

III KONFERENCJA ŁĄCZNOŚCI

DWUDZIESTOLECIE WOJSK ŁĄCZNOŚCI I INFORMATYKI WOJSKA POLSKIEGO



Ewolucja wojskowych
systemów teleinformatycznych
oraz Lessons Learned
w świetle misji pokojowych i stabilizacyjnych

PRACA ZBIOROWA



15 SBWD
STOWARZYSZENIE PRZYJACIÓW

KONFERENCJA
DWUDZIESTOLECIE CYFRYZACJI
WOJSK ŁĄCZNOŚCI I INFORMATYKI
W WOJSKU POLSKIM.

EWOLUCJA WOJSKOWYCH SYSTEMÓW
TELEINFORMATYCZNYCH
ORAZ LESSONS LEARNED W ŚWIETLE MISJI
POKOJOWYCH I STABILIZACYJNYCH.

**ŚWIATOWY ZWIĄZEK POLSKICH ŻOŁNIERZY ŁĄCZNOŚCI
15 SIERADZKA BRYGADA WSPARCIA DOWODZENIA
STOWARZYSZENIE PRZYJACIÓŁ 15SBWD**

**KONFERENCJA
DWUDZIESTOLECIE CYFRYZACJI
WOJSK ŁĄCZNOŚCI I INFORMATYKI
W WOJSKU POLSKIM.**

**EWOLUCJA WOJSKOWYCH SYSTEMÓW
TELEINFORMATYCZNYCH
ORAZ LESSONS LEARNED W ŚWIETLE MISJI
POKOJOWYCH I STABILIZACYJNYCH.**

21 marca 2012

SIERADZ 2012

RECENZENCI:

płk dr hab. inż. Jan POSOBIEC

płk dr hab. inż. Marek KUBIŃSKI

REDAKCJA:

mjr mgr inż. Radosław URYCKI

Andrzej DURSKI

KOMITET NAUKOWY:

płk dr inż. Piotr DELA

ppłk dr inż. Maciej MARCZYK

ppłk dr inż. Mariusz FRĄCZEK

KOMITET ORGANIZACYJNY:

gen. bryg. dr inż. Józef NASIADKA

płk Roman JANUSZEWSKI

Światowy Związek Polskich Żołnierzy Łączności

Stowarzyszenie Przyjaciół 15 SBWD

mjr mgr inż. Radosław URYCKI

Beata MICHALSKA

Agnieszka SOBCZAK

Andrzej DURSKI

PROJEKT OKŁADKI:

Beata MICHALSKA

Książka sfinansowana z dotacji Ministerstwa Obrony Narodowej

Opracowanie zawiera materiały wygłoszone podczas konferencji.

Forma i treść przedstawienia materiałów odpowiada wersji przekazanej przez autorów.

SPIS TREŚCI

WSTĘP.....	9
<i>mjr mgr inż. Radosław URYCKI</i>	
 SIECIOCENTRYCZNOŚĆ W DZIAŁANIACH KOALICYJNYCH (SIEĆ AMN - AFGHANISTAN MISSION NETWORK)	11
<i>plk Paweł KRZYMIŃSKI</i>	
 XX-LECIE CYFRYZACJI SYSTEMU ŁĄCZNOŚCI SZ RP.....	23
<i>gen. bryg. w st. spocz. Wojciech WOJCIECHOWSKI</i>	
 SIECI TELEINFORMATYCZNE KOMPONENTU WOJSK LĄDOWYCH...	33
<i>plk dr inż. Piotr DELA</i>	
 MIEJSCE ZESPOŁU WSPARCIA TELEINFORMATYCZNEGO NA STANOWISKU DOWODZENIA POZIOMU TAKTYCZNEGO WOJSK LĄDOWYCH	51
<i>ppłk dr inż. Maciej MARCZYK</i>	
 WSPARCIE TELEINFORMATYCZNE WŁĄD W UJĘCIU ORGANIZACJI OPARTEJ NA WIEDZY	59
<i>ppłk Adam GRYCZON</i>	
 SYSTEM OCHRONY SIECI TELEINFORMATYCZNYCH PRZED DZIAŁANAMI NIEUPRAWNIONYMI SOPAS	69
<i>mjr mgr inż. Bartosz JASIUL</i> <i>dr inż. Rafał PIOTROWSKI</i>	
 KONCEPCJA I ZAKRES WYKORZYSTANIA GBWI DO OCHRONY UDOSTĘPNIANYCH INFORMACJI	77
<i>mjr mgr inż. Robert GONIACZ</i> <i>dr inż. Łukasz APIECIONEK</i>	
 FIDELIS XPS - SYSTEM OCHRONY PRZED WYCIEKIEM INFORMACJI ..	85
<i>Tomasz STYPIK</i>	

CYBERTERRORYZM – ANALIZA ZJAWISKA	97
<i>dr inż. Ernest LICHOCKI</i>	
MOBILNY SYSTEM DYSPOZYTORSKI	107
<i>Robert ABRAMCZUK</i>	
REALIZACJA DLA SŁUŻB MUNDUROWYCH	113
<i>Szymon KUPAJ</i>	
WEB PORTAL JAŚMIN ZINTEGROWANY SYSTEM WSPARCIA DOWODZENIA ORAZ ZOBRAZOWANIA POŁA WALKI C4ISR	131
<i>mgr inż. Henryk KRUSZYŃSKI</i>	
<i>dr inż. Łukasz APIECIONEK</i>	
<i>inż. Rafał MOTYLEWSKI</i>	
<i>mgr inż. Marek JELIŃSKI</i>	
NARODOWY SYSTEM TAKTYCZNEJ ŁĄCZNOŚCI RADIOWEJ NASTAR ..	141
<i>Stanisław KOSICKI</i>	
SYSTEM ŁĄCZNOŚCI POŁOWEJ (TACTICAL COMMUNICATIONS SYSTEM) STORCZYK. HISTORIA, STAN AKTUALNY I KIERUNKI ROZWOJU	151
<i>dr inż. Jan JACH</i>	
ŁĄCZNOŚĆ TROPOSFERYCZNA – MOŻLIWOŚCI ZASTOSOWANIA W MISJACH POKOJOWYCH I STABILIZACYJNYCH	155
<i>dr inż. Zbigniew FIOŁNA</i>	
WYKORZYSTANIE APARATOWNI TRANSMISYJNEJ TROPOSFERYCZNO – HORYZONTOWEJ W SYSTEMIE ŁĄCZNOŚCI ..	169
<i>mgr inż. Jacek GOŁĄBEK</i>	
SYSTEMY ŁĄCZNOŚCI POZAHORYZONTALNEJ	175
<i>Erwin BRODA</i>	

MOŻLIWOŚCI TELETRANSMISYJNE RADIOSTACJI RODZINY RKS-8000/RKP-8100	181
<i>Jerzy PAKIESER</i>	
<i>Marcin WIŚNIEWSKI</i>	
<i>Jacek WOJTKOWIAK</i>	
JEDNOCZESNA PRACA RADIOSTACJI RKS-8000/RKP-8100	189
<i>Jacek WOJTKOWIAK</i>	
<i>Adam DOBKOWSKI</i>	
<i>Marcin RYMON-LIPIŃSKI</i>	
INTELIGENTNY KONSULTANT NA POTRZEBY KLASYFIKACJI OBIEKTÓW W ZAUTOMATYZOWANYCH SYSTEMACH DOWODZENIA – DEMONSTRATOR TECHNOLOGII	201
<i>dr inż. Ksawery KRENC</i>	
<i>inż. Michał OTOKA</i>	
MODERNIZACJA ZAUTOMATYZOWANYCH WOZÓW DOWODZENIA IRYS 2000 – PROPONOWANY ZAKRES ZMIAN I OCZEKIWANE REZULTATY	209
<i>mgr inż. Marek PARADIUK</i>	
NOWE OPROGRAMOWANIE RADIOSTACJI F@STNET.....	215
<i>Jacek TRUSZKOWSKI</i>	
NOWOCZESNE ŚRODKI ŁĄCZNOŚCI I TRANSMISJI DANYCH POLA WALKI W ZASTOSOWANIU PRAKTYCZNYM I TENDENCJE ROZWOJOWE	223
<i>Zygmunt SALATA</i>	
NIEZAWODNOŚĆ ZASILANIA W WARUNKACH POLOWYCH	237
<i>mgr inż. Jacek GOŁĄBEK</i>	
KOMPLEMENTARNY SYSTEM ZASILANIA POKŁADOWEGO MOCY POJAZDÓW WOJSKOWYCH “ELEKTRIT”	243
<i>Krzysztof MŁYNARCZYK</i>	

