

# polska Zbrojna



KIELCE 2012  
**MSP0**  
WYDANIE SPECJALNE/SPECIAL EDITION





# PIERŚCIEŃ Z JAŚMINU

Dzięki Systemowi Wsparcia Dowodzenia C3IS Jaśmin studenci Akademii Obrony Narodowej przygotowują się do dowodzenia na polu walki przyszłości.

# JASMINE RING

Thanks to C3IS Jasmine Command Support System the National Defense University of Warsaw students prepare to take command at the battlefield of the future.

Odbývające się od kilku lat w pierwszej połowie maja Ćwiczenie dowódczo-sztabowe o kryptonimie „Pierścień” jest najważniejszym przedsięwzięciem dydaktycznym Akademii Obrony Narodowej. Podczas kilkudniowego szkolenia żołnierze-studenci zdają praktyczny sprawdzian z wiedzy zdobytej na wojskowej uczelni. W tym roku był on o tyle trudny, że odbywał się nie tak jak dotychczas w akademickich lub garnizonowych salach, lecz na poligonie, na polowych stanowiskach dowodzenia pracujących w trybie dwudziestoczterogodzinnym.

## WYJĄTKOWY POLIGON

Tematyka i cele akademickiego „Pierścienia” nie zmieniły się od jego pierwszej edycji. Co roku najważniejszym zamierzeniem jest doskonalenie umiejętności oficerów związanych z pracą sztabową w ramach zespołów funkcjonalnych stanowiska dowodzenia, a także usprawnianie współpracy z terenowymi organami administracji wojskowej i samorządowej. Wprawdzie przygotowująca „Pierścień” kadra Wydziału Zarządzania i Dowodzenia AON stara się zaskoczyć studentów danego rocznika opracowanymi dla nich zadaniami, to jednak dziedzina, do której się odnoszą, nie może być niespodzianką. Uczestnicy ćwiczenia mierzą się bowiem z typowymi dla wojsk lądowych zagadnieniami działań bojowych, takimi jak wykonanie uderzeń na przemieszczającego się przeciwnika, walka w odosobnieniu (okrążeniu), wsparcie i zabezpieczenie wojsk w obronie, działanie w sytuacji zagrożenia użyciem broni masowego rażenia.

Owczesny rektor AON generał dywizji **Romuald Ratajczak** zdecydował, że tegoroczny „Pierścień” w jednym punkcie bę-

The command-and-staff exercise, coded Pierścień (Polish for Ring), organized for several years in the first half of May, is the most important didactic event of the National Defense University (AON, Akademia Obrony Narodowej). During a several-day training, the student soldiers take a practical exam to verify their knowledge gained in the years of studying at the military university. The training was particularly difficult this year, because it was not organized in school or garrison rooms, as before, but at a military training ground, at the 24/7 field command posts.

## EXTRAORDINARY TRAINING GROUND

The subject and aims of the academic Pierścień Exercise have not changed since its first edition. Every year, the most important objective is perfecting officers' skills in their staff work, within command post functional units, and raising the quality of cooperation with regional military and local government administrative bodies. Even though each year the faculty of the AON Department of Management and Command tries to surprise the students with prepared tasks, their scope cannot be unexpected. Participants of the exercise have to cope with land forces-specific combat action problems, such as attack on enemy troops on the move, combat warfare in isolation (encirclement), support and protection of forces in defense, or operating in a situation of threat with the WMD use.

Major General **Romuald Ratajczak**, the AON President, decided that this year's Pierścień Exercise would significantly differ from previous editions in one respect. The exercise was planned outside the university site or any military unit.



dzie się różnił od poprzednich ćwiczeń. Zaplanowano jego przeprowadzenie nie w obiektach Akademii lub w którejś z jednostek wojskowych, lecz dla maksymalnego urealnienia szkolenia stanowiska dowodzenia zostały rozwinięte „na bojowo” na drawskim poligonie. Dziekan Wydziału Zarządzania i Dowodzenia pułkownik profesor doktor habilitowany **Jarosław Wolejszo** podkreślił, że dzięki temu zaplanowano zadania, których zrealizowanie nie byłoby możliwe w koszarach czy na terenie Akademii, a które są ogromnym wyzwaniem dla sztabu. „Nie wszyscy studenci mieli w trakcie swojej służby okazję do pracy na polowych stanowiskach dowodzenia czy do udziału w przemieszczaniuich w pełnym znaczeniu, to jest z użyciem grup rozpoznawczych i operacyjnych”, powiedział profesor. „«Pierścień» im to umożliwił”.

