SITK RP - KONFERENCJA WROCŁAW 24-25.05.2023 r.

KSLiTK Lech Majewski

Cyberbezpieczeństwo a rewolucja cyfrowa (na przykładzie domeny cywilnej i wojskowej)

Abstrakt

Pojawienie się nowych technologii cyfrowych stwarza nowe możliwości rozwoju i budowania zdolności materialnych, ale i duże zmiany w życiu społecznym, w wymiarze prawnym, czy w zakresie etyki.

Śmiało można stwierdzić, że ten kto szybciej i lepiej wykorzysta możliwości, jakie daje sztuczna inteligencja, kosmos i cyberprzestrzeń - będzie kształtował przyszłość świata, tworzył nową cywilizację, zmieniał podstawy jej funkcjonowania. Ten proces już się rozpoczął.

Największe potęgi militarne na świecie na pierwszym miejscu stawiają cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpracę z pilotowanymi samolotami lub załogowymi okrętami, sztuczną inteligencją oraz wykorzystaniu przestrzeni kosmicznej i cyberprzestrzeni. Należy tu podkreślić, ze podjęte działania pozwalają prowadzić działania bojowe w czasie rzeczywistym.

Powstaje świat zdeformowany poznawczo w którym trudno jest ocenić obiektywnie zaistniałe sytuacje. Bowiem inaczej oceniają sytuację Stany Zjednoczone, a inaczej Europa, inaczej Chiny i Rosja.

System polityczny Chin pozwala łatwiej i szybciej opanowywać domenę cyber. Chiny sukcesywnie uzyskują przewagę technologiczną, opanowują nowe technologie, nie mają przy tym cywilizacyjno-kulturowych obiekcji.

Żyjemy w okresie rewolucyjnych zmian technologicznych, w okresie czwartej rewolucji przemysłowej, która zachodzi bardzo szybko. Rewolucja cyfrowa wpływa na nasze codzienne życie, determinuje rozwój państwa i jego miejsce w strukturze przyszłego świata. Staje się rdzeniem postępu, a w Siłach Zbrojnych jest zapowiedzią nowego typu wojny.

Siłą napędową czwartej rewolucji przemysłowej jest kombinacja nowoczesnych komputerów o wysokiej mocy obliczeniowej, robotów, zestawów autonomicznych i rozszerzonych technologii informacyjnych, ale i lepsze poznanie i wykorzystanie ludzkiego genomu.

To właśnie wzajemne połączenie różnych urządzeń, dostęp do jak największej ilości informacji, wsparcie technologiczne jak i decentralizacja decyzji może przekładać się na autonomiczność decyzji, szybszą komunikację i efektywną współpracę. Jednocześnie nowa sytuacja skutkuje potrzebą szybkiego identyfikowania problemów, z którymi wcześniej nie mieliśmy do czynienia.

Kluczową rolę odgrywa tu analityka Big Data i algorytmy sztucznej inteligencji. Inteligentne systemy dysponują wszechstronną wiedzą i zdolnościami poznawczymi, które potrafią samodzielnie wykonywać zadania.

Oprócz istniejących domen prowadzenia działań wojennych: lądowej, morskiej, powietrznej, zaczyna dominować domena kosmiczna oraz cyberprzestrzeń (cyfrowa) .

W lipcu 2016 roku, podczas Szczytu NATO w Warszawie, uznano przestrzeń cybernetyczną za kolejną domenę (wtedy czwartą), w której mogą być prowadzone działania operacyjne. Jednocześnie członkowie NATO podkreślili, że dołożą wszelkich starań, aby nowa domena operacyjna była broniona w taki sam sposób, w jaki Sojusz chroni swoje operacje w wymiarze lądowym, morskim i powietrznym. W tym celu przyjęto 7 zobowiązań znanych jako Cyber Defence Pledge, które sojusznicy zgodzili się rozwijać i wzmacniać. Jednocześnie uzgodniono, że stan wdrażania w/w zobowiązań będzie monitorowany i sprawdzany przez NATO w odstępach rocznych.

