ISSN 0867-2245

AKADEMIA OBRONY NARODOWEJ

ZESZYTY NAUKOWE

KWARTALNIK
nr 2(99)

Warszawa 2015

AKADEMIA OBRONY NARODOWEJ

ZESZYTY NAUKOWE

KWARTALNIK
nr 2(99)

WARSZAWA 2015

Adres redakcji: 00-910 Warszawa 72
al. gen. Antoniego Chruściela 103, bl. 4
tel./fax: 261-813-516
e-mail: zn@aon.edu.pl

„Zeszyty Naukowe Akademii Obrony Narodowej" są indeksowane w międzynarodowej bazie Index Copernicus Master List.

Nakładem Akademii Obrony Narodowej

Skład, druk i oprawa: Wydawnictwo Akademii Obrony Narodowej, zam. nr 1309/2015, nakład 150 egz.

SPIS TREŚCI

BEZPIECZEŃSTWO NARODOWE
NATIONAL SECURITY

SZTUKA WOJENNA
ART OF WAR

EKONOMIA BEZPIECZEŃSTWA I LOGISTYKA
ECONOMY OF SECURITY AND LOGISTICS

KSZTAŁCENIE I PRZYGOTOWANIE ZAWODOWE
VOCATIONAL TRAINING AND PREPARATION

KOMUNIKATY, KOMENTARZE, RECENZJE I SPRAWOZDANIA
COMMUNICATIONS, COMMENTS, REVIEWS AND REPORTS

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

BEZPIECZEŃSTWO NARODOWE

TEORIA I PRAKTYKA DZIAŁAŃ HYBRYDOWYCH

dr inż. Mirosław BANASIK
Akademia Obrony Narodowej

dr inż. Ryszard PARAFIANOWICZ
Centrum Operacyjne Ministra Obrony Narodowej

Streszczenie

Artykuł jest poświęcony teorii i praktyce działań hybrydowych, które wpływają na bezpieczeństwo środowiska międzynarodowego. Wyniki analiz odniesiono do problemu zdefiniowanego w formie pytań: w czym wyraża się istota i ewolucja działań hybrydowych? Jaki jest charakter współczesnych działań hybrydowych? Przedstawione w artykule argumenty uzasadniają podejmowanie badań nad działaniami hybrydowymi, które stosowane przez podmioty państwowe bądź organizacje niepaństwowe, w swoim wymiarze stanowią realne zagrożenie dla bezpieczeństwa w Europie i na świecie. Współczesna praktyka działań hybrydowych, m.in. w konflikcie zbrojnym na Ukrainie, uwidoczniła, że nastąpiła diametralna zmiana strony stosującej działania hybrydowe. Po raz pierwszy to przeciwnik zdecydowanie silniejszy, mocarstwo światowego formatu – Rosja, wykorzystuje pełne spektrum oddziaływania hybrydowego na przeciwnika słabego i niezdolnego do obrony integralności własnego terytorium.

Słowa kluczowe: bezpieczeństwo, wojna hybrydowa, terroryzm, Rosja, Ukraina.

Wprowadzenie

Początek XXI wieku charakteryzuje się nowymi wyzwaniami w obszarze bezpieczeństwa międzynarodowego. Powszechna jest opinia, że zakończenie zimnej wojny nie oznaczało wyeliminowania wewnętrznych lub regionalnych źródeł konfliktu i nie zapewniło trwałego pokoju na świecie. Jak oceniają eksperci, społeczność międzynarodowa stoi w obliczu nie tyle bezpośredniego konfliktu zbrojnego, ile jednej z odmian działań militarnych. Powstania zbrojne, działania partyzanckie, wojny wewnętrzne i inne odmiany konfliktów o małej skali wkrótce staną się powszechnymi odmianami konfliktu w nowym porządku świata. Dlatego można założyć, że w najbliższym czasie różne państwa zostaną uwikłane, bezpośrednio lub pośrednio, w nowe odmiany konfliktów zbrojnych[1]. Doświadczenia wielu państw wyniesione z walk z przeciwnikiem nieokreślonym, pozbawionym jasnych struktur organizacyjnych i niestosującym standardowej taktyki nadają innego wymiaru postrzeganiu prowadzenia działań zbrojnych. Pewne wydaje się, że podważony został paradygmat bezpieczeństwa oparty na kluczowym znaczeniu technologii w organizacji systemów obronnych państw, a także sposobów prowadzenia działań zbrojnych[2]. Od kilku lat we współczesnych publikacjach z zakresu nauk o bezpieczeństwie coraz szerzej podejmowany jest problem asymetryczności i hybrydowości współczesnych konfliktów zbrojnych. Kwestie związane z tą problematyką zaczynają stanowić osnowę myślenia strategicznego. W wielu armiach świata przeprowadza się na poziomie strategicznym analizy i studia doświadczeń zdobytych zarówno w małych lokalnych konfliktach zaistniałych w przeszłości, jak i w wielonarodowych operacjach początku XXI wieku[3]. Próby poszukiwania nowych koncepcji

[1] M. Wrzosek, *Zagrożenia militarne a bezpieczeństwo Europy* [w:] Kwartalnik Bellona 2012, nr 4, s. 7.

[2] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011, s. 4.

[3] B. Balcerowicz, *Pokój i nie pokój na progu XXI wieku*, Wyd. Bellona, Warszawa 2002, s. 17.

utrzymania równowagi bezpieczeństwa międzynarodowego podyktowane są coraz większym rozdźwiękiem między ideami okresu po zimnej wojnie a obecną praktyką polityki bezpieczeństwa wielu państw. Zasadniczym problemem, jak się wydaje, jest niemożność przezwyciężenia stagnacji, w jakiej znalazła się współczesna sztuka wojenna na skutek rosnącej złożoności konfliktów oraz sposobów i metod ich rozstrzygania[4]. To jest konfliktów zbrojnych o takim charakterze, gdzie elementami decydującymi o końcowym sukcesie nie są ani wyższość technologiczna, ani doskonałość organizacyjna, ani przewaga psychologiczna. Precyzyjne przewidywanie przyszłości, a szczególnie konfliktów zbrojnych, jest niezwykle trudne ze względu na rozwijającą się dynamikę działań i nieprzewidywalność reakcji stron konfliktu. Wpisuje się to w starą maksymę, że „(...) wojna obfituje w namiętności, niedokładne informacje i błędy oceny, wreszcie wiele dzieje się w niej za sprawą przypadku"[5]. Niemniej na podstawie występujących trendów można sformułować tezę, że o dominację we współczesnym świecie będą walczyć różnorodne podmioty. Narastać będzie liczba miejsc, w których będą mogły wystąpić konflikty zbrojne. Nastąpi zwiększenie zagrożenia dla bezpieczeństwa i interesów państw Sojuszu Północnoatlantyckiego i państw pretendujących do członkostwa w nim.

Przedstawione argumenty uzasadniają podjęcie badań nad działaniami hybrydowymi, które stosowane przez podmioty państwowe bądź niepaństwowe, w swoim wymiarze stanowią realne zagrożenie dla bezpieczeństwa w Europie i na świecie.

Artykuł jest poświęcony teorii i praktyce działań hybrydowych, które wpływają na bezpieczeństwo środowiska międzynarodowego. Wyniki analiz odniesiono do problemu zdefiniowanego w formie pytań: w czym wyraża się istota i ewolucja działań hybrydowych? Jaki jest charakter współczesnych działań hybrydowych?

Istota i ewolucja działań hybrydowych

Etymologia terminu „hybrydowość" wywodzi się z łacińskiego słowa *hybryda*, oznaczającego „mieszańca", osobnika powstałego ze skrzyżowania dwóch genetycznie różnych osobników, należących do różnych gatunków, odmian czy ras[6]. W innym ujęciu „hybrydowość" można zdefiniować, jako „...właściwość powstałą w wyniku skrzyżowania lub zmieszania cech, elementów należących do różnych, często odmiennych strukturalnie i odległych genetycznie, przeciwstawnych przedmiotów, organizmów lub stanów. Hybrydyzacja oznacza więc scalenie odmiennych istotowo cech wokół jednego, odrębnego bytu, przy zachowaniu specyficznych własności gatunkowych decydujących o „wyższości" nowego, hybrydowego organizmu pod względem np. odporności na choroby, wytrzymałości czy większych zdolności adaptacyjnych"[7]. W najprostszym ujęciu *hybryda* jest połączeniem elementów o różnym pochodzeniu i/lub strukturze. W przypadku konfliktów czy wojen hybrydowych stanowią one swoistą mieszankę najskuteczniejszych form i metod prowadzenia działań.

Konflikt hybrydowy, jako swoista kombinacja działań konwencjonalnych i nieregularnych, znany jest od wieków. Od starożytności jednym z głównych wyznaczników prowadzenia działań militarnych było prawidłowe rozpoznanie bieżącej sytuacji i dostosowanie do niej swoich działań[8]. Istotne jest to, że przy niezmiennej naturze wojny, sposoby i metody jej prowadzenia, a także zwyciężania uległy zasadniczym przeobrażeniom[9]. Współczesne siły zbrojne muszą mierzyć się z nowymi wyzwaniami, ryzykiem i zagrożeniami, w tym o charakterze asymetrycznym. Działania hybrydowe mogą być kombinacją wybranych form działań wojny symetrycznej[10]

[4] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna* [w:] Asymetria i hybrydowość – stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011, s.11.

[5] C. Clausewitz, *O wojnie,* Lublin 1995, s. 15. *Wojna jest* [...] *aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli.* Sformułowanie to zawiera dwa istotne aspekty. Po pierwsze, wojna zakłada przemoc, co odróżnia ją od innych form rywalizacji politycznej czy gospodarczej. Po drugie jest narzędziem służącym do osiągnięcia **celu politycznego**, dalszym ciągiem stosunków politycznych kontynuowanych innymi środkami.

[6] *Słownik wyrazów obcych,* PWN, Warszawa 1980, s. 290.

[7] A. Gruszczak, *Hybrydowość współczesnych wojen* (...), s. 11.

[8] Sun Tzu, *Sztuka wojny*, Gliwice 2004.

[9] J. Keegan, *Historia wojen,* Warszawa 1998, s. 11.

[10] „Asymetria" i „asymetryczność" są pojęciami określającymi różnorodne formy dysproporcji, zróżnicowania i dysharmonii, które w sposób naturalny lub zamierzony występują w otoczeniu przeciwstawnych sobie rzeczywistości. Dotyczą one zarówno ich sfery materialnej, to jest gospodarczej, ekonomicznej, naukowej, technicznej, informacyjnej i militarnej, jak również sfery duchowej – obejmującej aspekty kulturowe, religijne czy etyczne. Wzajemna symetryczność czynników (...) minimalizuje możliwość generowania zagrożeń oraz stabilizuje względnie trwałą równowagę ich zmian. Oznacza to, że „asymetryczność" jest antonimem stanu „symetrycznej" równowagi, odnoszącej się do całokształtu zjawisk spo-

i asymetrycznej[11], w której działające siły prowadzą klasyczne operacje wojskowe, a jednocześnie muszą równolegle podejmować zdecydowane próby zdobycia kontroli nad miejscową ludnością w strefie działań bojowych, poprzez zapewnienie bezpieczeństwa i stabilności[12]. W chwili obecnej środowisko międzynarodowe staje przed nowym wyzwaniem, jakim jest przeciwdziałanie zagrożeniu wypływającemu z ewentualnego konfliktu hybrydowego. Wymaga to nowego, bardziej szczegółowego i kompleksowego podejścia. Jednowymiarowy, terytorialny obraz wojny zastąpiony został wielowymiarowym, wielopoziomowym kompleksem działań militarnych i pozamilitarnych służących jednoczesnemu osiąganiu zróżnicowanych celów. Tradycyjne pole bitwy zostało zastąpione przestrzenią konfrontacji militarnej. Role wypełniane przez uczestników konfliktu zbrojnego nie są zdefiniowane i przypisane na stałe, często się zmieniają i to w sposób radykalny, powodując, że wysiłki zmierzające do pacyfikacji/stabilizacji lub destabilizacji przestrzeni publicznej ulegają rozproszeniu. Obecnie występujące trendy, a szczególnie doświadczenia wynikające z ostatnich konfliktów zbrojnych z udziałem Hezbollahu i Hamasu oraz z działań w Afganistanie, a ostatnio agresji Rosji na Ukrainie upoważniają do sformułowania tezy, że tradycyjne klasyfikowanie wojen[13] utraciło swoją aktualność i nie odpowiada rzeczywistości. Stratedzy oraz analitycy wojskowi coraz częściej wskazują na zacieranie się granic między poszczególnymi modelami i kategoriami wojen oraz łączenie się różnorodnych form prowadzenia działań zbrojnych i stosowanej taktyki[14]. Istnieje również pewna zbieżność, polegająca na zacieraniu się granic między zdolnościami przynależnymi do państwa a zdolnościami aktorów pozapaństwowych. Proces ten jest coraz bardziej przyspieszany przez globalizację i wpływ nowych technologii. W odniesieniu do współczesnych konfliktów zbrojnych hybrydyzacja może być rozumiana jako współistnienie elementów „starych" i „nowych" wojen, klasycznych konfliktów zbrojnych i wojen „ponowoczesnych", starcia narodowych armii i konfliktów asymetrycznych, supertechnologii wojskowych i prymitywnych broni, walki o terytoria i zasoby oraz sporów o tożsamość i wartości, konfrontacji wschodniej cywilizacji destrukcyjno-pasożytniczej z cywilizacją chrześcijańską Zachodu[15].

Hybrydowość w odniesieniu do założeń strategicznych, planowania operacyjnego i prowadzenia działań operacyjno-taktycznych jest cechą dysfunkcjonalną. Utrudnia integrowanie poszczególnych formacji, jednostek i związków operacyjno-taktycznych sił zbrojnych, a tym samym uniemożliwia efektywne, jednolite dowodzenie w czasie rzeczywistym. Według Thomasa Hubera, autora koncepcji wojny jako produktu złożonego, użycie w działaniach bojowych oddziałów sił zbrojnych oraz rozproszonych sił nieregularnych nie będzie skuteczne bez scentralizowanego, sieciocentrycznego kierowania operacjami militarnymi oraz odpowiedniego rozpoznania przestrzeni konfrontacji militarnej[16].

Wyczerpująca definicja działań hybrydowych, aby była właściwa, musi uwzględniać możliwie wszystkie doświadczenia tego typu działań z ostatnich dziesięcioleci. Uproszczone twierdzenie, że wojna hybrydowa to działania o charakterze partyzanckim + nowoczesne technologie, jest tylko częścią prawdy i odnosić się może jedynie do podmiotów niepaństwowych. Podobna działalność ze strony podmiotu, jakim jest państwo, jest znacznie szersza. Spektrum metod wykorzystywanych przez

łecznych i cywilizacyjnych oraz ich wzajemnych związków, relacji i oddziaływań. Według: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, AON, Warszawa 2003, s. 11.

[11] Konflikt asymetryczny cechuje się odmiennością celów oraz metod działania, wykorzystywanych środków i zasobów, a także rozbieżnością wartości, norm i zasad, którymi kierują się walczące strony. Przeciwsymetryczność (*dissymmetry*) polega na braku równowagi pomiędzy uczestnikami konfliktu pod względem zaangażowania w konflikt oraz sposobów wykorzystania posiadanych zasobów na płaszczyźnie operacyjnej, nie zaś zróżnicowania, co do samego rodzaju zasobów czy też zasad prowadzenia konfliktu. Rozumiana w ten sposób asymetria w konflikcie (*asymmetry within warfare*) nie wpływa na zmianę charakteru konfliktu z symetrycznego na asymetryczny (*asymmetric warfare*), lecz stanowi wspomnianą rzecz ujmując – przewagę militarną. Według: J. Russel, *Asymetric Warfare* [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Wyd. Strategic & Combat Studies Institute, Shivenham, 2002 r., s. 120–122.

[12] J.J. Mc Cuen, *Hybrid Wars* [w:] Military Review 2008, nr 2, s. 108.

[13] B. Balcerowicz, *Konflikty zbrojne i wojny w zmieniającym się środowisku bezpieczeństwa*, Warszawa 2004, s. 34.

[14] M. Boot, *War Made New: Technology, Warfare and the Course of History: 1500 to Today*, Gotham Books, New York, October 2006, C. Gray, *Another Bloody Century: Future Warfare*, Phoenix, London 2005.

[15] A. Gruszczak, *Hybrydowość współczesnych wojen*, s. 11.

[16] T.M. Huber, *Compound Warfare: A Conceptual Framework, Compound Warfare: That Fatal Knot*, U.S. Army Command and General Staff College Press, red. T.M. Huber, Fort Leavenworth 2002 r., s. 1–7.

dane państwo obejmować może od tradycyjnego prowadzenia walki zbrojnej z wykorzystaniem broni niekonwencjonalnej, cybernetycznej oraz walki informacyjnej, po działania służb specjalnych, w których obszarze pozostaje dezintegracja społeczeństw, przez aktywację działania agentury wpływu[17], a także terroryzm czy wspieranie i wykorzystywanie działalności kryminalnej. Całość działań podporządkowana zostaje nadrzędnemu celowi politycznemu danego państwa.

Istotne osiągnięcia w badaniach nad działaniami hybrydowymi zaprezentował Frank Hoffman. Zdefiniował on model współczesnych wojen hybrydowych z perspektywy doświadczeń ostatnich konfliktów na świecie. Za punkt wyjścia posłużyła hipoteza, iż wojna w Libanie z 2006 roku uzmysłowiła, że w „teatrze wojny" na stałe zapewnił sobie miejsce typ uczestnika łączącego w sobie cechy aktora konwencjonalnego i nieregularnego. Na podstawie zapisów przyjętych w Narodowej Strategii Obronności (National Defense Strategy) USA z 2005 roku, Hoffman wysunął wniosek, iż wiele uczyniono na rzecz precyzyjnego określenia zagrożeń i wyzwań dla bezpieczeństwa współczesnego świata. Jednak dynamika przemian powoduje, że niezbędne staje się dużo częstsze, niż dotychczas, weryfikowanie aktualności stanowiska[18]. Podkreśla on również, że cechą wojen hybrydowych jest powszechne występowanie aktów terroryzmu oraz różnorodnych form przestępczości kryminalnej[19]. Z kolei łotewski analityk Janis Berznis nazywa wojnę hybrydową mianem *wojny IV generacji*[20]. Natomiast według poglądów rosyjskich, określana jest *wojną nowej generacji.* Zdaniem szefa Sztabu Generalnego SZ Rosji, w wojnach nowej generacji zasady prowadzenia wojny fundamentalnie się zmieniły. Wzrosła rola niemilitarnych środków (ekonomicznych, kulturowych) służących do osiągnięcia celów politycznych i strategicznych. Takie środki są znacząco bardziej efektywne niż klasyczne metody militarne[21]. W trakcie działań hybrydowych „...szerokie zastosowanie mają działania asymetryczne, pozwalające niwelować przewagę przeciwnika w walce zbrojnej. Do nich zalicza się wykorzystanie sił specjalnych i wewnętrznej opozycji dla stworzenia stałego frontu na całym terytorium wrogiego państwa, oddziaływanie informacyjne, a także stale zmieniające się formy i sposoby oddziaływania"[22]. W konflikcie hybrydowym w rosyjskim ujęciu nie ma różnicy między wojną a pokojem, w klasycznym rozumieniu tych pojęć, oraz pomiędzy umundurowanym personelem a działaniami pod przykryciem. „Taka kombinacja, zwłaszcza w czasie, *gdy wojny nie są deklarowane, a po prostu się zaczynają*, jest bardzo różna od tego, na czym skupiają się tradycyjnie teoretycy wojny. Wojna hybrydowa ma potencjał do zmiany *całkowicie stabilnego kraju w arenę najbardziej intensywnego konfliktu zbrojnego w parę miesięcy, a nawet dni*[23]. Istotnym elementem, na który kładzie nacisk strona rosyjska w wojnie nowej generacji jest zacieranie się różnic między poziomami działań: strategicznym, operacyjnym i taktycznym oraz między działaniami ofensywnymi i defensywnymi. Bezkontaktowe, na dystans, oddziaływanie na przeciwnika staje się głównym sposobem osiągnięcia celów walki i operacji.

Z kolei w dokumencie NATO z 25 sierpnia 2010 r. *Bi-Sc Input To A New Nato Capstone Concept For The Military Contribution To Countering Hybrid Threats*[24] można znaleźć ocenę zagrożeń

[17] A.I. Kuk, *Kanwa wywiadu agenturalnego*, Warszawa 1994, s.19.

[18] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007, s. 12.

[19] F.G. Hoffman, *Conflicts in the 21st Century: The Rise of Hybrid Wars,* Potomac Institute for Policy studies, Arlington 2007 r., s. 14; R. Peters, *Hybrid threats: reconceptualizing the evolving character of modern conflict* [w:] Strategic Forum 2009 r., nr 240, s. 5.

[20] Termin *wojna czwartej generacji* po raz pierwszy był użyty przez strategów wojskowych w latach 80. dla scharakteryzowania przyszłych kierunków ewolucji wojny. Ewolucja dokonywała się na przestrzeni historii i obejmowała kilka faz. Wojna pierwszej generacji była zdominowana przez armie masowe i polegała na zadawaniu strat w stanie osobowym, a jej kulminacja przypadała na wojny napoleońskie. Dominacja i siła ognia charakteryzowały wojnę drugiej generacji, a jej przykładem może być pierwsza wojna światowa. Wojna trzeciej generacji, dzięki wykorzystaniu nowoczesnych technologii i rozwojowi przemysłowemu była zdominowana przez manewr, zastosowany na szeroką skalę przez Niemców w czasie drugiej wojny światowej. Ewolucja wojny czwartej generacji czerpała z rozwoju politycznego, społecznego, ekonomicznego i technologicznego, który miał miejsce po zakończeniu drugiej wojny światowej. Wszystkie zmiany zostały zaadoptowane i wykorzystane przez nowego, niekonwencjonalnego przeciwnika (http – patrz: bibliografia); T.X. Hammes, *Insurgency: Modern Warfare Evolves into a Fourth Generation* [w:] Strategic Forum, No. 214, January 2005 (http – patrz: bibliografia). S.C. Williamson, *From fourth generation warfare to hybrid war*, U. S. Army College, Carlisle Barracks, Pennsylvania 2009, s. 22.

[21] W. Gierasimow, *Rola Sztabu Generalnego w organizacji obrony kraju w związku z nowym Statutem Sztabu Generalnego zatwierdzonym przez prezydenta Federacji Rosyjskiej*, (http – patrz: bibliografia).

[22] Ibidem, s. 3.

[23] Ibidem, s. 4.

[24] BI-S.C. *Input to a new NATO capstone concept for the military contribution on countering hybrid threats*, International Military Staff, 29 September 2010.

hybrydowych dla bezpieczeństwa globalnego w XXI wieku. Studium przyszłości NATO[25] wskazuje, że przyszły przeciwnik będzie łączył różne modele wojen i symultanicznie stosował kombinację działań konwencjonalnych, nieregularnych, terrorystycznych i kryminalnych[26], określaną mianem *wojny hybrydowej*[27] lub *zagrożenia hybrydowego*. Określono, że treścią tych działań będzie łączenie konwencjonalnych zdolności z taktyką nieregularnych formacji zbrojnych, działaniami terrorystycznymi oraz kryminalnymi. Istotą działalności kryminalnej[28] w tym wypadku będzie destabilizowanie funkcjonowania lokalnych władz i wspieranie rebeliantów oraz wszelkich opozycjonistów poprzez dostarczanie wysoko zaawansowanej technologicznie broni i amunicji oraz środków finansowych. Grupy przestępcze, funkcjonujące jako struktura hierarchiczna w środowisku zurbanizowanym, będą stanowić zarówno zaplecze, jak i wsparcie dla szeroko pojętej działalności hybrydowej, obejmującej również narkoterrozryzm. Zakłada się, że przeciwnik, aby uzyskać przewagę, będzie stosował wszystkie wyżej wymienione modele walki jednocześnie[29]. Wielomodelowa forma prowadzenia walki może być stosowana przez jedną lub kilka formacji, pojedynczo lub symultanicznie, w różnym czasie i wymiarze. Zawsze jednak działania będą koordynowane na szczeblu operacyjnym lub taktycznym i zazwyczaj stanowić będą jedną przestrzeń walki dla osiągnięcia efektu synergii. Oponenci będą osiągać dużą efektywność działań, ponieważ będą operować w złożonym i kompleksowym środowisku, w tym wymiarze informacyjnym, zarówno w sferze fizycznej, jak i psychicznej. Hybrydowy przeciwnik będzie efektywnie stosował zaawansowane technologicznie systemy i wykorzystywał je w specyficzny sposób dla osiągnięcia własnych celów[30]. Przeprowadzone badania wskazują na to, że w przyszłym środowisku operacyjnym będzie dominować zagrożenie hybrydowe, skierowane w najbardziej wrażliwe punkty sił zbrojnych państw uczestniczących w konflikcie, bądź w infrastrukturę krytyczną państwa – strony konfliktu. Należy oczekiwać, że przyszły przeciwnik będzie stosował wszelkie możliwe formy i metody prowadzenia działań zbrojnych oraz różnorodną taktykę. Można założyć, że w przypadku wystąpienia konfliktu i prowadzenia działań interwencyjnych przeciwnik będzie *wtapiał* się w lokalną społeczność i preferował długotrwałe, nękające działania rebelianckie i partyzanckie, polegające na stosowaniu zasadzek, improwizowanych ładunków wybuchowych i ostrzałów rakietowych. Poza tym działania te mogą obejmować użycie wysoko zaawansowanych technologicznie systemów uzbrojenia z równoczesnym prowadzeniem klasycznych działań terrorystycznych oraz działań w cyberprzestrzeni, ukierunkowanych na przeciwdziałanie zarówno systemom uzbrojenia, jak i cywilnym systemom infrastruktury krytycznej[31].Oprócz tego należy uwzględnić, wymienioną wcześniej, działalność kryminalną, która z dużym prawdopodobieństwem wpłynie destrukcyjnie na funkcjonowanie państwa. Można założyć, że tego typu działalność może posłużyć do zapewnienia środków do prowadzenia działań o charakterze nieregularnym czy terrorystycznym. Rozwój technologii z kolei doprowadzi do tego, że coraz trudniej będzie można odróżnić działania regularne od nieregularnych, terrorystę od zwykłego obywatela, działania kinetyczne od niekinetycznych. Działania *hybrydowe* należy łączyć zarówno z organizacją, jak i stosowanymi środkami czy metodami ich użycia. W ostatnich latach odnotowywano, jeśli nie wzrost, to utrzymywanie się na stałym, wysokim poziomie ilości konfliktów, w których stroną inicjującą, a zatem narzucającą strategię byli aktorzy niepaństwowi, np. Hezbollah, Hamas czy Al-Kaida. Obecnie trend ten może zostać zatrzymany, bądź też będzie obecny w odniesieniu do państw nie tylko słabych, ale silnych, o olbrzymim

[25] *Multiple Futures Project...*, s. 34.

[26] Ibidem, s. 47.

[27] Według Departamentu Obrony USA, który dość ogólnie to zdefiniował, „(...) *działania hybrydowe, nieregularne działania wojenne to preferowanie niebezpośrednich i asymetrycznych metod, które mogą łączyć w sobie cały zestaw możliwości, zarówno wojskowych jak i innego typu, a mających na celu doprowadzenie do erozji siły przeciwnika, jego wpływów i woli*". Według: The Missile Defense Program 2009–2010, Missile Defense Agency, Department Obrony.(http – patrz: bibliografia).

[28] P.J. Smith, *Terrorism in the Year 2020: Examining the Ideational, Functional and Geopolitical Trends that Will Shape Terrorism in the Twenty-First Century*, NSDM Department, US Naval War College, Newport, USA, March 2008, s. 59 (http – patrz: bibliografia).

[29] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007, s. 7–8 (http – patrz: bibliografia).

[30] W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Naval Postgraduate School, Monterey, June 2002 (http – patrz: bibliografia).

[31] F.G. Hoffman, *Conflict in the*, s. 28.

potencjale gospodarczo-militarnym, jakim jest Federacja Rosyjska.

Konkludując, wspólnym elementem powyższych definicji i poglądów jest dążenie stron konfliktu hybrydowego do zbliżenia stosowanych przez nie metod, środków oraz sposobów prowadzenia działań militarnych i pozamilitarnych w celu maksymalizacji efektu synergii, pozwalającego na osiągnięcie trwałej przewagi nad przeciwnikiem. Uzyskanie przewagi jest czynnikiem powodującym strukturalną zmianę przestrzeni konfrontacji. Na podstawie wyników przeprowadzonych badań można stwierdzić, że zauważalny jest proces zacierania się różnic w sposobach percepcji elementów składowych konfliktów, diagnozowania i analizowania charakteru i zakresu oddziaływania konfliktu na środowisko bezpieczeństwa regionalne i międzynarodowe. Obowiązujące dotychczas wzorce doktrynalne prowadzenia działań militarnych utraciły swoją aktualność i nie jest możliwe, aby bezpośrednio przełożyć je na obecną rzeczywistość w konfrontacji z przeciwnikiem hybrydowym.

Współczesny wymiar działań hybrydowych

Przykładem ilustrującym pełne spektrum metod i form wojny hybrydowej, gdzie słabszy przeciwnik stosuje je przeciw silniejszemu, może być wieloletni konflikt Izraela z Hezbollahem[32]. Na podstawie doświadczeń Izraela z ostatniej dekady można postawić tezę, że następuje transformacja zdolności nieregularnych, stosowanych przez aktorów pozapaństwowych, w zdolności hybrydowe stosowane przez państwa[33]. Przyszłe wyzwania będą się wiązać z tym, że potencjalny przeciwnik będzie dysponował o wiele bardziej kompleksowym wachlarzem struktur organizacyjnych i stosował bardziej złożoną strategię i taktykę niż ta, z którą zetknęła się armia izraelska w 2006 roku[34]. Hezbollah wyraźnie udowodnił, że aktorzy pozapaństwowi są w stanie przeprowadzić wiarygodną ocenę możliwości strategicznych armii, określanych jako *zachodnie*, i skutecznie przeciwstawić się ich najnowocześniejszym zdolnościom.

W podsumowaniu można stwierdzić, że ciągły i nieprzerwany konflikt Izraela z jego niepaństwowym wrogiem pokazuje wielkość wysiłku wywiadowczego, militarnego i informacyjnego izraelskiej armii i służb specjalnych, jaki należy włożyć, aby stworzyć warunki do zneutralizowania i wyeliminowania organizacji stosującej terroryzm. Hezbollah dzięki wsparciu, jakie otrzymuje od Iranu oraz zakorzenieniu się w Libanie, stał się niebezpiecznym zagrożeniem nie tylko dla Izraela, ale i w regionie Bliskiego Wschodu. Zwycięstwo w 2006 r. Hezbollahu nad interweniującą armią Izraela pokazało, jak skuteczną jest organizacją, a drugiej strony, jakie zagrożenie stanowi dla państw sąsiadujących[35]. Dalszy proces globalizacji oraz rozwój zdolności zbrojnych Hezbollahu może rozwinąć się w znacznie dalszym i niebezpiecznym kierunku. Kwestia dalszej ewolucji tej organizacji jest z pewnością otwarta i nie można jej lekceważyć.

Wyzwania hybrydowe nie ograniczają się do aktorów pozapaństwowych. Doświadczenia wyniesione z operacji w Iraku i Afganistanie, a ostatnio z kryzysu ukraińskiego wskazują, że państwa

[32] Hezbollah (tłum."Partia Boga") jest szyickim ugrupowaniem polityczno-militarnym, które zostało stworzone na terenach Libanu w 1982 r. po izraelskiej operacji „Pokój dla Galilei", jako narzędzie do walki z głównym wrogiem Arabów – Izraelem. Swoje istnienie zawdzięcza irańskiej pomocy w postaci przysłania do Libanu reprezentacji instruktorów z Korpusu Strażników Rewolucji. Od tego czasu pozycja Hezbollahu stała się na tyle znacząca, że na terenie Bliskiego Wschodu stał się jednym z ważniejszych aktorów niepaństwowych oraz oponentem Izraela. Dzięki swojemu działaniu posiadł niebezpieczną zdolność wpływania na region. Według: M. Jadwiszczok, *Antyizraelskie ugrupowania terrorystyczne i ich zwalczanie*, Toruń 2010, s.104. oraz R. Ożarowski, *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011, s. 39.

[33] D.E. Johnson, *Military Capabilities for Hybrid War, Insight from the Israel Defense Force in Lebanon and Gaza*, RAND Corporation, 2010, s. 5 (http – patrz: bibliografia).

[34] M.B. Stannard, *Hezbollah Wages New Generation of Warfare* [w:] San Francisco Chronicle, 6 August 2006 (http – patrz: bibliografia).

[35] Za szczyt konfliktu Izraela z Hezbollahem uznaje się rok 2006. Po wycofaniu się armii izraelskiej z Libanu Hezbollah przesunął obszar swojego działania bezpośrednio pod granicę libańsko-izraelską. Od tego momentu przypuszczał kolejne ataki na osiedla izraelskie. Mimo to do 2006 obie strony toczyły ze sobą potyczki bez większej eskalacji na szerszy obszar państwa. Można uznać, że dotychczas Hezbollah wiedział, do jakich granic może się posunąć oraz jakich reperkusji może oczekiwać ze strony przeciwnej. Dopiero zasadzka z 12 czerwca 2006 roku na patrol izraelskich żołnierzy sprawiła, że rząd izraelski pod przywództwem Ehuda Olmerta podjął decyzje o przeprowadzeniu operacji zbrojnej przeciwko Hezbollahowi. Przewaga jakościowa armii Izraela nie przełożyła się na skuteczność. Nie udało się wyeliminować najważniejszych przywódców Organizacji oraz uszczuplić jej zasobów. Konflikt trwający ponad miesiąc pokazał, że oprócz siły militarnej Hezbollah może być równorzędnym przeciwnikiem w wojnie informacyjnej. Konflikt ten nie pozwolił Izraelowi na jednogłośne obwołanie się zwycięzcą. Pokazało to władzom izraelskim, że pokonanie grup militarnych Hezbollahu nie jest do końca możliwe. Według: K.E. Schulze, *Konflikt arabsko-izraelski*, Warszawa 2010, s. 142.

mogą przekształcić regularne pododdziały sił zbrojnych w formacje nieregularne, które będą dysponować klasycznymi zdolnościami i adaptować nową taktykę działania, a następnie wspierać pododdziały regularne. Wobec tego nie można postrzegać państw przez pryzmat posiadania tylko klasycznych sił zbrojnych, a aktorów pozapaństwowych kojarzyć wyłącznie z działaniami nieregularnymi, ponieważ w przyszłości hybrydowe siły zbrojne mogą być wykorzystywane w sposób nieprzewidywalny[36].

Modelowym przykładem, gdzie państwo, jako strona silniejsza, prowadzi wojnę hybrydową z przeciwnikiem słabszym, jest agresja Rosji na Ukrainie. W wojnie hybrydowej na Ukrainie można wyodrębnić 4 etapy: dywersję polityczną, budowanie pozycji społecznej i politycznej separatystów, interwencję zbrojną oraz odstraszanie, poprzez demonstrację potencjału sił niekonwencjonalnych. Charakterystyczne dla tego konfliktu jest to, że ww. etapy zachodzą często na siebie i charakteryzują się różną intensywnością. Pomimo wyraźnych oznak udziału regularnych sił zbrojnych władze rosyjskie oficjalnie zaprzeczają udziałowi w konflikcie[37].

Eksperci NATO stawiają tezę, że sytuacja kryzysowa wykracza daleko granice Ukrainy. Rosyjskie władze uważają, że obrona etnicznych Rosjan nie leży w gestii państw, w których oni mieszkają, i nie podlega ich prawom, rządowi czy konstytucji, ale podlega Rosji. Takie podejście rosyjskich władz do etnicznych Rosjan, które wg Kurta Volkera, ambasadora USA przy NATO, jest nie tylko „wyłomem w pojmowaniu prawa międzynarodowego, ale też techniką wojny hybrydowej, nazywaną *nowym podejściem,* która była już wcześniej stosowana m.in. w Estonii w 2007 r, w Gruzji w 2008 r. [...] Koncepcja powolnego, ale systematycznego działania powoduje naruszanie suwerenności, jest częścią strategicznego krajobrazu dobrze znanego Rosji już od pewnego czasu. [...]. Czasem obejmuje to bardziej otwarte i oczywiste posunięcia, czasem posunięcia są bardziej subtelne, jest to walka za pomocą ekonomii, czasami – ataków cybernetycznych przeprowadzanych pod pozorem działań niezależnych aktywistów". Jego zdaniem „ ... taki zbiór taktyk wojny hybrydowej używa Rosja od co najmniej 5–6 lat"[38]. Istnieje wiele przesłanek, aby stwierdzić, że konflikt rosyjsko-ukraiński jest dalej w fazie rozwojowej. Czas, który upłynął od rozpoczęcia rosyjskiej agresji na Ukrainę pozwolił analitykom zarówno polskim, jak i natowskim na rozpracowanie scenariuszy i metod wojny hybrydowej prowadzonej przez Rosję. Elementem, który ją zapoczątkował była aktywność w sferze walki informacyjnej. Analizując scenariusz rosyjskiej agresji na Ukrainie, można podać w wątpliwość tezę, że rosyjska agresja rozpoczęła się wraz z protestami na Majdanie. Wiele wskazuje na to, że w rzeczywistości rosyjski atak rozpoczął się na długo przed opuszczeniem kraju przez prezydenta Wiktora Janukowycza. Militarny udział w konflikcie, gdzie przebrani, a w zasadzie nieposiadający oznak identyfikacyjnych rosyjscy żołnierze wojsk powietrznodesantowych pojawili się na Krymie i w Donbasie, został poprzedzony ofensywą informacyjną[39]. W latach poprzedzających konflikt strona rosyjska rozpoczęła medialną ekspansję na Ukrainie. Orężem, który został użyty do destabilizacji struktury informacyjnej mediów ukraińskich, okazały się rosyjskie koncerny medialne, przy pomocy których prowadzono skoordynowaną infiltrację informacyjną Ukrainy. Ekspansja przebiegała za pomocą wykupienia udziałów w mediach od ukraińskich oligarchów. W ten sposób ukraińskie społeczeństwo zaczęło odbierać informacje, które naświetlały sytuację z punktu widzenia interesów Rosji, a nie Ukrainy. Została dokonana medialna manipulacja społeczeństwa. Na tak wytworzony grunt nałożyła się integracja środowisk prorosyjskich i aktywacja rosyjskiej agentury wpływu[40]. Można wyodrębnić kilka kluczowych sposobów ataku oraz główne cele interwencji. Po pierwsze dezinformacja. Udział rosyjskich żołnierzy jest maskowany poprzez tworzenie ochotniczych sił separatystycznych. Koncentracja rosyjskich oddziałów przerzucanych na Ukrainę odbywała się pod pretekstem ćwiczeń w nadgranicznych obwodach. O ile ten sposób można zaliczyć do tradycyjnych, był stosowany w wojnie z Gruzją[41], to *novum* stano-

[36] M. Williams, *The Future*,s. 9.

[37] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond* (http – patrz: bibliografia).

[38] Przegląd NATO. Magazyn –polska wersja językowa (http – patrz: bibliografia).

[39] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku* [w:] Punkt widzenia 2014, nr 42, wyd. OSW, Warszawa 2014, s. 23.

[40] A.I. Kuk, *Kanwa wywiadu agenturalnego*, Warszawa 1994, s. 12.

[41] Raport OSW, *Zmiany w potencjale militarnym Federacji Rosyjskiej (po rosyjskiej operacji wojskowej w Gruzji*), OSW Warszawa 2009, s. 4.

wiło przygotowanie do wojny w cyberprzestrzeni. Z chwilą rozpoczęcia agresji, w sieci ujawniły się setki stron i portali społecznościowych. Pozornie „niezależnych i obiektywnie informujących" o wydarzeniach, a w rzeczywistości wzajemnie powiązanych i koordynujących aktywne działania dezinformacyjne[42]. Bardzo skuteczną metodą okazała się także plotka, potwierdzana informacjami przekazywanymi przez rosyjskich polityków i wojskowych. Zaobserwowano, że celem przekazywania takich informacji jest wytworzenie atmosfery zastraszenia zarówno podczas mobilizacji ukraińskiej armii, która przebiegała w atmosferze strachu i nieufności, jak i w trakcie prowadzenia działań militarnych. Przykładem tego może być stwierdzenie jednego z deputowanych do Rady Najwyższej Ukrainy, że „... straty poniesione pod Debalcewe to wynik paniki, której źródłem były rosyjskie media bombardujące żołnierzy informacjami o pełnym okrążeniu, co przerodziło kontrolowany odwrót w bezładną ucieczkę"[43]. Rosja wykorzystuje najsłabsze punkty strony ukraińskiej. Celem ataków informacyjnych jest propagowanie negatywnych zjawisk w społeczeństwie i elitach władzy Ukrainy. Takie zjawiska jak powszechna korupcja, potężny nacjonalizm panujący w zachodnich obwodach Ukrainy oraz rozdźwięki pomiędzy obozem władzy prezydenta i premiera pozostają podstawowymi celami ataków wojny informacyjnej.

Wojnie informacyjnej przeciwko Ukrainie towarzyszą podobne działania Federacji Rosyjskiej w Europie i na świecie. Rosja prowadzi intensywną kampanię informacyjną, mającą na celu wzmocnienie podziałów w Unii Europejskiej i NATO, co do konieczności i zakresu pomocy dla Kijowa oraz zasadności sankcji wobec niej samej. Wykorzystuje do tego zarówno kontakty interpersonalne z zachodnimi politykami, zachęty ekonomiczne oraz oddziaływanie medialne[44]. W przestrzeni informacyjnej prezentuje się i akcentuje rosyjską wersję wydarzeń, a generalnym celem, jak się wydaje, pozostaje poróżnienie opinii publicznej. Kluczowym punktem takiej strategii jest kształtowanie obrazu Rosji jako ofiary cynicznej gry zachodniego establishmentu, oskarżanego przy tej okazji o całkowite zniekształcanie wizerunku prezydenta Rosji oraz przyczyn i przebiegu konfliktu ukraińskiego.

Ukraina przegrywa wojnę informacyjną. Ukraińskie instytucje przeciwdziałania pozostają jeszcze w początkowej fazie ich tworzenia. Sytuację dodatkowo utrudnia fakt, że system bezpieczeństwa i prawa międzynarodowego nie przewiduje takiej sfery działalności wojennej. Ani Karta ONZ, ani dokumenty założycielskie OBWE nie definiują pojęcia wojny informacyjnej, ani metod monitoringu i nie nakładają zakazu jej prowadzenia. Prawo międzynarodowe jest bezradne wobec rosyjskiej agresji, czego przykładem jest brak reakcji misji OBWE na ukraińskie dowody w sprawie rosyjskich działań dezinformacyjnych, a nawet udziału regularnych jednostek armii rosyjskiej w konflikcie. Obserwatorzy międzynarodowi są po prostu bezradnymi figurantami.

Przechodząc do militarnego udziału Rosji w konflikcie i początków wojny, można postawić tezę, że strona rosyjska dominującą rolę w opracowaniu planu konfliktu na Ukrainie, a następnie kierowaniu jego przebiegiem powierzyła służbom specjalnym. W połączeniu ze wsparciem regularnych jednostek SZ FR powstała sytuacja bezwzględnej przewagi militarnej w rejonie prowadzonego konfliktu. W chwili obecnej szacuje się, że w regionie Donbasu i przy granicy z Ukrainą dyslokowanych zostało do 44 batalionowych grup taktycznych (BTG). Ocenia się, że możliwości armii rosyjskiej pozwalają w ciągu miesiąca zwiększyć ich liczbę do 80, a w ciągu 3 – do 120. Strona rosyjska w przeciwieństwie do wcześniejszych interwencji w Czeczenii oraz Gruzji i na Ukrainę kieruje pododdziały o jak najmniejszej liczbie poborowych[45]. Działania zbrojne realizowane są przede wszystkim przez wojska specjalne, powietrznodesantowe i specjalistyczne, wspierane przez najemników (Czeczeni, Kozacy) i opłacanych ochotników, a także przez przeszkolonych i doposażonych lokalnych separatystów. Proces rotacji sił i sprzętu jest ciągły i oscyluje w granicach 2–3 transportów kolejowych dziennie. W okresie do końca stycznia 2015 r. w rejonie Donbasu Rosjanie dysponowali 16 BTG, 340 czołgami, 720 BWP i transporterami opancerzonymi (IFV/APC), 173 działami artyleryjskimi oraz 92 wieloprowadnicowymi wyrzutniami rakietowymi (MLRS); separatyści – 10 BTG, 340 czołgami, 329 IFV/APC, 372 działami artyleryjskimi oraz 472 MLRS[46]. Zgromadzony potencjał mili-

[42] J. Darczewska, op. cit., s. 28.

[43] R. Cheda, *Rosyjska wojna informacyjna – lekcja z Ukrainy* (http – patrz: bibliografia).

[44] *Sankcje i Rosja*, red. J. Ćwiek-Karpowicz, S. Secrieu, Wyd. PISM Warszawa 2015, s. 99.

[45] Raport OSW, op. cit., s. 35.

[46] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond.* (http –

tarny zapewnia całkowitą swobodę operacyjną stronie rosyjskiej. Jednak i przy tak bezwzględnej przewadze strona rosyjska wykorzystuje konwoje humanitarne jako jeden ze elementów zakamuflowanego dozbrajania sił separatystycznych. Zaobserwowana została korelacja pomiędzy rosyjskimi konwojami humanitarnymi a wzrostem intensywności działań zbrojnych separatystów.

Na podstawie przeprowadzonych badań można stwierdzić, że plan przeprowadzenia szybkiego rozbicia sił ukraińskich i obalenia władz w Kijowie został porzucony na rzecz stopniowego osłabiania państwa ukraińskiego i jego sił zbrojnych, połączonego z systematycznym zwiększaniem zdobyczy terytorialnych. Sytuację kryzysową dodatkowo komplikuje fakt, że USA i państwa Europy Zachodniej jednoznacznie poleciły władzom ukraińskim ograniczyć działania obronne w taki sposób, aby nie były one uznane przez Rosjan za prowokacyjne i nie dawały pretekstu do dalszej eskalacji konfliktu[47]. Bierna postawa ukraińskich sił bezpieczeństwa w połączeniu z brakiem natychmiastowego wsparcia militarnego ze strony państw Zachodu, w tym przede wszystkim w niezbędne dane wywiadowcze i krytyczne zdolności militarne, doprowadziły do wzmocnienia sił separatystycznych. Według opinii prof. Karbera[48] „... w najbliższej przyszłości nie ma mowy o możliwości odzyskania przez Ukrainę nie tylko Krymu zaanektowanego przez Rosję wbrew sprzeciwom Zachodu, ale i pozostałych obszarów na wschodzie kraju, nad którymi władze w Kijowie straciły kontrolę. Co więcej, zagrożony jest nawet obecny rozejm, którego całkowite zerwanie groziłoby Ukrainie dalszymi stratami terytorialnymi"[49].

Reasumując, można przyjąć, że brak stanowczej reakcji Zachodu, zmniejszające się zdolności obronne ukraińskich sił zbrojnych oraz stałe wzmacnianie rosyjskiej obecności wojskowej na Ukrainie mogą w przyszłości skutkować dalszą eskalacją konfliktu. Federacja Rosyjska może potraktować ukraiński „sukces", jako szablon do dalszego wykorzystania. Staje się jasne, że zagrożona jest nie tylko Ukraina, ale każde państwo, które zamieszkuje mniejszość rosyjska. Metody stosowane przez Rosjan w wojnie hybrydowej na Ukrainie mogą być transferowane w inne rejony, w tym również na państwa bałtyckie. Można przyjąć, że głównym i skutecznym działaniem powstrzymującym rosyjskie agresywne zapędy jest jedność państw zachodnich i wsparcie Ukrainy krytycznymi zdolnościami wojskowymi.

Doświadczenie z ostatnich konfliktów, gdzie na szeroką skalę stosowano elementy działań hybrydowych, pokazują, że potencjał aktorów niepaństwowych, szczególnie do oddziaływania w sferze militarnej, stale rośnie. Co więcej, wzrasta także motywacja w państwach agresorach do stosowania nietradycyjnych form i sposobów prowadzenia walki zbrojnej. Zagrożenia hybrydowe stały się bardzo efektywne nie tylko przeciwko siłom koalicji, np. w operacjach w Iraku czy Afganistanie, ale również przeciwko dużym, ciężkim i hierarchicznym międzynarodowym organizacjom bezpieczeństwa (NATO, OBWE, ONZ), które z zasady są bardzo sztywne pod względem mentalnym i doktrynalnym. W zarysie teoretycznym potrzebę przeciwstawienia się zagrożeniom hybrydowym ujmuje nowa Koncepcja Strategiczna NATO[50], wskazując na rozwijanie współpracy w celu zwalczania niekonwencjonalnych zagrożeń. Praktycznie zaś obecny konflikt trwający na Ukrainie weryfikuje te zapisy i przyjęte dotychczas postrzeganie wojny hybrydowej, która była prowadzona zazwyczaj przez stronę słabszą. Potęga państwa rosyjskiego w połączeniu z elementami wojny hybrydowej dowodzi słabości, w jakiej znalazły się instytucje bezpieczeństwa międzynarodowego oraz zostały zakwestionowane dotychczas przestrzegane porozumienia międzynarodowe. O ile w aspekcie teoretycznym większość ekspertów stoi na stanowisku, że niepowstrzymanie na obecnym etapie agresywnych działań rosyjskich na Ukrainie będzie skutkować rosnącym zagrożeniem destabilizacji całego regionu Europy Środkowej i Wschodniej, o tyle praktyka dowodzi raczej tendencji podejmowania działań kunktatorskich. Stąd też, jak się wydaje, brak jest decyzji prezydenta USA, a także przywódców państw Europy Zachodniej w sprawie dostarczenia Ukrainie niezbędnego wsparcia militarnego, co jest coraz szerzej krytykowane przez niezależne ośrodki opiniotwórcze.

patrz: bibliografia).

[47] Ibidem (http – patrz: bibliografia).

[48] Prof. Phillip Karber – dyrektor amerykańskiego konserwatywnego think-tanku Potomac Foundation oraz wykładowca Georgetown University.

[49] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond* (http – patrz: bibliografia).

[50] *Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Organisation,* NATO Public Diplomacy Division, Brusseles – Belgium 2010, s. 3, 5, 10.

Wnioski

Na podstawie przeprowadzonych badań można stwierdzić, że istota działań hybrydowych polega na wielowymiarowym, jednoczesnym oddziaływaniu w sferze militarnej z zastosowaniem klasycznych i nieregularnych działań zbrojnych, w sferze informacyjnej, cybernetycznej i ekonomicznej. Głównym polem bitwy będzie umysł pojedynczego człowieka, wybranych grup społecznych i elit władzy, dlatego wojna nowej generacji będzie nierozerwalnie związana z działaniami dezinformacyjnymi i psychologicznymi. Ewolucja działań hybrydowych, szczególnie w ciągu ostatniego dziesięciolecia, była bardzo dynamiczna i potwierdziła skuteczność osiągania trwałej przewagi nad przeciwnikiem. Wyzwania hybrydowe nie ograniczają się już wyłącznie do aktorów pozapaństwowych i do stereotypu myślowego, że to przeciwnik słabszy wykorzystuje tę formę działań przeciwko silniejszemu. Doświadczenia wyniesione z operacji w Iraku i Afganistanie, a przede wszystkim z konfliktu zbrojnego na Ukrainie, wskazują, że to państwa mogą przekształcić regularne pododdziały sił zbrojnych w formacje nieregularne, które będą dysponować klasycznymi zdolnościami i adaptować niekonwencjonalne metody działania, a następnie wspierać pododdziały regularne. Wobec tego nie można postrzegać państw przez pryzmat posiadania tylko klasycznych sił zbrojnych, a aktorów pozapaństwowych kojarzyć wyłącznie z działaniami nieregularnymi. Współczesna praktyka działań hybrydowych w konflikcie zbrojnym na Ukrainie uwidoczniła, że nastąpiła diametralna zmiana strony stosującej działania hybrydowe. Po raz pierwszy, to przeciwnik zdecydowanie silniejszy, mocarstwo światowego formatu – Rosja, wykorzystuje pełne spektrum oddziaływania hybrydowego na przeciwnika słabego i niezdolnego do obrony integralności własnego terytorium. Konflikt zbrojny pokazał nie tylko słabość państwa ukraińskiego, ale co ważniejsze niewydolność, w jakiej znalazły się organizacje odpowiadające za zapewnienie bezpieczeństwa międzynarodowego: NATO, OBWE i ONZ. Dalsza eskalacja działań hybrydowych na Ukrainie bez wątpienia zagraża państwom „prawej flanki" Sojuszu Północnoatlantyckiego. Metody stosowane przez Rosjan w wojnie hybrydowej na Ukrainie mogą być transferowane nie tylko na obszar państw powstałych po rozpadzie Związku Radzieckiego, ale również na państwa bałtyckie, Polskę i Rumunię. Sytuacja kryzysowa na Ukrainie nie tylko zmieniła stan bezpieczeństwa w regionie Europy Środkowej i Wschodniej. Z dużym prawdopodobieństwem można założyć, że przedłużający się konflikt będzie miał swoje konsekwencje, wyrażające się w obniżeniu poziomu bezpieczeństwo międzynarodowego.

Bibliografia

Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Organization, wyd. NATO Public Diplomacy Division, Brusseles – Belgium 2010.

Asymetria i hybrydowość – stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011.

Balcerowicz B., *Pokój i nie pokój na progu XXI wieku,* Wyd. Bellona, Warszawa 2002.

Balcerowicz B., *Konflikty zbrojne i wojny w zmieniającym się środowisku bezpieczeństwa*, Warszawa 2004.

BI-S.C. *Input to a new NATO capstone concept for the military contribution on countering hybrid threats*, International Military Staff, 29 September 2010.

Cheda R., *Rosyjska wojna informacyjna – lekcja z Ukrainy*. http://wiadomosci.wp.pl/kat,1356,title-,Rosyjska-wojna-informacyjna-lekcja- z-Ukrainy,wid,17301467,wiadomosc.html?ticaid=11494f&_ticrsn=3 [Dostęp: 12.02.2015 r.].

Clausewitz C., *O wojnie,* Lublin 1995.

Cole R., Irregular threats and challenges, [w:] Marine Corps Gazette 2010, nr 1.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku,* [w:] Punkt widzenia, Nr 42, OSW Warszawa 2014.

Freier E., The defense identity crisis: It's a hybrid world, Parameters 2009 r., nr 3.

Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.

Gentile G. P., The imperative for an American general purpose army that can fight, [w:] Orbis 2009., nr 3.

Glenn R. W., Thoughts on „Hybrid" Conflict, [w:] Small Wars Journal, http://www.smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf [Dostęp: 12.02.2015 r.].

Gierasimow W., *Rola Sztabu Generalnego w organizacji obrony kraju w związku z nowym Statutem Sztabu Generalnego zatwierdzonym przez prezydenta Federacji Rosyjskiej*. http://www.avnrf.ru/index.php/vse-novosti-sajta/620-rol-generalnogo-shtaba-v-organizatsii-oborony-strany-v-sootvetstvii-s-novym-polozheniem-o-generalnom-shtabe-utverzhdjonnym-prezidentom-rossijskoj-federatsii [Dostęp: 12.03.2015 r.].

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna,* [w:] Asymetria i hybrydowość – stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, wyd. BBN, Warszawa 2011.

Hammes T., *Insurgency: Modern Warfare Evolves into a Fourth Generation*, "Strategic Forum", No 214, January 2005.
<http://www.scribd.com/doc/1569981/US-Air-Force-sf214>. [Dostęp: 08.02.2011 r.].
Hoffman F. G., *Hybrid vs Compound War: The Janus Choice – Defining Today's Multifaceted Conflict*, „Armed Forces Journal", October 2009. < http://www.armedforcesjournal.com/2009/10/4198658>. [Dostęp: 05.05. 2011 r.].
Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007. <https://dde.carlisle.army.mil/documents/sis/docs/Hybrid_Wars.pdf>. [Dostęp: 08.02.2011 r.].
Hammes T., *The Sling and the Stone*, Minneapolis, 2006.
Huber T. M., Compound Warfare: A Conceptual Framework, [w:] Compound Warfare: That Fatal Knot, U.S. Army Command and General Staff College Press, Fort Leavenworth 2002.
Johnson D.E., *Military Capabilities for Hybrid War, Insight from the Israel Defense Force in Lebanon and Gaza*, RAND Corporation, 2010.
Keegan J., *Historia wojen,* Warszawa 1998.
Kuk A.I., *Kanwa wywiadu agenturalnego*, Warszawa 1994.
Lasica D.T., Strategic Implications of Hybrid War: A Theory of Victory, school of Advanced Military studies, United Army Command and General staff College Press, Fort Leavenworth 2009.
Liedel K., Piasecka P., Aleksandrowicz T., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Warszawa 2014.
Marks T.A., Counterinsurgency and operational art [w:] Low Intensity Conflict & Law Enforcement 2005, nr 3.
McKinley J., Al-Baddawa A., Rethinking Counterinsurgency, [w:] RAND Counterinsurgency Study, RAND Corporation, Santa Monica 2008.
Multiply Futures Project - Navigating Towards 2030, Allied Command Transformation, Final Report April 2009. https://transnet.act.nato.int/WISE/NATOACTRes/MultipleFu/file/_WFS/20090503_MFPfinalrep.pdf [Dostęp: 12.02.2015 r.].
Nemeth W.J., *Future War and Chechnya: A Case for Hybrid Warfare* [w:] Naval Postgraduate School, Monterey, June 2002.
Ożarowski R., *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011.
Portal Gławred, http://inosmi.ru/glavred_info/ [Dostęp 12.03.2015 r.].
Przegląd NATO. Magazyn –polska wersja językowa. http://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/PL/index.htm [Dostęp: 01.03.2015 r.].
Russel J., *Asymetric Warfare* [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Wyd. Strategic & Combat Studies Institute, Shivenham, 2002.
Schulze K. E., *Konflikt arabsko-izraelski*, Warszawa 2010.
Shirreff R., *Unity of purpose in hybrid conflict: managing the civilian/ military disconnect and operationalizing the comprehensive approach*, Chatham House, Londyn 2010.
Słownik wyrazów obcych, PWN, Warszawa 1980.
Smith P.J., *Terrorism in the Year 2020: Examining the Ideational, Functional and Geopolitical Trends that Will Shape Terrorism in the Twenty-First Century*, NSDM Department, US Naval War College, Newport, USA, March 2008.
Stannard M.B., *Hezbollah Wages New Generation of Warfare* [w:] San Francisco Chronicle", 6 August 2006.
Sun Tzu, *Sztuka wojny*, Gliwice 2004.
The Missile Defense Program 2009–2010, Missile Defense Agency, *Departament Obrony* [Dostęp: 10.03.2015 r.].
The Russian Military Forum: *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond.* http://csis.org/event/russias-hybrid-war-campaign-implications-ukraine-and-beyond [Dostęp: 12.03.2015 r.].
Williams M., *The Future Security Environment,* RUSI, 2008. <http://www.rusi.org/downloads/assets/Future_Security_RP_13_Feb_2008.pdf>. [Dostęp: 07.02.2011 r.].
Wrzosek M., *Zagrożenia militarne a bezpieczeństwo Europy*, [w:] Kwartalnik Bellona 2012, nr 4.

THE THEORY AND THE PRACTICE OF HYBRID OPERATIONS

Abstract

The article is devoted to the theory and the practice of hybrid operations, which affect the security of the international environment. The results of the analyses have been referred to the problem defined in the form of questions about the causes and methods for implementation and directions for countering hybrid threats. Arguments presented in the article substantiate research on hybrid operations, which, used by the state or non-state organisations, are a real threat to security in Europe and the world.

Key words: security, hybrid warfare, terrorism, Russia, Ukraine.

Introduction

The beginning of the twenty-first century has been characterised by new challenges in the field of international security. The end of the Cold War has not meant the elimination of internal or regional sources of conflict and has not provided a lasting peace in the world. As experts say, the international community is facing not only a direct armed conflict but a variety of military operations. The insurrections, the guerrilla actions, the internal wars and other varieties of small-scale conflicts will soon become common variations of the conflict in the new world order. Therefore, it can be assumed that different states will be involved directly or indirectly with new varieties of armed conflict[1] in the near future. The experience of many countries learned from fighting against an undetermined opponent, devoid of clear organisational structures and not complying with standard tactics give another dimension to the perception of conducting military operations. This has undermined the security paradigm based on the key meaning of technology in the organisation of the state's defence systems, as well as ways of conducting military operations[2]. For several years, in modern publications on the subject of security science, the problem of asymmetric and hybrid modern armed conflicts has been dealt with. The issues related to those problems are permanently becoming a matrix of strategic thinking. In many of the world's armies at the strategic level, analysis and studies of the experience gained from both small local conflicts in the past, and in multinational operations at the beginning of the twenty-first century[3] have been carried out. The attempts to find new approaches to maintain the balance of international security are increasingly dictated by the gap between the ideas of the period after the „Cold War" and the current practice of the security policies of many countries. The main problem, it seems, is the inability to overcome stagnation faced by the contemporary art of war as a result of the increasing complexity of conflicts and the ways and methods of their settlement[4]. This means such conflicts where the factors which determine the final success or superiority are not technological, and feature neither organisational perfection nor psychological advantage. An accurate prediction of the future, especially armed conflict, is extremely difficult due to the growing dynamism and the unpredictability of response actions by sides in a conflict. This fits in with the old maxim that „(...) the war is full of passion, inaccurate information and error evaluation, and finally a lot happens therein by the chance"[5]. Nonetheless, based on the present trends, a thesis that different actors will fight for dominance in the modern world can be formulated. The number of places where armed conflicts can occur will increase. There will be an increased risk to the safety and the interests of NATO's countries and states aspiring for membership in it.

The above arguments justify the research on hybrid operations, which are used by the state and non-state and are a real threat in their dimension to security in Europe and the world.

The article is devoted to the theory and the practice of hybrid operations, which affect the security of the international environment. The results of the analyses referred to the problem defined in the form of questions: what expresses the essence and the evolution of hybrid operations? What is the modern nature of hybrid operations?

The nature and the evolution of hybrid operations

The etymology of the term „the hybridity" is derived from the Latin word hybrid, meaning „crossbreed", an individual formed from the crossing of two genetically different individuals belonging to different species, varieties or races[6].

[1] M. Wrzosek, *Zagrożenia militarne a bezpieczeństwo Europy* [w:] Kwartalnik Bellona 2012, nr 4, s. 7.

[2] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011, s. 4.

[3] B. Balcerowicz, *Pokój i nie pokój na progu XXI wieku,* Wyd. Bellona, Warszawa 2002, s. 17.

[4] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna* [w:] Asymetria i hybrydowość – stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011, s.11.

[5] C. Clausewitz, *O wojnie,* Lublin 1995, s. 15. *Wojna jest* [...] *aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli.* Sformułowanie to zawiera dwa istotne aspekty. Po pierwsze, wojna zakłada przemoc, co odróżnia ją od innych form rywalizacji politycznej czy gospodarczej. Po drugie jest narzędziem służącym do osiągnięcia **celu politycznego**, dalszym ciągiem stosunków politycznych kontynuowanych innymi środkami.

[6] *Słownik wyrazów obcych,* PWN, Warszawa 1980, s. 290.

In other words, „the hybridity" can be defined as „... the property created as a result of intersection or mixing features, elements belonging to often structurally different and genetically distant opposing objects, organisms, or states. Therefore, hybridisation means merging essentially different characteristics around one separate entity, while retaining the specific properties determining the genre „superior" by the new hybrid organism in terms such as e.g. resistance to diseases, durability and greater adaptability „[7]. In the simplest terms, *the hybrid* is a combination of elements from different origins and / or structures. In the event of conflicts or the hybrid wars, they are a mix of the most effective forms and methods of operations.

The hybrid conflict as a specific combination of conventional and irregular operations has been known for the centuries. Since ancient times, one of the main determinants for conducting military operations has been proper reconnaissance of the current situation and adapting one's own activities to it[8]. It is important that in the unchanging nature of war, the ways and methods of its conducting, as well as winning, have been fundamentally transformed[9]. The modern armed forces are facing new challenges, risks and threats, including asymmetrical ones. The hybrid operations may be a combination of selected forms of symmetrical[10] and asymmetrical[11] war operations, in which forces are lead classical military operations and, at the same time, must make decisive parallel attempts to gain control over the local population in a combat zone, ensuring security and stability[12]. At the moment, the international environment is faced with a new challenge, which is to prevent the threat of a possible conflict stemming from a hybrid conflict. This requires a new, more detailed and comprehensive approach. The one-dimensional territorial image of war has been replaced by a multi-dimensional, multi-level complex and non-military and military activities aimed at achieving different objectives simultaneously. The traditional battlefield has been replaced by a military confrontation space. The roles filled by the participants of the armed conflict are not defined and assigned on a permanent basis, and often change in a radical way, dispersing efforts to pacify/stabilise or destabilise the public space. Currently, developing trends, and particularly the experience from recent conflicts involving Hezbollah and Hamas, and the operations in Afghanistan, and more recently the aggression of Russia in Ukraine, entitle one to formulate a thesis that the traditional classification of wars[13] has lost its relevance and does not correspond to reality. Strategists and military analysts point to increasingly blurred boundaries between the various models and categories of wars and connect to various forms of military action and tactics used[14]. There is also some convergence, consisting in blurring the boundaries between the associated skills and abilities to the state of non-state actors. This process is further accelerated by globalisation and the impact of new technologies. With regard to armed conflicts, hybridisation can be understood as the coexistence of elements of the „old" and „new" wars, classical military conflicts,

[7] A. Gruszczak, *Hybrydowość współczesnych wojen* (...), s. 11.

[8] Sun Tzu, *Sztuka wojny*, Gliwice 2004.

[9] J. Keegan, *Historia wojen,* Warszawa 1998, s. 11.

[10] „Asymetria" i „asymetryczność" są pojęciami określającymi różnorodne formy dysproporcji, zróżnicowania i dysharmonii, które w sposób naturalny lub zamierzony występują w otoczeniu przeciwstawnych sobie rzeczywistości. Dotyczą one zarówno ich sfery materialnej, to jest gospodarczej, ekonomicznej, naukowej, technicznej, informacyjnej i militarnej, jak również sfery duchowej – obejmującej aspekty kulturowe, religijne czy etyczne. Wzajemna symetryczność czynników (...) minimalizuje możliwość generowania zagrożeń oraz stabilizuje względnie trwałą równowagę ich zmian. Oznacza to, że „asymetryczność" jest antonimem stanu „symetrycznej" równowagi, odnoszącej się do całokształtu zjawisk społecznych i cywilizacyjnych oraz ich wzajemnych związków, relacji i oddziaływań. Według: P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, AON, Warszawa 2003, s. 11.

[11] Konflikt asymetryczny cechuje się odmiennością celów oraz metod działania, wykorzystywanych środków i zasobów, a także rozbieżnością wartości, norm i zasad, którymi kierują się walczące strony. Przeciwsymetryczność (*dissymmetry*) polega na braku równowagi pomiędzy uczestnikami konfliktu pod względem zaangażowania w konflikt oraz sposobów wykorzystania posiadanych zasobów na płaszczyźnie operacyjnej, nie zaś zróżnicowania, co do samego rodzaju zasobów czy też zasad prowadzenia konfliktu. Rozumiana w ten sposób asymetria w konflikcie (*asymmetry within warfare*) nie wpływa na zmianę charakteru konfliktu z symetrycznego na asymetryczny (*asymmetric warfare*), lecz stanowi wspomnianą rzecz ujmując – przewagę militarną. Według: J. Russel, *Asymetric Warfare* [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Wyd. Strategic & Combat Studies Institute, Shivenham, 2002 r., s. 120–122.

[12] J.J. Mc Cuen, *Hybrid Wars* [w:] Military Review 2008, nr 2, s. 108.

[13] B. Balcerowicz, *Konflikty zbrojne i wojny w zmieniającym się środowisku bezpieczeństwa*, Warszawa 2004, s. 34.

[14] M. Boot, *War Made New: Technology, Warfare and the Course of History: 1500 to Today*, Gotham Books, New York, October 2006, C. Gray, *Another Bloody Century: Future Warfare*, Phoenix, London 2005.

„postmodern" wars, clashes of national armies and asymmetrical conflicts, the superb military technology and primitive weapons, the fight for territory and resources, and disputes about identity and values, and the confrontation of destructive - parasitic eastern civilisation with the Christian civilisation of the West[15].

The hybridity in relation tostrategic objectives, operational planning and conduct of operational-tactical activities is the dysfunctional hallmark. It makes it difficult to integrate the various formations, units and relationships of operational-tactical forces, and thus prevents effective, uniform command in real time. According to Thomas Huber, author of the concept of war as a complex product, the use in combat operations of detachments of the armed forces and dispersed irregular forces will not be effective without a centralised, network-centric military operations control and proper diagnosis of the military confrontation space[16].

The comprehensive definition of hybrid operations must take into account all the possible experience of this type of activity in recent decades. The simplistic assertion that hybrid war is guerrilla activities + modern technology is only part of the truth and can only refer to non-state actors. The similar activities performed by the state are much wider. The spectrum of methods used by the state may stretch from the traditional practice of armed struggle using non-conventional cyber weapons and information warfare, to special services operations, which are responsible for the disintegration of society, through the activation of the impact of the agencies[17], as well as terrorism and the promotion and use of criminal activity. The state will be subordinated by all activities to the overriding of its political purpose.

Significant achievements in research on hybrid operations were made by Frank Hoffman. He defined the modern model of hybrid warfare from the perspective of the experiences from recent conflicts in the world. The hypothesis that the war in Lebanon in 2006 made it clear that in the „theater of war" the type of participant combining the features of conventional and irregular actor held a permanent place served as a starting point. Pursuant to the provisions adopted in the 2005 edition of the National Defence Strategy USA, Hoffman put forward a proposal that much needs to be done to precisely identify the threats and security challenges of the modern world. However, the dynamics of the changes make it necessary to become a lot more common than previously verifying the updates position[18]. He also points out that the hybrid wars feature is the prevalence of the acts of terrorism and various forms of crime[19]. On the other hand, the Latvian analyst, Janis Berzins, called the hybrid war *the fourth generation war*[20]. However, according to the views of the Russians, it is *a new generation war*. According to the head of the General Staff of the Russian Armed Forces, the rules of war have changed fundamentally in the wars of the next generation. There is an increased role for non-military means (economic, cultural) taken to achieve political and strategic objectives. Such measures are significantly more efficient than traditional military methods[21]. In

[15] A. Gruszczak, *Hybrydowość współczesnych wojen* (...), s. 11.

[16] T.M. Huber, *Compound Warfare: A Conceptual Framework, Compound Warfare: That Fatal Knot,* U.S. Army Command and General Staff College Press, red. T.M. Huber, Fort Leavenworth 2002 r., s. 1–7.

[17] A.I. Kuk, *Kanwa wywiadu agenturalnego*, Warszawa 1994, s.19.

[18] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007, s. 12.

[19] F.G. Hoffman, *Conflicts in the 21st Century: The Rise of Hybrid Wars,* Potomac Institute for Policy studies, Arlington 2007 r., s. 14; R. Peters, *Hybrid threats: reconceptualizing the evolving character of modern conflict* [w:] Strategic Forum 2009 r., nr 240, s. 5.

[20] Termin *wojna czwartej generacji* po raz pierwszy był użyty przez strategów wojskowych w latach 80. dla scharakteryzowania przyszłych kierunków ewolucji wojny. Ewolucja dokonywała się na przestrzeni historii i obejmowała kilka faz. Wojna pierwszej generacji była zdominowana przez armie masowe i polegała na zadawaniu strat w stanie osobowym, a jej kulminacja przypadała na wojny napoleońskie. Dominacja i siła ognia charakteryzowały wojnę drugiej generacji, a jej przykładem może być pierwsza wojna światowa. Wojna trzeciej generacji, dzięki wykorzystaniu nowoczesnych technologii i rozwojowi przemysłowemu była zdominowana przez manewr, zastosowany na szeroką skalę przez Niemców w czasie drugiej wojny światowej. Ewolucja wojny czwartej generacji czerpała z rozwoju politycznego, społecznego, ekonomicznego i technologicznego, który miał miejsce po zakończeniu drugiej wojny światowej. Wszystkie zmiany zostały zaadoptowane i wykorzystane przez nowego, niekonwencjonalnego przeciwnika (http – patrz: bibliografia); T.X. Hammes, *Insurgency: Modern Warfare Evolves into a Fourth Generation* [w:] Strategic Forum, No. 214, January 2005 (http – patrz: bibliografia). S.C. Williamson, *From fourth generation warfare to hybrid war*, U.S. Army College, Carlisle Barracks, Pennsylvania 2009, s. 22.

[21] W. Gierasimow, *Rola Sztabu Generalnego w organizacji obrony kraju w związku z nowym Statutem Sztabu Generalnego zatwierdzonym przez prezydenta Federacji Rosyjskiej* (http – patrz: bibliografia).

the course of hybrid operations „... asymmetric action is broadly applied, allowing the advantage of an opponent in the armed fight to be mitigated. These include the use of special forces and internal opposition, to create a permanent front throughout the enemy country, the impact of information and the ever-changing forms and methods of interaction"[22]. In the hybrid conflict according to the Russians, there is no difference between war and peace, in the classic sense of these words, and between uniformed personnel and undercover operations. „This combination, especially at a time *when wars are not declared, but simply started,* is very different from that which traditional theorists of war are focused on. The hybrid war has the potential *to change completely the stable country in the arena of the most intense armed conflict in a few months or even days*[23]. An important element in the new generation war, as seen by the Russians, is the blurring of distinctions between the levels of strategic, operational and tactical activities, and between offensive and defensive operations. The non-contact and at a distance impact on the opponent becomes the main way to achieve the objectives of the fight and operation.

On the other hand, in the NATO documentof 25 August 2010 entitled *Bi-Sc Input To A New Nato Capstone Concept For The Military Contribution To Countering Hybrid Threats*[24], an assessment of the risks to the security of the global hybrid in the 21st century can be found. The NATO study[25] indicates that a future opponent will combine different models of war and simultaneously apply a combination of conventional, irregular, terrorist and criminal operations[26], referred to as *the hybrid war*[27] or *the hybrid threat.* It has been determined that the contents of these activities will be the ability to combine conventional capacity with the tactics of irregular armed formations, terrorist and criminal activities. The essence of criminal activity[28], in this case, would be destabilising the functioning of local authorities and supporting the rebels and all dissidents, by providing highly technologically advanced weapons and ammunition and financial resources. The criminal groups operating as a hierarchical structure in an urban environment will provide both facilities and support for the wider hybrid activity which also includes narcoterrorism. It is assumed that the opponent will apply all the above fight models at the same time[29] to gain an advantage. A multi-model form of fighting may be used with one or more formations, individually or simultaneously, at different times and in a different dimension. However, the action will always be coordinated at the operational and the tactical level and will usually provide a battle space to achieve synergies. The opponents will achieve a high efficiency of operations because they operate in a complex and comprehensive environmental dimension, both in the physical and mental domain. The hybrid opponent will effectively employ technologically advanced systems and use them in a specific way in order to achieve their own goals[30]. The research has indicated that, in the future operational environment, the hybrid threat directed at the most vulnerable points of the armed forces of the countries participating in the conflict or the critical infrastructure of the state parties to the conflict will dominate. It is expected that the next opponent will use all possible forms and methods of warfare and diverse tactics. It can be assumed that in the event of a conflict and conduct interventions, the opponent will be *blended* into the local community and prefer long-term, harassing rebel and guerrilla actions, based on the use of ambushes, improvised explosive devices and rocket fire. These may also include the use of high-tech weapons systems while keeping classic terrorist activities and actions in cyberspace aimed at preventing both

[22] Ibidem, s. 3.