### SIECIOCENTRYCZNA AKADEMIA

Dla wszystkich, także dla żołnierzy mających już doświadczenie w pracy na polowych stanowiskach dowodzenia, akademicki „Pierścień” był jednak przede wszystkim niepowtarzalną okazją do kierowania sztabem z użyciem narzędzi, którymi dysponuje tylko kilka polskich jednostek wojskowych, a mianowicie – sieciocentrycznego systemu wspomagania dowodzenia. Akademia Obrony Narodowej

In order to make the training as real as possible, the “combat-like” command posts were developed at Drawsko Pomorskie training ground. The dean of the Management and Command Department, Colonel **Jarosław Wolejszo**, Professor, emphasized that this helped to perform tasks which could not be executed in barracks or on university grounds, and which are a great challenge to the staff. “Not all students had a chance during their service to work at field command posts or redeploy a command post in its full sense, i.e. with the use of reconnaissance and operational groups,” said Colonel Wolejszo. “Pierścień Exercise made it possible.”

### NETWORK CENTRIC UNIVERSITY

First and foremost, the academic Pierścień Exercise was a unique occasion for everyone, including soldiers who already have experience in working at field command posts, to command the staff using tools that only several military units in Poland have access to, i.e. a network-centric command support system. AON is the only institution in our army that has the Automated Command Systems Laboratory at the Department of Management and Command, which in 2011 was equipped with C3IS Jasmine command support system developed by Teldat. It is a component-based command and communication system constructed and designed

## Znacznik ratownika – znacznik pojazdu / Rescuer Tag – Vehicle Tag

Jest elementem Systemu Zarządzania Kryzysowego Jaśmin. Umożliwia automatyczne zbieranie informacji o środowisku. W zależności od miejsca użycia urządzenia (modelu) wyróżniamy: Rescuer Tag – znakowanie ratowników prowadzących bezpośrednie działania w zagrożonym terenie, Vehicle Tag – znakowanie pojazdów biorących udział w akcji ratunkowej. Na potrzeby systemu zarządzania kryzysowego do urządzenia mogą zostać dołączone czujniki, na przykład do monitorowania stopnia wilgotności wałów przeciwpowodziowych czy skażenia chemicznego terenu.

#### Charakterystyka:

- **wyświetlacz:** monochromatyczny, graficzny,
- **magnetometr:** funkcja kompasu obrazowana na wyświetlaczu graficznym,
- **akcelerometr:** czujnik stanu zagrożenia (na przykład upadek czy brak ruchu) oraz czujnik aktywacji stanu uśpienia (oszczędność energii),
- **komunikaty tekstowe:** odbiór krótkich informacji tekstowych na wyświetlaczu graficznym,
- **klawisze funkcyjne:** przyciski UP, DOWN, OK
- **zasilanie baterijne:** trzy wymienne akumulatory typu AA,
- **ładowanie baterii:** port mini-USB
- **wymiary:** szerokość 79 mm, wysokość 63 mm, długość 30 mm,
- **masa:** < 250 g,
- **czas pracy baterii:** około 25 godzin
- **interfejsy:** mini-USB, wbudowany moduł CDMA/420 MHz, antena zewnętrzna, karta SIM (wymienialna), moduł GPS (wbudowany odbiornik z wewnętrzną anteną).



Rescuer Tag/Vehicle Tag is an element of the Jasmine Crisis Management System. It enables automatic collection of information about given environment. Depending on the place of use (model) of the device we have: Rescuer Tag – tagging rescuers operating directly in dangerous areas, Vehicle Tag – tagging vehicles taking part in rescue operations. The crisis management device can be supplemented with sensors, e.g. for monitoring the moisture content of embankments or chemical contamination.