Cyberprzestrzeń już w czasie pokoju poddawana jest ciągłym atakom. Systematycznie atakowana jest infrastruktura krytyczna, systemy łączności, przestrzeń informacyjna.

Na naszych oczach kształtują się dwa światy cyfrowe: Chiński i proamerykański. Trwa wielka rewolucja i rywalizacja. Polska, ale i inne państwa naszego układu, bardzo często są przedmiotem ataków cybernetycznych ze strony różnych państw, przede wszystkim ze strony Federacji Rosyjskiej. W takiej sytuacji, a szczególnie w kontekście wojny w Ukrainie nie powinniśmy pozwolić aby pozostać w tyle w tym zakresie.

Wszystko wskazuje na to że najważniejsza wojna XXI wieku rozegra się w świecie wirtualnym, w cyberprzestrzeni - w tym kierunku największe potęgi militarne prowadzą intensywne przygotowania i działania. Tworzą się nowe strategie prowadzenia wojen. Na pewno bezpieczeństwo Polski jest bardziej zagrożone teraz, niż na przykład 10 lat temu.

Coraz częściej mówimy o wojnie bezkontaktowej o autonomicznych środkach prowadzenia walki, robotach bojowych, nowych systemach broni elektromagnetycznej, laserowej, plazmowej i mikrofalowej, o bojowych egzoszkieletach, implantach uodporniających żołnierzy na stres.

Największe potęgi militarne na świecie na pierwszym miejscu stawiają cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpracę z pilotowanymi samolotami lub załogowymi okrętami, sztuczną inteligencją oraz wykorzystaniu przestrzeni kosmicznej i cyberprzestrzeni. Należy podkreślić, ze podjęte działania pozwalają prowadzić działania bojowe w czasie rzeczywistym.

Efektem tego jest zwiększenie znaczenia działań bezkontaktowych, w których walczące strony są poza zasięgiem bezpośredniej obserwacji, gdzie brak jest rubieży styczności bojowej wojsk, gdzie uderzenie na potencjalnego przeciwnika może zostać wykonane ze wszystkich kierunków, ze wszystkich domen prowadzenia działań operacyjnych.

Pentagon przewiduje, że w nadchodzącej dekadzie autonomiczne systemy staną się jednym z głównych środków walki. Obecnie trwające prace nad programem tzw. przyszłych systemów bojowych (FCS – *Future Combat Systems*), których wartość jest oceniana na ponad 120 mld dolarów. Jest to największy kontrakt w historii USA.

W Stanach Zjednoczonych coraz wyraźniej mówi się, ale i realizuje następujące filary modernizacji Sił Zbrojnych:

1. sieciowy (sieciocentryczny) system kierowania i dowodzenia. Idea połączenia wszystkiego ze wszystkim oraz tworzenie rzeczywistości rozszerzonej, pozwalającej na projektowanie dodatkowych informacji na obraz świata rzeczywistego. Poligonem doświadczalnym są oczywiście SP.

2. systemy autonomiczne współpracujące z ludźmi, wdrażane we wszystkich Rodzajach Sił Zbrojnych na masową skalę.

3. Sztuczna inteligencja – klucz do danych, a dane są dziś polem walki.

Nie mówi się o czołgach, samolotach, rakietach, okrętach, a nawet o satelitach – mówi się o sieciach, łączności, danych i potencjale technologii AI (artficial intelligence), który automatyzuje procesy, przewiduje przyszłe zdarzenia, szacuje ryzyka i profilaktyktykę. Nie megatony a megabity.

Wartość globalnego rynku sztucznej inteligencji w 2022 roku osiągnęła wartość około 450 mld. dol. Do 2030 roku wartość sektora AI wzrośnie do 1,3 bln dolarów oraz zwiększy wartość światowej gospodarki o prawie 16 bilionów dolarów. Do roku 2022 dzięki nowym technologiom powstało na świecie 133 mln. miejsc pracy.

