jest w telewizji publicznej nieprzerwanie od 18 listopada 1989 r. (*O Wiadomościach* 2017). „Wiadomości" mają więc zdecydowanie dłuższe tradycje od emitowanych przez programy komercyjne „Faktów" TVN oraz „Wydarzeń" Polsatu. Należy także mieć na uwadze fakt, iż przez wiele lat istniały gospodarstwa domowe, które ze względów technicznych lub ekonomicznych, miały dostęp jedynie do telewizji publicznej, co utrudniało im możliwość

zapoznania się z ofertą informacyjną telewizji prywatnych. Zmiana tego stanu rzeczy, którą przyniosła cyfryzacja przekazu sygnału telewizyjnego, nie zmienia faktu, że stacje komercyjne w niektórych gospodarstwach domowych w Polsce są obecne od niedawna i dopiero zyskują popularność i zaufanie widzów.

Po trzecie, główne wydanie „Wiadomości" TVP nadawane codziennie o godzinie 19.30 bez wątpienia ma wciąż wysoką oglądalność, a co za tym idzie uznać można je także za program opiniotwórczy. Na początku lat 90. ubiegłego stulecia program mógł liczyć nawet na 16 milionów widzów (Mielczarek 2007, s. 288). Wzrastająca liczba źródeł informacji, pojawienie się Internetu oraz rozwój telewizji komercyjnych doprowadziły do ponad czterokrotnego spadku oglądalności. W dalszym ciągu jednak „Wiadomości" mają widownię na poziomie zbliżonym do 3 milinów widzów, przy czym ostatni rok przyniósł radykalny spadek oglądalności, przy jednoczesnym wzroście liczby widzów programu „Fakty" w komercyjnej telewizji TVN (Kurdupski 2017).

Po czwarte wreszcie, przed „Wiadomościami", w odróżnieniu od innych programów informacyjnych nadawanych przez komercyjne stacje telewizyjne, stoją określone zadania wynikające z ustawy z 29 grudnia 1992 roku o radiofonii i telewizji. Program ten ma *realizować obowiązki i powinności nadawcy publicznego*, a więc cechować się *pluralizmem, bezstronnością, wyważeniem i niezależnością oraz innowacyjnością, wysoką jakością i integralnością przekazu*.

Stronniczość polityczna „Wiadomości" TVP: w stronę propagandyzacji

Przekonanie o tym, że główne wydanie programu informacyjnego nadawanego przez TVP1 nie jest bezstronne wyrażane jest bardzo często przez medioznawców, polityków, dziennikarzy i wielu bardziej wnikliwych widzów (Dobek-Ostrowska 2011, s. 150 i n.). Powszechnie przyjęta pozostaje także teza o silnej zależności pomiędzy władzami TVP – a tym samym także szefami działów informacji – a partią bądź koalicją rządzącą. Po każdych wyborach parlamentarnych, które prowadzą do zmiany partii rządzącej, wkrótce zmieniają się także szefowie TVP. Przed wyborami parlamentarnymi w 2015 roku wiele zarzutów dotyczących stronniczości „Wiadomości" wypowiadali politycy związani z będącą wówczas w opozycji partią Prawo i Sprawiedliwość. Tytułem egzemplifikacji wskazać można incydent, jaki miał miejsce w studiu „Wiadomości" w dniu 3. maja 2015 roku. Zaproszony w charakterze gościa programu informacyjnego oraz następującej po nim audycji „Dziś wieczorem" Marcin Mastalerek, ówczesny rzecznik Prawa i Sprawiedliwości w sposób demonstracyjny opuścił studio TVP, podkreślając, że „Wiadomości" są stronnicze i zbyt rzadko pokazują kandydata PiS na urząd prezydenta RP, Andrzeja Dudę. Po wspomnianych wyborach parlamentarnych i zmianach, jakie dokonały się w TVP o nierzetelności „Wiadomości" mówią obecne partie opozycyjne i przeciwnicy

rządzącej partii Prawo i Sprawiedliwość. Nieuniknione w tej sytuacji wydaje się pytanie: czy i dlaczego przeobrażania, jakie dokonały się w programie informacyjnym TVP po 2015 roku traktować należy inaczej od tych, jakie miały miejsce dotąd po kolejnych elekcjach parlamentarnych i będących ich konsekwencją zmianach rządów.

Aby udzielić odpowiedzi na to pytanie posłużono się analizą zawartości. Metoda ta, jak wskazywał jeden z jej prekursorów Bernard Berelson, ma na celu obiektywny, systematyczny i ilościowy opis jawnej treści komunikatu (Berelson 1952; Richardson 2007; Riffe, Lacy, Fico 2005; Krippendorff 2004; Pisarek 1983; Lisowska-Magdziarz 2004). Obiektywizm wynika z założenia, że badanie powinno zostać przeprowadzone w taki sposób, aby każdy kolejny badacz powtarzający analizę uzyskał takie same wyniki. Systematyczność badań wiąże się z określonym doborem materiału. Kryteria selekcji muszą być jasne, jednoznaczne i wynikające z obiektywnych przesłanek. Przykładowo, chcąc analizować określony program informacyjny pod kątem sposobu, w jaki prezentowany jest w nim wizerunek premiera obiektywizm wiąże się z koniecznością stworzenia takich kryteriów analizy, które będą w jak największym stopniu jednoznaczne dla wyniku badania, niezależnie od preferencji politycznych przeprowadzającego analizę. Z kolei systematyczność oznacza, że badane będą albo wszystkie wydania programu, albo tylko z wybranego dnia tygodnia, albo wedle innego czytelnego kryterium. Jedynie wówczas analiza zawartości stanowi metodę badawczą służącą uzyskaniu nowej wiedzy, nie jest zaś narzędziem służącym uzasadnieniu poglądów autora badania.

Odpowiedzi na pytanie badawcze udzielono na podstawie trzech przeprowadzonych badań: dwóch pierwotnych oraz jednego wtórnego. W pierwszym badaniu przeprowadzono analizę zawartości wybranych wydań programu „Wiadomości" TVP z okresu poprzedzającego ostatnie wybory parlamentarne (okres kampanii prezydenckiej – kwiecień 2015 roku) oraz okresu następującego po dokonanych zmianach (kwiecień 2016 roku). W drugim badaniu przeprowadzono analizę zawartości głównych wydań trzech programów informacyjnych: „Wiadomości" TVP, „Wydarzeń" Polsatu oraz „Faktów" TVN w okresie pomiędzy 6.07 a 10.07.2016 roku, a więc w dniach, gdy w Warszawie trwał szczyt NATO, w okresie jego przygotowań oraz w dniu następującym po zakończeniu szczytu. Wyniki badań własnych skonfrontowano z efektami badań uznanych medioznawców, Macieja Mrozowskiego i Tatiany Popadiak-Kuligowskiej zatytułowanymi „Ekspertyza programów informacyjnych głównych wydań TVP1 Wiadomości, TVN Fakty, Polsat Wydarzenia", a przeprowadzonymi na zlecenie Krajowej Rady Radiofonii i Telewizji w okresie od 4.02 do 11.02.2016 roku.

Uzyskane wyniki wskazują, że zmiany w sposobie prezentowania wydarzeń politycznych po wyborach w 2015 roku nie sprowadzają się do prostego zastąpienia stronniczości politycznej sprzyjającej byłym partiom rządzącym na rzecz premiowania nowego ugrupowania, którego przedstawiciele zasiadają

w ławach rządowych. W pierwszym z analizowanych okresów (kwiecień 2015 roku) czas poświęcony na prezentowanie działań rządu oraz ich ocenę ze strony opozycji był względnie zrównoważony, ponadto wydarzenia polityczne prezentowano z dystansem, akcentując niekiedy naturalny w państwie demokratycznym spór pomiędzy rządzącymi a opozycją, wskazywano na rolę trwającej kampanii wyborczej oraz podkreślano, że działania rządzących oraz opozycji nastawione są na uzyskanie poparcia w obliczu nadchodzących wyborów parlamentarnych i trwającej kampanii prezydenckiej. Przywoływani eksperci często pozytywnie wypowiadali się o projektach opozycji, a krytycznie o pomysłach rządowych, byli skłonni raczej do oceny problemów, nie zaś konkretnych opcji politycznych. W istniejących sporach społeczno-politycznych, takich jak dyskurs na temat przyjmowania do Polski uchodźców, wskazywano na szeroki wachlarz aspektów, jakie należy wziąć pod uwagę, dowodząc ambiwalentnego charakteru problemu, wokół którego rozmaite rozwiązania mają zawsze zarówno dobre, jak i złe strony. Analiza zawartości programów z kwietnia 2015 roku pozwala wskazywać na nieznacznie częstszą prezentacją Bronisława Komorowskiego jako kandydata na prezydenta niż Andrzeja Dudę. Nierzadko jednak pierwszy z pretendentów do urzędu głowy państwa prezentowany był w charakterze aktualnie piastującego stanowisko, a nie kandydata.

„Wiadomości" TVP z kwietnia 2016 roku wykazują odmienną optykę prezentowania rzeczywistości politycznej. W centrum polityki znajduje się partia rządząca, jej prezes oraz premier, nieco rzadziej prezydent, którzy podejmują z założenia słuszne działania na rzecz Polaków, jednocześnie zaś słaba, skłócona opozycja, na ogół nieskutecznie, próbuje blokować reformy i zmiany. Intencją opozycji jest, według przekazu programu, przede wszystkim utrudnianie słusznych działań rządu z uwagi na ochronę swoich interesów. Punkt widzenia opozycji, jej argumentacja, zwykle przedstawiane są w sposób na tyle skrócony, aby widz odebrał ją wyłącznie jako bezcelowe hamowanie działań demokratycznie wybranego rządu reprezentującego przekonania i interesy większości Polaków, którzy w wyborach poparli Prawo i Sprawiedliwość. Uwagę zwraca jednowymiarowość komentarzy i dobór ekspertów wypowiadających opinie w programie. Są to na ogół, często powtarzający się, dziennikarze prawicowych mediów, którzy potwierdzają i afirmują narrację programu. Uwagę zwraca jednowymiarowość w zakresie oceny problemów społeczno-politycznych, które mają zawsze tylko dobre lub złe konsekwencje, jak na przykład uchodźcy, którzy generują problemy społeczne, kulturowe, ekonomiczne i religijne.

Drugie z przeprowadzonych badań prowadzi do wniosków o odmiennym sposobie prezentacji szczytu NATO w Polsce przez „Wiadomości" TVP oraz programy komercyjne. W programie TVP akcentowana była przede wszystkim narodowa duma z rządowego sukcesu, jakim była organizacja szczytu oraz konsekwencje, jakie przyniósł on Polsce. Serwisy informacyjne telewizji

prywatnych omawiane wydarzenie prezentowały przez pryzmat wielu czynników: politycznych, historycznych, militarnych i społecznych. Podnoszono także historyczny charakter procesu, w wyniku którego Warszawa stała się miejscem organizacji szczytu NATO, podczas gdy „Wiadomości" TVP akcentowały w szczególności zasługi rządzących, eliminując historyczny kontekst szczytu. Warto jako przykład niezwykle wyrazisty, albowiem będący wynikiem analizy tylko ilościowej, niepoddanej jakiejkolwiek interpretacji, podać fakt, iż „Wiadomości" TVP 8 lipca nie zrelacjonowały wypowiedzi prezydenta Baracka Obamy na temat Polski. Prezydent USA powiedział tego dnia w Warszawie do prezydenta Dudy: *Jako wasz przyjaciel i sojusznik namawiam do zachowania instytucji demokratycznych*. Wypowiedź ta, niezwykle krytyczna wobec reform ustrojowych przeprowadzanych po ostatnich wyborach parlamentarnych, została przez „Wiadomości" TVP pominięta. Odmiennie jej znaczenie odczytały pozostałe analizowane programy informacyjne. Program „Fakty" telewizji TVN wypowiedź Obamy przedstawił w 32. sekundzie wydania z 8 lipca, zaś program „Wydarzenia" Polsatu w 42. sekundzie. Na marginesie odnotować można jedynie, że wypowiedź Baracka Obamy dotyczącą demokracji w Polsce zaprezentowały także niemal wszystkie programy informacyjne na świecie.