[23] Ibidem, s. 4.

[24] BI-S.C. *Input to a new NATO capstone concept for the military contribution on countering hybrid threats*, International Military Staff, 29 September 2010.

[25] *Multiple Futures Project...*, s. 34.

[26] Ibidem, s. 47.

[27] Według Departamentu Obrony USA, który dość ogólnie to zdefiniował, „ (...) *działania hybrydowe, nieregularne działania wojenne to preferowanie niebezpośrednich i asymetrycznych metod, które mogą łączyć w sobie cały zestaw możliwości, zarówno wojskowych jak i innego typu, a mających na celu doprowadzenie do erozji siły przeciwnika, jego wpływów i woli*". Według: The Missile Defense Program 2009–2010, Missile Defense Agency, Department Obrony (http – patrz: bibliografia).

[28] P.J. Smith, *Terrorism in the Year 2020: Examining the Ideational, Functional and Geopolitical Trends that Will Shape Terrorism in the Twenty-First Century*, NSDM Department, US Naval War College, Newport, USA, March 2008, s. 59 (http – patrz: bibliografia).

[29] F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007, s. 7–8 (http – patrz: bibliografia).

[30] W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Naval Postgraduate School, Monterey, June 2002 (http – patrz: bibliografia).

weapons systems and civil systems of the critical infrastructure[31] from operating. In addition, it must be taken into account, as stated earlier, that criminal activity is likely to be destructive for the functioning of a state. It can be assumed that this type of activity could be used to provide a means to carry out irregular or terrorist activities. On the other hand, the development of technology will mean it becomes ever more difficult to distinguish regular from irregular activities, terrorist from ordinary citizen, and kinetic from non-kinetic action. *The hybrid* operations should be combined, as well as the means employed and the methods of their use. In recent years, there has been an increase in the number of conflicts in which non-state actors have imposed strategy, for example Hezbollah, Hamas and Al Qaeda. Currently, this trend could be stopped with the huge economic and military potential of the Russian Federation.

In conclusion, the common element of the above definitions and views is that hybrid conflict parties aspire to seek the approximation of used methods, means and ways of conducting military and non-military operations in order to maximise synergies, allowing them to achieve a sustainable advantage over an opponent. An advantage is a factor causing a structural change in the space of confrontation. Based on the results of the study. it can be concluded that the process is noticeably blurring differences in the way components of conflicts are conceived, diagnosing and analysing the nature and extent of the impact of the conflict on the regional and international security environment. The existing patterns in any military doctrine up to now have lost their relevance and it is not possible to directly translate them into the present reality in the face of the hybrid enemy.

The contemporary dimension of the hybrid operations

An example illustrating the full range of the methods and forms of hybrid war, where the weaker enemy use them against the stronger opponent, may be the long-term conflict between Israel and Hezbollah[32]. Based on Israel's experience from the last decade, it can be argued that the irregular capability transformation used by non-state actors occurs in the hybrid ability applied by states[33]. The future challenges will be related to the fact that a potential opponent will have a much more complex range of organisational structures and will use a more complex strategy and tactics than the one that the Israeli army encountered in 2006[34]. Hezbollah clearly proved that non-state actors are able to make a reliable assessment of strategic opportunities of armies referred to as *western* and effectively resist their most modern capabilities.

In summary, it can be stated that the continuous and uninterrupted conflict of Israel with its non-state enemy shows the size of the intelligence, military and information gathering of the Israeli army and the special services, which must be used to create the conditions to neutralise and eliminate the organisation using terrorism. Hezbollah, with support from Iran and rooted in Lebanon, has become a serious threat not only to Israel, but also to the Middle East. The Hezbollah victory over Israel's army in 2006 showed it iss effective as an organisation, and, on the other hand, a threat to neighbouring countries[35]. The further process of

[31] F.G. Hoffman, *Conflict in the* (...), s. 28.

[32] Hezbollah (tłum. „Partia Boga") jest szyickim ugrupowaniem polityczno-militarnym, które zostało stworzone na terenach Libanu w 1982 r. po izraelskiej operacji „Pokój dla Galilei", jako narzędzie do walki z głównym wrogiem Arabów – Izraelem. Swoje istnienie zawdzięcza irańskiej pomocy w postaci przysłania do Libanu reprezentacji instruktorów z Korpusu Strażników Rewolucji. Od tego czasu pozycja Hezbollahu stała się na tyle znacząca, że na terenie Bliskiego Wschodu stał się jednym z ważniejszych aktorów niepaństwowych oraz oponentem Izraela. Dzięki swojemu działaniu posiadł niebezpieczną zdolność wpływania na region. Według: M. Jadwiszczok, *Antyizraelskie ugrupowania terrorystyczne i ich zwalczanie*, Toruń 2010, s.104. oraz R. Ożarowski, *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011, s. 39.

[33] D.E. Johnson, *Military Capabilities for Hybrid War, Insight from the Israel Defense Force in Lebanon and Gaza*, RAND Corporation, 2010, s. 5 (http – patrz: bibliografia).

[34] M.B. Stannard, *Hezbollah Wages New Generation of Warfare* [w:] San Francisco Chronicle, 6 August 2006 (http – patrz: bibliografia).

[35] Za szczyt konfliktu Izraela z Hezbollahem uznaje się rok 2006. Po wycofaniu się armii izraelskiej z Libanu Hezbollah przesunął obszar swojego działania bezpośrednio pod granicę libańsko-izraelską. Od tego momentu przypuszczał kolejne ataki na osiedla izraelskie. Mimo to do 2006 obie strony toczyły ze sobą potyczki bez większej eskalacji na szerszy obszar państwa. Można uznać, że dotychczas Hezbollah wiedział, do jakich granic może się posunąć oraz jakich reperkusji może oczekiwać ze strony przeciwnej. Dopiero zasadzka z 12 czerwca 2006 roku na patrol izraelskich żołnierzy sprawiła, że rząd izraelski pod przywództwem Ehuda Olmerta podjął decyzje o przeprowadzeniu operacji zbrojnej przeciwko Hezbollahowi. Przewaga jakościowa armii Izraela nie przełożyła się na skuteczność. Nie udało się wyeliminować najważniejszych przywódców Organizacji oraz uszczu-

globalisation and the development of the military capabilities of Hezbollah can develop in a much more dangerous direction. The question of the further evolution of the organisation is certainly open and cannot be underestimated.

The hybrid challenges are not limited to non-state actors. Lessons learned from operations in Iraq and Afghanistan, and more recently with the Ukrainian crisis, suggest that countries can turn regular units of the armed forces into irregular formations that will have classic abilities and adapt new tactics and then support regular units. Therefore, states cannot be seen through the prism of their classical armed forces only and non-state actors be associated with irregular activity only, because, in the future, hybrid armed forces can be used in an unpredictable way[36].

An example where the state as a stronger party conducts hybrid war with the weaker enemy is the Russian aggression in Ukraine. The hybrid war in Ukraine can be broken down into four stages: a political diversion, building the separatist's social and political position, an armed intervention and a deterrence by demonstrating the potential of unconventional forces. The characteristic of this conflict is that the above stages often overlap each other and have a different intensity. Despite clear evidence of the participation of Russian regular armed forces, the authorities officially deny involvement in the conflict[37].

The NATO experts argue that the crisis goes far beyond the borders of Ukraine. Russian authorities believe that the defence of ethnic Russians is not the responsibility of the countries in which they live and is not subject to their laws, the government or the constitution, but is subject to Russia. This approach by the Russian authorities to ethnic Russians, which, according to Kurt Volker, the US ambassador to NATO, is not only a „breakthrough in the understanding of international law, but also a hybrid war technique, called *the new approach*, which has been applied previously in Estonia in 2007, Georgia in 2008. [...] The concept of slow but systematic action causes a violation of sovereignty, and has been part of a strategic landscape well-known in Russia for some time. [...]. Sometimes this involves more open and obvious moves, sometimes moves are more subtle, an economic struggle, sometimes - cyber-attacks are carried out under the guise of the actions of independent activists". In his view, „... a set of the hybrid war tactics has been used by Russia for at least 5- 6 years"[38]. There are many good reasons to conclude that –this conflict in Ukraine is still in the development phase. The time that has elapsed from the start of the Russian aggression against Ukraine allowed both Polish and NATO analysts to work out the scenarios and methods of the hybrid war conducted by Russia. The element that initiated it was activity in the information warfare sphere. When analysing the scenario of Russian aggression in Ukraine, the idea that the Russian aggression only began with protests on the Maidan can be questioned. There are many indications that a Russian attack started well before President Viktor Yanukovych left the country. The military participating in the conflict were dressed, in fact, without any identification they were the Russian military airborne troops was preceded by an information offensive in the Crimea and Donbas region[39]. In the years preceding the conflict, Russia launched a media expansion into Ukraine. The weapon that was used to destabilise the information structure of the Ukrainian media turned out to be Russian media companies, which were used to coordinate the information infiltration of Ukraine. The expansion proceeded through the buying of shares in the media from Ukrainian oligarchs. In this way, Ukrainian society began to receive information that illuminated the situation from the point of view of Russia's interests, not Ukraine's. The public has been manipulated by the media. On the ground, thus prepared, the integration of the pro-Russian environment and activation of Russian intelligence overlapped[40]. Some key forms of attack and the main goals of the intervention can be extracted. The first is the disinformation. The contribution of

plić jej zasobów. Konflikt trwający ponad miesiąc pokazał, że oprócz siły militarnej Hezbollah może być równorzędnym przeciwnikiem w wojnie informacyjnej. Konflikt ten nie pozwolił Izraelowi na jednogłośne obwołanie się zwycięzcą. Pokazało to władzom izraelskim, że pokonanie grup militarnych Hezbollahu nie jest do końca możliwe. Według: K. E. Schulze, *Konflikt arabsko-izraelski*, Warszawa 2010, s. 142.

[36] M. Williams, *The Future* (...), s. 9.

[37] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond* (http – patrz: bibliografia).

[38] Przegląd NATO. Magazyn –polska wersja językowa. (http – patrz: bibliografia).

[39] J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku* [w:] Punkt widzenia 2014, nr 42, wyd. OSW, Warszawa 2014, s. 23.

[40]

Russian soldiers is masked by creating volunteer separatist forces. The concentration of Russian troops smuggled into Ukraine took place under the guise of exercises in the border districts. While this method can be classified as traditional and was used in the war with Georgia[41], *the novelty* was the preparation for war in cyberspace. From the beginning of the aggression, the network revealed hundreds of sites and community portals. Seemingly, „independent and neutral" information about the events in fact interrelated and coordinated the active disinformation[42]. A very effective method was a rumour confirmed by the information submitted by the Russian politicians and army. It has been observed that the purpose of the transfer of such information is to create an atmosphere of intimidation. Both the mobilisation of the Ukrainian army, which took place in an atmosphere of fear and distrust, as well the conduct of the military operations. The statement of one of the deputies of the Verkhovna Rada of Ukraine is an example of this, that „... the losses incurred under Debaltseve are a result of panic, the source of which was the Russian media bombarding the soldiers with information about them being surrounded, which turned controlled retreat into a disorderly escape"[43]. Russia uses the weakest points of the Ukrainian side. The aim of information attacks is to promote negative phenomena in society and the power elite of Ukraine. The phenomena, such as widespread corruption, the powerful nationalism prevalent in the western regions of Ukraine and the discord between the ruling president and prime minister's camp are the basic objectives of the information warfare attacks.

The information war against Ukraine is accompanied by similar actions of the Russian Federation in Europe and the world. Russia conducts an intensive information campaign aimed at strengthening the divisions in the European Union and NATO, as to the necessity and scope of assistance to Kiev and the reasonableness of sanctions against her. Russia is using interpersonal contacts with Western politicians, economic incentives and media impact[44]. The information exaggerates the Russian version of events, and it seems that the overall aim is to divide public opinion. The key point of this strategy is to create an image of Russia as a victim of cynical game of the Western establishment, accused on this occasion of a complete distortion of the image of the President of Russia and the causes and course of the Ukrainian conflict.

Ukraine is losing the information war. The anti-Ukrainian institutions are still in the early stages of their formation. The situation is further complicated by the fact that the security system and international law does not provide for such a sphere of activity of war. Neither the UN Charter nor the OSCE founding documents define the concept of information warfare or monitoring methods and do not impose a ban on its conduct. The international law is helpless in the face of Russian aggression, as exemplified by the lack of response of the OSCE mission to Ukraine to the evidence on the activities of Russian disinformation, and even the participation of regular units of the Russian army in the conflict. The international observers are simply helpless figureheads.

Turning to Russia's military participation in the conflict and the beginning of the war, it can be argued that the Russian side entrusted a dominant role in the development plan of the conflict in Ukraine and then directed its course to the special services. In conjunction with the support of regular units of the Russian Federation of Armed Forces, there was the situation of absolute military superiority in the region of the conflict. At present, it is estimated that in the Donbass region and the border with Ukraine 44 battalion tactical group (BTG) is dislocated. It is estimated that the capacity of the Russian army during the month allows their number to be increased to 80, and within 3 - to 120. The Russian side, in contrast to earlier intervention in Chechnya and Georgia, directs subunits to Ukraine with the fewest number of conscripts[45]. The military actions are carried out primarily by the special, airborne and specialised forces, supported by mercenaries (Chechens, Cossacks) and paid volunteers, as well as trained and retrofitted local separatists. The process of rotation of forces and equipment is continuous and fluctuates within 2-3 rail transports daily. Up

[41] Raport OSW, *Zmiany w potencjale militarnym Federacji Rosyjskiej (po rosyjskiej operacji wojskowej w Gruzji)*, OSW Warszawa 2009, s. 4.

[42] J. Darczewska, op. cit., s. 28.

[43] R. Cheda, *Rosyjska wojna informacyjna – lekcja z Ukrainy* (http – patrz: bibliografia).

[44] *Sankcje i Rosja*, red. J. Ćwiek-Karpowicz, S. Secrieu, Wyd. PISM Warszawa 2015, s. 99.

[45] Raport OSW, op. cit., s. 35.

to the end of January 2015, in the Donbas region, the Russians possessed 16 BTG, 340 tanks, 720 BMPs and armoured transporters (IFV/APC), 173 artillery guns and 92 multiple launch rocket systems (MLRS); Separatists - 10 BTG, 340 tanks, 329 IFV/APC, 372 artillery guns and 472 MLRS[46]. The accumulated military potential provides complete operational freedom to the Russian side. However, even with such absolute superiority, the Russians used humanitarian convoys as one of the elements for camouflaged retrofitting of the separatist forces. The correlation was observed between Russian humanitarian convoys and the increase of intensity of the separatists' armed activity.

Based on the survey, it can be concluded that the plan for the rapid breakdown of the Ukrainian forces and overthrowing the government in Kiev was abandoned in favour of a gradual weakening of the Ukrainian state and its armed forces combined with a systematic increase of the territorial gains. The crisis situation is further complicated by the fact that the US and Western European countries clearly instructed the Ukrainian authorities to limit defence activities in such a way that they are not recognised by the Russians to be provocative and do not provide a pretext for a further escalation of the conflict[47]. The passive attitude of the Ukrainian security forces in conjunction with the lack of immediate military support from Western countries, including, in particular, the necessary intelligence and the critical military capabilities, has led to the strengthening of the separatist forces. According toProfessor Karber[48] „... in the near future, there is no possibility of Ukraine recovering not only the Crimea, annexed by Russia over the objections of the West, but also the other areas in the east of the country, over which the authorities in Kiev lost control. What's more, the current ceasefire threatens Ukraine with a complete break away and further territorial losses"[49].

In summary, it can be assumed that the lack of a firm response from the West, the declining defence capabilities of the Ukrainian armed forces and the constant reinforcement of the Russian military presence in Ukraine may, in the future, lead to a further escalation of the conflict. Russia may treat Ukrainian „success" as a template for further use. It becomes clear that not only Ukraine is threatened, but any country that has a Russian minority. The methods used by the Russians in the hybrid war in Ukraine can be transferred to other areas, including in the Baltic States. It can be assumed that the principal and effective operation against Russian aggressive inclinations remains the unity of Western countries and support for Ukraine with critical military capabilities.

The experience from previous conflicts, in which elements of hybrid operations were used on a large scale, show that the potential of non-state actors, especially in the sphere of military influence, is growing. Moreover, the motivation in the aggressor countries for use of non-traditional forms and methods of conducting the armed struggle is increasing. The hybrid threats have become very effective, not only against coalition forces, for example in operations in Iraq and Afghanistan, but also against the big, heavy and hierarchical international security organisations (NATO, OSCE, UN), which in principle are very stiff in the mental and doctrinal aspects. In the theoretical outline, a need to address hybrid threats is recognized by the new NATO Strategic Concept[50] pointing to the development of cooperation in order to fight the unconventional threats. Practically, the present lasting conflict in Ukraine verifies the records adopted so far and the perception of the hybrid war, which was usually carried out by the weaker side. The power of the Russian state, combined with elements of hybrid war, has demonstrated the weakness of the international security institutions and has questioned the international agreements established so far. While, theoretically, most experts put forward the opinion that if Russian aggression does not halt at this stage in Ukraine, it will result in an increasing threat of destabilisation of the entire region of Central and Eastern Europe, and practice tends to show the trends related to procrastination. Therefore, it seems there is no decision by the US President and the leaders of the Western European

[46] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond.* (http – patrz: bibliografia).

[47] Ibidem (http – patrz: bibliografia).

[48] Prof. Phillip Karber – dyrektor amerykańskiego konserwatywnego think-tanku Potomac Foundation oraz wykładowca Georgetown University.

[49] The Russian Military Forum. *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond* (http – patrz: bibliografia).

[50] *Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Organisation,* NATO Public Diplomacy Division, Brusseles – Belgium 2010, s. 3, 5, 10.

countries for the provision of the necessary military support to Ukraine, which is increasingly criticised by the independent opinion institutions.

Conclusions

Based on the survey, it can be stated that the essence of t hybrid operations is to combine several forms and methods of action, simultaneously on several levels. First of all, direct military action, information warfare, including propaganda in the area of the attacked state and in the international arena and the wide application of economic and political blackmail. The evolution of the hybrid conflict, especially over the last decade, has been very dynamic. The hybrid challenges are no longer confined exclusively to non-state actors and the model in which a weaker opponent uses this kind of action against a stronger one. Lessons learned from operations in Iraq and Afghanistan, and most of all the armed conflict in Ukraine, show that countries can turn regular units of the armed forces into irregular formations that will have the skills and adapt classic unconventional methods of operation and then support regular units. Therefore, states cannot be seen through the prism of classical armed forces only and non-state actors only through irregular operations. The contemporary practice of hybrid operations in the armed conflict in Ukraine has revealed that there has been a diametrical change in existing hybrid operations. For the first time, a much stronger opponent, world-class power Russia, is using the full spectrum of forms and methods of hybrid operations with a weak enemy who is unable to defend the integrity of its territory of Ukraine. The armed conflict not only showed the weakness of the Ukrainian state, but more importantly the failure of the international security institutions: NATO, OSCE and the UN. The development of the hybrid conflict in Ukraine undoubtedly threatens 'right flank' states of NATO. The methods used by the Russians in the hybrid war in Ukraine can be transferred not only to the area of the states created after the collapse of the Soviet Union but also to the Baltic States, Poland and Romania. The security situation has not only disturbed the region of Central and Eastern Europe but directly affects international security.

Bibliography

Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Organization, wyd. NATO Public Diplomacy Division, Brusseles – Belgium 2010.

Asymetria i hybrydowość - stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, Wyd. BBN, Warszawa 2011.

Balcerowicz B., *Pokój i nie pokój na progu XXI wieku,* Wyd. Bellona, Warszawa 2002.

Balcerowicz B., *Konflikty zbrojne i wojny w zmieniającym się środowisku bezpieczeństwa*, Warszawa 2004.

BI-S.C. *Input to a new NATO capstone concept for the military contribution on countering hybrid threats*, International Military Staff, 29 September 2010.

Cheda R., *Rosyjska wojna informacyjna - lekcja z Ukrainy.* http://wiadomosci.wp.pl/kat,1356,title,Rosyjska-wojna-informacyjna-lekcja-z-Ukrainy,wid,17301467,wiadomosc.html?ticaid=11494f&_ticrsn=3 [Dostęp: 12.02.2015 r.].

Clausewitz C., *O wojnie,* Lublin 1995.

Cole R., Irregular threats and challenges, [w:] Marine Corps Gazette 2010, nr 1.

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku,* [w:] Punkt widzenia, Nr 42, OSW Warszawa 2014.

Freier E., The defense identity crisis: It's a hybrid world, Parameters 2009 r., nr 3.

Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.

Gentile G.P., The imperative for an American general purpose army that can fight [w:] Orbis 2009, nr 3.

Glenn R.W., Thoughts on „Hybrid" Conflict [w:] Small Wars Journal, http://www.smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf [Dostęp: 12.02.2015 r.].

Gierasimow W., *Rola Sztabu Generalnego w organizacji obrony kraju w związku z nowym Statutem Sztabu Generalnego zatwierdzonym przez prezydenta Federacji Rosyjskiej.* http://www.avnrf.ru/index.php/vse-novosti-sajta/620-rol-generalnogo-shtaba-v-organizatsii-oborony-strany-v-sootvetstvii-s-novym-polozheniem-o-generalnom-shtabe-utverzhdjonnym-prezidentom-rossijskoj-federatsii [Dostęp: 12.03.2015 r.].

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna* [w:] Asymetria i hybrydowość - stare armie wobec nowych konfliktów, red. W. Sokoła, B. Zapała, wyd. BBN, Warszawa 2011.

Hammes T., *Insurgency: Modern Warfare Evolves into a Fourth Generation*, "Strategic Forum", No 214, January 2005.
<http://www.scribd.com/doc/1569981/US-Air-Force-sf214>. [Dostęp: 08.02.2011 r.].

Hoffman F.G., *Hybrid vs Compound War: The Janus Choice – Defining Today's Multifaceted Conflict*, „Armed Forces Journal", October 2009. < http://www.armedforcesjournal.com/2009/10/4198658>. [Dostęp: 05.05. 2011 r.].

Hoffman F. G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies Arlington, Virginia, December 2007. <https://dde.carlisle.army.mil/documents/sis/docs/Hybrid_Wars.pdf>. [Dostęp: 08.02.2011 r.].

Hammes T., *The Sling and the Stone*, Minneapolis, 2006.

Huber T.M., Compound Warfare: A Conceptual Framework [w:] Compound Warfare: That Fatal Knot, U.S. Army Command and General Staff College Press, Fort Leavenworth 2002.

Johnson D. E., *Military Capabilities for Hybrid War, Insight from the Israel Defense Force in Lebanon and Gaza*, RAND Corporation, 2010.

Keegan J., *Historia wojen,* Warszawa 1998.

Kuk A.I., *Kanwa wywiadu agenturalnego*, Warszawa 1994.

Lasica D.T., Strategic Implications of Hybrid War: A Theory of Victory, school of Advanced Military studies, United Army Command and General staff College Press, Fort Leavenworth 2009.

Liedel K., Piasecka P., Aleksandrowicz T., *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Warszawa 2014.

Marks T. A., Counterinsurgency and operational art [w:] Low Intensity Conflict & Law Enforcement 2005, nr 3.

McKinley J., Al-Baddawa A., Rethinking Counterinsurgency, [w:] RAND Counterinsurgency Study, RAND Corporation, Santa Monica 2008.

Multiply Futures Project - Navigating Towards 2030, Allied Command Transformation, Final Report April 2009. https://transnet.act.nato.int/WISE/NATOACTRes/MultipleFu/file/_WFS/20090503_MFPfinalrep.pdf [Dostęp: 12.02.2015 r.].

Nemeth W. J., *Future War and Chechnya: A Case for Hybrid Warfare*, [w:] Naval Postgraduate School, Monterey, June 2002.

Ożarowski R., *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011.

Portal Gławred, http://inosmi.ru/glavred_info/ [Dostęp 12.03.2015 r.].

Przegląd NATO. Magazyn -polska wersja językowa. http://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/PL/index.htm [Dostęp: 01.03.2015 r.].

Russel J., *Asymetric Warfare*, [w:] *The Big Issue: Command and Combat in the Information Age*, red. D. Potts, Wyd. Strategic & Combat Studies Institute, Shivenham, 2002.

Schulze K. E., *Konflikt arabsko-izraelski*, Warszawa 2010.

Shirreff R., *Unity of purpose in hybrid conflict: managing the civilian/ military disconnect and operationalizing the comprehensive approach*, Chatham House, Londyn 2010.

Słownik wyrazów obcych, PWN, Warszawa 1980.

Smith P.J., *Terrorism in the Year 2020: Examining the Ideational, Functional and Geopolitical Trends that Will Shape Terrorism in the Twenty-First Century*, NSDM Department, US Naval War College, Newport, USA, March 2008.

Stannard M. B., *Hezbollah Wages New Generation of Warfare*, [w:] San Francisco Chronicle", 6 August 2006.

Sun Tzu, *Sztuka wojny*, Gliwice 2004.

The Missile Defense Program 2009-2010, Missile Defense Agency, *Departament Obrony* [Dostęp: 10.03.2015 r.].

The Russian Military Forum: *Russia's Hybrid War Campaign: Implications for Ukraine and Beyond.* http://csis.org/event/russias-hybrid-war-campaign-implications-ukraine-and-beyond [Dostęp: 12.03.2015 r.].

Williams M., *The Future Security Environment,* RUSI, 2008. <http://www.rusi.org/downloads/assets/Future_Security_RP_13_Feb_2008.pdf>. [Dostęp: 07.02.2011 r.].

Wrzosek M., *Zagrożenia militarne a bezpieczeństwo Europy*, [w:] Kwartalnik Bellona 2012, nr 4.

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

POTĘGA CYBERNETYCZNA PAŃSTW – POMIAR I ZASTOSOWANIE

dr Robert BIAŁOSKÓRSKI
Wydział Humanistyczny Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach

Streszczenie

Artykuł porusza problem pomiaru potęgi cybernetycznej państw na przykładzie dwóch modeli badawczych: modelu Cyber Power Index (CPI) oraz modelu A.M. Gomeza. Obie metody oparte są na analizie wskaźników, przy czym pierwszy model szacuje wyłącznie defensywną potęgę cybernetyczną, natomiast drugi zarówno jej wymiar defensywny, jak i ofensywny. Oba te wymiary cyberpotęgi stanowią obecnie główne determinanty kierunków poszukiwań rozwiązania ww. problemu badawczego. Ponadto model drugi służy do szacowania strategii państw w cyberprzestrzeni, spośród trzech wyróżnionych: – utrzymania potęgi cybernetycznej; – osiągania równowagi; – demonstrowania potęgi cybernetycznej. Prezentowane wyniki badań obu modeli różnią się dość znacznie, co potwierdza złożoność problematyki już w fazie koncepcyjnej i konieczność dalszych poszukiwań.

Słowa kluczowe: cyberprzestrzeń, potęga cybernetyczna, pomiar, model

Wstęp

Współczesna rewolucja informacyjna oparta jest na globalnej zależności od technologii informacyjno-komunikacyjnej (ang. *Information and Communication Technology*, ICT). Kształtujące się społeczeństwo informacyjne dysponuje coraz większymi zdolnościami i możliwościami oddziaływania w cyberprzestrzeni, stwarzającymi zarówno szanse, jak i zagrożenia. Dotyczy to wszystkich podmiotów systemu międzynarodowego, zarówno rządowych jak i pozarządowych. Każdy podmiot może być zarówno sprawcą, jak i ofiarą cyberzagrożeń, takich jak: cyberwojna, cyberszpiegostwo, cyberterroryzm i cyberprzestępczość[1], których identyfikacja stanowi jeden z głównych problemów cyberbezpieczeństwa[2]. W tej sytuacji problem pomiaru potęgi cybernetycznej stanowi jeden z kolejnych czynników istotnych przy szacowaniu potęgi państw. W artykule podjęto problematykę definiowania potęgi cybernetycznej państwa oraz metod jej pomiaru. Inspiracją do podjęcia badań był ich nowatorski charakter, brak opracowań w polskim piśmiennictwie naukowym oraz zakres zgodny z głównym kierunkiem zainteresowań naukowych autora problematyką zapobiegania konfliktom zbrojnym (ang. *conflict prevention*, CP) definiowanym jako: proces wczesnego ostrzegania i reagowania prewencyjnego, polegający na stałym monitorowaniu i analizowaniu rozwoju zdarzeń w rejonach ryzyka konfliktu zbrojnego (wczesne ostrzeganie) oraz bieżącym wypracowywaniu i podejmowaniu akcji prewencyjnych (reagowanie prewencyjne) w celu zapobiegania konfliktom zbrojnym[3]. Z uwagi na złożoność podjętej problematyki artykuł przedstawia jedynie zarys problemu badawczego, który wymaga pogłębionych studiów teoretycznych oraz badań empirycznych.

[1] Zob. R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

[2] Autor zaproponował konceptualną analizę cyberzagrożeń opartą na analizie czterech czynników: podmiotu atakującego, podmiotu atakowanego, celów oraz motywacji. Zob. R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century*, „Journal of Security and Sustainability Issues" 2012, nr 4, s. 255–258.

[3] R. Białoskórski, *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski* [w:] M. Sułek (red.), *Potęgometria*, t. II, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015, s. 52.

Pojęcie potęgi cybernetycznej

Definicja „potęgi cybernetycznej" jest ściśle związana z pojęciem „cyberprzestrzeni". Mattiolli Rossella uważa, iż trudno jest określić granice pomiędzy cyberprzestrzenią i cyberbezpieczeństwem, głównie ze względu na dynamiczny charakter cyberprzestrzeni i brak klasycznie pojmowanych atrybutów terytorialności[4]. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej definiuje bezpieczeństwo cyberprzestrzeni jako: (...) zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni"[5]. W literaturze przedmiotu cyberprzestrzeń jest w zasadzie definiowana, jako: 1) *globalna przestrzeń informacyjna*, rozumiana jako „przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi w sieć internetową"[6] lub „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie z uwzględnieniem wszystkich systemów komunikacji elektronicznej (w tym również klasycznej sieci telefonicznej), które przesyłają informacje pochodzące ze źródeł numerycznych lub przeznaczone do numeracji"[7] oraz 2) *strategiczny element systemu bezpieczeństwa państwa*, jako: „wrażliwy system – system kontroli państwa... składający się z setek tysięcy sprzężonych ze sobą komputerów, serwerów, przełączników i kabli światłowodowych, wprawiających w działanie infrastrukturę krytyczną"[8] lub „niezależna sieć infrastruktury technologii informacyjnej, obejmująca Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane procesory i kontrolery działające w krytycznej infrastrukturze przemysłowej"[9] lub „militarna przestrzeń operacyjna (obok: lądowej, powietrznej, morskiej i kosmicznej)"[10]. Biorąc powyższe pod uwagę, można wprost skonkludować, że *cyberprzestrzeń to globalna przestrzeń informacyjna, stanowiąca strategiczny element systemu bezpieczeństwa państwa*, i taką też definicję cyberprzestrzeni przyjmuje autor w ramach konwencji terminologicznej badanego problemu[11]. Nie należy jednak przy tym zapominać o rosnącym znaczeniu pozapaństwowych podmiotów transnarodowych, które także coraz aktywniej wykorzystują cyberprzestrzeń dla swoich celów, nie zawsze zbieżnych z celami państw, na terytorium których operują[12]. Autor w konwencji terminologicznej artykułu przyjął koncepcję realizmu z teorii stosunków międzynarodowych, zakładającą państwo unitarne jako jedyny podmiot stosunków międzynarodowych o anarchicznym charakterze, zwracając jednocześnie uwagę na nurt liberalny, zgodnie z którym w systemie międzynarodowym m.in. wzrasta znaczenie podmiotów niepaństwowych, takich jak: międzynarodowe organizacje pozarządowe (ang. *International Non-Governmental Organizations*, INGOs) oraz jednoznacznie negatywne podmioty transnarodowe, do których autor zaliczył – międzynarodowe organizacje terrorystyczne (ang. *International Terrorist Organizations*, ITOs) i międzynarodowe grupy przestępcze (ang. *International Criminal Groups*, ICGs). W najbliższym czasie należy oczekiwać eksplozji ich aktywności w cyberprzestrzeni, zwłaszcza ITOs, które dotychczas wykorzystują ją głównie dla celów medialnych, werbunkowych i łączności operacyjnej. Decyduje o tym przede wszystkim stosunkowo niewielki koszt dostępu do cyberbroni, przy jednoczesnych olbrzymich możliwościach jej destrukcyjnego oddziaływania,

[4] R. Mattioli, *The «State(s)» of Cybersecurity* [w:] G. Giacomello (red.), *Security in Cyberspace*, New York, London, New Delhi, Sydney, Bloomsbury, 2014, s. 27.

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

[6] *Słownik Języka Polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (dostęp: 27.01.2015).

[7] *Słownik komputerowy i encyklopedia informatyczna*, http://www.i-slownik.pl/323,cyberprzestrzen (dostęp: 27.01.2015).

[8] *The National Strategy to Secure Cyberspace*, The White House Washington, luty 2003, p. vii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (dostęp: 27.01.2015).

[9] *National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23*, 8 styczeń 2008, p. 7g, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (dostęp: 27.01.2015).

[10] *Department of Defense Strategy for Operating in Cyberspace*, lipiec 2011, http://www.defense.gov/news/d20110714cyber.pdf (dostęp: 27.01.2015).

[11] Konwencja terminologiczna jest umową pomiędzy autorem i czytelnikami odnośnie do definicji terminów, obowiązujących autora w całej publikacji, M. Mazur, *Cybernetyka i charakter*, wyd. 2, Wyd. AULA, Podkowa Leśna 1996, s. 27–28.

[12] Zob. E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego* [w:] M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, s. 78–94.

porównywanych niekiedy do skutków broni masowego rażenia. Zagadnienie szacowania potęgi cybernetycznej podmiotów niepaństwowych jest równie istotne jak państwowych i wymaga podjęcia wnikliwych studiów, tym bardziej, że problematyka ta w literaturze przedmiotu praktycznie nie występuje[13]. Niezależnie więc od silnych i słabych stron konkretnych definicji cyberprzestrzeni, takie jej postrzeganie plasuje ją w sferze bezpieczeństwa państwa (także w wymiarze międzynarodowym), w sferze ochrony i bezpieczeństwa rządowych sieci informacyjnych i infrastruktury krytycznej państwa[14]. W wymiarze operacyjnej przestrzeni bezpieczeństwa[15] cyberprzestrzeń wyróżnia m.in. fakt, iż jej użytkownicy (indywidualni i zorganizowani) są jednocześnie jej kreatorami oraz jej odmienna fizyczna charakterystyka (tworzenie, gromadzenie, przekształcanie, wymiana i wykorzystywanie przepływu informacji drogą elektroniczną), która silnie oddziałuje na wszystkie pozostałe przestrzenie operacyjne (lądową, powietrzną, morską i kosmiczną) tradycyjnie pojmowane w sensie przestrzeni geograficznych. Cyberprzestrzeń jest od nich nie tylko o wiele bardziej dynamiczna i nieprzewidywalna, ale można ją też po prostu włączyć lub wyłączyć[16].

Daniel T. Kuehl, definiując potęgę cybernetyczną państwa, szukał inspiracji w analogii do pionierskich pojęć potęg morskiej i powietrznej, których główną ideą jest zdolność do użycia i wykorzystania danego środowiska dla określonych celów. To doprowadziło go do konstatacji, że *potęga cybernetyczna to zdolność do użycia cyberprzestrzeni w celu wywarcia wpływu na zdarzenia we wszystkich przestrzeniach operacyjnych oraz uzyskania przewagi we wszystkich tworzących cyberpotęgę czynnikach*[17]. Pomiar potęgi cybernetycznej odnosi się więc wprost do pomiaru własności tego środowiska. Do jego głównych wskaźników badacz ten zaliczył: 1) wskaźnik zdolności technologicznych (stale zmienny i różny w dyspozycji różnych użytkowników – państwowych i niepaństwowych) oraz 2) wskaźnik zdolności organizacyjnych.

Joseph S. Nye definiuje z kolei potęgę cybernetyczną jako: zdolność do osiągania zakładanych celów za pomocą sprzężonych w cyberprzestrzeni elektronicznych zasobów informacyjnych[18]. Badacz ten rozpatruje cyberpotęgę w wymiarach wewnętrznych i zewnętrznych oddziaływań informacyjnych (wirtualnych) i fizycznych generujących cybernetyczną siłę miękką (ang. *soft power*) oraz twardą (ang. *intra cyberspace hard power*)[19]. Przykładowo – w wymiarze wewnętrznych oddziaływań informacyjnych możemy mieć do czynienia z miękką siłą cybernetyczną w postaci systemu norm i standardów oraz z twardą siłą w postaci cyberataków[20] typu DoS/DDoS (tabela 1).

Tabela 1

Wirtualny i fizyczny wymiar potęgi cybernetycznej

	Wewnętrzna potęga cybernetyczna	Zewnętrzna potęga cybernetyczna
Instrumenty informacyjne	Twarda: ataki typu DoS (ang. *Denial of Service*)/DDoS (ang. *Distributed Denial of Service*)[1] Miękka: system norm i standardów	Twarda: ataki na systemy SCADA (ang. *Supervisory Control And Data Acquisition*)[2] Miękka: działania dyplomatyczne wpływające na opinię publiczną
Instrumenty fizyczne	Twarda: rządowa kontrola przedsiębiorstw Miękka: działania wspierające ruchy obrońców praw człowieka	Twarda: ataki na routery lub magistrale sieciowe Miękka: działania szkalujące cyber-dostawców

[1] Atak DoS polega na zmasowanym wysyłaniu do atakowanego systemu komputerowego tak dużej ilości danych, że nie jest on w stanie ich obsłużyć, co spowalnia lub paraliżuje jego działanie. W ataku rozproszonym DDoS bierze udział duża liczba komputerów atakujących, nad którymi

[13] R. Białoskórski, Cyberthreats..., op. cit., s. 252–253. Zob. E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego* [w:] M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, s. 78–94.

[14] D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem* [w:] D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (dostęp: 27.01.2015), s. 2.

[15] Pojęcie operacyjności oznacza w tym przypadku praktyczne działanie w danym miejscu i czasie (Ibidem, przyp. 13).

[16] Zob. G.J. Rattray, *An Environmental Approach to Understanding Cyberpower*, 13 styczeń 2015, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (dostęp: 27.01.2015).

[17] D.T. Kuehl, *From Cyberspace...*, s. 12.

[18] J.S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (dostęp: 27.01.2015), s. 3–4.

[19] Ibidem, s. 3.

[20] Cyberatak (atak cybernetyczny) to najogólniej celowe zakłócenie prawidłowego funkcjonowania cyberprzestrzeni, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, s. 6. W artykule pojęcie to dotyczy szerszych działań w ramach operacji informacyjnych.

przejęto wcześniej kontrolę (np. zombie). R. Białoskórski, *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010, s. 47–48.

[2] SCADA jest systemem nadzorującym przebieg procesu technologicznego lub produkcyjnego, polegający na zbieraniu aktualnych danych (pomiary), ich wizualizacji, sterowaniu procesem, alarmowaniu oraz archiwizacji danych, http://pl.wikipedia.org/wiki/SCADA (dostęp: 27.01.2015).

Źródło: J.S. Nye, op. cit., s. 3.

Badacz ten proponuje również trzy warianty potęgi cybernetycznej[21], a mianowicie:

Wariant 1: (A zmienia strategię B, której B początkowo nie planowało)

Twarda siła: ataki DoS, złośliwe oprogramowanie (ang. *malware*), ataki na systemy sterujące procesami przemysłowymi SCADA, aresztowania blogerów;

Miękka siła: kampanie informacyjne ukierunkowane na zmianę preferencji hakerów, rekrutowanie członków organizacji terrorystycznych.

Wariant 2: (Agenda sterująca: A zmienia podjętą przez B strategię)

Twarda siła: zapory sieciowe (ang. *firewalls*), filtry, naciski na firmy;

Miękka siła: dostawcy usług internetowych (ang. *Internet Service Providers*, ISPs), Internetowa Korporacja ds. Nadanych Nazw i Numerów (ang. *The Internet Corporation for Assigned Names and Numbers*, ICAAN), ogólnie akceptowane standardy oprogramowania.

Wariant 3: (A wpływa prewencyjnie na strategię B, w taki sposób, że B nie rozpatruje niekorzystnych dla A decyzji)

Twarda siła: ściganie blogerów łamiących prawo;

Miękka siła: informowanie preferencyjne (np. stymulujące nacjonalizm i „patriotyczne hakerstwo"), normy budzące odrazę (np. pornografia dziecięca).

Brak powszechnie uznanych definicji potęgi cybernetycznej oznacza, że badacze zajmujący się problemem jej pomiaru powinni każdorazowo przyjmować własną konwencję terminologiczną, stosownie do przyjętej metody badawczej.

Pomiar potęgi cybernetycznej państw

Potęga cybernetyczna może być rozpatrywania w sensie defensywnym i wówczas mamy do czynienia z defensywną potęgą cybernetyczną (ang. *defensive cyber power*, DCP) oraz w sensie ofensywnym w postaci – ofensywnej potęgi cybernetycznej (ang. *offensive cyber power*, OCP). Powyższy czynnik m.in. determinuje kierunki koncepcji metod pomiaru potęgi cybernetycznej, nawet jeśli nie jest on wyrażony *expressis verbis*, jak to ma miejsce w omówionym przykładowo modelu CPI.

Model CPI

Koncepcja modelu pomiaru potęgi cybernetycznej CPI (ang. *Cyber Power Index*) opracowana została przez zespół wywiadu ekonomicznego (ang. *The Economist Intelligence Unit*, EIU) renomowanego czasopisma „The Economist" we współpracy z konsorcjum Booz Allen Hamilton. Jego celem jest tworzenie rankingów zdolności cybernetycznej państw grupy G20 w zakresie zapobiegania i przeciwdziałania atakom cybernetycznym oraz promowanie problematyki cyberbezpieczeństwa w środowisku międzynarodowym. Jest to więc *de facto* model pomiaru defensywnej potęgi cybernetycznej (DCP).

Polega on na obliczaniu wskaźników potęgi cybernetycznej państw. W tym celu opracowano matrycę 39 ilościowych i jakościowych wskaźników pogrupowanych w 4 kategorie oraz 19 podkategorii z uwzględnieniem ich średnich wag (tabela 2). Matryca została opracowana w maju 2011 roku metodą ocen ekspertów[22]. Każdy ze wskaźników otrzymuje przyznane przez ekspertów wartości w skali rosnącej od 0 do 100, gdzie 100 oznacza największą wartość potęgi cybernetycznej. Repozytoria danych stanowią narodowe i międzynarodowe źródła statystyczne, w tym: The Economist Intelligence Unit (EIU); The UN Educational, Scientific and Cultural Organization (UNESCO); The International Telecommunications Union (ITU); The World Bank (WB).

[21] J. Nye, op. cit., s. 7.

[22] Metoda ocen ekspertów wymaga przede wszystkim starannego doboru ekspertów, najczęściej na podstawie kryteriów formalnych (stopień naukowy, doświadczenie zawodowe, dorobek naukowy, nagrody) lub społeczno-moralnych (dobra opinia współpracowników, rzetelność, uczciwość, bezkompromisowość). W opracowaniu uśrednionej oceny grupowej należy uwzględnić różnice w ocenach ekspertów indywidualnych (większa swoboda wypowiadania się i prezentowania wyników) i grupowych (możliwe psychologiczne zahamowania) oraz aspekty etyczne. Zob. M. Sułek, *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004, s. 167–174.

Tabela 2

Matryca wskaźników i wag potęgi cybernetycznej modelu CPI[1]

Kategoria wskaźników	Waga [%]	Podkategoria wskaźników	Waga [%]	Wskaźniki
I. Wskaźniki prawno-regulacyjne	26,3	I.1. Wskaźniki rządowych zdolności cybernetycznych	27,1	1. Wskaźnik narodowych programów cybernetycznych
				2. Wskaźnik publiczno-prywatnego cyberpartnerstwa
		I.2. Wskaźniki polityki cyberbezpieczeństwa	24	3. Wskaźnik organów wykonawczych
				4. Wskaźnik regulacji prawnych
				5. Wskaźników zdolności zwalczania cyberprzestępczości
				6. Wskaźnik zobowiązań prawnomiędzynarodowych
				7. Wskaźnik planów cyberbezpieczeństwa
		I.3. Wskaźnik cybercenzury	15,5	8. Wskaźnik cybercenzury
		I.4. Wskaźnik skuteczności politycznej	15,5	9. Wskaźnik skuteczności politycznej
		I.5. Wskaźnik ochrony praw autorskich	17,8	10. Wskaźnik ochrony praw autorskich
II. Wskaźniki społeczno--ekonomiczne	25	II.1. Wskaźniki poziomu wykształcenia	25,2	11. Wskaźnik liczby słabych studentów do ogólnej liczby studentów
				12. Wskaźnik liczb lat nauki
		II.2. Wskaźniki sprawności technicznej	27,4	13. Wskaźnik wzrostu wydajności pracy
				14. Wskaźnik liczby badaczy w sektorze badań i rozwoju (BR) na milion mieszkańców
				15. Wskaźnik liczby naukowców i inżynierów
				16. Wskaźnik poziomu znajomości j. angielskiego
		II.3. Wskaźniki handlowe	17,3	17. Wskaźnik procentowy eksportu technologii informacyjno-komunikacyjnej do eksportu całkowitego
				18. Wskaźnik procentowy importu technologii informacyjno-komunikacyjnej do importu całkowitego
				19. Wskaźnik wolności handlu
		II.4. Wskaźniki innowacyjności	30,1	20.Wskaźnik procentowy udziału sektora badań i rozwoju (BR) w PKB
				21. Wskaźnik patentowy
				22. Wskaźnik procentowy udziału sektora własności prywatnej i z kapitałem mieszanym w PKB
III. Wskaźniki infrastruktury technologicznej	26,3	III.1. Wskaźniki dostępu do technologii informacyjno-komunikacyjnych	20,3	23. Wskaźnik dostępności internetu
				24. Wskaźnik dostępności telefonii mobilnej
				25. Wskaźnik procentowy punktów Wi-Fi na milion mieszkańców
				26. Wskaźnik dostępności portali społecznościowych
		III.2. Wskaźniki jakości technologii informacyjno-komunikacyjnych	21,9	27. Wskaźnik liczby abonentów internetu szerokopasmowego na 100 mieszkańców
				28. Wskaźnik dostępności międzynarodowego Internetu szerokopasmowego
		III.3. Wskaźnik procentowy nakładów na technologie informatyczno-komunikacyjne do PKB	20,3	29. Wskaźnik procentowy nakładów na technologie informatyczno-komunikacyjne do PKB
		III.4. Wskaźniki przystępności technologii informacyjno-komunikacyjnych	11,7	30. Wskaźnik taryf telefonii mobilnej
				31. Wskaźnik taryf Internetu szerokopasmowego
		III.5 Wskaźnik bezpieczeństwa serwerów	25,8	32. Wskaźnik bezpieczeństwa serwerów
IV. Wskaźniki zastosowań przemysłowych	22,5	IV.1. Wskaźnik inteligentnych sieci	21,1	33. Wskaźnik inteligentnych sieci
		IV.2. Wskaźnik E-Zdrowia	16,2	34. Wskaźnik E-Zdrowia

[1] Szczegółowy opis definicji oraz zasad przydzielania wartości poszczególnym wskaźnikom znajduje się w materiale źródłowym EIU w załączniku II na s. 26–32.

Kategoria wskaźników	Waga [%]	Podkategoria wskaźników	Waga [%]	Wskaźniki
		IV.3. Wskaźniki zastosowań komercyjnych	30,4	35. Wskaźnik procentowy liczby firm oferujących zamówienia przez Internet do ogólnej liczby firm wykorzystujących Internet w działalności biznesowej
				36. Wskaźnik procentowy liczby indywidualnych klientów składających zamówienia przez Internet do ogólnej liczby internautów
				37. Wskaźnik procentowy liczby indywidualnych klientów bankowości elektronicznej do ogólnej liczby internautów
		IV.4. Wskaźnik inteligentnych systemów transportowych	21,1	38. Wskaźnik inteligentnych systemów transportowych
		IV.5. Wskaźnik administracji elektronicznej	11,3	39. Wskaźnik administracji elektronicznej

Źródło: *Cyber Power Index. Findings and Methodology*, Economist Intelligence Unit, 2011, http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf, s. 22, 24.

Wagi poszczególnych kategorii wskaźników są zbliżone z nieznaczną dominacją kategorii wskaźników prawno-regulacyjnych i kategorii wskaźników infrastruktury technologicznej (*ex aequo* 26,3) przed kategorią wskaźników społeczno-ekonomicznych (25) oraz kategorią zastosowań przemysłowych (22,5).

Analizie poddano miary potęg cybernetycznych 19 państw z grupy G20 (bez Unii Europejskiej) reprezentujących pięć regionów geograficznych: Europę Zachodnią, Europę Wschodnią i Azję Środkową, Bliski Wschód i Afrykę, Azję i Pacyfik oraz Amerykę.

Wartości wskaźników są w odpowiedni sposób normalizowane i sumowane według kategorii.

Wskaźniki sprzyjające potędze cybernetycznej (np. wzrost wydatków na BR) są normalizowane zgodnie z regułą:

$$x = \frac{x - Min(x)}{Max(x) - Min(x)}$$

gdzie: *Min(x)* – minimalna wartość danego wskaźnika gospodarczego w grupie 19 państw;

Max(x) – maksymalna wartość danego wskaźnika gospodarczego w grupie 19 państw.

W ten sposób znormalizowane wartości są przekształcane z przedziału 0–1 do przedziału 0–100, co umożliwia ich bezpośrednie porównanie z innymi wskaźnikami, w taki sposób, iż państwo o najwyższym wskaźniku przyjmuje wartość 100, a o najniższym wskaźniku wartość 0.

Tabela 3

Wydatki na badania i rozwój w stosunku do PKB

Państwo	Udział BR w PKB
Republika Korei	4,04
Japonia	3,39
Niemcy	2,93
Stany Zjednoczone	2,79
Australia	2,39
Francja	2,26
Chiny	1,98
Kanada	1,73
Wielka Brytania	1,72
Włochy	1,27
Brazylia	1,21
Rosja	1,12
Turcja	0,86
Indie	0,81
RPA	0,76
Argentyna	0,65
Meksyk	0,43
Arabia Saudyjska	b.d.
Indonezja	b.d.

Źródło: The World Bank, Research and development expenditure (% of GDP), http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS (dostęp: 15.10.2015).

Wskaźniki niesprzyjające potędze cybernetycznej (np. taryfy telefonii mobilnej czy taryfy Internetu szerokopasmowego) są normalizowane z nieco inną regułą, przy tych samych oznaczeniach co wyżej, a mianowicie:

$$x = \frac{x - Max(x)}{Max(x) - Min(x)}$$

Wyniki pomiarów potęgi cybernetycznej 19 państw grupy G20 wskazują na dominację Wielkiej Brytanii, Stanów Zjednoczonych, Australii, Niemiec i Kanady (tabela 4). Największą wartość w pierwszej kategorii wskaźników prawno-regulacyjnych ze wszystkich kategorii wskaź-

ników uzyskały Niemcy (99,3) przed Stanami Zjednoczonymi oraz Wielką Brytanią (*ex aequo* 97,3).

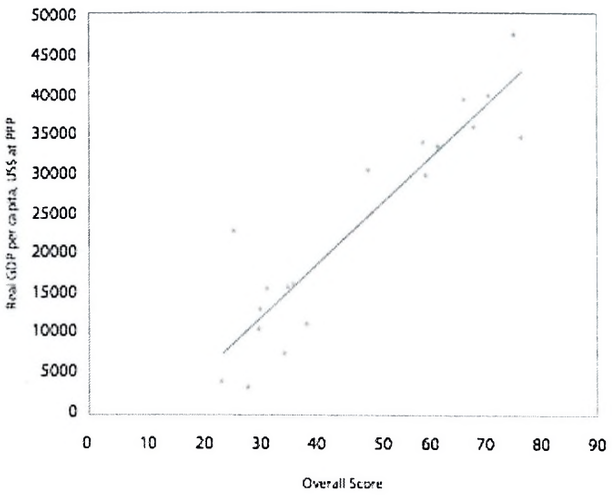
Tabela 4

Ranking potęgi cybernetycznej państw obliczonej modelem CPI (2011)

Pozycja	Państwo	Wartość CPI (w skali 0–100)	Region geograficzny
1	Wielka Brytania	76,8	Europa Zachodnia
2	Stany Zjednoczone	75,4	Ameryka
3	Australia	71,0	Azja i Pacyfik
4	Niemcy	68,2	Europa Zachodnia
5	Kanada	66,6	Ameryka
6	Francja	61,8	Europa Zachodnia
7	Republika Korei	59,7	Azja i Pacyfik
8	Japonia	59,3	Azja i Pacyfik
9	Włochy	49,5	Europa Zachodnia
10	Brazylia	38,6	Ameryka
11	Meksyk	36,3	Ameryka
12	Argentyna	35,4	Ameryka
13	Chiny	34,6	Azja i Pacyfik
14	Rosja	31,7	Europa Wschodnia i Azja Środkowa
15	Turcja	30,4	Europa Wschodnia i Azja Środkowa
16	RPA	30,2	Bliski Wschód i Afryka
17	Indie	28,3	Azja i Pacyfik
18	Arabia Saudyjska	25,7	Bliski Wschód i Afryka
19	Indonezja	23,5	Azja i Pacyfik

Źródło: *Cyber Power Index*..., s. 4.

Model funkcjonalny CPI umożliwia obliczanie korelacji pomiędzy wskaźnikami. Autorzy modelu zmierzyli także korelację wartości wskaźnika PKB na mieszkańca z ogólną wartością potęgi cybernetycznej 19 państw, uzyskując zaskakująco wysoki wynik – 0,92 (rysunek 1).



Źródło: *Cyber Power Index*..., s. 23.

Rys. 1. Współczynnik korelacji wielkości PKB per capita oraz ogólnej wartości potęgi cybernetycznej CPI

Autorzy modelu CPI w rzeczywistości mierzą jedynie defensywną moc cybernetyczną, chociaż nie deklarują tego w założeniach (a szkoda). Kategorie wskaźników mają bardzo zbliżone wagi, co pod tym względem zbliża tę motodę do tzw. ważenia neutralnego o jednakowych wagach i równomiernym rozkładzie wskaźników. Zróżnicowanie jest jednak wyraźne na poziomie wag podkategorii, których suma dla danej kategorii wynosi 100. Trudno kwestionować dobór wskaźników w tym modelu, aczkolwiek w kategorii wskaźników społeczno-ekonomicznych nie wyróżniono podkategorii wskaźników ekonomicznych, pomimo iż autorzy uznają znaczenie wskaźnika PKB per capita o bardzo wysokim wskaźniku korelacji z ogólną potęgą cybernetyczną państw G20. Zastanawiająca jest także pozycja Wielkiej Brytanii, jako lidera CPI, przed Stanami Zjednoczonymi.

Model A.M. Gomeza

Koncepcja pomiaru potęgi cybernetycznej państw zaproponowana przez Alberto Miguela Gomeza[23] została także oparta na metodzie wskaźnikowej, w której wyróżniono 50 wskaźników podzielonych na 6 kategorii: 1) infrastruktury, 2) gospodarki, 3) badań naukowych, 4) polityki

[23] Z treści źródłowego artykułu trudno jednoznacznie wywnioskować, czy A.M. Gomez jest autorem modelu, czy też tylko go charakteryzuje. Umownie jednak nazwano go modelem A.M. Gomeza. Zob. A.M. Gomez, *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (dostęp: 27.01.2015), p. IIIA.

i e-administracji, 5) społeczno-polityczną oraz 6) militarną. Na podstawie wyników pomiaru potęg cybernetycznych oraz analizy zdarzeń (zachowań państw) w cyberprzestrzeni (podmiot atakujący, obiekt atakowany oraz częstotliwość) A.M. Gomez wyróżnił cztery kategorie państw o ofensywnych i defensywnych zachowaniach w cyberprzestrzeni (tabela 5)[24]. Następnie, posługując się analizą statystyczną, dla każdej kategorii państw określił rodzaj stosowanego ataku, z uwzględnieniem roli podmiotu atakującego i atakowanego (tabela 6). W tym miejscu niejasna jest jednak przyjęta przez A.M. Gomeza reguła budowania macierzy typów cyberataków. W przypadku tej samej kategorii państw występujących jednocześnie w roli podmiotu atakującego i atakowanego powinno być pole puste. Przykładowo pole [EP-I; EP-I] oznacza, że Stany Zjednoczone są podmiotem atakującym samych siebie?

Tabela 5

Kategoryzacja zachowań państw w cyberprzestrzeni

Kategoria	Państwa
Defensywne I (EP-I)	Stany Zjednoczone
Ofensywne I (EA-I)	Chiny
Defensywne II (EP-II)	Australia, Kanada, Nowa Zelandia, Singapur, Japonia, Republika Korei, Filipiny, Rosja, Izrael
Ofensywne II (EA-II)	Chile, Indonezja, Malezja, Meksyk, Peru, Tajlandia, Wietnam, Indie, Iran, Pakistan, Bangladesz, Syria, Cypr, Turcja, Irak, Kuwejt, Gruzja, Liban

Źródło: A.M. Gomez, op. cit., s. 5, za: FireEye, *World war c: Understanding nation-state motives behind todays advanced cyber attacks*, FireEye, Tech. Rep.

Tabela 6

Macierz typów cyberataków

	Podmiot atakowany			
Podmiot atakujący	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	atak na sieci	złośliwe oprogramowanie	atak na sieci	złośliwe oprogramowanie
EA-I	kradzież danych	atak na sieci	złośliwe oprogramowanie	złośliwe oprogramowanie
EP-II	złośliwe oprogramowanie	atak na strony internetowe	DoS/ DDoS	złośliwe oprogramowanie
EA-II	atak na strony internetowe	atak na sieci	DoS/ DDoS	atak na strony internetowe

Źródło: A.M. Gomez, op. cit., s. 6.

Państwa zaklasyfikowane do dwóch kategorii defensywnych – EP-I (kat. pierwsza – liderzy) i EP-II (kat. druga – pozostali) cechują dominujące wartości wskaźników z kategorii: infrastruktury, gospodarki, badań naukowych oraz polityki i administracji cyfrowej przy jednocześnie ich pozytywnej korelacji ze wskaźnikami pozostałych kategorii. Natomiast państwa z kategorii ofensywnych (EA-I i EA-II) charakteryzują się niskimi wartościami wskaźników z ww. kategorii grup, przy wyższym poziomie wskaźników z kategorii społeczno-politycznej oraz dominujących wskaźnikach z grupy militarnej (zwłaszcza EA-I). Jednocześnie występuje ujemna korelacja pomiędzy wskaźnikami z pierwszych czterech kategorii a wskaźnikami społeczno-politycznymi. Państwa z kategorii ofensywnych cechuje także stały wzrost wskaźników infrastruktury i gospodarczych. Liderem wśród państw ofensywnych (EA-I) są Chiny, których także potęga ogólna i wojskowa od lat dynamicznie wzrasta – osiągając obecnie trzecią pozycję w świecie po Stanach Zjednoczonych[25]. Liderem wśród kategorii państw defensywnych (EP-I) są natomiast Stany Zjednoczone.

Na podstawie uzyskanych tą metodą wyników badań, A.M Gomez wyróżnił trzy podstawowe strategie państw w cyberprzestrzeni:

- *strategia utrzymania potęgi cybernetycznej* – stosowana przez państwa aktywnie demonstrujące posiadane zdolności w cyberprzestrzeni, w celu zwiększenia ich potęgi ogólnej;
- *strategia osiągania równowagi* – polega na dążeniu państw do maksymalizowania ich cyberpotęgi, w celu uzyskania przewagi nad potencjalnymi agresorami, zarówno w cyberprzestrzeni, jak i poza nią, unikając jednak sytuacji konfliktо-

[24] A.M. Gomez podaje nazwy kategorii państw jako pasywne (ang. *established passive*, EP) i agresywne (ang. *emmerging aggresive*, EA), natomiast autor posługuje się jego zdaniem właściwszą terminologią: defensywne (ang. *defensive*) i ofensywne (ang. *offensive*), przy czym skróty oznaczeń pozostawiono w oryginale.

[25] Zob. M. Sułek, *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013, s. 168–193.

wych, które mogą zminiejszać ich potęgę ogólną (np. w sferze ekonomicznej).

• *strategia demonstrowania potęgi cybernetycznej* – stosowana przez państwa, w celu demonstrowania ich wzrastających zdolności w cyberprzestrzeni.

Prezentując model pomiaru potęgi cybernetycznej państw A.M. Gomez nie podaje szczegółów metodologicznych, koncentrując się głównie na jego implementacji w określaniu kategorii strategii państw w cyberprzestrzeni, wyróżniając ich zarówno defensywny, jak i ofensywny charakter. Proponowane w konkluzjach trzy kategorie strategii państw mogą jednak budzić wątpliwości. W zasadzie wszystkie państwa na miarę posiadanych możliwości dążą do zwiększania potęgi w cyberprzestrzeni – także Stany Zjednoczone i Chiny. Inną kwestią jest jej demonstrowanie w postaci określonych działań. W tym zakresie zastanawia także plasowanie Stanów Zjednoczonych na pozycji lidera w kategorii państw defensywnych wobec kierowanych wobec nich podejrzeń m.in. o atak cybernetyczny za pomocą robaka komputerowego „Stuxnet".

Zakończenie

Większość proponowanych w literaturze przedmiotu definicji potęgi cybernetycznej odnosi się do podstawowej jednostki politycznej, jaką jest państwo. Taką też konwencję terminologiczną przyjął w artykule autor. Należy przy tym zwrócić jednak uwagę na konieczność postrzegania potęgi cybernetycznej nie tylko w sensie podmiotowym, jakim jest jej dysponent (w tym wypadku państwo), lecz także w sensie przedmiotowym, gdzie m.in. należy wyróżnić: defensywną i ofensywną potęgę cybernetyczną. Powyższe czynniki w znacznym stopniu determinują wybór i implementację metody jej pomiaru oraz uzyskane za jej pomocą wyniki. Wobec braku powszechnie uznanej definicji potęgi cybernetycznej, badacze zajmujący się jej pomiarem powinni przyjmować własną konwencję terminologiczną, stosownie do przyjętej metody badawczej.

Wybór modelu CPI oznacza badanie wyłącznie defensywnej potęgi cybernetycznej, chociaż jego autorzy tego faktu *directe* nie definiują. Model A.M. Gomeza jest z założenia bardziej złożony, gdyż na podstawie obliczenia potęgi cybernetycznej państw metodą wskaźnikową pozwala na określanie strategii państw w cyberprzestrzeni zarówno pod względem ich defensywnych, jak i ofensywnych zdolności. Proponowany przez A.M. Gomeza podział na trzy główne strategie budzi jednak wątpliwości, chociażby z uwagi na fakt, że *de facto* wszystkie państwa, na miarę posiadanych zdolności, dążą do zwiększenia ich potęgi cybernetycznej – także Stany Zjednoczone i Chiny.

Obie metody wykorzystują powszechnie znaną metodę wskaźnikową stosowaną w algorytmach wczesnego ostrzegania. Niektóre wskaźniki pomiaru cyberpotęgi są wspólne dla obu modeli (np. gospodarczy czy technologiczny), niektóre zaś cechują indywidualnie każdy z nich (np. militarny w modelu drugim). Zastanawiający w przytoczonych przez A.M. Gomeza wynikach pomiarów jest brak Wielkiej Brytanii, która w modelu CPI jest absolutnym liderem w rankingu cyberpotęg państw. Podobnie jest z plasowaniem Stanów Zjednoczonych na pozycji lidera w grupie państw defensywnych, wobec powszechnych podejrzeń o atak cybernetyczny za pomocą robaka komputerowego „Stuxnet".

W mojej ocenie powyższe metody pomiaru potęgi cybernetycznej państw nie rozwiązują w pełni problemu badawczego i należy je traktować jako propozycje inspirujące do dalszych zaawansowanych badań nad tą problematyką z uwzględnieniem nie tylko państw, ale i innych podmiotów systemu bezpieczeństwa międzynarodowego (np. organizacji terrorystycznych).

Bibliografia

Białoskórski R., *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010.

Białoskórski R., *Cyberthreats in the Security Environment of the 21st Century*, "Journal of Security and Sustainability Issues" 2012, nr 4.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

Białoskórski R., *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski* [w:] M. Sułek (red.), *Potęgometria*, tom 2, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015 (w druku).

Cyber Power Index. Findings and Methodology, Economist Intelligence Unit, 2011. http://www.boozallen.com/content/dam/boozallen/media/file/

Cyber_Power_Index_Findings_and_Methodology.pdf (dostęp: 27.01.2015).

Department of Defense Strategy for Operating in Cyberspace, lipiec 2011, http://www.defense.gov/news/d20110714cyber.pdf (dostęp: 27.01.2015).

Gomez A.M., *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (dostęp: 27.01.2015).

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, w: D. Kramer, H. Stuart, i L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (dostęp: 27.01.2015).

Mattioli R., *The «State(s)» of Cybersecurity*, w: Giampiero Giacomello (red.), *Security in Cyberspace*, New York; London; New Delhi; Sydney, Bloomsbury, 2014.

Mazur M., *Cybernetyka i charakter*, wyd. 2, Wyd. Podkowa Leśna; Wyd. AULA, 1996.

National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, 8 styczeń 2008, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (dostęp: 27.01.2015).

Nye J.S., *Cyber Power*, Cambridge: Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (dostęp: 27.01.2015).

Panas E., *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, w: M. Sułek (red.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

Rattray G.J., *An Environmental Approach to Understanding Cyberpower*, 13 styczeń 2015. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (dostęp: 27.01.2015).

Słownik Języka Polskiego, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (dostęp: 27.01.2015).

Słownik komputerowy i encyklopedia informatyczna, http://www.i-slownik.pl/323,cyberprzestrzen (dostęp: 27.01.2015).

Sułek M., *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004.

Sułek M., *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013.

The National Strategy to Secure Cyberspace, The White House Washington, luty 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (dostęp: 27.01.2015).

THE CYBER POWER OF STATES: MEASUREMENT AND APPLICATION

Abstract

The article discusses the problem of measurement of cyber power of states using the example of two research models: Cyber Power Index (CPI) and A.M. Gomez. Both methods are based on the analysis of indicators. The first model values only defensive cyber power, the second defensive and offensive as well. Both of these cyber power dimensions can be seen as the main determinants of the directions of research for solutions to the above mentioned research problem. The second model serves for the estimating of a state's strategies in cyberspace from the- maintenance of cyber power, the achievement balance, and the demonstration of cyber power. The results of both models differ considerably enough and already confirm the complexity of this problem during the conceptual phase and highlight the need for further research.

Keywords – cyberspace, cyberpower, measurement, model

Introduction

The modern revolution of inforrmation is based on the global dependence on information and communication technology (ICT). The information world has the greatest capabilities of interactions in cyberspace at its disposal, creating both threats and opportunities. It concerns all subjects of international systems, equal government and non-government. Each subject can be attacker and victim of cyberthreats, cyberwar, cyberespionage, cyberterrorism and cyberdelinquency[1], the identification of which is one of the main problems of cybersecurity[2].

[1] See: R. Białoskórski, *Cyberzagrożenia w sirodowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

[2] The author has suggested conceptual analysis of cyberthreat based on analysis of four factors: subject attacking, subject attacked, purposes and motivation. See: R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century*, 'Journal of Security and Sustainability Issues' 2012, No. 4, p. 255–258.

In this situation, the problem of measurement of cyber power is an important factor in the estimation of the power of states. In this article, the problem of defining the cyber power of states and how to measure it is addressed.

Inspiration for the research came from its innovatory character and the lack of elaboration in Polish scientific literature and consistent range with the main direction of scientific interest in the author's problem of *conflict prevention (CP)*, defined as the process of early warning and preventive reaction relying on constant monitoring and analysis of the evolution of events in the areas at risk of military conflict (*early warning*) and deciding on and taking preventive actions (*reaction preventive*) to prevent an armed conflict[3]. In view of the complexity of theproblem, the article only outlines the problems which that require more involved theoretical studies and empirical research.

Definition of cyber power

The definition of "cyber power" is related with "cyberspace". Mattiolli Rossella considers, that it is hard to define the border between cyberspace and cybersecurity, mainly from the point of view of the dynamic character of cyberspace and the lack of classically comprehended territoriality[4]. The Cybersecurity policy of the Republic of Poland defines security in cyberspace as a 'group of activities: the organisational, legal, technical, physical and educational affirmation of the undisturbed functioning of cyberspace'[5].

In literature, cyberspace is defined in principle, as: 1) a global information area, understood as a '*virtual area* in which communication proceeds between computers joined to an internet network'[6] or an 'area of opened intercommunication through joined computers and classic communication networks world-wide, taking into consideration all electronic communication systems (also the classical telecommuniation network) which send information from numeric dating sources or for assigning numeration[7] and 2) a strategic element of a state security system as a: 'responsive system – state control system... consists of thousands of computers, switches and fiber-optic cables, operating the critical infrastructure'[8] or 'independent network of information technology infrastructure, including internet, telecommunication networks, computer systems and integrated processors and controllers acting in industrial critical infrastructure'[9] or 'military operation space (near: ground, air, marine, space)'[10]. With reference to the above, it is possible to conclude that *cyberspace is a global information area, containing a strategic element of a state's security system* and this definition is accepted by the author in the terminological convention of the researched problem[11]. However, one should not forget about the growing influence of transnational non-state subjects, which more actively take advantage of cyberspace for purposes not always consistent with the purposes of states on whose territories they are operating[12].

In terminological convention, the author has accepted the concept of realism from the theory of international relations, setting up a unitary state as the only one subject of international relations about anarchic character, a note on the liberal stream, and the meaning of the growing

[3] R. Białoskórski, *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej – kazus syryjski*, in: M. Sułek (ed.), *Potęgometria*, Vol. II, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015, p. 52.

[4] R. Mattioli, *The «State(s)» of Cybersecurity,* in: G. Giacomello (ed.), *Security in Cyberspace*, New York, London, New Delhi, Sydney, Bloomsbury, 2014, p. 27.

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, 25 czerwiec 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (access: 27.01.2015).

[6] *Słownik Języka Polskiego*, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (access: 27.01.2015).

[7] *Słownik komputerowy i encyklopedia informatyczna*, http://www.i-slownik.pl/323,cyberprzestrzen (access: 27.01.2015).

[8] *The National Strategy to Secure Cyberspace*, The White House Washington, February 2003, p. vii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (access: 27.01.2015).

[9] *National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23*, 8 January 2008, p. 7g, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (access: 27.01.2015).

[10] *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (access: 27.01.2015).

[11] Terminological convention is agreement among author and readers for definition obligatory author in the whole publication. M. Mazur, *Cybernetyka i charakter*, Edition 2, Wyd. AULA, Podkowa Leśna 1996, p. 27–28.

[12] See: E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, Vol. I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, p. 78–94.

role of non-state subject, such as: *International Non-Governmental Organisations* (INGOs) and one-valued negative multinational subjects for which the author has included: *International Terrorist Organizations* (ITOs) and *International Criminal Groups* (ICGs). In the nearest future, we can expect an explosion of activity from these in cyberspace, especially the ITOs, mainly for mediumistic purposes, recruitment and operative communications. The relatively small cost of access to cyberweapons is a decisive factor compared to the simultaneous enormous capability of their destructive interaction, sometimes compared to weapons of mass destruction (WMD). The issue of estimating the cyber power of non-state subjects is equally important to that of the state and it requires advanced studyand is practically ignored in the literature[13]. Independently from the strong and weak points of concrete definitions of cyberspace, such perception places it in the sphere of the security of state (also in an international dimension), in the sphere of the protection and security of a government's communications networks and critical infrastructures of state[14]. In the operative dimension area of security[15], cyberspace differs in that users (individual and organised) are simultaneously its creators and its different physical characteristics (creation, stockpiling, transformation, exchange and taking advantage of flow of information by electronic means), which strongly affects all remaining operative areas (ground, air, marine and space)in the traditional sense of geographical area. Cyberspace is not only more dynamic and unforeseen from there, but it is also possible to include or to exclude it[16].

Daniel T. Kuehl, when defining cyber power, had searched for inspiration in analogy to the pioneer defining of marine power and air power, whose main idea is the ability to activate and utilise the environment for definite purposes. It verified that: *cyber power is the ability to use cyberspace for rendering influence on events in all operative areas and obtaining an advantage in all factors creating the cyber power*[17]. So, the measurement of cyber power is concerned with the measurement of a feature of the environment. This researcher has included its: 1) technological ability indicator (still changeable and variable for different users – state and non-state) and 2) organisational ability indicator.

Joseph S. Nye defines cyber power as the: ability for achievement of set up purposes behind the assistance of electronically linked information in cyberspace[18]. This researcher treats cyber power in the dimension of internal and external information interactions (virtual) and physical generating of *cyber soft power* and *intra cyberspace hard power*[19]. In the dimension of internal information interaction, we can deal with soft cyber power in the form of a system of norms and standards and with hard power in the form of DoS/DDoS cyberattacks[20] (table 1).

Table 1

Physical and Virtual Dimensions of Cyber Power

	Intra cyber space	Extra cyber space
Information Instruments	Hard: *Denial of Service* attacks (DoS)/ *Distributed Denial of Service* (DDoS)[1] Soft: Set norms and standards	Hard: Attack SCADA (*Supervisory Control And Data Acquisition*)[2] Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

[1] DoS attack relies on a large amount of data on an attacked computer system, that it is taken over or its activity paralysed. At the DoS attack, a lot of attacking computers controlled

[13] R. Białoskórski, Cyberthreats..., op. cit., p. 252–253. See: E. Panas, *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, Vol. I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013, p. 78–94.

[14] D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, in: D. Kramer, H. Stuart, L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (access: 27.01.2015), p. 2.

[15] Notion 'operative' means in this case practical operation in data and place.

[16] See: G.J. Rattray, *An Environmental Approach to Understanding Cyberpower*, 13 January 2015, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (access: 27.01.2015).

[17] D.T. Kuehl, *From Cyberspace...*, p. 12.

[18] J.S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (access: 27.01.2015), p. 3–4.

[19] Ibidem, p. 3.

[20] Most generally, cyberattack expedient disturbance of correct functioning of correct cyberspace, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, p. 6. In the article, this definition links to the widest operations in the framework of information operations.

earlier controlled by the intruder are engaged (e.g. Zombie). R. Białoskórski, *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010, p. 47–48.