ODPORNOŚĆ WOJSKOWYCH URZĄDZEŃ ELEKTRONICZNYCH NA NARAŻENIA ELEKTROMAGNETYCZNE O WYSOKIEJ ENERGII (HPM)	255
<i>Marek DRAS</i>	

WYBRANE PROBLEMY I WYMAGANIA EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH W ZARZĄDZANIU KRYZYSOWYM	273
<i>ppłk dr inż. Mariusz FRĄCZEK</i>	
<i>mgr inż. Arkadiusz SZALPUK</i>	

WSTĘP

21 marca 2012 roku Światowy Związek Polskich Żołnierzy Łączności, 15 Sieradzka Brygada Wsparcia Dowodzenia oraz Stowarzyszenie Przyjaciół 15SBWD po raz trzeci zorganizowały, pod honorowym patronatem Szefa Zarządu Planowania Systemów Dowodzenia i Łączności – P6 SG WP gen. bryg. Józefa NASIADKI, Konferencję: Dwudziestolecie Cyfryzacji Wojsk Łączności i Informatyki w Wojsku Polskim na temat „Ewolucja wojskowych systemów teleinformatycznych oraz Lessons Learned w świetle misji pokojowych i stabilizacyjnych”.

Celem konferencji, której pomysłodawcą jest gen. bryg. w st. spocz. Mirosław SIEDLECKI, pozostaje przedstawianie zmian zachodzących w wojskowych systemach i sieciach teleinformatycznych, towarzyszących im przeobrażeń organizacyjno-etatowych oraz ewolucji sprzętu łączności i informatyki. Wymiana doświadczeń zdobytych podczas pełnienia misji w Polskich Kontyngentach Wojskowych musi się odbywać w relacjach między żołnierzami, ale również między wojskiem a przemysłem. Bardzo ważnym elementem w planowaniu i codziennym szkoleniu jest umiejętne korzystanie z doświadczeń zdobytych przez wojska własne jak i koalicyjne. Obserwuje się rozwój e-learningu w Siłach Zbrojnych RP lecz najbardziej atrakcyjną formą przekazywania wiedzy i umiejętności pozostaje nadal kontakt bezpośredni, jak to się dzieje w opisywanym przedsięwzięciu.

Do uczestnictwa w Konferencji zostały zaproszone instytucje i jednostki organizacyjne resortu obrony narodowej, instytucje administracji publicznej i samorządowej oraz firmy oferujące sprzęt, oprogramowanie oraz usługi w dziedzinie szeroko rozumianej teleinformatyki.

Referaty bądź prezentacje opracowane były na podstawie niżej wymienionych zagadnień opublikowanych przez organizatorów w specjalnym komunikacie:

1. 20-lecie cyfryzacji Wojsk Łączności i Informatyki Wojska Polskiego.
2. Zmiany organizacyjno-etatowe w pododdziałach dowodzenia i łączności.
3. Rozwój systemów teletransmisyjnych stacjonarnych i polowych.
4. Narodowe systemy C4ISR.
5. Cyberterroryzm i cyberobrona.

Konferencję rozpoczął Dowódca 15 Brygady Wsparcia Dowodzenia płk Roman JANUSZEWSKI witając wszystkich zgromadzonych gości. Następnie słowa powitania i wprowadzenia w tematykę rozwoju wojsk łączności i informatyki wygłosił Szef ZPSDiŁ-P6 SG WP gen. bryg. Józef NASIADKA. Kolejne wystąpienia poprowadzili oficerowie Wojska Polskiego przedstawiając kierunki zmian technologicznych, doktrynalnych oraz organizacyjnych, a także aktualne działania na rzecz pogłębiania interoperacyjności w ramach Paktu Północnoatlantyckiego. Przedstawiciele firm komercyjnych zaprezentowali podczas wystąpień i na stanowiskach promocyjnych produkty, które mogą znaleźć zastosowanie w Siłach Zbrojnych RP. Przedstawione rozwiązania obejmowały bardzo szeroki obszar tematyczny. Omawiano nowe systemy telekomunikacyjne, teletransmisyjne: satelitarne, troposferyczne, radiowe KF i UKF, radiostacje osobiste, przedstawiono propozycje modernizacji i rozwoju obecnie eksploatowanych aparatowni i wozów dowodzenia. Wiele uwagi poświęcono sposobom przekazywania informacji, jej przetwarzania, ochrony przed nieuprawnionym dostępem oraz zobrazowania. Przedstawiono także rozwiązania nowych systemów zasilania stanowisk dowodzenia, elementów węzłów łączności i samych końcowych urządzeń teleinformatycznych.

Konferencję zakończył Zastępca Dowódcy Garnizonu Warszawa płk Andrzej ŚMIETANA, a gen. bryg. Józef NASIADKA dokonał podsumowania bardzo bogatej tematycznie Konferencji i wyraził nadzieję, że będzie ona kontynuowana w kolejnych latach.

Przedsięwzięciu towarzyszyła wystawa nowoczesnego sprzętu łączności i informatyki będącego na wyposażeniu 15BWD oraz stanowisko promocyjne NSR współorganizowane z WKU w Sieradzu, które były licznie odwiedzane przez dzieci i młodzież regionu sieradzkiego.

KONCEPCJA I ZAKRES WYKORZYSTANIA GBWI DO OCHRONY UDOSTĘPNIANYCH INFORMACJI

mjr mgr inż. Robert GONIAŁ

WOJSKOWY INSTYTUT ŁĄCZNOŚCI

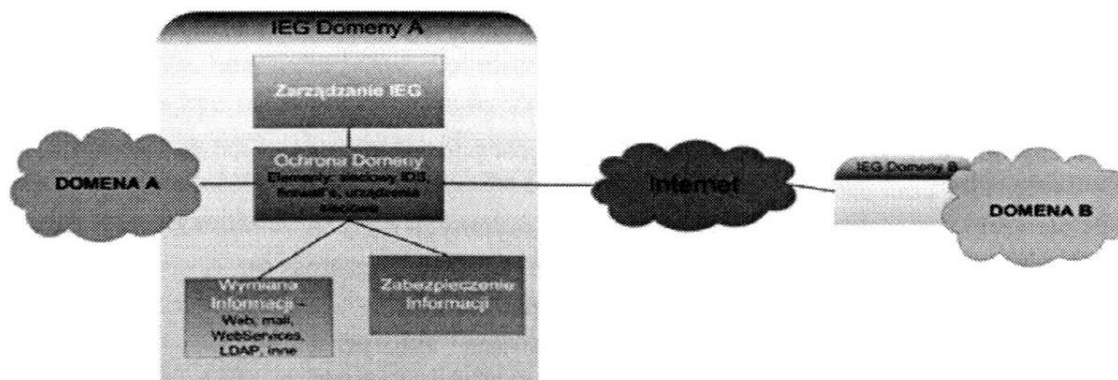
dr inż. Łukasz APIECIONEK

TELDAT Sp. J.

Celem artykułu jest przedstawienie koncepcji projektu GBWI (Gateway bezpiecznej wymiany informacji) oraz możliwości potencjalnych zastosowań do wymiany i ochrony informacji udostępnianych zewnętrznym użytkownikom. W artykule opisano koncepcję urządzenia oraz zaproponowane rozwiązania i mechanizmy kontroli przepływu i ochrony danych.

