Stanisław Koziej

Radom, 9.04.2022

WNIOSKI Z PIERWSZEJ FAZY WOJNY ROSYJSKO-UKRAIŃSKIEJ: aspekty działań niekinetycznych

(Tezy referatu na konferencji w Akademii Handlowej Nauk Stosowanych w Radomiu)

Debaty o jakiejkolwiek mocarstwowości państwa w Europie, w tym też o cybermocarstwowości, nie sposób dzisiaj prowadzić bez uprzedniej refleksji o najważniejszym obecnie weryfikatorze strategicznym wszelkich koncepcji i programów w dziedzinie bezpieczeństwa międzynarodowego i narodowego w Europie, czyli o wojnie rosyjsko-ukraińskiej. Dlatego i ja chcę rozpocząć od spojrzenia na wstępne i najbardziej ogólne wnioski z tej wojny, zarówno generalne, jak i w odniesieniu do Polski.

Agresja rosyjska na Ukrainę już na swoim starcie wykazała zaskakujące błędy strategiczne i operacyjne Rosji oraz równie niespodziewaną na taką skalę sprawność armii ukraińskiej, a przede wszystkim odporność i siłę narodu ukraińskiego. Rosyjska armia połamała wszelkie podstawowe zasady sztuki wojennej, jak zaskoczenie, przewaga, czy współdziałanie. Zamiast zaskoczenia obrońcy rosyjski agresor samozaskoczył siebie błędnymi ocenami zdolności armii ukraińskiej i przecenieniem własnej sprawności operacyjnej. Nie uwzględniono zasady przewagi realizując niespotykaną raczej koncepcję ofensywy kordonowej, tj. równomiernych, rozproszonych ataków na wszystkich kierunkach jednocześnie. Ponadto Rosja weszła w wojnę najwyraźniej z doktryną pozimnowojennych operacji ekspedycyjnych, zakładając zapewne, że agresja będzie taką karną ekspedycją prowadzącą do szybkiego obalenia władzy w Kijowie.

Do tego armia rosyjska w swej masie okazała się dużo słabsza niż świat, a także i sam Putin, postrzegał ją na podstawie oceny jej awangardowych formacji ostatnich lat. Dotyczy to zarówno doktryny wojskowej (największy blamaż Sztabu Generalnego, na którego czele stoi wszakże słynny gen. Gierasimow, twórca rosyjskiej doktryny wojen hybrydowych), jak i wyposażenia i uzbrojenia, wyszkolenia, nie mówiąc o morale rosyjskiego żołnierza, przypominającym morale dawnych masowych armii carskiej lub bolszewickiej.

Zupełnie błędna okazała się także organizacja systemu kierowania i dowodzenia siłami zbrojnymi w tej kampanii. Otóż nie wyznaczono dowódcy operacyjnego (polowego) na potrzeby dowodzenia kampanią wojenną w Ukrainie, a dowodzenie to sprawował bezpośrednio szef Sztabu Generalnego z Centrum Kierowania w Moskwie. Szef Sztabu będąc dowódcą wykonawczym w tej wojnie nie mógł nawet obiektywnie zameldować Putinowi, że źle przygotował i źle prowadzi tę kampanię. Musiałby sam siebie oceniać i obwiniać. Dlatego dość

długo trwała zmiana błędnej koncepcji wojny i reorientacja celów politycznych oraz wojskowych, skutkujących odejściem spod Kijowa. To błędny system, którego np. wystrzegają się Amerykanie, u których szef Połączonego Szefostwa Sztabów nie jest dowódcą sił zbrojnych, a po prostu „prawą ręką" najważniejszego decydenta państwowego, czyli prezydenta. Nawiasem mówiąc, u nas w Polsce niestety powrócono ostatnio do modelu rosyjskiego – szef Sztabu Generalnego jest jednocześnie przewidziany na Naczelnego Dowódcę w czasie wojny. Warto to zmienić na podstawie doświadczeń z wojny ukraińskiej.