[2] SCADA is the computer operation system controlling the steering of the technological and production process, relying on the collection and projection of the actual data (measurements)), controlling of process, alarming and data archiving, http://pl.wikipedia.org/wiki/SCADA (access: 27.01.2015).

Source: J.S. Nye, op. cit., p. 3.

This researcher suggests three variants of cyber power[21]:

Variant 1st: (A induces B do what B would initially otherwise not do)

Hard Power: denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers

Soft Power: information campaign to change initial preferences of hackers, recruitment of members of terrorist organisations

Variant 2st: (Agenda control: A precludes B's choice by exclusion of B's strategies)

Hard Power: firewalls, filters, and pressure on companies to exclude some ideas

Soft Power: ISPs and search engines self monitor, ICANN rules on domain names, widely accepted software standards

Variant 3rd: (A shapes B's preferences, so some strategies are never even considered)

Hard Power: threats to punish bloggers who disseminate censored material

Soft Power: information to create preferences (eg. stimulate nationalism and "patriotic hackers,"), develop norms of revulsion (e.g. child pornography)

The lack of a generally recognised definition of cyber power means that researchers working on the problem of its measurement should accept personal terminological convention appropriate to the accepted research method.

Measurement of cyber power of state

Cyber power can be treated as part of defence and then we deal with *defensive cyber power* (DCP), and, in its offensive meaning, - offensive cyber power (OCP). The above-mentioned indicator determines directions of concepts of methods of measurements of cyber power, even if it is not expressed *expressis verbis*, as it is the example in the discussed CPI model.

CPI Model

The concept of the model of measurement of the *cyber power index* (CPI) has been processed by a group of The Economist Intelligence Unit (EIU) from the famous magazine 'The Economist' in cooperation with the Booz Allen Hamilton Group. Its purpose is creating rankings of the cyber ability of the states of the G20 Group in the scope of prevention and counteraction of cyber attacks and the promotion of problems of cybersecurity in the international environment. So, there is a *de facto* model of measurement of defensive cyber power.

It relies on calculating indicators of the cyber power of the state.

For this purpose, a matrix of 39 quantitative and qualitative indicators grouped in 4 categories and 19 subcategories, taking into consideration their average weight, was arranged (table 2). The matrix was processed using expert estimates[22].

All the expert indicators showed values growing on a scale from 0 to 100, where the greatest value of cyber power is 100.

Data banks present national and international statistic sources: The Economist Intelligence Unit (EIU), The UN Educational, Scientific and Cultural Organization (UNESCO), The International Telecommunications Union (ITU); The World Bank (WB).

[21] J. Nye, op. cit., p. 7.

[22] The expert estimate method requires, first of all, the careful selection of experts, most often on the basis of formal criterion (degree scientific, professional experience, scientific possesions, awards) or socially-moral (good report of co-worker, reliability, honesty, intransigence). In estimating the averaged estimating group (great liberty speaking out and presenting of results) the differences in individual and group of experts' estimates (possible psychological brake) and ethical aspects must be considered. See: M. Sułek, *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004, p. 167–174.

Table 2

Matrix of indicators and weights of CPI cyber power index model[1]

Category of indicators	Weight [%]	Subcategory of indicators	Weight [%]	Indicators
I. Legal and Regulatory Framework	26.3	I.1. Government commitment ro cyber development	27.1	1. National cyber plan
				2. Public/private partnerships
		I.2. Cyber protection policy	24	3. Cyber enforcement authority
				4. Cybersecurity laws
				5. Cyber crime response
				6. International cybersecurity commitments
				7. Cybersecurity plan
		I.3. Cyber censorship	15.5	8. Cyber censorship
		I.4. Political efficacy	15.5	9. Political efficacy
		I.5. Intellectual property protection	17.8	10. Intellectual property protection
II. Economic and Social Context	25	II.1. Educational levels	25.2	11. Tertiary student enrollment as a percentage of total enrollment
				12. Expected years of education
		II.2. Technical skills	27.4	13. Labour productivity growth
				14. Researchers in research and development per million people
				15. Science and engineering degrees
				16. English literacy
		II.3. Trade	17.3	17. Information and communications technology exports as a percentage of total exports
				18. Information and communications technology imports as a percentage of total imports
				19. Openness to trade
		II.4. Innovation environment	30.1	20. Research and development as a percentage of gross domestic product
				21. Domestic patent filings
				22. Private equity and venture capital as a percentage of gross domestic product
III. Technology Infrastructure	26.3	III.1. ICT Access	20.3	23. Internet penetration
				24. Mobile cellular penetration
				25. Wi-Fi hotspots per million people
				26. Social media penetration
		III.2. ICT Quality	21.9	27. Fixed broadband subscribers per 100 inhabitants
				28. International Internet bandwidth
		III.3. IT Spending	20.3	29. Information technology spending as a percentage of gross domestic product
		III.4. ICT Affordability	11.7	30. Mobile phone tariffs
				31. Broadband Internet tariffs
		III.5 Secure servers	25.8	32. Secure servers
IV. Industry Application	22.5	IV.1. Smart grids	21.1	33. Smart grids
		IV.2. E-Health	16.2	34. E-Health
		IV.3. E-Commerce	30.4	35. Businesses placing orders via the Internet as a percentage of business using the Internet
				36. Individuals placing orders via the Internet as a percentage of Internet users
				37. Individual use of Internet banking as a percentage of Internet users
		IV.4. Intelligent transportation	21.1	38. Intelligent transportation
		IV.5. E Government	11.3	39. E-Government

Source: *Cyber Power Index. Findings and Methodology*, Economist Intelligence Unit, 2011, http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf, p. 22, 24.

[1] Detailed description of definition and principles of allocating of values are placed in the sorurce material of EIU in annex II, p. 26–32.

Weights of categories of indicators are approximated with insignificant domination of category of legal and regulatory indicators and the category of technological infrastructure (*ex aequo* 26.3) coming before the economic and social indicators category (25) and the category of industrial application (22.5).

The cyber power values of 19 states from the G20 (without the European Union) representing five geographic regions were analysed: Western Europe, East Europe and Middle Asia, Middle East and Africa, Asia and Pacific and America.

The values of the indicators are normalised in the proper manner and sum according to categories.

Favourable cyber power indicators (e.g. growth of expense on R&D) are normalised according to the rule:

$$x = \frac{x - Min(x)}{Max(x) - Min(x)}$$

gdzie: *Min(x)* – minimal value of given economic indicator in group of 19 states;

Max(x) – maximal value of given economic indicator in group of 19 states.

This way, normalised values are transformed from partition 0–1 to partition 0–100, which enables them to be directly compared to other indicators in such a way that the state accepts the highest indicator value 100, but the lowest indicator value 0.

Table 3

Expenses on research and development relative to GDP

Country	R&D/GDP
South Korea	4.04
Japan	3.39
Germany	2.93
United States	2.79
Australia	2.39
France	2.26
China	1.98
Canada	1.73
United Kingdom	1.72
Italy	1.27
Brazil	1.21
Russia	1.12
Turkey	0.86
India	0.81
South Africa	0.76
Argentina	0.65
Mexico	0.43
Saudi Arabia	lack data
Indonesia	lack data

Source: The World Bank, Research and development expenditure (% of GDP), http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS (access: 15.10.2015).

Unfavourable indicators of cyber power (e.g. mobile telephone or internet tariffs) are normalised with other rules, at the same designations as above:

$$x = \frac{x - Max(x)}{Max(x) - Min(x)}$$

The measurements of the cyber power of 19 states from G20 indicate the domination of the United Kingdom, the United States, Australia, Germany and Canada (table 4). From all the indicators, Germany has the biggest value in the first legal and regulatory category (99.3), before the United States and United Kingdom (*ex aequo* 97.3).

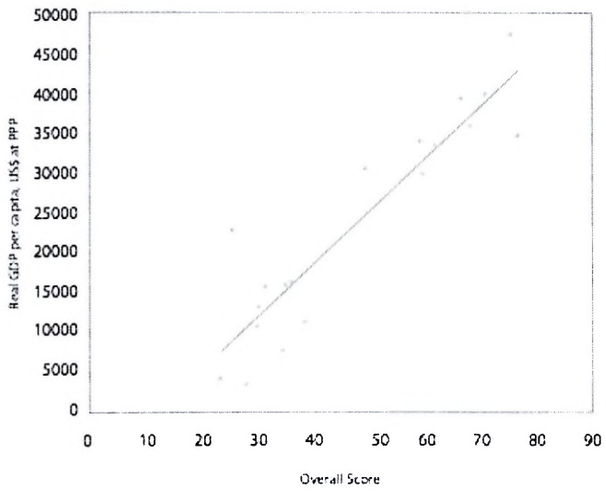
Table 4

Cyber Power Rankings CPI model (2011)

Rank	Country	CPI Score (0–100)	Geografical Region
1	United Kingdom	76.8	Western Europe
2	United States	75.4	America
3	Australia	71.0	Asia-Pacific
4	Germany	68.2	Western Europe
5	Canada	66.6	America
6	France	61.8	Western Europe
7	South Korea	59.7	Asia-Pacific
8	Japan	59.3	Asia-Pacific
9	Italy	49.5	Western Europe
10	Brazil	38.6	America
11	Mexico	36.3	America
12	Argentina	35.4	America
13	China	34.6	Asia-Pacific
14	Russia	31.7	Eastern Europe & Central Asia
15	Turkey	30.4	Eastern Europe & Central Asia
16	South Africa	30.2	Middle East & Africa
17	India	28.3	Asia-Pacific
18	Saudi Arabia	25.7	Middle East & Africa
19	Indonesia	23.5	Asia-Pacific

Source: *Cyber Power Index*..., p. 4.

The functional CPI model enables scaling of correlation among indicators. The authors of this model have also measured the correlation of value of GPD indicator on an inhabitant with the general value of the cyber power of 19 states, achieving a surprisingly high result – 0.92 (Figure 1).



Source: *Cyber Power Index*..., p. 23.

Figure 1. Scatter Plot of overall Cyber Power Rankings and GDP

The authors of the CPI model really only gauge the defensive cyber power, though they do not declare it in the foundations Categories of indicators have very similar weights, which, in this respect, approximate this method for so called 'natural weight' about the equal weights and even schedule of indicators. However, disparity is distinct at the level of subcategory weights which amount to 100 for a given category.

It is hard to challenge the selection of indicators in this model, although in the category of social and economic indicators the undercategory economic indicators is not marked, despite the authors regarding themeaning of GPD *per capita* indicator as a very high indicator of correlation with the general CPI of G20. The United Kingdom's position as leader ahead of the United States is also puzzling.

A.M. Gomez Model

The concept of measurement of cyber power of states has been based on the method suggested by Alberto Miguela Gomeza[23] and is also based on the indicator method, in which 50 indicators divided in 6 categories are placed: 1) infrastructure, 2) economy, 3) scientific research, 4) politics and e-goverment, 5) social-politic and 6) military. On the basis of the measurement result of cyber power and analyses of events (state's behaviour) in cyberspace (subject attacking, object attacked and frequency), A.M. Gomez has differentiated four categories of states regarding offensive and defensive behaviour in cyberspace (table 5)[24]. Next, using statistic analysis, he has defined the kind of applicable attack for each category of state, taking into consideration the role of the attacking and attacked subject (table 6). However, the construction matrix rule of the type of cyberattack proposed by A.M. Gomez is unclear. In the case of the same category of states taking a stand simultaneously in the role of attacking and attacked subject, there is obliged to be an empty field. For example, field [EP-I; EP-I] means that the United States is the attacking and attacked subject as well?

Tabel 5

Category of State in Cyberspace

Category of State	Country
Established Defensive I (EP-I)	United States
Emerging Offensive I (EA-I)	China
Established Defensive II (EP-II)	Australia, Canada, New Zealand, Singapore, Japan, South Korea, Philippines, Russia, Israel
Emerging Offensive II (EA-II)	Chile, Indonesia, Malaysia, Mexico, Peru, Thajland, Vietnam, India, Iran, Pakistan, Bangladesh, Syria, Cyprus, Turkey, Iraq, Kuwait, Georgia, Lebanon

Source: A.M. Gomez, op. cit., p. 5, FireEye, *World war c: Understanding nation-state motives behind todays advanced cyber attacks*, FireEye, Tech. Rep.

Tabela 6

Attack Type Matrix

	Target			
Initiator	**EP-I**	**EA-I**	**EP-II**	**EA-II**
EP-I	Network Attack	Malware	Network Attack	Malware
EA-I	Information Theft	Network Attack	Malware	Malware
EP-II	Malware	Defa-cement	DoS/ DDoS	Malware
EA-II	Defacement	Network Attack	DoS/ DDoS	Defa-cement

Source: A.M. Gomez, op. cit., p. 6.

[23] From the source of article it is hard to conclude, if A.M. Gomez is the author of this model or he characterizes it only. However, according to the conventionall terminology in this article, author calls its as A.M. Gomez model. See: A.M. Gomez, *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (access: 27.01.2015), p. IIIA.

[24] A.M. Gomez names categories of states as passive (established passive, EP) and aggressive (emerging aggressive, EA). The author prefers a defensive and offensive terminology, but he leaves summaries of designations the same as the original.

States classified for two defensive categories - EP-I (leaders) and EP-II (other) - feature a predominating value of indicators from these categories: infrastructures, economies, scientific research and politics and e-government, by remaining at their simultaneously positive correlations with the other indicators category. However, the states from the offensive category group (EA-I; EA-II) are characterised with low value indicators, and at a high level of indicators from the social and political category and especially from the military group predominating indicator (especially EA-I). Simultaneously, a negative correlation takes a stand among indicators from the first four categories and the social and political indicators. States from the offensive category also feature a constant growth of infrastructure and economic indicators. China is the leader of the offensive states (EA-I), whose general and military power has been dynamically growing for some years achieving third place in the world after the United States[25]. However, the United States is the leader in the category of defensive states (EP-I).

On the basis of these results, A.M. Gomez has differentiated three fundamental strategies of states in cyberspace:

- *maintenance of cyber power strategy* – used by states actively demonstrating their own ability in cyberspace, to increase their general power;
- *achievement balance strategy* - it relies on the aspiration of states for maximising cyberpower to obtain an advance on potential attackers in cyberspace and to escape a conflict situation, which can decrease its general power (e.g. in the economic sphere).
- *demonstration of cyber power strategy* – used by states to demonstrate their incremental ability in cyberspace.

In his model for measuring the cyber power of the state, A.M. Gomez gives no methodological details, concentrating mainly on its implementation in the definition of the category of strategy of states in cyberspace, in a defensive and offensive character. He concludes that three categories of the strategies of states can cause doubt. In principle, all states aim at escalation of power on measuring their own capability in cyberspace - the United States and China as well. The other problem is its demonstration in some activities. The United States role as leader in the category of defensive states directed to them to be suspicious about the cyber attack behind the computer bug 'Stuxnet'.

Conclusion

The definition of cyber power in the literature mostly concerns the state as a basic political unit. The author has accepted such terminological conventions in the article too. However, this means the need to perceive cyber power not only in its subjective meaning but also in the objective sense, e.g. defensive and offensive cyberpower. The above-mentioned indicators determine the choice and implementation of its method of measurement and achieving results. In accordance with the lack of a generally recognised definition of cyber power, researchers addressing this problem should accept individual terminological convention, appropriatefor the accepted research method. The choice of CPI model means research of exclusively defensive cyber power only, though authors do not define this fact. A.M. Gomez'z model is more compound from its foundation, because it allows the defining of state strategy in cyberspace on the basis of the indictators method, in respect of their defensive and offensive abilities too. A.M. Gomez's division into three main strategies introduces doubt, even in view of the fact that *de facto* all states, after measuring their own abilities, tend to increase their cyber power – including China and the United States. Both methods take advantage of the generally known indicators method applied in early warning algorythms. Some indicators of measurements of cyberpower are common for both types of models (e.g. economic or technological), some of them feature individually (e.g. military in the second model). In A.M. Gomez's results of measurement, the absence of the United Kingdom is puzzling, as it is the absolute leader in the state cyberpower rankings in the CPI model. The United States is placed as leader of the group of defensive states, in accordance with general suspicion about the cyber attack by the computer bug 'Stuxnet'.

The author concludes that the above-mentioned methods of measurements of the cyber power of states do not completely solve the research problem and should be treated as proposals for further advanced research of this problem not only considering the state but also the other subjects of the international security system (e.g. terrorist organisations).

[25] See: M. Sułek, *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013, p. 168–193.

Bibliography

Białoskórski R., *Bezpieczeństwo informacji. Słownik pojęć i skrótów*, Wyd. Ubezpieczeń, Warszawa 2010.

Białoskórski R., *Cyberthreats in the Security Environment of the 21st Century*, 'Journal of Security and Sustainability Issues' 2012, No. 4.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Wyd. WSCiL, Warszawa 2011.

Białoskórski R., *Modelowanie konfliktów zbrojnych z wykorzystaniem procesu analizy hierarchicznej - kazus syryjski*, in: M. Sułek (ed.), *Potęgometria*, Vol. 2, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2015.

Cyber Power Index. Findings and Methodology, Economist Intelligence Unit, 2011. http://www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf (access: 27.01.2015).

Department of Defense Strategy for Operating in Cyberspace, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (access: 27.01.2015).

Gomez A.M., *Identifying Cyber Strategies vis-a-vis Cyber Power*, http://www.academia.edu/6544932/Identifying_Cyber_Strategies_vis-a-vis_Cyber_Power (access: 27.01.2015).

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, in: D. Kramer, H. Stuart, i L.K. Wentz, *Cyberpower and National Security Policy*, National Defense University, Potomac Books, Inc., 2009. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf (access: 27.01.2015).

Mattioli R., *The «State(s)» of Cybersecurity*, in: Giampiero Giacomello (ed.), *Security in Cyberspace*, New York; London; New Delhi; Sydney, Bloomsbury, 2014.

Mazur M., *Cybernetyka i charakter*, Edition 2, Wyd. Podkowa Leśna; Wyd. AULA, 1996.

National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23, 8 January 2008, https://epic.org/privacy/cybersecurity/EPIC-FOIA-NSPD54.pdf (access: 27.01.2015).

Nye J.S., *Cyber Power*, Cambridge: Harvard Kennedy School, 2010, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (access: 27.01.2015).

Panas E., *Potęga transnarodowych organizacji społeczeństwa obywatelskiego*, in: M. Sułek (ed.), *Potęgometria*, tom I, Wyd. Europejskie Centrum Analiz Geopolitycznych, Warszawa 2013.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 25 June 2013, http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html (dostęp: 27.01.2015).

Rattray G.J., *An Environmental Approach to Understanding Cyberpower*, 13 January 2015. http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-10.pdf (access: 27.01.2015).

Słownik Języka Polskiego, http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (access: 27.01.2015).

Słownik komputerowy i encyklopedia informatyczna, http://www.i-slownik.pl/323,cyberprzestrzen (access: 27.01.2015).

Sułek M., *Metody i techniki badań stosunków międzynarodowych*, Oficyna Wyd. ASPRA-JR, Warszawa 2004.

Sułek M., *Potęga państw. Modele i zastosowania*, Wyd. Rambler, Warszawa 2013.

The National Strategy to Secure Cyberspace, The White House Washington, February 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (access: 27.01.2015).

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

płk dr Artur DĘBCZAK
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

ppłk Cezary PAWLAK
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

ANALITYCZNY MODEL OCENY HYBRYDOWOŚCI WSPÓŁCZESNYCH KONFLIKTÓW

kmdr por. Jarosław KEPLIN
Oddział Rozwoju Koncepcji
Centrum Doktryn i Szkolenia SZ

Streszczenie

Celem powyższego opracowania jest wyjaśnienie istoty działań hybrydowych, określenie ich przebiegu w poszczególnych fazach oraz zdefiniowanie i przedstawienie propozycji narzędzia (modelu analitycznego).

W opracowaniu scharakteryzowano hybrydowość współczesnych konfliktów oraz pojęcia zidentyfikowane podczas prac nad narodową Koncepcją udziału sił zbrojnych w przeciwdziałaniu zagrożeniom hybrydowym, realizowaną przez Centrum Doktryn i Szkolenia Sił Zbrojnych w ścisłej współpracy z grupą ekspertów dziedzinowych. Przedstawiono opracowaną propozycję modelu analitycznego opisującego przebieg możliwych zagrożeń we wszystkich rozpatrywanych obszarach, tj. politycznym, ekonomicznym, społecznym, militarnym, infrastruktury i informacyjnym (PEMSII).

Słowa kluczowe: bezpieczeństwo, hybrydowość, działania hybrydowe, strategia, zagrożenia, analityczny model działań hybrydowych

Wstęp

Metody stosowane podczas wojen XXI wieku wzbudzają szereg refleksji wśród licznych ekspertów na temat przyszłych środków i sposobów zapewniających bezpieczeństwo wewnętrzne i zewnętrzne państwa oraz stabilność regionu.

Kompleksowy charakter współczesnych konfliktów rozumiany jest jako szeroko pojęta *hybrydyzacja* i stanowi wyzwanie dla jej zrozumienia, a zarazem opracowania nowych rozwiązań do przeciwdziałania. Powinny one uwzględniać aktualne środowisko bezpieczeństwa, w tym jego asymetrię, podziały kulturowe i skutki uboczne globalizacji, gdyż stały się one obecnie jednym z głównych wyzwań dla zapewnienia bezpieczeństwa współczesnego świata.

Celem niniejszego artykułu jest wyjaśnienie istoty działań hybrydowych, ich zdefiniowanie oraz przedstawienie propozycji narzędzia do określenia przebiegu działań w poszczególnych fazach.

W części pierwszej opracowania scharakteryzowano hybrydowość współczesnych konfliktów oraz pojęcia zidentyfikowane podczas prac nad narodową koncepcją[1] realizowaną przez Centrum Doktryn i Szkolenia Sił Zbrojnych (CDiS SZ).

[1] Prace nad koncepcją realizowane są przez zespół projektowy CDiS SZ w ścisłej współpracy z grupą ekspertów dziedzinowych krajowych i zagranicznych. Prace te rozwijane są także w ramach Wielonarodowej Kampanii Rozwoju Zdolności (Multinational Capability Development Campaign – MCDC). Zakres pojęciowy w zakresie definicji i faz działań

W części drugiej, bazując na przyjętej terminologii oraz opisie faz, przedstawiono propozycję modelu analitycznego opisującego przebieg możliwych zagrożeń we wszystkich rozpatrywanych obszarach: politycznym, ekonomicznym, społecznym, militarnym, infrastruktury i informacyjnym (PEMSII)[2].

Działania hybrydowe – istota i terminologia

Współczesne konflikty zbrojne zarówno o charakterze regionalnym, jak i szerszym zasięgu, cechuje kompleksowość wykorzystania wszelkich możliwych środków. Wstępne analizy wskazują na zależności względem faz realizacji planu oraz przyjętych przez agresora celów polityczno-strategicznych. Ich kompleksowy charakter rozumiany jest jako szeroko pojęta hybrydyzacja i stanowi wyzwanie dla jej zrozumienia, a zarazem opracowania nowych rozwiązań w celu przeciwdziałania im.

Od kilku lat obserwuje się narastające wzajemne przenikanie i łączenie technik wojny regularnej i nieregularnej. Dodatkowo powszechnym zjawiskiem w polityce stało się uzależnianie ekonomiczno-gospodarcze przez potencjalnego agresora. Ponadto widoczne jest szerokie spektrum oddziaływania na społeczeństwa, grupy narodowe, etniczne czy religijne poprzez środki informacyjne i zabiegi dyplomatyczne. Doświadczenia wskazują, że rozwiązania te powinny uwzględniać m.in. obecne środowisko bezpieczeństwa, w tym jego asymetrię, podziały kulturowe i skutki uboczne globalizacji. Wynika to z faktu, że stały się one jednym z głównych wyzwań dla zapewnienia bezpieczeństwa współczesnego świata. Różnorodność środowiska bezpieczeństwa, a przede wszystkim skala wykorzystywanych środków, jest obecnie tematem licznych analiz i opracowań.

Można wnioskować, że kompleksowość działań oraz trudność ich wykrycia są efektem globalizacji, która może destrukcyjnie wpłynąć na narodowe sektory ekonomiczno-gospodarcze, pozwalając jednocześnie ukryć działania agresora, np. przez fikcyjne organizacje pozarządowe, firmy i korporacje.

Ponadto powszechny dostęp do informacji oraz manipulacja nią mają istotny wpływ na populacje, grupy mniejszości narodowych, etnicznych oraz religijnych, kreując tym samym panujące w nich nastroje. Zjawisko to powszechnie zaczęto nazywać *działaniami hybrydowymi* lub *wojną hybrydową*.

Etymologia terminu *hybrydowość* prowadzi do łacińskiego słowa *hybryda*, oznaczającego *mieszańca*, osobnika powstałego ze skrzyżowania dwóch genetycznie różnych osobników, należących do różnych gatunków odmian czy ras[3].

Jedną z pierwszych osób popularyzujących termin *wojna hybrydowa* był Frank G. Hoffman[4]. Według niego, wojna hybrydowa cechuje się *zbieżnością* [...] *fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów* [...] *sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone*[5].

Termin *wojna hybrydowa* zawęża pojęcie hybrydowości i utożsamiane jest z siłami zbrojnymi, które stanowią de facto minimalną część w całym spektrum działań podjętych przez potencjalnego agresora. Ponadto należy zauważyć, że powszechnie używany w anglojęzycznych opracowaniach termin *hybrid warfare* jest błędnie interpretowany jako wojna hybrydowa. Hybrydowość niesie za sobą złożoność i wielopłaszczyznowość działań, dlatego należy wziąć pod uwagę liczne, często krytyczne uwagi dotyczące terminu *wojna hybrydowa*, w tym aspekty prawne bezpośrednio z nim związane, takie jak brak wypowiedzenia wojny oraz wprowadzenia stanu wyjątkowego lub wojennego.

Zrozumienie charakteru tych działań oraz dokonanie zmian w postrzeganiu współczesnych konfliktów wymusza dostosowanie istniejących i wypracowanie nowych dokumentów normujących funkcjonowanie wszystkich resortów państwa odpowiedzialnych za jego bezpieczeństwo.

hybrydowych uzgodniono w ramach prac grupy roboczej ds. rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym* w dniu 16 września 2015 r. w Bydgoszczy.

[2] Metoda PEMSII zwana generalną segmentacją otoczenia. Dzieli otoczenie na: Polityczne, Ekonomiczne, Militarne, Społeczne, Infrastruktury, Informacyjne.

[3] *Słownik wyrazów obcych PWN*, Warszawa 1980, s. 290.

[4] Emerytowany ppłk marines, pracownik naukowy Instytutu Studiów Strategicznych Narodowego Uniwersytetu Obrony USA. Międzynarodowy Instytut Badań Politycznych (FPRI) www.fpri.org/taxonomy/tem/413/0.

[5] A. Gruszczak, *Hybrydowość Współczesnych Wojen – analiza krytyczna*. Artur Gruszczak www. bbn.gov, s.13. za Frank. G. Hoffman, *Hybrid Warfare and Challenges*, Joint Force Quarterly, 2009. Nr 52, s. 34.

Rozwiązania te mają przygotować struktury państwa do nowych wyzwań, w tym identyfikacji zagrożeń[6] i szacowania ryzyka[7]. Istnieje pilna potrzeba znalezienia nowych rozwiązań w zakresie zapewniania i utrzymywania bezpieczeństwa państwa oraz dostosowania strategii prowadzenia działań z użyciem sektora militarnego i pozamilitarnego, a przede wszystkim sposobów wykrywania symptomów zagrożeń i przeciwdziałania ich rozwojowi.

Biorąc pod uwagę szerokie spektrum, charakter i skalę działań oraz fakt, że celowo są ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się jednoznacznie zidentyfikować progu regularnej wojny, należy stosować w opracowaniach termin *działania hybrydowe* zamiast *wojna hybrydowa*.

Działania hybrydowe oddziałują na wszystkie lub wybrane obszary PEMSII z niejednolitą intensywnością oraz w różnym przedziale czasu, często w granicach obowiązującego prawa, zwłaszcza w początkowej fazie. Ich wzajemne relacje, przenikanie do kolejnych obszarów oraz powodowanie eskalacji zagrożeń wpisują się jako zespół przyczynowo-skutkowy w definicje ww. działań. W celu określenia możliwości wystąpienia działań hybrydowych należy scharakteryzować i skategoryzować obszary PEMSII pod względem ewentualnych zagrożeń z uwzględnieniem ich wagi, przyszłych trendów oraz występujących symptomów.

Należy zaznaczyć, że przede wszystkim działania hybrydowe muszą spełniać określone warunki dla powodzenia realizacji zakładanych celów długoterminowych. Oznacza to, że w każdym lub w kilku wybranych obszarach dane zagrożenia powinny osiągnąć tzw. punkty przełamania[8] w celu powodzenia realizacji planu, aby utrudnić lub uniemożliwić przeciwdziałanie. Większość tych przedsięwzięć realizowanych jest w pierwszej fazie jako działania skryte, wykorzystujące dane otoczenie, uwzględniające własny potencjał oraz zmiany i trendy w środowisku bezpieczeństwa. Dotychczasowe doświadczenia oraz te z przeszłości wskazują, iż obszar społeczny oraz ekonomiczny stanowią największe i najpoważniejsze zagrożenie. Przykładem są działania prowadzone na wschodzie Ukrainy oraz przez tzw. Państwo Islamskie.

Ujednolicenie glosariusza terminologii[9] w obszarze działań hybrydowych pozwoliło na opracowanie faz działań hybrydowych oraz modelu działań hybrydowych.

Fazy działań hybrydowych

Wiele krajów dostrzega zmiany w kontekście nowych wyzwań i zagrożeń, przede wszystkim w wykorzystaniu metod i skali ich występowania. Widoczne jest to na przykład w opracowaniu W. Gierasimowa[10], który przedstawił swój model[11] w postaci schematu składającego się z sześciu etapów narastania konfliktu oraz diagramu obrazującego połączenie działań militarnych i niemilitarnych. Wyróżnia on następujące fazy:

- działania utajnione,
- zaostrzenie,
- rozpoczęcie działań sygnalizujących konflikt,
- kryzys,
- rozstrzygnięcie,
- przywrócenie pokoju.

Na uwagę zasługuje także opracowanie fińskie[12]. Ujęto w nim sześć faz takich działań:

- przygotowanie strategiczne,
- przygotowanie polityczne,
- przygotowanie operacyjne,
- eskalacja napięcia,

[6] Zagrożenia – wszelkie destrukcyjne oddziaływania na podmiot, egzemplifikujące się w postaci sytuacji kryzysowych, a nawet kryzysów. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[7] Ryzyko – prawdopodobieństwo wystąpienia niekorzystnego zdarzenia wraz z jego skutkami w określonym czasie. Ocena ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa. Warszawa 2013, s. 13.

[8] Dla niniejszego opracowania przyjęto, że w układzie współrzędnych kartezjańskich punktem przełamania, jest punkt na wykresie obrazujący moment identyfikacji zagrożenia, gdzie należy podjąć wysiłki do zniwelowania skutków oddziaływania agresora. Zmienna ta na wykresie, charakteryzuje się zmianą jej wypukłości. Patrz Rys. nr 3. Przykładowy wynik analitycznego modelu zagrożeń hybrydowych.

[9] Terminologia została zawarta w załączniku nr 1.

[10] Generał Walerij Gierasimow – Szef Sztabu Generalnego Federacji Rosyjskiej.

[11] Przekład z: Валерий Герасимов, Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

[12] Andras Racz, Russia's Hybrid War in Ukraine. Fiński Instytut Stosunków Międzynarodowych Raport 43 z 2015, s. 59–63.

– obalenie władzy centralnej w regionie docelowym,

– ustanowienie alternatywnej władzy.

Dla porównania w opracowaniu łotewskiej[13] Narodowej Akademii Obrony wymieniono osiem faz tzw. wojny nowej generacji, które zawierają poniższe działania:

– niemilitarne, wpływające negatywnie na społeczność, ekonomię i działania polityczne,

– ukierunkowane na wprowadzenie w błąd ośrodków dyplomatycznych, politycznych oraz medialnych,

– mające na celu zastraszenie ludności i wskazanie bezcelowości dalszego oporu,

– destabilizacyjne i propagandowe,

– wprowadzające strefy zakazu lotów,

– oznaczające rozpoczęcie działań militarnych poprzez intensyfikację rozpoznania i użycie sił specjalnych,

– wielopłaszczyznowe, w tym informacyjne, dyplomatyczne oraz militarne jako wywarcie presji z użyciem paramilitarnych i regularnych sił zbrojnych,

– mające na celu zniszczenie sił przeciwnika przez siły specjalne i precyzyjne uderzenia oraz wojska lądowe.

Brak jednolitych opracowań w tym zakresie w NATO oraz państwach UE spowodowały konieczność podjęcia prac narodowych[14].

Dla pełnego zrozumienia badanej kwestii zespół autorski poddał analizie konflikty z elementami hybrydowymi, takie jak: w Somalii, w Libanie, na wschodzie Ukrainy oraz działania Państwa Islamskiego. W wyniku tych prac ujednolicono wszystkie występujące przypadki jako uniwersalne fazy przebiegu działań hybrydowych.

Wyróżniono następujące fazy działań hybrydowych (tab. nr 1). Szczegółowy opis faz przedstawiono w zał. nr 2:

– przygotowania;

– destabilizacji;

– działań militarnych;

– rozstrzygnięcia.

Tabela 1

Poglądowy schemat faz działań hybrydowych

FAZA I PRZYGOTOWANIA		FAZA II DESTABILIZACJI	FAZA III DZIAŁANIA MILITARNE	FAZA IV ROZSTRZYGNIĘCIE
CZĘŚĆ SKRYTA	CZĘŚĆ JAWNA			

Opracowanie własne.

Działania w fazie przygotowania można podzielić na dwie części: skrytą i jawną. Działania w części skrytej mają charakter niejawny. Charakteryzują się m.in. tym, że wykorzystywane są różnego rodzaju sposoby nacisku i wpływu kierowane przez korporacje, organizacje pozarządowe i religijne. Cechą szczególną tej fazy jest to, że potencjalne państwo, które jest celem ataku, nie jest świadome, że są prowadzone przeciwko niemu skoordynowane działania. Ich znaczenie jest kluczowe dla przygotowania i prowadzenia dalszych działań przez agresora. Działania te przechodzą w część jawną wtedy, kiedy państwo będące celem ataku **zauważa** działania wymierzone przeciwko niemu. W tej części fazy można dostrzec tworzenie atmosfery nieuchronności krachu finansowego, bezradność organów rządzących, słabość resortów siłowych oraz możliwość wystąpienia konfliktu zbrojnego przy zachowaniu dotychczasowej polityki zarówno na arenie dyplomatycznej, jak i gospodarczej. Następuje psychologiczne i ideologiczne rozbudzanie separatyzmów i dążeń ideologicznych lub religijnych.

Efektywna realizacja fazy przygotowania gwarantuje przejście do kolejnej – fazy destabilizacji. Charakteryzuje się ona m.in. zakłóceniem działania centralnych i lokalnych ośrodków władzy, struktur siłowych, przedstawicieli mediów i biznesu przy wykorzystaniu metod i narzędzi powszechnie stosowanych (politycznych, ekonomicznych, gospodarczych i społecznych, itp.), jak i zaawansowanych technologicznie (np. cyberatak). W tej fazie wyszczególnić można szeroko zakrojone działania informacyjne – opcjonalnie dezinformacyjne (na wszystkich poziomach: od komunikacji strategicznej po przekazy lokalne) za pomocą wszelkich dostępnych środków przekazu

[13] Janis Berzins, Rassia's New Generation Warfare in Ukraine. Implikations for Latvian Defense Policy National Defence Academy of Latvia. Policy Paper nr 2 z 2014, s. 6. Za Techikinov i Bogdanov 2013, s. 15–22.

[14] Zadanie opracowania *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym*, zlecone przez Szefa Sztabu Generalnego WP.

informacji na obszarze ewentualnego konfliktu oraz w jego otoczeniu międzynarodowym w celu osiągnięcia pożądanej reakcji. Jeżeli celem głównym agresora będzie jedynie destabilizacja pewnych obszarów danego kraju, to działania te mogą się zakończyć. W przypadku, gdy cele agresora nie są całkowicie osiągnięte, może on przejść do kolejnej fazy, tj. działań militarnych.

Na tym etapie zauważyć można m.in. tworzenie lokalnych oddziałów separatystów złożonych np. z mniejszości narodowych lub religijnych działających przy wsparciu przywódców duchowych, organizacji terrorystycznych, sił zbrojnych oraz służb specjalnych agresora. Ich głównym zadaniem jest podsycanie napięcia, potwierdzenie bezradności władz oraz zablokowanie możliwości prowadzenia akcji przez resorty, siłowe np. policję, armię atakowanego kraju i w skoordynowany sposób przejęcie kontroli nad kluczowymi obiektami i obszarami mającymi wpływ na powodzenie operacji. Do obiektów posiadających szczególne znaczenie można zaliczyć m.in. przejścia graniczne, stacje przekaźnikowe mediów, kluczową infrastrukturę taką jak główne skrzyżowania dróg, mosty oraz węzły kolejowe i lotniska. Należy podkreślić, że w tej fazie działania militarne wspierane są przez skoordynowane i szczegółowo zaplanowane działania dyplomatyczne oraz informacyjne.

Ostatnią zdefiniowaną fazą jest rozstrzygnięcie. Charakteryzuje się ona ustanowieniem władz centralnych i lokalnych zależnych od agresora. Rozstrzygnięciem jest przede wszystkim akceptacja wymuszonej sytuacji politycznej. Przy niepowodzeniu zakładanych celów działań hybrydowych, po fazie działań militarnych może dojść do otwartego regularnego konfliktu zbrojnego. Jednakże w tym przypadku **nie są to** działania hybrydowe.

Analityczny model działań hybrydowych

Zagrożenia we współczesnym świecie charakteryzują się różnorodnością i złożonością ich występowania. Warto podkreślić, że bezpieczeństwo państwa[15] nie jest jedynie stanem, ale przede wszystkim dynamicznym procesem, na który mają wpływ różnorodne determinanty[16]. Powoduje to trudności w dokonaniu właściwej oceny zagrożenia. Złożoność jego występowania w poszczególnych obszarach znacznie komplikuje możliwość znalezienia właściwej metodyki, niezbędnej do określenia faktycznego wpływu na zagrożenia[17].

Zasadne jest wykorzystanie metody modelowania[18]. Tworząc modele i konfrontując je z rzeczywistością m.in. poprzez obserwację, sprawdza się, jakie prawa rządzą zachodzącymi zjawiskami. Zrozumienie powyższego stanowi inherentny czynnik pozwalający przewidzieć przebieg zjawisk w przyszłości[19]. Dotyczy to także problematyki bezpieczeństwa państwa. Jak zauważa Anna Antczak-Barzan[20] *brak umiejętności identyfikacji potencjalnych zagrożeń w ujęciu długofalowym na podstawie rozwijających się trendów wewnętrznych i zewnętrznych (w bliższym i dalszym otoczeniu państwa) może prowadzić do katastrofy. Polityka krótkowzroczności oraz dbania o partykularne prywatne interesy oraz walki pomiędzy poszczególnymi frakcjami politycznymi już nieraz doprowadziły nasze państwo do klęski*[21].

Powyższe ustalenia i wnioski są podstawą do stwierdzenia, że zidentyfikowane zagrożenia powinny być poddane systematycznej analizie i monitorowaniu. Obecnie opracowany analityczny model zagrożeń hybrydowych ma za zadanie pomóc zrozumieć symptomy i mechanizmy powstawania zagrożeń, a także umożliwić identyfikowanie nowych, które mogą w istotny sposób wpłynąć na funkcjonowanie i możliwości rozwoju państwa, a w szczególności mogą mieć istotne znaczenie dla bezpieczeństwa zarówno wewnętrznego, jak

[15] Bezpieczeństwo państwa – taki rzeczywisty stan stabilności wewnętrznej i suwerenności państwa, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń (w sensie zaspokojenia podstawowych potrzeb egzystencjonalnych i behawioralnych społeczeństwa oraz traktowania państwa jako suwerennego podmiotu w stosunkach międzynarodowych). *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydanie szóste, AON, Warszawa 2002, s. 19.

[16] Szerzej zob. A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 226.

[17] Zagrożenia – wszelkie destrukcyjne oddziaływania na podmiot, egzemplifikujące się w postaci sytuacji kryzysowych, a nawet kryzysów. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[18] Modelowanie matematyczne i badanie złożonych układów analitycznych. Maciej Rymanowski, Kraków 2007, s. 11.

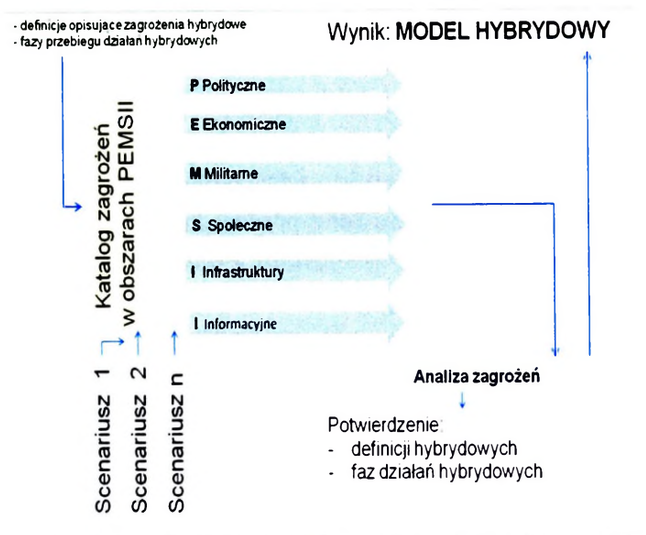
[19] Ibidem.

[20] Dr hab nauk społecznych w zakresie nauk o polityce (PAN).

[21] A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 238.

i zewnętrznego. Takie podejście powinno również przyczynić się do przygotowania narzędzi przeciwdziałania potencjalnym zagrożeniom.

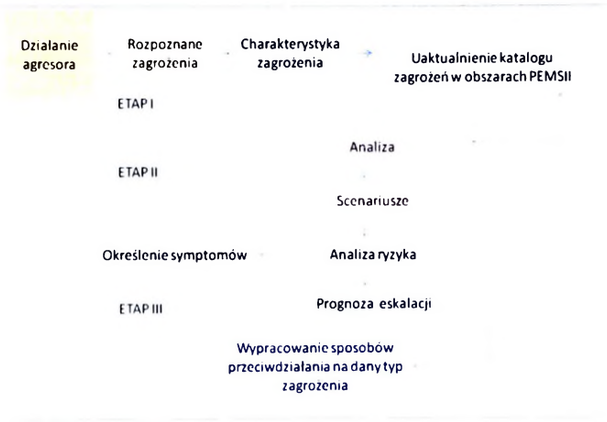
Przygotowując analityczny model działań hybrydowych przyjęto określone założenia. Po pierwsze, prace prowadzi się w oparciu o metodykę zarządzania projektem PRINCE2[22]. Miało to na celu wykorzystanie efektywnych zasad zarządzania, które są niezbędne podczas realizacji projektu, w tym zapewnienia usystematyzowanego podejścia gwarantującego jego powodzenie. Niemniej należy pamiętać, iż metodyka ta dostarcza wiedzę na temat stosowanych technik, ale nie precyzuje szczegółowo jak z nich korzystać. Kolejne ustalenie to określenie danych wejściowych. Zaliczono do nich: katalogi zagrożeń w obszarach PEMSII, definicje z obszaru zagrożeń hybrydowych oraz fazy przebiegu działań hybrydowych. Na potrzeby opracowania analitycznego modelu założono także, że środowisko bezpieczeństwa będzie podzielone na obszary: polityczne, ekonomiczne, militarne, społeczne, infrastruktury oraz informacyjne. Zespół autorski w trakcie prowadzonych badań zdefiniował dla każdej z wymienionych domen osobny katalog zagrożeń wraz z ich charakterystyką. Ideę modelu przedstawia rys. 1:



Opracowanie własne.

Rys. 1. Schemat ideowy analitycznego modelu zagrożeń hybrydowych

W trakcie opracowywania modelu hybrydowego przyjęto następującą metodologię procesu przetwarzania danych (rys. 2):



Opracowanie własne.

Rys. 2. Metodologia procesu analizy zagrożenia

W pierwszym etapie procesu, na podstawie zagrożeń wynikających z działania agresora, dokonuje się charakterystyki zagrożenia i umieszczenia go w katalogach. W drugim etapie wybiera się newralgiczne zagrożenie celem przeprowadzenia jego analizy oraz opracowania scenariuszy przypadków. Scenariusze te obejmują ogół czynności mających na celu zrozumienie czynników wywołujących te zagrożenia oraz symptomy ich powstania i zachodzące między nimi związki. W ramach tego etapu poszczególne zagrożenia bada się m.in. ze względu na:

– intencje: interes, potrzeby, politykę, wolę,

– możliwości: zdolności, metody, zasoby, ograniczenia,

– dane historyczne: przypisane incydenty, podejmowane próby, potwierdzone operacje, częstotliwość, efektywność tych działań,

– sygnały: nowe potwierdzone lub niepotwierdzone dowody.

Takie podejście daje możliwość oszacowania ryzyka wystąpienia zagrożeń. W założeniach przyjęto, że przy szacowaniu ryzyka istotne będą: zidentyfikowane zagrożenia z katalogu, prawdopodobieństwo zaistnienia, podatność obszarów PEMSII oraz ich wpływ i skutki na bezpieczeństwo państwa. Należy podkreślić, że oszacowanie wartości dwóch podstawowych parametrów składowych, tj. prawdopodobieństwa i skutków, jest kluczowe dla określania podatności na ryzyko. Poziom ryzka szacowany jest w oparciu o użycie dyskretnej skali stopniowania prawdopodobieństwa, która została przedstawiona poniżej (tab. 2).

[22] PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009. Metodyka zarządzania projektami. Stosowana do sterowania i zarządzania projektami.

Tabela 2

Dyskretna skala stopniowania prawdopodobieństwa

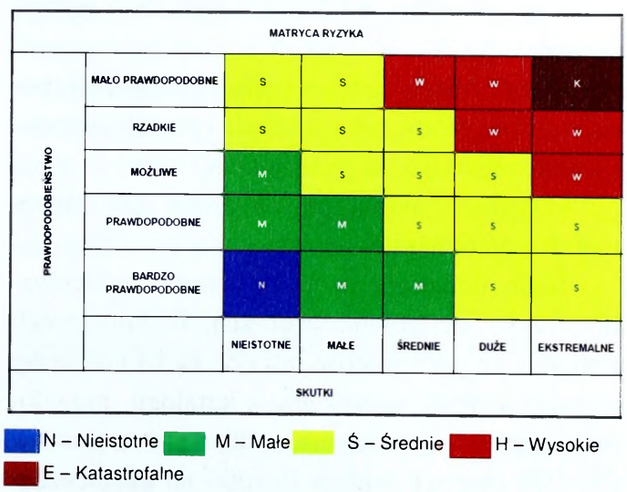
MAŁO PRAWDOPODOBNE	Zagrożenia wcześniej niezidentyfikowane i nieudokumentowane, które mogą wystąpić tylko w wyjątkowych i sprzyjających okolicznościach. Przyjmują wartość 0–20%
RZADKIE	Zagrożenia udokumentowane, symptomy czy też inne okoliczności zagrożenia są mało znane. Przyjmują wartość 20–40%
MOŻLIWE	Zagrożenia udokumentowane, symptomy czy też mechanizm powstawania znany. Może zdarzyć się w określonym czasie w sprzyjających warunkach. Przyjmują wartość 40–60%
PRAWDOPODOBNE	Zagrożenia znane i wcześniej spotykane. Jest prawdopodobne, że w przypadku sprzyjającego środowiska wystąpią w większości okoliczności. Przyjmują wartość 60–80%
BARDZO PRAWDOPODOBNE	Zagrożenia doskonale znane i systematyczne. Panuje odpowiednie środowisko dla ich powstania. Oczekuje się, że zagrożenia te zdarzą się w większości okolicznościach. Przyjmują wartość 80–100%

Źródło: Opracowanie własne w oparciu o: *Ocenę ryzyka na potrzeby zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

Oszacowana wartość ryzyka na matrycy odzwierciedla zależność pomiędzy prawdopodobieństwem oraz skutkami[23]. Każdemu zidentyfikowanemu ryzyku odpowiada jedno określone pole (patrz tab. 3).

Tabela 3

Matryca ryzyka



Źródło: Opracowanie własne na podstawie: Field Manual No. 5–19 (100–14), Composite Risk Managemement, Department of the Army. Washington, DC, July 2006 oraz Oceny ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

[23] Skutek – faktyczne konsekwencje jakiegoś działania. Na podstawie PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009, s. 27.

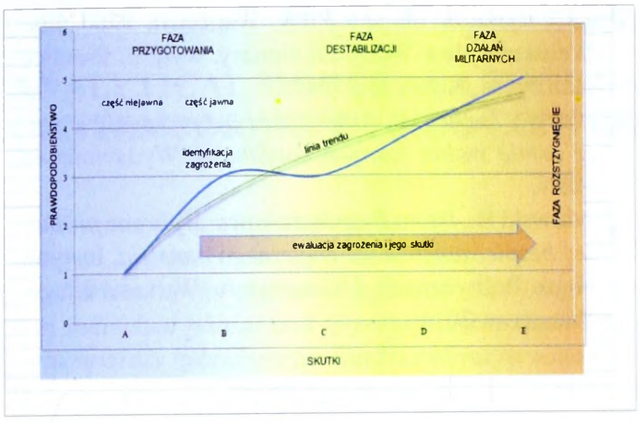
W dalszej kolejności, bazując na ocenach podatności na ryzyko dla wszystkich zidentyfikowanych zagrożeń, uzyskane dane umieszcza się w arkuszu klasyfikacyjnym, gdzie następuje ich grupowanie i wartościowanie w obszarach PEMSII wraz z opisem ich skutków. Zgodnie z przyjętą skalą (tab. 3) hierarchizuje się ryzyko od najbardziej do najmniej istotnego. W tym przypadku wyróżnić można dwa różne podejścia. Pierwsze z nich traktuje czynniki ryzyka, które posiadają najwyższe prawdopodobieństwo wystąpienia jako najistotniejsze, a drugie postrzega wpływ na obszary otoczenia jako najważniejszy.

Takie podejście umożliwia powiązanie ze sobą zagrożeń i dodatkowo ułatwia identyfikację szans[24] oraz określenie trendu. W konsekwencji może pomóc to w ich przeciwdziałaniu oraz wykryciu wcześniejszych symptomów, które w normalnej działalności mogłyby być niezauważone.

Zaprezentowany model pozwala na wyodrębnienie z istniejącej grupy wyzwań w środowisku bezpieczeństwa konkretnych szans i zagrożeń dla danego obszaru. Odzwierciedla on jednocześnie przebieg i rozwój zagrożenia z uwzględnieniem faz działań hybrydowych.

Poniższy rysunek (rys. 3) przedstawia poglądowy wynik wybranego zagrożenia, umiejscowionego w układzie współrzędnych, gdzie osi odciętych nadano wartości skutków, a na osi rzędnej zobrazowano prawdopodobieństwo wystąpienia danego typu zagrożenia. Na podstawie uzyskanych wyników wyraźnie widać działania podjęte przez agresora – określone przy pomocy krzywej oznaczonej kolorem niebieskim. Pełna identyfikacja zagrożenia następuje w chwili osiągania przez to zagrożenie punktu przełamania. Dodatkowo pozwala to obserwować ewaluację zagrożenia w poszczególnych fazach działań, przy braku podjęcia efektywnego przeciwdziałania. Ponadto umożliwia to wyznaczenie linii trendu. Na podkreślenie zasługuje fakt, że tak przeprowadzona analiza zagrożeń daje możliwość wypracowania strategii przeciwdziałania.

[24] Szanse – wszelkie okoliczności sprzyjające osiągnięciu interesu podmiotu. Patrz szerzej: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.



Opracowanie własne.

Rys. 3. Przykładowy wynik na podstawie analitycznego modelu zagrożeń hybrydowych, w jednym z obszarów PEMSII

W opracowaniach Anny Antczak-Barzan można dostrzec podobny sposób metodologii przy określaniu szans i zagrożeń w kontekście badania środowiska bezpieczeństwa Polski. Zauważa ona, że subiektywny dobór zmiennych nie pozwala na pełne zobrazowanie tego, co kryje się za poszczególnymi szansami czy zagrożeniami.

Podkreśla ona, że w pierwszej kolejności istnieje konieczność szerszego spojrzenia na dane zagrożenie, aniżeli wyciągania bezpośrednich wniosków. Według autorki *ostateczny wynik uzależniony jest od liczby szans i zagrożeń jakie można zidentyfikować w obszarze z każdego wyzwań, a tych może być bardzo wiele.* Dodatkowo wskazuje ona, że wyzwania same w sobie sygnalizują więcej zagrożeń niż szans, a część z nich jest realna, gdyż *albo już [one] występują, albo jeśli obecny kurs zostanie utrzymany, istnieje niemal pewność, że wystąpią [one] w najbliższej przyszłości, a wiele szans jedynie potencjalnych – zaistnieją w sytuacji, gdy spełnione zostaną liczne warunki*[25].

Celowość przyjętych rozwiązań w polskim modelu analitycznym oraz opracowanych faz działań hybrydowych potwierdziły opinie ekspertów krajowych i zagranicznych w ramach prowadzonych prac grupy roboczej w Multinational Capability Development Campaign (MCDC).

[25] Na podstawie: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 228.

Podsumowanie

Hybrydowość współczesnych konfliktów należy postrzegać jako konglomerat wszystkich działań podjętych przez potencjalnego agresora lub agresorów w obszarach PEMSII. Przeciwdziałanie tym zjawiskom nie jest wg. utartych schematów domeną samych sił zbrojnych czy układu pozamilitarnego, których faktyczne użycie następuje w trzeciej fazie działań hybrydowych. Opracowane definicje i fazy działań hybrydowych pozwoliły na usystematyzowanie zachodzących zjawisk. Dodatkowo narzędzie, jakim jest analityczny model działań hybrydowych, pozwala na identyfikację zagrożeń oraz umożliwia wyznaczenie ryzyka i ich ewentualnej eskalacji. Działanie takie pozwoli na opracowanie strategii przeciwdziałania zagrożeniom. Wymaga to jednak wysiłku międzyresortowego w celu osiągnięcia synergii, uaktualniania katalogów zagrożeń z uwzględnieniem aktualnej sytuacji międzynarodowej, stanu zewnętrznego i wewnętrznego państwa oraz trendów ich rozwoju w strategii długoterminowej. Brak umiejętności identyfikacji potencjalnych zagrożeń w ujęciu długofalowym może prowadzić w konsekwencji do nieodwracalnych skutków.

Bibliografia

Antczak-Barzan A., *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014.

Berzins J., Rassia's New Generation Warfare in Ukraine: Implikations for Latvian. Defense Policy. National Defence Academy of Latvia. Policy Paper nr 2. Riga 2014.

Валерий Герасимов. Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

Gruszczak A., *Hybrydowość Współczesnych Wojen – analiza krytyczna*. www. bbn.gov.

Hoffman F.G., *Hybrid Warfare and Challenges*, Joint Force Quarterly, JFQ Wyd. 51 2009.

Koziej S. i Brzozowski A., *Nauki o bezpieczeństwie: potrzeby i oczekiwania praktyki bezpieczeństwa narodowego. Tożsamość nauk o bezpieczeństwie*, Instytut Nauk Politycznych Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Wydawnictwo Adam Marszałek.

Materiały z prac grupy roboczej w ramach Wielonarodowej kampanii Rozwoju Zdolności (*Multinational Capability Development Campaign* – MCDC).

Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009.

Racz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA Report, Helsinki 2015.

Rymanowski M., *Modelowanie matematyczne i badanie złożonych układów analitycznych*, Kraków 2007.

Słownik wyrazów obcych PWN, Warszawa 1980. Por. Webster's New World Dictionary. wyd. 2. Prentice Hall Press. Nowy Jork 1986.

Sokala W., Zapała B., *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Wydawnictwo BBN.

Zdrodowski B., *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014.

Załącznik 1

TERMINOLOGIA Z OBSZARU DZIAŁAŃ HYBRYDOWYCH

Załącznik ten przedstawia wybrane definicje wg terminologii opracowanej przez grupę ekspercką w ramach rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym.*

Strategia działań hybrydowych

zapewnia osiągnięcie celów z wykorzystaniem dostępnego potencjału przy uwzględnieniu zmian i trendów w otoczeniu. W zależności od fazy planu jej wdrażania, realizowana jest w sposób skryty lub jawny przy wykorzystaniu instrumentów niemilitarnych i militarnych.

Działania hybrydowe

działania mające na celu osiągnięcie celów politycznych i strategicznych z możliwością utrzymania dotychczasowych stosunków gospodarczych i/lub dyplomatycznych. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora. Mogą być one prowadzone w środowisku politycznym, ekonomicznym, militarnym i społecznym, w tym mniejszości narodowych, etnicznych i religijnych.

Model działań hybrydowych

przyjęty sposób działania ograniczony zdolnościami i wolą potencjalnego agresora, występujący we wszystkich lub wybranych obszarach: politycznym, ekonomicznym, militarnym, społecznym, informacyjnym i infrastruktury.

Załącznik 2

FAZY DZIAŁAŃ HYBRYDOWYCH

Załącznik ten przedstawia fazy działań hybrydowych zdefiniowane przez grupę ekspercką w ramach rozwoju *Koncepcji udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym.*

FAZA I – Przygotowanie

1a część skryta

Działania w tej fazie mają charakter niejawny, poprzez wspieranie oraz wykorzystanie różnego typu grup nacisku i wpływu. Ich znaczenie jest kluczowe dla przygotowania i prowadzenia dalszych działań

1b część jawna

Ma miejsce w przypadku ujawnienia symptomów działań hybrydowych. Prowadzący je tworzy atmosferę sprzyjającą kontynuowaniu osiągania celów, zarówno w wymiarze wewnętrznym, jak i międzynarodowym.

FAZA II Destabilizacja

Zakłócenie funkcjonowania ośrodków władzy, struktur bezpieczeństwa, z wykorzystaniem środowiska informacyjnego we wszystkich lub wybranych obszarach, między innymi politycznym, ekonomicznym i społecznym. Faza ta może być celem samym w sobie lub obejmować osiąganie innych celów pośrednich.

FAZA III Działania militarne

Wykorzystywanie i wspieranie grup paramilitarnych i/lub regularnych sił zbrojnych. Aktywności tej towarzysza działania niemilitarne, w tym także dyplomatyczne oraz informacyjne.

FAZA IV Rozstrzygniecie

Akceptacja powstałej sytuacji politycznej.

ANALYTICAL MODEL AS A TOOL USED IN DESCRIBING CONTEMPORARY HYBRID CONFLICTS

Abstract

The aim of the article is to give a vivid insight into the essence of hybrid activity, to define the course of it in individual phases and to present the proposed tool, namely the analytical model. The article analyses the contemporary hybrid warfare and the terms formulated based on the works devoted to create the national Concept of Armed Forces Contribution in Countering Hybrid Warfare implemented by the Doctrine and Training Centre of PAF, in close cooperation with the group of subject matter experts. The article specifies the proposed analytical model concerning the course of possible threats in all PEMSII model fields, namely political, economic, social, military, information and infrastructure.

Key words: security, hybridity, hybrid activity/warfare, strategy, threats, hybrid warfare analytical model

Introduction

Methods used during the wars of the 21st century cause doubts among experts, especially when it comes to future means and ways that provide the internal and external security of a country and the stability of a region.

The complex manner of contemporary conflicts can be understood as broadly defined hybridity and it represents a real challenge, not only for understanding its role, but also for looking for new solutions in order to counter it. These solutions should provide for current environmental security, including its asymmetry, cultural splits and the side effects of globalisation, for they have become one of the main current challenges concerning the provision of contemporary world security.

The aim of the article is to explain the essence of hybrid warfare, to define it and to present the proposed tool used to define the course of activity in certain phases.

The first part of the article covers the hybridity of contemporary conflicts and it explains the terms highlighted based on the works devoted to create the national concept implemented by the Doctrine and Training Centre of PAF.

Based on the agreed terminology and the phase description, the second part of the article presents the recommended analytical model that describes the course of possible threats in all PEMSII areas, which are political, economic, social, military, infrastructure and informational.

Hybrid warfare – the essence and terminology

Contemporary armed conflicts of a regional and broader scope are characterised by the complexity of use of all the possible means. The preliminary analyses show the dependencies concerning plan implementation phases and the political and strategic aims represented by the aggressor. Their complex manner is very often understood as broadly defined hybridisation and reflects the challenge, not only of becoming familiar with the ideas themselves, but also to come up with new solutions in order to counter them.

In the last few years, there has been a growing tendency to join and combine regular and irregular war techniques. Additionally, economic subservience by the potential aggressor has become a very common phenomenon in the political sphere. What is more, the use of informational means and diplomatic measures as part of a very broad spectrum of influence on societies, national ethnic and religious groups has become more visible than before. The recent past has shown that these solutions should include, among others, the current environmental security (with its asymmetry, cultural splits and the side effects of globalisation). This is connected to the fact they have become one of the main challenges for providing contemporary world security. The diversity of environmental security and, above all, the scale of means used is the background for heated debate nowadays which can be seen in the numerous analyses and research papers.

It can be assumed that the complexity of all the above mentioned activities and the difficulty in identifying them are the effect of globalisation, which can have a disruptive influence on national economic sectors keeping the aggressor's activity hidden by, for instance, creating fictional non-governmental organisations, companies and corporations at the same time.

What is more, the universal access to information and the activity focused on manipulating it significantly influence the populations, national and ethnic and religious minorities creating a certain atmosphere within them. This phenomenon has started to be called hybrid warfare or hybrid warfare.

The word 'hybridity' derives from Latin, meaning hybrid – which stands for the offspring of two creatures of different 'half-blood species'.

One of the first people to bring the term 'hybrid warfare' into general use was Frank G. Hoffman. According to him, hybrid warfare is defined by the "convergence of the physical and psychological, the kinetic and non-kinetic, and combatants and noncombatants, convergence of military force and the interagency community, of states and non-state actors, and of the capabilities they are armed with.

The term 'hybrid warfare' narrows down the idea of hybridity and is often equated with armed forces, which, in fact, are only a marginal part of the whole spectrum of the potential aggressor's activity. Moreover, it has to be stated that the term *hybrid warfare*, which is broadly used in documents in English, is very often interpreted incorrectly as a hybrid war. Hybridity generates complexity and multidimensionality of activity, so one should take into account numerous, often critical remarks concerning the term *hybrid warfare*, including legal aspects directly connected with it, which are: the lack of declaring war or state of emergency/war.

The awareness of the manner of such activity and introduction of changes in perceiving of contemporary conflicts impose the adapting of the actual and providing new documents regulating/ standardising the functioning all states responsible for their security. Such solutions are there to prepare the state's structure for new challenges, including identification of threats and risk calculation. The need arose to find new solutions concerning providing and maintaining state security and adjusting the strategy for carrying out activities with the use of the military and non-military sector, above all with the measures focused on identifying the symptoms of threats and countering their progression.

Taking into account the broad spectrum, the scale of activity and the fact that they are intentionally constricted and kept on the level below the possible threshold of regular war by the aggressor, the term 'hybrid warfare instead of 'hybrid war' is recommended for use in latter documents.

Hybrid warfare activity has an impact on practically all or selected PEMSII areas with an uneven intensity and in a different period of time, often balancing upon the boundaries of existing law, especially at the initial phase. Their mutual relations, interpenetration into other areas and causing escalation of threats on the basis of cause and effect dependency comply with the definitions of the above mentioned activity. In order to precisiely define the possibility of the occurrence of hybrid warfare, one needs to highlight and categorize PEMSII areas with regard to potential threats, bearing in mind their importance, future trends and actual symptoms.

It should be mentioned that hybrid warfare needs to fulfill certain requirements when it comes to the successful implementation of deemed long-term goals. This means that in every, or in a few selected areas, certain threats should reach so called "breaking points" in order to successfully fulfill the plan/ schedule and to hinder or indispose countering them. Most of these actions take place in the first phase, as covert activity making use of a certain environment and taking into account their own potential and changes in the environmental security. It can be stated that, so far, the social and economic areas are the biggest and the most serious threats. Activities on the territory of Ukraine and Islamic Countries may provide examples.

The unification of the glossary concerning hybrid warfare allowed hybrid warfare phases and the hybrid warfare model to be provided for.

The phases of hybrid warfare

Many countries recognise the changes in the context of new challenges and threats, especially in the use of methods and where they occur. This is evident, for example, in the elaboration of

W. Gerasimov[1], who presented his model[2] in a form of a diagram that consists of six stages of the future conflict. The diagram shows a combination of military and non-military activities. He distinguishes the following phases:

- secret actions,
- situation exacerbation,
- the beginning of activities indicating conflict,
- crisis,
- solving,
- peace restoration.

The Finnish[3] elaboration includes six phases of actions:

- strategic preparation,
- political preparation,
- operational preparation,
- tension escalation,
- government overthrow central in the target region,
- alternative power establishment.

In comparison, the Latvian[4] National Defence Academy elaboration lists eight phases called: a new generation war, which include the following:

- nonmilitary actions having a negative impact on society, economic and political areas,
- actions aimed at misleading diplomatic, political and media centres,
- actions aimed at frightening the population and indicating the pointlessness of further resistance,
- destabilisation and propaganda,
- introduction of no-fly zone,
- the beginning of military operations by intensifying reconnaissance and the use of special forces,
- multidimensional, informational, diplomatic and military actions in order to exert pressure with the use of paramilitary and regular forces,
- destruction of enemy forces by special forces, precision strike and ground operations.

The lack of standardised studies in this field in the NATO and EU countries resulted in the necessity of working nationally[5].

The project team analysed conflicts with hybrid elements, such as in Somalia, in Lebanon, in the east of Ukraine and action carried out by the Islamic State for the better understanding of these issues. All existing cases have been unified and function as universal hybrid warfare phases of action.

A detailed description of the phases is presented in appendix no. 2:

- preparation,
- destabilisation,
- military activity,
- resolution.

Table 1

The diagram of the phases of hybrid warfare

PHASE I PREPARATION		PHASE II DESTABILISATION	PHASE III MILITARY ACTIVITY	PHASE IV RESOLUTION
covert part	overt part			

Source: own elaboration.

Activities at the preparation stage can be divided into two parts: covert and overt. The activities in the covert part are implicit. They may be characterised by the use of all sorts of ways to pressure and influence, led by corporations, NGOs or religious groups.

This phase is represented by the fact that the potential state, which is under attack, is not unaware of the fact that coordinated actions are carried out within it. Their importance is crucial when further actions are carried out by the aggressor.

When it comes to preparing these actions, they turn into an overt part when the target state notices the actions being taken against it.

[1] Валерий Герасимов – Chief of Staff Russian Federation

[2] Валерий Герасимов, Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

[3] Andras Racz, Russia's Hybrid War in Ukraine. Fiński Instytut Stosunków Międzynarodowych Raport 43 z 2015, s. 59–63.

[4] Janis Berzins, Russia's New Generation Warfare in Ukraine. Implications for Latvian Defence Policy National Defence Academy of Latvia. Policy Paper nr 2 z 2014, s. 6. for Techikinov i Bogdanov 2013, s. 15–22.

[5] The task of developing *The concept of contribution of Polish Armed Forces in countering hybrid threats*, commissioned by the Chief of General Staff of PAF.

In this part, one can see the phase of creating an atmosphere of financial meltdown inevitability, helplessness of government, weakness of security ministries and the possibility of armed conflict occurrence while maintaining current policy, both in the diplomatic and economic arena. The awakening of psychological and ideological separatism and ideological or religious aspirations take place.

The effective implementation of the development phase ensures the transition to the next - destabilisation phase. This is characterised by the disruption of the central and local centres of power, security structures, media and business, representatives, with the use of exploited methods and tools (political, economic, social, etc.) or cyber attack.

In this phase, one can specify the high scale of information activities - optional disinformation (at all levels: from strategic communications to local broadcasts) using all available means of communication in the area of possible conflict and in its international environment in order to achieve the desired reaction. If the main objective of the aggressor is only to destabilise certain areas (PEMSII) of the country, it means that these actions can be completed. If the aggressor's targets are not fully achieved, they can move onto the next phase - military activities.

At this stage, one can point out the formation of a local affiliates separatists group, made up of ethnic minorities or religious groups with the support of spiritual religious leaders, terrorist organisations, armed forces and special services of the aggressor.

Their main task is to stoke tension to confirm the helplessness of authorities and block possibilities of action by the ministries of power, e.g. the police and the army, and to take control of key facilities and areas which are necessary for affecting the success of the operation in a coordinated way. Objects of special significance include, border crossings, media relay stations, the key infrastructure such as crossroads, bridges and railway junctions and the airports. It should be emphasised that, at this stage, military activities are supported by coordinated and detailed planned diplomatic actions and expressed by information activities.

The last defined phase is resolution. It is characterised by the establishment of central and local authorities dependent on the aggressor. Resolution means mainly the acceptance of a forced political situation. If goals are not achieved, the phase of military activities may turn into open regular armed conflict. However, in this case, there are no hybrid activities/warfare any more.

Analytical model of hybrid warfare

Threats in the contemporary world are characterised by their diversity and the complexity of their occurrence. It is worth emphasising that national security[6] is not only the state but, above all, a dynamic process that is affected by a variety of determinants[7]. This results in difficulties in making a proper threat assessment. The complexity of its occurrence in certain areas radically affects the opportunity to find the appropriate methodology needed to determine the actual impact and what individual threats[8] mean.

The use of the method of modelling[9] is legit in this case. By creating models and confronting them with reality, among other things, through observations, one can check the occurring laws defining the phenomenon. Understanding this process is the inherent factor in predicting the course of events in the future[10]. This also applies to issues of national security. Anna Antczak-Barzan[11] states that "lack of ability to identify potential hazards in the long term based on developing internal and external trends (a close and further outlying state) can lead to disaster. Acting by focusing on only

[6] Security of the state – the actual state of internal stability and sovereignty of the state, which reflects the lack or presence of any threats (in the sense of existential basic needs and behavioural treatment of the public and the state as a sovereign subject in international relations). *Słownik terminów z zakresu bezpieczeństwa narodowego*, Wydanie szóste, AON, Warszawa 2002, s. 19.

[7] See the wider view: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 226.

[8] Threats - any disruptive effects on the subject, revealed in the form a crisis situation. See more widely: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

[9] Modelowanie matematyczne i badanie złożonych układów analitycznych. Maciej Rymanowski, Kraków 2007, s. 11.

[10] Ibidem.

[11] Professor of social science in the science of politics (Polish Academy of Sciences).

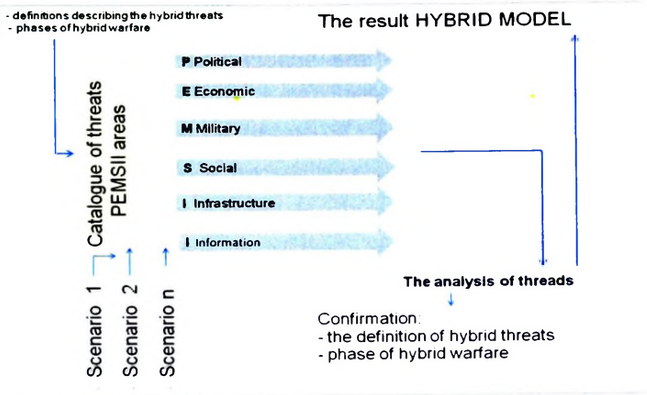
selected issues and taking care of particular private interests and the fight between different political factions have led more once to disaster"[12].

The findings above and the conclusions are the basis for discovering that the identified threats should be subjected to systematic analysis and monitoring. Currently, the analytical model of hybrid threats is designed to help to understand the symptoms and mechanisms of threats and allow to identify new ones that may significantly affect the functioning and the possibility of development of the state. In particular, they may be important for both internal and external safety. Such approach should also contribute to creating tools that would help counter potential threats.

While preparing an analytical model of hybrid warfare, certain assumptions have been adopted. Firstly, the work is carried out based on the PRINCE2[13] project management methodology. The aim of it was to use the principles of effective management that are required during the project, including the provision of a structured approach to ensure its success. However, even though this methodology provides knowledge about the techniques used, it does not specify in detail how to use them. Next is the input data. This includes: catalogue of threats in PEMSII areas, and the input data needed for definitions of hybrid threats and phases of hybrid warfare. In order to develop the analytical model, it has been assumed that environmental security will be divided into: political, economic, military, social, infrastructure and information areas. During the work, the project team defined characteristics separately as threads for each of these domains.

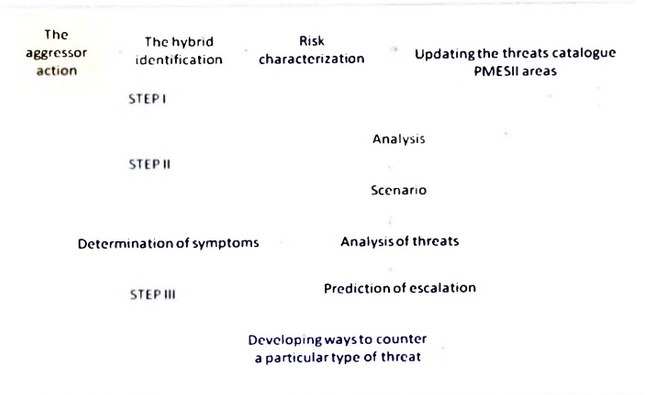
The idea of the model is illustrated in Figure 1.

During the development of the hybrid model, the following methodology of data processing was adopted (Fig. 2).



Source: own elaboration.

Figure 1. Schematic diagram of the analytical model of hybrid threats



Source: own elaboration.

Figure No. 2. Methodology of hybrid threats

At the first stage of the process, based on the risks arising from the actions of the aggressor, characterisation of threads takes place and they are put into catalogues. The second step requires selecting the most critical threat, to carry out the analysis and to develop case scenarios. These scenarios include all activities aimed at understanding the factors causing these risks and the creation of their symptoms and the relationship between them. During this stage, the threats are due to their:

– intentions: the interests, needs, politics, will,

– possibilities: the ability, methods, resources, constraints,

– historical data: assigned incidents, attempts, confirmed operations, frequency and effectiveness of these activities,

– signals: newly confirmed or anecdotal evidence.

This approach makes it possible to estimate the risk of threats. By risk estimation, it will be

[12] Translation from: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014, s. 238.

[13] PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009. Metodyka zarządzania projektami. Stosowana do sterowania i zarządzania projektami.

crucial to identify: the risks from a catalogue, the probability of the susceptibility of PEMSII areas and their impact and implications on the security of the state. It should be emphasised that the estimation values of the two basic parameters of the components - probability and effects – is significant in determining susceptibility to risk. The level of risk is estimated based on the use of a discreet grading scale of probability, which is included below (Tab. 2).