#### Parameters/Features:

- Display: monochromatic, graphic
- Magnetometer: compass function shown on graphic display
- Accelerometer: danger sensor (e.g. fall or lack of movement) and sleep mode activation sensor (energy saving)
- Text reports: receipt of short text information on graphic display
- Function keys: UP, DOWN, OK
- Batteries: 3 replaceable AA accumulators
- Battery charging: mini USB port
- Dimensions: (width 79 mm, height 63 mm, length 30 mm)
- Weight: <250 g
- Battery working life: about 25 hours
- Interfaces: mini-USB, built-in CDMA/420MHz modem, external antenna, SIM card (replaceable), GPS module (built-in receiver with internal antenna)



jako jedyna instytucja w naszej armii ma bowiem Laboratorium Zautomatyzowanych Systemów Dowodzenia Wydziału Zarządzania i Dowodzenia, które w 2011 roku zostało wyposażone w opracowany przez firmę Teldat System Wsparcia Dowodzenia C3IS Jaśmin. Ten system dowodzenia i łączności o budowie komponentowej został zaprojektowany i zbudowany zgodnie ze standardami rekomendowanymi w koncepcji NATO – Network Enabled Capability oraz Service-Oriented Architecture. Obecnie SWD Jaśmin jest dostępny w trzech podstawowych wersjach: dedykowanej dla szczebla operacyjnego i taktycznego HMS (Headquarters Management System), przeznaczonej do działania na poziomie taktycznym (również operacyjnym), BMS (Battlefield Management System) oraz DSS (Dismounted Soldier System), przewidzianej dla najniższych poziomów dowodzenia, w tym dla poszczególnych żołnierzy.

Na potrzeby ćwiczenia użyto komponenty Systemu Wsparcia Dowodzenia C3IS Jaśmin, niezbędne do zbudowania sieci dowodzenia dwóch brygad i dwóch batalionów (jak przewidywał scenariusz ćwiczenia), poczynając od poszczególnych żołnierzy, przez pojazdy, na sztabie skończywszy. Łącznie podczas ćwiczenia pracowało aż 150 stacji roboczych. To istotne, ponieważ do udziału w nim zaproszono cywilne organy zarządzania kryzysowego (na szczeblu wojewódzkim był to Zachodniopomorski Urząd Wojewódzki, a na szczeblu powiatowym – Starostwo Powiatu Drawskiego). W związku z tym one także zostały wyposażone w komponenty Jaśmina.

Współpraca między wojskiem a strukturami cywilnymi nie może odbywać się z wykorzystaniem wojskowej sieci dowodzenia (ze względów bezpieczeństwa), więc firma Teldat udostępniła przygotowaną dla lokalnej administracji nie tylko specjalną wersję Jaśmina – SZK (System Zarządzania Kryzysowego), lecz również skonstruowane z myślą o ratownictwie kryzysowym terminale (znaczniki) ratownicze. Podczas ćwiczenia zaprezentowano wersję SZK Burzyk, opracowaną przez naukowców z Laboratorium Badawczego Systemów Mobilnych Politechniki Poznańskiej. Bezzałogowy samolot klasy mikro filmował wały przeciwpowodziowe, a obraz wraz z danymi z terminali ratowniczych (monitorujących położenie pojazdów oraz wilgotność wałów) był przesyłany dla starostwa i wojewody do stacji roboczych systemu.

in accordance with the standards recommended in the NATO Network Enabled Capability concept and Service-Oriented Architecture. Currently, Jasmine is available in three basic versions: Headquarters Management System (HMS) intended for the operational and tactical level, Battlefield Management System (BMS) for tactical (and operational) level activities, and Dismounted Soldier System (DSS) for the lowest levels of command, down to a single soldier.

The exercise engaged C3IS Jasmine components necessary to build a command network of two brigades and two battalions (according to the exercise script), from a single

soldier, through vehicles, up to the staff. The total of as many as 150 working stations operated during the Pierścień Exercise. This is important, because civil crisis management bodies (West Pomeranian Voivodeship Office at regional level and Drawsko Powiat Starosty at poviat level) were invited to participate in the exercise, and were as well provided with Jasmine components. As it is obvious that the army and civil structures cannot cooperate using the army command network (for security reasons), Teldat shared with the local administration not only their special version of Jasmine Crisis Management System, but also emergency terminals (tags) designated to carry out crisis rescue operations. This Jasmine version was presented during the exercise. Burzyk, a micro-UAV, developed by scientists at the Mobile Systems Research Laboratory at the Poznań University of Technology, filmed flood embankments, and the image with data from emergency terminals (monitoring the position of vehicles and embankment moisture content) was presented at the system working stations prepared for the local administration officials.