Zupełnie inaczej przystąpiła do wojny obronnej Ukraina. Od 2014 roku armia ukraińska przygotowywała się do walki z regularną armią innego państwa, a nie z nieregularnymi formacjami i grupami buntowników. Widać, że ma lepszą, adekwatną do takich warunków, doktrynę wojskową, a jej taktyka góruje nad rosyjską. Widać też zdecydowaną przewagę morale broniącej się armii nad armią agresora. Nie mówiąc już o czynniku chyba najważniejszym – woli i determinacji obronnej narodu ukraińskiego, której wyrazicielem i reprezentantem w świecie stał się prezydent Wladimir Zeleński.

W ten sposób od „twardych", czy też - jak często ostatnio się mówi: kinetycznych - treści sztuki wojennej przechodzimy do niematerialnego, niekinetycznego wymiaru wojny, którego elementem jest także to, co jest tematem przewodnim obecnej konferencji – działania w rzeczywistości wirtualnej, w infosferze, w cyberprzestrzeni.

Wbrew oczekiwaniom wojna nie rozpoczęła się od zmasowanych uderzeń rosyjskich w cyberprzestrzeni. Chyba Rosja nie dysponuje takimi zdolnościami, choć była o to podejrzewana. Tu może być podobnie, jak w ogóle ze zdolnościami bojowymi armii rosyjskiej. Przez wiele ostatnich lat obserwowaliśmy w akcji tylko awangardę armii rosyjskiej, najlepiej wyszkolone i uzbrojone oddziały, np. w Syrii, czy nawet w Ukrainie w 2014 roku i na tej podstawie świat oceniał wysoko armię rosyjską. Tymczasem w Ukrainie zobaczyliśmy nie elitarne oddziały a armię masową, z wszystkimi jej słabościami jakościowymi.

Bardzo możliwe, że podobnie jest z rosyjskimi zdolnościami do operacji w cyberprzestrzeni: wystarczające okazały się one do dywersji politycznych (np. cyberinterwencji w wybory w państwach zachodnich, w tym w USA), ale zbyt małe do większej kampanii cyber-obezwładnienia państwa na potrzeby wojny. Odnotowane były jedynie różne akcje na mniejszą skalę, w tym kontroperacje przeciw Rosji wykonywane przez różne podmioty pozapaństwowe, jak np. Grupa Anonymus.

Interesujących wniosków dostarcza wojna informacyjna, jaką przeciw Rosji prowadził Zachód, a zwłaszcza USA. Idzie tu o masowe ujawnianie w formie przecieków medialnych lub wręcz wprost komunikatów oficjeli państwowych różnych informacji i ocen wywiadowczych, przemieszanych zapewne ze spekulacjami lub fałszywymi informacjami, na temat możliwych opcji działań rosyjskich lub możliwych prowokacji ze strony Rosji. To bardzo komplikowało realne działania rosyjskie w różnych fazach wojny, zarówno w fazie jej przygotowania, jak i prowadzenia.

Drugim niezmiernie istotnym obszarem doświadczeń z tej wojny jest zachodnie wsparcie Ukrainy bieżącymi informacjami wywiadowczymi, zwłaszcza wywiadu satelitarnego czy elektronicznego. Dzięki temu dowództwo ukraińskie znało dokładnie położenie i ruchy armii rosyjskiej chyba nawet bardziej niż sami Rosjanie. Tym bardziej, że ich nowy system informatycznego wsparcia dowodzenia załamał się prawdopodobnie już na samym początku wojny. Nie zdziwiłbym się, gdyby stało się to w wyniku jego cyberobezwładnienia.