Badania wtórne przeprowadzone w innym okresie czasu silnie korespondują z wynikami badań pierwotnych. Raport końcowy opracowany na zlecenie Krajowej Rady Radiofonii i Telewizji wskazuje, że wyniki przeprowadzonej i opisanej w raporcie analizy zawartości „Wiadomości" dały podstawę do niezwykle krytycznej oceny (Mrozowski, Popadiak-Kuligowska 2016). Chodziło nie tylko o mankamenty ustalone w analizie ilościowej, ale także o niepokojące naruszenia prawa i etyki dziennikarskiej. Wyniki badań wskazały, że wymóg pluralizmu przekazywanych informacji i punktów widzenia w analizowanych wydaniach programu „Wiadomości" realizowany był w ograniczonym zakresie. W newsach dotyczących wydarzeń politycznych z reguły uwzględniano głosy opozycji parlamentarnej, jednak zwykle były to wypowiedzi krótsze i bardziej ogólne, funkcjonujące w przekazie na zasadzie: opozycja jak zwykle atakuje rząd i nie ma nic konkretnego do zaproponowania, a jak już coś zaproponuje (np. projekt PO w sprawie Rodzina 500+), to tylko dla propagandowego efektu. Testem na pluralizm informacji w analizowanym okresie był też między innymi społeczny protest przed pałacem prezydenta RP przeciwko nowelizacji ustawy o policji – protest pokazano poprawnie, ale relacja reportera starała się odwrócić uwagę od jego istoty i zdyskredytować protestujących. W efekcie widz nie wiedział, o co chodzi protestującym.

Wnioski

Wyniki badań analizy zawartości programu „Wiadomości" TVP prowadzą do niepokojących konstatacji. Oto główne wydanie serwisu informacyjnego

o najdłuższej historii w III RP staje się programem propagandowym, w istocie rzeczy odległym zarówno od realizacji powinności wynikających z przywołanej już ustawy, jak i od standardów programów informacyjnych typowych dla państw europejskich o ugruntowanym ustroju demokratycznym. Warto z całą pewnością pogłębiać zasygnalizowane tu jedynie kierunki analizy zawartości „Wiadomości" TVP. Wydaje się, że wobec szczególnej roli telewizyjnych programów informacyjnych w okresie kampanii wyborczych, wartościowe mogą być analizy porównawcze zarówno w czasie, jak i pomiędzy wybranymi programami informacyjnymi, przeprowadzone w okresie nadchodzących kampanii wyborczych.

Bibliografia

Berelson, B. (1952) *Content Analysis in Communication Research*. New York: The Free Press.

Bernays, E. (1928) *Propaganda*. New York: Horace Liveright.

Cull, N. J., Culbert, D. H., Welch, D. (2003) *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*. Santa Barbara, Denver, Oxford: ABC-CLIO.

Curran, J. (2002) *Media and Power*. London, New York: Routledge.

Dahl, R. A. (2015) *On Democracy*. New Haven: Yale University Press.

Dobek-Ostrowska, B. (2011) *Polski system medialny na rozdrożu: media w polityce, polityka w mediach*. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego.

Groseclose, T., Milyo, J. (2005) *A social-science perspective on media bias*. "Critical Review", nr 17 (3-4), s. 305-314.

Hopmann, D. N., Van Aelst, P., Legnante, G. (2011) *Political balance in the news: A review of concepts, operationalizations and key findings*. "Journalism", nr 13 *(*2).

Jowett, G. S., O'Donnell, V. (2012) *Propaganda and Persuasion*. Los Angeles, London, New Delhi, Singapore, Washington DC: Sage Publications.

Krippendorff, K. (2004) *Content Analysis: An Introduction to Its Methodology*. Thousand Oaks, London, New Delhi: Sage Publications.

Kurdupski, M. (2017) *„Fakty" wyprzedziły „Wiadomości" w 2016 roku. „Teleexpress" na czele dzienników (raport)*. Dostęp: 2.01.2017. Tryb dostępu: http://www.wirtualnemedia.pl/artykul/fakty-wyprzedzily-wiadomosci-w-2016-roku-teleexpress-na-czele-dziennikow-raport.

Lisowska-Magdziarz, M. (2004) *Analiza zawartości mediów. Przewodnik dla studentów: wersja 1.1*. Kraków: Uniwersytet Jagielloński.

McNair, B. (2011) *An Introduction to Political Communication*. London, New York: Routledge, Taylor & Francis Group.

McNair, B. (2012) *Journalism and Democracy: An Evaluation of the Political Public Sphere*. London, New York: Routledge.

Mielczarek, T. (2007) *Monopol, pluralizm, koncentracja: środki komunikowania masowego w Polsce w latach 1989-2006*. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Mrozowski, M., Popadiak-Kuligowska, T. (2016) *Ekspertyza programów informacyjnych głównych wydań TVP1 Wiadomości, TVN Fakty, Polsat Wydarzenia na zlecenie KRRiT z okresu 4.02.2016 r. do 11.02.2016 r.* Dostęp: 2.01.2017. Tryb dostępu: http://www.krrit.gov.pl/Data/Files/_public/Portals/0/komunikaty/12.04.2016/krrit_eksperyza.pdf.

Norris, P. (2000) *A Virtuous Circle: Political Communications in Postindustrial Societies*. New York: Cambridge University Press.

O Wiadomościach (2017) Dostęp: 2.01.2017. Tryb dostępu: https://wiadomosci.tvp.pl/17361638/o-wiadomosciach.

Pisarek, W. (1983) *Analiza zawartości prasy*. Kraków: Ośrodek Badań Prasoznawczych.

Pratkanis, A., Aronson, E. (2001) *Age of Propaganda: The Everyday Use and Abuse of Persuasion*. New York: Holt Paperbacks.

Richardson, J. E. (2007) *Analysing Newspapers: An Approach from Critical Discourse Analysis*. Houndmills, Basingstoke, Hampshire, New York: Palgrave Macmillan.

Riffe, D., Lacy, S., Fico, F. G. (2005) *Analyzing Media Messages: Using Quantitative Content Analysis in Research*. Mahwah, New Jersey, London: Lawrence Erlbaum Associates.

Sartori, G. (1987) *The Theory of Democracy Revisited. Part One: the contemporary debate*. Chatham: Chatham House Publishers.

Shoemaker, P. J., Vos, T. (2009). *Gatekeeping Theory*. New York, London: Routledge.

Soroka, S. N. (2012) *The Gatekeeping Function: Distributions of Information in Media and the Real World*. "The Journal of Politics", nr 74 (2), s. 514-528.

Strömbäck, J. (2005) *In Search of a Standard: four models of democracy and their normative implications for journalism*. "Journalism Studies", nr 6 (3), s. 331-345.

Wiarygodne informacje – czy są dziś w cenie? TNS OBOP (2016). Dostęp: 2.01.2017. Tryb dostępu: http://www.tnsglobal.pl/wp-content/blogs.dir/9/files/2016/05/K.023_Wiarygodne_informacje_O03a-16.pdf

Toggle, C. A. (1998) *The bias toward finding bias in television news*. "Communication Reports", nr 11 (1).

Wilke, J. (2015) *Propaganda*. W: Donsbach, W. (red.), *The Concise Encyclopedia of Communication*. Malden, Oxford, Chichester: Wiley.

Streszczenie

„Wiadomości" są głównym programem informacyjnym nadawanym przez TVP. Mimo istnienia wielu alternatywnych źródeł informacji rola opiniotwórcza i popularność „Wiadomości" wydaje się być bardzo wysoka. W tym kontekście uwagę zwraca daleko idąca stronniczość polityczna tego programu. Analizy zawartości programu dowodzą jednak, że po ostatnich wyborach parlamentarnych w 2015 roku „Wiadomości" TVP1 nie są już tylko stronnicze, ale stanowią przykład współczesnej propagandy politycznej.

Słowa kluczowe: stronniczość medialna, program informacyjny, bezpieczeństwo informacyjne

The evolution of Wiadomości TVP1: from media bias to political propaganda

Abstract

Wiadomości is the main news program broadcast by TVP. Despite the existence of many alternative sources of information, the opinion-forming role and the popularity of Wiadomości seems to be very high. In this context, attention is drawn far-reaching political bias of the program. The content analysis of the program argue, however, that after the recent parliamentary elections in 2015, Wiadomości TVP1 are not only biased, but there is an example of modern political propaganda.

Keywords: media bias, information program, safety information

Joanna Świątkowska
Uniwersytet Pedagogiczny w Krakowie

Działania prowadzone w cyberprzestrzeni jako metoda ingerencji w demokratyczny proces wyborczy

Walka informacyjna, czyli proces składający się, według definicji Leopolda Ciborowskiego, z trzech elementów: zdobywania, zakłócenia i ochrony informacji jest zjawiskiem znanym od wieków (Ciborowski 1999, s. 9). Ma on historię tak długą, jak długa jest egzystencja człowieka na ziemi. Już Sun Tzu – chiński strateg pisał, że *największym osiągnięciem jest pokonać wroga bez walki* (Sun Tzu 1994). Cytat ten, choć nie wprost, opisuje istotę walki informacyjnej. W najbardziej zaawansowanej odsłonie to informacja może stać kluczowym zasobem potrzebnym do realizacji założonych celów. Dziś osiągnięcie tak dojrzałego poziomu jej wykorzystania jest realne. Umożliwiają to nowoczesne technologie. Hipoteza niniejszego tekstu mówi, że współcześnie walka informacyjna prowadzona w cyberprzestrzeni ma szansę stać się siłą kształtującą rzeczywistość – przede wszystkim społeczno-polityczną. Można stać się zasobem strategicznym wpływającym na funkcjonowanie poszczególnych państw. Zagrożone są szczególnie podmioty o ustroju demokratycznym-zbudowane na transparentności i wolnym dostępie do informacji.

Walka informacyjna – cechy podstawowe i zmiany wynikające z zastosowania nowych technologii

Sednem prowadzenia walki informacyjnej jest wykorzystywanie informacji w taki sposób, aby ułatwić osiągnięcie ustalonego celu[1]. Informacja jest jednocześnie obiektem, wobec którego prowadzone są działania jak i narzędziem, które stosuje się, aby osiągnąć założony efekt. Walki informacyjnej nie prowadzi się nigdy w odosobnieniu – pełni ona raczej rolę wspierającą. Jest zawsze używana do osiągnięcia celu nadrzędnego określonego przez przestrzeń w jakiej prowadzi się działania. Na przykład, gdy stosowana w przestrzeni politycznej będzie miała za zadanie osiągnąć dany cel polityczny, podobnie w sferze gospodarczej, militarnej itd. Kolejną charakterystyką walki informacyjnej jest to, że może być ona zorientowana na oddziaływanie bądź na człowieka, bądź na nieożywiony system, który w oparciu o informacje funkcjonuje. W każdej z tych opcji używane będą różne, adekwatne narzędzia i metody. W kontekście oddziaływania na człowieka, najważniejszym elementem będzie osiąganie wpływu na jego percepcję, a w konsekwencji na jego zachowanie. Z punktu widzenia maszyn, konsekwencje mogą być bardzo szerokie. Oddziałujący może doprowadzić do kradzieży informacji, modyfikacji, usunięcia danych itd. W najbardziej zaawansowanej formie skutkiem może być zakłócenie procesów realizowanych przez dane

urządzenia, co może doprowadzić do fizycznych zniszczeń. Na potrzeby niniejszego tekstu zaproponowany zostanie podział walki informacyjnej na dwie kategorie – miękką oraz twardą. Kryterium wyróżniającym będzie następstwo danego działania. Jeśli walka zorientowana będzie na samą informację (jej kradzież, manipulowanie itd.) lub gdy jej celem będzie osiąganie wpływu na percepcję, to wtedy będziemy mówili o miękkiej formie walki. Kiedy jednak skutkiem jej stosowania będzie osiągnięcie efektów materialnych – zniszczeń, paraliżu procesów – wtedy będziemy mieli do czynienia z walką o charakterze twardym.