1. Wstęp

W obecnych działaniach zachodzi konieczność wymiany informacji za pomocą zdefiniowanych typów protokołów jak również w postaci sformalizowanych typów dokumentów (WWW, Webservice, pdf, ftp itp.). Bardzo istotnym problemem jest współdzielenie tych informacji pomiędzy domenami (partnerami), w których udostępniane są zasoby o różnym poziomie wrażliwości. Określając współdzielenie informacji zazwyczaj ustala się stronę o tzw. niższym i wyższym poziomie bezpieczeństwa (wrażliwości) (ang. *Low/High Security Domain*) oraz to, że poziom bezpieczeństwa można zastosować dla całej domeny oraz dla poszczególnych jej składowych (użytkowników, zasobów, usług itp.). Idea mechanizmów umożliwiających kontrolę przepływu informacji na brzegu sieci została zidentyfikowana i zdefiniowana przez NATO i jest ogólnie określana jako IEG (ang. *Information Exchange Gateway*). Urządzenie tego typu może być elementem niezbędnym do kontroli wymiany informacji pomiędzy narodowymi systemami współdziałającymi w realizacji określonego celu np. misje wojskowe, minimalizacja skutków klęsk żywiołowych, pomoc humanitarna w sytuacjach kryzysowych, koordynacja działań służb państwa (wojsko, policja, straż pożarna, straż graniczna, jednostki samorządu terytorialnego). Jego zastosowanie istotne jest także w zakresie współdziałania na poziomie międzynarodowym. Idea i architektura referencyjna urządzenia przedstawiona jest na poniższym rysunku.



Rys. 1. Architektura referencyjna IEG

W referacie zaprezentowana jest architektura GBWI dostarczająca i zapewniająca bezpieczną wymianę informacji pomiędzy heterogenicznymi systemami o różnym poziomie wrażliwości. Prezentując te rozwiązania należy mieć na uwadze, że obecnie istnieją i wprowadzane są, podobne mechanizmy i infrastruktury, jednakże służą one do zabezpieczania poszczególnych (dedykowanych) protokołów (np. e-mail, WebServices). Często występują jako rozwiązania typu *proof-of-concept* testowane w ramach ćwiczeń międzynarodowych np. CWIX (poprzednio CWID). Komercyjnie oferowane rozwiązania zazwyczaj przetwarzają i zabezpieczają przepływ danych związany z usługami sieciowymi i określane są mianem XML gateway lub XML guard (np. IBM WebSphere DataPower XML Security Gateway, Layer7 XML Firewall). Rozwiązaniem opartym na architekturze IEG NATO Reference Architecture jest rozwiązanie proponowane przez firmę Nexor. Z przeprowadzonych analiz przedmiotowych wynika, że zaproponowane rozwiązanie jest interesujące i zgodne z ogólną ideą NATO. Zapewnia ono bezpieczną wymianę informacji pomiędzy domenami, jednakże nie jest w nim ujednolicony mechanizm wymuszania polityki bezpieczeństwa dla każdego kontrolowanego protokołu (oddzielne mechanizmy w modułach i elementach: *mail guard*, *XML data guard*). Próbą rozwiązania wyżej wymienionych ograniczeń jest prezentowany w tym referacie GBWI, w którym zaproponowano jednolity mechanizm wymuszania polityki bezpieczeństwa w centralnym elemencie GBWI oraz nie ograniczono kontroli przepływu informacji do jednego protokołu.

2. Ogólne wymagania

Zapewnienie pewnego i niezawodnego rozwiązania umożliwiającego przepływ informacji z domeny *high security* do domeny *low security* wymaga zastosowania i spełnienia określonych wymagań dotyczących architektury i rozwiązań technicznych. W architekturze referencyjnej zakłada się, że wymiana danych pomiędzy domenami odbywa się poprzez urządzenie brzegowe, które zabezpiecza domenę o wyższym poziomie wrażliwości i monitoruje ruch wchodzący i wychodzący z domeny. Separacje domen o wyższym i niższym poziomie wrażliwości zaproponowano rozwiązać przy pomocy pojedynczego modułu, który stanowi centralny element GBWI (XML guard). Jest on odpowiedzialny za wymuszanie polityki bezpieczeństwa w odniesieniu do poszczególnych protokołów. Jednakże, aby zapewnić taką funkcjonalność zastosowano jednolitą metodę reprezentacji i przetwarzania poszczególnych typów protokołów w odpowiednich elementach typu proxy. W centralnym elemencie GBWI wszystkie typy kontrolowanych protokołów reprezentowane są w jednolity sposób przy pomocy komunikatów SOAP/XML. Element ten jest odpowiedzialny za podjęcie decyzji, na podstawie obowiązującej polityki bezpieczeństwa, o zezwoleniu lub zabronieniu przepływu danych pomiędzy połączonymi domenami.

Zezwolenie lub wstrzymanie przepływu danych jest podejmowane na podstawie:

- źródło i cel danych;
- etykietę (etykiety) bezpieczeństwa przesyłanych danych;
- obowiązującą politykę bezpieczeństwa dla danego protokołu.

Zezwolenie na transfer danych następuje w przypadku, gdy:

- źródło i cel danych zostały zidentyfikowane i autoryzowane;
- została zweryfikowana etykieta bezpieczeństwa danych;
- polityka bezpieczeństwa zezwala na transfer danych w oparciu o poziom i prawa dostępu.

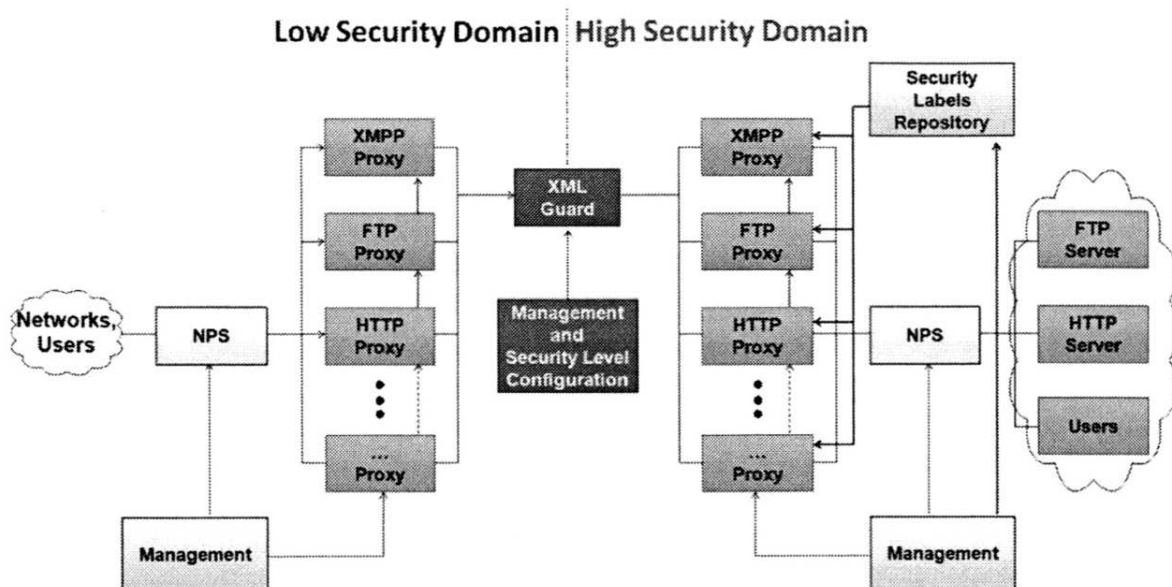
GBWI musi być w stanie kontrolować ruch pomiędzy domenami, „rozpoznawać” typy protokołów i filtrować pakiety IP (na podstawie polityki filtrowania pakietów TCP/IP). Dodatkowo na poziomie warstwy sieciowej stosowane są mechanizmy IPS/IDS (ang. *Intrusion Prevention System/Intrusion Detection System*) dla ruchu wchodzącego i wychodzącego. W GBWI zastosowano komercyjne rozwiązania IPS/IDS zintegrowane z zaawansowanymi elementami sieciowymi typu firewall. Dodatkowo zapewniona jest analiza zawartości transmitowanych danych pod kątem wykrywania złośliwego oprogramowania i wirusów. Komunikaty SOAP przesyłane pomiędzy proxy poszczególnych protokołów i XML guard muszą posiadać etykiety, które zabezpieczone są mechanizmami zapewniającymi ich integralność i niezaprzeczalność.