Table 2

Discreet probability grading scale

UNLIKELY	Threats previously unidentified and undocumented, which could occur only in exceptional and favourable circumstances. The value 0–20%
RARE	Threats are documented, risk symptoms or other circumstances are little known. The value of 20–40%
POSSIBLE	Threats are documented, symptoms or mechanism of formation is known. It can happen at a certain time in favourable conditions. The value of 40–60%
PROBABLE	Threats known and previously encountered. It is likely that in the case of a favourable environment they may occur in most circumstances. The value of 60–80%
VERY LIKELY	Threats are well known and systematic. There is a suitable environment for their creation. It is expected that these threats will happen in most circumstances. The value 80–100%

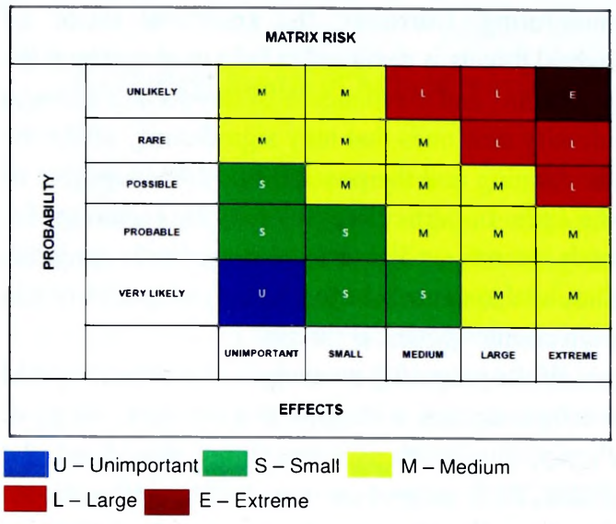
Source: Own study based on: *Ocena ryzyka na potrzeby zarządzania kryzysowego.* Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

The estimated value of the risk matrix reflects the relationship between probability and effects[14]. Each corresponds to the identified risk of one specific field (see Tab. 3).

In the more distant past, based on the vulnerability assessments of the risk for all identified threats, the resulting data is placed in a sheet classification, where they are grouped and evaluated in the area of PEMSII together with a description of their effects. According to the scale (Tab. 3), the risk is being prioritised from most to least important. In this case, one can distinguish two different approaches. The first one considers risks that have the highest probability of occurrence as the most important, and the other perceives the impact on the environment as the most important area.

Table 3

Risk matrix



Source: Own elaboration based on: Field Manual No. 5–19 (100–14), Composite Risk Management, Department of the Army. Washington, DC, July 2006 oraz Oceny ryzyka na potrzeby zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

This approach allows the threats to be linked together and also helps to identify the opportunities[15] and threats and to determine the trend. As a consequence, it may help in preventing and detecting the early symptoms, which in ordinary activities could remain unnoticed.

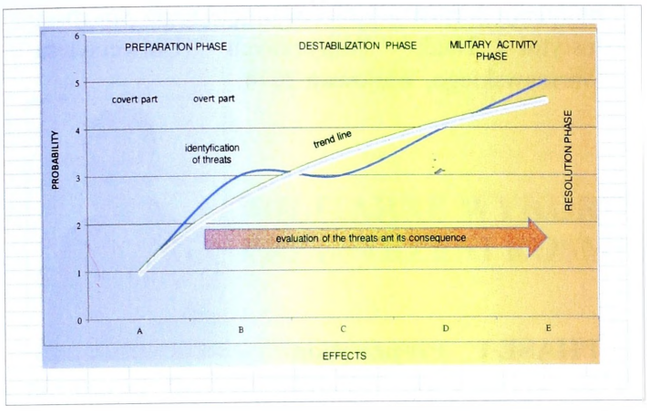
The presented model enables the identification of existing group challenges in environmental security, and specific opportunities and risks for the area. It reflects both the course and evolution of the risk, including the phases of hybrid warfare.

The following figure (Fig. 3) depicts an illustrative result of the threats positioned in the coordinate system where the x-axis shows the threat and the other shows the probability of the type of threat. The results clearly show the actions taken by the aggressor - determined using the blue curve. The full identification of the threats occurs by the time the breaking point is achieved by this threat. In addition, it allows the evaluation of threats in particular phases of the actions to be observed and the failure to adopt effective countermeasures. In

[14] Effect - the actual consequences of an action. Based on: PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009, s. 27.

[15] Opportunities - any circumstances for achieving the interest entity. Based on: B. Zdrodowski, *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 46.

addition, it allows the trend line to be determined. It is worth emphasising that such analysis makes it possible to develop strategies to combat threats.



Source: own elaboration.

Figure 3. Example output based on an analytical model of hybrid threats, one of the areas PEMSII

There is a slight resemblance in the studies of Anna Antczak-Barzan when it comes to methodology, by determining the opportunities and threats in the context of the examination of the Polish security environment.

She notices that a subjective selection of variables does not fully illustrate what lies behind the various opportunities and threats. She emphasises that, firstly, there is a need to pay more attention to threats rather than to focus on direct conclusions. According to the author, the final result depends on the number of opportunities and threats that could be identified in the area of each of the challenges and these can be various.

In addition, she indicates that the challenges themselves mean bigger risks rather than opportunities, and some of them are realistic because they have either already occurred, or, if the current rate remains maintained, it is almost certain that they will occur in the near future, and many potential chances arise when a number of conditions are met[16].

The desirability of the solutions adopted in the Polish analytical model of hybrid warfare and phases were confirmed by national and international experts in the working group in the framework of the Multinational Capability Development Campaign (MCDC).

[16] Based on: A. Antczak-Barzan, *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014, s. 228.

Conclusion

The contemporary conflicts' hybridity should be seen as a conglomerate of all possible activities conducted by the aggressor or aggressors in PEMSII areas. Methods for countering these activities is not only the domain of the armed forces or non-military system, whose actual use takes place in the third phase of hybrid warfare. The definitions and hybrid warfare phases made it possible to put the events in chronological order. In addition, the analytical hybrid warfare model enables threats to be identified and points out the risk and potential escalation. Such activity makes it possible to figure out the threats countering strategy. However, it demands the engagement of all departments in order to achieve synergy, up-dating the threats catalogues bearing in mind the current multinational situation, the internal and external state of the country and their development trends in long-term strategy. The lack of capability to identify potential threats in the long term may consequently lead to non-reversible consequences.

Bibliography

Antczak-Barzan A., *Rangi wyzwań dla bezpieczeństwa Polski w XXI wieku. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, INPUW, Warszawa 2014.

Berzins J., Rassia's New Generation Warfare in Ukraine: Implikations for Latvian. Defense Policy. National Defence Academy of Latvia. Policy Paper nr 2. Riga 2014.

Валерий Герасимов. Новые вызовы требуют переосмысления форм и способов ведения боевых действий, Военно-Промышленный Курьер, номер 8 (476), 27.02–05.03.2013 года.

Gruszczak A., *Hybrydowość Współczesnych Wojen – analiza krytyczna*. www. bbn.gov.

Hoffman F.G., *Hybrid Warfare and Challenges*, Joint Force Quarterly, JFQ Wyd. 51 2009.

Koziej S. i Brzozowski A., *Nauki o bezpieczeństwie: potrzeby i oczekiwania praktyki bezpieczeństwa narodowego. Tożsamość nauk o bezpieczeństwie*, Instytut Nauk Politycznych Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Wydawnictwo Adam Marszałek.

Materiały z prac grupy roboczej w ramach Wielonarodowej kampanii Rozwoju Zdolności (*Multinational Capability Development Campaign* – MCDC).

Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

PRINCE2 – Skuteczne zarządzanie projektami. Piąta edycja Crown Copyright. UK 2009.

Racz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs, FIIA Report, Helsinki 2015.

Rymanowski M., *Modelowanie matematyczne i badanie złożonych układów analitycznych*, Kraków 2007.

Słownik wyrazów obcych PWN, Warszawa 1980. Por. Webster's New World Dictionary. wyd. 2. Prentice Hall Press. Nowy Jork 1986.

Sokala W., Zapała B., *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, Wydawnictwo BBN.

Zdrodowski B., *Istota Bezpieczeństwa. Wybrane problemy bezpieczeństwa wewnętrznego państwa*, Instytut Nauk Politycznych Uniwersytetu Warszawskiego, Warszawa 2014.

Appendix 1

TERMINOLOGY FROM THE ACTIVITIES OF HYBRID

This annex presents some definitions by. terminology developed by an expert group within the development *Concept of contribution of the Polish Armed Forces in countering the hybrid warfare.*

Hybrid warfare strategy

It guarantees achieving goals with the use of available capability and potential taking into account changes and trends in the environment. Depending on the plan phase of its implementation, it is conducted overtly or covertly using military and non-military instruments.

Hybrid activity/warfare

Actions that aim at achieving political and strategic goals with the possibility of maintaining previous economic and/or diplomatic relations. Hybrid warfare is conducted by state and/or non-state entities in a planned and coordinated way and it combines different ways of making pressure and making dependent on potential aggressor. All the actions can be conducted in a political, economic, military and social environment, including national, ethnic and religious minorities.

Hybrid warfare conduction

Generally accepted modus operandi that is restricted by potential aggressor's will and capabilities. It takes place in all or selected areas which are: political, economic, military, social, informational and infrastructural.

Appendix 2

PHASE I Preparation

1a covert part

Actions of this phase are covert due to its support and use of different types of pressure and influence groups. Their meaning is crucial for the preparation and conduction of further actions.

1b overt part

It takes place when hybrid warfare symptoms are exposed. The leading entity creates an atmosphere which is advantageous for goals achievement, not only in national, but also in international dimension.

PHASE II Destabilisation

Disorganization of centers of power and national/nations' security structures with the use of information tools available in all or selected areas, including political, economic and social spheres. This phase can be a target itself or include achieving other indirect goals.

PHASE III Military activity

The use and support of paramilitary and/or regular armed forces. The activity is often represented by non-military actions, including diplomatic and informational support.

PHASE IV Resolution

The acceptance of a resulting political situation

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

SZTUKA WOJENNA

MILITARNE WYKORZYSTANIE PRZESTRZENI KOSMICZNEJ

mjr mgr inż. Radosław BIELAWSKI
Akademia Obrony Narodowej

mjr mgr inż. Rafał ZAJKOWSKI
Akademia Obrony Narodowej

Streszczenie

Artykuł przedstawia próbę zidentyfikowania i zaprezentowania wybranych problemów wykorzystania przestrzeni kosmicznej. W publikacji dokonano analizy aktów prawnych począwszy od 1957 roku – daty rozpoczęcia się ery eksploracji kosmosu. Przedstawiono koncepcje określenia granicy między przestrzenią powietrzną a przestrzenią kosmiczną. Przedstawione zostały etapy tworzenia międzynarodowego prawa kosmicznego oraz nakreślono znaczące akty prawne mające wpływ na dalsze jego doskonalenie. Na podstawie projektu założeń do projektu ustawy – Prawo kosmiczne opisano genezę, zakres i zasady, w myśl których ustawa powstaje. W dalszej części omówione zostały militarne aspekty i zagrożenia wykorzystania przestrzeni kosmicznej w obliczu tworzonego prawa. Dokonano przedstawienia wybranych problemów i możliwych konsekwencji polityczno-militarnych, wynikających z użytkowania przestrzeni kosmicznej. Opisano i zanalizowano zagrożenia, które poparte odpowiednimi przykładami, zostały opisane w tej publikacji.

Słowa kluczowe: przestrzeń powietrzna, przestrzeń kosmiczna, suwerenność, bezpieczeństwo narodowe.

Wprowadzenie

Rozwój techniki na przełomie wielu lat spowodował, że człowiek buduje obiekty latające, które mają zdolność nie tylko do poruszania się w atmosferze okołoziemskiej, lecz również w przestrzeni kosmicznej. Niefortunny lot statku kosmicznego Apollo 13[1], który wystartował 11 kwietnia 1970 roku z celem lądowania na powierzchni Księżyca, wzniósł się na odległość ponad 400 tys. km od powierzchni Ziemi, przewyższając tym samym średnią maksymalną wysokość lotu konwencjonalnego współczesnego samolotu pasażerskiego kilkadziesiąt razy. Lot każdego statku powietrznego w przestrzeni powietrznej państwa jest monitorowany zarówno przez cywilne, jak i wojskowe organy ruchu lotniczego. Niestety ruch obiektów w przestrzeni kosmicznej, odbywających misję nad terytorium państwa, nie jest śledzony. Obiekty nie podlegają także zasadom ruchu lotniczego. Niezależnie od intencji i przeznaczenia takiego obiektu, sytuacja ta rodzi wątpliwości dotyczące ograniczenia suwerenności państwa, nad którym odbywa się lot, co stanowi poważny problem współczesnego bezpieczeństwa.

Dynamiczny rozwój technologii kosmicznych spowodował, że obecnie przestrzeń kosmiczna jest miejscem odbywania lotów przez obiekty nie tylko mające na celu zbadanie przestrzeni kosmicznej w celach naukowych, lecz coraz częściej staje się ona obszarem komercji. Polska przez ostatnie 30 lat zbudowała własny sektor kosmiczny, który

[1] Cel misji statku kosmicznego Apollo 13 o indeksie COSPAR 1970-29A, którym było lądowanie na Księżycu nie został osiągnięty. W trakcie misji doszło do eksplozji zbiornika z tlenem, co spowodowało, że załoga musiała walczyć o życie. Po dwóch dniach lotu, na trasie na Księżyc nastąpiła eksplozja butli z tlenem, która miała miejsce w module serwisowym. Eksplozja spowodowała, że moduł ten został pozbawiony energii, aby zapewnić dotarcie statkowi na Księżyc i wrócić na Ziemię. 17 kwietnia załoga szczęśliwie powróciła na Ziemię, mimo wielu problemów. Lot Apollo 13, był najodleglejszym lotem od Ziemi. Rekord ustanowiony w dniu 15 kwietnia 1970 wynosił 400 171 km i niej jest on pobity do dzisiaj, dostępny na http://nauka.money.pl/slownik-naukowy/apollo-13-724888.html [dostęp dnia: 31.11.2014].

składa się z 50 jednostek badawczo-rozwojowych będących w gestii przedsiębiorstw. Ich domeną są technologie informacyjne, telekomunikacja czy elektronika. Konieczne więc wydaje się stworzenie prawa kosmicznego na poziomie państwa, które określałoby zasady funkcjonowania obiektów, a także prawa i obowiązki użytkowników. Okazuje się, że jest to proces obarczony wieloma problemami oraz konsekwencjami, które rozwinięte będą szerzej w dalszej części tej publikacji.

Celem artykułu jest przedstawienie wybranych problemów, towarzyszących budowaniu prawa kosmicznego w aspekcie militarnym. Zaprezentowano wybrane, współczesne zagrożenia, jakie może nieść za sobą użytkowanie przestrzeni kosmicznej, w aspekcie obowiązujących aktów prawa międzynarodowego. Głównym problemem badawczym była próba odpowiedzi na pytanie: *Jakie znaczenie militarne dla państwa ma przestrzeń kosmiczna?* Podjęcie badań i szukanie odpowiedzi na postawiony problem badawczy były zainspirowane hipotezą autorów, którzy założyli że: *z punktu widzenia polityczno-militarnego przestrzeń kosmiczna jest tak samo ważna dla zachowania suwerenności państwa jak przestrzeń powietrzna.* Chcąc rozwiązać problem badawczy, skorzystano z metod badawczych, takich jak: analiza, porównanie, uogólnianie, wnioskowanie i synteza.

Początki ery lotów kosmicznych

Najwcześniejsze zapiski odnoszące się do prawa kosmicznego pochodzą z 1932 roku. Powstała wówczas pierwsza monografia autorstwa V. Mandla – prekursora uważanego za ojca prawa kosmicznego. Sytuacja ta miała miejsce 10 lat wcześniej, zanim człowiek wystrzelił pierwszą rakietę, która dotarła do przestrzeni kosmicznej[2]. Okres ten rozpoczął nową erę kosmiczną – *Space Age*. Przed wystrzeleniem pierwszego Sputnika w 1957 roku powstało wiele publikacji, które w treści odwoływały się do problemów prawnych i działalności człowieka w przestrzeni kosmicznej.

Już starożytni Rzymianie wyznawali zasadę *cuius est solum, eius est usque ad coelum,* co oznacza, że *władca ziemi jest władcą nieba ponad nią*[3]. Maksyma ta jest często uzupełniana słowami – *usque ad sidera*, tłumaczona jako: *aż do gwiazd.* Wynika stąd, że państwo jest w tej przestrzeni suwerenne i może sprawować władzę nad każdym znajdującym się w niej obiektem. Szybko okazało się, że egzekwowanie prawa w stosunku do obiektów znajdujących się w przestrzeni kosmicznej byłoby ekstremalnie trudne. Pojawiły się wówczas dwie koncepcje respektowania prawa. Pierwsza z nich uznawała, że wysokość trajektorii lotu statku kosmicznego w przestrzeń nie podlega już suwerenności państw – *res omnium communis*[4]. Oznacza to, że jurysdykcja państw nad przestrzenią powietrzną ograniczona jest do pewnej wysokości, którą jest granica przestrzeni powietrznej z przestrzenią kosmiczną. Trudno jest jednak jednoznacznie określić tę granicę[5]. Jednym ze zwolenników tej dewizy był A. G. Haley, który wysunął tezę, że przestrzeń kosmiczna zaczyna się tam, gdzie na lecący obiekt przestaje oddziaływać siła oporu powietrza, a podlega on oddziaływaniom siły odśrodkowej[6]. Innym zwolennikiem był G. Zadrożny, pomysłodawca tzw. wolności powietrznej. Nawiązywała ona analogicznie do wolności pełnego morza[7], czyli na wysokość 20–30 km ponad powierzchnię ziemi.

Druga koncepcja uznania prawa dotyczyła nieszkodliwego przelotu statku kosmicznego przez przestrzeń powietrzną. W 1957 roku zaproponowano stworzenie międzynarodowej konwencji, która dzieliłaby przestrzeń na trzy części (rys. 1). Konwencja ta byłaby analogiczna do konwencji o podziale morza.

[2] Pierwszą rakietą, która dotarła do przestrzeni kosmicznej, była niemiecka rakieta V2 w czasie lotu testowego 3 października 1942 roku. 4 października 1957 roku Związek Radziecki wystrzelił Sputnika 1, który stał się pierwszym sztucznym satelitą na orbicie Ziemi. Pierwszym lotem załogowym była misja Wostok 1, której start odbył się 12 kwietnia 1961 roku. Na pokładzie statku kosmicznego znajdował się pierwszy w dziejach ludzkości kosmonauta Jurij Gagarin, który dokonał jednego okrążenia wokół Ziemi.

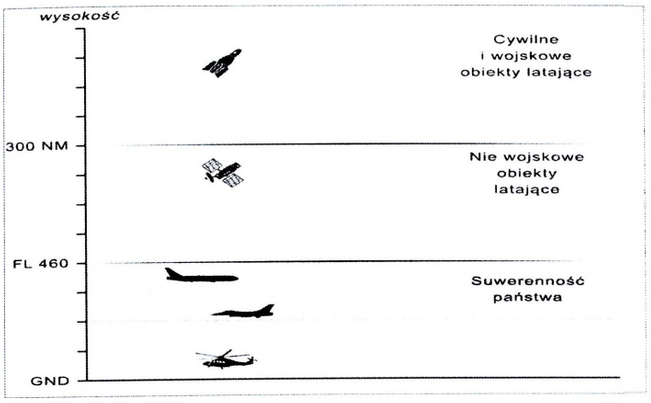
[3] *Internetowy słownik wyrazów obcych i zwrotów obcojęzycznych Władysława Kopalińskiego*, dostępny na www.slownik-online.pl/ [dostęp: 01.11.2014].

[4] Rzeczy służące do powszechnego użytku: powietrze, woda płynąca, morze i brzegi morza – K. Kolańczyk, *Prawo rzymskie*, Warszawa: LexisNexis, 2007, s. 266.

[5] M.N. Shaw, *Prawo międzynarodowe*, Książka i Wiedza, Warszawa 2012, s. 291.

[6] Obiekt musi osiągnąć odpowiednią prędkość, która umożliwi mu pokonanie siły grawitacji ziemskiej i oddalenie się w przestrzeń kosmiczną.

[7] Konwencja Narodów Zjednoczonych o prawie morza z 1982 roku. Zgodnie z nią każde państwa ma prawo do 12-milowej strefy wód terytorialnych, do szelfu kontynentalnego oraz do nie przekraczającej 200 mil wyłącznej strefy ekonomicznej – W. Jędrzejewski, *Status Morza Kaspijskiego*, dostępny na http://www.psz.pl/Wojciech-Jedrzejewski-Status-Morza-Kaspijskiego [dostęp: 03.12.2014].



Opracowanie własne.

Rys. 1. Propozycja podziału przestrzeni kosmicznej wysunięta przez Coopera w 1957 roku

Pierwsza część tej przestrzeni rozciągałaby się od ziemi do wysokości, jaką mogą osiągnąć klasyczne samoloty. Strefa ta podlegałaby jurysdykcji państwa, nad którym się ona znajduje i w której państwo jest suwerenne[8]. Drugi przedział obejmowałby przestrzeń powietrzną do wysokości 300 mil. Ta strefa miałaby być dostępna jedynie dla niewojskowych obiektów latających wszystkich państw. Trzecia strefa natomiast, rozciągająca się powyżej wysokości 300 mil, miałaby być dostępna dla obiektów zarówno cywilnych, jak i wojskowych wszystkich państw. Z uwagi na fakt, że propozycja ta ograniczała prawo przelotu[9], nie została przyjęta.

Koncepcji tworzenia prawa kosmicznego w okresie początku ery kosmicznej było jeszcze kilka. Reasumując, można wskazać dwie przodujące koncepcje, które pojawiły się w tamtych latach. Jedna z nich dotyczyła nieszkodliwego przelotu przez przestrzeń kosmiczną. Druga natomiast zakładała, że na wysokości trajektorii przelotu obiekt nie podlega już suwerenności państwa[10]. Kwestie te są problemem sięgającym czasów obecnych.

Tworzenie międzynarodowego prawa kosmicznego

Po sześciu latach od rozpoczęcia lotów w przestrzeń kosmiczną rozpoczęto znaczące działania dotyczące rozwoju prawa kosmicznego. Wynikiem tych prac była rezolucja nr 18/1962 przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych[11] w 1963 roku. Przedmiotem treści dokumentu była działalność w dziedzinie badań kosmosu wraz z Księżycem i innymi ciałami niebieskimi. Brak uzgodnienia limitu pionowego, w którym to państwo jest odpowiedzialne za przeloty, spowodowało problem z ustaleniem odpowiedzialności za działalność w tej przestrzeni[12]. Po raz kolejny pojawia się potrzeba zdefiniowania i ścisłego jej określenia. Uznano wówczas, że najwyższa granica przestrzeni atmosferycznej to taka, na której satelita, przemieszczając się po trajektorii, przechodzi do atmosfery[13].

Kolejnym aktem prawnym był traktat kosmiczny z 1967 roku podpisany równocześnie przez Rosję, Wielką Brytanię i Stany Zjednoczone. Jednym z założeń tego dokumentu jest potwierdzenie przez podpisujące państwa, że przestrzeń kosmiczna wraz z Księżycem i innymi ciałami niebieskimi nie podlega zawłaszczeniu. Inną ważną kwestią, jaką zawiera dokument, jest zastrzeżenie, że badanie i eksploracja kosmosu powinna służyć ludzkości. Wprowadzono tutaj zasadę niedyskryminacji, polegającą na możliwości badania przestrzeni kosmicznej nie tylko przez potęgi państwowe, lecz również przez inne państwa. Układ z 1967 roku nadal jednak nie określa dokładnie i nie precyzuje granicy przestrzeni kosmicznej i przestrzeni powietrznej. Ustanawia on jedynie podstawy międzynarodowego prawa kosmicznego. Układ ten jest częścią prawa międzynarodowego i respektuje jego zasady[14].

W przeciągu kilkudziesięciu lat powstało jeszcze kilka aktów prawnych regulujących działal-

[8] Państwo suwerenne rozumiane jako niezależne i samowładne, wg słownika *The American Heritage Dictionary of the English Language* (AHD), dostępny na https://ahdictionary.com [dostęp: 04.11.2014].

[9] Prawo przelotu określone w konwencji chicagowskiej i uznane jako jedna z wolności lotniczych. Jest to przywilej przelotu nad terytorium państwa bez lądowania. Państwo A przyznaje przewoźnikowi państwa B prawo przelotu nad jego terytorium – *Konwencja o międzynarodowym lotnictwie cywilnym podpisana w Chicago dnia 7 grudnia 1944 r.* (DzU z dnia 26 czerwca 1959 r.).

[10] M. Polkowska, *Suwerenność państwa w przestrzeni powietrznej, geneza, zakres i ewolucja*, LIBER, Warszawa 2009.

[11] Zgromadzenie Ogólne jest jednym z sześciu organów głównych Organizacji Narodów Zjednoczonych-ONZ, powołany na mocy Karty Narodów Zjednoczonych. Zgromadzenie podejmuje decyzje w formie uchwał, które mają charakter obowiązujący w kwestiach wewnętrznych.

[12] P. Durys, F. Jasiński, *Wybór aktów prawnych do nauki międzynarodowego prawa lotniczego i kosmicznego*, Warszawa 1999, s. 228.

[13] R.W. Fixel, *The law of aviation*, Bloomington 1999, s. 65.

[14] L. Tate, *The status of the outer space treaty at International law during „war" and „those measures short of war"*, JSL 2006, s. 181.

ność człowieka w kosmosie, takich jak np. Konwencja zakazu zbrojeń i międzynarodowej stacji kosmicznej z 1976 roku czy Konwencja o wczesnej notyfikacji wypadku nuklearnego z 1986 roku. Między państwami zawierane są również umowy bi i multilateralne, ograniczane zazwyczaj do naukowej i technologicznej współpracy w dziedzinie badania kosmosu. Dotyczą one takich kwestii jak: teledetekcja, ochrona środowiska, współpraca misji kosmicznych, meteorologia[15]. Obecnie nie ma skonstruowanego międzynarodowego prawa kosmicznego, które zawierałoby zasady żeglugi powietrznej. W dobie wielu zagrożeń, w tym także możliwości ograniczenia suwerenności państwowej w przestrzeni kosmicznej i powietrznej, problem jest bardzo aktualny. Szacuje się, że na obecnym etapie rozwoju prawa kosmicznego w świecie, liczba aktów prawnych będzie rosnąć. Należy zauważyć, że w ostatnich latach charakter działalności państw w kosmosie uległ zmianie. Wiele inicjatyw pochodzi od sektora prywatnego, co według prawników zmieni charakter tego prawa z publicznego na mieszany o naturze publiczno-prawnej[16].

Prawo kosmiczne w Polsce

Przystąpienie Polski w 2012 roku do Europejskiej Agencji Kosmicznej[17] umożliwia takim podmiotom jak jednostki badawczo-rozwojowe oraz małe, średnie i duże przedsiębiorstwa wykorzystanie wiedzy i infrastruktury agencji. Obecnie rośnie zapotrzebowanie na usługi świadczone przez sektor kosmiczny. Taki stan rzeczy zobowiązuje Polskę do stworzenia krajowego prawa kosmicznego. W zakresie tego prawa dotychczas obowiązują w Polsce akty prawa europejskiego i międzynarodowego. Nowe prawo wymaga uregulowania kilku kwestii. Jedną z nich są zasady wyrażania zgody na działalność w przestrzeni powietrznej przez podmioty krajowe. Innymi są reguły prowadzenia krajowego rejestru obiektów kosmicznych, odpowiedzialności państwa oraz kwestie odszkodowawcze. Jego zapisy wymuszają stworzenie i administrowanie rejestru obiektów kosmicznych wypuszczanych w przestrzeń kosmiczną przez polskie podmioty. Celem nowobudowanej ustawy – Prawo kosmiczne jest uregulowanie problematyki użytkowania obiektów kosmicznych, w taki sposób, aby nie była ona przeszkodą w rozwoju polskiego sektora kosmicznego[18].

Zakres projektowanego aktu prawnego obejmował będzie działalność kosmiczną w zakresie pokojowego wykorzystania przestrzeni kosmicznej w myśl kilku fundamentalnych zasad. Jedną z nich jest reguła wolności badań i użytkowania przestrzeni kosmicznej dla dobra i w interesie wszystkich krajów. Inna zakłada nieprzywłaszczanie przestrzeni kosmicznej oraz jej pokojowe wykorzystanie. Dokument określa zasady oraz wymogi wypuszczenia obiektów kosmicznych[19] w przestrzeń kosmiczną. Zgoda na nie będzie wydawana w formie decyzji administracyjnej, a wpis do Krajowego Rejestru Obiektów Kosmicznych będzie czynnością techniczną, potwierdzającą wypuszczenie obiektu kosmicznego. Założenia do projektu ustawy określają warunki uzyskania zgody na wyniesienie obiektu kosmicznego. Jednym z nich jest zgodność z interesami bezpieczeństwa narodowego i polityki zagranicznej[20]. Poza tym innymi ważnymi warunkami będą: bezpieczeństwo działalności kosmicznej, ubezpieczenie stwierdzające zawarcie umowy ubezpieczenia cywilnego za szkody związane z działalnością kosmiczną, oświadczenie o niezakłócaniu działalności innych państw w zakresie pokojowych badań i użytkowaniu przestrzeni kosmicznej.

Przedmiotem nowobudowanego prawa kosmicznego są zasady regulujące korzystanie z przestrzeni kosmicznej kierowanych tam obiektów. Mają one charakter administracyjny i dotyczą właściwie sektora prywatnego. W aktach tych nie ma zapisów o charakterze militarno-politycznym. Logiczne wydaje się, że użytkowanie przestrzeni kosmicznej związane może być także z zagroże-

[15] M. Polkowska, *Prawo kosmiczne w obliczu nowych problemów współczesności*, LIBER, Warszawa 2011.

[16] C.J. Cheng, *New sources of international space law*, Hague 1998, s. 207.

[17] Europejska Agencja Kosmiczna – *European Space Agency* (ESA) jest międzynarodową organizacją krajów europejskich. Celem działalności agencji jest eksploracja i wykorzystanie przestrzeni kosmicznej, dostępny na: http://www.esa.int [dostęp: 04.12.2014].

[18] *Projekt założeń do ustawy – Prawo kosmiczne*, Ministerstwo Gospodarki, Projekt z dnia 19 sierpnia 2014 r.

[19] Obiekt kosmiczny w myśl projektu ustawy – Prawo kosmiczne, to urządzenie które będzie wypuszczone lub zostało wypuszczone w przestrzeń kosmiczną, jego części składowe, a także jego urządzenie nośne i części tego urządzenia.

[20] Zgodnie z art. 106 Kodeksu postępowania administracyjnego ministra właściwego do spraw obrony narodowej oraz ministra właściwego do spraw zagranicznych.

niami skierowanymi przeciwko państwu. Takie niebezpieczeństwo niosą za sobą rakiety balistyczne, satelity szpiegowskie oraz inne obiekty. Ryzykiem mogą być także różnego rodzaju badania nad bronią nuklearną, detonacje oraz inne przedsięwzięcia militarne. Brak jest nadal zdefiniowania i określenia granicy pomiędzy przestrzenią kosmiczną a przestrzenią powietrzną, gdzie interesy państwa i jego suwerenność powinny być chronione i zachowane.

Militarne aspekty i zagrożenia wykorzystania przestrzeni kosmicznej

Zainteresowanie militarnymi możliwościami wykorzystania kosmosu narodziło się długo przed wystrzeleniem na orbitę pierwszego sputnika w 1957 roku. Siły zbrojne różnych państw były też w sposób otwarty bądź zakamuflowany inspiratorem i sponsorem wielu różnorodnych przedsięwzięć kosmicznych, spożytkowanych następnie dla celów cywilnych. Od początku ery kosmicznej interesy wojskowe były jednym z decydujących czynników działalności kosmicznej państw. To właśnie działania militarne wymusiły badanie i użytkowanie kosmosu. W celu zwiększenia potęgi sił zbrojnych aktywnie wykorzystywano i nadal eksploatuje się satelity o różnorodnych funkcjach i zadaniach. Ocenia się, że około 70% wystrzelonych w przestrzeń kosmiczną satelitów spełniało i spełnia liczne zadania o charakterze militarnym. Obiekty te, są w ścisłym znaczeniu uzbrojeniem. Nie stwarzają one niebezpieczeństwa bezpośredniego ataku w kosmosie lub z kosmosu[21]. Zważywszy na powyższe, należy zadać sobie pytanie, czy budowa prawa kosmicznego służy tylko i wyłącznie sferze cywilnej?

Zaawansowane środki łączności, telekomunikacji czy technologii informatycznych oraz inne, tak bardzo dynamicznie rozwijające się technologie w kosmosie mogą tak naprawdę służyć innym celom niż tylko komercji. Takie systemy doskonale zabezpieczają również działalność wojskową i mogą być użyte w celach militarnych. Dotyczy to w szczególności systemów wczesnego uprzedzenia i nawigacji satelitarnej, z których korzystają urządzenia wojskowe, systemy naprowadzania, środki rażenia oraz samoloty wojskowe. Zatem, pomimo iż budowa prawa kosmicznego ma charakter administracyjny i służy między innymi rozwojowi technik, w szczególności informacyjno-telekomunikacyjnych nie można, a nawet nie powinno się wykluczać różnego rodzaju zagrożeń. Sformułowania zawarte w treści aktów międzynarodowego prawa kosmicznego, w tym także w projekcie założeń do projektu ustawy – Prawo kosmiczne[22] mogą pozostać wyzwaniem przyszłości, a nie realną normą prawnomiędzynarodową.

Z militarnego punktu widzenia należy zwrócić szczególną uwagę na fakt, że prawo kosmiczne określa zakaz używania i rozmieszczania w przestrzeni kosmicznej broni nuklearnej oraz innych rodzajów broni masowego rażenia. Dotyczy to ich umieszczania na orbicie wokół Ziemi, instalowania na ciałach niebieskich lub umieszczania gdziekolwiek w kosmosie i w jakikolwiek sposób[23]. Zabronione jest także dokonywanie wybuchów atomowych, jak również wojskowe lub inne wrogie używanie technik modyfikujących strukturę kosmosu. Pomimo zapisów o charakterze demilitaryzacyjnym, międzynarodowe prawo kosmiczne nie zabrania rozmieszczania na pokładzie obiektów oraz bezpośrednio w przestrzeni kosmicznej broni konwencjonalnej[24]. Zapisy prawa nie zabraniają również przelotu przez przestrzeń kosmiczną obiektów z bronią jądrową oraz innymi rodzajami broni masowego rażenia, jeżeli taki przelot nie jest zakwalifikowany jako rozmieszczanie takiego obiektu w kosmosie.

Obecnie prowadzi się prace w kierunku zakazu prób i rozmieszczania w kosmosie broni antysatelitarnej, która byłaby zdolna uszkadzać czy niszczyć systemy kosmiczne państw oraz obsługujące je systemy naziemne. Dokonanie takiego aktu byłoby z punktu widzenia prawa międzynarodowego kwalifikowane jako zbrojny atak na państwo obce. Wprowadzenie restrykcji dotyczących

[21] C.T. Szyjko, *Rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej* [w:] Bezpieczeństwo kosmosu, Warszawa 2010.

[22] Opracowanym przez Ministerstwo Gospodarki – projekt z dnia 19 sierpnia 2014 r. planowany do wejścia w życie ustawy do końca 2015 r.

[23] C.T. Szyjko, *Rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej*...

[24] Broń konwencjonalna (klasyczna), to wszystkie rodzaje broni z wyjątkiem broni masowej zagłady (broń jądrowa, chemiczna i biologiczna) powodująca masowe rażenie ludzi i zwierząt oraz niszczenie i skażenie sprzętu bojowego, terenu, obiektów i pokrycia roślinnego na dużych obszarach – *Słownik języka polskiego PWN* dostępny na http://sjp.pwn.pl/ [dostęp: 04.12.2014] oraz *Ilustrowany Leksykon Lotniczy – Uzbrojenie*. Warszawa 1991, s. 34.

użycia broni antysatelitarnej stało się logicznym uzupełnieniem już zawartych i obowiązujących umów międzynarodowych dotyczących zakazu umieszczania broni jądrowej oraz broni masowego rażenia, systemów obrony przeciwrakietowej oraz ofensywnych zbrojeń strategicznych. Założenia takie, z punktu widzenia przyszłej działalności w przestrzeni kosmicznej są bardzo ważne. Wykluczają one przekształcenie kosmosu w teatr działań wojennych czy platformę zdolną do wykonania ataku na inne państwo.

Obecnie akty prawa międzynarodowego zakazują działań o charakterze ofensywnym jedynie w stosunku do Księżyca i innych ciał niebiskich. Ewolucja przepisów prawa zmierza do całkowitego zakazu używania broni nie tylko jądrowej, masowego rażenia, ale również konwencjonalnej. Kosmos będzie miejscem rozwoju technik informacyjnych, telekomunikacyjnych, satelitarnych oraz innych, które będą wykorzystywane nie tylko do celów komercyjnych. Jak wiadomo, informacja oraz jej przekazywanie, czasem na duże odległości, a w szczególności dane w czasie rzeczywistym są doskonałym źródłem informacji pożądanych w czasie konfliktów militarnych. Reasumując, należy podkreślić, że wprowadzenie broni do kosmosu doprowadzić może do wielu negatywnych skutków oraz spowodować poczucie zagrożenia. Poza tym, taka działalność przysporzyłaby utrudnień dla cywilnej działalności w tym środowisku, prowadząc do ograniczenia dalszego badania kosmosu.

Militarna działalność satelitarna w przestrzeni kosmicznej

W przestrzeni okołoziemskiej znajduje się wiele różnych sztucznych satelitów: biologicznych, geofizycznych, telekomunikacyjnych, astronomicznych i innych. Większość z nich ma zadania naukowe oraz zastosowania komercyjne. Statek kosmiczny, wahadłowiec czy inne obiekty z załogami na pokładzie – to satelita załogowy. Wśród nich istnieją także satelity rozpoznawcze, określane mianem satelity-szpiega. Są to urządzenia mające na celu zdobycie, przetworzenie i przechowywanie pożądanych przez podmiot nią władający, sygnałów, obrazów lub innego typu informacji, które są wykorzystywane do celów wojskowych czy wywiadowczych. Satelity te spełniają dwa podstawowe zadania. Pierwsze dotyczy pozyskiwania danych, wraz z możliwością ich transmisji w czasie rzeczywistym, natomiast drugie daje sposobność przechwytywania sygnałów telekomunikacyjnych. Jak widać, urządzenia te są w stanie zbierać bardzo wartościowe dane z punktu widzenia militarnego. Przykładem są tutaj działania operacyjne prowadzone przez Stany Zjednoczone. Najprawdopodobniej z technologii tej korzystano podczas akcji schwytania Osamy bin Ladena. Podczas prowadzenia operacji w Pakistanie dochodziło do problemów związanych z wykorzystaniem przestrzeni powietrznej przez bezzałogowe statki powietrzne (*Unmanned Aerial Vehicles* – UAVs), które wykonywały loty o charakterze rozpoznawczym i mogły dostarczyć cennych danych o miejscu przebywania terrorysty. Zgoda taka nie musi być udzielana dla satelitów, które, choć z mniejszą dokładnością, są w stanie dokonać rozpoznania terenu.

Kto ma informację, ten ma władzę lub też, nie ma co ukrywać, olbrzymią przewagę. Jaki jest zatem status prawny satelity szpiegowskiego? Pierwszy problem nasuwa się już przy ocenie z punktu widzenia naruszenia przestrzeni danego państwa. Przelot takiego obiektu odbywa się nad terytorium państwa, które to powinno udzielić na taki przelot zezwolenia. Nie dość, że granica przestrzeni kosmicznej z przestrzenią powietrzną nie jest ustalona prawnie, a zatem nie ma granicy suwerenności (maksymalnej wysokości, w której państwo jest w pełni autonomiczne), to ponadto może wydawać się, że jest to argument absurdalny. Ruch obrotowy Ziemi powoduje, że każde państwo po upływie czasu posiada inny „wycinek" przestrzeni kosmicznej. W odpowiedzi na protesty społeczności międzynarodowej uznano, że ruch Ziemi jest w tym względzie obojętny. Przy istniejącym stanie prawnym należy zadać pytanie odwrotne: czy w celu poszanowania suwerenności państwa może ono zestrzelić satelitę, odbywającego lot nad jego terytorium? W tej kwestii istotną rolę odegrała Organizacja Narodów Zjednoczonych[25]. Rezolucja nr 1472 z 12 grudnia 1959 roku powołała Komitet do Spraw Pokojowego Wykorzystania Przestrzeni Kosmicznej, który podjął de-

[25] Organizacja Narodów Zjednoczonych – *United Nations* (UN) – organizacja międzynarodowa, której głównym celem działalności jest utrzymanie międzynarodowego pokoju i bezpieczeństwa. Obecnie organizacja zrzesza 193 państwa, dostępny na http://www.un.org [dostęp: 04.12.2014].

klarację (w formie dziesięciu punktów) dotyczącą zasad prawnych, regulujących działalność państw w kosmosie. Oczywisty wydaje się fakt, że satelity (w tym także załogowe) podlegają wyłącznej jurysdykcji państwa, które jest ich własnością[26]. Poza tym satelita rozpoznawczy nie narusza zasad istniejącego międzynarodowego prawa kosmicznego, ponieważ nie wymienia ono *expressis verbis* – zakazu korzystania z tego typu środków. Ponadto można także uważać, że działalność rozpoznawczo-wywiadowcza służy utrzymywaniu pokoju oraz ograniczeniu proliferacji terroryzmu, który jest niewątpliwie współczesnym zagrożeniem. Prawo wojenne nie zabrania również stosowania różnego typu środków do pozyskania informacji na drodze szpiegostwa. Nie określa ono także zasad odbywania żeglugi powietrznej (kosmicznej) przez jakikolwiek obiekt kosmiczny, a więc, jako niezabroniony, jest on dozwolony.

Problemem są sytuacje, w których następuje lądowanie satelity lub przypadki, gdy spadnie on cały lub jego części na terytorium innego państwa. W takim przypadku odpowiedzialne za niego jest państwo, które taki obiekt wyniosło w przestrzeń kosmiczną. Oznacza to również, że nie może uchylić się ono od sankcji z tego tytułu, powołując się na przesłanki typu siła wyższa, skrajny przymus, czy stan wyższej konieczności. Przykładem jest rakieta kosmiczna, która spadła u wybrzeży Syberii w 1969 roku, raniąc japońskich marynarzy, czy nieudane wyniesienie radzieckiego satelity, który 24 stycznia 1978 roku spadł na terytorium Kanady, powodując skażenie materiałem radioaktywnym na powierzchni 120 tys. km^2. Innym problemem jest fakt, że państwo, na którego terytorium spadł satelita rozpoznawczy, może pozyskać informację dotyczącą działalności wywiadowczej państwa, które jest właścicielem tego satelity, pomimo że w obliczu prawa jest jego właścicielem.

Działalność balistyczna w przestrzeni kosmicznej

W obliczu dynamicznego rozwoju technologii rakietowych oraz braku uregulowań prawnych bardzo niebezpieczne w kontekście interesów państwa wydają się być rakiety balistyczne. Z założenia, jest to rodzaj broni przeznaczony do niszczenia i obezwładniania celów na bardzo duże, nawet kilkutysięczne odległości od miejsca ich wystrzelenia. Tor lotu takiego pocisku może odbywać się także w przestrzeni kosmicznej. Wyobraźmy sobie także, że broń taka niekoniecznie musi stanowić zagrożenie dla innych państw. Jej inną funkcją może być ochrona Ziemi przed zagrożeniami z kosmosu. 15 lutego 2014 roku w efekcie wybuchu w atmosferze meteoru o średnicy 15 metrów w Czelabińsku w Rosji doszło do ogromnych strat w mieście i ranienia 1200 osób.

Rosyjscy naukowcy zaproponowali rozwiązanie dla zagrożeń nadciągających w kierunku Ziemi z przestrzeni kosmicznej[27]. Rosyjskie rakiety balistyczne dalekiego zasięgu SS-18 Satan, zdolne do przenoszenia nawet 10 głowic nuklearnych każda, mogłyby stanowić obronę Ziemi przed dużymi meteorytami. Rakieta według naukowców nadaje się idealnie, ma 34 metrów długości, masę około 200 ton i zasięg około 11 tys. km. Rosja posiada około 60 takich pocisków. Ich jednostka napędowa oparta jest na stosunkowo tanim paliwie rakietowym-hydrazynie, które magazynowane jest w pocisku na stałe. Dzięki temu skraca się czas jego użycia w ciągu 20 minut od rozkazu do jego odpalenia. Ponadto „Szatan" od momentu wejścia w stan gotowości może przebywać w nim nawet do 10 lat. Cały czas, jaki zająłby na zniszczenie meteorytu wynosiłby 5 godzin. Na ustalenie trajektorii lotu potrzebne są dwie godziny, jedna na analizę i podjęcie decyzji przez głowę państwa oraz skoordynowanie działań na Ziemi, a kolejne dwie godziny na dotarcie rakiety do celu od czasu jej inicjacji. Szacuje się, że rakieta SS-18 Satan jest w stanie skutecznie zneutralizować meteoryt o wymiarach nawet do 100 metrów średnicy. Na ten rok Rosjanie zapowiedzieli wykonanie manewrów na szeroką skalę oraz wystrzelenie międzykontynentalnych rakiet balistycznych. Ponadto wojska kosmiczne Federacji Rosyjskiej przeprowadziły testy nowego rakietowego systemu kosmicznego „Angara", a w czerwcu odbył się start rakiety nośnej „Sojuz-2.1b" z aparatem kosmicznym „GLONASS-M" i astronomicznym aparatem telekomunikacyjnym „Gonets-M"[28].

[26] Ł. Tecław, *Status prawny satelity szpiegowskiego*, dostępny na http://studentprawa.edu.pl/artykuly/item/2259-status-prawny-satelity-szpiegowskiego [dostęp: 04.12.2014].

[27] Tekst dostępny na http://losyziemi.pl/ [dostęp: 04.12.2014].

[28] *Rosyjskie wojska kosmiczne przeprowadzą ćwiczenia wojskowe*, tekst dostępny na http://polish.ruvr.ru/news [dostęp: 04.12.2014].

Agencja Stanów Zjednoczonych (*Missile Defence Agency* – MDA) trzy lata temu, w ramach swojego projektu rozpoczęła budowę systemu śledzenia obiektów międzyplanetarnych o nazwie *Space Tracking and Surveillance System* (STSS). System przewidziany jest także do śledzenia rakiet balistycznych. Prowadzony program połączony jest z testami naziemnych i morskich pocisków przechwytujących. Satelity systemu STSS mają niszczyć broń balistyczną przeciwnika, zanim te wejdą w zasięg konwencjonalnych radarów. System jest w stanie wykryć zagrożenia w zakresie bliskiej podczerwieni i świetle widzialnym, z wysokości 1350 km. Po wykryciu startu pocisku balistycznego system używa innych detektorów do śledzenia trajektorii lotu rakiety. Wyniki przeprowadzonych już pięć lat temu testów są obiecujące i zmierzają do stworzenia zintegrowanego systemu i rozpoczęcia stosowania go w warunkach bojowych. W czasie prób przeprowadzonych we wrześniu 2010 roku dwa testowe satelity STSS wyniesione na orbitę śledziły sześć amerykańskich rakiet oraz rakietę balistyczną Minuteman-3. Obecnie rolę systemu wczesnego ostrzegania spełniają konstelacje satelitów innego programu *Defense Support Program* (DSP). Jego satelity obserwują Ziemię z orbity geostacjonarnej. Są one w stanie wykrywać jedynie start pocisku balistycznego zmierzającego w przestrzeń kosmiczną, bez możliwości śledzenia jego trajektorii. Jeśli dalsze badania i wdrożenia elementów systemu STSS będą przebiegać pomyślnie, z czasem staną się one częścią systemu obrony przeciwrakietowej USA i będą mogły być również używane przez inne placówki rozmieszczone w Europie, a może i w Polsce.

Budowa systemów rakietowych oraz pocisków balistycznych, które są w stanie osiągnąć wysokość przestrzeni kosmicznej, zmierza w dwóch kierunkach. Pierwszy z nich zakłada użycie rakiet balistycznych, czyli *de facto* broni, do celów pokojowych, a dokładniej do obrony ludzkości przed zagrożeniami, jakie niesie za sobą kosmos. Drugi przewiduje dalszy dynamiczny rozwój broni rakietowej o zasięgu międzykontynentalnym. Czy te dwa kierunki rozwoju będą nadal utrzymane, pokaże to czas. W odpowiedzi na rozwój broni balistycznej buduje się systemy, które są w stanie przechwytywać, śledzić i w razie potrzeby unieszkodliwiać wrogie działania, a przynajmniej je kontrolować. Należy też zwrócić uwagę, że zarówno pociski balistyczne o zasięgu do kilkudziesięciu tysięcy kilometrów, jak również systemy satelitarne mogą stworzyć poważne zagrożenie dla suwerenności i obronności państw w szczególności tych, które takiej broni nie posiadają. Trzeba również podkreślić, że właścicielami takich systemów są największe mocarstwa światowe, takie jak: USA, Rosja czy Chiny. Budowa tych systemów w aspekcie prawa kosmicznego nie jest na chwilę obecną żadną przeszkodą. Może właśnie dlatego, że nakłady finansowe, długofalowa budowa oraz możliwe do osiągnięcia polityczno-militarne cele są ważniejsze niż określenie granicy przestrzeni kosmicznej i poszanowania suwerenności państw, jako właścicieli nie tylko przestrzeni powietrznej, ale również i kosmicznej.

Podsumowanie

Problem ustalenia górnej granicy przestrzeni powietrznej, w której odbywają się kontrolowane przeloty statków powietrznych, istnieje od dekad. Z jednej strony jest to sytuacja komfortowa dla mocarstw, które nie muszą liczyć się z zgodą na przelot i które to stwarzają sobie przewagę, polegającą na tym, że w dowolny sposób mogą korzystać z przestrzeni kosmicznej innych państw. Z drugiej zaś strony loty takie stwarzają niebezpieczeństwo naruszenia suwerenności państw, nad którym inny kraj odbywa lot środka rażenia, jakim są rakiety balistyczne czy dokonuje innych operacji o charakterze wojskowym, takich jak rozpoznanie satelitarne. Na podstawie analizy wybranych problemów wynikających z tworzenia międzynarodowego prawa kosmicznego i przytoczonych w treści przykładów udowodniono, że tworzenie takiej ustawy, mającej charakter *stricte* administracyjny pociąga za sobą realne zagrożenia militarne.

Po analizie dostępnych aktów prawnych i publikacji można przedstawić następujące wnioski:

- Obecnie brak jest ustalenia prawnego granicy pomiędzy przestrzenią powietrzną a kosmosem. Problemy dotyczące rozgraniczenia powierzchni pozostają nie do końca wyjaśnione. Brak jest także innych klauzul o charakterze demilitaryzacyjnym, dotyczącym przestrzeni kosmicznej w prawie międzynarodowym i krajowym. Skutkuje to brakiem całkowitej ochrony państwa przed zagrożeniami militarnymi z przestrzeni kosmicznej.

• Współczesne akty prawa międzynarodowego oraz projekt założeń do ustawy zaproponowany przez Ministerstwo Gospodarki wykazują administracyjny charakter prawa w tym obszarze. Pomimo że dotyczą one sektora cywilnego, oddziałują na interesy bezpieczeństwa państwa. Akty, poprzez brak zapisków dotyczących demilitaryzacji kosmosu, dopuszczają przeloty obiektów militarnych (w tym także jako nosicieli uzbrojenia) w przestrzeni kosmicznej rozciągającej się nad terytorium państwowym. Można zatem konstatować, że zagraża to suwerenności państwa i jego bezpieczeństwu.

• Środki rażenia czy satelity szpiegowskie mają podwójne zastosowanie. Służą jako klasyczna broń oraz mogą chronić interesy nie tylko właścicieli takiej technologii, ale również innych państw przed zagrożeniami.

• Międzynarodowe i krajowe akty prawne dotyczące przestrzeni kosmicznej będą zmierzać ku ujednoliceniu zasad oraz stworzenia jednolitej przestrzeni powietrzno-kosmicznej. Przestrzeń ta powinna być odpowiednio podzielona. Taki stan rzeczy określi jej przynależność i spowoduje całkowite poszanowanie suwerenności państwa oraz zniweluje możliwość zagrożeń o charakterze militarnym. Problemem są także kwestie techniczne, polegające na śledzeniu takich obiektów w przestrzeni kosmicznej. Na podstawie wyników testów, prowadzonych między innymi przez USA, można wnioskować, że w niedalekiej przyszłości będzie to bardzo realne.

Bibliografia

Karta Narodów Zjednoczonych z 26 VI 1945 roku (DzU z 1947 roku nr 23, poz. 90 ze zm).

Projekt założeń do projektu ustawy – Prawo kosmiczne, Ministerstwo Gospodarki, Projekt z dnia 19 sierpnia 2014 r. dostępny na http://www.legislacja.rcl.gov.pl [dostęp: 29.10.2014].

Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej łącznie z Księżycem i innymi ciałami niebieskimi z 27 stycznia 1967 roku, Moskwa, Londyn, Waszyngton – DzU z 1968 roku, nr 14, poz. 82.

Apfel N.H., *Space law*, New York 1988.

Berezowski C., *Międzynarodowe prawo lotnicze,* Warszawa 1964.

Cheng C.J., *New sources of international space law*, Hague 1998.

Durys P., Jasiński F., *Wybór aktów prawnych do nauki międzynarodowego prawa lotniczego i kosmicznego*, Warszawa 1999.

Fixel R.W., *The law of aviation*, Bloomington 1999.

Galicki Z., *Prawna delimitacja przestrzeni kosmicznej – problem nadal nierozwiązany*, referat z konferencji naukowej nt. „Wykorzystanie przestrzeni kosmicznej. Świat – Europa – Polska", Uniwersytet Warszawski, 25 września 2009 roku.

Ilustrowany Leksykon Lotniczy – Uzbrojenie. Warszawa: WKŁ 1991.

Kolańczyk K., *Prawo rzymskie*, Warszawa: LexisNexis, 2007.

Midle M., *International air law and ICAO*, Utrecht 2008.

Polkowska M., *Prawo kosmiczne w obliczu nowych problemów współczesności.* Warszawa: LIBER, 2011.

Polkowska M., *Suwerenność państwa w przestrzeni powietrznej. Geneza, zakres i ewolucja.* Warszawa: LIBER, 2009.

Shaw M.N., *Prawo międzynarodowe.* Warszawa: Książka i Wiedza, 2012.

Szyjko C.T., *Rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej* [w:] Bezpieczeństwo kosmosu, Warszawa 2010.

Tate L., *The status of the outer space treaty at International law during „war" and „those measures short of war"*, JSL 2006.

Tecław Ł., *Status prawny satelity szpiegowskiego*, dostępny na http://studentprawa.edu.pl/artykuly/item/2259-status-prawny-satelity-szpiegowskiego [dostęp: 04.12.2014].

Żylicz M., *Prawo lotnicze międzynarodowe, europejskie i krajowe.* Warszawa: LexisNexis, 2011.

http://geopolityka.org/ [dostęp 22.11.2014].

http://nasa.com/ [dostęp 22.11.2014].

http://space.gov.za/ [dostęp 22.11.2014].

MILITARY USE OF OUTER SPACE

Abstract

The article makes an attempt to identify and discuss selected problems related to the use of outer space, as the consequences resulting from the structure of the draft law - the law of space. In an analysis of legal acts ranging from 1957, when the era of space exploration began, concepts for defining the boundary between airspace and outer space are described. A major research problem was the attempt to answer the question: what meaning does

space have for the State in the political and military context? The research and the search for answers to the main problem were inspired by the hypothesis of the authors who believed that: from the politico-military point of view, space is just as important for the preservation of State sovereignty as the airspace. It has been proven that, from the politico-military point of view, it is important for the preservation of State sovereignty, as the owner of these two spaces. Stages for the creation of international space law are presented and significant legislation affecting the further development of international law of space is outlined. On the basis of the draft guidelines to the Space Law Bill, the origins, scope and principles under which the act arises are described. After this, the aspects and threats of using space in the face of that law is discussed. Moreover, selected problems and possible politico-military consequences resulting from the use of outer space are put forward and threats are described based on examples.

Keywords: airspace, outer space, sovereignty, national security.

Introduction

The development of techniques over many years has allowed man to create flying objects that have the ability not only to move through the Earth's atmosphere, but also in outer space. The failed flight of the Apollo 13[1] spacecraft, which was launched on 11 April 1970, with the goal of landing on the surface of the moon, rose over a distance of more than 400 thousand miles from the surface of the Earth, surpassing the average maximum flight level of a conventional, modern airliner about 27 times. The flight of any aircraft within the airspace of the State is monitored by both the civilian and military air traffic authorities. Unfortunately, the movement of objects in space, taking place on a mission to the territory of a Member State, is not tracked. Objects are not subject to the rules of air traffic. No matter the intent and purpose of such a facility, this situation raises doubts regarding the sovereignty of the State over which the flight takes place, which is a serious safety problem for the modern State.

The dynamic development of space technologies has meant that some objects have flown in space not only to examine it for scientific purposes, and more often it has become an area of commercialism. For the last 30 years, Poland has been developing its own space industry, which consists of 50 research and development units that are under the responsibility of the companies. Their domain is information technology, telecommunications and electronics. It is necessary to formulate a space law at the State level, which would identify the operating principles of objects, as well as the rights and obligations of users. It turns out that it is a process saddled with many problems and we will look at the consequences of these in this publication.

The purpose of this article is to discuss selected problems accompanying the building of space law from civilian and military aspects. Selected contemporary threats, which may entail the using of space in terms of existing international instruments, are examined. Ideas and hypotheses, justified by the results of the analysis of legal acts and other papers, are presented in the content and summary of this work.

The beginnings of the space age and the law

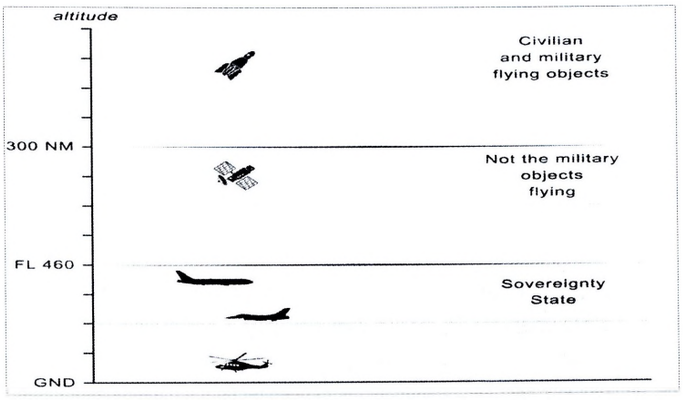
The earliest records relating to space law were observed in 1932. Then, the first monograph by V. Mandla arose and is regarded as a forerunner of cosmic law. This situation occurred 10 years earlier, before man boosted the first rocket into space[2]. This period began a new era of space – the Space Age. Before the launch of the first Sputnik in 1957, a lot of publications made reference to legal issues and human activities in outer space.

[1] The purpose of the mission of Apollo 13 spacecraft for the index COSPAR 1970-29A, which was landing on the Moon, was not achieved. In the course of the mission, a tank of oxygen exploded, forcing the crew to fight for their lives. This explosion of oxygen cylinders took place in the service module. The explosion stripped the module of the power to ensure access to a ship on the Moon and return to Earth. On 17 April, the crew happily returned to Earth, despite the many problems. Apollo 13 was flyingt far away from Earth. The record established on 15 April 1970 was 400 171 km, available at: http://nauka.money.pl/slownik-naukowy/apollo-13-724888.html [access: 31.11.2014].

[2] The first rocket that reached space was the German V2 rocket during flight test on October 3, 1942. on October 4, 1957 the Soviet Union launched Sputnik 1, which became the first artificial satellite to orbit the Earth. The first human spaceflight was Vostok 1, which start April 12, took place in 1961. Aboard the spacecraft was the first in the history of mankind, cosmonaut Yuri Gagarin made one orbit around the Earth.

The ancient Romans had already professed the principle *cuius est solum, eius est usque ad coelum*, which means that the Lord of the Earth is the ruler of the sky above it[3]. This maxim is often supplemented with the words-*usque ad sidera*, translated as: up to the stars. It follows that the State is sovereign in this space and can enforce power over every object in it. Soon it quickly became apparent, unfortunately, that law enforcement in relation to objects in space would be extremely difficult. There are two concepts of respecting the law. The first shows that the height of spacecrafts' trajectory into space is not yet subject to the sovereignty of States - res *communis omnium*[4]. This means that the Member States jurisdiction over airspace is limited to a certain height, which is the border airspace from outer space. However, it is difficult to clearly define the border[5]. One of the supporters of this currency was A. G. Haley, who put forward the idea that space begins where the flying object interacts with the air resistance force, and is subject to repercussions on the centrifugal force[6]. Another supporter was G. Chew, founder of the so-called, *freedom of the sky*. It referred to the freedom of the high seas[7], which is a height of 20-30 km above the surface of the Earth.

The second concept recognised the right of innocent flight of spacecraft through airspace. The creation of an international convention, which tried to divide space into three parts (Fig. 1), was proposed in 1957. This Convention would be analogous to the division of the sea.



Source: own description

Fig. 1. The proposal of space division presented by Cooper in 1957

The first part of this space would extend beyond the length of the ground to a height that classic aircraft can reach. This area shall be subject to the jurisdiction of the State over which it resides and in which the State is a sovereign[8]. The second period would cover the airspace up to a height of 300 miles. This zone should only be available for non-military flying objects from all Member States. The third zone, on the other hand, extending above a height of 300 miles, would be available for both civilian and military craft of all Member States. In view of the fact that this proposal limited the right of the flight[9], it was not accepted.

Concepts of creation of the space law during the beginning of the space age were still few. To sum up, two leading concepts that emerged in those years can be highlighted. One of them was a harmless flight through outer space. The other was that the height of the flight trajectory is not already State sovereignty[10]. These issues are still 7a problem today.

[3] *Internetowy słownik wyrazów obcych i zwrotów obcojęzycznych Władysława Kopalińskiego*, available at: www.slownik-online.pl/ [access: 01.11.2014].

[4] Things for use by the general public: air, flowing water, the sea and the shores of the sea – K. Kolańczyk, *Prawo rzymskie*, Warsaw: LexisNexis, 2007, p. 266.

[5] M.N. Shaw, *Prawo międzynarodowe*, Książka i Wiedza, Warsaw 2012, p. 291.

[6] Object must reach the proper speed, which will enable it to overcome the Earth's gravity and distance in outer space.

[7] The United Nations Convention on the law of the sea of 1982. According to it, each Member State shall have the right to a 12 mile territorial waters zone, the continental shelf and to not more than a 200 NM exclusive economic zone – W. Jędrzejewski, *Status Morza Kaspijskiego*, available at: http://www.psz.pl/Wojciech-Jedrzejewski-Status-Morza-Kaspijskiego [access: 03.12.2014].

[8] A sovereign State shall be construed as an independent and self-authority, according to the dictionary *The American Heritage Dictionary of the English Language* (*AHD*), available at: https://ahdictionary.com [access: 04.11.2014].

[9] The right of the flight specified in the Chicago Convention and recognised as one of the freedoms. It is a privilege to fly across the territory of a Member State without landing. The State (A) grants the State (B) carrier the right to fly over its territory – *Convention on International Civil Aviation, 7 December 1944* (15 U.N.T.S. 295, ICAO Doc 7300/9).

[10] M. Polkowska, *Suwerenność państwa w przestrzeni powietrznej, geneza, zakres i ewolucja*, Warsaw 2009.

Create a cosmic international law

Six years after the first flight into space, a significant action began on the development of space law. The result of these activities was resolution No 18/1962, adopted by the General Assembly of the United Nations[11] in 1963. The subject of content the document has been established in the field of space research, together with the Moon and other celestial bodies. Lack of understanding of the vertical limit, in which the State is responsible for the flights, has caused a problem with the fixing of responsibility for activities in this area[12]. Once again, there is a need to define with a strict definition. The highest atmospheric space frontier is the one on which the satellite, moving after the trajectory, goes into the atmosphere[13].

The next Act was the 1967 space treaty signed at the same time by Russia, the United Kingdom and the United States. One of the assumptions of this document is to confirm that assigning space, along with the Moon and other bodies of blue, is not subject to appropriation. Another important issue contained in the document is the claim that the study and exploration of outer space should serve humanity. The principle of non-discrimination on the possibility of exploration of space was introduced here, not only by the power of the State, but also by other countries. This fact from 1967 still does not define exactly and does not specify what is outer space and airspace. It establishes the basics of the international space law. This system is a part of international law and respects its rules[14].

Over several decades, new legal acts have emerged regulating human activities in space, such as, for example, the Arms ban Convention and the International Space Station from 1976 and the Convention on Early Notification of a Nuclear Accident of 1986. Bi and multilateral agreements were concluded between member states, usually limited to science and technology cooperation in the field of space research. They cover issues such as: remote sensing, environmental protection, collaboration space missions, and meteorology[15]. Currently, there is no international space law designed that includes air navigation rules in this area. In an era of multiple risks, including the possibility of State sovereignty in outer space and air, the space problem is very relevant. It is estimated that at the current stage of development of space law in the world, the number of acts will grow. It should be noted that, in recent years, the nature of the activities of States in outer space has changed. Many initiatives have come from the private sector, which according to lawyers will change the nature of the rights from public to mixed civil-public[16].

Space law in Poland

Poland's accession to the European Space Agency in 2012 allows such entities as the research and development unit, as well as small, medium and large companies to use the knowledge and infrastructure of the Agency. Currently, there is demand for services provided by the space sector. Such a State of affairs obliges the country to create a national space law. The terms of this law has been effect in European and international legislation. The new law requires the settlement of several issues including the rules of consent for activities in airspace by national entities. Other conduct rules include the national register of space objects, the liability of the State and compensation issues. The new law forces Poland to create and administer the register of space objects diffused into outer space by Polish entities. The purpose of the Act is to regulate using the cosmic law of cosmic objects, in such a way that it is not an obstacle to the development of the Polish space sector[17].

The scope of the proposed agreement will include space activities in the peaceful uses of outer space in accordance with a number of

[11] The General Assembly is one of the six principal organs of the United Nations-The United Nations, established by the Charter of the United Nations. The Assembly shall take its decisions in the form of resolutions, which are in force in the internal issues.

[12] P. Durys, F. Jasiński, *Wybór aktów prawnych do nauki międzynarodowego prawa lotniczego i kosmicznego*, Warsaw 1999, p. 228.

[13] R. W. Fixel, *The law of aviation*, Bloomington 1999, p. 65.

[14] L. Tate, *The status of the outer space treaty at International law during „war" and „those measures short of war"*, JSL 2006, p. 181.

[15] M. Polkowska, *Prawo kosmiczne w obliczu nowych problemów współczesności*, Warsaw 2011.

[16] C. J. Cheng, *New sources of international space law*, Hague 1998, p. 207.

[17] *Projekt założeń do ustawy–Prawo kosmiczne*, The Ministry of Economy, the draft of August 19, 2014.

fundamental principles. One of them is the rule of freedom of exploration and the use of outer space for the benefit and in the interests of all countries. Another assumes no expropriation of outer space and its peaceful use. This document defines the rules and requirements for the release of the cosmic[18] objects into space. Consent for the release of an object into space would be issued in the form of an administrative decision, and an entry in the National Registers of Objects Launched into Outer Space will be the technical activity confirming the release of the space object. The foundation of the draft law shall lay down the conditions for obtaining approval for launches of a space object. One of them is compatibility with the interests of national security and foreign policy[19]. Besides other important terms are: the security of space activities, insurance, stating the conclusion of the agreement of civil insurance for damage in connection with space activities, a statement of support for natural processes for other States in the peaceful exploration and use of outer space.

The new space law includes rules governing the use of outer space and objects released there. It is administrative in nature and it concerns the private sector. There are no records of a military-political dimension. There are well known issues regarding the use of outer space which may be associated with threats directed against the State. Such a danger comes from ballistic missiles, spy satellites and other objects. The risk may also come from a different kind of research on nuclear weapons, detonations and other military projects. The boundary between outer space and airspace, where the interests of the State and its sovereignty should be protected and preserved, is not defined.

Military aspects and the threat of the use of outer space

Interest in the military possibilities of the cosmos originated long before the first Sputnik was launched into orbit in 1957. The armed forces of the various Member States were also an open or thinly disguised inspiration behind a variety of space ventures for civilian uses. Since the beginning of the space age, military interests have been one of the decisive factors of the space activities of States. The military dominated exploration and the use of outer space. The armed forces actively used and still operate satellites with various functions and tasks. It is estimated that about 70% of the bullets fired in space comply with the satellites and a number of military tasks. These objects are weapons in the strict sense and do not pose a direct danger of attack in space or from space, but contribute to the strengthening of stability in international relations[20]. In view of the above, you should ask yourself whether the construction of space law is only and exclusively the realm of civilians, or whether it is a duality?

Advanced means of communications, telecommunications and information technology and other, such dynamically developing technologies in space can really serve different purposes than just commercialism. These kinds of systems perfectly secure military activity and can be used for military purposes. These concern, in particular, the early notice and navigation satellite used by military equipment, guidance systems, means of destruction and military aircraft. Therefore, despite the fact that the construction of space law is civilian and serves, inter alia, the development of techniques, in particular telecommunications and information, it cannot and indeed should not exclude all sorts of threats. The wording contained in the body of international law on spacecraft, including the project objectives to the draft law - the space law[21], may remain wishful, the challenge of the future, and not a viable norm of international law.

From a military point of view, particular attention should be paid to the fact that the space law is the prohibition on the use and deployment in outer space of nuclear weapons and other weapons of mass destruction. This applies to their deployment in orbit around the Earth, installing them on celestial bodies or wherever in the cosmos

[18] Space object, in accordance with the draft law- the space law, is a device that will be released or has been launched into space, its components, as well as its load-bearing equipment and parts of this device.

[19] In accordance with article 106 of the code of administrative procedure the proper Minister of National Defence and Minister responsible for Foreign Affairs.

[20] C.T. Szyjko, *Rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej* [in:] Bezpieczeństwo kosmosu, Warsaw 2010.

[21] Developed by the Ministry of Economy-project of 19 August 2014. Planned until the entry into force of the Bill by the end of 2015.

and in any way[22]. It is also forbidden to make nuclear explosions, as well as military or any other hostile techniques for modifying the structure of the cosmos. Despite records of demilitarisation, in international law it is not prohibited to deploy on board objects and conventional weapons in space[23]. The law does not prohibit flight in space of objects with nuclear weapons and other weapons of mass destruction, if such travel is not certified as such a deployment object in space.

Currently ongoing work is being addressed towards prohibiting the deployment of weapons in space and anti-satellite weapons, which would be able to damage or destroy the space systems and systems serving them on the ground. Such an act would be, from the point of view of the international law, qualified as an armed attack on a foreign State. The introduction of restrictions on the use of anti-satellite weapons has become a logical complement to the already concluded and existing international agreements on the prohibition of the placement of nuclear weapons and weapons of mass destruction, missile defense systems and offensive strategic arms. Such assumptions are very important from the point of view of future activities in outer space. They are transforming space into a theatre or a platform able to perform an attack on another country.

Currently, acts of international law only forbid offensive acts on the Moon and other celestial bodies. The evolution of the law aims to prohibit the use weapons of mass destruction, not just nuclear, but also conventional ones. The Cosmos will be the place of development information technology, telecommunications, satellite and other things, which will be used not only for commercial purposes. As you know, information and its transfer, sometimes over long distances, especially data in real time, are perfect „weapons" commonly desired during military conflicts. To sum up, it should be outlined that the introduction of weapons into outer space can lead to many negative effects, and would result in a sense of threat. In addition, these activities could cause inconveniences for civilian operations in this environment, both in the sense of purely practical complications, as well as limiting further examination of the cosmos.

Military satellite activity in outer space

Earth space released many different artificial satellites: biological, geophysical, telecommunications, astronomy and more. Most of them have scientific tasks and commercial applications. The spacecraft, the space shuttle and another objects with crew on board - the manned satellite. Among them, there are also reconnaissance satellites, known as spy-satellites. These devices are designed to capture, process and store the wielding, signals, pictures, or any other type of information desired, which are used for military or intelligence needs. These satellites meet two basic tasks. The first relates to the data, with the possibility of transmission in real time, while the second gives you the opportunity to intercept the telecommunications signals. As you can see, these devices are able to collect valuable data from the military point of view. For example, here are the operational activities carried out by the United States. It is most likely that technology was used during the capture of Osama bin Laden while conducting operations in Pakistan led to the problems related to use of Unmanned Aerial Vehicles (UAVs), which carried out the intelligence flights and could provide valuable data about the location of the terrorist. Such consent must be granted for satellites, which, though with less accuracy, are able to make a diagnosis of the land.

Whoever has information has power or there is nothing to hide an enormous advantage. What, therefore, is the legal status of spy satellites? The first problem arises during assessment from the point of view of a breach of the State concerned. The flight of an object carried out on the territory of a Member State should have permission for that flight. The limit of space from airspace is not legally established, and, therefore, there is no boundary of sovereignty (the maximum height in which the State is fully autonomous), it can seem that the argument is absurd. Earth's rotation means that each State, after a period of time, has a different „slice" of space. In response to protests from the

[22] C.T. Szyjko, *Rewizja zasad pokojowego wykorzystania przestrzeni wokółziemskiej…*

[23] Conventional weapon – all types of weapons, with the exception of weapons of mass destruction (nuclear weapons, chemical and biological) resulting in massive electricution of humans and animals and the destruction and contamination of the combat equipment, terrain, facilities and plant cover in large areas – *Słownik języka polskiego PWN* available at: http://sjp.pwn.pl/ [access: 04.12.2014] and *Ilustrowany Leksykon Lotniczy – Uzbrojenie*. Warszawa 1991, p. 34.

international community, it was considered that the ground motion is neutral in this regard. On the existing state of the law, one must ask the question: in order to respect the sovereignty of Member States, can a Member State shoot down the satellite that flies over its territory? In this matter, an important role is played by the United Nations[24]. Resolution No 1472, of 12 December 1959, created the Committee on the Peaceful Uses of Outer Space (COPUOS), which made a declaration (in the form of ten points) on the legal principles governing the activities of States in outer space. It seems that satellites (including human ones) are subject to the exclusive jurisdiction of the State, which is their owner[25]. Besides, a reconnaissance satellite does not break existing rules of international law, because space does not mention *expressis verbis*-prohibition on the use of such measures. In addition, one can also consider that intelligence-reconnaissance activities serve to maintain peace and reduce the proliferation of terrorism, which is undoubtedly a contemporary threat. The law of war does not prohibit using various means to obtain information by means of espionage. The principles of air navigation services (space) by any space object are not specified, and neither whether it is prohibited.

Another situation is where a satellite lands on the territory of another State or when it falls on its land in any form. In this case, the State is responsible for the object. It also means that one may not revoke it from the sanctions, citing reasons of force majeure, an extreme coercion or State of necessity. An example of this is the space rocket that fell on the coast of Siberia in 1969 wounding Japanese sailors, and the failed launches of the Soviet satellites, which, on 24 January 1978, fell on the territory of Canada, causing contamination of radioactive material on a surface of 120,000 square km^2. Another related issue is the fact that the State, on whose territory the fallen reconnaissance satellite can acquire information on the intelligence activities of the State which owns the satellite, despite the fact that in the face of the law it is its owner.