Możliwe też, że jednym z efektów cyber-obezwładnienia systemów dowodzenia – choć nie tylko – były dość duże straty wśród rosyjskiej generalicji i wyższych oficerów. Nie tylko, bo nawet chyba ważniejszą przyczyną jest sam nakazowy, czy też instrukcyjny model dowodzenia w armii rosyjskiej. W przeciwieństwie do modelu dowodzenia przez cele, który daje podwładnym swobodę co do sposobów osiągania postawionych im celów, model nakazowy obejmuje szczegółowe określanie przez przełożonych zadań i sposobów ich wykonania. Dlatego wyżsi przełożeni muszą często pojawiać się u podwładnych, by kontrolować, pilnować i w razie czego pomagać korygować zadania operacyjne i bojowe. Stąd wielu rosyjskich generałów na linii frontu. W warunkach cyberobezwładnienia podstawowego systemu informatycznego przebywając na linii frontu musieli posługiwać się prostszymi i zapewne słabo szyfrowanymi środkami łączności. To pozwalało na stosunkowo łatwe ich namierzanie, a potem naprowadzanie na nich uderzeń bronią precyzyjną z dronów lub nawet zwykłych strzelców wyborowych, polujących na ważne „miękkie" obiekty w ugrupowaniu przeciwnika. Kadra dowódcza jest szczególnie atrakcyjnymi celami dla strzelców wyborowych.

Wojna w Ukrainie cały czas pokazuje, jak dużą rolę w jej prowadzeniu odgrywa tzw. komunikacja strategiczna, czyli oddziaływanie informacyjne na opinię publiczną. Prowadzą ją oczywiście wszystkie strony: Rosja, Ukraina oraz szeroko rozumiany Zachód, będący w stanie proxy war z Rosją. Bardzo wyraźnie widać to zwłaszcza na przykładzie ujawnianych rosyjskich zbrodni wojennych na terytoriach okupowanych przez armię rosyjską. Zwycięży strona, która dotrze do opinii publicznej z najbardziej wiarygodnym przekazem.

Interesujące mogą być wnioski z prowadzenia komunikacji strategicznej przez Zachód. Rządy demokratycznych państw Zachodu są bowiem w swoich decyzjach i działaniach bardzo zależne od swojej opinii publicznej. Autorytarny reżim putinowskiej Rosji nie musi się specjalnie przejmować niuansami takiej komunikacji i posługuje się najbardziej prymitywnymi kłamstwami propagandowymi w stosunku nie tylko do obcej opinii publicznej, ale także swojej. Ukraina jako państwo w stanie wojny o przetrwanie też może posługiwać się wyraźnie tendencyjnymi komunikatami. Natomiast państwa zachodnie stają przed większymi wyzwaniami. Każda wpadka komunikacyjna może pociągać za sobą poważne konsekwencje.

Nie ma tu czasu na szerszą analizę, więc ograniczmy się do dwóch takich „wpadek". Pierwsza to w mojej ocenie samoograniczenie, jakie ogłosił „urbi et orbi" prezydent J. Biden mówiąc, że w tej wojnie nigdy nie wyśle żołnierzy do Ukrainy. To było osłabienie własnej siły strategicznej w proxy war z Rosją. Jedna z ważnych zasad strategii mówi: „Nigdy nie mów przeciwnikowi, czego nie

zrobisz.” J. Biden powiedział i W. Putin miał i ma swobodę eskalacyjną, z której ochoczo korzystał. Taki komunikat do własnej, zachodniej, opinii publicznej osłabił też wolę wsparcia dla Ukrainy. Drugi błąd to sposób rozegrania problemu z dostarczeniem Ukrainie polskich Mig-ów. Zamiast rozstrzygać ten problem poufnie, Polska i USA weszły w publiczny spór na tym tle. Straciła na tym Ukraina, której chcemy pomagać, skorzystała putinowska Rosja, z którą walczymy.