Tylko w 2019 roku światowe wydatki na AI osiągnęły prawie 40 mld. dol. 44% więcej niż rok wcześniej (2/3 USA; 5,5% Europa).

Szacuje się, że cyberataki w 2021 roku kosztowały nawet 11,4 mln. $ na minutę! Jedna złotówka zainwestowana w przemysł kosmiczny zwraca się czterokrotnie.

W Polsce w ciągu najbliższych pięciu lat zapotrzebowanie na specjalistów zajmujących się sztuczną inteligencją sięgnie 200 tys. osób.

Wiele państw na czele z Rosją prowadzi intensywne działania cybernetyczne łamiąc prawo międzynarodowe, ingerując w ich politykę wewnętrzną. Używając siły militarnej przeciwko sąsiadom: Gruzji i Ukrainie, ale i odpowiada także za agresywne działania wobec państw NATO. Wszystkie te działania wpływają również na wewnętrzne procesy polityczne państw.

W marcu 2021 roku prezydent Biden powiedział, że prezydent Rosji jest „zabójcą" i że zapłaci za ingerencję w wybory w USA.

Polska wydaje setki miliardów na nowe uzbrojenie.

Jednak czy decydenci zdają sobie sprawę, że droga do przyszłości Sił Zbrojnych, do skutecznej obrony państwa, to sztuczna inteligencja, systemy autonomiczne i sieciocentryczność, że tu jest potencjał, a nie w czołgach czy rakietach, że żaden, nawet najnowocześniejszy środek współczesnego pola

walki nie ma żadnego znaczenia, jeśli nie będzie wpięty w odporną na zakłócenia i bardzo przepustową sieć informatyczną.

Gwałtowny rozwój technologii informatycznych spowodował jej zastosowanie do działań w cyberprzestrzeni. Szczególnie w celu uszkodzenia infrastruktury krytycznej (banki, energetyka czy obiekty przemysłowe i wojskowe np. systemy kierowania i dowodzenia).

Robotyzacja w przemyśle, ale i na polu walki w krótkim okresie doprowadzi do ich pełnej autonomii podczas realizacji stawianych zadań.

Australia: armia stawia na roboty i nowe podejście do robotów.

Australijczycy nie tylko widzą rosnące zagrożenia, ale podejmują konkretne działania. Zaczynają prowadzić szeroki program testów i badań dotyczących przełomowych technologii w tym autonomicznych robotów lądowych. Program bazuje na szerokiej współpracy wojska, przemysłu i nauki, ale i oczywiście ze Stanami Zjednoczonymi.

W Australii nie mówi się o samych robotach, ale już się je eksploatuje, testuje lub rozwija programy rozwojowe.

TURCJA: planuje stworzenie lotniskowca dla 30-50 dronów bojowych (wcześniej planowane dla F-35 – zakup S-400 zmienił plany).

Satelity Elona Muska są niezbędne dla ukraińskiej armii i ludności cywilnej - pomagają w ustalaniu rosyjskich pozycji, umożliwiają kontakt z bliskimi, a przemówienia prezydenta Wołodymyra Zełenskiego mogą być transmitowane na całym świecie.
Dzięki systemowi od SpaceX Kremlowi nie udało się odciąć Ukrainy od świata zewnętrznego, a plany Kremla okazały się nierealne.

Wojna w Ukrainie bardzo wyraźnie pokazuje, że coraz większy dostęp do sztucznej inteligencji, kosmosu i najnowszych technologii powoduje, ze prawda staje się pierwszą ofiarą zaistniałej sytuacji.

Na przykładzie ostatnich zdarzeń politycznych, sytuacji w masmediach oraz wewnętrznej sytuacji w Ukrainie coraz częściej mówimy o „mgle wojny". Powstaje przekazywana informacja na podstawie której trudno jest określić dynamikę zdarzeń w zaistniałej sytuacji np. sytuacji i strat na froncie ukraińskim.