Pojawienie się cyberprzestrzeni opartej o funkcjonowanie sieci i systemów teleinformatycznych zrewolucjonizowało prowadzenie walki informacyjnej. Wyniosło ją na zupełnie inny poziom. Przede wszystkim sama rola informacji wzrosła tak bardzo, że dzisiaj traktowana jest jako zasób strategiczny (np. w gospodarce). Po drugie, narzędzia teleinformatyczne dały możliwość niespotykanego wcześniej oddziaływania na rzeczywistość. Są one ogólnodostępne, relatywnie tanie, łatwe w obsłudze, niezwykle efektywne. W konsekwencji pojawienie się cyberprzestrzeni zaktywizowało ogromne rzesze podmiotów. Przed erą Internetu jednostki nie dysponowały tak ogromnymi możliwościami wywierania wpływu na otoczenie za pomocą. Cyberprzestrzeń umożliwia w prawdziwie rewolucyjny sposób pozyskiwanie, tworzenie, gromadzenie i rozpowszechnianie informacji. Przykładowo prowadzenie blogów, własnych stron internetowych daje szansę wypromowania wyprodukowanej przez siebie treści wśród olbrzymiej masy odbiorców. W kontekście miękkiej walki informacyjnej Internet jest niezwykle potężnym orędziem. Możliwość osiągania wpływu na innych, manipulacji, dezinformacji stała się niezwykle łatwa[2]. Można docierać nie tylko do pojedynczych jednostek, ale do całych grup realnie kształtując emocje społeczeństw i wpływając na wydarzenia społeczno-polityczne. W odniesieniu do twardej walki informacyjnej skutki mogą być jeszcze poważniejsze. Immanentne cechy Internetu – wszechobecne połączenia między systemami oraz ich współzależność sprawiły, że wyłącznie za pomocą dostępu do komputera połączonego z siecią, wiedzy i umiejętności, pojedynczy aktorzy uzyskali szansę dokonywania działań o znacznych skutkach. Kiedyś możliwości działań zarezerwowane raczej dla aktorów państwowych[3], dziś mogą stać się udziałem prawie każdego. Przy użyciu narzędzi cyfrowych można bowiem, fizycznie uszkodzić elementy kluczowe z punktu widzenia funkcjonowania, bezpieczeństwa i rozwoju państw. Przykłady takich działań są już znane. Rok 2010 był tutaj przełomowy. Wtedy to bowiem po raz pierwszy w historii cyberatak dokonał rozległych fizycznych zniszczeń. Wirus znany jako Stuxnet zainstalowany został w irańskiej elektrowni atomowej i doprowadził do uszkodzenia wirówek uranowych. Kolejne zdarzenie miało miejsce w grudniu 2014 roku. W wyniku cyberataku uszkodzeniu uległa huta stali w Niemczech. W konsekwencji ataku

doszło do spowolnienia programu atomowego tego państwa. W powszechnej opinii panuje przekonanie, że była to operacja przeprowadzona przez Stany Zjednoczone wraz z Izraelem. W grudniu 2015 r. miał miejsce rozległy atak na ukraiński system energetyczny, w wyniku którego tysiące obywateli odciętych zostało od prądu. Strona ukraińska oskarżyła o działania Rosjan (*USA oskarża…* 2016). Choć to przykłady pokazujące wykorzystanie Internetu do prowadzenia twardej walki informacyjnej przez państwa, to w przyszłości nie można wykluczyć, że przy łatwym dostępie do zasobów podobne działania podejmą inne podmioty.

Walka informacyjna prowadzona w cyberprzestrzeni jest nadal narzędziem wspierającym główne działania konwencjonalne. Jednak dzięki nowoczesnym technologiom jej waga i rola wzrasta tak szybko i intensywnie, że obserwujemy epokową zmianę w jej prowadzeniu. Podążamy w kierunku sytuacji, w której informacja będzie kluczowym zasobem decydującym o osiągnięciu założonego celu. Będzie środkiem ciężkości stosowanej strategii. W tej sytuacji znaczenie innych zasobów, także konwencjonalnych może drastycznie zmaleć. Kształtowanie rzeczywistości, sytuacji społeczno-politycznej nie będzie wymagało podejmowania brzemiennych w skutkach decyzji o uruchomieniu na przykład siły militarnej. Realizować cele można będzie za pomocą oddziaływania na środowisko informacyjne rywala. Z punktu widzenia osiągania celów politycznych najbardziej optymalną sytuacją jest możliwość realizacji interesów danego podmiotu, bez ponoszenia szeroko rozumianych kosztów lub przy ich maksymalnym obniżeniu. Użycie tradycyjnych metod i konwencjonalnych narzędzi może być bardzo nieopłacalne. Na przykład decyzja o fizycznym podboju przeciwnika będzie z pewnością wiązała się z ryzykiem zaistnienia strat materialnych i finansowych po stronie atakującego. Należy także brać pod uwagę koszty polityczne w postaci reakcji społeczności międzynarodowej oraz możliwe działania odwetowe. Optymalizacja wyboru działań, to zatem ważny powód prowadzący do zmiany strategii działań. Kolejny wiąże się z asymetrycznością zasobów. Dla wielu graczy wejście w otwarty konflikt, gdzie liczą się konwencjonalne siły nie jest możliwy. Szukając zatem, możliwości osiągania wpływu na innych uciekać będą do unikatowych działań.

Omówione w dalszej części artykułu przykłady pokazują, że na takie działania szczególnie zagrożone są kraje o ustroju demokratycznym. Skierowanie walki informacyjnej prowadzonej przy użyciu nowoczesnych technologii na fundament państw – ich demokratyczne wybory – może zasadniczo wpłynąć na ich sytuację. W tym scenariuszu cytat z Sun Tzu może być bardziej realny niż kiedykolwiek wcześniej. Pokonanie wroga bez walki może być całkowicie możliwe. To zagrożenie, na które współczesne państwa powinny być coraz bardziej przygotowane.

Oddziaływanie na proces wyborczy za pomocą cybernarzędzi

Rozwój cyberprzestrzeni i jej wpływ na walkę informacyjną sprawił, że zarówno z punktu widzenia optymalizacji działań, jak i z punktu widzenia poszukiwania nowych metod osiągania celów, to właśnie ta metoda walki będzie coraz częściej używana. Walka informacyjna, twarda i miękka, prowadzona przy użyciu nowoczesnych technologii ma szansę spowodować zmianę reguł prowadzenia politycznej gry i zmodyfikować układ sił poszczególnych graczy. Na naszych oczach mają miejsce wydarzenia, który potwierdzają taką predykcję. Jaskrawym przykładem są wielopłaszczyznowe ingerencje w żywotne procesy współczesnych państw. Odbywają się one z użyciem narzędzi cyfrowych i są zorientowane na naruszenie procesów wyborczych – fundamentów funkcjonowania państw demokratycznych. Zanim analizie poddane zostaną konkretne przykłady warto wskazać kilka modeli prowadzenia owych działań. Z punktu widzenia ingerencji cyfrowej w procesy wyborczej wyróżnić można co najmniej trzy scenariusze (Świątkowska 2017). Działania w ramach ich podejmowane stanowią mieszankę działań twardych oraz miękkich.

W pierwszym modelu najbardziej poważnym celem ingerencji może być dosłowna manipulacja wynikami wyborów. Zamiar ten można osiągnąć poprzez włamanie się do systemów wyborczych i sfałszowanie wyników. Takie działanie jest jednak najtrudniejsze. Wynika to zarówno z technicznych trudności, jak i choćby z faktu, że wiele państw wciąż jeszcze tworzy papierowe kopie zapasowe oddanych głosów.

Drugi scenariusz jest mniej wyrafinowany technologicznie, ale ma zdecydowanie większą szansę realizacji. W tym modelu celem jest nie tyle całościowe zmanipulowanie wyniku wyborczego, ale raczej podkopanie zaufania wyborców do istoty procesu demokratycznego – jego przebiegu czy też wyników. Wystarczy zasiać niepewność czy wybory odbyły się w sposób prawidłowy. Dla części społeczeństwa – szczególnie wspierającej kandydata przegranego – może być to powód, aby kwestionować wyniki. Obniży to także poziom legitymizacji wygranej strony. W konsekwencji może zaistnieć chaos wewnętrzny w państwie, osłabienie siły politycznej władzy, obniżenie zaufania społeczeństwa. Z takim przeciwnikiem dużo łatwiej prowadzić dalszą grę, wpływać na jego zachowanie i decyzję. Społeczeństwa oraz władze skłócone, zaangażowane w spory wewnątrzkrajowe, będą mniej skłonne do prowadzenia aktywnej polityki zagranicznej. W końcu, problemy związane z kwestionowaniem prawidłowości wyborów mogą także obniżyć wiarygodność i pozycję międzynarodową danego państwa. Jego polityka będzie zdecydowanie mniej skuteczna. Z punktu widzenia potencjalnych adwersarzy, to niezwykle korzystny rozwój wydarzeń.

Trzeci scenariusz wiąże się realizacją takich działań, które wpłyną na przebieg samej kampanii wyborczej. Będą miały realny wpływ na to, jak wyborcy

głosują. Tutaj środki cyfrowe mogą zostać zaangażowane na wiele różnych sposobów. W ostatecznym rezultacie strona atakująca będzie zainteresowana wygraną jednego z kandydatów, który bardziej odpowiada z punktu widzenia realizacji interesów.

Powyższe określenie trzech możliwych metod i celów oddziaływania na proces wyborczy powinno zostać uzupełnione analizą konkretnych, już zaistniałych przypadków. Pozwoli to, zaobserwować trendy i najczęściej stosowane *modus operandi.*

Jednym z pierwszych dostrzeżonych i szerzej dyskutowanych incydentów cybernetycznych związanych z ingerencją w wybory demokratyczne były wydarzenia jakie miały miejsce na Ukrainie. Tuż przed wyborami prezydenckimi w 2014 roku doszło do ataków hakerskich na serwery ukraińskiej Komisji Wyborczej. Organizacja o nazwie Cyber Berkut, w powszechnej opinii wspierająca prorosyjski kurs Ukrainy, przyznała się do przeprowadzenia ataku. Ogłosiła, że w jego wyniku udało się przechwycić 1.2 GB e-maili, 1.78 GB innych dokumentów (Smolaks 2014), a także udało się doprowadzić do uszkodzenia funkcjonowania systemu wyborczego (*CyberBerkut announces…* 2014). Tę drugą część informacji Komisja Wyborcza szybko zdementowała. Potwierdzono natomiast utratę informacji. Opisane wydarzenia wpisują się w scenariusz oznaczony numerem drugim. Dokonanie ataku na podmiot, który odpowiedzialny jest za właściwy przebieg wyborów miało między innymi podważyć zaufanie społeczeństwa do procesu wyborczego i wybranych władz. Choć w wyniku ataku udało się jedynie wykraść informacje i nie wpłynął on na wynik wyborów, to był to wyraźny sygnał wysłany w stronę społeczeństwa Ukrainy i opinii międzynarodowej, że fundamenty tworzące życie społeczne i polityczne w tym kraju mogą zostać zagrożone przez cyberataki. Podjęte działania wytworzyły przekonanie, że jest możliwe, że pro-rosyjskie siły, z którymi Ukraina jest w konflikcie, są w stanie wpłynąć na wynik niezależnych wyborów. Sytuacja miała swój ciąg dalszy. W trakcie wyborów w rosyjskich mediach umieszczony został zrzut ze strony internetowej Komisji Wyborczej, wedle którego cząstkowe wyniki wyborcze wskazywały na zwycięstwo lidera radykalnego ruchu „Prawy Sektor" Dmytra Jarosza (*Russian TV announces…* 2014). Oczywiście były to informacje sfabrykowane. Mogły jednak doprowadzić do dwóch rezultatów. Po pierwsze do pojawienia się olbrzymiej dezinformacji i chaosu zarówno wśród społeczeństwa ukraińskiego, jak i wśród międzynarodowej opinii publicznej. Rzekome duże poparcie dla lidera radykalnych sił politycznych mogłoby wpisywać się w promowaną przez Rosję tezę, że rewolucja na Ukrainie jest działaniem niebezpiecznych, agresywnie nastawionych grup społecznych i politycznych. Po drugie, w obliczu wcześniejszych doniesień o atakach hakerskich na system wyborczy, wątpliwa informacja o uzyskaniu dużego poparcia dla kandydata, który zupełnie nie był faworytem, mogła utwierdzić opinię publiczną, że akt głosowania

został jednak skutecznie zmanipulowany, a wynikom nie można wierzyć. Obniżenie wiarygodności władz oraz pokazanie słabości państwa mogło być celem działania.