Gdy mówimy już bezpośrednio o zbrojnych działaniach wojennych, to niewątpliwie w ostatnich wojnach, w tym w wojnie w Ukrainie, szczególną skutecznością wykazuję się drony. Są nie tylko środkiem rozpoznania i kierowania ogniem, ale także środkiem rażenia, w tym w szczególności środkiem przeciwpancernym. Spektakularne sukcesy odnosiły w wojnie karabachskiej w ubiegłym roku i teraz na frontach wojny ukraińskiej. Drony są jedną z egzemplifikacji całej klasy nowoczesnych środków walki, które możemy najogólniej określić jako wysoce zinformatyzowane systemy walki i wsparcia. Są to zwłaszcza: wszelkie systemy rakietowe i przeciwrakietowe, przeciwlotnicze, broń inteligentna (precyzyjna), wszelkie bezzałogowce powietrzne, morskie i lądowe, samoloty, śmigłowce, okręty podwodne (rakiety i torpedy) itd. Pewność wykorzystania takiego sprzętu zależy od pełnego dysponowania ich podsystemami informatycznymi („panowanie cyber/informatyczne”). Nie jest tajemnicą, ze producent takich systemów dysponujący tzw. kodami dostępowymi może mieć wpływ na ich wykorzystanie przez użytkownika. Może np. wprowadzić ograniczenia w jej użyciu. Dlatego kupowanie wysoce zinformatyzowanej broni za granicą wiąże się jednocześnie z utratą pełnej swobody, wręcz suwerenności, we władaniu taką bronią.

Już dziś operacje w cyberprzestrzeni odgrywają coraz ważniejszą rolę. Im bardziej będą informatyzowane systemy wojskowe, tym bardziej będą zależne od swobodnego funkcjonowania w cyberprzestrzeni. Pamiętać musimy w tym kontekście także o lawinowo wzrastającym znaczeniu rozwoju sztucznej inteligencji, dla której cyberprzestrzeń jest naturalnym środowiskiem. Walka o panowanie w cyberprzestrzeni będzie jeszcze istotniejszym warunkiem powodzenia, niż znana nam dobrze w ostatnim wieku walka o panowanie w powietrzu. Kto nie będzie panował we własnej cyberprzestrzeni, nie będzie miał żadnych szans w walce zbrojnej. Tak jak dzisiaj ten, który nie ma zdolności do obrony powietrznej, w tym przeciwrakietowej, ma małe szanse na prowadzenie skutecznych działań zbrojnych.

Niewątpliwie informatyzacja sił zbrojnych jest najważniejszą właściwością ich modernizacji na progu XXI wieku. Stawia to na pierwszym miejscu konieczność własnej, narodowej produkcji wysoce zinformatyzowanych systemów walki i wsparcia, a przede wszystkim ich podsystemów sterowania (z własnymi kodami dostępowymi). Im bardziej powszechne stają się wysoce zinformatyzowane systemy walki i wsparcia, tym ta potrzeba jest silniejsza, a jej sprostanie istotniejsze dla bezpieczeństwa państwa. Dlatego jest to najważniejsze, najbardziej perspektywiczne wyzwanie stojące zarówno przed siłami zbrojnymi, jak i przed przemysłem obronnym.

Ale skuteczne funkcjonowanie w cyberprzestrzeni to nie tylko skuteczne władanie wysoce zinformatyzowanymi systemami walki i wsparcia, to też nie tylko ochrona własnych systemów przed cyberatakami przeciwnika, ale w coraz większym stopniu zdolności do prowadzenia operacji ofensywnych w cyberprzestrzeni. Pokazują to także działania wojenne w Ukrainie. Przy pomocy cyberataków można niszczyć i obezwładniać funkcjonowanie infrastruktury przeciwnika, ale także dezorganizować i wykluczać z walki całe systemy broni, zwłaszcza właśnie te najnowsze, wysoce zinformatyzowane. Dlatego przewiduje się, że w przyszłych wojnach o powodzeniu w coraz większym stopniu decydować będą walki w cyberprzestrzeni.

Z tego też powinien wynikać wniosek dla Polski: im bardziej strategicznie myślimy o naszym bezpieczeństwie, im dalej w przyszłość sięgamy planami i programami, tym bardziej stawiać powinniśmy na budowę i rozwój cyberzdolności. Tym bardziej to powinien być nasz priorytet wśród priorytetów. Dodatkowo przemawia za tym, moim zdaniem, jeszcze jeden niezmiernie istotny argument.