[24] United Nations (UN) – international organisation, whose main purpose is to maintain international peace and security. Currently, the Organization has 193 Member States, available at: http://www.un.org [access: 04.12.2014].

[25] Ł. Tecław, *Status prawny satelity szpiegowskiego*, available at: http://studentprawa.edu.pl/artykuly/item/2259-status-prawny-satelity-szpiegowskiego [access: 04.12.2014].

Ballistic activities in outer space

In view of the dynamic development of missile technology and the lack of legislation, ballistic missiles seem to be very dangerous in the context of the interests of the Member States. By design, these are the kinds of weapons intended to destroy and incapacitate targets at a few thousand distance from the place of their launch. These projectiles can also make a flight path in space. Imagine also that this weapon does not necessarily pose a threat to other countries. Another of its functions may be protecting the Earth against threats from outer space. In Chelyabinsk in Russia, there were 1200 casualties on 15 February 2014 as a result of the explosion in the atmosphere of a Meteor with a diameter of 15 metres.. Russian scientists have proposed a solution for attacking threats in the direction of the Earth from outer space[26]. Russian long-range SS-18 Satan ballistic missiles, capable of carrying up to 10 nuclear warheads each, could provide Earth with defence against large meteors. According to researchers, the rocket is ideal, is 34 metres long, has a weight of approximately 200 tons and a range of about 11,000 km. Russia has about 60 such missiles. Their engine is based on the relatively low-cost rocket fuel-hydrazine, which is stored in the projectile on a permanent basis. This shortens the time of its use within 20 minutes from firing. In addition, the „Satan", from the moment you put it on standby, may be present for up to 10 years, all the time, which would focus on the destruction of the meteorite in 5 hours. To determine the trajectory of a flight two hours are needed, one to analyse and for the head of state to make a decision State and to coordinate actions on the ground, and another two hours to reach the rocket f. It is estimated that the SS-18 Satan is able to effectively neutralise a meteorite with dimensions up to 100 metres in diameter. This year, the Russians have announced the execution of large-scale maneuvers and the launch of intercontinental ballistic missiles. In addition, the space forces of the Russian Federation carried out the testing of a new space system rocket „Angara", and the rocket bearing „Soyuz-2.1b" with a cosmic „GLONASS-M"

[26] Text available at http://losyziemi.pl/ [access: 04.12.2014].

and telecommunications astronomical „Gonets-M" apparatus [27] was started.

The Missile Defence Agency (MDA)i began construction of a system called the Space Tracking and Surveillance System (STSS) three years ago. The system will also track ballistic missiles. The programme is connected with ground-based interceptors and sea tests. Satellites of STSS will destroy the enemy`s ballistic weapons before they come in range of conventional radar detectors. The system is able to detect threats in near-infrared and visible light, from a height of 1350 km. Upon detection of a ballistic missile launch, the system uses other detectors to track the trajectory of a rocket flight. The results from tests five years ago are promising and are going to create an integrated system and start using it in combat conditions. During the tests carried out in September 2010, two satellites in orbit with STSS followed six American missiles and a Minuteman-3 ballistic missile. Currently, the role of an early-warning system meets the constellations of the satellites Defence Support Programme (DSP). Its satellites observe the Earth from geostationary orbit. They are only able to detect the start of a ballistic missile entering space, without being able to trace its trajectory. If further study and implementation of the system will successfully run the STSS, they will become part of the missile defecse system of the USA and can also be used by other establishments located in Europe, and perhaps in Poland.

The construction of missile systems and ballistic missiles, which are able to reach the height of space, is moving in two directions. The first one involves using ballistic missiles, which are de facto weapons, for peaceful purposes, namely to defend mankind against dangers posed by space. The second provides for further dynamic development of the missile with intercontinental range. Whether this will be proved and developments will continue to be maintained, only time will tell. In response to the development of ballistic weapons, there are building systems which are able to capture, track and, if necessary, deal with hostile actions, or at least control them. Moreover, it should be noted that ballistic missiles with a range up to tens of thousands of kilometres away, as well as satellite systems, can create a serious threat to the sovereignty and defence of the Member States, in particular those which do not possess such weapons. It is necessary to point out that the owners of such systems are the greatest world powers, such as: the USA, Russia or China. The construction of these systems in terms of space law is not an obstacle at the moment. Maybe that's because the financial outlays, long-term construction and opportunity to achieve political and military objectives are more important than identification of delamination space and respect for the sovereignty of States, as owners of not only the sky but also exploration.

Summary

The problem of determining the upper limit of the airspace, which hosts controlled flights of aircraft, has existed for decades[28]. On the one hand, it's a comfortable situation for powers who do not need to reckon with flight permission and provides an advantage that one can make use of the space of the other Member States. On the other hand, such flights pose a danger of the violation of the sovereignty of States, over which a different country takes a lot of the destruction of ballistic missiles or other military operations shall be carried out, such as satellite reconnaissance. On the basis of specific problems arising in the course of the development of international law and in the provisions for cosmic examples, it has been proven that creating such a law, which has a strictly administration-civilian character, entails real threats of a military nature.

After analysing the available acts and publications, the following conclusions can be made:

- At the moment there is a lack of legal arrangements between delimitation agreement for airspace and outer space. Problems relating to the delimitation of the surface are not completely explained. There are no other clauses of a demilitarisation character on the space of national law and the world. This leads to a lack of complete country protection against military threats.
- Contemporary acts of international law and the draft guidelines to the Bill proposed by the Ministry of Economy show the legal and judicial nature of the act. Despite the fact that it relates

[27] *Rosyjskie wojska kosmiczne przeprowadzą ćwiczenia wojskowe*, available at: http://polish.ruvr.ru/news [access: 04.12.2014].

[28] N.H. Apfel, *Space law*, New York 1988, p. 58–60.

to the civil sector, it affects the interests of the security of the State. Acts of law, through the lack of notes relating to the demilitarisation of space, allow overflights of military objects (including missile carriers) in outer space above the territory of the State. One suspects that this reconciles its national sovereignty and security.

• Means of destruction or spy satellites have an ambivalent use. They serve as a classic weapon, and can protect the interests of not only the owners of such technology, but also other Member States against dangers arising from the construction and reaction occurring in the universe or to fight against such modern-day threats as terrorism. These are real 21st century threats against activities in the name of the general good (social).

• Legal acts will tend toward unification of rules and creation of a single air-outer space exploration area. This space should be owned by the State, over which it extends. This state of affairs will completely respect the sovereignty of Member States and the possibility of the application of military threats. There are certainly technical issues, consisting of tracking such objects in space. On the basis of results of tests carried out by the United States, among other things, it can be concluded that in the near future it will be very real.

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

EKONOMIA BEZPIECZEŃSTWA I LOGISTYKA

MOŻLIWOŚCI ZASTOSOWANIA NOWOCZESNYCH NARZĘDZI INFORMATYCZNYCH W KIEROWANIU SYSTEMEM LOGISTYCZNYM W ĆWICZENIACH WSPOMAGANYCH KOMPUTEROWO NA PRZYKŁADZIE ĆWICZENIA ŚLĄSK-14

ppłk dr Sławomir BYŁEŃ
Akademia Obrony Narodowej

Wprowadzenie

W ocenie specjalistów, jedną z najskuteczniejszych form szkolenia dowództw i sztabów są ćwiczenia dowódczo-sztabowe wspomagane komputerowo CAX (*Computer Assisted Exercise*), w których na bazie opracowanego scenariusza ćwiczenia wykorzystuje się komputerowe systemy symulacyjne, zastępujące praktyczne działanie wojsk. Dla kierownictwa ćwiczenia (KĆ) zarządzającego potencjałem logistycznym rozmieszczonym na połowie obszaru państwa, kluczowe znaczenie ma sprawnie funkcjonujący system informatyczny, pozwalający kontrolować praktycznie każdy podległy element, w tym szczególnie w kierowaniu systemem logistycznym szczebla operacyjnego. Wobec powyższego należy założyć, że bez dobrze zaprojektowanych i wdrożonych narzędzi informatycznych niemożliwe jest zarządzanie potencjałem logistycznym dużej organizacji wojskowej.

Przedmiot badań

Przedmiotem badań były możliwości wykorzystania narzędzi informatycznych w ćwiczeniu pk. Śląsk-14 w organizowaniu i kierowaniu systemem logistycznym przez Inspektorat Wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej (IWsp SZ RP).

Cel, problemy i metody badawcze

Cele opracowania: a) **cel poznawczy** – *Zbadanie możliwości wykorzystania systemów informatycznych w kierowaniu systemem logistycznym w ćwiczeniach dowódczo-sztabowych wspomaganych komputerowo;* b) **cel praktyczny** – *ustalenie przydatności posiadanych przez Centrum Symulacji i Komputerowych Gier Wojennych (CSiKGW) narzędzi informatycznych w zarządzaniu systemem logistycznym w ćwiczeniu szczebla operacyjnego.*

Zważywszy na cel główny, cele cząstkowe zostały zdefiniowane jako: *możliwości zabezpieczenia potrzeb IWspSZ, występującego w roli kierownictwa ćwiczenia we wsparciu ćwiczenia dowódczo-sztabowego wspomaganego komputerowo przez CSiKGW. Weryfikacja potrzeb informatycznych KĆ w zakresie modelowania działań logistyki wojskowej z możliwościami posiadanymi przez CSiKGW. Ocena wpływu systemów informatycznych na kierowanie organizacją wojskową odpowiedzialną w Siłach Zbrojnych RP za funkcjonowanie systemu logistycznego szczebla operacyjnego w CAX.*

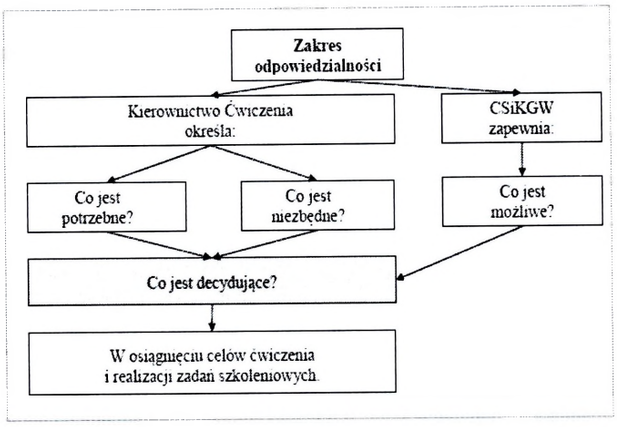
Realizacja tak zarysowanych celów pracy wymagała udzielenia odpowiedzi na następujące pytania badawcze: *w jakich obszarach zadaniowych logistyki wojskowej możliwe jest wykorzystanie systemu symulacyjnego i innych narzędzi do wsparcia CAX? Jaki jest wpływ systemów informatycznych na kierowanie systemem logistycznym w CAX?*

Z uwagi na tak sformułowane problemy badawcze zastosowanie znalazły następujące metody badawcze: **analiza materiałów i dokumentów** operacyjnego i organizacyjnego przygotowania do ćwiczenia pk. Śląsk-14. **Analiza materiałów dydaktycznych** wykorzystanych do szkolenia operatorów stacji roboczych systemu JTLS i aplikacji JEMM w ćwiczeniu na rzecz kierowania systemem logistycznym szczebla operacyjnego.

Wnioskowanie na podstawie wyników symulacji i danych statystycznych z przeprowadzonego ćwiczenia. **Obserwacja uczestnicząca**, ponieważ autor z ramienia CSiKGW w ćwiczeniu pełnił rolę kierownika zespołu koordynacyjnego, wspomagającego w okresie przygotowania ćwiczenia pracę zespołu autorskiego (ZA), a w ćwiczeniu pracę KĆ. W tym czasie posiadał bezpośredni kontakt z wszystkimi szefami zespołów funkcjonalnych KĆ.

Możliwości zabezpieczenia potrzeb Inspektoratu Wsparcia SZ w organizacji ćwiczenia dowódczo-sztabowego wspomaganego komputerowo przez CSiKGW

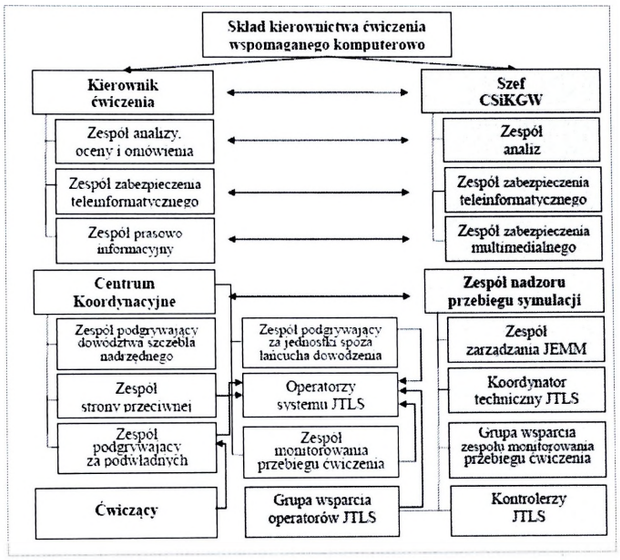
Zadanie pracowników CSiKGW wydzielonych do zespołów funkcjonalnych KĆ polegało na zabezpieczeniu niezbędnych potrzeb KĆ do sprawnego przeprowadzenia ćwiczenia. W szczególności wykorzystania w ćwiczeniu systemu symulacyjnego i innych narzędzi wspomagających proces dowodzenia i kierowania przebiegiem ćwiczenia oraz sprzętu teleinformatycznego i kwaterunkowego. Rolę i zakres odpowiedzialności CSiKGW w formie graficznej przedstawia rysunek 1.



Źródło: opracowanie własne na podstawie wystąpienia szefa CSiKGW na szkoleniu kierownictwa ćwiczenia pk. Śląsk-14, prezentacja ppt [28.11.2014].

Rys. 1. Rola i zakres odpowiedzialności pracowników CSiKGW w osiągnięciu założonych celów ćwiczenia

Ze schematu wynika, że zadaniem CSiKGW jest wsparcie KĆ w zabezpieczeniu jego potrzeb w stopniu zapewniającym osiągnięcie celów ćwiczenia i zrealizowania zadań szkoleniowych. Miejsce zespołów funkcjonalnych CSiKGW wydzielanych do CAX pk. Śląsk-14 zobrazowano na rysunku 2.



Źródło: opracowanie własne na podstawie dokumentacji ćwiczenia Śląsk-14.

Rys. 2. Miejsce zespołów funkcjonalnych CSiKGW w czasie prowadzenia ćwiczenia

Do szczegółowych zadań zespołów funkcjonalnych CSiKGW w czasie prowadzenia CAX, w tym ćwiczenia pk. Śląsk-14 należy:

a) zespół analiz:

– gromadzenie, analiza i synteza informacji będących efektem symulacji,

– gromadzenie i archiwizowanie informacji historycznych oraz prognozowanie zdarzeń przyszłych,

– współpraca z zespołem analizy oceny i omówienia ćwiczenia (ZAOIOĆ) w zakresie uzgodnień dotyczących zakresu, formy i terminu przekazywania informacji;

b) zespół zabezpieczenia teleinformatycznego:

– administrowanie sieciami komputerowymi CSiKGW i monitorowanie ich,

– administrowanie sieciami telefonicznymi CSiKGW i monitorowanie ich;

– współpraca z ZAOiOĆ KĆ wymagająca uzgodnień w zakresie odpowiedzialności osób funkcyjnych i zgłaszania odchyleń symulacji od założonych celów;

c) zespół zabezpieczenia multimedialnego:

– obsługa multimedialna odpraw, usługi audio/foto/video,

– administrowanie systemem wideokonferencji CSiKGW,

– wymaga ustaleń: gdzie, kiedy i co ma być zrobione;

d) zespół zarządzania aplikacją JEMM:

– nadzór nad zgodnością działania systemu podawania wiadomości z przebiegiem symulacji oraz celami i zagadnieniami szkoleniowymi ćwiczenia,

– administracja scenariuszem JEMM,

– administracja techniczna JEMM;

e) grupa wsparcia zespołu monitorowania przebiegu ćwiczenia:

– nadzór nad zgodnością przebiegu symulacji z celami i zagadnieniami szkoleniowymi ćwiczenia,

– koordynacja przebiegu symulacji,

– na polecenie kierownika ćwiczenia ingerowanie w przebieg symulacji;

f) grupa kontrolerów systemu symulacyjnego JTLS:

– monitorowanie stanu symulacji w zakresie odpowiedzialności,

– bieżące korygowanie błędów operatorów;

g) grupa wsparcia operatorów systemu symulacyjnego JTLS:

– merytoryczne wsparcie operatorów systemu JTLS,

– wsparcie zespołów podgrywających w zakresie interpretacji użycia i działania jednostek w systemie JTLS;

h) zespół realnego zabezpieczenia logistycznego ćwiczenia:

– udostępnienie i przekazanie ćwiczącym na czas ćwiczenia bazy lokalowej, kwaterunkowej i technicznej CSiKGW,

– nadzór nad przestrzeganiem wymogów bezpieczeństwa i higieny pracy oraz warunków przeciwpożarowych.

Analiza potrzeb modelowania działań operacyjno-logistycznych i uzupełnieniowych w systemie symulacyjnym JTLS w trakcie ćwiczenia Śląsk-14

Dane wejściowe:

– forma ćwiczenia: ćwiczenie dowódczo-sztabowe wspomagane komputerowo;

– rodzaj ćwiczenia: sprawdzające, militarne, jednoszczeblowe, w obiektach stacjonarnych;

– kierownictwo ćwiczenia: Inspektorat Wsparcia Sił Zbrojnych RP;

– miejsce: CSIKGW oraz obiekty stacjonarne ćwiczących jednostek i instytucji;

– liczba ćwiczących dowództw: główny ćwiczący (4), drugoplanowy (9);

– zagadnienia szkoleniowe stanowiące problematykę operacyjno-logistyczną i administracyjną konieczną do rozwiązania w zakresie modelowania w systemie symulacyjnym:

• zabezpieczenie logistyczne wojsk operacyjnych i sojuszniczych sił wzmocnienia (SSW);

• ewakuacja zagrożonych składów materiałowych;

• ewakuacja techniczna niesprawnego sprzętu wojskowego;

• uzupełnianie personalne wojsk operacyjnych;

• działania ochronno-obronne na obszarze odpowiedzialności Wojewódzkich Sztabów Wojskowych (WSzW);

• użycie sił obrony terytorialnej;

• współdziałanie z pozamilitarnymi ogniwami obronnymi.

Dane wyjściowe:

– konieczność modelowania procesów logistycznych i uzupełnieniowych;

– konieczność wprowadzenia jednostek komponentów: lądowego i powietrznego;

– konieczność modelowania działań sił ochronno-obronnych (bataliony i kompanie ochrony i obrony obiektów) oraz sił obrony terytorialnej (brygady i pułki OT);

– konieczność modelowania instytucji TOAW (WSzW, WKU);

– konieczność modelowania układu pozamilitarnego;

– konieczność modelowania sił przeciwnika;

– konieczność przemieszczenia SSW transportem kołowym i kolejowym (budowa sieci kolejowej).

Potrzeby modelowania procesów logistycznych

Z zawartego w dokumencie normatywnym[1] wykazu podsystemów logistycznych wynika, że model logistyczny w systemach symulacyjnych powinien posiadać możliwości odwzorowania rze-

[1] *Doktryna Logistyczna Sił Zbrojnych Rzeczypospolitej Polskiej*, D-4(B), MON, Bydgoszcz 2014, s. 11.

czywistych procesów logistycznych[2] we wszystkich obszarach funkcjonalnych logistyki wojskowej, w tym:

– **w zakresie kierowania organami i jednostkami logistycznymi**: tworzenie łańcucha logistycznego i jego modyfikacji w trakcie gry, monitorowanie przepływu zasobów logistycznych i kierowanie infrastrukturą logistyczną;

– **w zakresie zabezpieczenia materiałowego**: umieszczenie w bazie danych scenariusza ćwiczenia parametrów środków bojowych i materiałowych (ŚBiM), obiektów logistycznych, składów zaopatrzenia, modelowania zużywania środków zaopatrzenia, monitorowania stanu zapasów zaopatrzenia w jednostkach, modelowania przepływu ŚBiM (zaopatrywania, uzupełniania i odtwarzania zapasów) i ich ewakuacji;

– **w zakresie zabezpieczenia technicznego**: opracowanie w bazie danych parametrów uzbrojenia i sprzętu wojskowego (SpW), modelowania zaopatrywania w SpW oraz technicznych środków materiałowych (TŚM), modelowania strat w SpW (bojowych i niebojowych), monitorowania stanu faktycznego SpW oraz liczby sprzętu do ewakuacji i remontu;

– **w zakresie zabezpieczenia medycznego**: wprowadzenie do bazy danych parametrów stanów osobowych wojskowych i cywilnych, modelowania strat osobowych (bojowych i niebojowych), modelowania ewakuacji i leczenia rannych i chorych oraz zaopatrywania w krew i materiały medyczne;

– **w zakresie zabezpieczenia transportowego**: opracowanie i wprowadzenie danych modelowania przewozu wojsk i środków zaopatrzenia transportem samochodowym, kolejowym, wodnym śródlądowym, powietrznym i morskim, modelowania sieci transportowej drogowej, kolejowej, wodnej śródlądowej i przesyłowej, modelowania urządzeń przeładunkowych w centrach logistycznych, węzłach kolejowych, w portach morskich i lotniczych oraz urządzeń przesyłowych sieci rurociągowej.

Wyniki badań

Zdefiniowane powyżej potrzeby w zakresie modelowania procesów logistycznych i uzupełnieniowych w systemie symulacyjnym i innych aplikacjach posiadanych przez CSiKGW wymagały jednoczesnego przygotowania operatorów stacji roboczych JTLS, operatorów do wprowadzania danych i obsługi aplikacji JEMM oraz przeszkolenia użytkowników aplikacji iGeoSIT. Łączne potrzeby w zakresie przeszkolenia osób funkcyjnych KĆ do obsługi narzędzi informatycznych przedstawiono w tabeli 1.

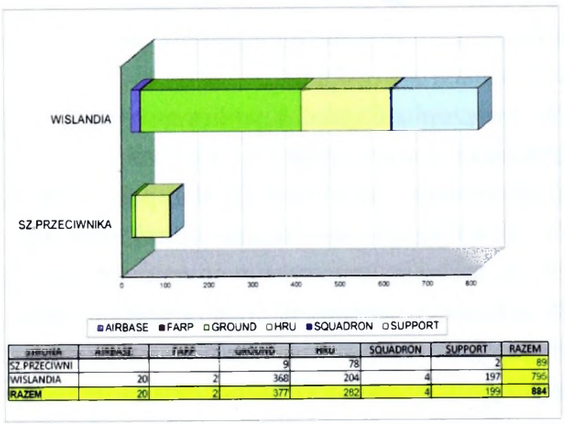
Tabela 1

Wykaz żołnierzy przeszkolonych do obsługi narzędzi informatycznych w ćwiczeniu

Nazwa szkolenia	Liczba poszkodowanych żołniezy	Liczba obsadzony stacji roboczych
Kurs operatorów stacji roboczej JTLS	64	32
Kurs operatorów aplikacji JEMN	39	39
Kurs użytkowników aplikacji iGeoSIT	20	15

Opracowanie własne.

Jednocześnie wysiłek pracowników CSiKGW skupiony był na wprowadzeniu do bazy danych systemu JTLS setek tysięcy danych do modelowania prawie 900 jednostek wojsk własnych i przeciwnika oraz prawie 13 000 obiektów infrastruktury, występujących w scenariuszu ćwiczenia. Szczegółowe dane z podziałem na rodzaje jednostek i klasy obiektów zobrazowano na rysunku 3 i 4.

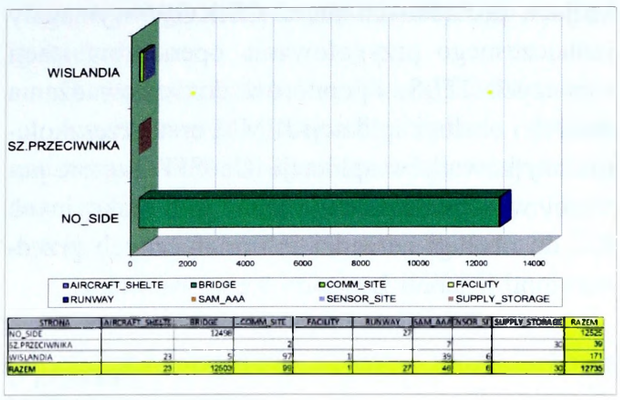


STRONA	AIRBASE	FARP	GROUND	HRU	SQUADRON	SUPPORT	RAZEM
SZ.PRZECIWNI			9	78		2	89
WISLANDIA	20	2	368	204	4	197	795
RAZEM	20	2	377	282	4	199	884

Źródło: R. Kaniewski, Zespół Analiz CSiKGW.

Rys. 3. Wykaz jednostek wprowadzonych do bazy danych scenariusza

[2] **Proces logistyczny** rozumiany jako „... uporządkowany łańcuch operacji związany z przepływem materiałów", K. Ficoń, *Logistyka ekonomiczna. Procesy logistyczne,* BEL Studio, Warszawa 2008, s. 152.



STRONA	AIRCRAFT_SHELTE	BRIDGE	COMM_SITE	FACILITY	RUNWAY	SAM_AAA	SENSOR_SITE	SUPPLY_STORAGE	RAZEM
NO_SIDE		12498			27				12525
SZ.PRZECIWNIKA			2			3		30	39
WISLANDIA	23	5	97	1		35	6		171
RAZEM	23	12503	99	1	27	46	6	30	12735

Źródło: R. Kaniewski, wyd. cyt.

Rys. 4. Wykaz obiektów infrastruktury wprowadzonych do bazy danych scenariusza

Analiza możliwości modelowania działań operacyjno-logistycznych i administracji wojskowej szczebla operacyjnego w systemie symulacyjnym JTLS

Według ekspertów wojskowych za najbardziej efektywne narzędzia w procesie szkolenia dowództw i sztabów uznawane są systemy symulacji komputerowej pola walki. Symulacja komputerowa traktowana jest jako forma ćwiczeń, w której ćwiczący podejmują decyzje i mogą na podstawie otrzymanych meldunków i informacji obserwować ich skutki, a błędne decyzje nie wywołują realnych konsekwencji, dlatego mają szczególną wartość szkoleniową. Nie bez znaczenia jest także możliwość wielokrotnego rozegrania tych samych sytuacji, co ze względu na brak czasu na takie działanie i zbyt duże koszty jest mało realne w ćwiczeniach z wojskami.

W ćwiczeniu Śląsk-14 wykorzystywany był amerykański system symulacyjny, przeznaczony do modelowania i symulacji działań połączonych JTLS (*Joint Theater Level Simuolation*), wykorzystujący symulację konstruktywną w ćwiczeniach CAX. Z analizy dokumentacji producenta i przeprowadzonych testów i ćwiczeń wynika, że moduł logistyczny w systemie JTLS posiada możliwości imitowania procesów logistycznych we wszystkich obszarach funkcjonalnych podsystemów logistycznych, w tym:

- kierowania organami i jednostkami logistycznymi;
- zabezpieczenia materiałowego (m.in. modelowanie zaopatrywania, uzupełniania i odtwarzania zapasów zaopatrzenia);
- zabezpieczenia technicznego (m.in. modelowanie strat UiSW bojowych i niebojowych, wykonywania remontów UiSW);
- zabezpieczenia medycznego (modelowanie strat osobowych, leczenia chorych i rannych);
- zabezpieczenia transportowego (m.in. modelowanie konwojów zaopatrzeniowych, transportu powietrznego, morskiego, kolejowego, kołowego, wodnego śródlądowego i rurociągami);
- sterowania przepływami zapasów środków zaopatrzenia materiałowego:
  - automatyczne (przez system);
  - ręczne (zgodnie z decyzją ćwiczących i złożonym zapotrzebowaniem).

Zastosowane w systemie JTLS rozwiązania umożliwiają realizację procesów logistycznych w sposób automatyczny, ręczny lub mieszany. Oznacza to, że system JTLS, w zależności od celów ćwiczenia, umożliwia ZA podjęcie decyzji dotyczącej wyboru sposobu sterowania przepływem zasobów logistycznych. W większości ćwiczeń prowadzonych w CSiKGW realizacja odbywa się sposobem mieszanym. Ręcznie dla jednostek podległych ćwiczącym dowództwom, automatycznie dla niećwiczących jednostek występujących w strukturze organizacyjnej ćwiczenia, wliczając w to wojska własne i siły przeciwnika.

Analiza możliwości wykorzystania aplikacji JEMM w procesie kierowania systemem logistycznym w ćwiczeniu Śląsk

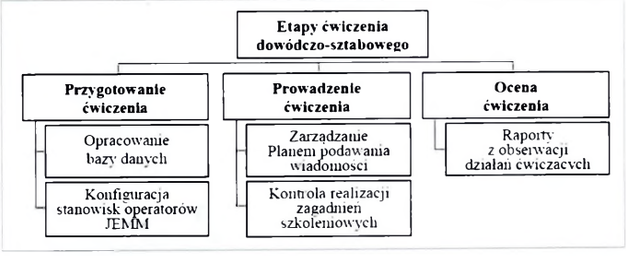
Moduł wspomagający zarządzanie ćwiczeniem JEMM (*Joint Exercise Management Module*) jest narzędziem zaprojektowanym przez agencję NC3A do wsparcia prowadzenia ćwiczenia dowódczo-sztabowego, w tym CAX. Narzędzie zostało zaprojektowane na aplikacji strony internetowej (*Web Site*), umożliwiając kierownictwu ćwiczenia wpływanie na przebieg ćwiczenia poprzez wprowadzanie epizodów dla ćwiczących, zgodnie z założeniami i zagadnieniami szkoleniowymi. Narzędzie umożliwia ponadto kontrolę ćwiczących poprzez śledzenie ich reakcji na zaistniałe zdarzenia.

Z opisu zawartego w dokumentacji systemowej wynika, że aplikacja zapewnia[3]:

[3] M. Sołoducha, *Wykorzystanie modułu JEMM w ćwiczeniu pk. ŚLĄSK-14*, materiał szkoleniowy do szkolenia kierownictwa ćwiczenia, Archiwum elektroniczne CSiKGW, Warszawa 2014, prezentacja ppt.

– dostęp do dokumentacji ćwiczenia;
– zobrazowanie przebiegu scenariusza ćwiczenia;
– możliwość bieżącej interakcji przygotowanymi lub opracowywanymi incydentami;
– rozmównicę pomiędzy użytkownikami JEMM;
– możliwości tworzenia i kontroli zapotrzebowań na informację oraz jej wsparcie;
– możliwość monitoringu poprawności działania ćwiczącego organu dowodzenia poprzez obserwatorów wydzielanych z ZAOiOĆ i zespołu zgrywania systemów walki (ZZSW);
– dostarczanie meldunków z kontroli realizacji zadań ćwiczącego dowództwa;
– synchronizację incydentów z symulacją;
– zobrazowanie miejsc zaplanowanych incydentów na mapie.

Aplikacja JEMM jest wykorzystywana we wszystkich etapach ćwiczenia. Zakres realizowanych zadań w poszczególnych etapach został zaprezentowany na rysunku 5.

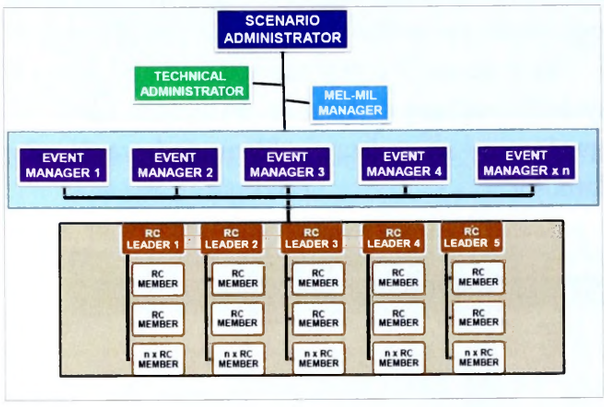


Źródło: opracowanie własne na podstawie dokumentacji z ćwiczenia Śląsk-14.

Rys. 5. Zakres realizowanych zadań operacyjno-logistycznych w poszczególnych etapach ćwiczenia

Z przeprowadzonych badań wynika, że miejsca pracy operatorów JEMM należy rozmieszczać we wszystkich komórkach funkcjonalnych KĆ, w tym zespole analizy, oceny i omówienia ćwiczenia (ZAOiOĆ), zespole monitorowania przebiegu ćwiczenia (ZMPĆ), zespole podawania wiadomości (ZPW – MEL/MIL) oraz zespołach podgrywających: dowództwo szczebla nadrzędnego i sąsiadów (HICON, SITFOR); podwładnych ćwiczącego szczebla (LOCON); stronę przeciwną (OPFOR); za jednostki i instytucje spoza struktury dowodzenia (WHITE CELL).

Do każdego scenariusza ćwiczenia należy przygotować strukturę organizacyjną zarządzającą aplikacją JEMM, składającą się z wielu osób funkcyjnych. Przykładową strukturę obsady etatowej na potrzeby zastosowania aplikacji przedstawiono na rysunku 6.



Źródło: M. Sołoducha, *Wykorzystanie modułu JEMM w ćwiczeniu pk. Śląsk-14*, CSiKGW, Warszawa 2014, prezentacja ppt.

Rys. 6. Obsada stanowisk JEMM we wsparciu kierowania systemem logistycznym w ćwiczeniu Śląsk-14

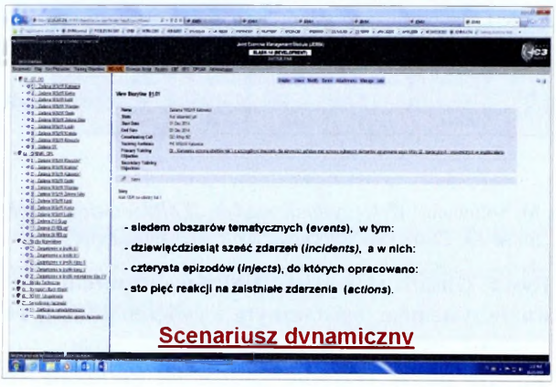
Łącznie pełna obsada stanowisk związanych z zarządzaniem ćwiczeniem z wykorzystaniem aplikacji JEMM, w zależności od rozmachu ćwiczenia, w tym szczególnie liczby sprawdzanych obszarów zadaniowych (*Event Manager*), liczby zespołów podgrywających (*RC Lider*) oraz liczby członków zespołu podgrywającego (*RC Member*) oraz liczby wysyłanych obserwatorów (*OT Observer*) przy ćwiczących SD i PK, może wynosić nawet do kilkudziesięciu żołnierzy na zmianę (np. CAX Anakonda-14). W ćwiczeniu pk. Śląsk-14 zostało przeszkolonych 39 użytkowników aplikacji JEMM, którzy następnie obsadzili taką samą liczbę stacji roboczych z zainstalowaną aplikacją JEMM.

Z przedstawionego powyżej schematu wynika, że za koordynację wprowadzania zdarzeń logistycznych i operacyjnych odpowiada szef ZPW, a za wprowadzanie zdarzeń odpowiadają prowadzący zdarzenia operacyjno-logistyczne. Natomiast wyniki symulacji podejmowanych działań logistycznych na podstawie wprowadzonych do systemu JTLS incydentów logistycznych mają charakter losowy. Ich wyniki przesyłane są na SD/PK ćwiczących dowództw logistycznych i instytucji administracji wojskowej telefonicznie, drogą mailową lub faxem.

W czasie trwania CAX wykorzystywana jest opracowana w okresie przygotowania ćwiczenia baza danych operacyjno-logistycznych, zawierająca wykaz obszarów tematycznych (*events*), podzielonych na grupy zdarzeń – epizodów (*in-*

cidents) logistycznych, które z kolei zawierają informacje dotyczące epizodów w ramach danego incydentu (*inject*). Końcowym elementem jest określenie sposobu realizacji każdego incydentu logistycznego (*action*) w systemie symulacyjnym.

Na rysunku 7 został zaprezentowany faktyczny folder z bazą danych do ćwiczenia Śląsk-14, opracowany na podstawie Planu podawania wiadomości.



Rys. 7. Baza danych operacyjno-logistycznych aplikacji JEMM do ćwiczenia Śląsk-14

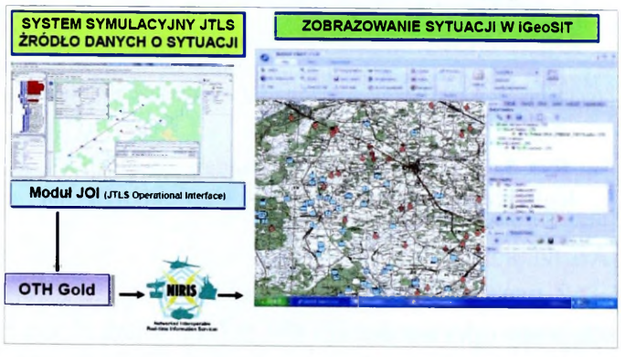
Z analizy zawartości bazy danych wynika, że na potrzeby ćwiczenia utworzono siedem działów tematycznych, zawierających dziewięćdziesiąt sześć zdarzeń z czterystoma epizodami, do których zaplanowano sto pięć reakcji na przygotowane w systemie JTLS zdarzenia. Za pozytyw należy uznać, że aplikacja JEMM jest na tyle elastyczna, iż umożliwia dokonywanie zmian w opracowanych zdarzeniach scenariusza, jak również wprowadzanie nowych zdarzeń i planowanych reakcji ćwiczących SD i PK na te zdarzenia. Z przeprowadzonych badań wynika, że w trakcie ćwiczenia do scenariusza dodatkowo wprowadzono dwanaście obszarów tematycznych, związanych z obowiązującym w CAX systemem meldunkowym.

Analiza możliwości modułu zobrazowania przestrzennego iGeoSIT procesie kierowania systemem logistycznym w ćwiczeniu Śląsk

Aplikacja iGeoSIT (*the Interim Geo-Spatial Intelligence Tool*) jest narzędziem integrującym w czasie rzeczywistym różne typy informacji geoprzestrzennych i operacyjnych, bazujących na wspólnych podkładach mapowych, umożliwiających zobrazowanie tych informacji w postaci połączonego obrazu sytuacji operacyjnej. Aplikacja jest produktem Agencji NATO ds. Łączności i Informatyki NCIA (*NATO Communications and Information Agency*). Dostęp do aplikacji użytkownik zapewnia sobie poprzez wpisanie adresu serwera iGeoSIT w oknie Internet Explorer i przycisk uruchamiania aplikacji.

Możliwości aplikacji[4]: zobrazowanie połączonego obrazu sytuacji operacyjnej, aktualizacja położenia podległych pododdziałów i instytucji wojskowych, wyświetlanie informacji o jednostkach, tworzenie warstw przez użytkownika z informacjami geoprzestrzennymi i operacyjnymi, generowanie meldunków sytuacyjnych.

W ćwiczeniu Śląsk-14 aplikacja iGeoSIT w wersji 2.1.0 wykorzystana była do stworzenia połączonego obrazu sytuacji operacyjno-logistycznej na SD i PK jednostek bezpośrednio podległych szefowi IWsp SZ, rozmieszczonych w trzynastu lokalizacjach na terenie Południowej Polski. Zadanie to realizowane było poprzez bieżące, automatyczne przesyłanie informacji logistycznej z systemu symulacyjnego JTLS, użytkowanego w CSiKGW do aplikacji iGeoSIT zainstalowanej na SD i PK w MSD ćwiczących dowództw i sztabów. Współpraca systemu JTLS z aplikacją iGeoSIT została zobrazowana na rysunku 8.



Źródło: W. Biało, wyd. cyt.

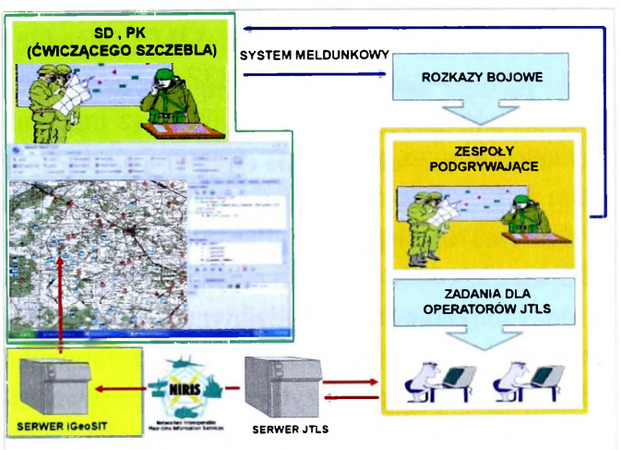
Rys. 8. Schemat współpracy aplikacji IGeoSIT z systemem symulacyjnym JTLS

Z opracowanego na potrzeby ćwiczenia założenia i prowadzonych w trakcie ćwiczenia obserwacji wynika, że źródłem danych o sytuacji logistycznej był system symulacyjny działań

[4] W. Biało, *Rola i zakres wykorzystania aplikacji iGeoSIT w ćwiczeniu pk. ŚLĄSK-14*. Materiał szkoleniowy do szkolenia kierownictwa ćwiczenia, Archiwum elektroniczne CSiKGW, Warszawa 2014, prezentacja ppt.

połączonych JTLS. Na podstawie zaimplementowanego w JTLS Modułu JOI (JTLS *Operational Interface*) poprzez protokół OTH Gold[5] (*Over the Horizon Gold*) uzyskane z systemu JTLS informacje logistyczne były przekazywane przez system NIRIS (*Networked Interoperable Real-time Information Services*) do aplikacji iGeoSIT. System NIRIS jako system integrujący i konwertujący różne protokoły transmisji danych, umożliwił użytkownikom dostęp do informacji logistycznej i położeniu z różnych systemów i aplikacji w czasie rzeczywistym.

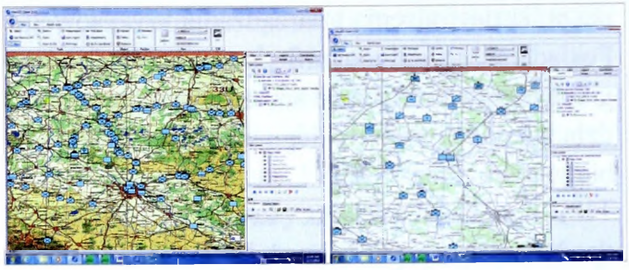
Na rysunku 9 została zobrazowana procedura przepływu informacji logistycznej pomiędzy system JTLS i aplikacją iGeoSIT.



Źródło: W. Biało, wyd. cyt.

Rys. 9. Schemat wykorzystania aplikacji iGeoSIT w ćwiczeniu Śląsk-14

Praktyczna realizacja opisanych powyżej rozwiązań w ćwiczeniu Śląsk-14 została odzwierciedlona na rysunku 10. w postaci zobrazowania sytuacji operacyjnej jednostek i instytucji podległych ćwiczącym SD i PK. Z wywiadów przeprowadzonych z uczestnikami ćwiczenia wynika, że dzięki zastosowaniu aplikacji iGeoSIT ćwiczące SD i PK w czasie ćwiczenia posiadały bieżące zobrazowanie w czasie rzeczywistym sytuacji operacyjnej, w tym logistycznej w swoim obszarze odpowiedzialności.



Źródło: zrzuty zobrazowania z aplikacji iGeoSIT, CAX ŚLĄSK-14, CSiKGW, Warszawa 2014.

Rys. 10. Przykład zobrazowania położenia jednostek logistycznych i instytucji administracji wojskowej w aplikacji iGeoSIT

Reasumując, dotychczasowe rozwiązania obowiązujące w ćwiczeniach CAX prowadzonych w poprzednich latach nie zakładały posiadania zobrazowania sytuacji operacyjno-logistycznej na SD i PK. Jedyną wiedzę o położeniu podwładnych ćwiczący uzyskiwali w formie meldunków logistycznych i sytuacyjnych od podwładnych. Mankament związany z brakiem zobrazowania stanowił jedną z bolączek artykułowanych przez ćwiczące SD i PK. Implementacja aplikacji iGeoSIT w ćwiczeniu Śląsk-14 stanowi duży postęp w zapewnieniu ćwiczącym bieżącej informacji o położeniu podległych poddziałów logistycznych i instytucji administracji wojskowej.

Analiza możliwości zastosowania Pakietu Grafiki Operacyjnej PGO w procesie kierowania systemem logistycznym w ćwiczeniu Śląsk-14

Pakiet Grafiki Operacyjnej (PGO) jest programem informatycznym przeznaczonym do zobrazowania sytuacji operacyjno-taktycznej na podkładzie map numerycznych (zdjęć lotniczych i satelitarnych) oraz do przeprowadzenia operacyjnej oceny terenu. Ponadto stanowi platformę bazową dla specjalistycznych systemów informatycznych, opracowywanych w CIiŁON (Centrum Informatyki i Łączności Obrony Narodowej)[6], wykorzystujących elementy zobrazowania graficznego na podkładzie map i zdjęć cyfrowych, jako moduł w innych użytkowanych systemach informatycznych. Między innymi służy do zobrazowania geoprzestrzennego systemów wspo-

[5] JTLS posiada możliwość współpracy z innymi wojskowymi systemami teleinformatycznymi poprzez protokoły: Link-16, AdatP-3 i również protokół OTH Gold. Zob.: P. Boryn, *Rozproszone ćwiczenia CAX jako nowoczesna forma szkolenia dowództw i sztabów*, dostępny: http://www.csikgw.aon.edu.pl/.

[6] Od 01.04.2011 roku zmiana nazwy CIiŁON na RCZPI (Resortowe Centrum Zarządzania Projektami Informatycznymi).

magania dowodzenia i zarządzania kryzysowego. Posiadany zasięg geograficznego działania oprogramowania praktycznie umożliwia zobrazowanie działania na obszarze całego świata, za wyjątkiem biegunów[7].

Program umożliwia: kreślenie umownych symboli graficznych z wykorzystaniem znaków wojskowych, zgodnych ze standardami NATO oraz układu pozamilitarnego; wyszukiwanie obiektów geograficznych i wyświetlanie granic administracyjnych; operowanie zdjęciami satelitarnymi, lotniczymi itp.; prowadzenie analiz przestrzennych i kartograficznych oraz oceny terenu; plotowanie i drukowanie sytuacji graficznych na mapach w różnych skalach[8].

Zastosowanie PGO w ćwiczeniu Śląsk-14 wymagało rozwiązania wielu ograniczeń. Wprawdzie oprogramowanie PGO nie zawiera wewnątrz informacji, które mogłyby stanowić tajemnicę służbową lub państwową, to jednak wymaga, aby wytwarzane zestawienia posiadały klauzulę tajności nie większą niż informacje w bazie danych systemu symulacyjnego. W związku z tym należało poddać dokumenty i pliki zawierające wytworzone zestawienia rygorowi rejestracji, przede wszystkim zapisy plików na nośnikach wymiennych oraz przesyłki poczty elektronicznej zawierające treść zestawień. Dostęp do wydruków i nośników należało ograniczyć zgodnie z zasadami ochrony informacji niejawnych w wojsku.

W zasadzie PGO jest przygotowany do użytkowania na pojedynczym komputerze. Konieczność wykorzystania większej liczby komputerów roboczych w ćwiczeniu Śląsk-14, połączonych ze sobą przy użyciu lokalnej sieci komputerowej na każdy z nich, wymagała zainstalowania oddzielnego pełnego pakietu oprogramowania.

Ponadto w PGO możliwe jest jedynie współużytkowanie w sieci danych geograficznych, co oznacza, że każdy użytkownik PGO steruje jego pracą przy użyciu interfejsu graficznego. Interfejs posiada wiele okien i pasków. Spośród wszystkich dostępnych narzędzi graficznych niewątpliwie centralną rolę odgrywa **Okno Map**. To właśnie w nim użytkownik obserwuje wyniki działań na mapach, które z reguły zajmują największą powierzchnię ekranu monitora. Wszystkie pozostałe okna spełniają role pomocnicze. Jego graficzną cechą charakterystyczną jest występowanie suwaków w dolnej i prawej krawędzi, służących do przesuwu obrazu. Szczególnie bogate formy kształtu kursor przyjmuje wewnątrz **Okna Map**. Przykładowy obraz okna mapy PGO przedstawia rysunek 11.

Źródło: *Instrukcja obsługi Pakietu Grafiki Operacyjnej*, MON, Warszawa 2006, s. 9.

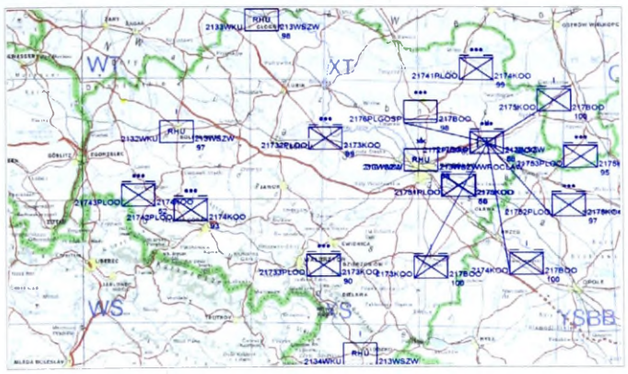
Rys. 11. Przykład wyglądu Okna Mapy PGO

Kolejne ograniczenie odnosi się do tego, że PGO nie zapewnia żadnych mechanizmów ochrony danych. Dane jawne i niejawne traktowane są w sposób identyczny. Wobec tego do użytkownika należy zapewnienie należytej ochrony przetwarzanym informacjom niejawnym. W związku z tym system powinien być użytkowany zgodnie z odpowiednimi normami, przez odpowiednio wyszkolony i zweryfikowany personel. Ponieważ dane o sytuacji zapisywane są w nieszyfrowanym pliku roboczym programu, to zapewnienie integralności i poufności danych leży po stronie użytkownika lub kanału transmisyjnego (w przypadku przekazywania pliku z zapisaną sytuacją, wydruku na drukarkę sieciową itp.).

Praktycznie w ćwiczeniu Śląsk-14 za pomocą aplikacji PGO Centrum zapewniało ćwiczącym dowództwom i sztabom, m.in. przygotowanie zobrazowania położenia podległych pododdziałów i instytucji, które zgodnie z systemem meldunkowym i obiegiem informacji w ćwiczeniu, w określonych terminach przesyłało do zespołów podgrywających podwładnych ćwiczącego szczebla (GO LOCON). Rysunek 12. ilustruje przykład odwzorowania sytuacji taktycznej z systemu JTLS w PGO.

[7] *Instrukcja Obsługi Pakietu Grafiki Operacyjnej*, MON, Warszawa 2006, s. 6–8.

[8] Dostęp: http://www.rcpi.wp.mil.pl/.



Rys. 12. Zobrazowanie położenia jednostek logistycznych i administracji wojskowej podległych WSzW Wrocław z systemu JTLS w aplikacji PGO

Grupy operacyjne po otrzymaniu wygenerowanego zobrazowania z systemu JTLS, poprzez aplikację JEMM, przesyłały je dwa razy na dobę do ćwiczących SD i PK (wraz opracowanymi meldunkami sytuacyjnym i logistycznym). Dla ćwiczących informacje zawarte z wygenerowanym w PGO położeniem podległych jednostek i instytucji stanowiły uzupełnienie i potwierdzenie z innego źródła informacji uzyskanych od podwładnych w formie meldunków sytuacyjnych.

Podsumowanie

Wpływ zastosowania systemów informatycznych na kierowanie systemem logistycznym w ćwiczeniu Śląsk-14

Prowadzone w czasie CAX pk. Śląsk-14 badania wykazały, że eksploatacja posiadanych narzędzi informatycznych, wspomagających kierowanie systemem logistycznym w ćwiczeniu, stanowi ogromne ułatwienie pracy KĆ, które poprzez zarządzanie obiegiem informacji i kierowanie przebiegiem ćwiczenia posiadało pełny wgląd w rozwój sytuacji operacyjno-logistycznej, w tym możliwość oceny ćwiczących dowództw i sztabów.

Praca KĆ, ćwiczących dowództw i sztabów, jak również zespołów podgrywających za niećwiczące pododdziały w CAX, w dużej mierze polega na gromadzeniu i przetwarzaniu różnych informacji, co sprawia, że wspomaganie informatyczne staje się niezwykle pożytecznym narzędziem w rękach KĆ. W przypadku ćwiczenia pk. Śląsk-14 odpowiednio dobrane i wdrożone do scenariusza ćwiczenia narzędzia informatyczne pozwoliły zaoszczędzić KĆ wiele czasu i przeznaczyć go na kierowanie systemem logistycznym.

W kierowaniu ćwiczeniem, oprócz wykorzystania systemu symulacyjnego, KĆ może również zaoszczędzić czas, wykorzystując inne narzędzia elektroniczne służące do wspomagania procesu kierowania systemem logistycznym ćwiczenia. Do narzędzi tych należy zaliczyć JEMM, iGeoSIT i PGO. Na przykład prowadzenie w ćwiczeniach papierowej (pisanej) wersji Planu podawania wiadomości i przekazywanie ich środkami łączności lub nawet drogą mailową nie zapewnia automatycznej rejestracji korespondencji dokumentów. Natomiast moduł zarządzania informacją JEMM stworzył możliwości pełnej kontroli nad przepływem informacji logistycznych pomiędzy poszczególnymi komórkami KĆ a ćwiczącymi SD i PK.

Poprzez wykorzystanie narzędzi teleinformatycznych następuje wzrost efektywności pracy, ponieważ jeden żołnierz, uczestnik ćwiczenia jest w stanie zrealizować większą liczbę zadań. Ocenia się, że zastosowanie różnego rodzaju nowych technologii z pewnością zwiększa zaangażowanie, szczególnie młodej kadry przyzwyczajonej do korzystania z dobrodziejstw współczesnej techniki. Z przeprowadzonych z uczestnikami ćwiczenia badań (obserwacji, wywiadów i rozmów) wynika, że występuje wzrost zaangażowania w ćwiczeniach, wyróżniających się nowatorskimi rozwiązaniami. W celu poprawy zadowolenia osób funkcyjnych KĆ, ćwiczących SD i PK jednostek i instytucji bezpośrednio podległych szefowi IWsp SZ zbadano, które z zastosowanych narzędzi spełnia wymogi użytkowników, a w których niezbędne jest doskonalenie ich funkcjonalności.

Należy pamiętać, że nie ma idealnego systemu symulacyjnego do modelowania wszystkich typów jednostek występujących poszczególnych rodzajach Sił Zbrojnych i rodzajach wojsk i służb. W przypadku jednostek podległych IWsp SZ dotyczy to szczególnie WSzW, WKU, krr, WKTR oraz TOAW. Administracja wojskowa posiada swoją specyfikę i wymaga określonych właściwości systemu informatycznego. System informatyczny, który jest idealny do modelowania działań militarnych prowadzonych przez wojska operacyjne, na pewno nie jest tak pożyteczny dla TOAW. Dlatego też ZA, w tym szczególnie pracownicy CSiKGW (specjaliści logistyki) skupili się na opracowaniu rozwiązań umożliwiających poprawę funkcjonalności modułu logistycznego w systemie JTLS.

Wnioski i rekomendacje

Wniosek 1. Struktura kierownictwa ćwiczenia ze względu na swoją złożoność i ogrom zadań stojących przed jej komórkami funkcjonalnymi wymaga doskonałej organizacji pracy.

Rekomendacja 1. Aby sprostać takim wyzwaniom, jak kierowanie i dowodzenie dużą liczbą jednostek logistycznych, uzupełnieniowych i instytucji bezpośrednio podporządkowanych IWsp SZ i jednocześnie wykonywać swoją pracę w sposób racjonalny, niezbędne jest odpowiednie wspomaganie komputerowe.

Wniosek 2. Decydując się na wykorzystanie jakiegokolwiek systemu informatycznego, KĆ powinno liczyć się z wieloma wymaganiami, które trzeba spełnić, aby ćwiczenie mogło przebiegać sprawnie. Najważniejsze to konieczność przeszkolenia odpowiedniej liczby osób – operatorów systemów i aplikacji zastosowanych w ćwiczeniu. W przypadku systemu JTLS było to 64 operatorów, natomiast przygotowanie PPW, wprowadzenie do systemu JEMM, a następnie jego obsługa w trakcie ćwiczenia, to zaangażowanie w różnych etapach następnych od kilkunastu do kilkudziesięciu osób. Obsługa aplikacji iGeoSIT to kolejne 15 osób personelu, który należało przygotować zarówno do obsługi aplikacji (użytkownicy), jak i do zarządzania aplikacją (administrator techniczny).

Rekomendacja 2. W tej sytuacji szczególnego znaczenia nabiera system szkolenia wszystkich osób funkcyjnych KĆ, a szczególnie operatorów systemu symulacyjnego JTLS i aplikacji JEMM we wparciu KĆ w kierowaniu systemem logistycznym.

Wniosek 3. CSiKGW, posiadając zintegrowany system symulacyjny działań połączonych JTLS, zapewnia warunki do takiego przygotowania i prowadzenia ćwiczenia, w których wprowadzanie danych do systemu odbywa się tylko raz, a informacje te są dostępne dla wszystkich uczestników ćwiczenia. Takie rozwiązanie zapewnia oszczędność czasu, poprawia efektywność a także ogranicza ryzyko pomyłki przy wprowadzaniu danych.

Rekomendacja 3. Należy z odpowiednim wyprzedzeniem powoływać zespół autorski w składzie którego powinni być oficerowie z największym doświadczeniem i wiedzą operacyjno-logistyczną.

Wniosek 4. Właściwe wykorzystanie możliwości dzisiejszej techniki pozwala KĆ na bardziej efektywną pracę w kierowaniu systemem logistycznym. Dzięki zintegrowanym systemom informatycznym wiele programów może współpracować ze sobą, stanowiąc nieocenioną pomoc dla KĆ.

Rekomendacja 4. Implementacja w CSiKGW zintegrowanych systemów symulacyjnych i innych narzędzi wspomagających proces kierowania systemem logistycznym, niweluje wiele niezgodności i pomyłek, a poprzez to zdecydowanie podnosi jakość świadczonych usług.

Wniosek 5. Kluczową dla KĆ korzyścią w kierowaniu systemem logistycznym jest możliwość ograniczenia liczby żołnierzy zaangażowanych w ćwiczenie wspomagane komputerowo.

Rekomendacja 5. Wobec powyższego, do sprawnego i efektywnego zarządzania i kierowania systemem logistycznym wćwiczeniu niezbędne jest zastosowanie takich rozwiązań informatycznych, które przy zaangażowaniu mniejszej liczby osób zapewnią wysokie standardy. Chodzi głównie o zagwarantowanie kierownictwu ćwiczenia dostępu do aktualnych informacji o jednostkach (pododdziałach) logistycznych, uzupełnieniowych i jednostkach administracji wojskowej wprowadzonych do systemu, zapewnienie pełnej kontroli nad stanami osobowymi, sprzętem bojowym i zapasami, a także bieżącego monitorowania przebiegu ćwiczenia.

Reasumując, zastosowane w ćwiczeniu nowoczesne narzędzia informatyczne to najbardziej merytorycznie i technologicznie zaawansowana klasa systemów wspomagających procesy dowodzenia podległymi jednostkami logistycznymi oraz kierowania dowództwami i sztabami na stanowiskach dowodzenia i punktach kierowania instytucjami podległymi IWsp SZ. Nowoczesne rozwiązania informatyczne znacznie ułatwiają pracę KĆ i niosą ze sobą wiele innych korzyści. Między innymi pozwalają na optymalizację realizowanych procesów kierowania systemem logistycznym poprzez oferowanie gotowych narzędzi, służących do automatyzacji wymiany danych pomiędzy komórkami wewnętrznymi KĆ oraz pomiędzy KĆ a ćwiczącymi dowództwami.

Z punktu widzenia KĆ kierującego systemem logistycznym SZ RP, w zakresie zarządzania przepływem informacji w ćwiczeniu, system informatyczny okazuje się bardzo dobrym sposobem, z jednej strony na ograniczenie kosztów ćwiczenia (mniejsza liczba uczestników ćwiczenia), a z drugiej na sprawne i skuteczne zarządzanie informacjami operacyjno-logistycznymi. Zalety

wspomagania komputerowego w ćwiczeniu kierowania systemem logistycznym można by mnożyć w nieskończoność, należy jednak pamiętać również o ryzyku i zagrożeniach, jakie ono ze sobą niesie. Przede wszystkim należy mieć na uwadze to, że żaden system nie zastąpi dobrze wykwalifikowanej kadry logistycznej, a narzędzia informatyczne są jedynie uzupełnieniem, a nie alternatywą dla ludzi kierujących systemem logistycznym.

Bibliografia

Biało W., *Rola i zakres wykorzystania aplikacji iGeoSIT w ćwiczeniu pk. Śląsk-14*, CSiKGW, Warszawa 2014, prezentacja ppt.

Boryn P., *Rozproszone ćwiczenia CAX jako nowoczesna forma szkolenia dowództw i sztabów*, www.csikgw.aon.edu.pl.

Doktryna logistyczna Sił Zbrojnych Rzeczypospolitej Polskiej D-4(B), MON, Bydgoszcz 2014.

Dokumentacja systemowa JTLS, JEMM, iGeoSIT, PGO.

Ficoń K., *Logistyka ekonomiczna. Procesy logistyczne*, BEL Studio, Warszawa 2008.

Instrukcja obsługi Pakietu Grafiki Operacyjnej, MON, Warszawa 2006.

Instrukcja o przygotowaniu i prowadzeniu ćwiczeń z dowództwami, sztabami i wojskami w Siłach Zbrojnych RP DD/7.1.1 (A). MON, Warszawa 2010.

Knetki J., *Centrum Symulacji i Komputerowych Gier Wojennych*", „PWL", nr 2/2005.

Koncepcja przygotowania i przeprowadzenia ćwiczenia dowódczo-sztabowego wspomaganego komputerowo pk. Śląsk-14, Inspektorat Wsparcia Sił Zbrojnych, Bydgoszcz 2013.

Organizacja szkolenia dowództw i sztabów w Siłach Zbrojnych RP, MON, DD/7.1(A), Warszawa 2010.

Sołoducha M., *Wykorzystanie modułu JEMM w ćwiczeniu pk. Śląsk-14*. CSiKGW, Warszawa 2014, prezentacja ppt.

http://www.rcpi.wp.mil.pl/.

USE OF MODERN INFORMATION TOOLS IN THE CONTROL OF THE LOGISTICS SYSTEM IN COMPUTER ASSISTED EXERCISES USING THE EXAMPLE OF EXERCISE SILESIA-14

Abstract

In the twenty-first century, information flows have become necessary to ensure the efficient and effective management of military organisations, which is required for support in the form of modern information tools. The military organisation requires rapid data collection, processing and analysis to manage them, not only within the organisational structure, but also to derive information from subordinates. The above mentioned factors have become an indispensable part of the functioning of the Computer Assisted Exercises (CAX's).

This article covers the role of full information exercises and which systems and technology are the most commonly used exercises conducted at the War Game & Simulation Center (WG&SC). Some of the research has been characterised with modern tools in the form of a simulation system and other applications that support management and a verification exercise of their usefulness in training commands and staffs using the example of the exercise organised by the Inspectorate for Polish Armed Forces Support, under the codename Silesia-14.

Key word: logistic, system, informatical tools

Introduction

In the opinion of specialists, one of the most effective forms of training commands and staffs is *Command Post Exercises* (CAX's), called *Computer Assisted Exercises* (CAX's), in which the scenario developed based on exercise, used computer simulation systems, replaces the practical effect of the use of troops. Of key importance is an efficient information system that allows every element of the military organisation to be virtually controlled. Therefore, effective and well thought out information tools to help manage military organisations, whose activities take place without access to computer systems would be much more difficult.

Information tools used in the exercise codenamed Silesia-14, organised by the *Inspectorate for Polish Armed Forces Support*, were studied, whose main task is organising and controlling the operational level of logistics systems of the Armed Forces.

Purpose, problems and research methods

The premise was to write an article to familiarise readers with the information tools (IT) possessed by the WG&SC, constituting the professional products for use in the *Command Post Exercises* (CPX), commonly called *Computer Assisted Exercise* (CAX). in the tools in the WG&SC simulation systems and others possible for use in support of the job of *Directing and Control Staff Exercise* (DICONSTAFF) are an important part of *Command Posts* (CP) and *Points of Control* (PC), subordinated to *the Inspectorate for Polish Armed Forces Support*.

The main objective of the study is: *Introducing the GW&SC offer in the use of IT systems for military logistics exercised at the operational level command in Computer Assisted Exercises.*

When considering the main goal, sub-goals have been defined as: *Characterisation of the role and purpose of WG&SC in supporting Command Assisted Exercises. Verification of the information needs of Exercise Directing and Control Staff in the modelling of military logistics activities with the capabilities possessed by WG&SC. Assessment of the impact of information systems on the management of the military organisation in the Polish Armed Forces responsible for the functioning of logistics system operating level in CAX.*

The implementation of the objectives outlined are required to answer the following research questions: *What is the role and purpose of WG&SC in support of Computed Assisted Exercise? In what areas of the military logistics task you can use the simulation system and other tools to support CAX? What is the impact on the management of information systems in the CAX logistics system?*

Because of such formulated research problems, the use of research methods were as follows: **Analysis of materials and documents** operational and organisational preparation for the exercise, Silesia-14. **Analysis of teaching materials** used for training operator workstations in the JTLS system and JEMM applications in the exercise. **Scientific inference** is based on the results of simulation and statistical data from the performed exercise. **The diagnostic poll** conducted an uncategorised technique interview with important persons directing the Exercise and selected representatives of operational groups and a polling technique conducted with JTLS operators' workstations. **The** author received the permission of WG&SC for the exercise and served as the head of the coordination team, supporting the period for preparing exercises for the job of the *Core Planning Team* (CPT) and during the *Directing and Controlling Staff* (DICONSTAFF) exercises. At that time, direct contact was maintained with all the functional team leaders in the exercise.

Role of Computer Assisted Exercise

The exercise is a kind of test of the ability to apply theoretical knowledge in the field of organising and conducting various types of operational-tactical activities. The best exercises enable the preparation of commanders and staff officers for commanding troops. They are an essential part of the training process, which aims at comprehensive preparation of commanders (bosses, commanders, supervisors in the described exercise) and staffs to perform the tasks (command and control) as intended.

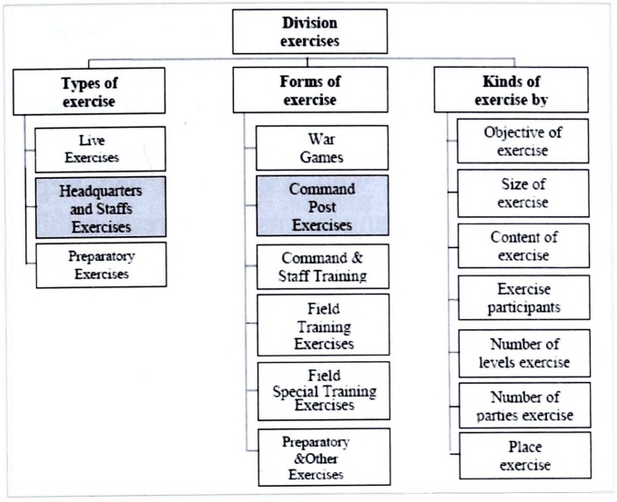
The essence of the training process is a purposeful, planned and systematic implementation of undertakings and methodological training to prepare, maintain and improve individual and team skills of headquarters and staffs, as well as the improvement of the forms and methods of the training process. The content of training (including logistics) is to solve problems of organisation and the carrying out of different types of combat and non-military and emergency response within and outside the country, and solving the problems of the future battlefield, according to the practitioner level of command and its destination[1]. Under the current classification of the *Armed Forces*, included in the next national doctrinal document, exercises are divided according to various criteria shown in Figure 1.

The above document states that one of the entities training are headquarters and staffs, along with elements of the communication system providing internal and external information exchange and distribution of cell administration offices and state and local government and non-military cells for defence of the state[2]. The

[1] *Organization of training commands and staffs in the Armed Forces of the Republic of Poland*, MOD, DD/7.1(A), Warsaw 2010, p. 6.

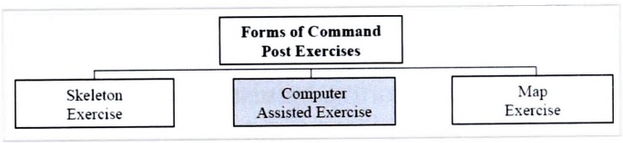
[2] Ibidem, p. 6.

Inspectorate for Polish Armed Forces Support, having different specialised services, units and institutions, has a duty to train them through, inter alia, the organisation and conduct of basic forms of Command Post Exercises, shown in Figure 2.



Source: own study on the basis of the documentation of the *Instruction* ..., pp. 6–18.

Fig. 1. Classification of exercises in the Polish Armed Forces



Source: own study on the basis of the documentation of the *Organization* ..., p. 9.

Fig. 2. Types of Command Post Exercises

CAX is a type of exercise conducted by the headquarters and staffs of the military unit level and above. During this exercise, the computer simulation system introduces real-time decisions generated by e command and staffs, known as *Primary or Secondary Participants* (PP/SP) or *Players*. Back to the Participants, simulation results are disseminated in the form of standard documents proving accordance with the approved by DICONSTAFF of the reports system[3]. CAX is designed to improve the skills of individual staff and ripping the functional cells commands and staffs (including logistics and personnel) in the preparation of operations and command during combat operations. Due to the criterion of their conduct, CAX should be primarily carried out in the centres of computer simulation, using simulation programs and other tools to support the process of command.

In the CAX, within the framework of the defined scenario, both implemented processes and organisational structure are reflected in virtual reality. On the other hand, *Participants* (*Players*) under the responsibility of, carry out their tasks in accordance with standard operating procedures: make decisions, subordinate task forces and control their activities. While the teams leading LOCON (*Lower Control*), using operators workstations, introduce *Players* computer simulation system decisions and, in return, provide them the information generated by the system simulation in the form of standard documents. A characteristic feature of the simulation system is that both the computer system and the operators of the system remain "invisible" for *Participants* in making their decision and direct the activities of subordinate troops[4]. Thanks to this, opportunities are created for Participants to use organic means of communication and command support, not dealing with the technical problems associated with the operation of computers, but focused on operational tasks, and not on the processes of simulation.

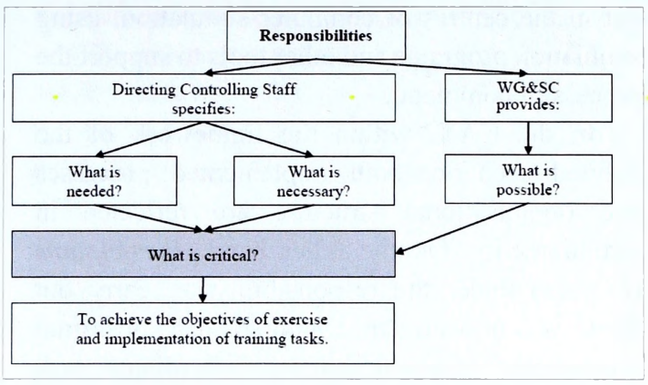
Only after the successful completion of the CAX, should headquarters go to the skeletal exercise , with the development of a desktop or mobile command system, and then to exercise with the troops (LIVEX).

The role and purpose of WG&SC in Computer Assisted Exercises

The task of WG&SC staff dedicated to functional teams is to secure the needs of DICONSTAFF, necessary for the efficient conduct of the exercise. In particular, this support relates to the use of exercise: simulation system and other tools to support the process of command and control the course of exercises and information technology equipment and accommodation facility. The role and responsibilities of WG&SC in graphical form are shown in Figure 3.

[3] Ibidem, p. 8.

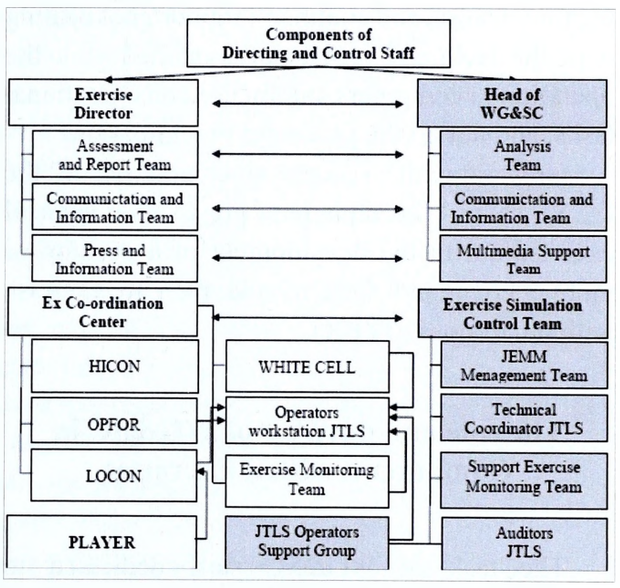
[4] J. Knetki, *War Games and Simulation Center*", „PWL", nb 2/2005 p. 25.



Source: own study on the basis of the presentation of the Head WG&SC, Warsaw, [28.11.2014].

Fig. 3. The role and responsibilities of WG&SC staff in achieving its objectives exercises

The diagram shows that the WG&SC task is to support the DICONSTAFF in securing its needs, to the extent necessary to achieve the objectives of the exercise and the tasks of training. The position of WG&SC functional teams, secreted into CAX Silesia-14, is illustrated in Figure 4.



Source: own study on the basis of the documentation of the exercise Silesia-14, WG&SC, Warsaw 2014.

Fig. 4. Place of functional teams on WG&SC during the conducting of exercises

Specific tasks of WG&SC CAX functional teams while driving, including the exercise Silesia-14, include:

a) Analysis Team AAR (After-Action Review):

– collection, analysis and synthesis of information being the result of the simulation,

– collection and archiving of historical information and forecasting future events,

– cooperation with Analysis, Assessment and Report Team in terms of the arrangements for the scope, form and timing information;

b) Communication and Information Team:

– monitoring and administration of WG&SC computer networks,

– monitoring and administration of WG&SC telephone networks;

– cooperation with Assessment and Report Team, making arrangements is the responsibility of the functional and reporting deviations from targets simulation;

c) Multimedia Support Team:

– multimedia DICONSTAFF support;

– provision of services audio / photo / video;

– video conferencing system administration WG&SC;

– requires settlements: *where?, when? and what? is to be done;*

d) JEMM Management Team:

– control over the implementation of the compliance of the activities in the message delivery system with the course of the simulation, objectives and training exercises issues,

– JEMM scenario administration,

– JEMM technical administration;

e) Support Group Exercise Monitoring Team:

– monitoring compliance with the objectives of the simulation and training exercises issues,

– supervision over the consistency, with the objectives of the simulation and training exercises issues,

– coordination of the simulation,

– alteration of the simulation by order of the Exercise Director;

f) JTLS Controllers Group simulation system:

– monitor the status of the simulation in terms of responsibility,

– correct errors by current operators;

g) Support Group for JTLS simulation system operators:

– professional support system for JTLS operators;

– support teams leading up to the interpretation of the use and operation of the units in the JTLS system;

h) Real Live Support (RLS) Team:

– making available and transferring housing base and technical issues of WG&SC to DICONSTAFF,

– supervision of compliance with the requirements of health and safety and fire conditions.