Ta nowa infosfera (nie zawsze doceniana) przyczyniła się miedzy innymi do tego, ze NATO, UE, ale i Stany Zjednoczone nie były zdolne ocenić sytuacji na wschodzie i powstrzymać agresywne działania Rosji. Dominacja mediów

społecznościowych w systemie demokratycznym stała się bezsprzeczna i trudna do opanowania. Setki tysięcy pośredników nie produkcyjnych w strukturach państwa staje się dużą bolączka zachodu, często kształtuje i spowalnia rozwój.

W aspekcie dominacji cyfrowej, szybkim rozwojem nowych sposobów komunikacji w tym mediów społecznościowych dużym problemem staje się legitymizacja władzy. Media społecznościowe wydatnie mogą się przyczynić do zakłócenia sytuacji w państwie, mogą stać się elementem strategii biznesowej. Bardzo wyraźnie zmniejsza się rola autorytetów. Korzystanie z Internetu bez ograniczeń i nadzoru może uzależniać i powodować problemy psychologiczne szczególnie wśród osób młodych.

Dlatego ważnym aspektem operowania w cyberprzestrzeni jest posiadanie umiejętności monitorowania informacji ze szczególnym uwzględnieniem dynamiki rozwoju wirtualnych społeczności. Internet to doskonały środek dla fałszywych liderów, kreujących się jako osoby kompetentne, co w dobie post-prawdy nie jest w żaden sposób weryfikowane. Tego typu mechanizmy społeczne są często wykorzystywane przez organizacje terrorystyczne i przestępcze, ale i instytucje polityczne i państwowe.

Jeżeli porównamy potencjał militarny i ekonomiczny UE, NATO i USA do potencjału Rosji to różnice są porażające, a jednak Rosja zaatakowała….

Powstał świat zdeformowany poznawczo w którym trudno jest ocenić obiektywnie zaistniałe sytuacje. Inna jest ocena sytuacji przez USA, Europę, Chiny, nie mówiąc już o Rosji. Zachód na czele z Francją czy Niemcami często obawia się możliwości dominacji USA.

W innej sytuacji są Chiny. Ich system polityczny pozwala im łatwiej i szybciej opanowywać domenę cyber. Chiny sukcesywnie uzyskują przewagę technologiczną, opanowują nowe technologie, nie mają cywilizacyjno - kulturowych obiekcji.

W świecie demokratycznym, powstanie wielkich światowych korporacji cyfrowych przy braku odpowiedniej reakcji świata politycznego powoduje niszczenie małego biznesu oraz klasy średniej , generuje napięcia społeczne. Biznes z Doliny Krzemowej, generuje ogromne pieniądze i uzyskuje przewagę nad polityką.

Powstaje węzeł gordyjski: jeżeli podzielimy potężne zachodnie koncerny – nie będzie możliwości konkurencji z potężnymi Chińskimi.

W Chinach kapitał cyfrowy nie ma przewagi nad polityką, nad rządem.

Dyskusja i konflikt - swoboda wyrażania poglądów są normalnością w demokratycznych społeczeństwach. W Internecie istnieją narzędzia, które umożliwiają monitorowanie i administrowanie tego typu procesami.

Największym zagrożeniem wydają się być zamknięte grupy kontrolowane przez liderów, których potencjału i aspiracji nie da się zweryfikować w rzeczywistym świecie. Wykorzystując prosty schemat, trójkąt oprawca -ofiara - wybawca można zilustrować relacje zarówno w radykalnych organizacjach jak i w życiu codziennym. Efektem jest proces sprawiający gwałtowną brutalizację stosunków międzyludzkich.