Biorąc pod uwagę stopień zaawansowania prowadzonych działań, ingerencja w proces wyborczy na Ukrainie była jednak wyłącznie incydentem w porównaniu z serią wydarzeń jaka miała miejsce podczas amerykańskiej kampanii wyborczej. Kwestie związane z cyberbezpieczeństwem stały się kluczowym czynnikiem, który znacznie wpłynął na przebieg całego procesu wyborów. Ich oddziaływanie było wielowymiarowe i przybierało bardzo zróżnicowane formy. Wykorzystywano zarówno twarde, jak i miękkie metody prowadzenia walki politycznej. Początek stanowiło ujawnienie informacji, że faworytka wyścigu wyborczego Hillary Clinton w trakcie pełnienia funkcji sekretarza stanu używała prywatnego maila do prowadzenia działań służbowych. Sprawa była tak poważnym nadużyciem, że kandydatkę do fotelu prezydenta przesłuchiwało FBI, a przeprowadzone śledztwo wykazało, że przez jej prywatną skrzynkę mogło przejść ponad 100 wiadomości, którym wcześniej nadano status informacji niejawnych (*FBI odkryło*… 2016). W konsekwencji newralgiczne informacje mogły dostać się w niepowołane ręce. Choć postępowanie władz nie przyniosło postawienia oficjalnych zarzutów wskazywano, że Clinton wykazała się *skrajnym niedbalstwem* (*USA: FBI wznawia…* 2016). Pomimo braku zarzutów, sprawa rzuciła fatalne światło na kandydatkę. Ukazała ją jako osobę nie dbającą wystarczająco o najcenniejsze zasoby państwowe, niegodną powierzenia najważniejszych z punktu widzenia interesów publicznych spraw i obowiązków. Punkt zwrotny przyniosła także ogłoszona na jedenaście dni przed wyborami, decyzja dyrektora FBI Jamesa Comey'a o tym, że agencja wznowi dochodzenie w sprawie skrzynki mailowej Clinton (*USA: FBI wznawia*… 2016). Informacja ta pojawiła się w kluczowym momencie kampanii i jeszcze mocniej nadszarpnęła wizerunek kandydatki. Drugim elementem wykorzystania cyberprzestrzeni w trakcie amerykańskiej walki wyborczej był cyberatak dokonany na systemy Komitetu ds. kampanii wyborczych Demokratów oraz na konta e-mailowe prominentnych członków tej partii (*Atak rosyjskich…* 2016). W wyniku tego działania wypłynęły informacje dotyczące funkcjonowania partii Demokratów. Materiały pojawiły się na portalu Wikileaks i stały się przedmiotem dyskusji na temat funkcjonowania amerykańskich elit. Wiele z nich wywołało polityczne dyskusje bardzo szkodzące kandydatce. Także samo wykorzystanie portalu WikiLeaks w powszechnej opinii wspierającego „przejrzystość życia publicznego" było zręcznym manewrem umacniającym wrogie starania. Już w trakcie kampanii Demokraci na czele z samą Clinton publicznie wskazywali, że za działania prowadzone w cyberprzestrzeni odpowiadają hakerzy powiązani z Kremlem. Rzekomo mieli oni wspierać w walce wyborczej kandydata Republikanów – Donalda Trumpa (*Kolejny atak hakerski*… 2016). Choć w prawie całym okresie

kampanii wyborczej Clinton przeważała w sondażach, ostatecznie to Trump zwyciężył i został prezydentem USA. Po zakończeniu wyborów i po przeprowadzeniu działań analitycznych oraz śledczych, amerykańskie władze oficjalnie potwierdziły, że Rosjanie, prowadząc ofensywne działania w cyberprzestrzeni, manipulowali wyborami w USA i wpłynęli na ostateczny ich wynik (*Background*… 2017). Zrealizowany został trzeci modelowy scenariusz. W sposób perfekcyjny udało się wpłynąć na percepcję, opinię, osądy społeczeństwa amerykańskiego. Doskonale dopasowano narrację i przekaz do aktualnych resentymentów społeczeństwa USA. Tradycyjne strategie walki informacyjnej wzmocniono zastosowaniem nowych technologii. W konsekwencji zdarzeń prezydent Barack Obama, zdecydował się na nałożenie oficjalnych sankcji dyplomatycznych na Rosję i jej oficjeli. Było to bezprecedensowe zdarzenie, pokazujące, że kwestie związane z cyberbezpieczeństwem stały się elementem „najwyższej polityki" (Choucri 2012, s. 3) i kwestią bezpieczeństwa politycznego i narodowego współczesnych państw.

Podsumowanie

Powyższa analiza jasno pokazuje, że ofensywne działania prowadzone w cyberprzestrzeni mogą realnie wpłynąć na najważniejsze procesy jakie mają miejsce we współczesnych państwach. Przewidywania Sun Tzu stały się bardziej realne niż kiedykolwiek wcześniej. Pokonać, a przynajmniej wpłynąć na wroga, można zupełnie bez walki. W wyniku działań prowadzonych w cyberprzestrzeni rywal jest w stanie – wykorzystując informacje, a dzięki nim m.in. wpływając na nastroje, percepcję opinii publicznej – wpłynąć na to, kto przejmuje stery rządzenia państwem. Wobec już zauważalnych sukcesów jest bardzo prawdopodobne, że ten nowy typ działań będzie stosowany w przyszłości. Rządy Niemiec czy Czech już oficjalnie mówią o tym, że obawiają się, że przy pomocy cyberdziałań obcy gracze będą chcieli także wpłynąć na ich wybory. Dzięki nowym technologiom walka informacyjna zyskała całkowicie nowe możliwości oddziaływania. Prawdziwe możliwości i konsekwencje, jakie dla politycznej sytuacji międzynarodowej oraz stabilności systemu bezpieczeństwa przyniosą te działania, przyjdzie nam dopiero poznać. Niestety mogą być one znacznie poważniejsze niż można było sądzić jeszcze kilka lat temu. W dodatku będą one szczególnie dotkliwe dla państw demokratycznych, gdzie wolny i swobodny dostęp do informacji stanowi fundament funkcjonowania życia społecznego.

Przypisy

[1] W tym kontekście w niniejszym artykule zastosowane zostanie pewne uproszczenie. Według logiki zaproponowanej przez Leopolda Ciborowskiego należy bowiem rozróżnić różne kategorie – sygnały, bodźce itd.

[2] Sprzyjają temu także mechanizmy anonimizujące działania prowadzone w sieci, pozwalające podszywać się pod innych, fałszować swoją tożsamość. Są to między innymi: The Onion Router (TOR), czyli projekt zapobiegający analizie ruchu sieciowego, system TAILS, serwery proxy, generatory tożsamości, anonimowe skrzynki e-mail itd.

[3] Posiadających zasoby, możliwości dużo bardziej zaawanasowane, niedostępne dla innych graczy.

Bibliografia

Atak rosyjskich hakerów na Demokratów „elektronicznym Watergate" (2016). Dostęp: 01.12.2016. Tryb dostępu: http://www.polskieradio.pl/5/3/Artykul/1654098,Atak-rosyjskich-hakerow-na-Demokratow-elektronicznym-Watergate.

Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (2017). Dostęp: 06.01.2017. Tryb dostępu: https://assets.documentcloud.org/documents/3254259/ICA-2017-01.pdf.

Choucri, N. (2012) *Cyberpolitics in International Relations.* Massachusetts: MIT Press.

Ciborowski, L. (1999) *Walka informacyjna*. Toruń: Europejskie Centrum Edukacyjne.

CyberBerkut announces destruction of electronic system of Ukraine's Central Election Commission (2014). Dostęp: 01.09.2016. Tryb dostępu: https://sputniknews.com/voiceofrussia/news/2014_05_23/CyberBerkut-announces-destruction-of-electronic-system-of-Ukraines-Central-Election-Commission-5809/.

FBI odkryło 15 tysięcy maili Hillary Clinton. Potwierdzają kontakty z prywatnymi sponsorami? (2016). Dostęp: 25.11.2016. Tryb dostępu: https://www.wprost.pl/swiat/10020338/FBI-odkrylo-15-tysiecy-maili-Hillary-Clinton-Potwierdzaja-kontakty-z-prywatnymi-sponsorami.html.

Kolejny atak hakerski na Partię Demokratyczną w USA (2016). Dostęp: 01.12.2016. Tryb dostępu: http://www.polskieradio.pl/5/3/Artykul/1649186,Kolejny-atak-hakerski-na-Partie-Demokratyczna-w-USA.

Russian TV Announces Right Sector Leader Led Ukraine Polls (2014). Dostęp: 08.11.2016. Tryb dostępu: http://www.rferl.org/a/russian-tv-announces-right-sector-leader-yarosh-led-ukraine-polls/25398882.html.

Smolaks, M. (2014) *Pro-Russian Hackers Attack Central Election Commission Of Ukraine*. Dostęp: 04.05.2016. Tryb dostępu: http://www.techweekeurope.co.uk/workspace/cyberberkut-hackers-attack-central-election-commission-of-ukraine-146180#pxotB6YAl0D5gvdw.99.

Sun Tzu (1994) *Sztuka wojny*. Warszawa: Przedświt.

USA oskarża Rosję o cyberatak na Ukrainę (2016). Dostęp: 11.10.2016. Tryb dostępu: http://www.rp.pl/Konflikt-na-Ukrainie/160219754-USA-oskarza-Rosje-o-cyberatak-na-Ukraine.html.

Świątkowska, J. (2017) *Walka informacyjna może zagrozić także Polsce.* Dostęp: 10.01.2017. Tryb dostępu: http://biznesalert.pl/swiatkowska-walka-informacyjna-moze-zagrozic-takze-polsce/.

USA: FBI wznawia śledztwo ws. maili Hillary Clinton (2016). Dostęp: 25.12.2016. Tryb dostępu: http://wiadomosci.onet.pl/swiat/wybory-w-usa-fbi-wznawia-sledztwo-ws-maili-hillary-clinton/fdlcht.

Streszczenie

W ostatnim czasie cyberbezpieczeństwo zyskało dużą uwagę opinii publicznej. Jednak to ostatnie minione miesiące pokazały nowe możliwości jakie daje oddziaływanie w cyberprzestrzeni. Za jej pomocą można skutecznie ingerować w fundamenty polityczne adwersarzy. Artykuł dokonuje analizy wpływu działań prowadzonych w cyberprzestrzeni na procesy wyborcze. Dzięki temu omówione zostanie prowadzenie walki informacyjnej opartej na nowych technologiach i jej wpływ na stabilność sytuacji międzynarodowej oraz bezpieczeństwo międzynarodowe.

Słowa klucze: cyberbezpieczeństwo, cyberataki, wybory, manipulacja, walka informacyjna.

Cyberactivities as Tools For Interference in Democratic Electoral Processes

Summary

Recently, cybersecurity has gained a lot of public attention. However, these past months only have shown the new opportunities offered by cyberspace. By using cybertools, one can effectively intrude into the foundations of its adversaries' political order. The article analyses the impact of activities conducted in cyberspace on electoral processes. A new form of information warfare –

undertaken with the use of new technologies – is discussed, as well as its impact on the stability of international relations and international security.

Key words: cybersecurity, cyberttacks, elections, manipulation, information warfare.

*

Z historii wojskowości

Tomasz Jan Biedroń
Uniwersytet Pedagogiczny Krakowie

Struktura Narodowej Organizacji Wojskowej w Krakowie i formy pracy jej wydziałów

Decyzją członków konspiracyjnego Komitetu Głównego i Zarządu Głównego Stronnictwa Narodowego („Kwadrat") z 13 października 1939 roku postanowiono utworzyć organizację wojskową, niewiążącą się „na razie" z innymi konspiracyjnymi organizacjami wojskowymi, działającymi na terenie kraju – tymczasowo bez jednolitej nazwy. Ustalono, że w każdym okręgu Stronnictwo Narodowe mogło posiadać organizację wojskową z własną nazwą. Dopiero na początku 1940 r. Organizacja Wojskowa SN zaczęła przyjmować jednolitą nazwę: Narodowa Organizacja Wojskowa, faktycznie dopiero przyjętą 1 lipca 1941 r. we wszystkich okręgach w kraju [1].

1. Powstanie Narodowej Organizacji Wojskowej w Krakowie

Zgodnie z wytycznymi Komendy Głównej NOW, pod koniec listopada 1939 r., przybył do Krakowa ppor. rez. Władysław Jaworski „Jacek", „Wit" pełniący funkcje członka prezydium SN i kierownika wydziału organizacyjnego, a równocześnie w organizacji wojskowej SN kierownika łączności z terenem, aby przekazać organizacji krakowskiej instrukcje dotyczące nowych metod pracy w konspiracji i zasad tworzenia organizacji wojskowej SN.

Początkowo jego poglądy dotyczące tworzenia własnej organizacji wojskowej nie znalazły poparcia i zrozumienia zarówno w samym kierownictwie okręgu, jak i wśród niektórych działaczy SN w Krakowie. Rozbite na skutek aresztowania Kierownictwo Okręgu Krakowskiego SN, aresztowanie prezesa Zarządu Okręgu, prof. Józefa Haydukiewicza, wyjazd trzech członków zarządu poza granice kraju w wyniku działań wojennych (prof. Władysława Folkierskiego, inż. Adama Doboszyńskiego i Franciszka Jelonkiewicza), nie było w stanie sprostać wyznaczonemu zadaniu. Należało wpierw uzupełnić skład Zarządu Okręgu SN, aby móc dopiero prowadzić rozmowy, co też wkrótce uczyniono [2]. Ppor. Jaworski prowadził rozmowy z krakowskimi działaczami SN m.in. z emerytowanym płk. dypl. Tadeuszem Wołkowickim „Hipolitem", Stanisławem Rymarem, dr. Stanisławem Nowogrodzkim, Tadeuszem Surzyckim, Janem Ostaszewskim celem przekonania ich do idei powołania niezależnej organizacji wojskowej. Instrukcja Zarządu Głównego SN o tworzeniu samodzielnej organizacji wojskowej SN, z odrębną od organizacji politycznej strukturą organizacyjną, własną komendą główną, komendami okręgowymi, powiatowymi, spotkała się ze sprzeciwem grupy konspiracyjnych wpływowych działaczy Okręgu Krakowskiego SN.