Needs analysis modelling combat operations, logistics and personnel in the system during the simulation exercises of JTLS Silesia-14

Input data:

– form of exercise: *Command Post Exercise*, *Computer Assessed Exercise*;

– type of exercise: exercise control, military, one level, in stationary objects;

– Exercise Directorate: *the Inspectorate for Polish Armed Forces Support*;

– place: WG&SC and stationary objects: of Participants exercise - the units and institutions;

– the number of commands: the Primary Participants (4), Secondary Participants (9);

– training issues, which are related to combat operations, logistics and administrative arrangements necessary for simulation system modeling:

• combat service support of own operational troops and allied forces;

• evacuation threatened material bases;

• technical evacuation out-of-order military equipment;

• personal replenishment of operational troops;

• protective and defensive actions in the area of responsibility of the *Regional Military Headquarters* (RMH);

• the use of *Territorial Army* (TA) forces;

• interoperability with non-military defence cells.

Output data:

– the need for modelling logistics processes and personnel;

– the need for modelling military units components: land and air;

– the need for modelling activities, protective and defensive forces (battalions and companies to protect and defend objects) and territorial defence forces (brigades and regiments TA);

– the need for modelling territorial bodies of military administration (*Regional Military Headquarters* and *Military Replenishment Command* (MRC));

– the need for modelling non-military system;

– the need for modelling the enemy's forces;

– the need for transport by road and rail of allied forces (the construction in JTLS simulation system of the railway network).

Modelling logistics processes

From the national normative document[5] contained in the list of subsystems logistics that logistic model simulation systems should have the possibility of mapping the actual logistics processes[6] in all functional areas of military logistics, including:

– **in the range of management bodies and logistics units**: the creation of the logistics chain and its modifications in the course of the game, to monitor the movement of logistics resources and logistics infrastructure management;

– **in the range of material support**: introduction to database parameters in the scenario of munitions and material exercises, logistics facilities, supply depots, modelling the consumption of supplies, monitoring inventory supply in units, modelling flow (supplies, inventory replenishment and recovery) and their evacuation;

– **in the range of technical support**: introduction to database parameters, armaments and military equipment, modelling and supply of technical means material (TSM), modelling of losses in military equipment (combat and non-combat), monitoring of the facts and evacuation of equipment and repairs;

– **in the range of medical support**: introduction to database parameters of the personnel of military and civilian casualties, modelling (combat and non-combat), modelling of evacuation and treatment of the wounded and sick, and blood and medical supplies;

– **in the range of transport support:** data entry and modelling the transport of troops and supplies by road agents, rail, inland waterway, air and maritime transport network, modelling of road,

[5] *Logistics Doctrine of the Armed Forces of the Republic of Polish*, DD/4, NDM, Warsaw 2004, p. 11.

[6] Understood as **a logistics process** „...orderly chain of operations associated with the movement of materials", K. Ficoń, *Economic Logistics. Logistics processes*, BEL Studio, Warsaw 2008, p. 152.

rail, inland waterway and transmission; modelling handling equipment, logistics centres, junctions, seaports and airports as well as pipeline network transmission equipment.

Results of studies

The requirements defined above for modelling logistics processes and personnel in the system simulation and other applications owned by WG&SC require simultaneous preparation: JTLS workstation operators, operators for data entry and support for the JEMM application and user training in the iGeoSIT application. The total needs of DICONSTAFF for training of functional persons to handle the information tools were as shown in Table 1.

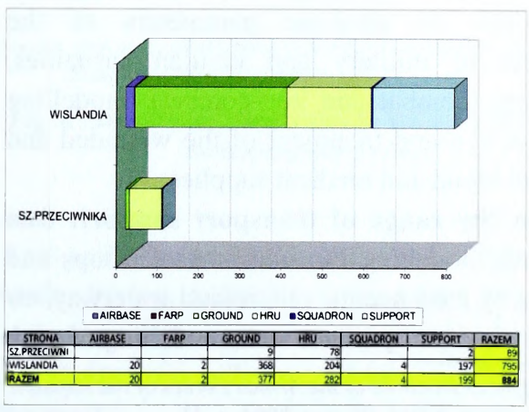
Table 1

List of soldiers trained to handle information tools in exercise

Name of training	Number of trained soldiers	Number of workstations occupied
Course operators JTLS workstation	64	32
Course operators JEMM application	39	39
Course users iGeoSIT application	20	15

Source: own study on the basis of the documentation of the exercise, Silesia-14, WG&SC, Warsaw 2014.

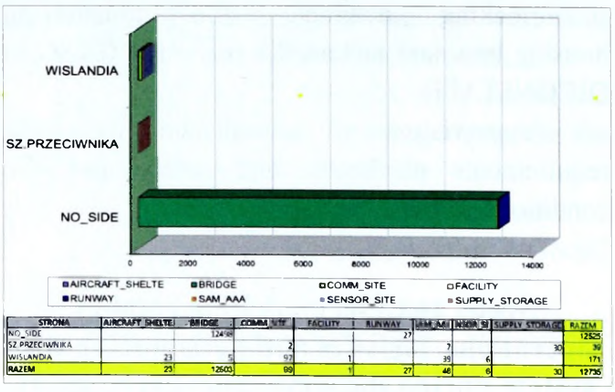
At the same time, WG&SC's efforts focused on the introduction to the JTLS system database of hundreds of thousands of pieces of data for modelling of almost 900 own and enemy units and nearly 13,000 facilities, occurring in the scenario exercise. The detailed data by type of units and class objects is depicted in Figure 5 and 6.



STRONA	AIRBASE	FARP	GROUND	HRU	SQUADRON	SUPPORT	RAZEM
SZ.PRZECIWNI			9	78		2	89
WISLANDIA	20	2	368	204	4	197	795
RAZEM	20	2	377	282	4	199	884

Source: R. Kaniewski, WG&SC Analysis Team, [28.11.2014].

Fig. 5. List of units entered into the scenario database



STRONA	AIRCRAFT_SHELTE	BRIDGE	COMM_SITE	FACILITY	RUNWAY	SAM_AAA	SENSOR_SITE	SUPPLY_STORAGE	RAZEM
NO_SIDE		12498			27				12525
SZ.PRZECIWNIKA			2			7		30	39
WISLANDIA	23	5	93	1		35	6		171
RAZEM	23	12503	95	1	27	46	6	30	12735

Source: R. Kaniewski, WG&SC Analysis Team, [28.11.2014].

Fig. 6. List of facilities entered into the scenario database

Analysis of possibilities for modelling of combat operations, logistical and military administration at the operational level in the simulation system JTLS

According to military experts, the most effective tool in the training commands and staffs is considered to be the battlefield computer simulation systems. Computer simulation is treated as a form of exercise, in which the Player can make decisions and reports based on the information received and observe its effects, and mistakesthat do not produce real consequences and, thus, have a particular value for training. It is not without significance that the possibility of replaying the same situation due to the lack of time for such action and the costs is not realistic in exercises with LIVEX troops (*Live Exercise*).

In the Silesia-14 exercise, an American system simulation, JTLS (*Joint Theater Level Simulation*) was used, designed for modelling and simulation combat operations, using constructive simulation CAX exercises. The analysis of the manufacturer's documentation, tests and exercises proved that the logistics module in the JTLS system has the capability to imitate logistics processes in all functional areas of logistics subsystems, including:

- command and control of logistics units;
- support for material (e.g. modelling supply, inventory replenishment and recovery supplies);
- support for the technical (e.g. modelling loss of combat systems and modelling of repair and maintenance combat systems);
- support for the medical (e.g. modelling loss of personnel, modelling of medical treatment in own units);

– support for transport (e.g. modelling supply convoys, air, sea, rail, vehicular, inland waterways and pipelines);

– flow control stocks of material supply:

• automatic (by the system);

• hand (according to the decision of exercisers and logistics requisition).

The JTLS solutions used in the system enable the implementation of logistics processes automatically, manually, or by mixed means. This means that the JTLS system, depending on the purpose of the exercise, lets you decide what to choose and how to control the flow of logistics resources. Most of the exercises conducted in the WG&SC were implemented in a mixed way: by hand for subordinate exercisers of units, and automatically for non-exercisers units occurring in the organisational structure of the exercise, including its own troops and enemy forces.

Analysis of the possibility of using a JEMM application supporting the management of an exercise

The JEMM *(Joint Exercise Management Module)* module supporting management exercises is a tool designed by the NC3A agency to support the conduct of the *Command Post Exercise*, including *Computer Assisted Exercise*. The tool is designed for an application *website*, enabling management to exercise influence on the course of the exercise by introducing episodes for exercisers, according to the assumptions and training issues. The tool also allows *Players* control by tracking their reaction to events as they happen.The application provides, from the description in the system documentation[7]:

– access to the documentation exercise;

– visualisation of running the exercise scenario;

– the possibility of ongoing interaction with the incident prepared or under development;

– auditorium between JEMM users;

– the ability to create and control requests for information and its support;

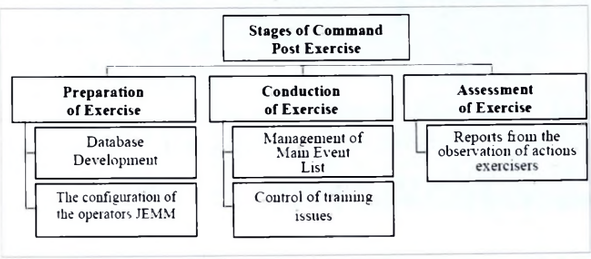
– the possibility of practicing proper operation of the monitoring command authority by observers from the *Team Analysis and Evaluation* exercise and *Team Ripping Fighting Systems*;

– providing reports on monitoring the implementation of the tasks of practicing leadership;

– synchronisation of incidents with simulation;

– display of planned incidents on a map.

The JEMM application is used in all stages of the exercise. The scope of the tasks at various stages is shown in Figure 7.



Source: own study on the basis of the documentation of the exercise Silesia-14.

Fig. 7. The scope of performed tasks in various stages of the exercise

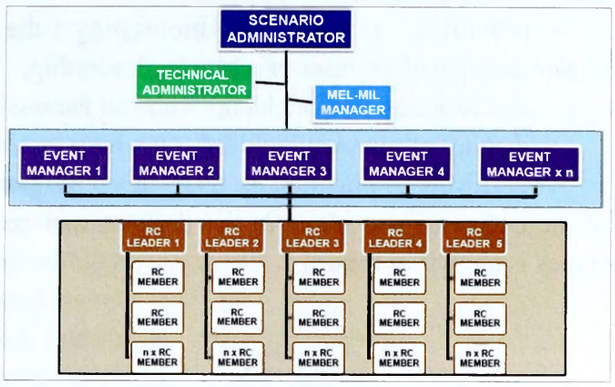
The study shows that jobs are routed to JEMM operators in all functional cells of the DICONSTAFF in: Team Analysis, Evaluation and Report exercises (AE&R), Team Monitor the Course of the Exercises (MCX), Team Main Events or Injects List Messages (MEL / MIL) and Teams leading up: parent and neighbor command-level (HICON, SITFOR); the participants level (LOCON); the Opposite Forces (OPFOR); and for units and institutions outside the chain of command (WHITE CELL).

For each scenario, an organisational structure and a management JEMM application consisting of a series of posts should be prepared. A sample of the posts structure prepared for the purposes of the application is shown in Figure 8.

A total film management positions exercise using the JEMM application, depending on the momentum exercise, in particular the number of task areas to be examined (*Event Manager*), the number of teams leading up (*RC Leader*) and the number of team members leading up (*RC Member*) and the number of sent observers (*OT observer*) when exercising PC and CP, can change up to several dozen soldiers (e.g. CAX Anakonda-14). In this exercise, codenamed Silesia-14, 39 users

[7] M. Sołoducha, *JEMM using the module in the exercise codename Silesia-14*. Produce training material for Training Exercise Directorate, Electronic Archive WG&SC, Warsaw 2014, ppt presentation.

of the JEMM application were trained, who then occupied the same number of workstations with the JEMM application installed.



Source: M. Sołoducha, *JEMM using the module in the exercise code-named Silesia-14*, WG&SC, Warsaw 2014, ppt presentation.

Fig. 8. The structure of posts JEMM

It follows from the above diagram that the coordination of the events corresponds to the chief of MEL/ MILG, who is responsible for placing the leading events. In contrast, the simulation results based on JTLS entered into the system are random incidents. Their results are sent to CP / PC exercisers headquarters by phone, email or fax. During developed CAX and during the preparation of the exercise, a database containing a list of subject areas (events), divided into groups of events - episodes (incidents), is used, which in turn contains information on the episode in the context of the incident (inject). The final element is to determine how to implement each incident (action) in the system simulation.

Figure 9 shows what was presented to the actual folder database in exercise Silesia-14, developed on the basis of the MEL/MIL.

An analysis of the content of the database that was created for the purpose of practicing seven thematic sections, containing ninety-six events with four hundred episodes, which is scheduled for one hundred and five reactions in the system prepared for the JTLS event. It should be considered that the JEMM application is sufficiently flexible that it allows you to make changes to the developed scenario events, as well as the introduction of new events and the planned response and the CP/PC *Players* for these events. The study shows that during the exercise scenario, twelve thematic areas associated with the legislation applicable in the reporting CAX system were also introduced.

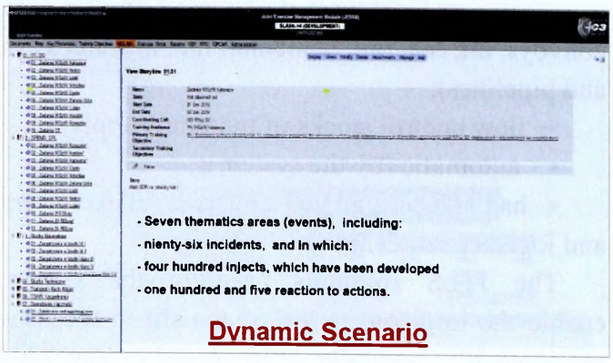


Fig. 9. JEMM application database for exercise Silesia-14

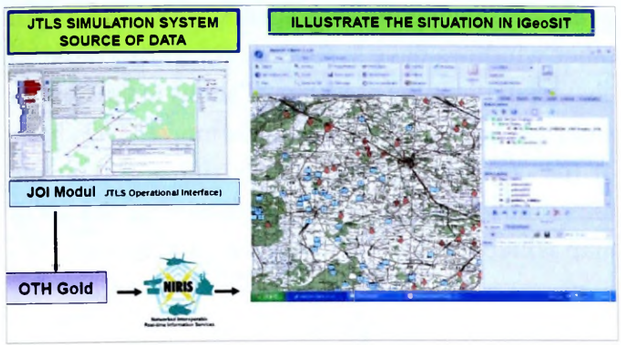
Analysis of the spatial visualizstion capabilities of the iGeoSIT

The IGeoSIT application (the Interim Geospatial Intelligence Tool) is a tool which integrates different types of real-time geospatial and operational information, based on common primers mapping, enabling this information to be displayed in the form of a Common Operational Picture (COP) of the situation. The application is a product of the NATO Agency for Communication and Information (NCIA). The user ensures that the serverhas access to the application by typing the address in the iGeoSIT Internet Explorer window and launching the application.

Application possibilities[8]: displaya Common Operational Picture of the situation; updates the subordinate position of subdivisions and military institutions; displays information on units; creates user layers of geospatial and operational information; and generates situational reports.

In this exercise, the Silesia-14 application iGeoSIT version 2.1.0, was used for the common picture of the operational and tactical CP and PC units subordinates directly sent to the Chief of the Inspectorate from Armed Forces Support, arranged in thirteen locations in the south of Poland. This task was accomplished through ongoing, automatic transfer of information from the JTLS simulation system, operated in WG&SC with the iGeoSIT application installed on the Command Posts displayed in practicing commands and staffs garrisons. The cooperation of the iGeoSIT JTLS application is illustrated in Figure 10.

[8] W. Biało, *The role and scope of application use in the exercise iGeoSIT codename Silesia-14*. Produce training material for Training Exercise Directorate, Electronic Archive WG&SC, Warsaw 2014, ppt presentation.

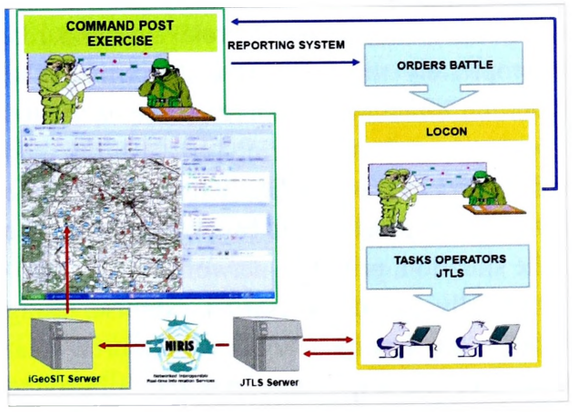


Source: W. Biało, op. cit., ppt presentation.

Fig. 10. Scheme of cooperation of the iGeoSIT application with the JTLS simulation system

The source of data on the situation was *Joint Theater Level Simulation*, which was developed for the exercise of assumptions and exercises conducted during the observation The Module implemented in JTLS JOI (*JTLS Operational Interface*) protocol over OTH Gold[9] (*Over the Horizon Gold*) obtained from the system JTLS information and was provided by the NIRIS system (*Interoperable Networked Real-time Information Services*) iGeoSIT applications. The NIRIS system is a system that integrates and converts various data transmission protocols, allowing users to access information from a variety of systems and applications in real time.

In Figure 11, the procedure flow information between the JTLS system and the iGeoSIT application is shown.

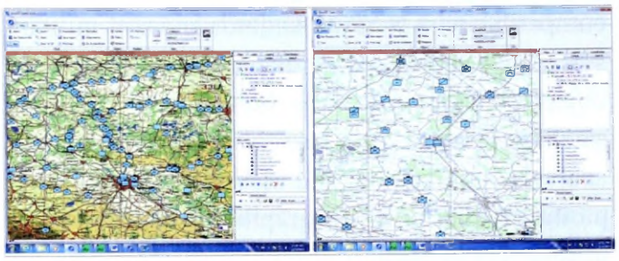


Source: W. Biało, op. cit., ppt presentation.

Fig. 11. IGeoSIT application usage patterns in the exercise, Silesia-14

[9] JTLS can cooperate with other military information and communication systems through protocols: Link-16, AdatP-3 and well as the Protocol OTH Gold. See.: P. Boryn, *Distributed CAX exercise as a modern form of training commands and staffs*, available: www.csikgw.aon.edu.pl, [access: 15.12.2014].

Practical realisation of the above solutions in the exercise, Silesia-14, is reflected in Figure 12 as a picture of the situation of operational units and institutions subordinate to the *Command Posts and Points Control*. Interviews with *Exercise Participants* show that by using the iGeoSIT application, CP and PC exercising during exercise have ongoing real-time display of the operational situation, including logistics in their area of responsibility.



Source: screenshots illustrate the iGeoSIT application, WG&SC, Warsaw 2014.

Fig. 12. Example illustrate the position of logistic units and institutions of military administration in the iGeoSIT application

In summary, the existing solutions, existing CAX exercises conducted in previous years, did not assume an operational picture of the situation on the CP card and the PC. The only knowledge of the position of the Participants was to obtain reports from subordinates. The drawback associated with the lack of imaging was one of the ills articulated by exercising CP and PC. Implementation of the application in the exercise, Silesia-14, represents a major advance in providing the Participants with real-time information about the location of subordinate subdivisions and institutions.

The analysis of the possibility of applying the Operations Graphics Package in the exercise, Silesia-14

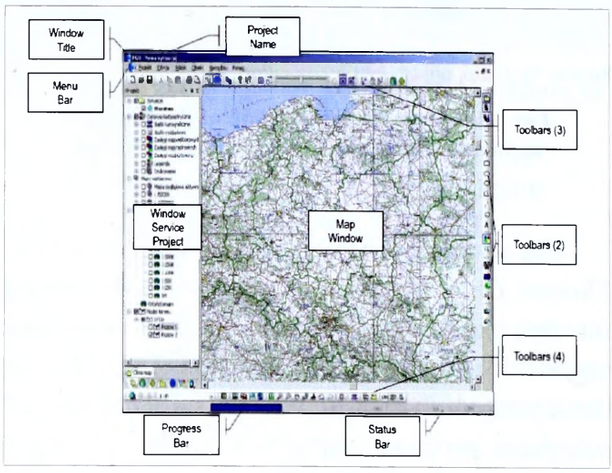
The Operational Graphics Package (OGP) is a program designed and produced to illustrate the operational and tactical situation on the back of digital maps (aerial and satellite imagery) and to carry out an operational assessment of the area. In addition, the base provides a platform for specialised

systems, developed in CIT&CND (*Center for Information Technology and Communications of National Defence*) [10], using a graphical display on the substrate maps and digital images, as a module used in other systems. Among other things, it serves to illustrate geospatial command support systems and crisis management. Geographical coverage of the software enables you to visualise the action virtually all over the world, except the poles[11].

The program allows for: drafting contractual graphic symbols using military characters, compatible with NATO standards and non-military systems; searching and displaying geographical objects of administrative boundaries; operating satellite imagery, air, etc .; conducting spatial analysis and mapping and assessment of the land; plotting and printing the graphic situation on maps of different scales[12].

The use of the OGP in the exercise, Silesia-14 requires addressing a number of limitations. Although the OGP software does not include inside information that could constitute a state or official secret, it requires that the statement produces no greater security classification than the information in the database of the simulation system. Therefore, it should have documents and files containing the r registration statement made primarily in records files on removable media and mail delivery with content summaries. Access to the print and media should be limited in accordance with the principles of protection of classified information in the military. In fact, the OGP is ready for use on a single computer. The need to use a larger number of computers working in the exercise, Silesia-14, interconnected using a local area network to each of them required the installation of separate full software.

In addition, the OGP can only share geographic data in the network, which means that each user OGP controls his work using the graphical interface. The interface has a number of windows and bars. Of all the available graphical tools, the Map Window undoubtedly plays a central role. The user can observe the results of the maps, which generally occupy the largest area of the screen. All other windows have secondary roles. Its graphical characteristic is the presence of slides in the bottom and right edges, used to feed the image. The shape of the cursor takes particularly rich forms inside the Windows Map. A sample image of the OGP map window is shown in Figure 13.



Source: *Manual Package Operations Graphic*, MOD, Warsaw 2006, p. 9.

Fig. 13. An example of the appearance of windows OGP Maps

Another limitation relates to the fact that the OGP does not provide any mechanisms for data protection. Explicit and implicit data are treated in the same way. Therefore, the user must ensure proper protection of classified information being processed. Therefore, the system should be operated in accordance with the relevant standards, by appropriately trained staff and verified. The data on the situation is stored in an encrypted file workspace, thus ensuring the integrity and confidentiality of the data lies with the user or the transmission channel (in the case of a transfer file with the situation, print to a network printer, etc.).

Practically, in the Silesia-14 exercise, using the OGP application, WG&SC assured that commanders and staffs, among others, illustrated the preparation of the subordinate position of subdivisions and institutions, which, according to the registration system and the circulation of information in the exercise, had sent teams leading up to the practitioner level subordinates (*LOCON*) within the time limits.

Figure 14 illustrates an example of mapping a JTLS system tactical situation in OGP.

[10] Since 01.04.2011, the change of name *Center for Information Technology and Communications Ministry of National Defence* (CIT&C NDM) to *Ministerial Project Management Center of Information* (MPMCI).

[11] *Manual Package Operations Graphic*, NDM, Warsaw 2006, pp. 6–8.

[12] Available: http://www.rcpi.wp.mil.pl/, access: [15.12.2014].

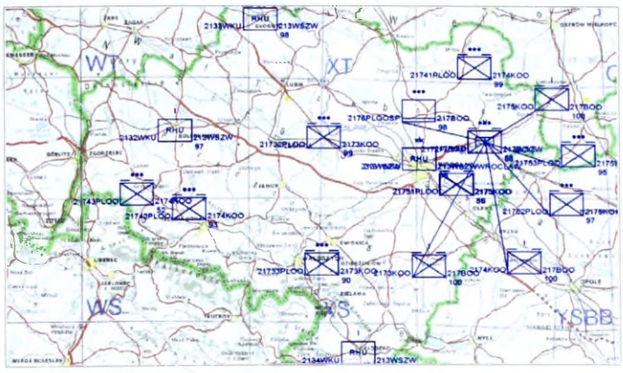


Fig. 14. Displays the position of logistics and military administration of Wroclaw RMS subordinate OGP system with the JTLS application

Operational groups, after receiving a generated JTLS imaging system through a JEMM application, transmit twice a day to exercising CP and PC (including situation reports prepared and logistics). For Players of information generated in the OGP position, the subordinate units and institutions complement and confirm from another the source of information obtained from subordinates in the form of situational reports.

Summary

Impact of the use of information systems for management of the organisation

During the CAX codenamed Silesia-14, studies conducted have shown that the operation of existing tools, supporting the management of logistics system in the exercise, considerably facilitates the work of the Exercise Directorate, which, through the management of information flow and directing the course of the exercise, had a full insight into the development of the operation and logistics, including the ability to assess the commands and staffs.

In the Jobs Exercise Directorate (DICONSTAFF), *Players* (practicing commands and staffs), as well as the *Operational Teams*, the exploitation of existing tools in CAX relies heavily on the collection and processing of a variety of information, which makes supporting information an extremely useful tool in the hands of the Exercise Directorate. In the case of the codenamed Silesia-14, exercise tools properly selected and implemented to the scenario helped save DICONSTAFF, charged with the organisation and directing the course of the exercise, a lot of time and optimised its operation.

In addition to the use of exercise in the management of the simulation system, DICONSTAFF can also save much time by using other electronic tools, used to assist in the management exercise. These tools include JEMM, iGeoSIT and OGP. For example, conducting exercises on a paper (written) version of the MEL / MIL Plan and transferring their means of communication or even an e-mail does not provide automatic registration of correspondence documents. In contrast, the information management module JEMM has created the conditions for full control over the flow of information between DICONSTAFF and CP / PC cells.

Through the use of ICT tools, an increase in efficiency is achieved, as one soldier, the participant, is able to accomplish more tasks. It is estimated that the use of all sorts of new technology will increase the commitment of, especially, young staff accustomed to the benefits of modern technology. The exercise studies conducted with the participants (observation, interviews and conversations) showed that there is an increased involvement in the classes, distinguished by innovative solutions. In order to improve the satisfaction of functional DICONSTAFF, exercisers from CP and PC units and institutions reporting directly to the Chief of the Inspectorate Armed Forces Support examined which of the tools used met the requirements of the users, and where it is necessary to improve their functionality.

Please note that there is no ideal simulation system for modelling all types of units present in the Armed Forces and the types of forces and services. In the case of subordinate units of the Inspectorate for Armed Forces Support, this is, in particular, Regional Military Staffs, Military Command Replenishment, traffic control company, Military Transport Command and territorial bodies of military administration. Military administration has its own characteristics and requires certain properties of the system. A system which is ideal for modelling military operations carried out by operational forces is certainly not as useful for territorial bodies of military administration. Therefore, the *Core Planning Team*, especially the WG&SC staff (logistics specialists) have focused on developing solutions that improve the functionality of the JTLS logistics system.

Conclusions

Conclusion 1. The Exercise Directorate structure, due to its complexity and the enormity of the tasks facing the functional cells, requires excellent organisation. Recommendation 1: To meet these challenges, such as control and command of a large number of units directly subordinate and at the same time to do their work in a rational manner, it is necessary to support the computer.

Conclusion 2. Deciding on the use of any system, DICONSTAFF should take into account the number of requirements that must be met in order that the exercise can take place smoothly. The most important requirement is the need to train adequate numbers of people - operators, systems and applications used in the exercise. In the case of JTLS, it was the number of 64 operators, and the preparation of the MEL/MIL Plan, the introduction of the JEMM system and his staff during the exercise, and from a dozen to several dozen people were involved in different stages. The iGeoSIT Application supports another 15 staff members who had to be prepared both to support applications (*users*) and for application management (*technical administrator*). Recommendation 2: In this situation, the system is particularly important for functional training of all DICONSTAFF students, especially JTLS simulation system operators and JEMM applications.

Conclusion 3. WG&SC, having an integrated JTLS system of simulation, provides the conditions for the preparation and conduct of such exercises, in which the input to the system is done only once, and this information is available to all participants in the exercise. This solution saves time, improves efficiency and reduces the risk of data entry error. Recommendation 3: It should be invoked in the advance *Core Planning Team*, the composition of which should include officers with the most experience and knowledge of operational-tactics and logistics.

Conclusion 4. The proper use of the capabilities of present technology allows DICONSTAFF to work more effectively. With the integrated information systems, multiple programs can work together, giving DICONSTAFF invaluable assistance. Recommendation 4: Implementation of the WG & SC integrated simulation systems and other tools to help manage the process eliminates many inconsistencies with the idea, and through it, definitely improves the quality of services provided.

Conclusion 5. The key for DICONSTAFF benefit is the ability to reduce the number of troops involved in the exercise. Recommendation 5: Consequently, for the efficient and effective management and control exercise, it is necessary to use such software solutions that involve fewer people and ensure high standards. It's mainly about the *Exercise Directorate* to ensure access to current information on the units (subunits) entered into the system, providing full control over personal conditions, combat equipment and supplies, as well as ongoing monitoring of the course of the exercise.

To sum up, the most substantial and technologically advanced class of systems supporting the processes of command and control headquarters and staffs use modern tools. Modern solutions greatly facilitate the work of DICONSTAFF and bring many other benefits. Among other things, they allow for the optimisation of the processes by offering ready-made tools used to automate the exchange of data between cells and between the internal cells and DICONSTAFF and *Players*.

From the point of view of the Exercise Directorate dealing with the management of the flow of information in the exercise, the functional system turns out to be a very good way, on the one hand, to reduce the cost of training (fewer participants exercise), and on the other to ensure efficient and effective management of information. The advantages of computer support could be multiplied indefinitely, but one must also remember the risks and dangers that it brings. First of all, it should be noted that no system is a substitute for a well-qualified staff, and the tools are only a supplement to, and not an alternative for, people.

Bibliography

Biało W., *The role and scope of application use in the exercise iGeoSIT codename Silesia-14*, WG&SC, Warsaw 2014, presentation ppt.

Boryn P., *Distributed CAX exercise as a modern form of training commands and staffs*, WG&SC, Warsaw 2010, www.csikgw.aon.edu.pl.

Logistics doctrine of the Polish Armed Forces, DD/4, MOD, Warsaw 2004.

Technical Documentation of System JTLS, JEMM, iGeoSIT, OGP.

Ficoń K., *Economic Logistics. Logistics processes,* BEL Studio, Warsaw 2008.

Operating Instructions Operating Graphics Package, MOD, Warsaw 2006.

Instructions for preparing and conducting exercises with Headquarters, staffs and troops in the Armed Forces of the Republic of Poland, DD/7.1.1 (A), MOD, Warsaw 2010.

Knetki J., *War Gemes and Simulation Center*, „PWL", nb 2/2005.

The concept of preparing and conducting Computer Assisted Exercises codename Silesia-14, Armed Forces Support Inspectorate , Bydgoszcz 2013.

Organization of training commands and staffs in the Armed Forces of the Republic of Poland, MOD, DD/7.1(A), Warsaw 2010.

Sołoducha M., *JEMM using the module in the exercise codename Silesia-14*. WG&SC, Warsaw 2014, presentation ppt.

http://www.rcpi.wp.mil.pl/.

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

CONTEMPORARY DETERMINANTS OF THE PROFESSIONAL DEVELOPMENT OF LOGISTICS OFFICERS IN LAND FORCES OF THE POLISH ARMED FORCES

ppłk Grzegorz SMERECKI
General Command of the Armed Forces
Manpower Department (J-1)
Personnel Division

Abstract

This article shows some factors which allow logistics officers of the Polish Armed Forces to develop on professional grounds, essential in preparation for carrying out tasks according to the various conditions of the contemporary and future battleground. The author, with his professional background in the achievement of a principal military career, presents the procedures that are obligatory in the process of filling the official posts for the officers. In the later part of the article, the formal and legal conditions of the development of logistics corps have been elaborated. At the end, an attempt to set the directions of the professional improvement of logistics officers has been undertaken.

Key words: logistics officer's corps, formal and legal conditions of the officer's development, the professional development of officers, personnel management skills, career pragmatics.

Development of the staff - is a continuation of (complement) the learning process and training, taking into account current and future requirements. Development of the staff is systemic and is the result of adopted (existing) rules of pragmatic personnel management. Training Doctrine of the Armed Forces of the Republic of Poland, AAP-7

Introduction

The 21st century brings new tasks and challenges for the Polish Armed Forces (PAF), which necessitates changes in the system of the professional development of professional soldiers. This situation applies to soldiers of all military specialties, whereas related specifically to the officers responsible for effective military logistics. An important factor in the development of logistics officers is their preparation for the implementation of tasks depending on the changing conditions of contemporary and future battlefields, including the development of measures being carried out and to identify new threats. It becomes necessary, therefore, that they continuously improve through the integration of continuing professional development carried out to varying levels and forms. These actions have been carried out for years but, nonetheless, they have failed to develop a fully integrated system of professional excellence in the Armed Forces and development of logistics officers, adequate to needs and expectations.

The aim of the article is to highlight the determinants of the development of the logistics officer corps of the Polish Armed Forces and seek to identify the directions for the training of logistics officers.

Characteristics of the logistics officer's corps of the Land Forces

The professional development of professional soldiers (Enlisted Soldiers and Commissioned Officers) is conditioned by accomplished courses, training, post-graduate and doctor degrees. Today (since 5 December 2013), their full range is defined in the Act of 11 September 2003 of professional military service[1]. The completion of specified forms of professional development directly determines the development of professional soldiers representing the professional personnel of the Polish Armed Forces, which, according to a formally effective division from 1 January 2014, is one of the three executive corps:

1) Commissioned Officers, including: junior officers, senior officers and generals and admirals;

2) Non-Commissioned Officers, including junior non-commissioned officers, non-commissioned officers and senior non-commissioned officers;

3) Privates' corps.

Commissioned and Non-Commissioned Officers corps and Privates are divided into specialties' groups, in which military specialties are separated. Due to the changing circumstances, to ensure that the needs of the Armed Forces are met by regulation[2], the Minister of National Defence creates and abolishes the corps, determines their division into specialties' groups and military specialties[3].

From 1 January 2010 eighteen occupational corps[4] operate within the Polish Armed Forces. Logistics is tenth in the illustrated catalogue of the military occupational corps (marked with characters „38"). In the logistics corps, there are four specialties groups as follows: general logistics (marked with a character „A"), supply (marked with a character „B"), the transport and movement of troops (marked with a character „C"), infrastructure (marked with a character „D") and technical (marked with a character „T").

[1] Act of 11 September 2003 *of professional military service*, Dz. U. of 2014. Item. 1414, as amended. d., art. 36 passage 2.

[2] Ibidem, art. 6 passage 1 pt 2.

[3] Ibidem, art. 4.

[4] Regulation of the Minister of National Defence of 11 December 2009 *on corps, specialties groups and military specialties*, Journal of 2009 No. 216, item. 1678, as amended. d.

Table 1

Division of the logistics corps for specialties groups and the number of specialties in the military personnel corps, as of March 2015

The specialities groups	The number of specialities		
	Officers	NCOs	Privates
A – general logistics	1	3	-
B - supply	5	8	14
C - the transport and movement of troops	2	4	3
D - infrastructure	9	10	9
T - technical	4	20	25

Source: Compiled on the basis of the Regulation of the Minister of National Defence on 11 December 2009 on the bodies of occupational corps, specialities groups and military specialties, MoND Journal of 2009, No. 216, item. 1678, as amended.

The logistics occupational corps is divided into five specialties groups, of which there are 117 specialties in the military personnel of the Polish Armed Forces. Among the highlighted catalogue of specialties for the officer corps are 21 military specialties, nine for the infrastructure group, five specialties for the supply group and four for the technical group.

Table 2

Division of the logistics corps for military specialties dedicated to officers, as of March 2015

The specialities group	The military specialities
A – general logistics	General
B - supply	Combat Assets
	Food
	Uniforms
	Fuel and Greases
	Maintaining and Supply
C - the transport and movement of troops	Organisation of transport and movement of troops
	Organisation of Cargo
D - infrastructure	General
	Land Infrastructure
	Airfield Infrastructure
	Navy Infrastructure
	Enviromental Protection
	Power Supply
	Technical Maintenance of Infrastructure
	Urban Planning
	Accommodation
T - technical	Vehicle Maintenance
	Weapons and Electronics
	Utilisation of Military Equipment
	Technical Supervision

Source: Compiled on the basis of the Regulation of the Minister of National Defence on 11 December 2009 on the bodies of occupational corps, specialities groups and military specialties, MoND Journal of 2009, No. 216, item. 1678, as amended.

Posts of the Land Forces logistics corps are allocated in the structures of military units of the Land Forces. Military positions are designed for officers, non-commissioned officers and privates.

Table 3

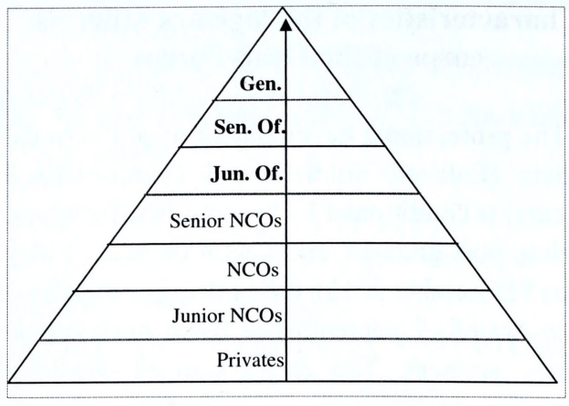
The general division of the military personnel and ranks

Military personnel	Position	Military rank
Officers	Generals	General (Admiral)
		Lieutenant General (Vice Admiral)
		Major General (Rear Admiral Upper Half)
		Brigadier General (Rear Admiral Lower Half)
	Senior Officers	Colonel (Captain)
		Lieutenant Colonel (Commander)
		Major (Lieutenant Commander)
	Junior Officers	Captain (Lieutenant)
		Lieutenant (Lieutenant Junior Grade)
		Second Lieutenant (Ensign)
NCOs	Senior NCOs	Chief Warrant Officer Grade 4
		Chief Warrant Officer Grade 3
		Chief Warrant Officer Grade 2
	NCOs	Chief Warrant Officer Grade 1
		First Sergeant (Senior Chief Petty Officer)
		Sergeant (Chief Petty Officer)
	Junior NCOs	Specialist (Petty Officer First Class)
		Lance Corporal (Petty Officer Second Class)
		Corporal (Petty Officer Third Class)
Privates	Privates	Private First Class (Seaman Apprentice)
		Private (Seaman)

Source: Compiled on the basis of the Act on 21 November 1967 about the general defence duty of the Republic of Poland.

Optimal distribution of military positions (best under specific circumstances) for the logistics corps has a structure similar to an isosceles triangle, in which it constitutes the basis for positions with the lowest degree and, with the transition to the apex of the triangle, decreases the number of positions while degrees are rising.

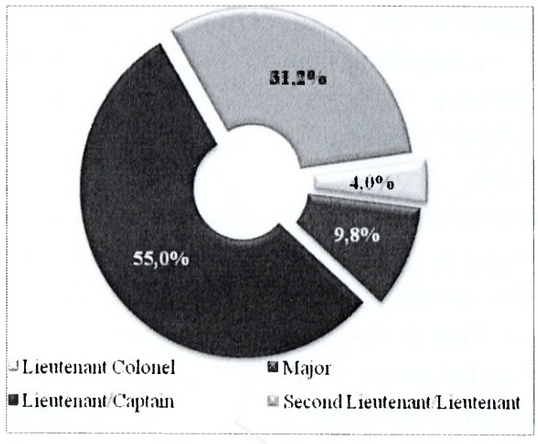
The distribution of military positions shown above enables the movement of soldiers to higher positions, applying the principle of equal access for all of them. As a result, the "best of the best" soldiers are prepared to take the positions.



Source: Self-study

Fig. 1. Expected distribution of military positions

Percentage distribution of military positions in various degrees of logistics corps in the Land Forces held for officers in December 2014 is shown in figure 2.

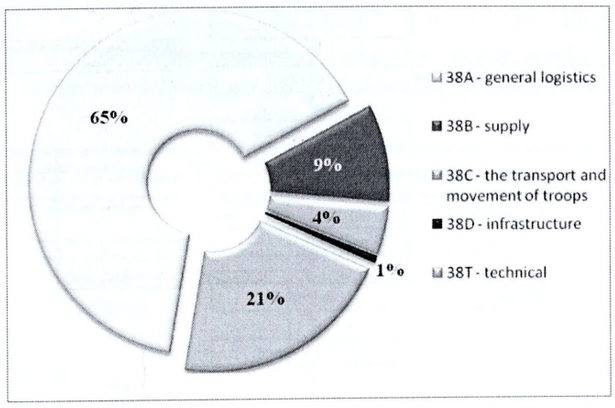


Source: Self-study

Fig. 2. Percentage distribution of military positions in various degrees of logistics corps in the Land Forces

The distribution shown is consistent with the indicated standard distribution of an isosceles triangle with respect to the positions for junior officers in the rank of Lieutenant and Captain, and positions for senior officers in the rank of Major and Lieutenant Colonel. The positions of each specialties group in the logistics corps structures of the Land Forces is quantitatively varied.

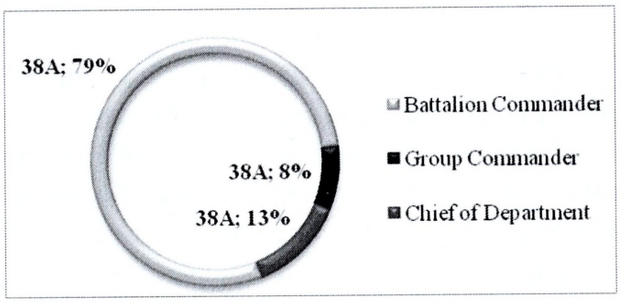
The largest number of positions in logistics corps represents a general logistics group (65% of all positions), then comes the technical group (21%), and the smallest group is infrastructure (only 1%).



Source: Self-study

Fig. 3. Percentage distribution of military positions in various specialties groups of logistics corps in the Land Forces

The purpose of a more complete analysis of the positions of the logistics officers' corps should be made by imaging positions in various degrees and specialties groups.

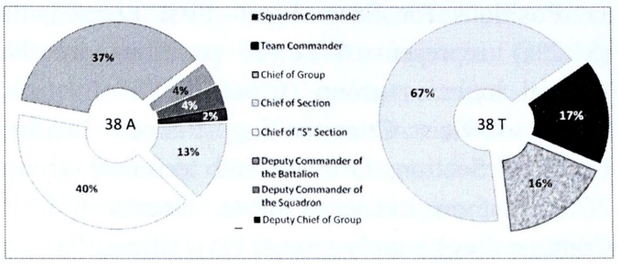


Source: Self-study

Fig. 4. Percentage distribution of military positions for Lieutenant Colonels of logistics corps in the Land Forces

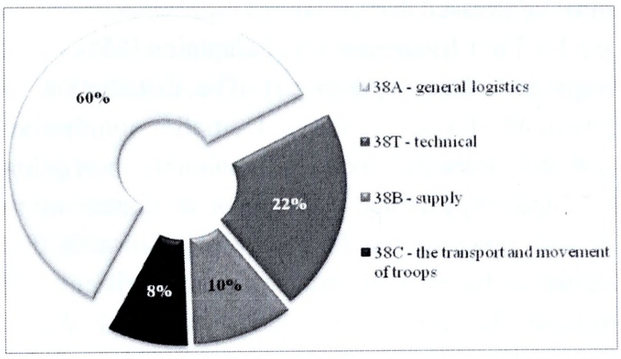
Positions for Lieutenant Colonels represent 4% of the positions in the logistics corps in the Land Forces, which include the positions: Chief of Department (Chiefs of Division Departments), Battalion Commander and Group Commander. They are only the general logistics group.

Positions for Majors (9.8%) represent positions in the general logistics group (Chief of "S" Section, Deputy Commander of the Battalion, Squadron Commander, Deputy Commander of the Squadron, Team Commander) and technical group (Chief of Section, Chief of Group, Deputy Chief of Group).



Source: Self-study

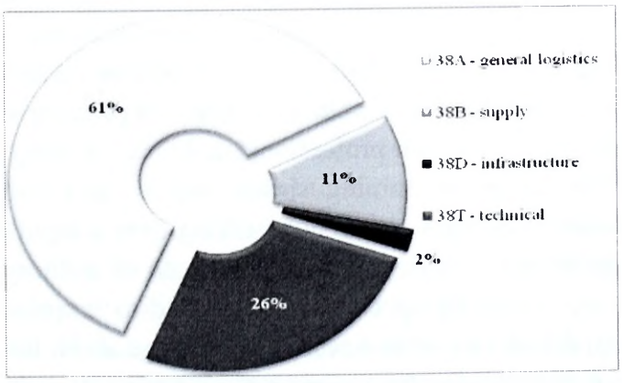
Fig. 5. Percentage distribution of military positions for Majors of logistics corps in the Land Forces



Source: Self-study.

Fig. 6. Percentage distribution of military positions for First Lieutenants and Captains of logistics corps in the Land Forces

Positions for First Lieutenants and Captains (55%) represent 60% of positions in the general logistics group (Officer Commanding, Chief of "S" Section, Staff Officer, Chief of Section) and 22% in the technical group (Staff Officer, Officer Commanding, Director of the Course, Deputy Chief), supply group 10% (Staff Officer) and 8% in the transportation and movement of troops (Staff Officer, Officer Commanding).



Source: Self-study.

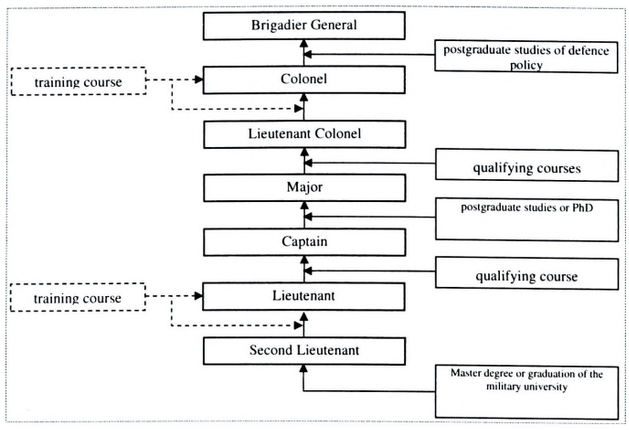
Fig. 7. Percentage distribution of military positions for Second and First Lieutenants of logistics corps in the Land Forces

Positions for Second and First Lieutenants (31.2%) represent 61% of positions in the general logistics group (Chief of "S" Section, Deputy Officer Commanding, Platoon Leader, Chief of Section, Officer) and technical group 26% (Platoon Leader, Officer, Deputy Officer Commanding), supply group 11% (Officer, Platoon Leader) infrastructure group 2% (Platoon Leader, Officer).

Summing up discussion on the characteristics of the logistics officer corps of the Land Forces, it must be stressed that the largest number of positions are for First Lieutenants and Captains (55% of all logistics officers' positions). The distribution of positions shown indicates a smaller number of first positions for Second Lieutenants in relation to Captains' positions. The lack of conservation of the structure stands in comparison with that shown in figure 1 for the expected distribution of military positions. This is particularly significant information for the largest group of logistics officers' corps, which is a general logistics group (65%). The development of logistics officers from other groups should be focused on preparing officers in higher ranks to change their specialties group.

Identification of formal and legal conditions of development logistics officers' corps

Development of the military career of professional soldiers and conduct of service were authorised in the Act of 11 September 2003 of professional military service[5]. Qualification requirements for appointment to various posts in the officers' corps depend on postgraduate studies and qualifying and training courses implemented in the system of professional soldiers' training. The forms of training shown are divided into courses that are required for taking over a higher position or following a different path of military career (qualifying courses), designed to increase qualifications or to develop knowledge about the position held or for assigning the other position on the same functional path (training courses).



Source: Self-study.

Fig. 8. Qualification requirements for officers' appointment on military posts

Qualification requirements for officers' appointment to various military posts depend on the professional postgraduate degree and qualifying courses, which are shown by the solid line on the right side of the figure. In contrast, training courses are shown in the broken line on the left side of the figure.

The authorities competent to appoint professional soldiers to military positions and to release them from these posts, depending on the rank of the position, are the Minister of National Defence and the chiefs and commanders described in table 4 according to their authority to assign and release professional soldiers to and from positions.

In addition, powers relating to the release of a professional soldier from a position in the military unit in which he held this position and his assignment to another military position in another unit by the authority are shown in Table 4 .

Each time, prior to the appointment of a professional soldier for the military post, the authority with appropriate powers verifies their qualifications, taking into account:

a) job description of the post:

b) the military career path of the corps (specialities group);

c) forms of professional development;

d) qualification requirements of the post;

e) qualifications of a professional soldier;

f) experience, completed forms of professional development and conduct of military service of a professional soldier;

g) directions of the professional soldier's career set out in the evaluation form.

[5] Act of 11 September 2003 *of professional military service*, Dz. U. of 2014. Item. 1414, as amended. d.

Table 4

The authorities competent to appoint professional soldiers to military positions and to release them from these posts

No	Authorities	Appointment Competencies
1	Minister of National Defence	as regards the military positions for Colonels (Captains) and Generals (Admirals), and which is authorised according to separate laws
2	Chief of General Staff of Armed Forces, General Commander of Armed Forces, Operational Commander of Armed Forces, Chief of Support Inspectorate of Armed Forces, Chief of the Military Police, Chief of Armaments Inspectorate of DoD and Chief of Healthcare Inspectorate of DoD	as regards the military positions for Lieutenant Colonels (Commanders) in subordinate military units with reservation of paragraphs 3 and 4
3	Corps Commander, Chancellor of the Military University, Division Commander, Flotilla Commander, Commander of Warsaw Garrison	as regards the military positions for Majors (Lieutenant Commanders) in subordinate military units with reservation of paragraph 4
4	Brigade Commander, Chief of Military Reserve and Mobilisation Staff, Wing Commander, Chancellor of the Military Academy, Regiment Commander, Commanding Officer and Commander in the rank of Lieutenant Colonel	as regards the military positions for Captains (Lieutenants) in subordinate military units with reservation of paragraph 5
5	Director of the National Defence Ministry of the Military Personnel	as regards the military positions for Lieutenant Colonels (Commanders) in other military units not mentioned in paragraphs 2-4, also in units subordinate to Chief of Warsaw Garrison with reservation of paragraph 3

Source: Self-study.

The evaluation systems carried[6] out since 2014 on an annual basis are an important factor in the planning of soldiers' military careers, , under which a direct supervisor summarises the annual conduct of duty of a subordinate soldier by:

1) evaluation of the duties involved;

2) assessment of the powers and predispositions of a soldier:

a) responsibility,

b) determination of purpose,

c) the accuracy and speed of decision-making,

d) resistance to stress,

e) communication and teamwork,

f) adherence to regulations, standards and rules,

g) developing and improving their own skills,

h) attention to equipment and property,

i) manners and attention to appearance;

3) determining the direction of professional development and the identification of training needs of a evaluated soldier.

In the evaluation process, the receipt of a very good or excellence rating on a scale of five ratings in the last official evaluation allows the appointment of officer training at the next highest military position, which may occur depending on vacancies. The period of occupancy of a military position of the same military rank is at least three years. If justified by the needs of the Armed Forces (advisability: dismissal from the post and assignment to the post), this period may be shorter, but no less than two years. Reclassification of a junior officer to the next higher military rank may take place after at least three years in the military rank possessed and receiving an overall evaluation rate of at least very good at the last evaluation. If justified by the needs of the Armed Forces, the period of service in the military rank possessed might be shorter, but no less than two years.

If an active duty officer receives a good rate in the evaluation determining an appointment to the next military position and is appointed to the same or an equivalent post, he is not reclassified to a higher military rank in the occupied post.

If an active duty officer receives a fair rate in the evaluation determining an appointment to the same or an equivalent post, he is not reclassified to a higher military rank in the occupied post

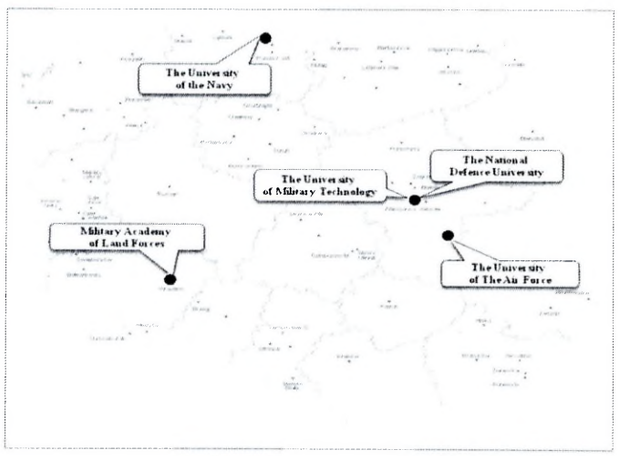
[6] Regulation of the Minister of National Defence on 26 May 2014 *on evaluation of professional soldiers*, Journal of 2014 No. 764.

and can even be dismissed from professional military service (an optional dismissal). Receipt of a poor rate in the evaluation results in dismissal from professional military service (mandatory dismissal).

When considering the formal and legal conditions of the development of logistics officers, the dynamics of changes in the requirements to determine assignment for military posts in the officers' corps should be noted. Officers conducting the appropriate forms of training hold a new position before the qualification courses and before the appointment or after the appointment of development courses.

Trends in the development system of professional logistics officers of the Land Forces

The development system of professional soldiers is conducted by five military universities: The National Defence University, the University of Military Technology, the University of the Navy, the Military Academy of Land Forces and the University of the Air Force.



Source: Self-study.

Fig. 9. The military universities conducting professional development of officers

The professional development of officers, including the logistics officers, is carried out under the provisions of the Decision of the Minister of National Defence No. 420 of 12 September 2008 on the implementation of the Polish Armed Forces training system of professional soldiers[7]. The system of training professional soldiers introduced above consists of two categories:

1) postgraduate qualification courses, preparing to hold a position with a higher rank, whose principal purpose is to update and broaden military knowledge and expertise, as well as the acquisition of powers necessary for carrying out duties at the higher position;

2) development courses, complementary knowledge and preparing to carry out duties at a specific post according to a post's job description.

In addition, the system of development of officers assumes that qualification courses will mainly be implemented in the „functional paths of career" such as commanding staff, support, and specific for positions in various ranks[8].

The Minister of Defence decision of 7 March 2014[9] pointed to the Chief of the General Staff of the Polish Army with responsibility for logistics system by virtue of his official position as an authority possessing the qualifications appropriate to model the course[10] of service for the logistics corps.

The need to prepare logistics officers for carrying out their duties on the following positions taking into account the availability of posts as shown above their distribution, the specifics of the service, new equipment, and the need to change a specialties group points to the need for a set of plans in the officers' development system.

Summary

The main source for taking the first military posts of the officers' corps should be graduates from The University of Military Technology, The University of the Navy and The University of The Air Force[11]. Particular attention should be paid to

[7] Decision No. 420 of the Minister of National Defence on 12 September 2008 on the introduction of the Polish Armed Forces training system for professional soldiers, Journal of 2008 No. 18 pos. 241.

[8] http://www.dnisw.mon.gov.pl (10/02/2015).

[9] Decision No. 76 of the Minister of National Defence of 7 March 2014 *on the indication of persons having qualifications relevant to the corps (groups)*, Journal of 2014 No. 86.

[10] Decision No. 274 of the Minister of National Defence of 4 June 2008 *on models course of service officers and NCOs professional,* Journal of 2008., No. 12, pos. 142.

[11] Ordinance of the Minister of Defence No. 11 dated 6 June 2014 *on establishing conditions and procedure for admissions candidates for professional soldiers to military schools in the academic year 2015/2016*, Journal of 2014, No. 181.

properly identifying the needs of the numbers of graduates (logistics corps) in the coming years, taking into account the implemented organisational changes in the planned transfers of officers to higher positions and the outflow of professional military service (income of graduates correlated with the outflow of officers from professional military service).

The need to improve integration of the development system of logistics officers should be noted. Changes in individual components of the system according to the emerging should be noted and included in the plans and courses of studies to meet the evolving expectations.

The logistics officers' corps, as well as the other seventeen corps, are subject to the same rules of eligibility for appointment to military positions. The main factors for the appointment of the logistics officers to the Land Forces positions are the availability of officers with adequate qualifications. Therefore, special attention should be paid to the proper planning of professional development of the logistics officers' corps, which should take place on the basis of an annually conducted evaluation system and making an annual assessment of military personnel management. The result of the evaluation of military personnel should precisely identify the needs of training in relation to selected logistics officers.

The distribution of the positions of the logistics officers' corps of the Land Forces shown above points to a variety of military positions in specialties groups and ranks, where the largest group is the general logistics group (65%). The development of logistics officers should allow the flow of the officers in positions of the logistics corps in all kinds of Armed Forces and take into account the preparation of officers in ranks of senior officers to change their specialties group.

Bibliography

Act of 21 November 1967 *about the general defence duty of the Republic of Poland,* Journal of 2015, No. 144, as amended. d., Art. 74.

Act of 11 September 2003 *of professional military service*, Dz. U. of 2014. Item. 1414, as amended. d.

Regulation of the Minister of National Defence of 11 December 2009 *on corps, specialties groups and military specialties*, Journal of 2009 No. 216, item. 1678, as amended. d.

Regulation of the Minister of National Defence of 9 September 2014 *on the mode of determination of professional soldiers for the military posts and dismissal from these posts*, Journal of 2014, No. 1292.

Regulation of the Minister of National Defence on 26 May 2014 *on evaluation of professional soldiers*, Journal of 2014 No. 764.

Decision No. 420 of the Minister of National Defence on 12 September 2008 *on the introduction of the Polish Armed Forces training system for professional soldiers*, Journal of 2008 No. 18 pos. 241.

Decision No. 76 of the Minister of National Defence of 7 March 2014 *on the indication of persons having qualifications relevant to the corps (groups)*, Journal of 2014 No. 86.

Decision No. 274 of the Minister of National Defence of 4 June 2008 *on models course of service officers and NCO professionals*, Journal of 2008., No. 12, pos. 142.

Ordinance of the Minister of Defence No. 11 dated 6 June 2014 *on establishing conditions and procedures for admission of candidates for professional soldiers to military schools in the academic year 2015/2016*, Journal of 2014, No. 181.

http://www.dnisw.mon.gov.pl (10/02/2015).

WSPÓŁCZESNE UWARUNKOWANIA ROZWOJU ZAWODOWEGO OFICERÓW KORPUSU OSOBOWEGO LOGISTYKI WOJSK LĄDOWYCH SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Streszczenie

W artykule ukazano czynniki umożliwiające rozwój zawodowy oficerów korpusu osobowego logistyki wojsk lądowych Sił Zbrojnych Rzeczypospolitej Polskiej, istotny dla przygotowania do realizacji zadań w zależności od zmieniających się uwarunkowań współczesnego i przyszłego pola walki. Autor z uwagi na posiadane doświadczenie kadrowe w realizacji zasad pragmatyki kadrowej przedstawia procedury obowiązujące w procesie obsadzania stanowisk służbowych przeznaczonych dla oficerów. W dalszej części omówione zostały uwarunkowania formalno-prawne rozwoju oficerów korpusu osobowego logistyki. Na końcu podjęto próbę określenia kierunków doskonalenia zawodowego oficerów logistyki.

Słowa kluczowe: korpus oficerów logistyki, uwarunkowania formalno-prawne rozwoju oficerów, system rozwoju zawodowego oficerów, kompetencje kadrowe, pragmatyka kadrowa.

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

BEZPIECZEŃSTWO LOTÓW A SZKOLENIE W ZAKRESIE ZARZĄDZANIA ZASOBAMI ZAŁOGI W ZAROBKOWYM PRZEWOZIE LOTNICZYM

dr n. med. Robert GAŁĄZKOWSKI
SP ZOZ Lotnicze Pogotowie Ratunkowe

płk rez. dypl. pil. Mirosław TOMASZEWSKI
SP ZOZ Lotnicze Pogotowie Ratunkowe

Streszczenie

W niniejszej publikacji jej autorzy, na tle zagrożeń dla bezpieczeństwa operacji lotniczych, identyfikują przyczyny narodzin szkoleń realizowanych w zakresie zarządzania zasobami załogi (Crew Resource Management – CRM), definiują ich charakter, istotę i cele. Przedstawiają również, uwarunkowany szeregiem czynników, proces ich ewoluowania, skupiając się na rozwiązaniach przyjętych w zarobkowym przewozie lotniczym na świecie. W ramach tego zagadnienia przedstawiają zasadnicze, charakterystyczne dla kolejnych generacji szkoleń CRM, zmiany w zakresie i w sposobie ich prowadzenia.

Słowa kluczowe: bezpieczeństwo lotów, zarządzanie zasobami załogi, CRM, czynnik ludzki, świadomość sytuacyjna, podejmowanie decyzji, ADM, komunikacja, współpraca w załodze

(...) do powszechnej wiadomości z trudem przebija się myśl, że katastrofy lotnicze zdarzają się z tych samych powodów, co wszystkie inne wypadki spotykające człowieka. Różnica polega na tym, że w lotnictwie banalny błąd może mieć tragiczne następstwa.

David BEATY

Wstęp

Jak wskazują liczne doświadczenia oraz wyjątkowo bogata w tym zakresie literatura przedmiotu, człowiek, z jego możliwościami i ograniczeniami, od zarania lotnictwa stanowi najsłabsze ogniwo w układzie pilot – statek powietrzny. Niestety, w dobie dynamicznego postępu technologicznego i nieprzerwanie rozwijającego się przemysłu lotniczego, także w lotnictwie ukierunkowanym na zarobkowy przewóz lotniczy, problem ten wciąż nie znajduje rozwiązania. Według danych opublikowanych przez Aircraft Crashes Record Office (ACRO)[1], dla 2,51% ogólnej liczby zdarzeń lotniczych nie udało się określić ich przyczyny, sabotaż jako przyczyna zdarzenia lotniczego stanowi 3,25% ogólnej liczby zdarzeń, warunki atmosferyczne są przyczyną 5,95% ogólnej liczby zdarzeń, niesprawności techniczne to przyczyna 20,72% ogólnej liczby zdarzeń i wreszcie błąd człowieka, określany mianem „czynnik ludzki", to niestety przyczyna aż 67,57% ogólnej liczby zdarzeń lotniczych[2].

Zobrazowanie ogromnej wagi czynnika ludzkiego, jako głównej przyczyny zaistniałych zdarzeń lotniczych, nastąpiło stosunkowo późno, bo dopiero w późnych latach siedemdziesiątych XX wieku. Wówczas to, w czerwcu 1979 roku, na konferencji zorganizowanej przez National Aeronautics Space Administration (NASA)[3], jej organizatorzy opierając się na wynikach badań kilkuset zdarzeń lotniczych, wskazali na konieczność określenia i wdrożenia działań naprawczych ukierunkowanych na przeciwdziałanie skutkom

[1] Aircraft Crashes Record Office (ACRO), organizacja pozarządowa z siedzibą w Genewie, kompiluje dane statystyczne dotyczące wypadków lotniczych.

[2] Dane dotyczą wyłącznie statków powietrznych zdolnych do przewozu więcej niż sześciu osób, z wyłączeniem samolotów bojowych, śmigłowców i balonów. Według: http://www.baaa-acro.com/.

[3] George E. Cooper, Maurice D. White, John K. Lauber. "Resource Management on the Flight Deck". Proceedings of a NASA/Industry Workshop Held at San Francisco, California, June 26–28, 1979, NASA Conference Publication 2120.

braku umiejętności współpracy w załodze, braku umiejętności oceny sytuacji w powietrzu i braku umiejętności podejmowania właściwych decyzji. Konferencja poświęcona w całości zagadnieniom i psychologicznym aspektom zarządzania zasobami w kokpicie pilotów nie wskazywała gotowych rozwiązań. Uświadamiała jej uczestnikom i całemu środowisku lotniczemu problem istotny dla bezpieczeństwa operacji lotniczych, który dopiero z ich udziałem mógł znaleźć rozwiązanie. Przyjmuje się, że konferencja NASA z 1979 roku, a przede wszystkim działania będące jej pokłosiem, zaowocowały narodzinami szkolenia lotniczego, które w świecie lotniczym określa się jako Zarządzanie Zasobami Załogi (Crew Resorce Management – CRM).

Od tego czasu, dla uzyskania jak najwyższej efektywności szkoleń CRM, władze i operatorzy lotniczy poszukują programów, metod i technik szkoleń, które w połączeniu z możliwymi do wykorzystania narzędziami wspomagającymi proces edukacji spowodują, że czynnik ludzki, w przeważającej liczbie raportów komisji badających zdarzenia lotnicze, przestanie być wskazywany jako zasadnicza przyczyna ich wystąpienia.

Celem niniejszego opracowania jest zobrazowanie procesu ewaluowania szkoleń CRM w zarobkowym przewozie lotniczym na świecie. Wskazanie ich istoty, celu oraz znaczenia w systemie szkoleń lotniczych realizowanych dla poprawy bezpieczeństwa lotów.

Istota i cele szkoleń CRM

Narodziny nowego rodzaju szkoleń, traktujących o „czynniku ludzkim", w żadnym razie nie deprecjonowały i w dalszym ciągu nie deprecjonują znaczenia szkoleń ukierunkowanych na zdobycie przez personel latający specjalistycznej wiedzy lotniczej, w tym wiedzy niezbędnej do bezpiecznego pilotowania danego typu statku powietrznego, w strukturze i według standardów określonych przez danego (oferującego określony zakres usług) operatora lotniczego. Istotą szkoleń CRM w lotnictwie jest połączenie powyższej wiedzy z wiedzą i umiejętnością wykorzystania, w stopniu maksymalnym, wszelkich dostępnych dla załogi zasobów, w tym również umiejętności poznawczych i interpersonalnych poszczególnych jej członków, tak w sytuacjach normalnych, jak i przede wszystkim, w sytuacjach ekstremalnych zaistniałych na pokładzie statku powietrznego.

W tym znaczeniu umiejętności poznawcze rozumiane są jako procesy myślowe wykorzystywane w celu nieprzerwanej, właściwej analizy i oceny sytuacji (świadomość sytuacyjna) oraz w celu podejmowania właściwych decyzji w każdym etapie lotu i w każdej (normalnej, nienormalnej, awaryjnej) sytuacji na pokładzie statku powietrznego. Umiejętności interpersonalne zaś, rozumiane są jako umiejętności odpowiedzialne za jakość komunikacji w załodze, który przekłada się bezpośrednio na efektywność (bądź jej brak) pracy w zespole określanym mianem załogi statku powietrznego. Jakkolwiek, w czasie poprzedzającym włączenie szkoleń CRM do systemu szkoleń lotniczych, pojęcia świadomości sytuacyjnej, planowania i podejmowania decyzji czy też komunikacji i współpracy w załodze nie były w środowisku lotniczym pojęciami obcymi, to jednak oferowane w ramach szkoleń CRM nowe spojrzenie na zależności zachodzące między nimi nadały im nowego, szczególnego dla bezpieczeństwa wykonywania operacji lotniczych, znaczenia.

Świadomość sytuacyjna – W literaturze przedmiotu znaleźć można wiele jej definicji.

Z zasady, w swym przesłaniu są one do siebie bardzo zbliżone, a ich różnorodność podyktowana jest, przede wszystkim, specyfiką środowiska do którego dana definicja jest adresowana. Najbardziej uniwersalną i jednocześnie najbardziej powszechną w środowisku lotniczym jest propozycja definicji autorstwa Dr. Mica R. Endsleya[4], według którego *świadomość sytuacyjna, to postrzeganie elementów otaczającego nas środowiska w określonym czasie i przestrzeni, rozumienie ich znaczenia oraz przewidywanie konsekwencji z nich płynących w najbliższej przyszłości*[5].

W budowaniu świadomości sytuacyjnej (tworzeniu indywidualnego obrazu otaczającej nas

[4] Dr. M.R. Endsley, uznawany za światowego lidera w badaniach i stosowaniu świadomości sytuacyjnej w systemach zaawansowanych. Autor ponad 200 publikacji na temat świadomości sytuacyjnej, najczęściej cytowany w naukowych i profesjonalnych czasopismach zajmujących się problematyką świadomości sytuacyjnej.

[5] Tłumaczenie własne: *Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." "Toward a Theory of Situation Awareness in Dynamic Systems,* Human Factors. The Journal of the Human Factors and Ergonomics Society, March 1995.

rzeczywistości) zasadnicze znaczenie ma nasza percepcja, rozumiana jako zdolność do odbierania (za sprawą posiadanych zmysłów) bodźców zewnętrznych, ich rozpoznawania, interpretowania i reagowania na nie. Według znawców literatury przedmiotu uzupełnieniem do tak budowanej świadomości sytuacyjnej jest również bagaż życiowych doświadczeń oraz wpływy kulturowe i społeczne[6]. Innymi słowy, wykorzystując swoje zmysły, doświadczenie, posiadaną wiedzę, obserwując w sposób ciągły i rozumiejąc to, co się wokół nas działo chwilę wcześniej, co dzieje się obecnie i przewidując, co może wydarzyć się w najbliższej przyszłości, jesteśmy w posiadaniu świadomości sytuacyjnej, a więc – panujemy nad sytuacją. W każdym momencie jej trwania jesteśmy w stanie zaplanować swoje dalsze działanie, przewidzieć jego skutki i w konsekwencji podjąć decyzję o realizacji danego, bądź o wyborze innego sposobu działania.

W życiu codziennym, wykorzystując posiadaną świadomość sytuacyjną, podejmujemy mniej lub bardziej trafne decyzje niezliczoną ilość razy. Należy jednak mieć na względzie fakt, iż w życiu codziennym skutki błędnych decyzji zazwyczaj nie bywają katastrofalne. Niestety konsekwencją błędnej decyzji pilota, w skomplikowanym obszarze działalności lotniczej, najczęściej jest utrata życia załogi i pasażerów. Według badań prowadzonych przez Australian Transportation Safety Board (ATSB), w 85% wszystkich zbadanych zdarzeń lotniczych, gdzie jako przyczynę ich zaistnienia wskazano „czynnik ludzki", mówi się o utracie świadomości sytuacyjnej. Potwierdzeniem powyższych danych są efekty analiz zdarzeń lotniczych z udziałem śmigłowców przeprowadzonych przez European Helicopter Safety Analysis Team (EHSAT). Według ustaleń EHSAT, 84 na 202 zaistniałe zdarzenia lotnicze związane były z częściowym lub całkowitym brakiem świadomości sytuacyjnej[7].

W trakcie wykonywania zadania lotniczego, dla właściwej oceny sytuacji, pilot oprócz posiadanej wiedzy i doświadczenia czerpie szereg informacji obserwując przestrzeń wokół statku powietrznego, wykorzystuje dostępne wyposażenie awioniczne statku powietrznego, korzysta z informacji uzyskanych drogą radiową od naziemnych służb ruchu lotniczego lub od innych użytkowników przestrzeni powietrznej. Natłok informacji lub jej brak albo niezrozumienie choćby jednej, za to niezbędnej w kluczowym dla prawidłowej oceny sytuacji momencie, generuje błąd lub łańcuch błędów. Należy przy tym pamiętać również o tym, że niewiedza, zmęczenie, stres, brak skupienia na zadaniu, znudzenie, rozluźnienie, lekceważenie sygnałów ostrzegawczych czy też nadmierne pobudzenie lub euforia, potęgują prawdopodobieństwo powstania ciągu niekorzystnych zdarzeń.

W aspekcie świadomości sytuacyjnej, celem szkoleń CRM jest uzmysłowienie szkolonym jej ogromnego znaczenia dla bezpieczeństwa wykonywanych operacji lotniczych. Ważne jest również wskazanie mechanizmu budowania świadomości sytuacyjnej oraz zagrożeń skutkujących jej częściową lub całkowitą utratą. Co jednak z punktu widzenia CRM najistotniejsze, to uświadomienie dowódcom statków powietrznych istnienia zasobu, który w procesie utrzymania świadomości sytuacyjnej, w każdym momencie trwania lotu, pozostaje w gotowości do wykorzystania. Zasobu, którym są pozostali członkowie ich załóg.

Podejmowanie decyzji – W teorii i praktyce zarządzania to proces polegający na zbieraniu i przetwarzaniu informacji o przyszłym działaniu, sama zaś decyzja definiowana jest jako świadomy, nielosowy wybór jednego z rozpoznawanych i uznanych za możliwe wariantów przyszłego działania. Kategoryzując decyzje ze względu na ilość informacji i warunki, w jakich decyzje podejmujemy, możemy podzielić je na[8]:

- decyzje podejmowane w warunkach pewności (w sytuacjach, w których możemy bezbłędnie przewidzieć ich efekty);
- decyzje podejmowane w warunkach ryzyka (w sytuacjach, w których możemy określić zbiór konsekwencji i przyporządkować im pewne prawdopodobieństwo wystąpienia);
- decyzje podejmowane w warunkach niepewności (w sytuacjach, w których nie możemy zidentyfikować wszystkich konsekwencji ani też określić z jakim prawdopodobieństwem wystąpią).

Mając na względzie skalę niepożądanych konsekwencji jakie w lotnictwie mogą zaistnieć

[6] Według: *CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES).* UK Civil Aviation Authority, 2006.

[7] Według: S. Burigan. *Situational awareness – staying ahead of the aircraft.* AirRescue, International Air Rescue & Air Ambulance Magazine, Vol.2/2012, 33–37.

[8] A.K. Koźmiński, W. Piotrowski. *Zarządzanie. Teoria i Praktyka.* PWN, Warszawa 2002; M. Kostera. *Podstawy organizacji i zarządzania,* WSPiZ, Warszawa 2001.

w wyniku podjęcia błędnej decyzji, proces szkolenia i przygotowania personelu lotniczego (niezależnie od charakteru lotnictwa, jego przeznaczenia i zadań) skupiony jest na maksymalnie możliwym wyeliminowaniu sytuacji, w których decyzje podejmowane będą w warunkach ryzyka bądź niepewności. Stąd, między innymi, w działalność lotniczą wdraża się szereg standardów (standaryzacje czynności załogi w określonych operacjach, standardowe procedury operacyjne, standardowe procedury odlotów i przylotów, listy kontrolne na potrzeby sytuacji normalnych, nienormalnych i awaryjnych itp.), które proces decyzyjny mają uczynić procesem w zdecydowanej mierze automatycznym, podświadomym, opartym na posiadaniu szeroko pojętej wiedzy lotniczej, doświadczeniu, ale przede wszystkim, na znajomości i zastosowaniu w praktyce ustalonych schematów zachowań.

Dlaczego więc, mimo rozumienia istoty problemu i takiej skali działań prewencyjnych, wypadki lotnicze z winy częściowej lub całkowitej utraty świadomości sytuacyjnej i w konsekwencji tego – błędnej decyzji, wciąż się zdarzają?