3. Architektura

GBWI jest koncepcją urządzenia brzegowego zabezpieczającego wymianę informacji pomiędzy współpracującymi domenami o różnych poziomach wrażliwości. Architektura stanowi kilka współpracujących ze sobą elementów fizycznych:

- 2 x NPS;
- XML guard;
- 2 x zestaw proxy dla danego protokołu.

Zgodnie z koncepcją NATO [1] NPS (ang. *Node Protection Service*) jest elementem brzegowym GBWI. Zabezpiecza dostęp do warstwy sieciowej domeny *high security* jak również do funkcji zarządzania i konfiguracji GBWI. Bazowymi funkcjami tego elementu jest wykrywanie i przeciwdziałanie nieautoryzowanemu dostępowi do sieci – IPS/IDS. Dla zwiększenia bezpieczeństwa domeny *high security* NPS pracuje w trybie NAT/PAT (ang. *Network Address Translation/Network Port Translation*) umożliwiającym ukrycie adresacji sieciowej. Dodatkowo mechanizmy filtracji pakietów IP zapewniają transmisję tylko i wyłącznie określonych protokołów na dopuszczonych do tego portach. Innymi kluczowymi elementami GBWI są proxy poszczególnych protokołów. Każdy z nich dedykowany jest dla określonego protokołu (HTTP, XMPP, ftp itp.) i jest odpowiedzialny za konwersję strumienia danych do komunikatów SOAP zawierających etykiety bezpieczeństwa. Należy zwrócić uwagę, że niektóre przesyłane dane mogą zawierać etykiety bezpieczeństwa natomiast większość z protokołów ich nie zawiera. Dla drugiego przypadku GBWI posiada mechanizm, który jest odpowiedzialny za dołączanie dodatkowych etykiet bezpieczeństwa. Etykiety bezpieczeństwa przechowywane są w SLR (ang. *Security Label Repository*) rodzajem bazy danych, zaprojektowanej dla typów danych/protokołów, które nie posiadają możliwości przechowywania informacji (metadanych) o etykietach bezpieczeństwa np. dokumenty pdf, większość formatów bitmap. SLR może być bazą danych SQL lub bazą LDAP. Etykiety bezpieczeństwa definiują minimalny poziom bezpieczeństwa domeny, do której mają być transferowane dane. Zakłada się, że tylko administrator GBWI dodaje etykiety bezpieczeństwa do repozytorium na żądanie użytkownika, a dane, które nie posiadają etykiety bezpieczeństwa nie będą wysłane z domeny. Architektura GBWI przedstawiona jest na poniższym rysunku.



Rys. 2. Architektura referencyjna GBWI

4. Etykietowanie danych

Zabezpieczanie danych wymaga mechanizmu, który umożliwia systemowi na identyfikację poziomu zabezpieczenia zasobów (dokumenty, zawartość stron WWW, obrazy itp.). W GBWI realizacja tego mechanizmu wymaga etykietowania danych. Kontrola przepływu wielu protokołów przez GBWI komplikuje to rozwiązanie ponieważ dane reprezentowane i udostępniane są w postaci wielu formatów (dokument, komunikat XML, zawartość strony WWW itp.). W rezultacie reprezentacja etykiet bezpieczeństwa, dla różnych zasobów, mogą się różnić, a w przypadku niektórych protokołów (np. XMPP) istnieje własny sposób oznaczania danych wrażliwych. Dlatego GBWI musi rozpoznawać i dokonywać transformacji tych etykiet bezpieczeństwa do własnego formatu, aby egzekwować zdefiniowaną w domenie politykę bezpieczeństwa.

GBWI definiuje model etykietowania danych złożony z następujących elementów: sekcja klasyfikacji, sekcja referencji do zasobu oraz sekcja podpisu.

Sekcja klasyfikacji jest zestawem następujących własności: właściciel, klasyfikacja bezpieczeństwa i kategoria. Właściciel opisuje źródło pochodzenia (wydania) etykiety. Klasyfikacja określa poziom wrażliwości np.: „TAJNE”, „ZASTRZEŻONE”, itp., kategoria określa etykietowany zasób.

Sekcja referencji zasobu zawiera dane, które wskazują na etykietowany zasób. Wskaźnik ten może być wyrażony jako URI (zasób identyfikowany przez URI – strona WWW, plik ftp) lub wyrażenie typu XPath dla zasobu XML, który sam zawiera etykietę bezpieczeństwa. Sekcja podpisu zawiera dane, które zapewniają odbiorcę etykiety, że pochodzi z określonego źródła i nie została zmieniona.

GBWI definiuje własny format etykiety bezpieczeństwa: dokument XML dla elementów innych niż plik XML, element XML dla plików XML.

Nazwa elementu	Opis	Możliwe atrybuty
Klasyfikacja	Odpowiada sekcji 'klasyfikacja'. Określa takie informacje jak: właściciel, klasyfikacja, kategoria.	atrybut 'Level' atrybut 'Owner' atrybut 'Category'
Referencja	Odpowiada sekcji 'referencja do zasobu'. Odwołanie do etykietowanego zasobu przez URI lub XPath.	atrybut 'URI' lub 'XPath'
Podpis	Odpowiada sekcji 'podpis'. Zgodne z http://www.w3.org/2000/09/xmlsig# [zawiera podpis etykiety.	Dozwolone przez standard XMLDSIG.

Przykład etykiety bezpieczeństwa dla dokumentu "example.doc":

```
<?xml version="1.0" encoding="utf-8"?>

<SecurityLabel xmlns:dsig="http://www.w3.org/2000/09/xmlsig#"
xmlns="http://some.pl/gbwilabel#">

    <Classification Owner="NATO" Level="RESTRICTED"
Category="NONE"/>

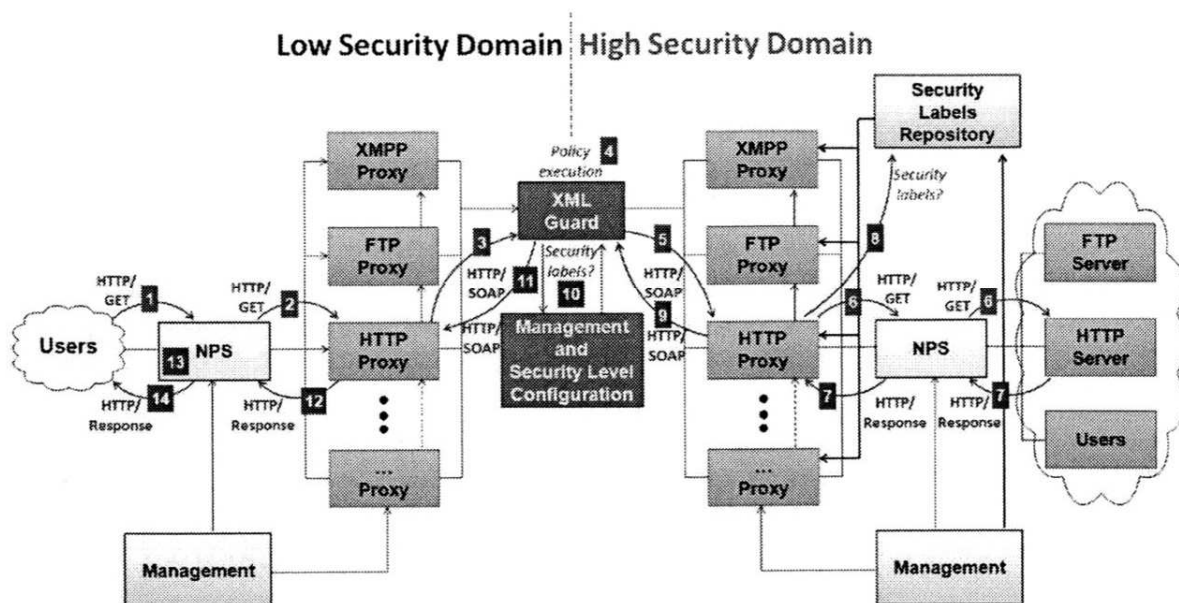
    <Reference Uri="file://192.168.19.87/documents/example.doc"/>

    <dsig:Signature>
        ...
    </dsig:Signature>

</SecurityLabel>
```

5. Przykład wymiany dokumentów

Poniżej przedstawiony jest przykład scenariusza współdzielenia dokumentów np. MS Office, pliki pdf, obrazy, mapy pomiędzy domenami. Wymiana informacji może być realizowana za pomocą stron WWW udostępnionych przez portal. GBWI może kontrolować przepływ danych do domeny *low security*. Na poniższym rysunku przedstawiono przykładowy przepływ danych.