## ZBUDOWANIE SIECI DOWODZENIA NA POTRZEBY ĆWICZENIA „PIERŚCIEŃ” NIE BYŁOBY MOŻLIWE BEZ OGROMNEGO UDZIAŁU WOJSK LĄDOWYCH

ZBUDOWANIE  
SIECI  
DOWODZENIA NA  
POTRZEBY ĆWICZENIA  
„PIERŚCIEŃ” NIE BYŁOBY  
MOŻLIWE BEZ  
OGROMNEGO UDZIAŁU  
WOJSK LĄDOWYCH

### ARMY'S FUTURE

It is necessary to point out that developing the command network for the needs of the Pierścień Exercise would not have been possible without a significant contribution of the land forces. Several hundred troops from the 100th Communication Battalion, the 12th Command Battalion of the 12th Mechanized Division, command battalions of the 12th Mechanized Brigade, and the 7th Coastal Defense Brigade, as well





## Indywidualny terminal taktyczny / Tactical Terminal Tablet

Mobilny komputer taktyczny jest elementem nasobnej lub pokładowej platformy sprzętowej dla użytkowników końcowych, głównie Sieciocentrycznej Platformy Teleinformatycznej Jaśmin. Może pracować między innymi jako urządzenie przenośne przeznaczone dla systemu DSS Jaśmin (Dismounted Soldier System) lub jako wyposażenie stanowiska pracy w pojeździe (we współpracy z adapterem instalacyjnym), wchodząc w skład wyposażenia systemu BMS Jaśmin (Battlefield Management System). Obecnie jest to jedyny tej klasy terminal w Polsce i jeden z nielicznych w świecie, spełniający normy obronne, dotyczące między innymi odporności mechanicznej i środowiskowo-klimatycznej. Umożliwia, na przykład, pracę w wodzie oraz jest wytrzymały na upadki i wstrząsy.

### Charakterystyka:

- **procesor:** architektura ARM, 1.2 GHz, dwu- lub czterordzeniowy,
- **pamięć operacyjna:** 2 GB DDR3,
- **dyski:** 2 x karta SD (wymienne),
- **wyświetlacz:** LCD 7" dotykowy, system operacyjny: Android, Windows,
- **wyposażenie podstawowe:** dwie kamery wideo, akcelerometr, magnetometr, GPS i czytnik kart kryptograficznych,
- **wyposażenie dodatkowe:** wyświetlacz HMD (Helmet Mounted Display) i dedykowany adapter instalacyjny do pracy w pojeździe,
- **interfejsy:** 1 x VGA, 2 x USB 2.0, 1 x Gigabit Ethernet, 1 x Audio, 1 x Wi-Fi (802.11 b/g/n), 1 x Bluetooth, 1 x moduł GSM lub CDMA (opcjonalnie).

Tactical Terminal Tablet is a mobile tactical computer, a man-pack element or on-board equipment for end-users, mainly for the Jasmine Network Centric Data Communication Platform. The terminal can be used mainly as a portable device with the Jasmine DSS (Dismounted Soldier System) or as workplace equipment in a vehicle (compatible with an installation adapter), as part of, for example, the Jasmine BMS (Battlefield Management System). Currently in its class it is the only terminal in Poland, and one of the few in the world, meeting defensive standards, such as anti-shock, climatic and environmental. It is shock-resistant and can be operated in water.

### Parameters:

- Processor: ARM architecture, 1.2 GHz, dual or quad core
- Random Access Memory: 2 GB DDR3
- Hard Disc Drive: 2 x SD card (replaceable)
- Display: LCD 7" touch screen
- Operational System: Android, Windows
- Basic Equipment: two video cameras, accelerometer, magnetometer, GPS receiver and cryptographic card reader
- Additional equipment: HMD (Helmet-Mounted Display) and installation adapter for vehicles
- Interfaces: 1 x VGA, 2 x USB 2.0, 1 x Gigabit Ethernet, 1 x Audio, 1 x Wi-Fi (802.11 b/g/n), 1 x Bluetooth, 1 x GSM or CDMA modem (optional)

Zbudowanie sieci dowodzenia na potrzeby ćwiczenia „Pierścień” nie byłoby możliwe bez ogromnego udziału Wojsk Lądowych. Rozwinięciem systemu Jaśmin oraz zapewnieniem sprawności 150 terminali roboczych oraz 37 serwerów zajmowało się kilkuset żołnierzy z 100 Batalionu Łączności, 12 Batalionu Dowodzenia z 12 Dywizji Zmechanizowanej oraz z batalionów dowodzenia 12 Brygady Zmechanizowanej i 7 Brygady Obrony Wybrzeża. Uczestniczyli w tym również specjaliści z Centrum Wsparcia Mobilnych Systemów Dowodzenia Wojsk Lądowych (CWMSD).