Prowadzą do niego trzy główne czynniki: brak autorytetów, pogorszenie się podstawowych warunków życia (co często prowadzi do stresu i ostatecznie paniki) oraz funkcjonowanie silnych grup nacisku wpływających na bezbronną ofiarę.

W zaistniałej sytuacji, biorąc pod uwagę powstające zagrożenia istnieje pilna potrzeba budowy nowej kategorii polityków, dobrze wykształconych i rozumiejących rzeczywistość, umiejących podjąć stosowne decyzje i to zmienić.

Pandemia Covid przyspieszyła rozwój nowych technologii, sztucznej inteligencji, zmieniła system komunikacji społecznej. Rozwinęła pracę zdalną oraz wirtualne uczenie się na kursach online, zdalne internetowe zakupy, ale i skłonności depresyjne szerokiej grupy społeczeństwa. Zdaniem ekspertów pandemia przyśpieszyła rewolucję cyfrową o wiele lat.

Na naszych oczach domena cyber używana do dezinformacji stała się potężną bronią. Dobrym przykładem jest tutaj Ukraina.

Co by było gdyby Rosja w Ukrainie od początku zaczęła atakować infrastrukturę krytyczną? Rosjanie stworzyli sobie fałszywy obraz Ukrainy. Nie traktowali Ukrainy jako państwa obcego. Sądzili, że Ukraińcy popierają Rosję. Posiadali zniekształcony obraz sytuacji w Ukrainie. Przeoczyli między innymi Majdan, który wszystko zmienił.

Na początku chcieli przejąć państwo nie zniszczone, mieli poczucie przewagi – na szczęście fałszywe.

W trudnej sytuacji Ukraina pokazała ogromną siłę woli, ogromną kreatywność rządu, ale i normalnych ludzi, wielką wolę walki o wolność i demokrację o przynależność do świata zachodniego.

Proces ograniczania szkód jakie niosą ze sobą barbarzyńskie ataki rosyjskie rozpoczęli już na poziomie budowania infrastruktury informatycznej.

Dobrze zaprojektowali sieć komputerową która funkcjonuje nawet w przypadku zainfekowania poszczególnych terminali. Sieć rozproszona okazała się bardzo odporna na ataki hakerskie, oczywiście jeżeli tylko cyberprzestępcy nie zlokalizują kluczowych urządzeń odpowiedzialnych za przekierowywanie większości ruchu.

Okazało się, że ważnym środkiem podnoszącym bezpieczeństwo infrastruktury jest nadmiarowość komponentów sieciowych – pozwala to na duplikację kanałów przekazu i utrzymanie podstawowych funkcji nawet w przypadku zniszczenia części z nich.

Na poziomie infrastruktury zagwarantowali również właściwe serwisowanie, która zawsze wiąże się z warunkiem doboru zaufanych i zweryfikowanych podwykonawców – co szczególnie w Ukrainie nie było proste.

Do dzisiaj tylko 77 państwa wypracowały własne cyber-strategie, tylko dwadzieścia ma swoje, specjalne dowództwa, a jedynie 17 z nich jest zdolne do przeprowadzania cyberataków.

Przykładem największych operacji tego typu mogą być operacja Izraela przeciwko syryjskiej obronie powietrznej, wojna rosyjsko - gruzińska i oczywiście rosyjsko-ukraińska, czy też amerykańska kontrofensywa przeciwko ISIS.

Obecnie trudno jest zdefiniować rejestr wirtualnych operacji. Tego typu działania wykroczyły już poza ramy klasycznego szpiegostwa czy działań hakerskich. W przypadku kiedy celem staje się całe państwo, można mówić o proliferacji cyberbroni.

W tej chwili na współczesnym polu walki konieczny staje się kolejny wysoce wyspecjalizowany specjalista – informatyk polowy, na przykład na podobieństwo koordynatora lotnictwa JTAC, sapera, czy chemika.