Rys. 3. Przykład bezpiecznego udostępniania dokumentów przez portal WWW w GBWI
(przepływ danych)

Użytkownik z domeny *low security* próbuje uzyskać dostęp do dokumentów zlokalizowanych w domenie *high security* udostępnionych przez portal. Przykład przepływu danych prezentuje kontrolowane udostępnianie dokumentów pomiędzy domenami o różnych poziomach wrażliwości.

1. Użytkownik z domeny *low security* łączy się pod określony adres i port IP do NPS w domenie *low security*.
2. NPS rozpoznaje protokół w oparciu o port i protokół TCP/IP. Przekierowuje ruch do HTTP proxy w domenie *low security*.
3. HTTP proxy w domenie *low security* dokonuje konwersji komunikatu GET na komunikat HTTP/SOAP i przesyła go do XML Guard.
4. XML Guard sprawdza etykiety bezpieczeństwa w komunikacie HTTP/SOAP i sprawdza ustawienia polityki bezpieczeństwa.
5. W przypadku poprawności etykiety przekazuje przetwarzany komunikat do HTTP proxy w domenie *high security*.
6. HTTP proxy w domenie *high security* dokonuje konwersji komunikatu HTTP/SOAP do postaci źródłowej i przesyła go przez NPS do Web portal (HTTP Server) w celu uzyskania dostępu do zasobu.
7. Dokument z HTTP Server jest wysyłany do HTTP proxy w domenie *high security* przez NPS.
8. Proxy sprawdza, czy dokument (każdy dokument) posiada swoje etykiety bezpieczeństwa. Jeżeli nie, proxy wysyła do SLR żądanie o etykietę/etykiety dla dokumentu, który ma być wysłany.
9. Po odebraniu przez proxy etykiet/etykiety bezpieczeństwa konwertuje dokument do postaci komunikatu HTTP/SOAP z odpowiednimi etykietami i przesyła go do XML Guard. Kiedy etykieta bezpieczeństwa nie istnieje, dokument nie może być wysłany do innej domeny zgodnie z polityką bezpieczeństwa.
10. XML Guard sprawdza etykiety bezpieczeństwa dołączone do komunikatu HTTP/SOAP i konfrontuje je z obowiązującą polityką bezpieczeństwa.

11. Kiedy etykieta bezpieczeństwa jest aktualna i ważna XML Guard wysyła komunikat do HTTP proxy w domenie low security.
12. HTTP proxy w domenie low security konwertuje komunikat HTTP/SOAP z powrotem do postaci źródłowej i przesyła go do użytkownika przez NPS.
13. NPS sprawdza, czy dane mogą być przesłane przez GBWI zgodnie z zasadami filtrowania pakietów IP.
14. Dokument/dokumenty wysyłane są z GBWI do użytkownika końcowego.

6. Podsumowanie

W referacie przedstawiono główne założenia i architekturę GBWI. Jest to rozwiązanie bazujące na idei IEG opracowanej przez NATO i realizowanej w chwili obecnej przez różne kraje w postaci własnych rozwiązań. Projekt GBWI jest w chwili opracowywania tego referatu w fazie implementacji i wstępnych testów. Pierwsze planowane testy w zakresie sprawdzenia niektórych mechanizmów i weryfikacji koncepcji przewidziane jest podczas ćwiczeń CWIX 2012.

Bibliografia

- [1] Guidance document on the implementation of gateways for information exchange between NATO and external CIS communities, version 1.21 dated 16th February 2007 AC/322(SC/4) N(2007)0007, MULTI REF.
- [2] W3C recommendation, XML Signature Syntax and Processing (Second Edition), <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/>, June 2008.
- [3] Network Working Group, RFC 3920, Extensible Messaging and Presence Protocol (XMPP): Core, October 2004.
- [4] Network Working Group, RFC 3921, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, October 2004.

WEB PORTAL JAŚMIN

ZINTEGROWANY SYSTEM WSPARCIA DOWODZENIA ORAZ ZOBRAZOWANIA POLA WALKI C4ISR

mgr inż. Henryk KRUSZYŃSKI

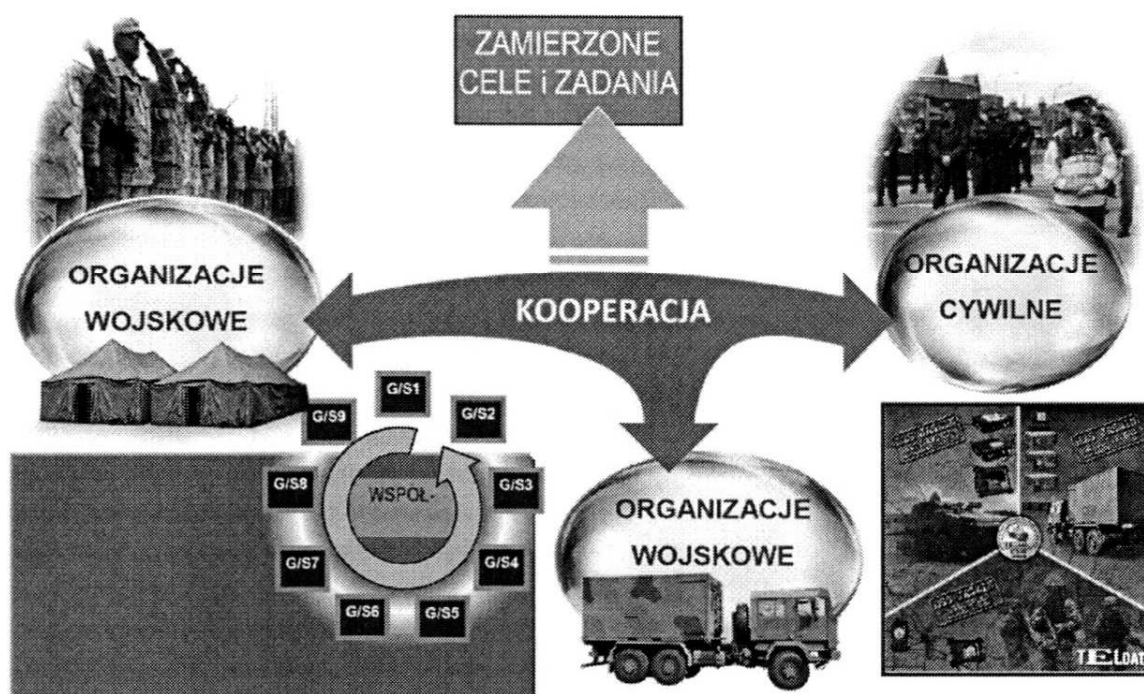
dr inż. Łukasz APIECIONEK

inż. Rafał MOTYLEWSKI

mgr inż. Marek JELIŃSKI

TELDAT Sp. j.

Niezbędnymi elementami w zapewnieniu skutecznej współpracy w ramach sztabu, jak i strukturami dowodzenia wojskowymi oraz organizacjami cywilnymi, jest: pozyskiwanie, gromadzenie i współdzielenie informacji, skuteczna współpraca oraz powszechna świadomość sytuacyjna. Są one istotnie uwzględnione w doktrynach i koncepcjach NATO oraz Unii Europejskiej takich jak: NNEC, EU NEC. Cele tych doktryn można osiągnąć stosując nowoczesne technologie informatyczne.



Obecnie, aby osiągnąć zamierzone cele i wypełnić powierzone zadania zarówno wojskowe jak i cywilne sztaby wymagają nowoczesnej technologii, aby zapewnić skuteczną współpracę w ramach ich organizacji. Ponadto, współpraca cywilno-wojskowa jest niezbędna dowódcy, który „wiąże” działanie jednostek wojskowych z organizmami cywilnymi działającymi na teatrze wojennym.