Tworzona organizacja wojskowa odczuwała brak ludzi o odpowiednich kwalifikacjach wojskowych na szczeblach komend, okręgów i powiatów. Przedstawiciele ZG Stronnictwa Narodowego uważali, że pion wojskowy, a zwłaszcza tworzone komendy, powinny być obsadzone wyłącznie oficerami zawodowymi, posiadającymi doświadczenie wojskowe w zakresie dowodzenia, co było poważnym utrudnieniem w budowaniu organizacji wojskowej SN. Okazało się bowiem, że wśród członków i sympatyków stronnictwa nie było wystarczającej liczby oficerów zawodowych poza przeniesionymi z przyczyn politycznych w stan spoczynku jeszcze przed 1939 rokiem (np. mjr Władysław Owoc, kpt. Józef Drelichowski, płk Euzebiusz Hausner, płk Tadeusz Wołkowicki). Wielu po zakończeniu działań wojennych znalazło się poza granicami kraju. Z konieczności musiano więc, poprzestać na cywilach posiadających zaledwie przeszkolenie wojskowe w zakresie rezerwy. W omawianym okresie najczęściej spotykanym stopniem wojskowym w szeregach organizacji wojskowej SN był podporucznik rezerwy lub podchorąży rezerwy. Z konieczności zaczęto więc, do komend poszczególnych szczebli wprowadzać ludzi, którzy w ogóle nie odbyli nawet służby wojskowej, a przy obsadzaniu stanowisk w organizacji wojskowej brano pod uwagę nie wyszkolenie wojskowe, ale zdolności organizacyjne i przydatność w pracy konspiracyjnej.

I chociaż początkowo Zarząd Okręgu SN nie mógł utworzyć Komendy Okręgu Krakowskiego organizacji wojskowej z powodu braku oficerów zawodowych, to mimo tego wydał instrukcję o uruchomieniu pracy organizacyjnej w podległych powiatach i rekrutacji ludzi do powstających organizacji wojskowych. Już pod koniec 1939 roku powstały pierwsze komendy powiatowe NOW w czterech najbliżej Krakowa leżących powiatach: krakowskim, bocheńskim, myślenickim, miechowskim. Z nich utworzono następnie jako jeden z pierwszych Podokręg Krakowski NOW. Kolejne komendy NOW zorganizowano w powiatach: tarnowskim, brzeskim oraz w Pilźnie, gdzie już we wrześniu 1939 r. powstała bardzo silna placówka organizacji wojskowej SN. Na ich bazie powstał Podokręg Tarnowski NOW [3]. Zatem o wiele wcześniej od Komendy OK NOW w Krakowie powstały komendy w niektórych powiatach.

2. Formowanie się i struktura Komendy Okręgu Krakowskiego Narodowej Organizacji Wojskowej

W pierwszym okresie tworzenia Komendy Okręgu Krakowskiego NOW brak było odpowiedniego kandydata na stanowisko komendanta okręgu. Wprawdzie odpowiednie kwalifikacje posiadał płk dypl. Tadeusz Wołkowicki „Hipolit", to jednak na propozycję ppor. Jaworskiego objęcia stanowiska Komendanta Okręgu NOW w Krakowie, odmówił, tłumacząc się podeszłym wiekiem i „małą sprężystością działania". Dowodził, że funkcję tę winien objąć człowiek młody, prężny, energiczny, mogący wiele zdziałać dla organizacji. Naciskany przez ppor.

Jaworskiego zobowiązał się w końcu do znalezienia odpowiedniego kandydata na komendanta.

Na przełomie marca-kwietnia 1940 r. płk dypl. Tadeusz Wołkowicki zaproponował kandydata na komendanta OK NOW, zawodowego wojskowego w stopniu pułkownika, znajomego z wojska. Był to oficer w stanie spoczynku, ale jeszcze stosunkowo młody i energiczny. Został więc, zaprzysiężony przez ppor. W. Jaworskiego, który tymczasowo powierzył mu funkcję p.o. komendanta, aż do chwili zorganizowania przez niego komendy OK NOW i zapoznania się z terenem, ludźmi, organizacją. Jak się wkrótce okazało ów pułkownik, nie nadawał się na to stanowisko i niewiele też zdziałał [4].

Do pomocy przy organizowaniu Komendy Okręgu Krakowskiego NOW, p.o. Komendanta Głównego NOW ppor. rez. Bolesław Kozubowski zaproponował swojego znajomego ppor. rez. Franciszka Szweda ps. „ Franek", „Romanowski", który niebawem został kierownikiem wydziału organizacyjnego w Komendzie OK NOW. Próba utworzenia komendy Okręgu Krakowskiego nie powiodła się, bowiem zarówno pułkownik, jak i ppor. Franciszek Szwed nie znali terenu i ludzi i z tego powodu nie mogli sprostać pracy organizacyjnej. Prawdopodobnie stało się to powodem odwołania pułkownika z funkcji p.o. komendanta OK NOW, względnie jego rezygnacji. Komendantem został wówczas ppor. rez. Franciszek Szwed „Franek", który podobnie zresztą jak odwołany pułkownik, również nie sprostał zadaniu, ponieważ nie posiadał kontaktów z terenem, gdzie nie był znany, na dodatek był w stopniu ppor. rez., co utrudniało mu kontakty wśród zawodowych oficerów, dlatego jego osiągnięcia organizacyjne były mizerne. Stanowisko komendanta zawdzięczał w dużej mierze przyjacielskim kontaktom z ppor. Bolesławem Kozubowskim pełniącym wówczas obowiązki Komendanta Głównego NOW [5].

W lipcu 1940 r., zagrożony aresztowaniem, przybył z Brzozowa do Krakowa mjr Władysław Owoc „Paweł", „Fruktus". Mjr Owoc w Brzozowie był prezesem powiatowej organizacji SN. Na początku 1941 r. został mianowany Komendantem Okręgu Krakowskiego NOW. Po latach w swojej pracy napisał, że dowództwo nad Okręgiem przejął od ppor. Szweda, choć nie bez oporów z jego strony. Major Owoc posiadał cechy dobrego konspiratora, był człowiekiem doświadczonym, opanowanym i rozważnym, cechy te w konspiracji odgrywały niebagatelną rolę. Poza tym znał osobiście wielu działaczy i konspiratorów, co bardzo ułatwiało mu wiązanie porwanych kontaktów organizacyjnych, często zrywających się na skutek niemieckich aresztowań. Znali go dobrze również ci, którzy później stali się agentami Gestapo. Wyjątkowemu szczęściu mógł on zawdzięczać fakt, iż ani razu nie wpadł w ręce Gestapo, które zastawiało na niego wielokrotnie pułapki. Na co dzień zawsze skromny i niepozorny, jego ubiór oraz postać zwykłego, prostego, spracowanego człowieka mogła mylić i dezorientować – na pierwszy rzut oka. Zewnętrznemu obserwatorowi trudno było dopatrzyć się w sylwetce mjr Owoca

osoby wysokiej rangi społecznej, a tym bardziej komendanta Okręgu Krakowskiego NOW. Podobny sposób postępowania w konspiracji przyjął kpt Adam Stabrawa zastępca, a następnie komendant Podokręgu Kraków-Miasto, chodzący na co dzień w ubraniu roboczym, stanowiącym doskonały kamuflaż.

Mjr Owoc komendę Okręgu Krakowskiego zorganizował z ludzi zupełnie nowych, nieznanych na terenie Krakowa. Sam ciągle zmieniał miejsca zamieszkania, kwatery oraz nazwiska, przez co uniknął aresztowania, mimo prowadzonej aktywnej działalności konspiracyjnej. Ten wędrowny tryb życia wymagał niespożytych sił, a mjr Owoc je posiadał. Zawsze niestrudzony w istocie przez cały czas wojny żył wyłącznie sprawami NOW. Jego żywe bezpośrednie i pełne osobiste zaangażowanie się sprawami NOW nastrajało dowódców i żołnierzy podobnym duchem, jemu zaś zjednywało osobistą sympatię u podwładnych. Do końca wojny pełnił obowiązki Komendanta Okręgu Krakowskiego NOW.

Bez osobowości typu mjr Owoca, kpt Stabrawy NOW w okręgu krakowskim nie mogłoby ani istnieć, ani rozwijać się. Prawa walki z okupantem w miarę upływu czasu uformowały zespół dowódców tego właśnie typu, a rozwój form walki doprowadził do tego, iż nieodłącznym atrybutem postaci konspiratora w pewnym etapie tej walki stała się broń. Konspiratorzy, postacie zwykle bez własnych nazwisk, bez prawa do własnej sylwetki i twarzy, ludzie bez własnych domów i życia osobistego, jedynie w broni znajdowali ochronę, a w oddziałach dywersyjnych i partyzanckich jedyną możliwą dla nich formę życia. W ten sposób konspiracja nieuchronnie przeradzała się w dywersję i partyzantkę. Wszelako dla dowódcy tego szczebla i pokroju, jakim był mjr Owoc, partyzantka nie mogła być sferą bezpośredniego osobistego działania. Mjr Owoc, jako konspirator ze stylu i trybu życia, rozumiał dobrze konieczność organizowania oddziałów partyzanckich i oddziały te skutecznie organizował. Z chwilą przejęcia dowództwa przez mjr. Władysława Owoca nastąpił duży postęp w pracy organizacyjnej całego okręgu. Mjr Owoc jeżdżąc nieustannie od powiatu do powiatu odbudowywał i poszerzał konspiracyjne szeregi Narodowej Organizacji Wojskowej. Przeorganizowane oraz uzupełnione nowymi ludźmi zostały poszczególne Wydziały Krakowskiego Okręgu NOW: „Kościuszko", „Ugory".

Duże zasługi w organizowaniu Komendy OK NOW oddali: Henryk Grabowski „Ambroży", przysłany przez KG NOW do pomocy mjr. Owocowi, pełniący funkcję kierownika wydziału propagandy, oraz Władysław Augustyn „Spytek" przedwojenny działacz Stronnictwa Narodowego w powiecie brzeskim, sprawujący funkcję kierownika wydziału organizacyjnego OK SN. Augustyn znał dobrze teren i ludzi niemal całego krakowskiego okręgu, szczególnie jego wschodnią część. Oddał nieocenione usługi w nawiązywaniu porwanych skutkiem działań wojennych i aresztowań nici organizacyjnych. To właśnie Augustyn i mjr Owoc w ciągu 1941 i 1942 r., jeżdżąc nieustannie od powiatu do powiatu,

odbudowali struktury NOW i SN. W wielu powiatach ponownie zaczęły działać Komendy Powiatowe [6].

Od chwili objęcia dowództwa przez mjr Owoca nastąpił zdecydowany zwrot w stylu pracy okręgu. Reorganizacji poddano wydziały OK NOW, uzupełniając je nowymi ludźmi w sposób zapewniający im stałą obsadę przez cały okres okupacji. Komendy podokręgów i powiatów organizowane były na wzór komendy okręgu. Jednak nie zawsze wszystkie referaty były takie same. Tworzono je w zależności od potrzeb i możliwości kadrowych.

Komenda Okręgu Krakowskiego NOW składała się z siedmiu wydziałów [7].

Wydział Operacyjny

Przez krótki czas szefem Wydziału Operacyjnego był płk dyplomowany Florian Smykal „Strzała", a dopiero po nim płk dypl. Euzebiusz Hauser „Jot", pełniący funkcję szefa sztabu i szkolenia w komendzie okręgu. Płk Hauser był także zastępcą komendanta OK NOW majora Owoca. Do zadań Wydziału operacyjnego należało opracowywanie programów szkolenia dla Okręgu Krakowskiego NOW. Programy obejmowały: szkolenie bojowe, naukę o broni, strzelanie, naukę służby wojskowej oraz musztrę, które następnie przekazywano do podokręgów w formie rozkazów szkoleniowych. Wydział opracowywał plany operacyjne akcji przeprowadzanych przez własne oddziały przeciwko Niemcom oraz inne zadania, jak np. likwidacja konfidentów współpracujących z okupantem. W podokręgach i powiatach często funkcje komendanta i referenta operacyjnego były łączone, przykładem był Podokręg Kraków – Miasto „Krajewski" [8].