Wojskowe sieci są dobrze zabezpieczone przed ingerencją z zewnątrz, jednaki i tu możliwe jest przeniknięcie do nich. Na przykład jak do sterylnych komputerów irańskiej elektrowni nuklearnej.

We współczesny świecie, nic nie jest w stanie powstrzymać rozwoju nowych cybertechnologii, przede wszystkim na poziomie infrastruktury krytycznej. Dlatego też tak ważne jest, aby umieć określać potencjalne miejsca ataku, określać jego prawdopodobieństwo i mieć wypracowane procedury minimalizowania szkód. Dobrym przykładem posiadania takich umiejętności jest Ukraina.

Najbardziej rozwinięte państwa świata posiadają w Siłach Zbrojnych odpowiednie struktury, które umożliwiają neutralizację zagrożeń na szczeblu strategicznym i operacyjnym. Działania poszczególnych cyber dowództw są porównywalne z operacjami klasycznych wojsk specjalnych. One również potrzebują doskonale wyszkolonych i wyposażonych specjalistów wykonujących konkretne zadania.

W tym celu wiele państw tworzy nowe struktury dowódcze. Na przykład w Stanach Zjednoczonych poszczególne rodzaje sił zbrojnych mają swoje cyberdowództwa.

Coraz więcej państw powołuje odrębne rodzaje sił zbrojnych i dowództw do przeciwdziałania zagrożeniom w Sieci.

W 2017 roku powstałe w 2009 Dowództwo Cybernetyczne Stanów Zjednoczonych zostało wydzielone i stało się dziesiątym dowództwem wojskowym.

W roku 2017 Niemcy utworzyły Dowództwo Przestrzeni Cybernetycznej i Informacyjnej. W 2016 zwiększyła środki na cyberbezpieczeństwo Wielka Brytania.

Takie działania podejmują także państwa spoza NATO. W 2016 roku w Rosji utworzono wojska informacyjne . Również w 2016 wojska lotnicze Republiki Korei utworzyły nowe centrum cyberbezpieczeństwa.

Również w Polsce od listopada 2018 roku powstaje nowy rodzaj Sił Zbrojnych - Wojska Obrony Cyberprzestrzeni.

Na podstawie ustawy o obronie ojczyzny powstaje Komponent Wojsk Obrony Cyberprzestrzeni, który będzie podlegał Dowódcy Komponentu WOC.

Struktura Wojsk Obrony Cyberprzestrzeni - opiera się na Centrum Operacji Cybernetycznych – istniejącej już w Wojsku Polskim jednostce. Trzykrotnie zwiększy się tam liczba etatów.

Cyberżołnierze to nie jest wojsko przyszłości to są żołnierze operujący już dzisiaj.

Zmiany zachodzą również w Narodowym Centrum Kryptolgii oraz Inspektoracie Informatyki.
Obie instytucje zostały połączone w Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni.

Została również powołana Szkoła Podoficerska Łączności Informatyki w Zegrzu (w miejsce dotychczasowego Centrum Szkolenia Łączności Informatyki) oraz Liceum Informatycznego przy Wojskowej Akademii Technicznej.

Cyber komponent powstaje w WOT – docelowo będzie liczył 100 specjalistów. WAT zostały utworzone studia na kierunku kryptologia, gdzie każdego roku studiuje ponad 100 studentów.

W 2017 roku minister Macierewicz ogłosił zamiar przeszkolenia 1 tys. hakerów (tyle co mają Niemcy, więcej niż Rosja). W Polsce brakuje 50 tys. Informatyków.

Na WAT zostały otwarte studia podyplomowe dotyczące cyberbezpieczeństwa, zwiększone zostały limity na kierunkach kryptologia i cyberbezpieczeństwo, informatyka, elektronika i telekomunikacja oraz systemy informatyczne w bezpieczeństwie. Poświęcone cyberbezpieczeństwu studia wojskowe prowadzi też Akademia Marynarki Wojennej w Gdyni. W 2019 moduł szkoleniowy Legii Akademickiej został rozszerzony o komponent cyberbezpieczeństwa.