Szefowi sztabu, odpowiedzialnemu za pracę sztabu dla realizacji misji polegającej na ciągłym dostosowywaniu się do bieżących wymogów pola walki trudno jest w sposób odpowiedni i wiarygodny koordynować podległych mu żołnierzy bez pomocy specjalistycznych narzędzi.



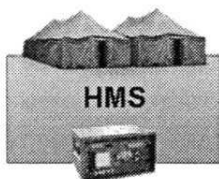
Na szczeblu operacyjnym muszą być użyte niezawodne środki komunikacji w celu zapewnienia szerokopasmowej, cyfrowej łączności bezprzewodowej wraz z połączeniami satelitarnymi między różnymi punktami dowodzenia. W rezultacie, nie będzie problemu z ilością informacji wymienianej między punktami dowodzenia współpracujących ze sobą organizacji. Stąd też, przy pomocy odpowiednio zaprojektowanych systemów informatycznych dowódcy będą mogli skupić się na swoich zadaniach, podejmować trafniejsze decyzje oraz zwiększyć szybkość i skuteczność dowodzenia.

System JAŚMIN składa się z następujących komponentów sprzętowych i programowych:



Wytwarzany jest w 3 wersjach dedykowanych na określony szczebel dowodzenia.

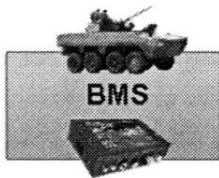
- HMS JAŚMIN – poziom operacyjny i taktyczny – mobilne stanowiska dowodzenia;



HMS JASMINE – (Headquarters Management System). Przeznaczony jest do wykorzystania na stacjonarnych i stacjonarno-polowych stanowiskach i punktach dowodzenia.



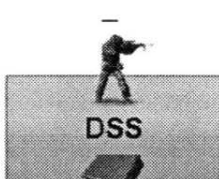
- BMS JASMIN – poziom taktyczny – wozy bojowe;



BMS JASMINE – (Battlefield Management System). Przeznaczony jest do zastosowania w mobilnych systemach dowodzenia na poziomie taktycznym z uwzględnieniem radiowych środków łączności.



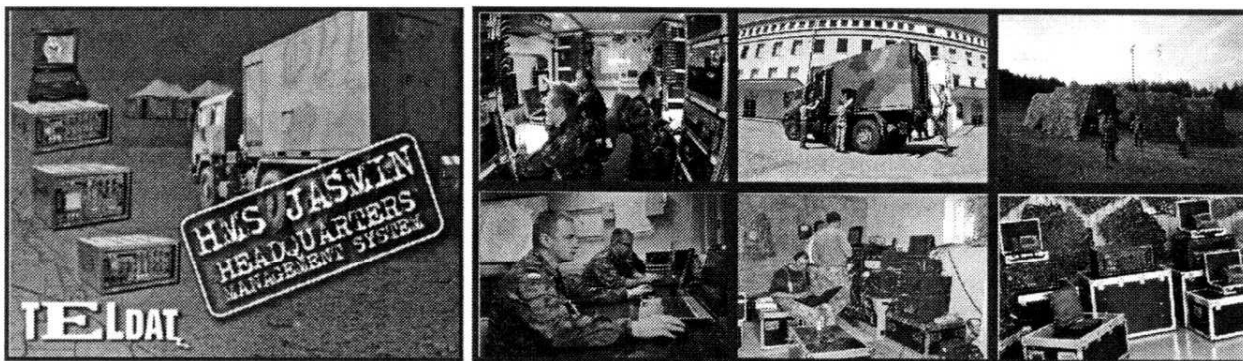
- DSS JASMIN – poziom taktyczny – drużyny oraz pojedynczy żołnierze.



DSS JASMINE – (Dismounted Soldier System). Przeznaczony jest dla żołnierzy działających w ramach zespołów. Zapewnia pełną integrację żołnierzy z ich wyposażeniem oraz systemem BMS JASMINE zainstalowanym w pojazdach bojowych.

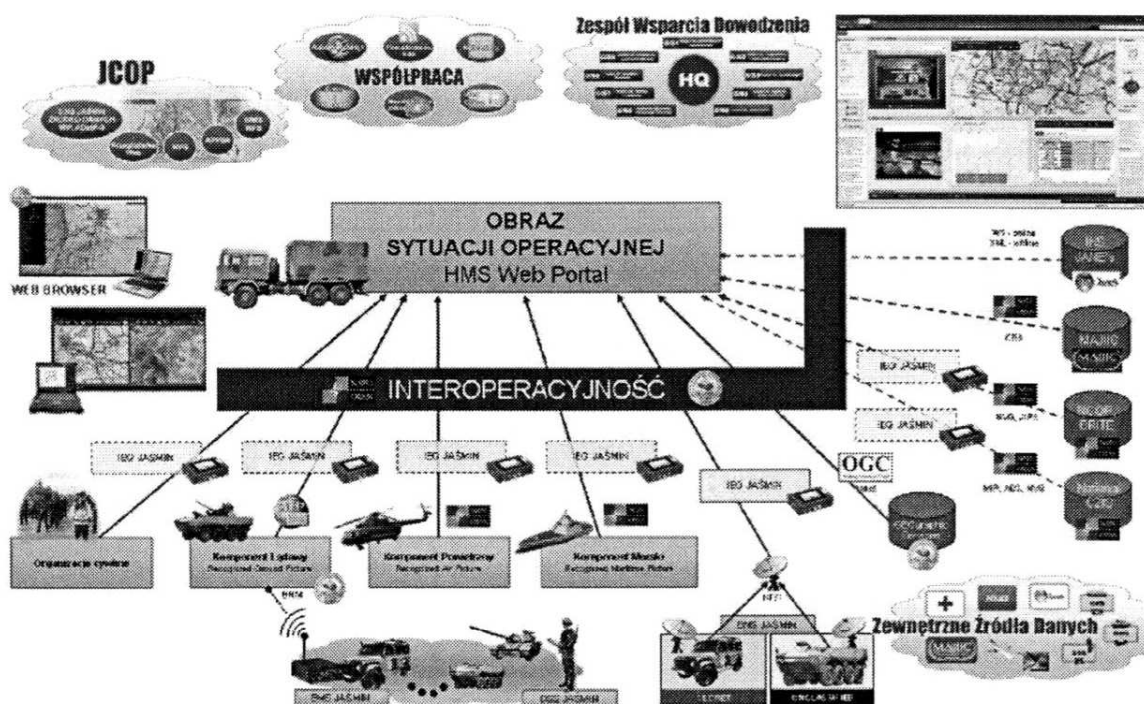


Głównym założeniem Systemu Zarządzania Komponentami (*Modułami*) Bojowymi – HMS JAŚMIN jest usprawnienie pracy dowódców w obrębie sztabu na szczeblu dowodzenia dywizji, brygady i batalionu. Jest to możliwe dzięki portalowi znajdującemu się w lokalnej sieci teleinformatycznej stanowiska/punktu dowodzenia.