Wydział Organizacyjny

Wydziałem Organizacyjnym kierował Walerian Gołuński „Jarosz" od 1942 r. do chwili aresztowania w 1943 r. Na jego miejsce ppłk Owoc powołał we wrześniu 1944 r. ppor. Władysława Gałkę, „Lis", „Wiktor", dotychczasowego komendanta Podokręgu Kraków Zewnętrzny, zasłużonego oficera NOW i dobrego organizatora. Najważniejsze zadanie wydziału organizacyjnego polegało na tworzenie struktur i oddziałów NOW, zapewnienie ich dyspozycyjności, sprawności organizacyjnej, bojowej oraz bezpieczeństwa konspiracyjnego. Do szefa wydziału należał sprawowanie kontroli nad podległymi komendami i oddziałami, przeprowadzanie częstych inspekcji w podległych placówkach. Szef wydziału organizacyjnego sprawował faktycznie także funkcję zastępcy komendanta okręgu, w przypadku, gdy komendant z powodu zagrożenia dekonspiracją musiał chwilowo zawieszać swoją działalność, ukrywając się, co się kilka razy zdarzyło, gdy Gestapo trafiło na ślad mjr. Owoca „Pawła". Wydział organizacyjny sprawował też kontrolę nad Narodową Organizacją Wojskową Kobiet (NOWK), komendantką której była Krystyna Żychowicz „Grażyna". Do czasu powołania oddzielnego Wydziału Młodzieżowego, Wydział Organizacyjny sprawował kontrolę w sprawach wojskowych, nad grupą młodzieży zorganizowanej w SN. Do Wydziału należało

szkolenie wojskowe młodzieży, nabór z jej szeregów żołnierzy NOW, członków grup dywersyjnych i tworzenie na ich bazie oddziałów partyzanckich [9].

Wydział Wywiadu

Wydział Wywiadu był kierowany przez por. Zygmunta Czownickiego „Walek", „Marian". Do Wydziału spływały informacje z komend terenowych. Każdy żołnierz był zobowiązany do meldowania o wszelkich ważnych spostrzeżeniach swoim przełożonym. Informacje te zbierano, segregowano i przesyłane do wydziału szczebla wyższego. Wydział wywiadu zebrane w ten sposób informacje wojskowe przesyłał do odpowiedniej komórki KG NOW. Wydział rozporządzał własną siecią informatorów. Zajmował się również rozpracowywaniem i tropieniem agentów Gestapo przenikających przez cały okres okupacji do środowisk konspiracyjnych, rozpracowujących sztaby komend i żołnierzy NOW. Przykładem tego były masowe aresztowania, które dotknęły organizację w 1940 i 1944 roku. Zbierano też materiały i informacje o osobach współpracujących z Niemcami oraz o takich, które swym zachowaniem narażały na szwank dobre imię Polaka [10].

Wydział Młodzieżowy

Na przełomie roku 1941/1942 Zarząd Główny SN podjął decyzję o wyodrębnieniu z szeregów NOW młodzieży, która do 1939 r. nie odbyła przeszkolenia wojskowego. Powstała ogólnopolska organizacja młodzieżowa o kryptonimie „ Szczerbiec". W 1942 roku w Krakowskim Okręgu NOW „Ugory" z wydziału organizacyjnego wyłoniono Okręgowe Kierownictwo Młodzieży o kryptonimie „Opole", politycznie podporządkowane OK SN. Kierownictwo OKM „Opole" zostało włączone w struktury NOW. Kierownikiem został Zdzisław Skorodecki „ Poremut", „Maciej", „Busecki", zastępcą Jan Szponder „Janusz", „Gradyw", kierownikiem Młodzieży Wielkiej Polski na miasto Kraków Jan Pazoła „Stanisław", kierownikiem wychowania Lech Masłowski „Jerzy", kierownikiem wychowania wojskowego Stanisław Mierzwiński „Michał". Po aresztowaniu Skorodeckiego przez gestapo w listopadzie 1943 roku, nastąpiła kolejna zmiana w kierownictwie OKM „Opole", nowym kierownikiem został Lech Masłowski „Jerzy", jego zastępcą Jan Pazoła „Stanisław" (kierownictwo organizacyjne), kierownikiem Miasta Krakowa i wychowania Kazimierz Szpytman „Przemko", kierownikiem wychowania wojskowego Stanisław Mierzwiński. Jana Szpondera przeniesiono do warszawskiej centrali wydziału młodzieżowego NOW [11].

Działalność grup młodzieżowych nastawiono głównie na poszerzenie bazy członkowskiej, młodzież przechodziła konspiracyjne przeszkolenie wojskowe i ideologiczne według programów nakreślonych przez SN. Polityka ta wkrótce doprowadziła do znacznego powiększenia stanu osobowego NOW. Na terenie prawie każdego powiatu Krakowskiego Okręgu była zorganizowana grupa młodzieżowa w sile, co najmniej plutonu, zaś w powiatach utworzono Powiatowe Kierownictwa Młodzieżowe (PKM). Stan liczbowy grup młodzieżowych

w wymienionych miejscowościach szacowano różnie. Jedni członkowie młodzieżówki krakowskiej podawali 1462 osoby (w 1943r.), podkreślając, że jest to stan przybliżony, co i tak wydaje się być liczbą nieco zawyżoną, inni liczbę 700 osób, co wydaje się bardziej prawdopodobne. Pamiętać należy, że wymienione dane odnośnie liczebności młodzieży w okresie okupacji były podawane przez działaczy młodzieżówki w kilka lat po wojnie, w śledztwie, co może budzić uzasadnione wątpliwości.

Za namową Lecha Hajdukiewicza Jan Pazoła powrócił do Krakowa, obejmując w październiku 1944 roku tylko na jeden dzień kierownictwo wydziału młodzieżowego, gdyż został aresztowany przez Gestapo. Po Janie Pazole „Stanisław" kierownictwa Wydziału Młodzieżowego już nie obsadzano [12].

Wydział Propagandy

Początkowo Wydział Propagandy prowadził Władysław Furka „Emil", który latem 1940 roku zagrożony aresztowaniem przeniósł się do Warszawy. Wobec piętrzących się trudności w budowaniu struktur wojskowych NOW, w pierwszym okresie okupacji całość prac propagandowych spoczywała w rękach działaczy wywodzących się z politycznych komórek stronnictwa. W następnych latach za wydział propagandy odpowiadali: Henryk Grabowski „Ambroży" (od 1942r.), a po nim od 1944 roku Andrzej Gołębiowski „Roman" [13]. Do pracowników wydziału propagandy należeli m.in. Mieczysław Pszon „Długosz", Ryszard Niklewicz. Wydział był wspólny dla pionu politycznego i wojskowego. Kierownik wydziału propagandy był równocześnie członkiem komendy NOW odpowiedniego szczebla. W okresie okupacji wydział propagandy miał do spełnienia bardzo ważną rolę. Prowadził działalność informacyjną i ideowo- wychowawczą przy pomocy odpowiednich komórek w podokręgach i powiatach. Zajmował się drukowaniem i rozsyłaniem prasy konspiracyjnej za pomocą własnej sieci kolportażu. Posiadał również sekcje wykładowców i prelegentów.

Głównym zadaniem propagandy było dbanie o zachowanie patriotycznej postawy społeczeństwa oraz podtrzymywanie wiary w ostateczne zwycięstwo koalicji antyhitlerowskiej. Okręg Krakowski NOW wydawał w pierwszym okresie własne pismo „Pobudka", która w maju 1940 r. zmieniła nazwę na „Surma", drukowane w klasztorze Franciszkanów w Krakowie. Okręg dysponował także innymi tytułami wydawniczymi, m.in: „Na Posterunku", „Front Narodowy", „Znicz Narodowy", „Dziennik Narodowy", „Kierownik", „Obozowiec". Tak znaczny sukces propagandowy nie mógł być zrealizowany bez udziału okręgowego Wydziału Propagandy. Pierwszoplanową rolę pełnił w nim kierownik Wydziału Propagandy Henryk Grabowski. Oprócz szeroko rozwiniętej akcji wydawniczej, okręg posiadał własną sieć kolportażu, który funkcjonował także na obszarze komend powiatowych. Tą drogą z Warszawy dostarczany był główny organ SN i NOW „Walka". W latach 1942-1943, na skutek problemów technicznych oraz okresowych trudności z wydawaniem centralnej „Walki", kierownictwo okręgu

podjęło decyzję o powielaniu w Krakowie „Walki". W zamyśle pomysłodawców „Walka" miała być kolportowana w postaci tygodnika. Krakowska „Walka" zawierała krótki materiał polityczny, informacje frontowe, a czasami także lokalne oraz podziękowania dla ofiarodawców.

Sekcje wykładowców i prelegentów prowadziły w komórkach terenowych NOW szkolenie polityczne. Informowano m.in. o sytuacji na froncie, konfrontując je z celami politycznymi Polski. Rozpowszechniano również w społeczeństwie komunikaty specjalne jak np. „Przepowiednie Wernyhory", mające działać kojąco na społeczeństwo, podtrzymywać na duchu, przywracać wiarę w zwycięstwo [14].

Wydział Kwatermistrzowski

Wydziałem Kwatermistrzowskim kierował mjr „Krystynowicz". Do zadań tego Wydziału należało organizowanie kwater konspiracyjnych, sieci łączności konspiracyjnej oraz zabezpieczanie miejsc odpraw. Biurem Organizacji Kwater Konspiracyjnych oraz działem łączności kierował Władysław Łazarow „Strusiński", „Komar". Był to człowiek cichy, rozważny, doświadczony, a przy tym bardzo ruchliwy w pracy kwatermistrzowskiej, mało wdzięcznej i efektownej, niezastąpiony. W czasie jego działalności nie było żadnego przypadku dekonspiracji kwatery konspiracyjnej, czy miejsca odprawy. Zadanie to było szczególnie trudne w okupowanym kraju, gdy gestapo miało wszędzie swoich konfidentów. Do zabezpieczenia i ochrony miejsc odpraw organizacja wyznaczała specjalne, dobrze wyszkolone i uzbrojone oddziały. Kraków odegrał ważną rolę przy organizowaniu punktów kontaktowych, kwater, „melin" dla kurierów, zapewniających łączność między ZG SN a Bukaresztem. W Krakowie „zabezpieczano" kurierom dokumenty oraz organizowano przerzuty za granicę. O znaczeniu tej działalności niech świadczy fakt, że od 1944 roku szefem łączności organizacyjnej Komendy Okręgu NOW został Jan Szponder „Janusz" przysłany z Warszawy do Krakowa. Podlegały mu łączniczki przewożące prasę, broń, rozkazy i pieniądze. Były nimi m.in.: Wanda Fradera „Simona", Ewa Górka „Malina", Nowak-Przygocka „Jagoda", Maria Grochalska „Maria", Helena Madurowicz „Halina". W większości były to łączniczki przeniesione do Krakowa ze Lwowa [15].

Wydział Sporządzania Dokumentów

Wydział Sporządzania Dokumentów wyodrębnił się z Wydziału Organizacyjnego i podlegał bezpośrednio Komendantowi Okręgu, co świadczyło o wadze, jaką przywiązywano do jego działalności. Biuro Dokumentów zajmowało się wyrabianiem niemieckich dokumentów (Kennkart), metryk urodzenia dla żołnierzy, ukrywających się pod fałszywymi nazwiskami. Wyrabiano też inne dokumenty na żądanie dowództwa okręgu. Komórka ta zajmowała się szyfrowaniem przesyłanej korespondencji konspiracyjnej oraz gromadziła materiały archiwalne. Od 1943 roku Biuro Dokumentów prowadził Bronisław Białek „Mars" po rozbiciu i aresztowaniu członków komórki przez Niemców. W czerwcu 1944 r. przekazał ją Adamowi Fraderze „Radoma". Od chwili przejęcia

Biura Dokumentów od Bronisława Białka Adam Fradera prowadził go samodzielnie podobnie jak Roman Stec, a łącznikami na zewnątrz byli Bronisław Białek i jego żona Kamila „Małgorzata". W tym okresie biuro ściśle współpracowało z Biurem Dokumentacji AK i jemu też podlegało. Kierował nim wówczas Zbigniew Melanowski „Sokół". Wszystkie rozkazy, awanse, dokumenty, pisma przychodzące i wychodzące przechodziły przez kancelarię Komendy Okręgu Krakowskiego NOW prowadzoną wówczas przez Romana Steca „Gruby" [16].