Otóż zagrożenie dla naszego państwa stwarza przede wszystkim Rosja. A Rosja to mocarstwo nuklearne. Widzimy w Ukrainie, jak sam ten fakt już determinuje warunki strategiczne tej wojny. Zachód nie chce przekroczyć pewnego poziomu wsparcia Ukrainy, ponieważ obawia się ryzyka bezpośredniego konfliktu z nieobliczalnym mocarstwem nuklearnym. My na szczęście jesteśmy w NATO. Ale NATO nie musi trwać wiecznie. Ani też nie musi być tak na 100% skuteczne w odstraszaniu i obronie przed Rosją. Dzisiaj jest NATO z twardymi gwarancjami, jutro też będzie, ale czy na pewno będzie pojutrze? A popojutrze? Może tak, może nie. Musimy więc brać pod uwagę także ewentualność samodzielnego zapewniania sobie bezpieczeństwa. I im bardziej wybiegamy prognozami w przyszłość, tym bardziej musimy ją brać pod uwagę.

Czy zatem możemy samodzielnie odstraszyć nuklearną Rosję przed skutecznym szantażowaniem nas, przed wywieraniem presji i wymuszaniem jakichś ustępstw, przed agresją wreszcie? Choć Ukraina pokazuje, że na poziomie konwencjonalnym, dobrze uzbrojeni i przygotowani, wcale nie musielibyśmy przegrać wojny z Rosją o swoje istnienie, to czynnik nuklearny powoduje, że w osamotnieniu i bez broni nuklearnej nie zdołalibyśmy nuklearnej Rosji odstraszyć i powstrzymać przed agresją.

I tu wracam do cyberzdolności. Otóż ukazuje się coraz więcej analiz mówiących o możliwościach i jednocześnie ryzykach zakłócania, dezorganizowania, a nawet obezwładniania systemów broni nuklearnej przez cyberdywersję, cyberataki itp. Idzie tu o włamania do systemów rakietowych – w tym tych przeznaczonych do przenoszenia broni jądrowej, do kierowania lotem samolotów nosicieli takiej broni, do strategicznych systemów kierowania, do systemów logistycznych broni nuklearnej, czy wreszcie cyberzakłócania systemów rozpoznania, ostrzegania, naprowadzania broni nuklearnej itp. Pojawiają się poważne oceny mówiące o ogromnych ryzykach dla odstraszania nuklearnego, czy wręcz o erozji takiego odstraszania w erze cyberbroni.

Jeśli tak, to aktualne staje się pytanie, z którym przyjechałem na tę konferencję: czy Polska w obliczu zagrożeń ze strony mocarstwa nuklearnego nie powinna postawić na asymetryczne metody osłabiania siły nacisku nuklearnego przez rozbudowę własnych cyberzdolności do poziomu kontrnuklearnego? A jeśli powinna, to czy jest w stanie to zrobić? Czy stać nas na to w sensie finansowym? Chyba bardziej niż próba dorównania Rosji w innych obszarach siły zbrojnej. Czy moglibyśmy zapewnić odpowiednie warunki realizacji takiego priorytetu? Kadrowe, naukowe, produkcyjne?

Stawiam tezę, że tak, że gdybyśmy postawili sobie taki priorytet, to mielibyśmy możliwości jego realizacji. I że w wyniku tego Polska mogłaby stać się cybermocarstwem zdolnym do neutralizowania szantażu i zastraszania ze strony zagrażającego naszemu bezpieczeństwu mocarstwa nuklearnego. Tym samym Polska mogłaby zbudować skuteczny system bezpieczeństwa narodowego uwzgledniający różne warunki przyszłościowego kształtowania się międzynarodowego środowiska bezpieczeństwa – zarówno w opcji sojuszniczej, jak i samodzielnej.

Jestem ciekaw, jak Państwo weryfikowalibyście taką hipotezę.

==========