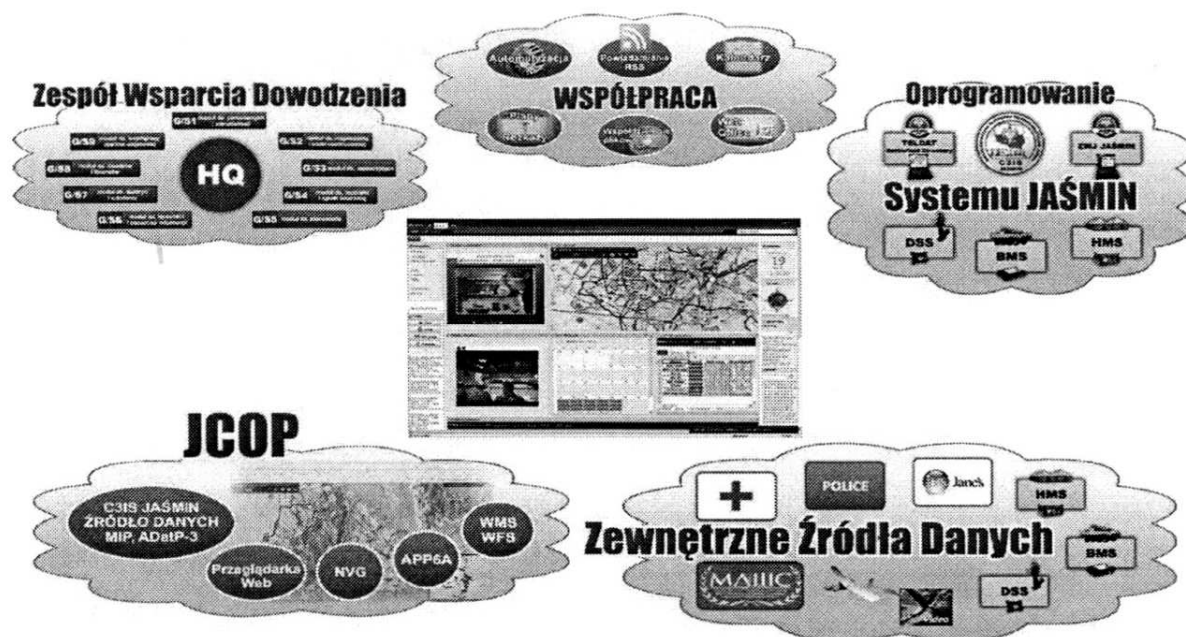
Portal Systemu Wspomagania Dowodzenia powstał z myślą o różnych sekcjach i grupach. Podstawą jego funkcjonalności jest serwer, który pozwala poszczególnym użytkownikom na bezpośredni dostęp do współdzielonych danych i dokumentów generowanych jako pliki (*raporty, plany, rozkazy, powiadomienia, ostrzeżenia, meldunki, itd*).

Poniższa ilustracja całościowo ukazuje wykorzystanie Systemu JAŚMIN wraz z HMS Web Portal:



System Jaśmin wraz z HMS Web Portal:

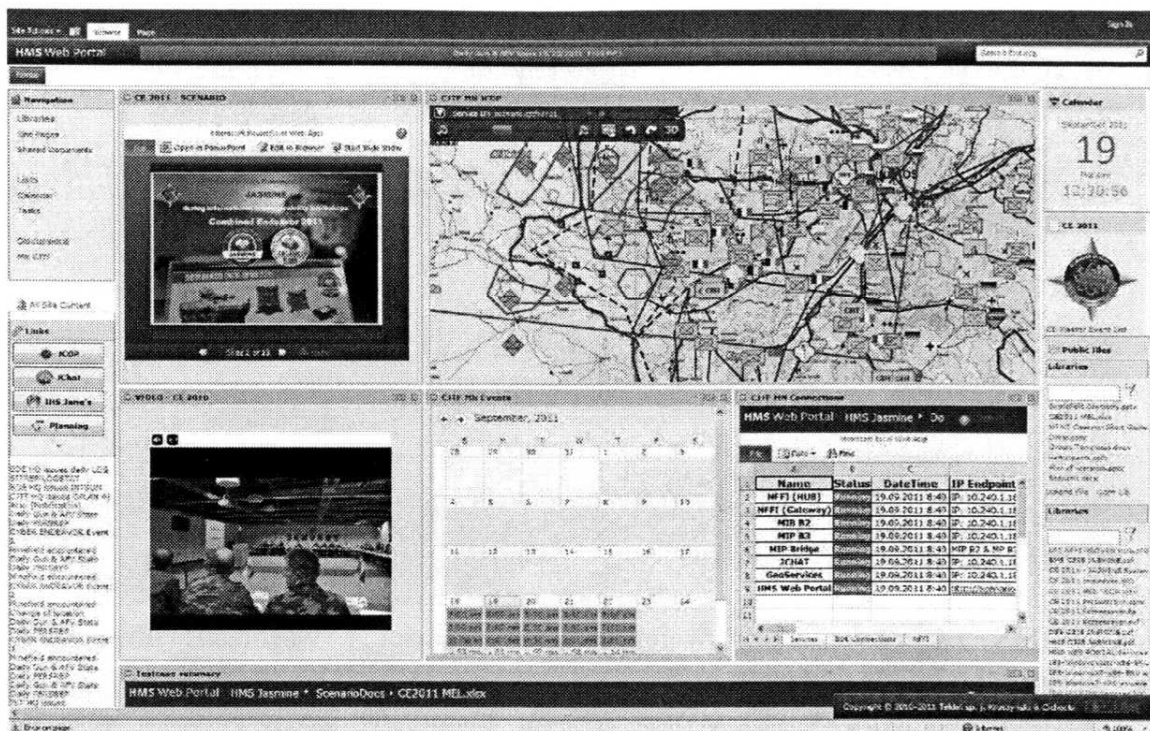
- usprawnia pracę w ramach specjalistycznych grup i sekcji Sztabu Dowodzenia;
- stanowi dostęp do funkcjonalności systemu z poziomu przeglądarki internetowej;
- daje możliwość zbierania informacji z pozostałych komponentów (lądowy, morski, powietrzny) celem utworzenia obrazu sytuacji operacyjnej;
- zapewnia bieżące śledzenie położenia wojsk własnych – jednostki, pojazdy, żołnierze – BFT;
- realizuje współpracę w ramach komponentu lądowego – poziom operacyjny i taktyczny – HMS – BMS – DSS;
- umożliwia współpracę z systemami NATO’wskimi – np.: NCOP, BRITE oraz usługą świadczącą cechy geograficzne (GEOS);
- zapewnia interoperacyjność międzysystemową poprzez Zestaw Usług C3IS JAŚMIN;
- kontroluje przepływ informacji za pomocą IEG JAŚMIN;
- stwarza możliwość natychmiastowej współpracy z organizacjami cywilnymi – obraz sytuacji operacyjnej (*odczyt*), raportowanie (*wprowadzanie*), komunikacja.



System HMS JAŚMIN dzięki swojej wszechstronności i wachlarzu oferowanych funkcjonalności pozwala dowódcy, oraz oficerom sztabu na:

- uzyskanie połączonego obrazu sytuacji operacyjnej z komponentu lądowego, morskiego i powietrznego celem zebrania w jeden spójny obraz danych z RGP (*Recognised Ground Picture*), RMP (*Recognised Maritime Picture*) i RAP (*Recognised Air Picture*);
- wsparcie dla dziewięciu (G/S 1-9) grup/sekcji w ramach sztabu;
- elementy ułatwiające współpracę oraz poszerzające świadomość sytuacyjną, takie jak dostęp do danych z poziomu przeglądarki internetowej, kanały informacyjne, wewnętrzne procesy automatyzacji, kalendarz, powiadomienia, elektroniczny obieg dokumentów, blogi, fora i wiele innych;
- pozyskanie danych z systemów typu BFT (*Blue Force Tracking*);
- stworzenie infrastruktury sieciowej IP z wykorzystaniem usług podstawowych (np.: poczta elektroniczna, VPN, VoIP, DHCP, DNS ...);
- kontrolę przepływu informacji z wykorzystaniem IEG (*Information Exchange Gateway*);
- współpracę z podległymi jednostkami korzystającymi z systemu BMS (*Battlefield Management System*) i DSS (*Dismounted Soldier System*) za pomocą protokołu (*Battlefield Replication Mechanism*) [12] [22];
- pozyskanie i wymianę danych z systemami zewnętrznymi takimi jak MAJIC, IHS Jane's, NCOP, BRITE, systemy narodowe C2IS członków państw NATO;
- współpracę z organizacjami cywilnymi w ramach CiMiC (*Civil Military Cooperation*);
- protokół replikacji danych dedykowany szczególnie dla radiowych łączy szeroko i wąskopasmowych.

HMS Web Portal JAŚMIN jest portalem Systemu HMS JAŚMIN, który powstał z myślą o różnych sekcjach i grupach współpracujących ze sobą w ramach sztabu. Umożliwia on użytkownikom tworzenie wielu dedykowanych podstron, zawierających specjalistyczne Web Party, połączonych z różnymi usługami systemu. Stanowi to podstawę działania stanowiska dowodzenia oraz oficerów funkcyjnych, realizujących powierzone im zadania.