3. Struktura Okręgu Krakowskiego Narodowej Organizacji Wojskowej

Okręg Krakowski NOW obejmował swym zasięgiem okrojone przedwojenne trzy województwa tj. województwo krakowskie, województwo lwowskie i powiat miechowski z województwa kieleckiego. Z województwa krakowskiego odłączono jego zachodnie powiaty tj. Żywiec, Biała oraz część powiatów tj. Maków, Wadowice, Oświęcim, Chrzanów, które zostały wcielone bezpośrednio do III Rzeszy. Natomiast z województwa lwowskiego odłączono powiaty wschodnie znajdujące się na prawym brzegu Sanu wraz z miastem Lwów. Powiaty te znalazły się pod okupacją radziecką do czerwca 1941 r., później przeszły pod okupację niemiecką i zostały włączone do Generalnego Gubernatorstwa (GG) z siedzibą w Krakowie.

W skład Okręgu Krakowskiego NOW wchodziło 21 powiatów według przedwojennej administracji, leżących w granicach: od Górnego Śląska na zachodzie po rzekę San na wschodzie. Ze względu na dużą ilość powiatów zorganizowanych w tym okręgu, cały teren krakowskiego okręgu NOW został podzielony na pięć podokręgów:

- Kraków – Miasto („Krajewski")-komendanci: mjr Szwed „Horawski", kpt/mjr Adam Stabrawa „Jur", „Szałas", „Borowy" , por./kpt Józef Krauze – Przedrzymirski „Sokół",
- Kraków – Zewnętrzny-Podkrakowski („Limba")-komendanci: kpt/mjr Teofil Trnka „Ryszard", „Śliwiński", por. Władysław Gałka „Lis", „Wiktor"
- Tarnów („Cis", „Sankta Maria")-komendant kpt/mjr Eugeniusz Antoni Borowski „Jastrzębiec", „Werner", „Leliwa",
- Podhale („Smrek")-komendant kpt/mjr Adam Stabrawa „Borowy",
- Krosno „Grab" „Podkarpacie"-komendant kpt/mjr Józef Drelichowski „Hen", „Czortyński", „Zwit" [17].

Podokręgami kierowały komendy podokręgów zorganizowane na wzór komendy okręgu. Podokręgi dzieliły się na powiaty, a te z kolei na obwody, opierające się na strukturze gminy wiejskiej lub miejskiej. W przypadku gminy wiejskiej obejmowały one kilka, a niekiedy kilkanaście wsi. Najmniejszą jednostką organizacyjną w strukturze NOW była na szczeblu wsi placówka.

Żołnierze Narodowej Organizacji Wojskowej w okręgu krakowskim w tym i w Krakowie zorganizowani byli w pięcioosobowe sekcje. Dwie sekcje tworzyły drużynę, dwie drużyny pluton. Wyższą komórką organizacyjną była kompania, która składała się z dwóch lub trzech plutonów. Ponieważ NOW nie posiadała w swoich szeregach znacznej liczby oficerów zawodowych, na dowódców wymienionych jednostek organizacyjnych byli wyznaczani podoficerowie, podchorążowie oraz nieliczni młodsi oficerowie zawodowi lub rezerwy, przeważnie uczestnicy kampanii wrześniowej 1939 r. Jak wiemy Narodowa Organizacja Wojskowa odczuwała brak w swoich szeregach oficerów starszych, których można by wyznaczyć do kierowania większymi jednostkami wojskowymi, dlatego nie organizowała jednostek większych niż kompania czy baon. Organizowaniem i kierowaniem większymi jednostkami wojskowymi miały zająć się komendy podokręgów i okręgów oraz Komenda Główna NOW. W wyniku akcji scaleniowej z Armią Krajową, tworzenie większych jednostek organizacyjnych NOW stało się nieaktualne. Poszczególne plutony czy kompanie NOW, mimo zachowania odrębności organizacyjnej, weszły jednak w skład większych struktur organizacyjnych AK takich jak pułki, brygady czy dywizje.

W każdym powiecie NOW zorganizowała od 2 do 4 plutonów o strukturze szkieletowej. Zorganizowane oddziały posiadały obsadzone stanowiska dowódcze do drużynowych lub sekcyjnych włącznie. Poszczególne drużyny nie liczyły więcej niż 3–4 żołnierzy. Dowódcy poszczególnych drużyn znali przyszłych żołnierzy i utrzymywali ich w zasięgu swoich wpływów. W przypadku ogłoszenia stanu pełnej gotowości bojowej składy drużyn miały być uzupełniane żołnierzami, z góry uprzednio upatrzonymi, ale początkowo niewłączonymi do konspiracji. Przysięgę mieli oni składać dopiero w chwili wcielania do oddziałów NOW [18].

W miarę rozbudowy struktury organizacyjnej NOW od 1942 r. zaczęto tworzyć grupy dywersyjno-sabotażowe. Grupy te tworzyli dowódcy terenowych jednostek organizacyjnych, którzy kierowali działalnością tych grup w terenie. W początkowym okresie głównym zadaniem grup dywersyjno-sabotażowych było prowadzenie akcji sabotażowych oraz zdobywanie broni palnej, umożliwiającej podejmowanie coraz śmielszych akcji zmierzających do utrudniania życia okupantowi. Umożliwiało to również podjęcie akcji zbrojnych, w ramach samoobrony, wobec poczynań represyjnych okupanta w stosunku do ludności polskiej. Oprócz akcji skierowanych przeciwko okupantowi prowadzono akcje porządkowe takie jak: niszczenie bimbrowni, likwidacja konfidentów, pospolitych złodziei i rabusiów, strzyżenie kobiet sympatyzujących z Niemcami, kary chłosty za wysługiwanie się Niemcom czy ograniczanie hucznych zabaw i pijaństwa podczas wiejskich wesel. Grupy te działały początkowa każda na swoim terenie i zbierały się tylko dla przeprowadzenia akcji lub szkolenia.

Autorowi nie udało się jednoznacznie określić stanu liczbowego sieci konspiracyjnej Krakowskiego Okręgu Narodowej Organizacji Wojskowej w czasie

jego największego rozkwitu tj. w okresie scalenia z AK. Jedni badacze dziejów NOW szacują stan liczbowy na 10000 żołnierzy, drudzy na 7000-8000, inni na 6000-7000, a jeszcze inni na 4000 żołnierzy. Zdaniem autora NOW w Okręgu Krakowskim scaliła z AK około 4000 żołnierzy.

Po scaleniu w miejsce poszczególnych komend SN utworzyło Wydziały Wojskowe, które z żołnierzy NOW niewcielonych do AK zaczęły organizować Obozowe Drużyny Bojowe (ODB). Oddziały te działały niezależnie od AK i podlegały tylko wyznaczonym komórkom SN. Zadaniem ODB było: w czasie okupacji – ochrona działalności SN, prowadzenie antyniemieckich akcji dywersyjnych oraz prowadzenie akcji porządkowych wobec społeczeństwa polskiego, w czasie ustępowania okupanta niemieckiego z ziem polskich – przeciwstawienie się próbom zdobycia władzy przez ugrupowania lewicowe, a zwłaszcza komunistom popieranym przez ZSRR. W powiecie miechowskim jeden posterunek w sile 10 ludzi tworzono na trzy wsie [19].

Niektóre Obozowe Drużyny Bojowe pod koniec 1944 r. zostały podporządkowane Armii Krajowej, jak w powiecie bocheńskim. Inne działały samodzielnie i do końca wojny były podlegały SN pod względem wojskowym i politycznym.

4. Zakończenie

Reasumując, Narodowa Organizacja Wojskowa w Okręgu Krakowskim w okresie II wojny światowej czynnie uczestniczyła w walce zbrojnej z okupantem niemieckim. Większość żołnierzy NOW nie była działaczami partyjnymi, a ich głównym celem nie była walka o władzę, lecz walka z okupantem aż do ostatecznego zwycięstwa. Za działalność konspiracyjną i trudy życia w konspiracji żołnierze NOW nie doczekali się w PRL uznania, awansów, czy odznaczeń. Wręcz przeciwnie, za swą przynależność do NOW dostawali się do więzień UBP lub byli aresztowani przez NKWD i wywożeni do łagrów na terenie ZSRR. Duża liczba żołnierzy NOW, chroniąc się przed aresztowaniem, opuściła potajemnie kraj udając się na przymusową emigrację (ppłk Owoc, mjr Stabrawa por. Rafalski). Wielu innych aresztowano i skazano w wyreżyserowanych procesach (Gołuński, Gałka, Pajdak), toczonych przed Wojskowymi Sądami Rejonowymi. Część z nich, zmieniła miejsca zamieszkania i nazwiska. Żołnierze NOW odpowiedzialni za prowadzenie dokumentacji poszczególnych oddziałów i sztabów, by uchronić siebie i kolegów, zniszczyli istniejące materiały archiwalne. Przez cały okres PRL-u żołnierze NOW byli żołnierzami niezłomnymi, nie wolno było pisać na ich temat, a jeżeli już, to tylko w czarno-białej optyce. Nie mogli też ze względów bezpieczeństwa przyznawać się do przynależności do NOW. Najczęściej podawali, że byli żołnierzami AK.

Autor dostrzega potrzebę dalszych badań nad NOW, powstania syntetycznej pracy obejmującej całokształt działalności wojskowej Narodowej Organizacji Wojskowej w Okręgu Krakowskim w okresie okupacji hitlerowskiej.

Przypisy

[1] W. Jaworski, *Stronnictwo Narodowe w czasie wojny 1939-1945*, sygn. III-68-4, Archiwum Wojskowego Instytutu Historycznego w Warszawie (dalej: WIH), s. 6-11, 19-20; *Krakowski Okręg Stronnictwa Narodowego w czasie wojny 1939-1945,* tom 5, 075/30, Instytut Pamięci Narodowej Oddział w Krakowie (dalej: IPNKr), s. 40-42; S. Rymar, *Pamiętniki,* cz. III, *Wojna i okupacja*, s. 148; J. J. Terej, *Rzeczywistość i polityka. Ze studiów nad dziejami najnowszymi Narodowej Demokracji*, Warszawa 1979, s. 116-120, 156-157; Endecja w latach 1887-1945, Legionowo 1960, s.71-72; J. Rokicki, *Blaski i cienie bohaterskiego pięciolecia*, Niemcy Zachodnie, 1949, s. 20-21; K. Komorowski, *Polityka i walka. Konspiracja zbrojna ruchu narodowego 1939-1945*, Warszawa 2000, s. 75-108.

[2] Pod koniec 1939 r. do Krakowa powrócili płk Tadeusz Wołkowicki i Wincenty Ogrodziński dzięki czemu udało się powołać Zarząd Okręgowy SN w składzie: Tadeusz Wołkowicki ps. „ Hipolit", p.o. prezesa, dr Stanisław Nowogrodzki – kierownik organizacyjny, Władysław Furka – kierownik wydziału propagandy i Tadeusz Surzycki – skarbnik, J. J. Terej, *Rzeczywistość i polityka*.., s. 151-152. Przed wybuchem wojny ilość kół SN w okręgu przekraczała liczbę 280, zaś liczbą członków przekraczała znacznie 12 tys. osób, *Krakowski Okręg Stronnictwa Narodowego*.., tom 5, 075/30, IPNKr, s. 39.

[3] *Krakowski Okręg SN*.., IPNKr, s. 44-45; Jaworski, *Stronnictwo Narodowe w czasie wojny 1939-1945* .., s. 20; J. Szczeklik, *Zarys historyczny Narodowej Organizacji Wojskowej Podokręgu Tarnowskiego.* Pilzno 1994, mps, s. 8; S. Gałka, *Narodowa Organizacja Wojskowa (NOW) w szeregach Armii Krajowej obwodu Bochnia,* Kraków 1993r., mps, s. 4; J. Guzik, *Racławickie wezwania. Monografia okupacyjna ziemi miechowskiej 1939-1945*, Wawrzeńczyce 1987, s. 65-66; G. Mazur, W. Rojek, *Inspektorat Nowosądecki AK*, Relacja mjr Adama Stabrawy, „Wojskowy Przegląd Historyczny" , 1996 nr 1, s. 116-120.

[4] Nie udało się ustalić nazwiska wspomnianego pułkownika. Niektórzy autorzy podają, że nosił czeskie nazwisko. Nie był to na pewno ani płk Adam Epler, zob. J. J. Terej, *Rzeczywistość i polityka*.., s. 158, ani płk Euzebiusz Hauser, którego nazwisko w rozmowie z autorem wymieniali kilkakrotnie działacze z OK NOW. Płk Hauser w swoich zeznaniach nigdy nie podawał, że pełnił taką funkcję.