Siły Zbrojne RP planują w najbliższym czasie wyposażyć w zautomatyzowane systemy dowodzenia wszystkie jednostki liniowe Wojsk Lądowych. Podczas zajęć w Laboratorium Zautomatyzowanych Systemów Dowodzenia Wydziału Zarządzania i Dowodzenia oraz w czasie ćwiczeń, takich jak „Pierścień”, słuchacze Akademii Obrony Narodowej mieli okazję przekonać się, jaką rewolucję spowoduje wprowadzenie tych systemów do służby w naszej armii. ■

as specialists from the Land Forces Mobile Command Systems Support Center worked to develop the Jasmine system and keep 150 working terminals and 37 servers in operational order.

The Polish Armed Forces plan to equip all land forces frontline units with automated command systems in the nearest future. During classes in the Automated Command Systems Laboratory at the Department of Management and Command and exercises, such as the Pierścień Exercise, students at AON have a chance to see that introducing such systems into our army can be a true revolution. ■



TRANSLATED BY DOROTA ASZOFF



# polska Zbrojna



KIELCE 2012  
**MSP0**  
WYDANIE SPECJALNE/SPECIAL EDITION

# SEKRETNY JĘZYK

**Największe natowskie ćwiczenia** systemów dowodzenia i łączności już po raz drugi odbyły się w Polsce.

Kilkanaście lat temu do sprawnego dowodzenia wielonarodową jednostką natowską wystarczała znajomość procedur sojuszniczych i języka angielskiego. Rozwój technologii sprawił jednak, że radiolinie zostały zastąpione przez łączność satelitarną, mapy papierowe wyparte przez trójwymiarowe obrazy generowane komputerowo, a dowódcy dostali do dyspozycji sieciocentryczne systemy dowodzenia, oznaczone symbolem C4ISR. Dzięki nim rozkazodawcy wszystkich szczebli mają pełną wiedzę o tym, co się dzieje z podległymi im żołnierzami. W ciągu kilku sekund otrzymują informacje o ich lokalizacji, błyskawicznie mogą przesłać im dane z rozpoznania, kierować wsparciem ogniowym, wysłać pomoc medyczną.

Amerykanie, Brytyjczycy, Niemcy, Holendrzy i Francuzi zaczęli pracować nad systemami C4ISR już na początku lat dziewięćdziesiątych ubiegłego wieku. Robili to samodzielnie lub w niewielkich grupach (złożonych z trzech, czterech państw), więc teraz, gdy przychodzi do wspólnych misji, narodowe systemy C4ISR nie są kompatybilne. Poważnym utrudnieniem są zabezpieczenia i klauzule bezpieczeństwa nakładane na dane, które na polu walki mogą zadecydować o zwycięstwie lub porażce. Największym wyzwaniem NATO stało się opracowanie standardów umożliwiających bezproblemową współpracę narodowych systemów dowodzenia i łączności o klauzuli NATO Secret.

## WIELONARODOWOŚĆ

Zagrożenia, jakie dla interoperacyjności niesie ze sobą cyfryzacja pola walki, jako pierwsi dostrzegli Amerykanie. W 1994 roku uruchomili program Joint Warrior Interoperability Demonstration, który początkowo miał jedynie doprowadzić do unifikowania istniejących w US Army systemów łączności i dowodzenia. Europa szybko się do tego programu przyłączyła i już w 1995 roku odbyły się w Niemczech pierwsze międzynarodowe warsztaty interoperacyjności wojsk łączności i informatyki – Combined Endeavor 95 (CE 95).

Jednym z amerykańskich priorytetów była wówczas integracja z sojuszem państw ubiegających się o członkostwo w NATO,

# SECRET LANGUAGE

The biggest NATO command and communication system testing exercise was organized in Poland for the second time.

Only a little over ten years ago, the proper command of English language and knowledge of standardized allied procedures were sufficient to effectively command a multinational NATO unit. However, technological advancement changed radio lines into satellites, paper maps into three-dimensional computer images, and commanders started to use network centric command and control systems known as C4ISR. The systems provide all-level commanders with full knowledge of what is happening with their subordinates: commanders can localize them, send them reconnaissance data, control fire support or send medical help, all in a matter of seconds.

Development of C4ISR systems first started at the beginning of 1990s in the USA, Great Britain, Germany, the Netherlands and France. These states worked alone or in small groups of three or four – in effect, when it comes to them working together in missions, their C4ISR systems are incompatible. The biggest impediment are security systems and classified data, the access to which in combat can sometimes make a difference in a win-or-lose situation. The biggest challenge for NATO is to define standards ensuring unproblematic cooperation of national command and communications systems with NATO Secret classification.