Zapewne dlatego, że jak powiedziano wcześniej, lotnictwo jest środowiskiem bardzo skomplikowanym, w którym bardzo duży przepływ informacji i bardzo duża ilość zmiennych (zmiany w sytuacji meteorologicznej, w sytuacji nawigacyjnej, w ruchu lotniczym, nieprzewidziane ciągi sytuacji awaryjnych itp.) powodują, iż możliwych do wystąpienia zagrożeń jest nieskończenie wiele, a jeśli tak, to niemożliwym jest przewidzieć je wszystkie, opisać i ująć w ramy standardowych zachowań załogi.

Jak więc ten problem rozwiązać?

W literaturze przedmiotu szeroko podejmowanym zagadnieniem jest temat procesów decyzyjnych pilotów w ich typowym, skomplikowanym środowisku działalności lotniczej (Aeronautical Decision Making – ADM). Co w tym najistotniejsze, to analizowanie i postrzeganie tychże procesów, przede wszystkim poprzez pryzmat indywidualnych postaw ludzkich, w tym głównie ich umiejętności oceny ryzyka i umiejętności zarządzania stresem.

Według znawców tejże problematyki, żeby zrozumieć ADM należy rozumieć jakie jest znaczenie tych postaw w procesie podejmowania decyzji, ale co więcej, jak dla zwiększenia bezpieczeństwa wykonywanej operacji lotniczej postawy te można modyfikować. Żeby zrozumieć ADM ważne jest również rozumienie czynników, które warunkują podejmowanie takich, a nie innych decyzji. Oprócz wiedzy, jak proces ten przebiega, nie mniej ważną jest wiedza, jak proces ten można poprawić[9].

W aspekcie procesów decyzyjnych, w szkoleniach CRM szczególny nacisk kładzie się na świadomość potrzeby i zrozumienie zasadności włączenia wszystkich członków załogi w proces decydowania w locie. Jak wskazuje teoria CRM, żeby wykorzystanie członków załogi było efektywne, konieczne jest ich zapoznanie z planem lotu i zamiarem jego realizacji przez dowódcę statku powietrznego już na etapie przygotowania do lotu. Co więcej, istotnym jest również systematyczne informowanie załogi o statusie lotu, o zmianach zaistniałych w założonym planie lotu oraz o związanych ze zmianami intencjach dowódcy[10].

W powyższym układzie świadomość sytuacyjna, kluczowa dla podjęcia właściwej decyzji, przestaje być wyłącznie świadomością sytuacyjną dowódcy. Posiadanie pełnej świadomości sytuacyjnej w załodze to zasób, który dla podjęcia najlepszej decyzji, szczególnie w sytuacji krytycznej i w deficycie czasu, może i powinien być przez dowódcę wykorzystany.

Jak wskazują liczne doświadczenia i obserwacje, zakres udziału załogi w procesie decyzyjnym zależy w dużym stopniu od kultury organizacyjnej i obowiązujących w danym środowisku norm społecznych. W kulturach i środowiskach, gdzie mimo szacunku dla autorytetu dowódcy dopuszcza się możliwość zastosowania demokratycznego stylu kierowania zespołem, wyżej proponowana teoria CRM ma pełne szanse powodzenia. W kulturach i środowiskach, w których autorytet dowódcy stanowi wartość nadrzędną, preferowany będzie autokratyczny model zarządzania[11]. W takich kulturach i środowiskach demokratyczne kierowanie działaniami załogi i wykorzystanie tkwiącego w niej potencjału postrzegane będzie jako oznaka

[9] Według: *Pilot's Handbook of Aeronautical Knowledge*. U.S. Department of Transportation, Federal Aviation and Administration, Flight Standard Service, 2008, Chapter 17 "Aeronautical Decision Making", 17–2.

[10] Według: *CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES)*. UK Civil Aviation Authority, 2006.

[11] Klasyfikacji stylów kierowania według Kurta Lewina, Ronalda Lipitta i Ralpha K. White'a.

słabości dowódcy, stąd zastosowanie teorii CRM, niestety, będzie zdecydowanie trudniejsze. Żeby jednak i temu stylowi zarządzania oddać sprawiedliwość należy mieć na uwadze fakt, iż jakkolwiek teoria CRM, z jednej strony, wskazuje na korzyści płynące z udziału członków załogi w procesie decyzyjnym dowódcy, to z drugiej strony, mówi również o tym, że istnieją sytuacje, w których autokratyczny styl zarządzania jest absolutnie pożądany, bo w danej, konkretnej sytuacji będzie najefektywniejszy[12].

Komunikacja – Według definicji słownikowej pojęcie komunikacji ma swój rodowód łaciński (communico, commucicare) i oznacza „czynić coś wspólnym, połączyć, udzielić komuś wiadomości, naradzić się"[13].

Z procesem komunikowania mamy do czynienia w każdym elemencie codziennego życia człowieka i powszechnie rozumiemy ten proces jako przekazywanie informacji pomiędzy jej nadawcą i odbiorcą. Żeby proces ten okazał się skutecznym, rolą nadawcy jest, korzystając z werbalnych i niewerbalnych nośników informacji, sformułowanie komunikatu tak, aby był zrozumiały dla odbiorcy, zaś rolą odbiorcy jest jego odkodowanie i co więcej, korzystając z tych samych nośników, przesłanie informacji zwrotnej do nadawcy o zrozumieniu bądź braku zrozumienia przesłanego komunikatu. Innymi słowy, komunikowanie, to podejmowana w określonym kontekście wymiana werbalnych i niewerbalnych sygnałów w celu osiągnięcia lepszego poziomu współdziałania[14]. Co za tym idzie, niewłaściwe formułowanie informacji lub użycie niewłaściwych (bądź niewłaściwie) jej nośników skutkować będzie brakiem możliwości jej poprawnego zrozumienia, a to z kolei przełoży się na brak efektywności działania, szczególnie podczas pracy w grupie.

Niewłaściwe formułowanie informacji lub użycie niewłaściwych (bądź niewłaściwie) jej nośników, to niestety nie jedyne przyczyny złej komunikacji, szczególnie wśród członków załóg statków powietrznych. Musimy bowiem pamiętać o uwarunkowaniach środowiska, w jakim wykonują oni swoje obowiązki.

Związane ze środowiskiem pracy załóg czynniki, które w najlepszym razie utrudniają, w najgorszym zaś razie prowadzą do poważnej degradacji poziomu komunikacji w załodze statku powietrznego, to przede wszystkim nieustający hałas oraz nieprzerwany potok różnorodnych (wizualnych i dźwiękowych) informacji płynących ze wskaźników urządzeń i systemów statku powietrznego.

Analizując problem komunikacji w szerszym aspekcie, uwzględniając relacje załoga statku powietrznego – służby ruchu lotniczego, wachlarz negatywnych dla komunikacji czynników poszerza się. Jakkolwiek nie można sytuacji takich uogólniać, tym bardziej przypisywać im miana reguły, to jednak otrzymywane drogą radiową informacje bywają często zakłócone, sprzeczne, niekompletne, niejednoznaczne lub niewiarygodne.

Nie sposób przy tym pominąć kwestii związanych z barierą językową, występującą zarówno w komunikacji wśród członków danej załogi, jak i między załogą a służbami ruchu lotniczego. Różny poziom znajomości języka angielskiego (szczególnie nieproceduralnego), akcent, żargon, czy wymagające w tej sytuacji szczególnego podkreślenia, różnice kulturowe, mogą być przyczyną różnego interpretowania odbieranych informacji. Komplement może być uznany za zniewagę a niewinny żart odebrany jako afront[15]. Nakładając na klasyczne warunki pracy załogi statku powietrznego, postępujące z każdą minutą lotu, znużenie i zmęczenie, tworzymy obraz sytuacji, w której poprawne, właściwe, komunikowanie się, zdaje się być naprawdę dużym wyzwaniem.

Z pewnością praca nad właściwą komunikacją, tak w załodze, jak i pomiędzy załogą a służbami ruchu lotniczego, jest przedsięwzięciem wymagającym rozwiązań na wielu płaszczyznach. Jest też z pewnością przedsięwzięciem trudnym, złożonym i niestety ciągłym. Ze względu jednak na znaczenie dobrej komunikacji dla bezpieczeństwa wykonywanych zadań lotniczych, jest przedsięwzięciem, ze wszech miar, potrzebnym.

To, co wydaje się kluczowe w szkoleniach CRM w aspektach dotyczących komunikacji, to przede wszystkim zrozumienie przez szkolonych tragicznych (najczęściej) konsekwencji jej braku w pracy załogi lotniczej. To także zrozumienie przez nich konieczności postrzegania dobrej komunikacji jako warunku decydującego o właści-

[12] Według: O. Truszczyński, M. Biernacki. *Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych.* Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

[13] *Słownik łacińsko-polski.* PWN, Warszawa 1973, s. 101.

[14] Według: Z. Necki. *Komunikacja międzyludzka.* Wyd. Profesjonalnej Szkoły Biznesu, Kraków 1996, s. 109.

[15] Według: R. Baron. *Barriers to Effective Communication: Implications for the Cockpit.* http://airlinesafety.com.

wym, efektywnym wykorzystaniu zasobów jakimi dysponują podczas lotu, szczególnie w sytuacjach nienormalnych i awaryjnych. To wreszcie rozumienie, że niewłaściwa komunikacja może sytuacje te wręcz wywoływać.

Co wymaga podkreślenia – w efekcie szkoleń CRM nie oczekuje się od załóg rozwiązywania wszystkich zidentyfikowanych i przeanalizowanych problemów właściwych dla procesu komunikowania się. Usunięcie wszystkich barier skutecznego komunikowania się nie leży bowiem w możliwościach załogi lotniczej. Żadnego wpływu załoga nie może mieć na hałas, wibracje, zakłócenia w łączności radiowej itp. To oczywiście domeny działalności innych specjalistów branży lotniczej. Z pewnością jednak załoga ma wpływ na wszystkie te elementy komunikacji interpersonalnej, które pozwolą każdemu z jej członków być dobrze przez pozostałych zrozumianym. Elementy, o których mowa, to przede wszystkim umiejętność zadawania pytań, umiejętność słuchania, umiejętność argumentowania wyrażanych opinii, umiejętność rozwiązywania konfliktów czy umiejętność wyrażania konstruktywnej krytyki[16]. Rozumienie ich znaczenia i nieustająca praca w ich doskonaleniu z pewnością służyć będą poprawie poziomu komunikacji w załodze, a co za tym idzie, służyć będą poprawie bezpieczeństwa wykonywanych operacji lotniczych

Współpraca w załodze – Współpraca według definicji encyklopedycznej to zdolność tworzenia więzi i współdziałania z innymi, umiejętność pracy w grupie na rzecz osiągania wspólnych celów. To również umiejętność zespołowego wykonywania zadań i wspólnego rozwiązywania problemów[17].

W literaturze przedmiotu tematyce współpracy, współdziałania czy tematyce pracy zespołowej towarzyszy niezmiennie pojęcie synergii, a ściślej – efektu synergii. Zgodnie z jego ogólnie przyjętym rozumieniem, to efekt zorganizowanego działania grupy ludzi, który jest większy (wyższy, lepszy) niż suma efektów działań realizowanych indywidualnie przez członków tejże grupy. Innymi słowy, efekt pracy, na który złoży się suma wysiłków pojedynczych elementów, będzie zawsze mniejszy od efektu pracy tych samych elementów zebranych w grupę.

Czy jednak praca w grupie zawsze będzie gwarantem lepszych efektów w pracy?

Niestety, nie zawsze. Dla osiągnięcia efektu synergii sam fakt pracy w grupie nie wystarczy. Dla jego osiągnięcia bowiem potrzeba woli współpracy ze strony każdego z tworzących ją elementów oraz wzajemnej interakcji pomiędzy członkami tej grupy. Nie zaistnieje ona z kolei, jeśli jej członkowie nie będą się z nią utożsamiać, nie będą rozumieć swojej w niej roli, nie będą zdeterminowani do jak najlepszego wykonanie zadania, czy wreszcie, nie będą poczuwać się do odpowiedzialności za efekty pracy grupy, którą tworzą.

Z powyższego wynika, że zdecydowanie większe szanse na efektywne działanie będzie mieć grupa osób dobrze sobie znanych, „obytych" ze sobą. Grupa osób, które doskonale rozumieją i wykorzystują we wzajemnej komunikacji również język ciała, które znają zarówno własne jak i pozostałych jej członków możliwości i ograniczenia.

Niewątpliwie tak „stworzona" grupa będzie pracować lepiej, sprawniej, efektywniej niż każda inna. Gdyby jednak zasadę tworzenia stałych zespołów chcieć wdrożyć do zasad funkcjonowania operatorów lotniczych, okaże się, że z racji uwarunkowań organizacyjnych, nie zawsze możliwe będzie jej spełnienie. Z reguły więc załogi statków powietrznych nie będą składać się z osób „obytych" ze sobą w stopniu wyżej opisanym.

Z tego też względu tak wiele uwagi poświęca się tworzeniu wszelkiego rodzaju standaryzacji zachowań załogi. Z tego również względu coraz więcej uwagi poświęca się problematyce kultury organizacyjnej, aktywnie promującej w swojej działalności dobrze pojmowane zasady wykorzystania zasobów załogi. Ważną rolę przypisuje się przy tym czynnikom tworzącym pozytywną atmosferę w pracy załogi lotniczej.

Towarzysząca pracy grupowej atmosfera, w literaturze przedmiotu określana często terminem „klimatu emocjonalnego", w swej istocie odnosi się do sposobu, w jaki pracujący w zespole ludzie postrzegają („czują") siebie i innych podczas realizowania wspólnych zadań. Według publikowanych wyników badań prowadzonych w tym obszarze, czynnikami warunkującymi zaistnienie pozytywnego klimatu emocjonalnego w załodze, w odniesieniu do każdego z jej członków, jest

[16] Według: O. Truszczyński, M. Biernacki. *Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych.* Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

[17] Według: www.pl.wikipedia.org

przede wszystkim jasność i zrozumienie zadania, chęć uczestnictwa i możliwość pełnego zaangażowania się w jego realizację, przejrzystość oczekiwań dowódcy i pozostałych członków załogi, ich uznanie dla podejmowanych wysiłków, dobra komunikacja, możliwość swobodnego wypowiadania się i co bardzo istotne – jednakowe dla wszystkich postrzeganie kwestii bezpieczeństwa[18].

Ogromną rolę w tworzeniu pozytywnego klimatu emocjonalnego w załodze odgrywa postawa kapitana – dowódcy załogi lotniczej. Mający problemy z komunikacją interpersonalną, wyniosły i oschły kapitan nigdy takiego klimatu nie stworzy. Nie stworzy go również kapitan nie przygotowany do wykonania zadania. Jego zdenerwowanie wynikające z niewiedzy bądź niewystarczającego przygotowania się do lotu najprawdopodobniej przełoży się na problemy w komunikowaniu się z załogą, problemy ze świadomością sytuacyjną i problemy z podejmowaniem decyzji. Załoga zdefiniuje natychmiast taką sytuację, jako sytuację, w której szanse na powstanie pozytywnej „chemii" w ich pracy, w pracy ich zespołu, są znikome.

Z drugiej strony, wystarczy, że przygotowany do wykonania zadania kapitan, świadomy znaczenia pozytywnego klimatu emocjonalnego we własnej załodze, prosząc służby ruchu lotniczego o np. instrukcje do kołowania, zamiast formuły *„proszę"* użyje formuły *„prosimy o instrukcje do kołowania"*[19]. Znaczenie komend radiowych pozostaje w istocie tożsame, z tą jednak różnicą, że dla tak czułej na zachowanie lidera załogi, jaką jest załoga lotnicza, będzie to wystarczający komunikat, aby postawę kapitana odebrać jako jednoznaczne zaproszenie do współuczestnictwa i współodpowiedzialności za realizację zadania.

W aspekcie współpracy w załodze, celem szkoleń CRM jest przede wszystkim wskazanie szkolonym szeregu uwarunkowań decydujących o uzyskaniu efektu synergii w pracy zespołu, jakim jest załoga lotnicza. Wiedza i świadomość o prawach i zależnościach właściwych dla pracy w załodze, a co ważniejsze, zastosowanie tej wiedzy w praktyce, niewątpliwie zwiększy efektywność jej działań. Większa z kolei efektywność, to większe bezpieczeństwo wykonywanych operacji lotniczych. Wspólnym celem w pracy załogi lotniczej jest bezpieczne wykonanie lotu. Aby prawdopodobieństwo bezpiecznego wykonania lotu było największe, załoga powinna współpracować na maksymalnie możliwym do uzyskania poziomie. Taki poziom współpracy nigdy nie będzie miał szansy zaistnienia, jeśli wiedza ta nie będzie wiedzą powszechną, a co ważniejsze, nie będzie powszechnie stosowana.

Co przy tym bardzo istotne, jakkolwiek kluczowe znaczenie w uzyskaniu pożądanego efektu synergii w następstwie współpracy w załodze lotniczej przypisuje się postawie kapitana, to jednak ważnym jest uświadomienie szkolonym, iż do jego uzyskania konieczną jest właściwa postawa każdego z członków załogi.

Ewolucja szkoleń CRM w zarobkowym przewozie lotniczym na świecie

Jak wskazano wcześniej, za miejsce, czas i okoliczności narodzin idei szkoleń CRM przyjmuje się zorganizowaną w USA, w roku 1979, konferencję National Aeronautics Space Administration (NASA), podczas której w sposób kompleksowy zaprezentowano wyniki badań wypadków lotniczych, jednoznacznie wskazujących na zależność bezpieczeństwa operacji wykonywanych z użyciem statków powietrznych od umiejętności poznawczych i interpersonalnych członków ich załóg.

Jak również wcześniej powiedziano, organizatorzy przedmiotowej konferencji podejmując się próby zdefiniowania ogromnego dla lotnictwa problemu, nie wskazali gotowych sposobów na jego rozwiązanie. Sama jednak inicjatywa i unaoczniona uczestnikom konferencji waga problemu wystarczyła, aby władze, organizacje i przewoźnicy lotniczy podjęli działania skutkujące poszukiwaniem, pozyskiwaniem, opracowywaniem i wdrażaniem programów szkoleniowych ukierunkowanych na poprawę interpersonalnych aspektów współpracy w załogach lotniczych[20].

Wymaga przy tym podkreślenia fakt, że od roku 1979 do dnia dzisiejszego, tak programy

[18] Według: *CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES).* UK Civil Aviation Authority, 2006.

[19] Przywołana komenda radiowa jest komendą przykładową użytą dla potrzeb niniejszego artykułu i nie jest komendą zaczerpniętą z obowiązującej frazeologii lotniczej.

[20] Według: O. Truszczyński, M. Biernacki. *Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych.* Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

szkoleń, jak i postrzeganie zakresu czy wręcz celowości ich wdrażania, ewoluowały w lotniczym świecie w sposób niejednokrotnie bardzo różny.

Pierwszymi, którzy podjęli się próby stworzenia przejrzystego modelu ewolucji szkoleń CRM byli amerykańscy naukowcy Robert L. Helmreich, Ashleigh C. Merritt i John A. Wilhelm. W opublikowanym w roku 1999 materiale „The Evolution of Crew Resource Management Training in Commercial Aviation" zdefiniowali pięć kolejnych generacji szkoleń CRM wskazując na istotne dla każdej z nich cechy charakterystyczne[21].

Generacja pierwsza – Cockpit Resource Management

Do opracowania pierwszych programów szkoleń CRM[22] wykorzystano specjalistów, których zasadniczą dotąd dziedziną działalności było przygotowywanie programów szkoleniowych ukierunkowanych na zwiększenie skuteczności pionu zarządzającego w firmach i koncernach funkcjonujących poza branżą stricte lotniczą.

Charakterystyczną cechą tych szkoleń była, przede wszystkim, ich mocno zarysowana formuła psychologiczna, przejawiająca się w prezentowaniu szkolonym ogólnych definicji związanych z przywództwem oraz zajęciami wypełnionymi testami i ćwiczeniami psychologicznymi, z reguły, niezwiązanymi ze specyfiką pracy w lotnictwie.

Zapewne z tego właśnie względu, pomimo ogólnej akceptacji tego rodzaju szkoleń w społeczności lotniczej, część pilotów odbierała je głównie jako próbę manipulowania ich osobowością.

Co jednak istotne, już w pierwszej generacji szkoleń CRM, szczególną uwagę zwracano na zdefiniowanie charakterystycznych stylów zarządzana w kokpicie statku powietrznego. Co więcej, podkreślano i wskazywano na potrzebę korygowania indywidualnych zachowań członków załóg lotniczych w kierunku rozwiązania, wszechobecnego w owym czasie, problemu niskiego poziomu asertywności pierwszych oficerów i autorytarnego stylu zarządzania doświadczonych kapitanów[23].

Niebagatelną korzyścią wynikającą z realizacji szkoleń pierwszej generacji było również ogólne przekonanie o potrzebie cyklicznego ich organizowania oraz o włączeniu symulatorów lotniczych do programów szkoleń CRM, wszędzie tam gdzie jest to tylko możliwe,.

Generacja druga – Crew Resource Management

Podobnie jak w przypadku generacji pierwszej, impulsem do szerszego postrzegania nowego rodzaju szkoleń była kolejna, poświęcona zagadnieniom CRM, konferencja National Aeronautics Space Administration (NASA), zorganizowana dla branży lotniczej w roku 1986.

Jak się okazało w jej trakcie, kilkuletni zaledwie okres realizacji szkoleń według powstałej w 1979 roku idei, pozwolił przewoźnikom lotniczym na wyciągnięcie i zgłoszenie szeregu istotnych wniosków. Jednym z głównych postulatów podnoszonych przez uczestników konferencji była zmiana w traktowaniu szkoleń CRM. Odbierane dotąd jako szkolenia z gruntu „nie te lotnicze", miały przestać być szkoleniami o specyficznym i wyjątkowym charakterze, które zwykle organizowano i realizowano w oderwaniu od innych szkoleń personelu latającego. Odtąd miały zająć stałe miejsce w przyjętym już systemie szkoleń lotniczych.

Co więcej, według nowego widzenia tego rodzaju szkoleń, ich zakresem należało objąć wszystkich członków stanowiących załogę statku powietrznego nie ograniczając się, jak dotąd, wyłącznie do kokpitu pilotów. Stąd też, w tym właśnie okresie, zmiana nazwy szkoleń CRM z Zarządzania Zasobami Kokpitu (Cockpit Resource Management – CRM), na funkcjonującą do dnia dzisiejszego nazwę – Zarządzanie Zasobami Załogi (Crew Resource Management – CRM).

Charakterystycznym dla drugiej generacji szkoleń CRM był także ich modułowy układ. Na zorientowane na naturalne środowisko pracy załogi statku powietrznego seminaria, składały się, przede wszystkim, moduły szkoleniowe poświęcone zagadnieniom budowania zespołu, świadomości sytuacyjnej i zarządzania stresem. Zasadniczym celem prowadzonych wówczas szkoleń było wypracowanie pożądanej strategii podejmowania decyzji oraz umiejętność zrywania łańcucha błędów popełnianych w zarządzaniu zasobami załogi.

Jakkolwiek jednak generalne założenia szkoleń CRM drugiej generacji znalazły swe odzwier-

[21] Według: E. Danecka-Łatka. *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy.* Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

[22] Pierwszy kompleksowy program szkoleń CRM został wdrożony w United Airlines w roku 1981. Według: E. Danecka-Łatka. *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy.* Problemy Zarządzania, vol. 9, nr 4, Wydział Zarządzania UW.

[23] Zjawisko tzw. kapitanozy, polegające na obawie pierwszych oficerów przed podważeniem autorytetu dowódcy. Według: http://www.lotnictwocywilne.republika.pl/crm.html.

ciedlenie w programach szkoleń wielu znaczących przewoźników lotniczych, niestety nie objęły one swym zasięgiem wszystkich, do których były adresowane[24]. Dlatego też, choć w odniesieniu do szkoleń generacji pierwszej, akceptacja środowiska lotniczego dla nowego charakteru szkoleń CRM była zdecydowanie większa, nie brakowało także głosów krytycznych zarzucających, w szczególności przewoźnikom odstającym od nowego trendu w szkoleniach CRM, kontynuację tzw. „psycho-bełkotu"[25].

Generacja trzecia – Dalszy rozwój szkoleń CRM

Początek lat dziewięćdziesiątych wniósł w obszar szkoleń CRM kilka istotnych nowości. Ich charakter coraz rzadziej odzwierciedlał prawidła uznane w świecie korporacji biznesowych, coraz częściej natomiast odnosił się do specyfiki pracy załóg lotniczych. Do udziału w szkoleniach poczęto włączać personel bezpośrednio współpracujący z pilotami, stąd nierzadko uczestnikami szkoleń pierwotnie dedykowanych wyłącznie dla członków załóg lotniczych, stawali się członkowie personelu pokładowego, mechanicy, dyspozytorzy a także personel obsługi.

W ramach szkoleń CRM tego okresu wiele uwagi zaczęto poświęcać również tzw. kulturze organizacyjnej, postrzegając ją jako czynnik warunkujący istnienie w organizacji lotniczej pożądanych dla bezpieczeństwa wykonywanych operacji lotniczych zachowań załogi. W ramach tego typu działań wprowadzono w życie specjalistyczne kursy dla kandydatów na kapitanów. Ich istota polegała na przekazaniu i zakorzenieniu w umysłach przyszłych dowódców statków powietrznych zasad dobrego przywództwa.

Początek lat dziewięćdziesiątych to również czas narodzin szkoleń CRM dedykowanych do personelu kontrolującego pracę załóg oraz personelu odpowiedzialnego za przygotowanie załóg do prowadzenia działalności lotniczej. Merytoryczna strona tego rodzaju szkoleń skupiała się przede wszystkim na wypracowaniu u szkolonych umiejętności obserwacji, analizy i oceny zachowań ludzkich, a w konsekwencji powyższego, na wykorzystaniu posiadanej wiedzy w procesie przygotowywania nowych programów szkoleniowych.

Co więcej, z racji pojawiania się na rynku lotniczym zaawansowanych technicznie i technologicznie konstrukcji lotniczych, coraz bardziej nasyconych środkami i urządzeniami ułatwiającymi ich obsługę, część linii lotniczych wzbogaciła programy szkoleń CRM o zagadnienia dotyczące automatyzacji w pracy załóg statków powietrznych.

Niestety, nie wszystkie wyżej opisane działania były działaniami wszędzie i w równym stopniu realizowanymi. Jak wskazuje literatura przedmiotu, chociaż okres szkoleń trzeciej generacji postrzega się jako czas pozytywnych zmian w koncepcji ich prowadzenia, to jednak niezamierzoną ale bardzo istotną konsekwencją poszukiwania nowych dróg rozwoju było minimalizowanie nacisku na realizację pierwotnego celu szkoleń CRM – redukcji skali błędu ludzkiego, jako wiodącej przyczyny zdarzeń lotniczych.

Generacja czwarta – Integracja i proceduralizacja szkoleń CRM

Naturalne jest, w szczególności dla projektów dużej skali, do których z pewnością zaliczyć można wdrożenie systemu szkoleń CRM w lotnictwie, że realizacja postulatów i wniosków takiemu projektowi służących, niezależnie od ich słuszności i etapu zgłaszania, zazwyczaj nie odbywa się w trybie natychmiastowym. Tak też było z jednym z postulatów zgłoszonych podczas konferencji NASA w roku 1986, według którego szkolenia CRM winny zaistnieć jako stały element w systemie szkoleń lotniczych.

Postulat ten doczekał się spełnienia dopiero w połowie lat dziewięćdziesiątych ubiegłego wieku. Wówczas to programy CRM stały się obowiązkowym elementem szkolenia personelu lotniczego we wszystkich liniach lotniczych.

Moment ten przyjmuje się umownie jako początek czwartej generacji szkoleń CRM.

W owym czasie wysiłki naukowców współpracujących z NASA ukierunkowane zostały na określeniu przydatności szkoleń CRM w kontekście bezpieczeństwa wykonywanych operacji lotniczych. Wnioski z prowadzonych przez nich badań, pozwoliły postawić tezę, iż jedną ze znaczących ułomności systemu szkoleń CRM była, mimo wielu podejmowanych w tym zakresie wy-

[24] Pierwsze szkolenia w oparciu o zmodyfikowane według założeń generacji drugiej programy w prowadziła Delta Airlines. Według: E. Danecka-Łatka. *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy.* Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

[25] „Psycho-babble". Według: Robert L. Helmreich, Ashleigh C. Merritt i John A. Wilhelm. *The Evolution of Crew Resource Management Training in Commercial Aviation.* The International Journal of Aviation Psychology, nr 1 (1999).

siłków, wciąż aktualna kwestia ograniczonego ich oddziaływania.

Co więcej, tam gdzie system ten był dostępny, przyjmowany i wdrażany, nie zawsze był powszechnie akceptowany i zapewne przez to proces jego „zagnieżdżenia" w ogólnym systemie szkoleń lotniczych okazywał się bardzo rozciągnięty w czasie.

Jedną, choć nie najistotniejszą przyczyną tego stanu rzeczy był naturalny opór samych szkolonych przed czymś nowym i nieznanym. Przyczyna główna, jak się w praktyce okazało o wiele trudniejsza do pokonania, leżała w uwarunkowaniach kulturowych krajów bądź regionów świata, w których funkcjonowało lotnictwo komunikacyjne i w których przyszło wdrażać wypracowane założenia szkoleń CRM.

Jako zobrazowanie powyższego problemu, w literaturze przedmiotu przytacza się często wnioski holenderskiego naukowca Geert'a Hofstede'a[26].

Analizując problem uwarunkowań kulturowych, przekładających się na jakość współpracy w załodze statku powietrznego, wyodrębnił on trzy grupy państw (regionów świata), będących z natury reprezentantami odmiennej specyfiki w obszarze implementacji programów CRM.

Pierwsza grupa to kraje (np. Chiny), w których niemal od urodzenia wpaja się ich obywatelom absolutny posłuch dla decyzji autorytetów i w których przejaw własnej inicjatywy stojący w sprzeczności z decyzją lidera odbierany jest zawsze jako brak okazania należnego mu szacunku.

Druga grupa, to z kolei kraje (np. USA) o bardzo wysokim poziomie poczucia indywidualizmu i niezależności, w których z natury przedkłada się cel jednostki nad interes grupy. Jakkolwiek takie właśnie postrzeganie i uznanie jednostki w społeczeństwie jest dążeniem ze wszech miar usprawiedliwionym, to jednak wychowanej tylko w takim duchu załodze statku powietrznego trudniej przyjdzie znaleźć „podstawy" do wspólnego, zespołowego rozwiązywania problemów.

Trzecia grupa, której przykładem może być Grecja i część krajów Ameryki Łacińskiej, to kraje, w których zespoły pracujące nad wspólnym zadaniem osiągają lepsze efekty, jeśli korzystają z jasno określonych sposobów postępowania. Co istotne, to właśnie w tej grupie państw występuje największa tolerancja na przyjęcie, zdefiniowanej w kategoriach wymaganych zachowań, koncepcji Zarządzania Zasobami Załogi.

Mając na uwadze powyższe, łatwiej zrozumieć wnioski naukowców badających problem różnic w implementacji założeń CRM w różnych częściach świata[27].

Odnosząc się w szczególności do programów CRM pierwszej i drugiej generacji stwierdzili bowiem, iż założenie o jednakowym poziomie ich przyjęcia wszędzie tam gdzie tylko będą miały szansę zaistnieć, było założeniem z gruntu błędnym. Popularne w owym czasie kupowanie szkoleń CRM od jednego przewoźnika celem ich dokładnego odwzorowania u drugiego, czy to w „handlu realizowanym między kontynentami czy między podmiotami danego kraju, nie mogło przynieść oczekiwanych korzyści bez uwzględnienia kultury organizacyjnej i specyfiki operacyjnej kupującego.

Z tego też względu koncepcja Zarządzania Zasobami Załogi czwartej generacji skupiała się przede wszystkim na uwzględnieniu odrębności kulturowej jej odbiorców. Co nie mniej istotne, koncepcja ta stawiała na tworzenie i stosowanie w praktyce standaryzacji, procedur, reguł do naśladowania i przepisów do przestrzegania.

Generacja piąta – Współczesność. Podstawy prawne w zakresie szkoleń CRM

Generacja piąta szkoleń CRM, to szkolenia realizowane w obecnej formie.

Przewoźnicy lotniczy wielu krajów zrzeszeni wokół władz lotniczych właściwych dla danego regionu świata mają możliwość i jednocześnie obowiązek stosowania w prowadzonej działalności zarobkowej, szkoleniowej i operacyjnej skonkretyzowanych standardów i procedur, sformułowanych przez te władze i zawartych w zbiorach obowiązujących przepisów.

Od 1979 roku właściwą władzą dla krajów europejskich, wyrażających dobrowolny akces przystąpienia do zrzeszenia, była organizacja nosząca nazwę Wspólnych Władz Lotniczych (Joint Aviation Authorities – JAA), zaś dokumentami szczegółowo charakteryzującymi obszar szkoleń, w tym między innymi szkoleń CRM, oraz obowiązki

[26] Według: E. Danecka-Łatka. *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy.* Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

[27] Według: Robert L. Helmreich, Ashleigh C. Merritt i John A. Wilhelm. *The Evolution of Crew Resource Management Training in Commercial Aviation.* The International Journal of Aviation Psychology, nr 1 (1999).

i zasady prowadzenia działalności lotniczej przez operatów lotniczych, były – Wspólne Wymagania Lotnicze (Joint Aviation Requirements – JARs)[28].

Z czasem przepisy wypracowane przez JAA, w istocie nie posiadające mocy prawnej, bo na zasadzie dobrowolności przyjmowane i stosowane przez kraje zrzeszone, zaczęły być zastępowane przepisami prawa Unii Europejskiej. Jej organem, powołanym do życia w roku 2002 i w kolejnych latach przejmującym wszystkie funkcje JAA, jest Europejska Agencja Bezpieczeństwa Lotniczego (European Aviation Safety Agency – EASA)[29]. W chwili obecnej, obok Komisji Europejskiej, organizacji EUROCONTROL oraz władz lotniczych krajów członkowskich Unii, EASA jest jednym z instytucjonalnych filarów systemu bezpieczeństwa lotniczego w Europie[30].

Jakkolwiek przepisy tworzone przez EASA, z mocy prawa unijnego, obowiązują wyłącznie kraje członkowskie Unii, pamiętać jednak trzeba, że Europejska Agencja Bezpieczeństwa Lotniczego prowadzi ścisłą współpracę z odpowiadającymi jej instytucjami na całym świecie, w tym z Międzynarodową Organizacją Lotnictwa Cywilnego (ICAO), Federalną Administracją Lotnictwa (FAA) w Stanach Zjednoczonych i władzami lotnictwa w Kanadzie, Brazylii, Izraelu, Chinach, Szwajcarii i Rosji. Celem porozumień roboczych między Agencją a tymi instytucjami jest harmonizacja norm i promowanie najlepszej praktyki w dziedzinie bezpieczeństwa lotniczego na całym świecie[31].

Wypracowane przez JAA i przejęte przez EASA regulacje bardzo obszernie i jednocześnie bardzo szczegółowo określają standardy dotyczące szkoleń CRM. Według tychże regulacji szkolenie to winno być przeprowadzone przez personel odpowiednio wykwalifikowany zaś jego program, ujęty w Instrukcji Operacyjnej operatora lotniczego, nie może pomijać żadnego z poniższych zagadnień:

- Błąd ludzki i niezawodność, łańcuch błędów, wykrywanie i zapobieganie błędom;
- Polityka bezpieczeństwa w przedsiębiorstwie, standardowe procedury operacyjne (SOP), czynniki organizacyjne;
- Stres, panowanie nad stresem, zmęczenie i czujność;
- Zbieranie i obróbka informacji, świadomość sytuacyjna, zarządzanie obciążeniem pracą;
- Podejmowanie decyzji;
- Porozumiewanie się i współpraca w kokpicie i poza nim;
- Przywództwo i zachowanie zespołu, synergia;
- Automatyka, automatyzacja, filozofia użycia automatyki (jeśli dotyczy typu);
- Specyficzne różnice w typach;
- Studiowanie przypadków.

Wybrane z powyższego zestawienia moduły szkoleniowe winny być również włączone do programu szkolenia na nowy typ statku powietrznego, programu szkolenia przejściowego (przy zmianie pracodawcy, operatora lotniczego), programu szkolenia dowódczego (dla kandydatów na dowódców statku powietrznego) oraz programu szkolenia okresowego (odświeżającego, powtarzalnego, organizowanego w cyklu rocznym).

Co ważne, operator powinien, tak dalece jak to możliwe, zapewnić wspólne szkolenie CRM członków załóg lotniczych i pozostałego personelu tworzącego załogę statku powietrznego.

Szkolenie to powinno odzwierciedlać kulturę organizacyjną danego operatora, zaś teoretyczna i praktyczna formuła prowadzonych zajęć winna zapewnić możliwość prowadzenia dyskusji i swobodnej wymiany doświadczeń, przede wszystkim w kontekście braków i zaniedbań w przepływie informacji oraz błędów w procesie komunikowania się członków załogi.

[28] Polska przystąpiła do JAA z dniem 26 listopada 2002 r.

[29] Europejską Agencję Bezpieczeństwa Lotniczego (EASA) powołano do życia na mocy rozporządzenia Rady i Parlamentu Europejskiego nr 1592/2002. Działalność rozpoczęła we wrześniu 2003 roku. Obecnie podstawą prawną jej funkcjonowania jest rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 z dnia 20 lutego 2008 r. w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Lotniczego oraz uchylające dyrektywę Rady 91/670/EWG, rozporządzenie (WE) nr 1592/2002 i dyrektywę 2004/36/WE (Dz. U. L 79 z 19.3.2008). Siedzibą EASA była początkowo Bruksela. Od listopada 2004 r. jej siedziba mieści się w Kolonii w Niemczech.

[30] Efektem zapisów rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 216/2008 z dnia 20 lutego 2008 r. nadającym EASA przypisane dotąd JAA kompetencje w zakresie licencjonowania personelu lotniczego, operacji lotniczych oraz oceny bezpieczeństwa statków powietrznych z państw trzecich, było oficjalne rozwiązanie, z dniem 30 czerwca 2009 roku, Zrzeszenia Władz Lotniczych (Joint Aviation Authorities – JAA).

[31] Według: http://easa.europa.eu/language/pl/more-about-EASA.php.

Jak należało się spodziewać, stosowane już od kilku miesięcy przepisy EASA[32], w żadnej mierze nie liberalizują standardów określonych we Wspólnych Wymaganiach Lotniczych wypracowanych przez JAA, a wręcz czynią je jeszcze bardziej restrykcyjnymi.

Nowe regulacje np. nie przewidują możliwości dopuszczenia pilota do prowadzenia operacji bez nadzoru, jeśli wcześniej nie uczestniczył w szkoleniu CRM w zakresie określonym dla szkolenia wstępnego.

Co więcej, niezależnie od charakteru operacji, które tenże pilot będzie wykonywał w zarobkowym przewozie lotniczym, wymaga się, aby przed przystąpieniem do ich wykonywania przeszedł również szkolenie w zakresie czynnika ludzkiego, co ważne, na poziomie określonym dla najwyższej kategorii licencji pilota – licencji pilota liniowego (Air Transport Pilot License – ATPL). Jeśli pilot nie spełnia powyższego warunku, obowiązek przeprowadzenia takiego szkolenia nałożony został na zatrudniającego go operatora lotniczego. Rolą operatora jest również przeprowadzenie przedmiotowego szkolenia według planu ściśle odzwierciedlającego zakres tematyczny dotyczący możliwości i ograniczeń człowieka, ujęty w programie szkolenia do uzyskania licencji ATPL.

Podsumowanie

Mając na względzie absolutnie dominującą pozycję czynnika ludzkiego w przyczynowości zdarzeń lotniczych, należałoby zakładać, że od chwili stwierdzenia takiego stanu rzeczy do chwili obecnej sytuacja w tej materii ulegnie diametralnej zmianie. Co więcej, należałoby również zakładać, że wszelkie działania czynnik ten ograniczające, w tym także szkolenia CRM, winny mieć absolutny priorytet w ich realizacji, przede wszystkim, w zarobkowym transporcie lotniczym.

Jak jednak wskazuje analiza procesu ewoluowania szkoleń CRM, a poprzez ich pryzmat, analiza działań podejmowanych dla ograniczenia negatywnych skutków czynnika ludzkiego w działalności lotniczej, nasze założenia nie do końca znalazłyby potwierdzenie w rzeczywistości.

Okazuje się bowiem, że niewspółmiernie długo, w odniesieniu do rangi problemu, rodziła się nasza lotnicza świadomość. Przyczyn takiego stanu rzeczy było wiele, jednak najistotniejsze z nich, to bez wątpienia brak jednakowej wrażliwości (władz, operatorów, personelu lotniczego) na świeżo zidentyfikowany problem oraz, przez bardzo długi czas, brak wypracowanych, wspólnych (między władzami, operatorami, personelem) standardów ograniczających negatywne skutki występowania czynnika ludzkiego. Nie bez znaczenia dla efektywności podejmowanych działań były też problemy organizacyjne, problemy natury ekonomicznej, jak i częste (głównie w środowisku załóg lotniczych) przekonanie o próbie psychologicznej manipulacji w ich umiejętności i kompetencje.

Na nasze (załóg i pasażerów) szczęście analizowany problem jest dzisiaj doceniony, zdefiniowany i właściwie rozumiany, nie znaczy to jednak, że zażegnany.

Podsumowując opracowany materiał, bezsprzecznie stwierdzić należy, iż istnienie czynnika ludzkiego, stanowiącego wciąż główną przyczynę większości zdarzeń lotniczych, równe jest istnieniu lotnictwa załogowego. Jakkolwiek rozumienie możliwości i ograniczeń wynikających z ludzkiej natury, jak również podjęcie działań skutkujących wyeliminowaniem czynnika ludzkiego z grupy przyczynowej zdarzeń lotniczych, tak długiej tradycji już nie ma, istotnym jest fakt, że problem został zauważony i próby jego rozwiązania podjęte.

Z jakim skutkiem?

Tak naprawdę trudno oszacować, bo trudno porównać liczbę zdarzeń lotniczych powstałych za sprawą czynnika ludzkiego w czasie, w którym z czynnikiem tym próbujemy walczyć, z liczbą zdarzeń, które mogłyby się wydarzyć w tym samym czasie, jeśli tej walki by nie podjęto. Zbyt wiele bowiem w analizowanym okresie pojawiło się zmiennych, z których zasadnicze znaczenie w kwestii „zafałszowania" wyników analiz, z pewnością miałaby wciąż wzrastająca liczba operatorów lotniczych, wciąż wzrastająca liczba wykonywanych operacji lotniczych, czy też wciąż rosnąca liczba nowych typów statków powietrznych. Wprawdzie, z jednej strony, statków powietrznych coraz bardziej bezpiecznych, z drugiej jednak strony, coraz bardziej technicznie wyrafinowanych i choćby z tego względu bardziej wy-

[32] Przepisy zawarte w rozporządzeniu Komisji (UE) nr 965/2012 z dnia 5 października 2012roku, ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do operacji lotniczych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008.

magających, zajmujących i obciążających pracę członków ich załóg.

Trudno oszacować liczby, bez wątpienia jednak stwierdzić należy, że gdyby walki z negatywnymi skutkami czynnika ludzkiego nie podjęto, zdarzeń z jego udziałem byłoby zdecydowanie więcej. To oczywiście nie oznacza, że możliwe do wykorzystania spektrum działań ukierunkowanych na wyeliminowanie czynnika ludzkiego z grupy głównych przyczyn zdarzeń lotniczych, zostało wyczerpane.

Co najwyżej ... jeszcze nieodkryte.

Bibliografia

Baron R., *Barriers to Effective Communication: Implications for the Cockpit.* http://airlinesafety.com.

Beaty D., *Pilot. Naga prawda. Czynnik ludzki w katastrofach lotniczych*, Wydanie I, Warszawa 2013.

Burigan S., *Situational awareness – staying ahead of the aircraft*, AirRescue, International Air Rescue & Air Ambulance Magazine, Vol. 2/2012, 33-37.

CAP 737 Crew Resource Management (CRM) Training. Guidance For Flight Crew. CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES). UK Civil Aviation Authority, 2006.

Cooper George E., White Maurice D., Lauber John K., *Resource Management on the Flight Deck*, Proceedings of a NASA/Industry Workshop Held at San Francisco, California, June 26–28, 1979, NASA Conference Publication 2120.

Danecka-Łatka E., *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy*, Problemy Zarządzania, vol. 9, nr 4, Wydział Zarządzania UW.

Gałązkowski R., *Powstanie Samodzielnego Publicznego Zakładu Opieki Zdrowotnej Lotnicze Pogotowie Ratunkowe. Nowa struktura i zadania*, Lotnicze Pogotowie Ratunkowe, praca zbiorowa pod redakcją R. Gałązkowski, Wydanie I, Warszawa 2010.

Helmreich Robert L., Merritt Ashleigh C. i Wilhelm John A., *The Evolution of Crew Resource Management Training in Commercial Aviation*, The International Journal of Aviation Psychology, nr 1 (1999).

Kostera M., *Podstawy organizacji i zarządzania*, WSPiZ, Warszawa 2001.

Koźmiński A.K., Piotrowski W., *Zarządzanie. Teoria i Praktyka*, PWN, Warszawa 2002.

Necki Z., *Komunikacja międzyludzka.* Wyd. Profesjonalnej Szkoły Biznesu, Kraków 1996.

"Pilot's Handbook of Aeronautical Knowledge". U.S. Department of Transportation, Federal Aviation and Administration, Flight Standard Service, 2008, Chapter 17 "Aeronautical Decision Making", 17-2.

Roguski J., *„Przełom". Polskie Lotnictwo Sanitarne 1955–2005*, praca zbiorowa pod redakcją R. Gałązkowski i P. Kłosiński, Wydanie I, Warszawa 2005.

Rozporządzenie Komisji (UE) nr 965/2012 z dnia 5 października 2012 r. ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do operacji lotniczych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 z dnia 20 lutego 2008 roku, w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Lotniczego.

Słownik łacińsko-polski, PWN, Warszawa 1973.

Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors, The Journal of the Human Factors and Ergonomics Society, March 1995.

Truszczyński O., Biernacki M., *Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych*, Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik–grudzień 2006.

Ustawa o ustanowieniu programu wieloletniego *Wymiana śmigłowców Samodzielnego Publicznego Zakładu Opieki Zdrowotnej Lotnicze Pogotowie Ratunkowe w latach 2005-2010*, z dnia 3 czerwca 2005 r. (Dz.U. Nr 122, poz. 1022).

Wspólne Wymagania Lotnicze JAR-OPS 3, Zarobkowy Przewóz Lotniczy (Śmigłowce), Zmiana 5, Wydanie z 1 lipca 2007 r.

Zarządzenie Ministra Zdrowia z dnia 03 marca 2000 roku w sprawie utworzenia Samodzielnego Publicznego Zakładu Opieki Zdrowotnej (Dz.Urz. MZ. 2000, Nr 1 poz. 4).

Zarządzenie Ministra Zdrowia z dnia 03 marca 2000 roku w sprawie likwidacji Centralnego Zespołu Lotnictwa Sanitarnego (Dz.Urz. MZ 2000, Nr 1 poz. 5).

Źródła internetowe:

http://airlinesafety.com
http://easa.europa.eu/language/pl/more-about-EASA.php
http://www.baaa-acro.com
http://www.lotnictwocywilne.republika.pl/crm.html
http://www.pl.wikipedia.org

FLIGHT SAFETY AND CREW RESOURCE MANAGEMENT TRAINING IN COMMERCIAL AIR TRANSPORT

Abstract

In this paper, the authors describe, against the backdrop of threats to the safety of aviation operations, the reasons why training in Crew Resource Management (CRM) came to exist and its nature, essence and purposes. Furthermore, the authors have covered the evolution of said training along with many factors that shaped this process. In making the presentation, the authors have focused on the solutions implemented in commercial air transport around the world. As part of this topic, they indicate the basic and generation-specific changes in the scope and manner of conducting the CRM trainings.

Key words: flight safety, crew resource management, CRM, human factor, situational awareness, decision-making, ADM, communication, crew cooperation

(...) what is still to be accepted is the commonality of the causes of mistakes that lead to accidents in all areas of human behaviour. The difference is that in aviation a banal mistake may have tragic consequences.

David BEATY

Introduction

Various experiences and a particularly extensive source of literature indicate that a human being, with all his capabilities and limitations, has always been the weakest link in the pilot-aircraft combination. Unfortunately, in an age of dynamic technological progress and continuously developing aircraft industry, this problem has not been solved yet, with commercial air transport being no exception. According to data published by the Aircraft Crashes Record Office (ACRO)[1], with respect to 2.51% of the total aviation occurrences where it has not been possible to indicate their cause, 3.25% of the total occurrences were classified as sabotage, while 5.95% of the total occurrences resulted from atmospheric conditions. Additionally, in 20.72% of the total occurrences, the cause was attributed to technical issues, whilst human errors, termed "human factor", were responsible for as much as 67.57% of the total occurrences[2].

The realisation of just how significant a role the human factor had played in the previous aviation occurrences happened comparatively late, i.e. in the late 1970s. It was then, in June of 1979, at a conference held by the National Aeronautics Space Administration (NASA)[3], that its organisers, backed by the results of investigations covering a few hundred aviation occurrences, indicated the importance of specifying and introducing corrective measures aimed at remedying the consequences of the inability to cooperate within crews, ascertain the situation in flight and make the appropriate decisions. The conference was dedicated as a whole to the questions and psychological aspects of managing resources in cockpits and did not provide any ready-made solutions. It made the conference participants and the whole aviation community aware of the problem that had a profound impact on the safety of aviation operations and could only have been solved through their participation. It has been accepted that the NASA conference of 1979, and particularly the subsequent actions which stemmed from it, has led to the creation of aviation training which is termed in the aviation community as "Crew Resource Management – CRM".

Ever since, in order to achieve the highest efficiency of CRM training, the authorities and air operators have been looking for programmes,

[1] Aircraft Crashes Record Office (ACRO), an NGO based in Geneva which compiles statistics related to air accidents.

[2] Data relate only to aircraft capable of carrying more than six people, excluding combat airplanes, helicopters and hot air balloons. According to: http://www.baaa-acro.com/.

[3] George E. Cooper, Maurice D. White, John K. Lauber. "Resource Management on the Flight Deck". Proceedings of a NASA/Industry Workshop Held at San Francisco, California, June 26–28, 1979, NASA Conference Publication 2120.

methods and techniques of training which, when combined with available tools for assisting the education process, will result in the human factor no longer being identified as the main cause of accidents in the majority of aircraft accident reports.

The aim of this paper is to show the process in which CRM training has evolved in commercial air transport around the world. It has also been attempted to show the nature of that training, the purpose and role played in the aviation training system used to increase flight safety.

The essence and aims of CRM training

The birth of a new type of training concerning the "human factor" has in no way depreciated the significance of training focused on air crews gaining expert aviation knowledge, including the knowledge necessary to pilot a certain type of an aircraft in a safe manner, in an organisational framework and in accordance with the standards specified by a given air operator (that offers a certain scope of services). The essence of the CRM training in aviation is the coupling of that knowledge with the ability to employ, as much as it is possible, any resources available to the crew, including the cognitive and interpersonal skills of individual members of the crew, both in normal situations and, primarily, in extreme situations that develop on board an aircraft.

In this meaning, the cognitive skills are defined as thought processes used for the purpose of uninterrupted, correct analysis and assessment of the situation (situational awareness); furthermore, for making correct decisions at any stage of a flight and in any circumstances the aircraft might be in (normal, abnormal and emergency). The interpersonal skills are considered to be those skills which are responsible for the quality of communication within the crew; communication in turn translates directly into the effectiveness (or lack thereof) of work in a team called the aircraft crew. Even though in the years prior to the inclusion of CRM training into aviation training syllabi, the notions of situational awareness, planning, decision making, as well as communication and cooperation amongst the crew were not foreign to the aviation community, the new perspective on the relation between them afforded in the CRM training gave them a new meaning, one that has particular bearing on the safety of aviation operations.

Situational awareness – there are numerous definitions of this term in the source literature.

In principle, all of them are quite similar, with some differences between them being a result of, first and foremost, the specificity of the environment to which they are individually addressed. The most universal and, at the same time, the most widespread in the aviation community is the definition advocated by Dr. Mica R. Endsley[4], according to which: *"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."*[5].

In establishing situational awareness (building an individual picture of reality around us),the key role is played by our perception, which is to be understood as an ability to take in external stimuli (through our senses) and to identify, interpret and react to them. The experts in the source literature claim that the situational awareness created in the above-mentioned manner is also supplemented by the wealth of life-time experiences and cultural and social influences[6]. In other words, when we use our senses, experience, and knowledge as well as when we continuously monitor and understand what has just happened and what is going on now and anticipate what may transpire in the nearest future, we establish situational awareness and,thus, control the situation. At every point of the situation, we are able to plan our next actions, predict the ramifications thereof and, therefore, make a decision as to executing a given course of action or opting for another one.

[4] Dr. M.R. Endsley is considered a global leader in research and application of situational awareness in advanced systems. She has penned more than 200 publications on situational awareness and is the most quoted author by scientific and professional magazines devoted to situational awareness.

[5] Own translation of: "*Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.*" *"Toward a Theory of Situation Awareness in Dynamic Systems,* Human Factors". The Journal of the Human Factors and Ergonomics Society, March 1995.

[6] See: *"CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES)".* UK Civil Aviation Authority, 2006.

In our day-to-day existence, based on the situational awareness we possess, we make more or less appropriate decisions a countless number of times. Nonetheless, one has to take into account the fact that in everyday existence the ramifications of erroneous decisions are rarely catastrophic. Sadly, in the complex field of aviation operations, an erroneous decision made by a pilot usually leads to fatalities among the crew and the passengers. According to research conducted by the Australian Transportation Safety Board (ATSB), loss of situational awareness was reported in 85% of all of the investigated aviation occurrences in which the "human factor" was indicated as a cause. The outcomes of analyses of aviation occurrences involving helicopters carried out by the European Helicopter Safety Analysis Team (EHSAT) serve to prove the correctness of the above. According to EHSAT's findings, 84 out of 202 aviation occurrences involved partial or complete lack of situational awareness[7].

In executing a flight task, so as to assess the situation properly, the pilot not only applies his knowledge and experience but also gathers a variety of information by monitoring the space outside the aircraft, utilising the onboard avionic equipment at his disposal and following the information broadcast by air traffic services or other pilots. Information overload, lack of information or failure to understand even a single piece of information at a moment crucial for conducting a proper assessment of a given situation triggers an error or a whole chain thereof. One must also remember that lack of knowledge, fatigue, stress, distraction, boredom, inattention, disregard for warning signals, excessive agitation and euphoria increase the possibility of triggering an error chain.

With respect to situational awareness, the aim of the CRM training is to demonstrate to the trainees the vast importance of said awareness vis-a-vis the safety of aviation operations performed. It is also crucial to present the mechanism in which situational awareness may be established as well as the threats leading to its partial or complete loss. However, the most essential thing from the point of view of CRM is making commanders realise that they have a certain resource at their disposal which may be employed at any stage of the flight as a part of the process aimed at maintaining situational awareness, namely other members of the crew.

Decision making – Both in the theory and practice of management, it is a process consisting in collecting and processing information about a future task, whereas the decision itself is defined as a conscious, non-random choice of one of the identified variants of the future action which has been considered feasible. It is possible to classify decisions according to the amount of information and the conditions in which those decisions are made:[8]

- decisions made under certainty (in situations when we are able to infallibly predict their consequences);
- decisions made under risk (in situations when we may identify a set of results and assign a certain probability of occurrence to said consequences);
- decisions made under uncertainty (in situations when we are both unable to identify all consequences and specify the probability of their occurrence).

Given the scale of undesirable consequences that may arise in aviation due to an erroneous decision, the process of training and preparing flight crews (regardless of the nature of aviation, its purpose and tasks) is focused on eliminating, to the highest extent possible, the situations in which the decisions would be made under risk or uncertainty. That is one of the reasons why there are numerous standards being introduced into aviation operations (standardising crew actions in certain operations, standard operational procedures, standard departure and landing procedures, normal, abnormal and emergency checklists etc.). Their aim is to make the decision-making process largely automatic, subconscious, resulting from one's general aviation knowledge and experience, but, above all else, to base it on familiarity with fixed behaviour patterns and their application in practice.

Why, despite understanding the essence of the matter and such an extensive scale of preventive actions, do the accidents resulting from partial or complete loss of situational awareness leading to an erroneous decision still happen?

[7] See: S. Burigan. *"Situational awareness – staying ahead of the aircraft"*. AirRescue, International Air Rescue & Air Ambulance Magazine, Vol.2/2012, 33–37.

[8] A.K. Koźmiński, W. Piotrowski. *"Zarządzanie. Teoria i Praktyka"*. PWN, Warszawa 2002; M. Kostera. *"Podstawy organizacji i zarządzania"*. WSPiZ, Warszawa 2001.

This is most likely because, as has already been mentioned here before, aviation is an extremely complicated environment in which there is a large flow of information and a significant number of variables (changes in the meteorological situation, navigational situation, air traffic, unforeseen chains of emergency situations etc.) which translate into an unlimited number of threats that may take place; hence, it is impossible to foresee and describe them and incorporate them in the framework of standardised crew behaviour.

How could this issue be solved, then?

The issue of a decision-making process applied by the pilots in their typical and complicated aviation environment (Aeronautical Decision Making – ADM) has been widely discussed in the source literature. The said issue is centered on the analysis and perception of those processes, with particular attention being paid to attitudes assumed by individuals, primarily with respect to risk assessment and stress management skills.

According to the experts in this field, in order to understand ADM, one has to understand the significance of these attitudes in the decision-making process, and even more importantly, the way in which those attitudes may be modified in order to increase the security of the performed aircraft operation. Moreover, to comprehend AMD it is also necessary to understand the factors that determine why these and only these decisions are made. Aside from learning how this process is being carried out, it is equally important to know how it is possible to improve it[9].

With respect to the decision-making processes, the CRM training is focused particularly on the awareness of the need and the rationale for involving all crew members in the process of making decisions in flight. As dictated by the CRM theory, in order to use the crew members in an effective way, it is necessary to familiarise them, as early as at the flight preparation stage, with the flight plan and the intention of the commander to carry it out. Moreover, it is crucial to continually update the crew on the flight status, the changes to the original flight plan and the commander's intentions brought about by such changes[10].

In the above-mentioned framework, the situational awareness which is crucial for making the right decision ceases to be solely the situational awareness of the commander. Having a complete situational awareness within a team is a resource that not only may, but should be used by the commander so as to make the best decision, particularly in a critical situation and under time-deficit conditions.

As suggested by numerous experiences and observations, the degree of participation of the crew in the decision-making process is largely dependent upon the organisational culture and social norms governing a given community. In the cultures and communities that allow for applying a democratic model of team management while maintaining a commander's authority, the above-mentioned CRM theory has all the chances of being successful. At the same time, in the cultures and communities in which commander's authority is of superior value, an autocratic management model will be preferred[11]. In such cultures and communities, the democratic approach to crew management and employing the crew's potential will be viewed as a sign of the commander's weakness, thus rendering the application of the CRM theory significantly harder, unfortunately. Nonetheless, to do justice to this management style, one has to bear in mind the fact that, albeit the CRM theory points out the advantages of involving the crew members in the decision-making process of the commander, it also warns that there are situations in which an authoritative management style is fully desired as it will be the most effective in a given specific situation[12].

Communication – the dictionary definition of this term states that its origins are to be traced to Latin (communico, communicare) and give it the following meaning: 'make something common, join, provide somebody with information, to confer'[13].

A communication process is to be found in every element of the day-to-day lives of human beings

[9] See: *"Pilot's Handbook of Aeronautical Knowledge"*. U.S. Department of Transportation, Federal Aviation and Administration, Flight Standard Service, 2008, Chapter 17 "Aeronautical Decision Making", 17–2.

[10] See: *"CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES)"*. UK Civil Aviation Authority, 2006.

[11] Management style classification introduced by Kurt Lewin, Ronald Lipitt and Ralpha K. White.

[12] See: O. Truszczyński, M. Biernacki. *"Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych"*. Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

[13] *Słownik łacińsko-polski*. PWN, Warszawa 1973, s. 101.

and it is commonly understood as transmission of information between the sender and the recipient. In order for this process to be effective, it is a sender's role to utilise both verbal and non-verbal information channels and to phrase the message in a way that will be comprehensible to the recipient; whereas it is a recipient's role to decode it and, additionally, to send feedback to the sender using the same information channels, thus notifying him of the message having been understood or not. In other words, communication is an exchange of both verbal and non-verbal signals in a given context done with a view to achieving a better level of cooperation[14]. Consequently, incorrect phrasing of information or usage of incorrect information channels (or using them incorrectly) will result an inability to understand it appropriately, which will in turn result in the ineffectiveness of an action, particularly while working in a group.

The incorrect phrasing of information or the usage of incorrect information channels (or using them incorrectly) are, unfortunately, not the only causes of bad communication, particularly among aircraft crews. It is necessary to remember the constraints of the environment in which they carry out their duties.

The factors connected with the crew work environment, which at best hamper and at worst lead to a significant degradation in the level of communication between the aircraft crew, are primarily an incessant noise and an uninterrupted flow of various (both visual and aural) data from displays of devices and systems installed in the aircraft.

Upon analysing the matter of communication in a broader aspect, when traffic between the aircraft crew and the air traffic services is taken into consideration, the spectrum of factors with an adverse influence on communication grows. Even though such situations should not be generalised, or even more importantly, should not be classified as rules, radio communication is frequently jammed, conflicting, incomplete, ambiguous or unreliable.

There is also the matter of issues connected with a language barrier, both existing between the members of a given crew and between the crew and the air traffic services. A gap in English proficiency (especially nonprocedural English), accent, jargon, or, what should be particularly stressed here, cultural differences, may be the cause of differences in how the received information is interpreted. A compliment may be considered an insult and an innocuous joke an affront[15]. Given the fact that the typical work conditions of an aircraft crew are exacerbated by fatigue and tiredness that deepen with every minute of the flight, we can clearly see that it is a situation when correct and suitable communication seems to pose quite a significant challenge.

Undoubtedly, working on correct communication amongst the crew members and between the crew and the air traffic services is an endeavour which calls for solutions on many levels. The said endeavour is most certainly both difficult and complex and, unfortunately, continuous. However, due to the role that good communication plays in ensuring the security of performed aviation operations, such an endeavour is surely most necessary.

It seems that the key element of CRM training, with respect to communication aspects, is primarily the recognition by the trainees of the (usually) tragic consequences of lack of communication between the aircraft crew during flight. Another element is the understanding on the part of the crew of the imperativeness of viewing good communication as a decisive factor in a proper, effective utilisation of the resources at their disposal during a flight, particularly in abnormal and emergency circumstances. Furthermore, it is also the understanding that incorrect communication may indeed breed such circumstances.

What needs to be stressed here is that, as a result of CRM training, the crews are not expected to solve all identified and analysed issues inherent in the communication process. It is outside flight crews' control to remove all barriers to efficient communication. A crew has no influence on noise, vibrations, radio static etc. Of course, these are the domains of other aviation specialists. Undoubtedly, however, a crew has some influence on all of the elements of interpersonal communication which will allow every member of the crew to be understood well by the others. The elements in question are primarily the ability to ask questions, listen, argue for their opinions, manage conflicts,

[14] See: Z. Necki. *"Komunikacja międzyludzka"*. Wyd. Profesjonalnej Szkoły Biznesu, Kraków 1996, s. 109.

[15] See: R. Baron. *"Barriers to Effective Communication: Implications for the Cockpit"*. http://airlinesafety.com.

and provide constructive critique[16]. The recognition of their importance and a continuing effort to hone them will surely lead to a step-up in the security of flight operations.

Crew cooperation – the encyclopedic definition of cooperation says that is as an ability to establish bonds with others and to collaborate with them; the ability to work as a team member in order to achieve common goals. It is also the ability to accomplish tasks collectively and to solve problems collaboratively[17].

In the source literature, the subject of cooperation, collaboration, and team work has been invariably accompanied by the notion of synergy, or, to be more precise, the synergy effect. This effect is commonly construed as an effect brought about by an organised activity undertaken by a group of people, whose result is more extensive (bigger, better) than a sum of effects undertaken individually by the members of said group. In other words, the result of work obtained from a sum of efforts made by individual elements will always be lower than the result of work of the same elements when they are grouped together.

However, will team work always be a sure-safe way to obtain better work results?

Sadly, not at all times. In order to achieve synergy, team work will not be sufficient. This is because of the fact that synergy only materialises if every component part wishes to cooperate and the members of the team want to interact with one another. Therefore, it will not be created if individual members do not identify with the team, are unclear as to their role in it, are lacking in determination to perform the task to the best extent possible, or do not accept responsibility for the results of work achieved by the group of which they are members.

As can be seen from the above, a group consisting of people who know one another well and are "familiar with one another's ways" has a much greater chance of acting efficiently. In such a group, its members understand one another perfectly and also resort to body language in their communication; they are people who know both their and other members' capabilities and limitations.

Any group "built" in such a manner will undoubtedly work in a better, smoother, and a more efficient manner than any other. Nevertheless, if one wanted to introduce the principle of forming permanent teams into the operators' operational rules, it would turn out that, due to organisational constraints, its continuous application could not be guaranteed at all times. Usually, then, the aircraft crews will not be composed of the people "who are familiar with one another's ways" to the degree indicated above.

For precisely these reasons, so much attention has been devoted to creating all types of standardised crew behaviours. Additionally, the question of organisational culture, one that actively promotes the application of well thought-out rules for using crew resources, has attracted a growing interest. An important role is also allocated to the factors fostering a positive atmosphere in flight crews' work.

An atmosphere in which team work takes place has been frequently referred to in the source literature as an "emotional climate", which in principle pertains to the way in which people who work together as a team perceive („feel") themselves and others when performing shared tasks. According to published research in this field, the determinants for creating a positive emotional climate in the crew, which apply to its every member, are willingness to participate in a task and an ability to fully participate in its accomplishment, the clarity of expectations of the commander and the rest of the crew, their appreciation of the efforts taken, good communication, the ability to speak freely and, what is particularly important, an outlook on the matters of security shared by everyone[18].

A huge role in creating a positive emotional atmosphere is played by the attitude displayed by the captain - commander of the flight crew. A captain who is lordly, frosty towards others and struggles with interpersonal communication will never create such an emotional atmosphere. Similarly, a captain who is unprepared for a task

[16] See: O. Truszczyński, M. Biernacki. *"Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych"*. Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

[17] See: www.pl.wikipedia.org

[18] See: *"CAP 737 Crew Resource Management (CRM) Training, Guidance For Flight Crew, CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES)"*. UK Civil Aviation Authority, 2006.

will fail to conjure up such an atmosphere. His being nervous due to lack of knowledge or insufficient preparations for the flight will most likely bring about communication issues between him and the crew, situational awareness issues and decision-making issues. The crew will immediately identify such a situation as a one in which the chances to create a positive "chemistry" in their work, in the work of the team, are marginable.

However, it is enough for a captain, one who is prepared to perform a task and is aware of the significance of positive emotional climate in his own crew, to ask the air traffic services for permission to taxi using the words *"we request taxi"* instead of "*request taxi*"[19]. The meaning of radio commands remains essentially unchanged, but for a crew as sensitive to the actions taken by the team leader as the flight crew is, this will be a sufficient message to accept the captain's attitude as an unmistakable invitation to take part in the task and share the responsibility therefor.

With respect to crew cooperation, the aim of CRM training is primarily to make the trainees aware of a host of determinants for obtaining the synergy effect in the work of the team, which a flight crew undoubtedly is. Knowledge and awareness of the rules and relationships characteristic for team work and, what is more important, the practical application of that knowledge will unquestionably augment the efficiency of the work undertaken by such a team. In turn, the higher the efficiency, the higher the safety of air operations. A common goal of actions undertaken by flight crews is to perform the flight safely. In order to achieve the highest probability of carrying out a safe flight, the crew should cooperate to the highest possible degree. Such a level of cooperation is unobtainable unless said knowledge becomes universal, and more crucially, commonly applied.

Importantly, even though the foremost significance in obtaining the desired synergy effect brought about by the cooperation within the flight crew is ascribed to the captain's attitude, it is crucial to make the trainees aware that, in order for that effect to materialise, every crew member must demonstrate a proper attitude.

[19] The radio command cited here is an example command used for the purposes of this article and it has not been taken from the applicable aviation nomenclature.

The evolution of CRM training in commercial air transport

As has been previously indicated, it is commonly accepted that the notion of CRM training was conceived at the National Aeronautics Space Administration (NASA) conference held in 1979, during which the results of the investigations into aviation accidents were presented in a comprehensive manner. The results showed conclusively that there is correlation between the safety of aircraft operations and the cognitive and interpersonal skills of their crews.

As has also been mentioned here the organisers of that conference, upon taking it on themselves to try to define a great problem for aviation, did not provide any ready-made solutions to it. Nonetheless, the initiative itself and the gravity of the issue demonstrated to the participants sufficed to spur the authorities, organisations and air carriers to take actions aimed at seeking, obtaining, developing and introducing training programmes focused on the improvement of interpersonal aspects of cooperation within flight crews[20].

It should be underlined here that in the period between 1979 and the present day both the training syllabi and the outlook on the scope or even the very purposefulness of the introduction thereof have evolved in the aviation community; not infrequently, this evolution has taken place by many divergent routes.

The trailblazing researchers, who undertook to create a transparent evolution model of CRM training, were U.S. researchers, Robert L. Helmreich, Ashleigh C. Merritt and John A. Wilhelm. In their work entitled "The Evolution of Crew Resource Management Training in Commercial Aviation", which was published in 1999, they defined five consecutive generations of CRM training and indicated the most characteristic features of each of those generations[21].

[20] See: O. Truszczyński, M. Biernacki. *"Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych"*. Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik – grudzień 2006.

[21] See: E. Danecka-Łatka. *"Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy"*. Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

First generation – Cockpit Resource Management

The task of developing the syllabi of the first CRM[22] programmes was assigned to the experts who had previously been primarily active in the field of developing training programmes aimed at boosting the effectiveness of management departments in the companies outside the aviation industry as such.

The predominant feature of this training was the significant degree of emphasis put on psychology, which manifested itself in teaching the trainees the general concepts connected with leadership and holding seminars with tests and psychological exercises that, usually, did not reflect the specific nature of aviation work.

Most likely it was precisely due to this reason that some of the pilots viewed them as mainly an attempt to manipulate their personality, even though such types of training were met with overall acceptance.

Nevertheless, what is of note, the very first generation of CRM trainings had already devoted particular attention to the goal of defining the characteristic managerial styles utilised in cockpits. What's more, the need to correct the individual behaviour of crew members with a view to remedying the then wide-spread problem of lack of assertiveness among the first officers and the authoritarian management style displayed by experienced captains was indicated and highlighted[23].

A considerable advantage brought about by putting in place the first generation training was also the overall conviction that there was a need for recurring CRM training and that simulators needed to be included in their syllabi to the widest extent possible.

Second generation – Crew Resource Management

As was the case with the first generation, the triggering event that prompted the community to view the new type of training in a wider perspective was the next NASA conference dedicated to CRM, which was organised for the aviation industry in 1986.

In the course of the proceedings, it became apparent that, in the intervening years between these two conferences, the training held in accordance with the idea dating back to 1979 afforded the carriers the possibility to draw and propose a great number of significant conclusions. One of the main demands voiced by the conference members was a change in which CRM training was to be approached. The training that had previously been viewed as fundamentally "outside the field of aviation" was to be no longer distinctive and exceptional in nature and organised and carried out separately from other training for flight personnel. From that point on, they were supposed to assume a permanent position in the previously developed aviation training system.

Moreover, in accordance with the new outlook on this types of training, their scope should be extended to include all members of the aircraft crews, thus stepping away from the previously applied rule of limiting them to the cockpit only. Therefore, at that time, the training was renamed from Cockpit Resource Management to Crew Resource Management.

Also characteristic of the second generation CRMs was the modular nature of the training. The seminars, focused primarily on the natural work environment of an aircraft crew, consisted of, first and foremost, the training modules dedicated to team building, situational awareness and stress management. The key objective of the training conducted at that time was to develop a desired strategy for taking decisions and the ability to interrupt the chain of errors made in crew resource management.

Even though the general assumptions of the second generation CRM training had been reflected in the training syllabi adopted by many prominent carriers, they did not reach all of those to whom they had been addressed[24]. Therefore, even though the level of acceptance for the new nature of CRM training was much higher in the aviation

[22] The first comprehensive CRM training program was launched by United Airlines in 1981. See: E. Danecka-Łatka. *"Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy"*. Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

[23] The so-called "captainitis" phenomenon, whereby first officers are afraid of undermining commander's authority. See: http://www.lotnictwocywilne.republika.pl/crm.html.

[24] The first training courses conducted in accordance with the syllabi modified to conform to the assumptions of the second generation CRM were conducted by Delta Airlines. See: E. Danecka-Łatka. *"Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy"*. Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

community than for the first generation training, there were also critical voices saying that the so-called "psycho-babble" was still continuing; such critique was levelled particularly at the carriers falling behind the new trend in CRM training[25].

Third generation – Further development of CRM

The first years of the 1990s brought about a few innovations in the CRM training area. As a result, its nature had been gradually shifting away from rules followed in the corporate world to the characteristic aspects of crew work. The training was also extended to include personnel that were directly cooperating with pilots; thus, quite often, the participants in the previously crew-only training courses were recruited from amongst flight attendants, technicians, dispatchers and maintenance personnel.

In the CRM training originating from that era, a lot of attention was also devoted to the so-called organisational culture, as it was perceived as a determinant for establishing certain types of crew behaviour required in the aviation organisation from the point of view of flight operations security. As a part of such actions, specialised courses for trainee captains were introduced. Their goal was to provide and instill in the minds of future aircraft commanders, the rules of good leadership.

The early 1990s also marked the birth of CRM training courses tailored for the supervision personnel and the personnel responsible for preparing crews for flight operations. The contents of this kind of training course were primarily centered on teaching the trainees the ability to observe, analyse and ascertain human behaviour, and, as a result, to apply the knowledge they gained in the course of developing new training programmes.

Moreover, as more and more technologically and technically advanced aircraft fitted with an increased number of technical means and devices facilitating their maintenance were being launched onto the aviation market, some of the aviation airlines had enhanced their CRM training courses by expanding them to cover flight deck automation.

Sadly, not all of the above-mentioned actions were pursued everywhere and to an equal degree. The source literature shows that, even though the third generation CRM training period had been viewed as an era when positive changes were introduced in the teaching concept, there was an unintentional, yet extremely important consequence of exploring the new ways of achieving progress, namely shifting the emphasis away from the initial aim of CRM training, i.e. the limitation of the role of human error as a primary cause of aviation occurrences.

Fourth generation – Integration and proceduralisation of CRM training

It is quite natural, particularly with respect to large scale projects, among which the introduction of CRM trainings in aviation may surely be numbered, that the accomplishment of demands and conclusions relating to such a project, regardless of their merits and the stage when they were submitted, does not happen immediately. That was the case with one of the demands voiced during the NASA conference of 1986 which advocated the need to make CRM training a permanent element of the aviation training system.