[5] Krakowski Okręg SN.., , s.49; Terej, *Rzeczywistość*..,s.158; W. Owoc, *Krakowska Narodowa Organizacja Wojskowa, wojna i okupacja.* Paryż 1977, s. 17-18; K. Komorowski, *Konspiracja Wojskowa Obozu Narodowego 1939-1945*, „Wojskowy Przegląd Historyczny" nr 1, 1988 r., s. 53; Jaworski podaje, że zawodowy pułkownik nosił czeskie nazwisko. W. Żychowicz twierdził natomiast, że mógł to być pułkownik Adam Epler, który nawiązał kontakty z dr Tadeuszem Surzyckim, z ramienia SN zajmującym się sprawami wojska, zob. J. J. Terej,

Rzeczywistość..,. s. 157-158; W. Żychowicz, *Przemówienie nad grobem Władysława Kosturka w dniu 15 V 1991r*., mps, s. 1.
[6] *Schemat Okręgu Krakowskiego Narodowej Organizacji Wojskowej 1939-1945*, sygn. 45/0, IPNKr; *Krakowski Okręg SN*.., IPNKr, s. 55-56; *Niepublikowane wspomnienia płk Rokickiego*..,s. 11.
[7] Owoc, *Krakowska NOW..,* . s. 17-19; Rokicki, *Blaski i cienie*.., s. 21.
[8] *Inspektorat Nowosądecki AK. Relacja mjr Stabrawy*,s. 119-120; *Niepublikowane wspomnienia płk Rokickiego*..,s. 12.
[9] W. Gołuński, *Narodowa Organizacja Wojskowa w Okręgu Krakowskim*, b.r.w, mps, s. 2; Stronczak, *Wojskowa Sieć Konspiracyjna SN*.., s. 89; Gałka, *NOW*.., s. 58-59.
[10] Gołuński, *NOW w Okręgu Krakowskim*.., s. 4.
[11] J. Pazoła „Stanisław", *Zarys historyczny działalności grup młodzieżowych NOW na terenie K.O „Opole"*, mps, s. 1-2; A. Stonczak, *PRO MEMORIA Oddziału Partyzanckiego „Szczerbiec*". Kraków 1996 , s. 38; *Analiza sprawy ewidencyjno-obserwacyjnej nr 14 z 9 IV 1957*, 08/418, Instytut Pamięci Narodowej Oddział w Poznaniu (dalej IPNP), s. 4/42, 5/42; *Protokół przesłuchania Mierzwińskiego Stanisława „Michał" w dniu 28 I 1948 r. przez oficera MBP w Warszawie kpt. Łyszkowskiego Stanisława*,08/418, IPNPo, s. 18/42, 19/42; *Protokół przesłuchania Pazoły Jana w WUBP w Poznaniu w dniu 13 I 1949*, 08/418, IPNPo, s. 22/42, 23/42; *Materiały do dziejów SN w latach 1939-1948*, 7821, Polska Akademia Nauk w Krakowie, s. 95.
[12] *Protokół przesłuchania Mierzwińskiego Stanisława „Michał"*.., 08/418, IPNPo, s. 18/42; *Protokół przesłuchania podejrzanego Padoły Jana 25 I 1949 roku w MBP przez ST. Ref. Wydz.II Dep. III Matejewskiego Ryszarda*, 08/418, IPNPo, 34/42, 35/42, 36/42.
[13] L. Kulińska, Związek Akademicki „Młodzież Wszechpolska" i „Młodzież Wielkiej Polski" w latach 1922-47 (struktury, funkcjonowanie i główni działacze), Kraków 2000, s.68; M. Orłowski, Prasa narodowców w okręgu krakowskim w okresie okupacji, mps, s. 1-8.
[14] *Krakowski Okręg SN*.., ,s. 56; *Schemat OK NOW*.., 45/0, s. 5-8; Gołuński *NOW OK*.., s. 3-4; M. Orłowski, *Prasa narodowców w okręgu krakowskim.*
[15] Gołuński, NOW OK.., s. 2-3; *Niepublikowane wspomnienia płk Rokickiego*..,s.14; Relacja ustna otrzymana od W. Fradery w dniu 6 V 1992r.; Gałka, *NOW w szeregach AK*.., s. 2-3.
[16] Gołuński, *NOW OK*.., s. 2,4-6; Jaworski, *Stronnictwo Narodowe w czasie wojny..,* s. 59; Relacja pisemna R. Steca, z 2.04.1992r., s.1-2; Relacja ustna A. Fradery z dnia 6 V 1992r.
[17] Owoc, *Krakowska NOW*.., s.18-19; Stronczak, *Wojskowa Sieć*.., s. 90-93; Podokręgi: Krakowski i Podhalański organizował Tadeusz Migas „Silnicki".

[18] Maur, Rojek, *Inspektorat Nowosądecki AK. Relacja mjr Adama Stabrawy.,* s. 118-119; Gołuński, NOW AK.., 6-7; A. Stronczak, *Narodowa Organizacja Wojskowa Okręg Kraków „Ugory". Podokręg Kraków Zewnętrzny „Limba", powiat Bochnia.* Kraków 1990, s. 10.
[19] Stronczak, *NOW OK..,* s. 9-10; A, Fitowa, *Bataliony Chłopskie w Małopolsce 1939-1945 – działalność organizacyjna, polityczna i zbrojna*. Warszawa 1984, s. 254; Owoc, *Krakowska NOW*.., s.38; Komorowski, *Konspiracja wojskowa obozu narodowego 1939-1945*.., s. 72.

Bibliografia

AK Okręg Krakowski krypt. „Akademia", tom 32-33, 075/18, Instytutu Pamięci Narodowej Oddział w Krakowie.

Analiza sprawy ewidencyjno-obserwacyjnej nr 14 z 9 IV 1957, 08/418, Instytut Pamięci Narodowej Oddział w Poznaniu.

Część opisowa do raportu statystycznego S.IV za okres miesiąca kwietnia 1951 r., tom 27, 056/1, Instytutu Pamięci Narodowej Oddział w Krakowie.

Daszkiewicz (1975), *Ruch oporu w rejonie Beskidu Niskiego 1939-1944*, Warszawa.

Endecja w latach 1887-1945 (1960). Legionowo.

Fitowa, A. (1984) *Bataliony Chłopskie w Małopolsce 1939-1945 – działalność organizacyjna, polityczna i zbrojna*. Warszawa.

Fitowa, A. (1961) *Bataliony Chłopskie*. „Wojskowy Przegląd Historyczny" nr 1.

Grzywacz-Świtalski, Ł. (1971) *Z walk na Podkarpaciu*. Warszawa .

Guzik, J. (1987) *Racławickie wezwania. Monografia okupacyjna ziemi miechowskiej 1939-1945*. Wawrzeńczyce: Związek Bojowników o Wolność i Demokrację. Koło Gminne.

Jan Gomoła, tom 1, 07/3199 , Instytutu Pamięci Narodowej Oddział w Krakowie.

Jan Pazoła, 075/28, paczka 121, tom 38, Instytutu Pamięci Narodowej Oddział w Krakowie.

Jaworski, W. *Stronnictwo Narodowe w czasie wojny 1939-1945*, sygn. III-68-4, Archiwum Wojskowego Instytutu Historycznego Akademii Obrony Narodowej w Warszawie.

Karczmarski, K. (2003) *Podziemie Narodowe na Rzeszowszczyźnie 1939-1944*, Rzeszów.

Komorowski, K. (1988) *Konspiracja Wojskowa Obozu Narodowego 1939-1945*. „Wojskowy Przegląd Historyczny" nr 1.

Komorowski, K. (2000) *Polityka i walka. Konspiracja zbrojna ruchu narodowego 1939-1945*. Warszawa.

Krakowski Okręg Stronnictwa Narodowego w czasie wojny 1939-1945, tom 5, 075/30, Instytutu Pamięci Narodowej Oddział w Krakowie.

Kraków czas okupacji 1939-1945 (2012). Kraków.

Kulińska, L. (2000) *Związek Akademicki „Młodzież Wszechpolska" i „Młodzież Wielkiej Polski" w latach 1922-47 (struktury, funkcjonowanie i główni działacze)*. Kraków.

List Krystyny Brzeskiej-Mastalskiej (1989). „Pod Prąd" Miesięcznik młodzieży szkół średnich, nr 5/6 (12-13).

Mazur, G., Rojek, W. (1996) *Inspektorat Nowosądecki AK,, Relacja mjr Adama Stabrawy*. „Wojskowy Przegląd Historyczny" nr 1.

Mazur, G., Rojek ,W., Zgórniak, M. (1998) *Wojna i okupacja na Podkarpaciu i Podhalu na obszarze Inspektoratu ZWZ-AK Nowy Sącz.* Kraków.

Owoc, W. (1977) *Krakowska Narodowa Organizacja Wojskowa, wojna i okupacja*. Paryż.

Pantera-Boczoń Władysław/Jacet/, 01251/89, Archiwum Instytutu Pamięci Narodowej w Warszawie.

Pazoła, J. „Stanisław" *Zarys historyczny działalności grup młodzieżowych NOW na terenie K.O „Opole".* Instytutu Pamięci Narodowej Oddział w Krakowie.

Protokoły przesłuchań członków NOW-Gomoła Jan, tom 28, paczka 120, 075/28.

Protokół przesłuchania Boczonia Władysława „Pantera" , MBP Warszawa 28 IX 1950 r., tom 2, 010/6 ,Archiwum Instytutu Pamięci Narodowej w Warszawie.

Protokół przesłuchania Mierzwińskiego Stanisława „Michał" w dniu 28 I Instytut Pamięci Narodowej Oddział w Poznaniu.

Protokół przesłuchania Pazoły Jana w WUBP w Poznaniu w dniu 13 I 1949, 08/418, Instytut Pamięci Narodowej Oddział w Poznaniu.

Protokół przesłuchania Mierzwińskiego Stanisława „Michał" w dniu 28 I 1948r. przez oficera MBP w Warszawie kpt. Łyszkowskiego Stanisława,08/418 Instytut Pamięci Narodowej Oddział w Poznaniu.

Protokół przesłuchania podejrzanego Padoły Jana 25 I 1949 roku w MBP przez ST. Ref. Wydz.II Dep. III Matejewskiego Ryszarda, 08/418, Instytut Pamięci Narodowej Oddział w Poznaniu.

Rokicki, J. (1949) *Blaski i cienie bohaterskiego pięciolecia*. Niemcy Zachodnie.

Schemat Okręgu Krakowskiego Narodowej Organizacji Wojskowej 1939-1945, sygn. 45/0, Instytutu Pamięci Narodowej Oddział w Krakowie.

Terej, J. J. (1979) *Rzeczywistość i polityka. Ze studiów nad dziejami najnowszymi Narodowej Demokracji*. Warszawa.

Ważniewski, W. (1969) *Walki partyzanckie nad Nidą 1939-1945.* MON.

Zespół KW PZPR-zbiory –„Godło" do „Rzemiosła" z dnia 25 XI 1943r, sygn.270, Archiwum Narodowe w Rzeszowie.

Streszczenie

Artykuł podejmuje problem powstania Narodowej Organizacji Wojskowej w Krakowie i formowanie się jej struktury w latach 1939-1945. Ukazuje zakres zadań wydziałów działających w ramach Komendy OK NOW i ich obsadę personalną.

Słowa kluczowe: Narodowa Organizacja Wojskowa, Kraków, struktura NOW, formy pracy wydziałów NOW, Armia Krajowa, historia wojskowości

Structure of National Military Organization in Cracow and forms of its departments' work

Abstract

The article presents the history of the creation of the National Military Organization in Cracow and the formation of its structure in 1939-1945. The article also include description of the Headquarters of the National Military Organization in Cracow, its departments' work and personnel.

Keywords: National Military Organization, Cracow, NMO's structure, work of the NMO's departments, Home Army, military history

Cykl monografii naukowych pt.: CZŁOWIEK W ŚWIECIE INFORMACJI zaplanowany został z myślą o podjęciu wspólnej refleksji nad kondycją człowieka w świecie nadmiarowości informacji i traktowania jej jako zasobu strategicznego oraz narzędzia walki informacyjnej. Przedstawiona „problematyka walki informacyjnej jest obecnie przedmiotem szczególnego zainteresowania. Wynika to z dynamicznego rozwoju systemów informacyjnych (informatycznych) i oplatającej glob sieci Internetu. Znaczenie informacji, w różnych jej formach i zakresach, dotyczy także kwestii bezpieczeństwa, obronności i edukacji obywatelskiej. Generuje to stosowne zapotrzebowanie badawcze wyjaśniające istotę tego zjawiska społecznego [...] Przedmiotowa monografia wnosi wartości teoretyczne, zwłaszcza do dyscypliny nauk o bezpieczeństwie, w zakresie związanym z walką informacyjną. Opisuje też zmienność uwarunkowań jako pewnego tła funkcjonalnego obecności tej specyficznej odmiany walki. Wskazuje też na pojawiające się wyzwania wynikające z opisu zagadnień związanych z walka informacyjną".

(z recenzji prof. zw. dr. hab. Michała Huzarskiego)

ISBN 978-83-8084-049- 2