To tam są szkoleni żołnierze, których głównym zadaniem będzie walka z wirusami komputerowymi, fake newsami, komputerową dezinformacją.

W Polsce pomimo powstania Polskiej Agencji Kosmicznej w dalszym ciągu bardzo poważnym problemem jest rozwój sektora kosmicznego oraz wykorzystanie jego możliwości oraz budowa satelitów. Niestety każdego roku problemy się nawarstwiają i jesteśmy coraz bardziej spóźnieni w stosunku do Europy i świata.

Biorąc pod uwagę podejmowane decyzje i realizowane przedsięwzięcia w zakresie cyberbezpieczeństwa, wydaje się, że powinien powstać jeden silny podmiot który powinien zapewnić spójność polskiej polityki cybernetycznej w kraju i zagranicą realizując strategiczne cele państwa, poprzez reprezentowanie polskiego interesu militarnego, gospodarczego i naukowego na arenie międzynarodowej (UE, NATO, ESA, EUMETSAT, EDA) zapewniając koordynację działań nauki, biznesu i administracji państwowej.

Niestety, a to często potwierdza sytuacja w Polsce, ale i również na świecie, że inicjatorzy nowych wyzwań bardzo często nie mieli zrozumienia i mieli poważne kłopoty.

Michale Flournoy kandydatka prezydenta Joe Bidena na sekretarza obrony w Stanach Zjednoczonych podczas przemówienia w Kongresie przedstawiła następujące propozycje modernizacji amerykańskich Sił Zbrojnych: megabity zamiast

megaton, cyfrowe technologie, systemy autonomiczne i bezzałogowe – ich współpraca z pilotowanymi samolotami lub załogowymi okrętami oraz sztuczną inteligencją powinny stanowić podstawę modernizacji Sił Zbrojnych.
Natomiast Premier Wielkiej Brytanii Boris Johnson w marcu 2021 r ocenił, że „siła cybernetyczna rewolucjonizuje sposób, w jaki żyjemy i toczymy wojny, podobnie jak to zrobiły Siły Powietrzne sto lat temu."
W przeszłości bardzo duże kłopoty ze swoimi rewolucyjnymi wizjami mieli gen. Douchet z Włoch czy gen. Mitchell ze Stanów Zjednoczonych. Polski przykład to gen. Zagórski i gen. Rayski, a po wojnie gen. Frey Bielecki, pierwszy polski dowódca WLiOP.
Śmiało można powiedzieć, że niewygodni "prorocy" szybko skończyli nie najlepiej. Często dopiero po śmierci zostali uznani i docenieni.
Czas pokazał i udowodnił, że wszyscy oni, jak i wielu innych, miało dużo racji i mówili prawdę.
Czy również tak będzie obecnie? Czy na pewno obecne nowe wyzwania nie przerosną decydentów? Czy obecnie proces modernizacji Sił Zbrojnych, ale i całego kraju idzie w dobrym kierunku?

gen. broni pil. w st. spocz. Lech Majewski

Były dowódca Generalny Rodzajów Sił Zbrojnych, Polskich Sił Powietrznych, 3 Korpusu Obrony Powietrznej we Wrocławiu oraz 1plm. Absolwent Wyższej Oficerskiej Szkoły Lotniczej, Akademii Lotniczej w Monino w byłym ZSRR, Akademii Sztabu Generalnego WP, Narodowego Uniwersytetu w Waszyngtonie w Stanach Zjednoczonych. Wykonywał loty na samolotach MiG-29, MiG-21, MiG-15, TS-11, TS-8, M-28 oraz loty zapoznawcze na F-18, F-16, Mirage -2000 i 2005, T-38, M-346.
Obecnie wiceprezes SSLW RP, przewodniczący KSLiTK przy SITKRP, wykładowca w AWSB na kierunku Bezpieczeństwo Narodowe.