## MULTINATIONALITY

Americans were the first to notice the threat that battlefield digitization poses to interoperability. In 1994, they launched the Joint Warrior Interoperability Demonstration program whose initial task was merely to unify all command and communication systems in the US Army. Europe quickly joined the program, and in 1995 organized the first international military exercise for interoperability of military communications and information system – Combined Endeavor 95 (CE 95).

Then, one of US priorities was integration with the alliance of states that wanted to join NATO. Apart from Ger-





U S D O P

**W trakcie ćwiczeń CWIX nasza armia ma okazję sprawdzić w praktyce stosowane przez siebie procedury i bezpieczeństwo wojskowych sieci komputerowych./ During CWIX, the Polish army has a chance to test applied procedures and the security of military computer networks in practice.**

do udziału w CE 95 zaproszono więc (oprócz Niemiec i Austrii) kraje uczestniczące w „Partnerstwie dla pokoju” – Czechy, Węgry, Bułgarię, Rumunię, Słowację, Słowenię i Polskę. Kiedy cztery lata później NATO się poszerzyło, Amerykanie (finansujący ćwiczenia z własnych funduszy) zdecydowali, że warsztaty te będą jednym z narzędzi wspierających integrację sojuszu z państwami, które niekoniecznie chcą być w NATO, ale deklarują gotowość do militarnej współpracy z paktem. To dlatego w CE 2011 wzięli udział żołnierze aż z 40 państw, w tym oficerowie i podoficerowie z byłych republik radzieckich – Armenii, Azerbejdżanu, Kazachstanu i Gruzji, a do obserwacji ćwiczeń zaproszono oficerów z Afryki Zachodniej i Środkowej.

### **ZŁOTE STANDARDY**

Dla naszych sojuszników zza oceanu od samego początku było jasne, że jedynym rozwiązaniem problemu interoperacyjności systemów dowodzenia jest wprowadzenie jednolitych dla wszystkich standardów technologicznych (na przykład takiej samej architektury baz danych czy sposobów programowania), które zagwarantują kompatybilność opracowywanych w ramach narodowych prac badawczo-rozwojowych systemów C4ISR.

Europejska część NATO podzielała opinię Amerykanów o potrzebie ich ujednolicenia, ale nie zgadzała się ze wskazaniami sojuszników, które standardy najlepiej się nadają na platformę unifikacji systemów C4ISR. Na przełomie wieków doszło więc do tak kuriozalnej sytuacji, że kraje sojuszu w ramach dużych wielonarodowych programów badawczych pracowały równolegle nad kilkunastoma standardami dla syste-

many and Austria, invitations to join CE 95 were delivered to Partnership for Peace states – the Czech Republic, Hungary, Bulgaria, Romania, Slovakia, Slovenia and Poland. When four years later NATO expanded, Americans (financing the exercise from their own funds) decided that the workshop will be one of the tools supporting integration of the treaty with the states that do not necessarily want to join NATO, but declare their readiness for military cooperation with the treaty. For that reason, soldiers from over 40 states participated in CE 2011, including officers and NCOs from the former Soviet republics – Armenia, Azerbaijan, Kazakhstan and Georgia, and officers from Western and Middle Africa were invited to observe the exercise.

### **GOLDEN STANDARDS**

For our US allies it was clear from the very beginning that the only solution to the problem of command system interoperability is introducing unified technological standards (e.g. the same architecture without data or programming methods), which will guarantee compatibility of C4ISR systems developed within the framework of national research and development projects.

NATO's European part shared the US view on the necessity of unification, but did not agree with their opinion on which standards are best for the C4ISR unification platform. All this led to a peculiar situation when at the turn of the century NATO states simultaneously worked on over a dozen standards for the C4ISR systems within big multinational research programs. To name just a few: MIP (Multi-



mów C4ISR, w tym między innymi MIP (Multilateral Interoperability Programme), NFFI (NATO Friendly Force Information) oraz ADatP-3 (Allied Data Publication Number 3).