That demand was finally met in the mid-1990s. At that time, the CRM programmes became a mandatory part of the training for aviation personnel of all airlines.

That moment has been customarily assumed as the time when the fourth generation of CRM training was born.

At that time, the efforts undertaken by the researchers cooperating with NASA were focused on establishing the usefulness of CRM with respect to the safety of air operations. The results of the research obtained by them allowed for a conclusion to be formed that one of the biggest deficiencies of the CRM training, despite ongoing efforts, had been the still-relevant question of its limited influence.

Moreover, where the system was available, adopted and implemented, it was not commonly accepted and most likely that was the reason why the process of its "anchoring" in the general aviation training system turned out to have been so protracted.

One of the reasons for this situation, albeit not the most crucial one, was a natural opposition on the part of the trainees against something new and unknown. The main reason, which as practice showed later,

[25] "Psycho-babble". See: Robert L. Helmreich, Ashleigh C. Merritt i John A. Wilhelm. *"The Evolution of Crew Resource Management Training in Commercial Aviation"*. The International Journal of Aviation Psychology, nr 1 (1999).

proved to be much harder to overcome, stemmed from the cultural circumstances of the countries or whole regions of the world in which passenger aviation was present and in which the postulated principles of CRM training were to be introduced.

The above-mentioned issue is frequently illustrated in the source literature by citing the conclusions made by a Dutch scientist, Geert Hofstede[26].

Following his analysis of cultural determinants influencing the quality of cooperation within crews, he established three groups of countries (world regions) which are natural representatives of the distinctive ways in which the matter of introducing CRM programmes is approached.

The first group comprises those countries (e.g. China), whose citizens are taught almost from the day they are born that they should obey to the letter any decisions made by an authority and in which any displays of their own initiative which are contrary to a decision made by a leader are always viewed as lack of due respect.

The second group comprises countries (such as the USA) in which individualism and independence are highly valued and in which an aim of an individual is given priority over interests of a group. Even though this way of looking at an individual and the recognition of his place in society is by all means justified, a crew that was brought up only in such a spirit will find it harder to establish "grounds" for a common, collective approach to problem solving.

The third group, represented by e.g. Greece and some of the countries in Latin America, are the countries in which teams working on common tasks achieve better results if they follow clearly defined rules of conduct. What's important is that this is precisely the group of countries in which there is the highest level of receptiveness to accepting the CRM concept defined in terms of required behaviours.

Given the above, it is easier to understand the conclusions made by the scientists examining the matter of differences in the implementation of CRM in various parts of the globe[27].

With reference to the first and second generation CRM programmes in particular, they stated that the assumption according to which said programmes would be equally adopted in any place they would be given a chance to exist, was fundamentally flawed. The common phenomenon at that time, i.e. a trade in CRM training courses, whereby one carrier would purchase such a training course from another carrier, both foreign and domestic, in order to reproduce it word for word at the receiving carrier's, could not have produced the anticipated advantages, as it did not take into account the organisational culture and operational specificity of the receiving carrier.

Due to that, the fourth generation CRM concept was primarily focused on taking into account the cultural differences among their target group. Equally important is the fact that the said concept brought to the forefront, the necessity to develop and follow in practice the standards, procedures, best practices and applicable regulations.

Fifth generation – Present day. Legal basis of CRM training

The fifth generation of CRM training is the training conducted in the current form.

The air carriers from many countries who are grouped around the aviation authorities having jurisdiction over a given part of the world have a possibility and, at the same time, an obligation to apply the specific standards and procedures set forth by those authorities and included in the applicable regulations in their commercial, training and operational activities.

Since 1979, the Joint Aviation Authorities (JAA) had been an authority with jurisdiction over those of the European countries that voluntarily joined this organisation, whereas the Joint Aviation Requirements (JARs) had been the documents describing in detail the area of training, including CRM training courses, and the obligations and rules connected with conducting aviation activities by air operators[28].

With time, the regulations developed by the JAA, which were, in fact, not binding, as they were adopted and followed by the associated countries on a voluntary basis, had been gradually superseded by the EU regulations. In 2002, a new

[26] See: E. Danecka-Łatka. *"Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy"*. Problemy Zarządzania, vol.9, nr.4, Wydział Zarządzania UW.

[27] See: Robert L. Helmreich, Ashleigh C. Merritt i John A. Wilhelm. *"The Evolution of Crew Resource Management Training in Commercial Aviation"*. The International Journal of Aviation Psychology, no. 1 (1999).

[28] Poland joined the JAA on 26 November 2002.

organisation was created, which as an EU body had taken over all of the duties of the JAA. It is called the European Aviation Safety Agency (EASA)[29]. Nowadays, aside from the European Commission, EUROCONTROL and aviation authorities from the EU Member States, the EASA is one of the institutional pillars of the air safety system in Europe[30].

Although the regulations drafted by the EASA, under EU law, are applicable to EU Member States, one has to bear in mind the fact that this organisation is in close cooperation with its counterparts around the world, including the International Civil Aviation Organisation (ICAO), the Federal Aviation Administration (FAA) in the United States and aviation authorities from Canada, Brazil, Israel, China, Switzerland and Russia. The aim of the working arrangements signed between the Agency and these authorities is the harmonisation of standards and promotion of best practices in the field of aviation safety around the world[31].

The regulations developed by the JAA and adopted by the EASA are quite comprehensive and, at the same time, set very strict standards for CRM training. Pursuant to these regulations, the CRM training courses should be conducted by appropriately qualified personnel, while their syllabus, which is to be included in the Operations Manual of the air operator, may not disregard any of the following topics:

- human error and reliability, error chain, identification and prevention of faults;
- the company's safety culture, SOPs, organisational factors;
- stress, stress management, fatigue and vigilance;
- obtaining and handling information, situational awareness, workload management;
- decision making;
- communication and coordination inside and outside the cockpit;
- leadership and team behaviour, synergy;
- automation, philosophy of the use of automation (if relevant to the type);
- type-related differences;
- case studies.

The training modules taken from the above list should also be included in the training syllabi of a type-specific training, conversion training (when switching between an employer and/or air operator), commander training (for candidates for aircraft commanders) and periodical training (refreshing, recurrent, annual).

What is important is that the operator should, as far as it is possible, provide joint CRM training for both the flight crews and other personnel comprising the aircraft crew.

Such training should reflect the organisational culture of a given operator, while the theoretical and practical framework should afford the opportunity to discuss and share experience in an uninhibited manner, particularly with respect to lack of exchange of information or any deficiencies therein, as well as errors in the communication process between crew members.

As should have been expected, the EASA[32] regulations which have been in force for a few months now in no way liberalise the standards specified in the Joint Aviation Requirements drawn up by the JAA; on the contrary, they have made them even more stringent.

For instance, the new regulations do not provide for allowing a pilot to conduct operations without supervision, unless he first takes part in the CRM training within the scope foreseen for the initial training.

Moreover, regardless of the nature of the operations which a given pilot will be undertaking in commercial air transport, it is mandatory for him

[29] The European Aviation Safety Agency (EASA) was established pursuant to the Regulation (EC) No 1592/2002 of the European Parliament and of the Council. It began its operations in September 2003. Its current legal basis is the Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, the Regulation (EC) No 1592/2002 repealing the Council Directive 91/670/EEC, and the Directive 2004/36/CE (Official Journal L 79, 19/3/2008). The headquarters of EASA was at first located in Brussels. In November 2004, the headquarters was moved to Cologne in Germany.

[30] The result of the provisions of the Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008, pursuant to which EASA had taken over from JAA the jurisdiction over licensing flight personnel, flight operations and assessment of safety of aircraft from third countries, was an official dissolution of the Joint Aviation Authorities (JAA) on 30 June 2009.

[31] See: http://easa.europa.eu/language/pl/more-about-EASA.php.

[32] Provisions included in the Commission Regulation (EU) No /2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008.

to undergo training in human factor, before being cleared for said operations; what is important is that the said training shall be conducted at a level applicable to the highest category of pilot license, i.e. Air Transport Pilot License (ATPL). Where the pilot fails to meet the above-mentioned requirement, the duty to conduct such training now rests with the air operator who employs said pilot. Additionally, it is the operator's role to conduct the subject-matter training in accordance with the schedule which must closely reflect the thematic scope concerning the possibilities and limitations of human beings covered by the ATPL syllabus.

Summary

Given the absolute dominance of the human factor in the causes of aviation occurrences it would be appropriate to assume that, in the intervening years between the establishment of this fact and the present day, such a situation would have undergone profound changes. Additionally, one should also assume that any actions limiting that factor, including the CRM training, should have an absolute priority with respect to their adoption, particularly in commercial air transport.

However, as proven by the analysis of the way in which CRM training evolved, and in light of it, the analysis of the actions taken to restrict the detrimental effects that the human factor has on air operations, our assumptions would likely fail to be confirmed by the reality.

It turns out that our aviation awareness has been rising for a disproportionately long time given the gravity of the issue. There were many reasons why this state of affairs had come about, chief among them was lack of equal responsiveness (on the part of authorities, operators, and flight personnel) to a newly identified problem and, for a long time, lack of agreed and common (for the authorities, operators, and personnel) standards for mitigating the adverse effects of the human factor. The efficiency of the actions that were undertaken was also diminished by organisational issues, financial problems and frequent (mainly among flight crews) belief that their skills and competences were being subjected to psychological manipulation.

Fortunately for us (i.e. the crews and the passengers), the issue analysed here has now been recognised, defined and correctly understood, but this does not mean that it has been obviated.

To sum up the material discussed above, it should be unequivocally stated here that the presence of the human factor, which continues to be the main cause of the majority of aviation occurrences, is inherently connected with the existence of manned aviation. Even though the understanding of the capabilities and limitations resulting from human nature as well as the process of applying actions aimed at eliminating human factor from the causes of aviation occurrences do not have such a long tradition, it is nevertheless significant that the problem has been noticed and attempted to be rectified.

But what are the results?

In fact it is hard to assess them because it is difficult to compare the number of aviation occurrences stemming from the human factor in the period of time in which we have attempted to combat it with the number of occurrences that might have taken place in that period of time, if such attempts had not been made. There have been too many variables in the analysed period, of which a fundamental role in "contaminating" the results of analyses would have an ever-increasing number of air operators, air operations and new aircraft. Those aircraft have been, on the one hand, increasingly safe but, on the other hand, more and more technically sophisticated, and, for this reason alone, more demanding, absorbing and burdening the crews with a greater workload.

It is hard to put a finger on the numbers; however, it may be stated without hesitation that, if the adverse effects of the human factor had not been tackled, there would have been many more aviation occurrences involving it. Naturally, this does not go to say that the potentially suitable avenues of action leading to the elimination of the human factor from the list of main causes of aviation occurrences have been explored.

It merely means that... they have not been discovered yet.

Bibliography

Baron R., *Barriers to Effective Communication: Implications for the Cockpit.* http://airlinesafety.com.

Beaty D., *Pilot. Naga prawda. Czynnik ludzki w katastrofach lotniczych*, Wydanie I, Warszawa 2013.

Burigan S., *Situational awareness – staying ahead of the aircraft*, AirRescue, International Air Rescue & Air Ambulance Magazine, Vol. 2/2012, 33-37.

CAP 737 Crew Resource Management (CRM) Training. Guidance For Flight Crew. CRM Instructors (CRMIS) and CRMI Instructors-Examiners (CRMIES). UK Civil Aviation Authority, 2006.

Cooper George E., White Maurice D., Lauber John K., *Resource Management on the Flight Deck*, Proceedings of a NASA/Industry Workshop Held at San Francisco, California, June 26–28, 1979, NASA Conference Publication 2120.

Danecka-Łatka E., *Zarządzanie zasobami załogi (CRM) w dobie globalizacji rynków pracy*, Problemy Zarządzania, vol. 9, nr 4, Wydział Zarządzania UW.

Gałązkowski R., *Powstanie Samodzielnego Publicznego Zakładu Opieki Zdrowotnej Lotnicze Pogotowie Ratunkowe. Nowa struktura i zadania*, Lotnicze Pogotowie Ratunkowe, praca zbiorowa pod redakcją R. Gałązkowski, Wydanie I, Warszawa 2010.

Helmreich Robert L., Merritt Ashleigh C. i Wilhelm John A., *The Evolution of Crew Resource Management Training in Commercial Aviation*, The International Journal of Aviation Psychology, nr 1 (1999).

Kostera M., *Podstawy organizacji i zarządzania*, WSPiZ, Warszawa 2001.

Koźmiński A.K., Piotrowski W., *Zarządzanie. Teoria i Praktyka*, PWN, Warszawa 2002.

Necki Z., *Komunikacja międzyludzka.* Wyd. Profesjonalnej Szkoły Biznesu, Kraków 1996.

"Pilot's Handbook of Aeronautical Knowledge". U.S. Department of Transportation, Federal Aviation and Administration, Flight Standard Service, 2008, Chapter 17 "Aeronautical Decision Making", 17-2.

Roguski J., *„Przełom". Polskie Lotnictwo Sanitarne 1955–2005*, praca zbiorowa pod redakcją R. Gałązkowski i P. Kłosiński, Wydanie I, Warszawa 2005.

Rozporządzenie Komisji (UE) nr 965/2012 z dnia 5 października 2012 r. ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do operacji lotniczych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 z dnia 20 lutego 2008 roku, w sprawie wspólnych zasad w zakresie lotnictwa cywilnego i utworzenia Europejskiej Agencji Bezpieczeństwa Lotniczego.

Słownik łacińsko-polski, PWN, Warszawa 1973.

Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors, The Journal of the Human Factors and Ergonomics Society, March 1995.

Truszczyński O., Biernacki M., *Zarządzanie zasobami załogi a efektywność wykonywania zadań lotniczych*, Polski Przegląd Medycyny Lotniczej Nr 4, Tom 12, październik–grudzień 2006.

Ustawa o ustanowieniu programu wieloletniego *Wymiana śmigłowców Samodzielnego Publicznego Zakładu Opieki Zdrowotnej Lotnicze Pogotowie Ratunkowe w latach 2005-2010*, z dnia 3 czerwca 2005 r. (Dz.U. Nr 122, poz. 1022).

Wspólne Wymagania Lotnicze JAR-OPS 3, Zarobkowy Przewóz Lotniczy (Śmigłowce), Zmiana 5, Wydanie z 1 lipca 2007 r.

Zarządzenie Ministra Zdrowia z dnia 03 marca 2000 roku w sprawie utworzenia Samodzielnego Publicznego Zakładu Opieki Zdrowotnej (Dz.Urz. MZ. 2000, Nr 1 poz. 4).

Zarządzenie Ministra Zdrowia z dnia 03 marca 2000 roku w sprawie likwidacji Centralnego Zespołu Lotnictwa Sanitarnego (Dz.Urz. MZ 2000, Nr 1 poz. 5).

Internet sources:

http://airlinesafety.com
http://easa.europa.eu/language/pl/more-about-EASA.php
http://www.baaa-acro.com
http://www.lotnictwocywilne.republika.pl/crm.html
http://www.pl.wikipedia.org

Zeszyty Naukowe AON nr 2(99) 2015
ISSN 0867–2245

KOMUNIKATY, KOMENTARZE, RECENZJE I SPRAWOZDANIA

RECENZJA KSIĄŻKI MARKA BODZIANEGO I KATARZYNY DOJWY „PUBLIC RELATIONS INSTYTUCJI BEZPIECZEŃSTWA"

Paweł KOCOŃ
Uniwersytet Ekonomiczny Katowice

Streszczenie

Public Relations, jako dziedzina sztuki i nauki, jest relatywnie nowym zjawiskiem. Bardzo szeroko stosowana zarówno w firmach nastawionych na produkt i zysk, jak i organizacjach non-profit. Korzystają z jej dobrodziejstw politycy, gwiazdy showbiznesu, prominentni biznesmeni, czy największe światowe korporacje. Korzysta także wojsko. U progu XXI wieku, kiedy szybkość przepływu informacji i jej wpływ na otoczenie są bardzo istotne, umiejętne wykorzystywanie i znajomość narzędzi komunikacji przyczynia się do lepszego zrozumienia misji wojska oraz zdobycia wsparcia społeczeństwa dla realizacji założonych celów.

Słowa kluczowe: Siły Zbrojne, Policja, Straż Miejska, Public Relations

Wstęp

Tematyka bezpieczeństwa to obszar niezwykle ważny nie tylko ze względu na sytuację międzynarodową, gdzie różnego rodzaju konflikty toczą się niemalże u granic Polski, ale także ze względów poznawczych. Ukonstytuowane niedawno w Polsce nauki o bezpieczeństwie mają wiele obszarów niezbadanych – atrakcyjnych dla badaczy. Jednym z takich obszarów jest rola komunikowania w zapewnieniu bezpieczeństwa. Przynajmniej częściowo lukę tą podjęli się zasypać Katarzyna Dojwa – politolożka i socjolożka doktor nauk humanistycznych pracująca w Instytucie Socjologii Uniwersytetu Wrocławskiego, oraz Marek Bodziany – żołnierz podpułkownik doktor nauk humanistycznych pracujący w Wyższej Szkole Oficerskiej we Wrocławiu. Ich dzieło „Public relations instytucji bezpieczeństwa" wpisuje się we wspomnianą lukę w naukach o bezpieczeństwie, a do tego zapoznaje czytelnika z istotną dziedziną zarządzania, jaką jest public relations.

Pisanie o instytucjach bezpieczeństwa obarczone jest ryzykiem niewłaściwego wyboru organizacji wybranych do opisu. Szeroko definiowane bezpieczeństwo jak na przykład jako (...) dziedzinę, która zmierza do zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach[1], pomnaża organizacje potencjalnie zajmujące się bezpieczeństwem. W tej sytuacji autorzy słusznie postąpili, wybierając do opisu wojsko, policję i straż gminną. Należy zauważyć, że opisywane straż gminna i policja są polskie, a wojsko amerykańskie (USA). Ten ostatni wybór autorzy argumentują tradycjami armii USA.

O ile wybór jest trafny, o tyle wydaje się, że argument taki powinien być uzupełniony adnotacją o toczonej przez siły zbrojne USA wojnie w Wietnamie, która stanowiła przełom w myśleniu o roli komunikowania z otoczeniem w działaniach sił zbrojnych. Otóż pomimo wszelkich danych mówiących o zwycięstwie wojsk USA – wyższych strat ludzkich Vietcongu, wyparcia partyzantów komunistycznych z opanowanych przez nich terytoriów czy wreszcie pokrzyżowanie ich planów zarówno w wymiarze taktycznym, jak i strategicznym, armia USA musiała się wycofać, oddając sojusznika na pastwę wroga tylko dlatego, że nie uzyskała akceptacji swoich działań. Doświad-

[1] S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Adam Marszałek, Toruń 2006, s. 7.

czenia wietnamskie, jakie zdobyła US Army, są niezwykle ważne i pouczające dla wojsk państw demokratycznych, a wykorzystanie tych doświadczeń wydaje się być wysoce zasadne.

Cześć metodologiczna pracy

Opisywana książka liczy 10 rozdziałów, gdzie pierwsze 5 poświęcone jest szeroko rozumianej metodyce i metodologii public relations. W pierwszym rozdziale autorzy kompetentnie opisują genezę public relations, wymieniając jako praźródła m.in. „Retorykę" Arystotelesa czy „Księcia" Niccolň Machiavelliego. Marek Bodziany i Katarzyna Dojwa piszą także o bardziej współczesnych twórcach public relations, takich jak Amos Kandall, Pineas Barnum czy Ivy Lee. Nie są przemilczane zagadnienia kontrowersyjne i drażliwe, takie jak wykorzystanie metod i technik public relations przez Goebelsa czy przez terrorystów.

Drugi rozdział „Public relations współcześnie" autorzy rozpoczynają od opisu modeli public relations autorstwa Gruniga i Hunta, by następnie przejść do opisu instytucjonalnych rozwiązań w dziedzinie PR[2] a w dalszej kolejności – do współczesnych definicji public relations. Przegląd definicji, jaki prezentują autorzy jest jednym z najszerszych na polskim rynku wydawniczym. Autorzy opisują także funkcje public relations. Bardzo ważnym wątkiem poruszanym przez autorów jest specyfika public relations instytucji publicznej. Autorzy wychodzą w swoich rozważaniach od cech charakterystycznych organizacji publicznej, aby przejść do celów, jakie stoją przed PR takiej organizacji, będących konsekwencją osiągania tych celów efektów wizerunkowych PR organizacji publicznej. Podrozdział autorzy kończą, przytaczając za Krystyną Wojcik[3] najczęstsze błędy popełniane przez pracowników PR organizacji publicznych.

Następny podrozdział traktuje o specyfice pracy osoby zatrudnionej w branży public relations. Autorzy szczegółowo opisują kompetencje, jakie winna mieć osoba pracująca w branży PR, ponadto wymieniają cechy charakterologiczne takich osób. Wydaje się, że pewnym niedostatkiem tego fragmentu książki jest brak refleksji na temat cech „PR owca" pracującego w opisanych organizacjach bezpieczeństwa. A przecież cechy żołnierza czy policjanta mogą nie pokrywać się z cechami pracownika public relations, a wręcz mogą być z nimi sprzeczne. Nadto ciężar spraw, które dotykają żołnierzy czy policjantów zajmujących się public relations jest większy niż spraw dotyczących fabryki – śmierć żołnierzy na polu walki, rozwikłanie sprawy morderstwa czy też informacja o znalezieniu zwłok osoby zaginionej to sprawy, jakimi się nie zajmują specjaliści pracujący w bankach czy w firmach doradczych. Byłoby to tym lepsze, że piśmiennictwo w tym zakresie jest stosunkowo ubogie, jeden z nielicznych artykułów na ten temat napisał kpt. Szczepan Głuszczak szef Sekcji Prasowej 11LDKPanc[4].

W czwartym rozdziale pracy autorzy poruszają praktyczne aspekty public relations. W tym rozdziale skupiają się oni nad instytucjonalnym osadzeniem tej działalności, czyli miejscem PR w organizacji. Autorzy opisują rodzaje otoczenia organizacji i grup docelowych PR a także – co ważne – szeroko prezentują rozróżnienia pomiędzy różnymi formami działalności firmy takimi jak wyżej wspomniane a także promocją, reklamą, marketingiem. Dogłębnie opisują tajniki wewnętrznego public relations, podsumowując rozważania o nim istotnym przykładem z działalności policji. Podobnie dużo piszą o komunikacji zewnętrznej organizacji i kontaktach z mediami. Zaletą tego tekstu jest bardzo dobre osadzenie w teorii zarządzania – autorzy korzystają z klasycznych pozycji dotyczących public relations i komunikowania, korzystając z nich w taki sposób, że czytelnik otrzymuje skoncentrowaną treść dokładnie odpowiadającą tematyce książki. Pewnym niedostatkiem tego rozdziału jest stosunkowo słabe osadzenie w realiach organizacji bezpieczeństwa, miejscu PR w ich taktyce i strategii. Wydaje się, że interesujące byłoby na przykład ukazanie relacji pomiędzy wojną psychologiczną a PR.

Następnym zagadnieniem, z jakim zmagają się autorzy, jest public relations w środowisku wielokulturowym. Jest to ważne zagadnienie z kilku względów:

– public realations organizacji publicznych odbywa się niemal zawsze w otoczeniu wielokulturowym. Dotyczy to nie tylko styku religii czy narodów ale także grup etnicznych i styków regionów.

[2] Public Relations.

[3] K. Wojcik, *Public relations. Wiarygodny dialog z otoczeniem*, Placet, Warszawa 2005, s. 794.

[4] Szczepan Głuszczak *Oficer Prasowy – wojskowy PRowiec*. www.proto.pl/PR/Pdf/Oficer_prasowy_wojskowy_PR-owiec.pdf pobrane 15.05.15.

– wokół styków kultur rozgrywają się konflikty – etniczne, religijne czy też ekonomiczne

– jednocześnie globalizacja i sieć informatyczna powodują, że w zakresie bezpieczeństwa możliwa jest współpraca pomiędzy przedstawicielami różnych kultur.

Autorzy „Public relations instytucji bezpieczeństwa" unieśli zadanie, jakie przed sobą postawili. Sposobem na rozwikłanie dylematów było – w przypadku autorów – odwołanie się do klasyki socjologicznej. Marek Bodziany i Katarzyna Dojwa opisują wielokulturowość, ujmując ją jako klucz do PR, aby następnie przejść do zagadnień teorii dialogu kultur. Trochę brakuje w tych dwu podrozdziałach opisu monokulturowości, czy też większego docenienia elementów wspólnych dla różnych kultur, które także pomagają we wzajemnym porozumieniu.

Następnie opisane są kulturowe uwarunkowania public relations. W tym miejscu autorzy słusznie przytaczają pojęcie glokalizacji, a także zarządzania międzykulturowego. Powołują się także na teorię konfliktu i teorię przypadkowości, co dopełnia treść wywodu. Rozdział o komunikacji międzykulturowej i jej związkach z PR nie może obyć się bez obszernego opisu barier komunikacji międzykulturowej i ograniczeń PR. W tym miejscu autorzy szczególną uwagę zwrócili na stereotypy i uprzedzenia. Jest to rozwiązanie bezpieczne i konserwatywne ze wszystkimi wadami i zaletami.

Część metodologiczną pracy zamyka opis zarządzania kryzysami w organizacji. Najpierw autorzy zajęli się kwestią znaczenia pozytywnego wizerunku dla organizacji, przy czym autorzy skupiają swoją uwagę na policji i wojsku w kontekście zmiany ustrojowej. Osią dalszych rozważań jest zarządzanie problemowe i rodzaje oraz atrybuty sytuacji kryzysowych. Podsumowaniem rozdziału są rozważania na temat PR w sytuacjach kryzysowych. W tym podrozdziale opisano, jak winno się prowadzić działania public relations w sytuacji kryzysowej; stanowi on swego rodzaju instrukcję dla osób zajmujących się PR – nie tylko zresztą w wojsku czy w policji. Jest na przykład w książce zamieszczony szczegółowy plan postępowania w sytuacji kryzysowej, zaczerpnięty z pozycji Tymona Smektały[5]. Autorzy wykazują rolę PR w sytuacji kryzysowej w organizacji, która nie jest tylko „panaceum" na jej kłopoty, ale pełni także rolę prewencyjną.

Metodologiczna część pracy sprawia wrażenie solidnej, tradycjonalistycznej budowli, która nie zawiera w sobie z jednej strony żadnych „gadżetów", ale z drugiej strony jest zbudowana ze sprawdzonego materiału. Autorzy obficie cytują między innymi Krystynę Wojcik, Frasera P. Seitela, Annę Adamus Matuszyńską i Tomasza Gobana Klasa. Dobór literatury jest trafny, a proporcje pomiędzy cytowaniami i ich komentarzem właściwe. Autorzy rozbudowali opis podstawowych pojęć do nieco ponad połowy książki. Tak wnikliwe rozpatrzenie problemu daje czytelnikowi możliwość rozpoznania tego, czym powinni kierować się pracownicy organizacji bezpieczeństwa odpowiedzialni za ich wizerunek. W ten sposób część metodologiczna pracy ma charakter postulatywny, a nie jest dekonstrukcją rzeczywistych algorytmów postępowania służb PR w opisywanych organizacjach.

Autorzy rzadko komentują przytaczane teksty, co nieco utrudnia lekturę tekstu osobom nie będącym naukowcami, ale z drugiej strony unika się w ten sposób chaosu i chybionych interpretacji. Czytelnik dowiaduje się więc, dlaczego opisane w książce działania PR winny spotkać się z pochwałą lub krytyką.

Studia przypadków

Pierwszym zagadnieniem, jakie rozpatrują autorzy, jest PR polskiej policji. Z pasją omawiają najpierw specyfikę wizerunku policji – organizacji zmagającej się ze trudnymi do spełnienia oczekiwaniami społeczeństwa i ze złym traktowaniem przez obywateli. Co istotne, policja jest organizacją, której brak realizacji celów działania może skutkować nie ograniczeniem przyznanych środków, ale wprost przeciwnie: przyznania większych uprawnień i funduszy. Innymi słowy, wzrost przestępczości spowodowany nieudolnością policji może przynieść jej profit w postaci przyznania szerszych uprawnień do działania, czyli de facto władzy.

Autorzy następnie opisują miejsce PR w strukturze policji i uwarunkowania prawne jej komunikacji z otoczeniem. Zwłaszcza opis tych ostatnich wydaje się niezwykle ważny. Z uwagi na hierarchiczność i autorytaryzm kultury organizacyjnej policji, omawiane są także inne praktyczne aspek-

[5] T. Smektała, *Public Relations w sytuacjach kryzysowych przedsiębiorstw*, Astrum, Wrocław 2001 s. 101–103.

ty pracy działu prasowego tej organizacji (to on jest odpowiedzialny za wizerunek tej formacji). Autorzy przeanalizowali także publikacje policyjnego miesięcznika „997" analizując przykłady różnorodnych działań komunikacyjnych tej organizacji.

Dużo informacji na temat PR policji znalazło się w rozdziale ósmym. Choć jest on zatytułowany „Case Study w sytuacji kryzysowej PR policji w świetle opolskiej afery taśmowej" to autorzy, zamiast jednej, omawiają w nim kilka ważnych spraw, które pokazały funkcjonowanie policji w sytuacjach dla niej kryzysowych. Pierwszą z takich sytuacji była niewątpliwie sprawa „Małej Madzi". Tu problemem było to, że dla dobra sprawy policja nie dzieliła się swoimi podejrzeniami wobec matki zabitej dziewczynki. Natomiast detektyw Rutkowski nie miał tego typu obostrzeń co spowodowało, że to on, a nie policja pierwszy powiadomił o winie matki ofiary. Tern sposób postępowania pana Rutkowskiego ukazał policję w niekorzystnym świetle, jako organizację powolną i niekompetentną. Problem polega na tym, że organizacja publiczna mająca obowiązek pracy dla dobra wspólnego została konkurentem organizacji komercyjnej mającej pozbawione skrupułów kierownictwo.

Pozostałe sprawy opisywane przez autorów występują na kartach książki na zasadzie „i śmieszno i straszno". Pewien aspekt komiczny jest w sprawie szkolenia policjantów, w którym jeden z elementów polegał na pchaniu samochodów. Obserwujący (i nagrywający) to szkolenie komentowali je jako symulację policyjnego pościgu. W istocie policjanci pchający pojazd „uciekający" i pojazd „goniący" w pościgu są komiczni, tyle tylko, że śmieszność nie jest w żaden sposób potrzebna organizacji zaufania publicznego, jaką jest policja. W toku postępowania kontrolnego okazało się że „pościg" by de facto przygotowaniem niesprawnych samochodów do zajęć statycznych. Problemem – także dotyczącym morale policji – była interpretacja zdarzenia przez obserwatorów a także nagrywanie go (z prześmiewczym komentarzem) zdarzenia przez funkcjonariuszy policji.

Straszno można określić aferę, która dała nazwę całemu rozdziałowi. 23 maja 2013 roku opublikowano w dwu gazetach rozmowę pomiędzy komendantem wojewódzkim policji a jego podwładną. Rozmowa dotyczy m. in. kwestii osobistych – relacji seksualnych pomiędzy komendantem i jego podwładną, a także niedopuszczalnych zachowań innych funkcjonariuszy. Policja ma w tym momencie dwa problemy:

1. Pojawienie się patologicznych zachowań w opolskiej policji.
2. Podsłuchiwanie rozmów funkcjonariuszy.

W społecznej świadomości zaistniał tylko pierwszy z problemów, który policja zaczęła rozwiązywać poprzez natychmiastowe zwolnienie komendanta i zawieszenie jego podwładnej. Tyle tylko, ze komendant nie niepokojony odszedł na emeryturę, a zamieszana w rozmowę policjantka zostaje poddana postępowaniu dyscyplinarnemu. Pojawia się ważny aspekt sprawy, jakim jest nierówność w traktowaniu kobiet i mężczyzn. Policja na ten zarzut zareagowała swoistym kontratakiem, mianując na wakujące stanowisko komendanta kobietę, co niejako skończyło aferę.

Autorzy z pasją i naukową dociekliwością potraktowali kryzysy wizerunkowe policji. Cześć z opisanych przykładów jest powszechnie znana, ale nowością, wkładem własnym autorów jest spojrzenie na opisane zdarzenia oczami policji. Spojrzenie z punktu widzenia interesów tej formacji, a nie jej publiczności. Na koniec autorzy sygnalizują obszar niewiedzy, jaki pozostaje po analizie „afery podsłuchowej" – są to rozmaite aspekty PR wewnętrznego policji.

Rozdział „Wojenne" i „Pokojowe" Public Relations Amerykańskich Sił Zbrojnych. Tytuł rozdziału jest o tyle mylący, że autorzy wspominają także o PR SZRP.

Opisując genezę wojskowego PR, autorzy słusznie powołują się na Wrighta Millsa a także wojnę wietnamską. Ta ostatnia została przez autorów potraktowana nieco po macoszemu, a szkoda, bo zaszła tu bardzo ważna rzecz – całkowita rozbieżność pomiędzy osiągnięciem celów w wymiarze wojskowym, takich jak kontrola terenu czy zadanie strat przeciwnikowi, z celami politycznymi, a co za tym idzie, komunikacyjnymi.

Błędy komunikacyjne z Wietnamu zostały naprawione już w czasie amerykańskich interwencji w Grenadzie i Panamie. Szczytem możliwości komunikacyjnych wojsk USA była pierwsza wojna z Irakiem w 1991. Nim siły irackie zostały zmuszone do wycofania z Kuwejtu po poniesieniu znacznych strat w ludziach i sprzęcie, zostały dosłownie przytłoczone propagandą koalicji. Autorzy recenzowanej książki dokładnie opisują kroki podjęte przez koalicję, by kreować i kontrolować przeka-

zy medialne. W uproszczeniu wyglądało to w ten sposób, że dziennikarze otrzymywali atrakcyjne newsy w zamian za wolność swojej wypowiedzi. Będzie to „deal" powtarzany m.in. w czasie działań w Strefie Gazy czy bombardowań Serbii.

Autorzy szczegółowo opisują także drugą wojnę w Iraku w 2003 roku. Tu działania PR są oceniane niżej przez autorów, niż te 12 lat wcześniej, choć trzeba przyznać, że służby PR USA miały kilka ciekawych pomysłów, jak stworzenie talii kart z najbardziej poszukiwanymi funkcjonariuszami reżimu, czy wykorzystanie historii Jessiki Lynch. Historia ta jest znana, ale trzeba zaznaczyć, że autorzy kompetentnie ją nie tylko opisali, ale i zinterpretowali. Podobnie było z niemal „ikonicznym" wydarzeniem z czasu tej wojny – obaleniem pomnika Saddama Husseina.

Wydaje się, że najbardziej niewykorzystaną szansą opisywanej książki jest podrzodział Public Affairs w siłach zbrojnych. Tak jak uprzednio, autorzy kompetentnie opisują pojęcie public affairs, by przejść do opisu rozwiązań praktykowanych w SZ RP. Opis ten jest koherentny i nie zawiera błędów merytorycznych. Problemem jest tu raczej usytuowanie i rozmiar. Lokalizacja opisu PR SZ RP jest nietrafna, bo jest on położony w tekście dotyczącym sił zbrojnych USA, których SZ RP nie są częścią. Ponadto widać, że autorzy zawarli „zgniły kompromis" pomiedzy opisem „kanonicznej" komunikacji z otoczeniem armii USA, a działaniami polskimi. Trzeba stwierdzić, że jest to jeden z nielicznych błedów w pracy. Nie tylko dla polskiego czytelnika (książkę należy wydać w języku obcym) znacznie ciekawsze będą perypetie polskiego komunkowania wojska z otoczniem. Poczynając od „ubrania w kamasze" stanu wojennego, gdzie nawet reporterzy telewizyjni byli ubrani w mundury wojskowe, poprzez powrót do tradycji II RP, a także perypetii wokół serialu „Kawaleria Powietrzna", do zmarnowanej szansy wizerunkowej, jaką była „Bitwa o City Hall" w czasie drugiej wojny Irackiej. Pominięto – a szkoda – wizerunek misji SZ RP w Iraku, Afganistanie czy na Wzgórzach Golan.

Siły Zbrojne Rzeczypospolitej Polskiej cieszą się dużym prestiżem społecznym[6] i prowadzą własną – zorientowaną silnie na marketing personalny – politykę komunikacyjną[7]. Dostrzegając kompetencje autorów i ich krytycyzm, należy wyrazić żal, że nie zajęli się krytyczną analizą tej polityki komunikacyjnej, że nie zmagali się z wyzwaniami stojącymi przed SZ RP choćby otwarciem na cywili szkół wojskowych, co jest jednocześnie szansą i zagrożeniem dla wizerunku SZ RP.

Ostatnie zadanie, jakie postawili przed sobą autorzy, można śmiało określić jako karkołomne. Postanowili oni „odczarować' wizerunek straży miejskiej (gminnej). Marek Bodziany i Katarzyna Dojwa opisali szeroko działania różnych tego typu formacji, nie unikając zarówno pozytywów, jak i błędów popełnianych przez funkcjonariuszy opisywanej formacji. Autorzy kończą swój opis pogłębioną analizą strony WWW wybranej straży miejskiej. Nadto w podrozdziale „Miesiąc ze strażą miejską" autorzy analizują dogłębnie i systematycznie działania wybranej formacji tego typu. Autorzy stawiają wniosek, że działania straży miejskiej ze swej natury rzadko przyciągają uwagę mediów, co przeszkadza jej funkcjonariuszom tworzyć właściwy wizerunek formacji.

Wypada w tym miejscu dodać, że straże są obciążone „grzechem pierworodnym" wynikającym z ich podległości władzom samorządowym. Są one więc często angażowane raczej do realizacji celu taktycznego, jakim jest stabilizacja budżetu gminy, a nie strategicznego, jakim jest dbanie o bezpieczeństwo. Mówiąc prościej, straż jest znacznie częściej angażowana do – za wszelką cenę – zbierania mandatów, niż do dbania o prewencję bezpieczeństwa.

Podsumowanie

Podsumowując, należy spytać, czy autorzy całościowo opisali temat sygnalizowany w tytule pracy. Tu należy powiedzieć, że nie tyle opisali wszystko (jest to niemożliwe), co wybrali reprezentatywne przykłady. Wielki nieobecnym zestawienia organizacji bezpieczeństwa są służby wywiadu i kontrwywiadu. Tak kontrowersyjne wydarzenia, jak weryfikacja funkcjonariuszy wywiadu PRL czy też rozwiązania WSI są warte pogłębionego opisu.

[6] M.in. Prestiż Zawodów Komunikat z badań CBOS 2009.

[7] M.in. Decyzja Nr 108 /MON Ministra Obrony Narodowej z dnia 7 kwietnia 2009 r. w sprawie zasad realizacji polityki informacyjnej w resorcie obrony narodowej (Dz. Urz. MON z 6 maja 2009 r. Nr 7, poz. 82).

Na zakończenie warto zweryfikować postawione cele pracy. Autorzy piszą: „oddawana do rąk czytelnika publikacja stawia rozmaite zapytania i wskazuje ścieżki, które prowadzą do niezmiernie istotnych zagadnień"[8].

To zbyt skromne podsumowanie pracy. Na solidnym fundamencie metodologicznym umieszczono tekst, który przede wszystkim inspiruje, drażni i skłania do dyskusji. Praca wraz z sygnalizowanymi miejscami budzącymi niedosyt, nie pozwala o sobie zapomnieć. Pazur, inspiracja, pewna doza kontrowersji zawarta w ostrej krytyce armii USA – to wszystko powoduje, że zachowane jest to, co w naukce najważniejsze – nowość i wyytczenie nieznanych ścieżek oraz inspiracja.

Wypada tylko napisać „Tak trzymać" i ciągle napominać autorów, by podjętą raz tematykę kontynuowali, wydając uaktualnioną książkę nie tylko po polsku, ale także w jezykach obcych.

[8] K. Dojwa, M. Bodziany, *Public Relations Instytucji Bezpieczeństwa*, WSO, Wrocław 2013, s. 233.

Bibliografia

Publikacje zwarte i czasopisma

Bodziany M Dojna K, *Public relations instytucji bezpieczeństwa*, WSO, Wrocław 2013.

Głuszczak S. Oficer Prasowy – wojskowy PRowiec *www.proto.pl/PR/Pdf/Oficer_prasowy_wojskowy_PR-owiec.pdf*

Koziej S., *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*. Adam Marszałek, Toruń 2006,

Smektała T., *Public Relations w sytuacjach kryzysowych przedsiębiorstw*, Astrum, Wrocław 2001.

Wojcik K., *Public relations. Wiarygodny dialog z otoczeniem*, Placet Warszawa 2005.

Dokumenty i raporty

Decyzja Nr 108 /MON Ministra Obrony Narodowej z dnia 7 kwietnia 2009 r. w sprawie zasad realizacji polityki informacyjnej w resorcie obrony narodowej (Dz. Urz. MON z 6 maja 2009 r. Nr 7, poz. 82).

Prestiż Zawodów Komunikat z badań CBOS 2009.

MAREK BODZIANOWSKI AND KATARZYNA DOJWA BOOK REVIEW – PUBLIC RELATIONS OF SECURITY INSTITUTIONS

Abstract

Public Relations, as a field of art and science, is a relatively new phenomenon.

Used very widely in companies focused on product and profit and non-profit organisations.

Politicians, celebrities, prominent businessmen, and the world's largest corporations enjoy its benefits. It is also used by the military.

At the dawn of the twenty-first century, when the speed of the flow of information and its impact on the environment were very important, skilful use and knowledge of communication tools contributed to a better understanding of the mission of the military and gained support for the carrying out of its goals in society.

Key words: The Armed Forces, Police, Municipal Police, Public Relations

Introduction

The subject of security is an area of great importance, not only because of the international situation, where all sorts of conflicts are taking place near to Poland's borders, but also for cognitive reasons. The science of safety has many unexplored areas that are attractive to researchers. One such area is the role of communication in ensuring safety. Catherine Dojwa – a political scientist and sociologist, doctor of Humanities working at the Institute of Sociology at the University of Wroclaw, and Marek Bodziany – soldier, Lieutenant Colonel, Doctor of Humanities working at the School of Officers in Wroclaw at least partially undertook to close that gap. Their work „Public relations of security institutions" fills the previously mentioned gap in safety science and, additionally, introduces the reader to the important area of management that is public relations.

Writing about security institutions carries the risk of improper selection of organisations. Widely defined safety such as (...) a field aiming to ensure the viability, growth and freedom in the achievment of its own interests in specific circumstances,multiplies the number of organisations potentially involved in security.

In this situation, the authors proceed in the right way, choosing the military, police and municipal guards that are to be described. It should be noted that the municipal police and the police are Polish and the military is American (USA). The authors argue that the last choice is miltary tradition.

While the choice is relevant, it seems that this argument should be supplemented by a note about the US forces war in Vietnam , which was a breakthrough in thinking regarding the role of communication within the environment in the activities of the armed forces. Despite of all the data regarding the victory of US armies, the higher Vietcong human losses, repression of communist guerrillas from the territories they dominated and, finally, the tangle of their tactical and strategic plans, the US military had to withdraw, leaving their ally at the mercy of the enemy just because it did not obtain approval for its actions. The experience gained by the US Army from Vietnam is extremely important and instructive for armies of democratic countries and these experiences seem to be highly relevant.

Methodological part of work

The book consists of 10 chapters; the first 5 are devoted to the widely understood methodology of public relations. In the first chapter, the authors describe the genesis of public relations, mentioning, among other things, Aristotle and Machiavelli's „Prince" as a pre-source . Marek Bodziany and Katarzyna Dojwa also write about more contemporary creators of public relations, such as Amos Kendall, Pineas Barnum and Ivy Lee. The controversial and sensitive issues, such as the use of methods and techniques of public relations by Goebbels or by terrorists, are also mentioned.

In the second chapter of „Public Relations Today," the authors begin by describing Grunig and Hunt's PR models and, then, go on to describe the institutional solutions in the field of PR 2 and, further, to a contemporary definition of public relations. The authors overview is one of the largest on the Polish publishing market. The authors also describe the functions of public relations. A very important theme raised by the authors is the nature of public relations in public institutions. They highlight the characteristics of a public organisation and identify their purpose before the PR, as a consequence of a PR image-public organisation achieving these objectives. The authors end the subsection by quoting Krystyna Wojcik's3 most common mistakes made by the staff of public PR organisations.

The next section deals with the work specifics of a person employed in the public relations industry. The authors describe in detail the responsibilities of a person working in the PR industry and, moreover, they exchange the behavioural attributes of such persons. It seems that there is herea lack of reflection on the characteristics of the PR person working in the described safety organisations. The features of a soldier or a policeman may not be the same as the characteristics of a public relations practitioner and, indeed, may be in conflict with them. Moreover, the weight of the issues that affect soldiers or police officers dealing with public relations is greater than the issues concerning ta factory - the death of soldiers on the battlefield and unravellinga murder case or information about finding the body of a missing person are matters which are not dealt with by professionals working in banks or in advisory firms. The literature in this area is relatively poor; one of the few articles on this subject was written by Capt. Stephen Głuszczak, the head of the press section of 11LDKPanc4.

In the fourth chapter, the authors describe the practical aspects of public relations. In this chapter, they focus on the institutional background of this activity and the place of PR in the organisation. The authors describe the types of environmental organisations and PR targeted groups and - more importantly – they broadly represent the distinction between the different forms of business mentioned above, as well as promotion, advertising and marketing. They describe the secrets of internal public relations in detail, summing up the discussion by including important examples of police activity. Similarly, they write a lot about the external communications of the organisation and its relations with the media. The advantage of this text is that it is very well embedded into management

theory - the authors make use of the classic positions on public relations and communication, using them in such a way that the reader receives a concentrated essence of the contents of a book. The shortcomings of this chapter are that it is relatively weak on the realities of security organisations and the role of PR in their tactics and strategies. It would be interesting, for example, to show the relationship between psychological war and public relations.

Public relations in a multicultural environment is another issue which the authors need to face. This is important for several reasons: - Public relations of public organisations almost always take place in a multicultural environment. This applies to religions and nations, as well as to ethnic groups and regional contacts: - there are ethic, religious and economic conflicts around contacts of culture

- at the same time, globalisation and the computer network mean that, in the scope of security, cooperation is possible between representatives of different cultures.

The authors of „Public relations of security institutions" managed to deal with the task put in front of them. The way to solve the dilemma was - in the case of these authors – to refer to the classics of sociology. Marek Bodziany and Katarzyna Dojwa describe multiculturalism, recognising it as the key to PR, then they move to questions of theory of dialogue between cultures. In these two subsections, there are no descriptions of mono - culture or a greater appreciation of elements common to different cultures helping mutual agreement.

Then, the cultural considerations of public relations are described. At this point, the authors rightly cite the concept of globalisation, as well as intercultural management. Also, they rely on the theory of conflict and the theory of randomness, which complements the content of the argument. The chapter on intercultural communication and its relationship with PR cannot do without a comprehensive description of intercultural communication barriers and restrictions on public relations. At this point, the authors paid special attention to stereotypes and prejudices. It is a safe and conservative solution with all the advantages and disadvantages.

The methodological part of the work closes with a description of crisis management in the organisation. First, the authorslook at the issue of the importance of a positive image for the organisation and focus on the police and military in the context of political change. An axis of further consideration is management of the problem and the types and attributes of emergencies. The summary of the chapter is a reflection on PR in crisis situations. This section describes how to lead a public relations crisis; it is a kind of manual for those involved in PR - and not only in the army or in the police. For example, a detailed action plan in a crisis situation, taken from the Tymon Smektały5 position is included in the book. The authors point to the role of PR in a crisis situation in an organisation that is not only a „panacea" for her troubles, but also acts as a preventative.

The methodological part of the work gives the impression of a solid, traditionalist structure that on the one hand does not include any „gadgets", but on the other hand, is built with proven material. The authors cite Christine Wojcik, Fraser P. Seitel, Anna Adamus Matuszyńska and Tomasz Goban Klasa. The selection of literature is accurate, and the balance between citations and commentary is correct. The authors expand the description of the basic concepts for little more than half the book. So, thorough consideration of the issue, reader gets the opportunity to identify what the employees of security organisations responsible for their image should take into consideration. In this way, the methodological part of work is postulate and it is not the deconstruction of actual algorithms of PR services that are acting in describing organisations.

The authors rarely comment on the quoted texts, which can make it difficult to read the text for people who are not scientists, but, on the other hand, avoids chaos and misinterpretation. The reader learns why the PR activities described should meet with praise or criticism.

Studies of cases

The PR of the Polish police is the first issue examined by the authors. First, they discuss with passion the specifics of the image of the police - an organisation struggling to meet the expectations of society and with the mistreatment of citizens. Importantly, the police is an organisation whose lack of implementation of the action objectives may result in no reduction of appropriations, but,

on the contrary, in granting more powers and funds. In other words, an increase in crime due to the incompetence of the police can bring profits in the form of granting wider powers, which means, de facto, authority.

The authors then describe the place of PR in the structure of the police and the legal conditions of its communication with the environment. The description of that last one seems to be very important. Due to the hierarchical and authoritarian organisational culture of the police, there are also other practical aspects of the work of the press department of the organisation (it is responsible for the image of the formation). The authors also analysed the police monthly „997" publication, taking into account examples of a variety of communication activities of the organisation.

Much information about police PR can be found in chapter eight. Although it is titled „Case Studies of the police PR crisis situation in the Opole tape scandal," the authorsdiscuss some important issues that have demonstrated the functioning of the police in emergency situations . Undoubtedly, the first such occasion was the matter of „Little Maggie". The problem here was that, for the good of the case, the police did not make public the suspicions against the mother of the murdered girl. However, the detective, Rutkowski, did not have this type of restriction which meant that it was he - not the police -who first announced that the victim's mother was guilty. Mr. Rutkowski's behaviour showed the police in a bad light, as slow and incompetent. The problem was that a public organisation with an obligation to work for the common good, became a competitor of a commercial organisation that had unscrupulous executives.

Other cases reported by the authors are mentioned in the book as „ ridiculous and terrible". The training of police officers, in which one of the elements relied on pushing cars, provided a certain comic aspect. Those following (who were recording) commented that this training was a simulation of a police chase. In fact, the policemen pushing the vehicle „fleeing" and the vehicle „chasing" are comical, but that ridicule isn't required in an organisation requiring public trust, such as the police. In the course of the audit procedure, it turned out that the „chase" was, de facto, the inefficient preparation of cars for static activities. The interpretation of the event by observers, as well as recording it (with mocking commentary) was the problem, which also concerned the morale of the police.

One can specify the affair, which gave its name to the whole unit, as "Terrible". On 23 May 2013, two newspapers published a conversation between the provincial police commander and his subordinate. The conversation concerns personal issues - sexual relations between the commander and his subordinate, as well as the unacceptable behaviour of other officers.

The police have, at this moment, two problems: 1. The appearance of pathological behavior in the police in Opole 2. The eavesdropping on officers' conversations

The public are only aware of the first problem, which was solved by the police through the immediate release of the commander and his subordinate. But the commander not disturbed was retired, and the policewoman involved in the conversation was subjected to disciplinary action. An important aspect of the case was the inequality in the treatment of men and women. The police responded to this objection with a kind of counterattack, appointing a woman to the vacant post of commander, which ended the affair.

The authors treated the police reputation with passion and scientific inquisitiveness. Some of the described examples are widely known, but ,what is new and is the authors own contribution, it is to look at the described events from the police point of view. At the end, the authors indicate that ignorance in this area remains after the analysis of the „phone hacking scandal" - these are the various aspects of internal police PR.

The chapter „War" and „Peace" of Public Relations of the United States Armed Forces has a confusing title and the authors also mentioned SZRP's PR.

Describing the genesis of military PR, the authors rightly refer to the Wright Mills and the War in Vietnam. This last one was treated a little neglectfully by the authors, which is a pity, because a very important thing has occurred here - the total discrepancy between the achievement of objectives in the military dimension, such as control of the land and enemy losses, and the political objectives followed by communication.

Communication errors from Vietnam were already fixed before the US intervention in Grenada and Panama. The peak of communications

capabilities in the US army was the first war with Iraq in 1991. Before Iraqi forces were forced to withdraw from Kuwait after incurring significant losses in people and equipment, they were literally overwhelmed by coalition propaganda. The authors of the reviewed book accurately describe the steps taken by the coalition to create and control media messages. In simple terms, it looked that way, that journalists received attractive news in exchange for the freedom of their expression. It will be a „deal" repeatedduring operations in Gaza and the bombing of Serbia, among others.

The authors describe the second war in Iraq in 2003 in detail. Here, PR activities are estimated by the authors to be worse than 12 years previously, although I must admit that the USA's PR had some interesting ideas, such as creating a deck of cards of the most wanted regime officials, regardless of the use of the Jessica Lynch story. This story is known, but it should be noted that the authors not only described it competently, but also interpreted it. The situation with the almost „iconic" of the toppling of the statue of Saddam Hussein was similar.

It seems that most missed opportunity of the book is the Public Affairs Section in the armed forces. As before, the authors competently describe the concept of public affairs, to describe the embodiments practiced in the Armed Forces. This description is coherent and contains no factual errors. The location and size are rather the problem. The location of the description of Polish Armed Forces' PR is irrelevant, because it is situated in the text concerning US armed forces, and the Polish Armed Forces were not part of it. In addition, you can see that the authors concluded there was a „rotten compromise" between the description of the „canonical" communication with the US Army and Polish activities. It must be said that this is one of the few errors in the work. Not only for the Polish reader (the book should be issued in a foreign language) will the adventures of Polish army communication with the environment be much more interesting. Starting with the „put in elastic-sides" of the state of war, where even TV reporters were dressed in military uniforms, by returning to the tradition of the Second RP, as well as the vicissitudes surrounding the „ Air Cavalry „ TV series, there was a wasted opportunity to improve the image, which was a „battle for City Hall" during the Second War in Iraq. The image of the Polish Armed Forces mission in Iraq, Afghanistan and the Golan Heights was unfortunately overlooked.

The Polish Armed Forces have a high social prestige and run their own highly marketing-oriented personal - communication policy. Recognising the competence of the authors and their criticism, we must express our regret that they did not address the critical analysis of this communication policy, and did not stuggle with the challenges of the Armed Forces, even the opening of military schools to civilians, which is both an opportunity and a threat to the image of the Polish Armed Forces.

The last task the authors were faced with, can be safely described as risky. They decided to „demystify" the image of the municipal police (municipal). Marek Bodziany and Katarzyna Dojwa widely reported the activities of various formations of this type, not avoiding the positives and mistakes made by officials of the described formation. The authors end their description with an in depth analysis of the web pages of selected municipal police. Moreover, in „A month with municipal guards," the authors deeply and systematically analysed the selected formations of this type. They concluded that municipal police action very rarely catches media attention, which prevents its officers creating a proper image of the formation.

It should be added here that the guards are burdened with „original sin" due to their subordination to local authorities. They are so often involved in achieving the tactical objective of stabilising the municipal budget, not in the strategic objective of taking care of security. To put it simply, a guard is more often engaged t - at any price – in collecting mandates, than to care for the prevention of security.

Summary

In summary, one should ask whether the authors described the theme indicated in the title integrally . Here, it must be said that it is impossible to describe everything, but they selected representative examples. The secret service and counterespionage are the great absentees of this work. Such controversial events, such as verification of the communist secret service

officers or WSI solutions are worth an in-depth description.

Finally, the goals of the work should be verified. The authors write that the: „Publication put into the hands of the reader asks the various questions and indicates the path that leads to extremely important issues"8

This is too modest a summary of the work. The text was provided on a solid methodological foundation, which primarily inspires, irritates and moves the discussion. The insufficiency of issues is not allowed to be forgotten. There is a certain amount of inspired controversy contained in the sharp criticism of the US military - which is most important in the science- and novelty in following unknown paths.

One could write „Go on" and constantly exhort the authors to continue to tackle the subject, issuing an updated book, not only in Polish but also in foreign languages.

Bibliography

Compact publications and magazines

Bodziany M Dojna K, Public relations instytucji bezpieczeństwa (Public relations of security institution), WSO, Wrocław 2013.

Głuszczak S. Oficer Prasowy – wojskowy PRowiec (Press Officer – PR man in Army) www.proto.pl/PR/Pdf/Oficer_prasowy_wojskowy_PR-owiec.pdf.

Koziej ST, Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku. (Between hell and paradise. Gray safety at the beginning of the twenty-first century) Adam Marszałek, Toruń 2006.

Smektała T, Public Relations w sytuacjach kryzysowych przedsiębiorstw. (Public Relations in crisis situations in companies) Astrum Wrocław 2001.

Wojcik K. Public relations. Wiarygodny dialog z otoczeniem, (Credible dialogue with the environment) Placet Warszawa 20005.

Documents and reports

Decission No 108/MON of Minister of National Defence, on 7 April 2009 on the principles of information policy in the Ministry of National (Dz. Urz. MON z 6 maja 2009 r. Nr 7, poz. 82).

Competition prestige; Communication Research CBOS 2009.

Odbiorcy „Zeszytów Naukowych AON"

Krajowi:

Ministerstwo Obrony Narodowej

Sztab Generalny WP

Biuro Bezpieczeństwa Narodowego

Dowództwo Wojsk Lądowych

Dowództwo 2. Korpusu Zmechanizowanego

Dowództwo Wielonarodowego Korpusu Północ-Wschód

Komenda Garnizonu Warszawa

Dowództwo Sił Powietrznych

Dowództwo Marynarki Wojennej

Ordynariat Polowy WP

Służba Wywiadu Wojskowego

Centralne Archiwum Wojskowe

Centralna Biblioteka Wojskowa

Biblioteka Główna Wojskowej Akademii Technicznej

Biblioteka Narodowa

Biblioteka Uniwersytecka w Warszawie

Biblioteka Uniwersytetu Opolskiego

Biblioteka Publiczna m.st. Warszawy

Biblioteka Uniwersytetu im. M. Curie-Skłodow-skiej w Lublinie

Biblioteka Uniwersytetu Łódzkiego w Łodzi

Biblioteka Uniwersytetu im. M. Kopernika w Toruniu

Biblioteka Uniwersytetu im. A. Mickiewicza w Poznaniu

Biblioteka Śląska w Katowicach

Biblioteka Uniwersytetu Wrocławskiego we Wrocławiu

Biblioteka Uniwersytetu Gdańskiego

Wojewódzka Biblioteka Publiczna im. Ł. Górnickiego

Książnica Pomorska w Szczecinie

Biblioteka Katolickiego Uniwersytetu Lubelskiego

Biblioteka Jagiellońska

Biblioteka Główna Szkoły Głównej Służby Pożarniczej

Biblioteka Uniwersytetu Śląskiego

Redakcja „Wojska i Wychowania"

Redakcja Wojskowa

Redakcja czasopisma „Myśl Wojskowa"

Redakcja „Przeglądu Wojskowo-Historycznego"

Zagraniczni:

Akademia NATO w Rzymie

Akademia Sztabu Sił Połączonych w Rzymie

Akademia Dowodzenia Bundeswehry w Hamburgu

Akademia Obrony Narodowej Danii

Wyższy Królewski Instytut Obrony w Brukseli

Akademia Obrony Narodowej Austrii w Wiedniu

Akademia Sił Zbrojnych Królestwa Niderlandów w Bredzie

Akademia Obrony Narodowej Szwecji w Sztokholmie

Akademia Wojskowa w Brnie

Akademia Wojskowa w Liptowskim Mikulaszu

Akademia Obrony Narodowej Węgier im. Miklosa Zrinyiego w Budapeszcie

Akademia Sztabu Generalnego Ukrainy w Kijowie

Genewskie Centrum Polityki Bezpieczeństwa

Połączone Kolegium Obrony w Paryżu

Akademia Wojskowa Litwy w Wilnie

Akademia Obrony Narodowej Łotwy

Bałtycka Akademia Obrony w Tartu

Akademia Obrony Narodowej SZ Bułgarii

Akademia Obrony Narodowej Grecji

Uniwersytet Obrony Narodowej USA

Akademia Sił Połączonych SZ USA

Akademia Sił Lądowych USA West Point

Uniwersytet Zachodniego Michigan

Centrum Europejskie w Stuttgarcie

Unia Federalistów Europejskich Jübek – Niemcy

Dom Europejski w Marienbergu – Niemcy

Federalna Akademia Polityki Bezpieczeństwa w Berlinie

Centrum Wyższych Studiów Obrony Narodowej w Madrycie

Uniwersytet Obrony Narodowej Rumunii

Akademia Obrony Narodowej Pakistanu

Akademia Obrony Narodowej Chin

Warunki publikowania
w „Zeszytach Naukowych AON"

Do redakcji „Zeszytów Naukowych AON" należy przekazać wersję elektroniczną pracy zapisaną w programie MS Word lub Adobe InDesign oraz jej wydruk. Artykuł powinien być napisany po polsku i angielsku. Objętość artykułu nie może przekraczać 1 arkusza autorskiego (co stanowi ok. 22 stron lub 40 000 znaków ze spacjami lub 3000 cm^2 powierzchni ilustracji (wzorów matematycznych, fizycznych, chemicznych, zależności logicznych, diagramów, schematów itp.). **Wersją pierwotną czasopisma jest wersja on-line**. Autor zobowiązany jest do złożenia w redakcji oświadczenia na temat praw autorskich (wzór oświadczenia znajduje się na stronie internetowej: www.aon.edu.pl).

Struktura artykułu

1. Tytuł niezawierający skrótów (chyba że są to skróty powszechnie znane).
2. Tytuł w języku angielskim.
3. Autor, współautorzy – tytuł, stopień naukowy, wojskowy, zawodowy, imię i nazwisko autora (autorów), nazwę reprezentowanej przez niego instytucji; e-mail kontaktowy do autorów, nr telefonu.

4. Streszczenie – krótka charakterystyka artykułu (temat, cel, podjęty problem), główne wnioski i osiągnięcia naukowe. Około 700-1500 znaków (w tym spacje) w języku polskim i angielskim. Streszczenie nie może zastąpić wprowadzenia do artykułu.
5. Słowa kluczowe – po polsku i angielsku (max. 5), przy czym pierwsze jest związane z nazwą dyscypliny naukowej, w obrębie której mieści się praca.

6. Artykuł (w tym wprowadzenie oraz wnioski) - wprowadzenie zawiera cel(e), problem(y), hipotezę(y), metody i, jeśli to możliwe, ocenia źródła, we wnioskach podsumowuje się opisane w artykule osiągnięcia naukowe.
7. Przypisy:

1. Wydawnictwo zwarte (książka)	– Autor/Autorzy – Tytuł – Oznaczenie wydania – Numer tomu i jego tytuł (w opisie pojedynczego tomu) – Miejsce wydania i wydawca – Rok wydania – Liczba tomów (w opisie wydawnictwa wielotomowego) – ISBN – Strona
2. Artykuł (rozdział) w wydawnictwie zwartym (książce)	– Autor/ Autorzy artykułu – Tytuł artykułu – Autor/ Autorzy dokumentu macierzystego – Tytuł dokumentu macierzystego – Oznaczenie wydania – Miejsce wydania i wydawca – Rok wydania – Lokalizacja w obrębie dok. macierzystego, oznaczenie woluminu, strony
3. Artykuł w wydawnictwie ciągłym (np. w czasopiśmie)	– Autor/Autorzy artykułu – Tytuł artykułu – Tytuł wydawnictwa ciągłego – Wydanie – Lokalizacja w obrębie dokumentu macierzystego (rok, ozn. zeszytu, strony)

8. Bibliografia – podana w porządku alfabetycznym lista źródeł i literatury.

Zalecamy, by autorzy zachowali dyscyplinę pisarską, trzymając się głównego zagadnienia. Teksty zbyt szczegółowe lub zbyt techniczne mogą nie zostać opublikowane. W razie potrzeby proszę skonsultować tekst z redaktorem naczelnym.

Wymagana objętość tekstów odnosi się do tekstu wraz z przypisami. Bibliografia, streszczenie i inne towarzyszące informacje nie są brane pod uwagę podczas liczenia znaków.

Nie należy numerować rozdziałów, tekst powinien mieć, co najwyżej 3 poziomy. Należy unikać wytłuszczeń i kolorowych liter. Kursywa lub cudzysłów powinny być używane wyłącznie do cytatów.

Wykresy, tabele, i inne obrazy (w programie Corel, Microsoft PowerPoint, Adobe Ilustrator) powinny być dołączone jako oddzielne, łatwe do zidentyfikowania, pliki. Autorzy powinni umieścić je także w tekście lub podać jednoznaczne wskazówki co do pozycji, w której powinny się znaleźć. Wszystkie grafiki powinny być stworzone tak, by ich zmniejszenie lub wydrukowanie w czarno-białej wersji nie ograniczyło ich czytelności. Jeśli obraz został zaczerpnięty z innego źródła, należy przytoczyć to źródło.

Wydruk komputerowy (maszynopis wydawniczy) powinien być:

- sporządzony na papierze formatu A4, druk jednostronny;
- złożony czcionką 12-punktową;
- z interlinią 1,5 wiersza;
- z marginesami: lewy – 3,5 cm, prawy – 1 cm.

Przyjmowanie artykułów – anonimowy proces oceny

Artykuły zamieszczane w kwartalniku są recenzowane, dzięki czemu utrzymywany jest stały, wysoki poziom naukowy publikacji. Proces oceny jest anonimowy. Do oceny każdej publikacji powołuje się co najmniej dwóch niezależnych recenzentów spoza instytucji afiliacji autora. W przypadku tekstów powstałych w języku obcym, co najmniej jeden z recenzentów jest afiliowany w instytucji zagranicznej, innej niż narodowość autora pracy.

Między recenzentem a autorem nie mogą występować:

a) bezpośrednie relacje osobiste (pokrewieństwo, związki prawne, konflikt),

b) relacje podległości zawodowej,

c) bezpośrednia współpraca naukowa w ciągu ostatnich dwóch lat poprzedzających przygotowanie recenzji.

Recenzja ma formę pisemną i kończy się wnioskiem o dopuszczenie artykułu do publikacji lub jego odrzucenie. Przez przedłożenie artykułów autorzy dają wydawcy prawo do opublikowania i dystrybucji artykułu w języku polskim lub innym, w Polsce lub za granicą, w formie drukowanej lub elektronicznej. Artykuł opublikowany w „Zeszytach Naukowych" nie może zostać opublikowany w innych czasopismach bez zgody przewodniczącego Rady Naukowej i redaktora naczelnego, bez odnośnika do tekstu źródłowego, oraz tylko w niezmienionej formie drukowanej lub elektronicznej. Autorzy oświadczają, że ich prace nie były dotychczas publikowane i mają do nich pełne prawa autorskie. Części zaczerpnięte z innych publikacji powinny mieć odpowiednie odnośniki. Autorzy ponoszą pełną odpowiedzialność za treść ich prac i za niewyjawianie informacji tajnych – według odpowiednich przepisów prawa. Autorzy wyrażają zgodę na przyszłe możliwe zmiany ich artykułów, powstałe w procesie recenzji, poprawki językowe i inne czynności związane z publikacją pracy. Autor wyraża także zgodę na ewentualne skrócenie artykułu, jeśli przekracza on dozwoloną objętość.

WYBRANE RODZAJE ARTYKUŁÓW NAUKOWYCH

Artykuł naukowy jest przede wszystkim opisem rezultatów badań naukowych własnych lub zespołu. Powinien się charakteryzować precyzyjnym i logicznym wywodem naukowym, zwięzłym i komunikatywnym językiem. W artykule naukowym wyróżnia się najczęściej kilka zasadniczych części, do których należą:

- tytuł – zwięzły, zawierający „słowa kluczowe" dla prezentowanej w artykule treści;
- wprowadzenie – zawierające syntetyczny opis stanu wiedzy na dany temat oraz określenie celu i problemu pracy, a także przyjętą hipotezę badawczą (postawienie hipotezy w niektórych sytuacjach problemowych nie jest konieczne); charakterystykę przedmiotu badań oraz zastosowanych metod i technik badawczych;
- część główna – opisująca i wyjaśniająca rezultaty przeprowadzonych badań. Wyniki powinny być przedstawione zwięźle i wyczerpująco.

– wnioski – zawierające podsumowanie wyników badań oraz refleksję dotyczącą weryfikacji hipotezy badawczej, poziomu osiągnięcia celu (celów) i rozwiązania problemu(ów) podjętego(tych) w artykule;

– literatura (przypisy, odnośniki) – sporządzona zgodnie z określonymi w danej dyscyplinie naukowej wymaganiami i zawierająca pełne piśmiennictwo związane z przedmiotem rozważań. Zalecane jest odwoływanie się głównie do publikacji recenzowanych;

– streszczenie – powinno mieć charakter informacyjny i zawierać w skondensowanej formie opis: charakteru badań, główne rezultaty i zasadnicze wnioski.

Artykuł przeglądowy – jest krytyczną analizą już opublikowanych materiałów (innych autorów) z określonej dziedziny wiedzy, które wykorzystuje się do sformułowania własnych tez i wniosków. Powinien on przedstawiać nowe idee wynikające z analizowanej literatury. Artykuł zawiera takie części, jak: tytuł, wprowadzenie, opisanie i wyjaśnienie wyników analizy, ich podsumowanie i wnioski oraz literaturę i streszczenie.

Uwagi:

Materiałów niezamówionych redakcja nie zwraca i nie informuje o powodach niezakwalifikowania do druku. Redakcja zastrzega sobie prawo dokonywania skrótów, zmiany tytułów, podtytułów i poprawek stylistycznych.

Publishing terms in "NDU Scientific Quarterly"

Accepting articles – anonymous evaluation process

The articles published in the quarterly are reviewed to maintain constant high scientific level of publications. The evaluation process is anonymous. At least two independent reviewers from outside the author's affiliating institution are called to review each publication. In cases of texts written in a foreign language, at least one reviewer is affiliated in a foreign institution other than the nationality of the work's author. Between the reviewer and the author the following cannot exist:

a) direct personal relations (relationships, legal unions, conflicts);

b) professional subordination relations;

c) direct scientific cooperation during last two years prior to review preparation.

Reviews are in written form and they end with a conclusion on allowing the article to be published or rejecting it.

By submitting articles, the authors give the editor the right to publish and distribute their articles in Polish or in another language, in Poland or abroad, in printed or electronic form. The article published in "Scientific Quarterly" cannot be published in other periodicals without the consent of the Chairman of the Scientific Council and the chief editor, without references to sources, and only in an unchanged printed or electronic form.

The authors declare that they have not published their works so far and that they possess full copyrights to them. Parts derived from other publications should have proper references. The authors bear full responsibility for the content of their works and for non-disclosure of classified information – according to respective law regulations.

The authors give their consent to possible future changes of their articles, resulting from review processes, language corrections and other actions regarding work publication. The authors also give their consent to possible shortening of articles in case they exceed permitted volume.

Other issues pertaining to copyrights are regulated by law currently in force (Act on Copyright from Feb. 4th, 1994).

Detailed requirements

The Scientific Quarterly's editorial office should receive an electronic version of the work saved in MS Word or Adobe InDesign, together with its printout. The article's volume cannot exceed 1 author's sheet (which is approx. 22 pages or 40 000 characters including spaces, or 3000 cm2 of illustrated surface (mathematical, physcal and chemical formulas, logical dependencies, diagrams, schemes etc.)

The article should contain, among others:

– title without abbreviations (unless commonly used ones);

– academic degree or title, military or professional rank, name and surname of author(s), name of institution represented by him;

– summary consisting in independent text briefly describing problems raised in the article;

– keywords (max. 5), while first one is connected to name of scientific discipline containing the work;

– main text together with drawings, photographs, tables;
– graphics material in separate file (in Corel, Microsoft PowerPoint, Adobe Illustrator program);
– list of literature referred to.

Furthermore, in non-English articles:
– title and keywords in English;
– summary in English.

The computer printout (editorial typescript) should be:
– made on A4 size paper, single-sided;
– made with 12-pt. font;
– with 1,5 line spacing;
– with margins: left – 3,5 cm, right – 1 cm.

Structure of article

1. Title.
2. Title in English.
3. Author, co-authors.
4. e-mail to authors, phone number.
5. Summary – short characteristics of article (subject, aim, raised problem), main conclusions and scientific achievements. Approx. 700–1500 characters (including spaces), both in article language and in English. Summary cannot supersede introduction to article.
6. Keywords – max. 5 words and expressions, both in article language and in English.
7. Article (including introduction and conclusions) – introduction contains aim(s), problem(s), hypothesis, methods and, where possible, it evaluates sources; scientific achievements described in the article are summarised in conclusions.
8. Annotations:

a) Coherent publication (book) – Author/authors:
– Title,
– Edition marking,
– Volume number and its title (in description of single volume),
– Place of edition and editor,
– Year of edition,
– Number of volumes (in multi-volume publication),
– ISBN,
– Page;

b) Article (chapter) in coherent publication (book) – Author/authors of article:
– Article's title,
– Author/authors of primary document,
– Primary document's title,
– Edition marking,
– Place of edition and editor,
– Year of edition,
– Localisation within primary document, volume and page markings;

c) Article in serial publication (e.g. in periodical) – Author/authors of article;
– Article's title,
– Title of serial publication,
– Edition,
– Localisation within primary document (year, marking of journal and page).

9. Bibliography – sources and literature, listed alphabetically.

We recommend the authors to maintain writing discipline, holding on to the main subject. Too detailed or too technical texts may not be published. If necessary, please consult the text with chief editor.

The required volume of texts applies to texts together with annotations. Bibliography, summary and other related information are not taken into account during character counting.

Chapters should not be numbered; the text should have 3 levels at most. Please avoid bold and coloured text. Italics or parentheses should be used only for citing.

Charts, tables and other pictures should be attached as separate, easily identifiable files. The authors should also place them in text or give unequivocal hints regarding position in which they should be found. All graphical elements should be created in such a way that reducing them or printing them in black and white do not limit their readability. If the picture was taken from another source, such a source should be cited.

Selected types of scientific articles

A scientific article is first of all a description of results of own or team's scientific research. It should feature precise and logical scientific reasoning, concise and communicative language. Most often, in a scientific article we recognize several principal parts, including:

– title – concise, containing "keywords" for content presented in article;

– introduction – containing synthetic description of current state of knowledge on the given subject and setting the aim and problem dealt with in the work, as well as adopted research hypothesis (setting hypothesis in certain problem situations is not necessary); characteristics of research subject, used methods and research techniques;

– main part – describing and explaining the results of research done. The results should be presented in a concise and comprehensive way.

– conclusions – containing summary of research results and reflection on verification of research hypothesis, level of meeting the goal(s) and solving problem(s) raised in the article;

– literature (annotations, references) – prepared according to requirements defined in given scientific discipline and containing full bibliography related to considered subject. It is recommended to refer to reviewed publications only;

– summary – it should be of informational character and contain, in a condensed form, the description of research character, main results and principal conclusions.

Review article – is a critical analysis of materials that are already published (of other authors) from given knowledge domain, used to formulate own theses and conclusions. It should present new ideas resulting from analysed literature. The article contains such parts as: title, introduction, description and explanation of analyses' results, their summary, conclusions as well as literature and synopsis.

Remarks

The editor's house does not return unsolicited materials and does not inform about reasons for negative qualification to print. The editor's house reserves the right to make abridgements, to change titles, subtitles and to make stylistic corrections.