Do symbolicznego porozumienia w tej sprawie między Europą a USA doszło na szczycie NATO w Pradze w 2002 roku. Zadanie opracowania programu osiągnięcia przez NATO sieciowej zdolności interoperacyjnej – NATO Network Enabled Capability (NNEC) – powierzono Radzie NATO do spraw Konsultacji, Dowodzenia i Kontroli (NATO Consultation, Command and Control Board – NC3B). Jesienią 2003 roku dziewięć państw – Kanada, Francja, Niemcy, Włochy, Holandia, Norwegia, Hiszpania, Wielka Brytania i Stany Zjednoczone – podpisało porozumienie zobowiązujące do realizacji programu. Nadzór nad wdrożeniem NNEC powierzono agencji NC3A (NATO Consultation, Command and Control Agency – Agencja NATO do spraw Konsultacji, Dowodzenia i Kierowania).

Start programu NNEC nie oznaczał, że wybrano jeden standard (na przykład określony sposób programowania baz danych), który muszą spełniać wszystkie systemy C4ISR. Program zakładał jedynie, że jego sygnatariusze skoncentrują swój wysiłek naukowo-badawczy na opracowaniu rozwiązań umożliwiających ich unifikację. Na poligon doświadczalny wybrano ćwiczenia CWIX (Coalition Warrior Interoperability eXercise, eXamination, eXperimentation, eXploration), których organizację zlecono NC3A.

### CWIX W POLSCE

Od dwóch lat ćwiczenia CWIX są organizowane w naszym kraju. Wprawdzie decyzja o przeniesieniu największych nатовskich ćwiczeń systemów dowodzenia i łączności z Norwegii do Polski zapadła w dużej mierze dzięki naszym zabiegom dyplomatycznym, nie bez znaczenia był fakt, że to polskie rozwiązania teleinformatyczne, w tym przede wszystkim sieciocentryczny system dowodzenia Jaśmin, zarówno w czasie CE, jak i CWIX, uzyskiwały najlepsze wyniki testów. Polska konstrukcja może współpracować nie tylko ze starszymi systemami, opartymi na standardzie MIP Baseline 2 (a takie mają w swojej armii między innymi Francuzi, Niemcy, Norwegowie i Szwedzi), ale również z tymi, których podstawą jest NFFI, ADatP-3, TEDS, NVG. Tak uniwersalnego rozwiązania nie mają nawet Amerykanie.

Na tegorocznych ćwiczeniach CWIX nie tylko zgłosiliśmy do sprawdzenia najwięcej systemów, ale z wynikiem 85 procent zaliczonych testów wyraźnie wyprzedziliśmy konkurencję, która pozytywnie zakończyła jedynie 70 procent zadań.

O tym, jak ważne jest osiągnięcie przez sojusz północnoatlantycki interoperacyjności systemów dowodzenia i łączności, mówił wizytujący CWIX generał **Stephane Abrial**, dowódca strategiczny NATO do spraw transformacji (ACT). Podkreślał on, że ćwiczenia odbywają się według programu wpisującego się w rozwój koncepcji Smart Defence (zacieśnianie współpracy pomiędzy członkami sojuszu dla zapewnienia większego bezpieczeństwa za mniejsze środki, między innymi dzięki wspólnym zakupom sprzętu i uzbrojenia wojskowego). „To doskonała okazja, żeby przetestować różne systemy dowodzenia, z jakich korzystają członkowie NATO i państwa partnerskie, a także zgrać ze sobą zespoły, które być może w przyszłości będą musiały z tych systemów korzystać”, mówił generał **Abrial**.

W podobnym tonie wypowiadał się szef Sztabu Generalnego Wojska Polskiego, generał **Mieczysław Cieniuch**: „Są to ćwiczenia

lateral Interoperability Programme), NFFI (NATO Friendly Force Information) and ADatP-3 (Allied Data Publication Number 3).

A symbolic European-US agreement on this matter was reached at the 2002 Prague NATO Summit. The task to develop a program helping NATO to achieve network interoperability [NATO Network Enabled Capability (NNEC)] was entrusted to the NATO Consultation, Command and Control Board (NC3B). In the fall of 2003, nine states (Canada, France, Germany, Italy, the Netherlands, Norway, Spain, Great Britain and the USA) signed an agreement obliging them to execute the program. The NATO Consultation, Command and Control Agency (NC3A) was appointed to supervise the implementation of NNEC.

Starting the NNEC program did not mean having chosen one standard (e.g. a certain method of programming without data) to be followed by all C4ISR systems. NNEC simply assumed that its signatories would concentrate their efforts on developing solutions enabling their unification. The CWIX Exercise organized by the NC3A was chosen as the “proving ground”.

### CWIX IN POLAND

For two years the CWIX Exercise has been organized in Poland. The decision to relocate NATO's biggest command and communication systems testing program from Norway to Poland was taken largely thanks to our diplomatic endeavors. However, the fact that Polish telematic solutions, particularly the **Jasmine network centric command and control system**, had the best test results both at the CE and the CWIX was not without significance. The Polish **Jasmine system** can cooperate not only with older systems based on the MIP Baseline 2 standard (French, German, Norwegian, Swedish and other armies work on such systems), but also those based on NFFI, ADatP-3, TEDS, NVG. Even Americans do not have such a universal solution.

At this year's CWIX Exercise, Poland not only submitted the greatest number of systems for testing, but also noticeably outran the competition with 85 percent of tasks completed with positive result, compared to their 70 percent.

The importance of achieving interoperability of command and communication systems by NATO was commented on by the Supreme Allied Commander Transformation visiting CWIX, General **Stephane Abrial**. He emphasized that the exercises are conducted according to the program being a part of the Smart Defense concept development (tightening cooperation between members of the treaty to ensure more security for less money through, e.g. joint purchases of equipment and military armament). “This is a perfect occasion to test various command systems used by the NATO members and partner states, and integrate teams which might have to use these systems in the future”, said General **Abrial**.

The Chief of the General Staff of the Polish Armed Forces, General **Mieczysław Cieniuch**, expressed the same opinion: “This is an exercise during which the representatives of 21 states try to find a common platform for command systems organization. The results of the exercises will be applied in all NATO member states. All this is done to im-





**GENERAŁ STEPHANE ABRIAL, DOWÓDCA STRATEGICZNY NATO:** Ćwiczenia CWIX to doskonała okazja, żeby przetestować różne systemy dowodzenia, z jakich korzystają członkowie NATO i państwa partnerskie, a także zgrać ze sobą zespoły, które być może w przyszłości będą musiały z tych systemów korzystać”

czenia, w czasie których przedstawiciele 21 państw próbują znaleźć wspólną platformę organizacji systemów dowodzenia. Rezultaty będą wprowadzone do użytku w całym sojuszu północnoatlantyckim. Wszystko ma sprzyjać poprawie interoperacyjności systemu dowodzenia sojuszniczego”.

#### CENNA LEKCJA

Polska bardzo dobrze wykorzystuje szansę, jaką jest organizacja ćwiczeń CWIX. Nasza armia ma okazję sprawdzić w czasie praktycznych międzynarodowych testów stosowane przez siebie procedury i bezpieczeństwo wojskowych sieci komputerowych. Choć koordynatorem prac związanych z organizacją, przygotowaniem oraz udziałem strony polskiej w CWIX był Departament Informatyki i Telekomunikacji MON, w ćwiczenia były zaangażowane również inne instytucje, nie tylko Zarząd Planowania Systemów Dowodzenia i Łączności P6, dowództwa rodzajów sił zbrojnych, ale przede wszystkim resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług, Centrum Wsparcia Teleinformatycznego Sił Zbrojnych oraz Centrum Wsparcia Mobilnych Systemów Dowodzenia.

Ochroną ćwiczeń w sferze cybernetycznej zajmował się polski zespół CIAT (Coalition Information Assurance Team), powołany i kierowany przez Departament Informatyki i Telekomunikacji MON. Odpowiadał on między innymi za monitorowanie sieci pod kątem ataków sieciowych, aktywności złośliwego oprogramowania oraz naruszeń ustalonej polityki bezpieczeństwa. ■

prove interoperability of the allied command and control system”.

#### VALUABLE LESSON

Poland makes the most of the opportunity to organize the CWIX Exercise. Our army has a chance to check applied procedures and security of military computer networks in practical, international tests. Although the activities related to the organization, preparation and Polish participation in CWIX were coordinated by the Informatics and Telecommunications Department at the Ministry of National Defense, other institutions were also engaged in the exercise. Not only those of the P6 Command and Communication Systems Planning Board and commands of military branches, but above all of the Ministerial Center for Network Security and ICT Services Management, the Armed Forces ICT Support Center and the Mobile Command Systems Support Center.

Cyber defense services during the exercise were provided by the Polish CIAT (Coalition Information Assurance Team), created and managed by the Informatics and Telecommunications Department. The team was responsible for monitoring the network against attacks, malicious software, violations of established security policy, and others. ■

TRANSLATED BY DOROTA ASZOFF