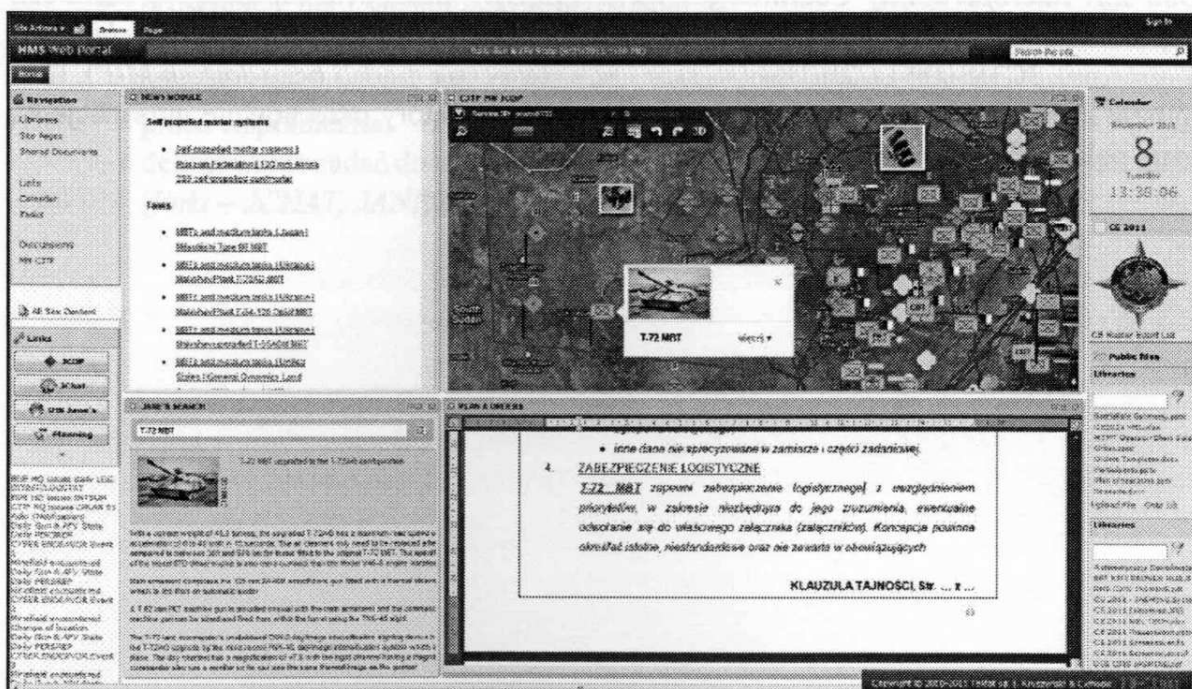
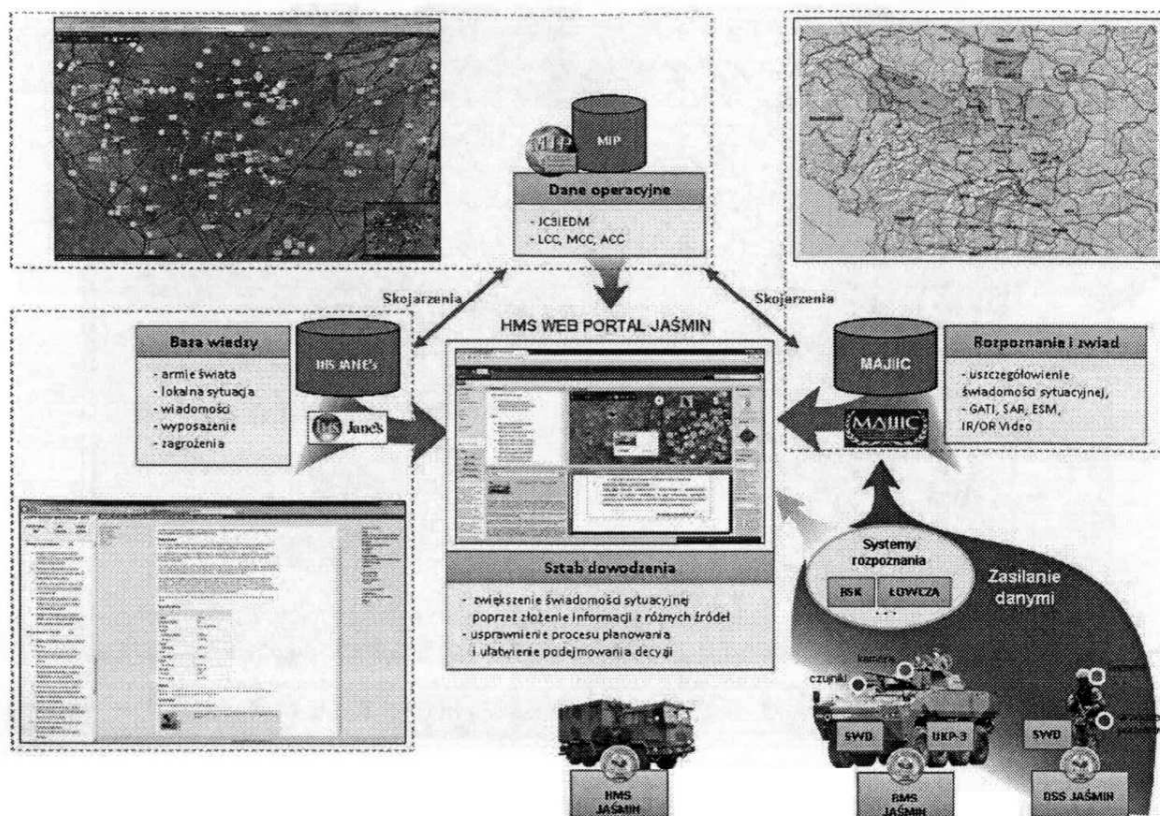


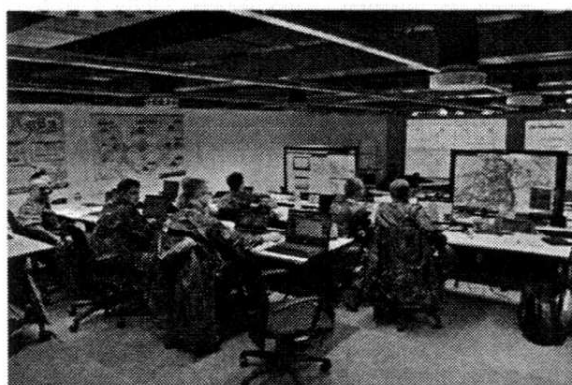
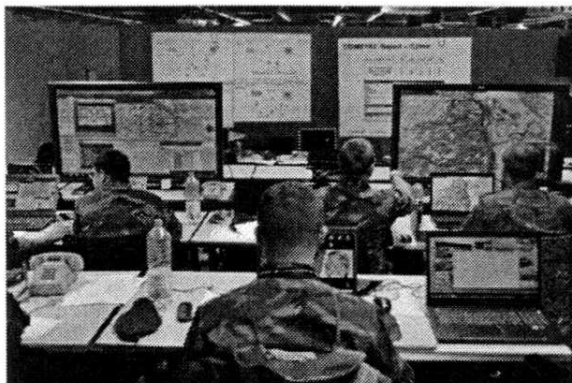
HMS Web Portal - Specjalistyczne Web Party:

- strona niezalogowanego użytkownika;
- specjalizowane widget'y – elastyczna architektura, dwustanowość widget'u (mały i duży);
- specjalizowane podstrony G/S1-9;
- prezentacje ppt uruchamiane w przeglądarce;
- podgląd bieżącej sytuacji – JCOP – filtry obszarowe, tematyczne;
- obsługa dokumentów MS Office (np.: word, xls) bezpośrednio w przeglądarce – praca współbieżna;
- definiowanie zadań do wykonania, obsługa kalendarza, dostęp do innych systemów (*linki – JCHAT, JANE's*) i specjalizowanych podstron (*P&O*).



System portalu HMS WEB Portal JAŚMIN umożliwia wymianę informacji między różnymi rodzajami baz danych, plików i innych formatów oraz na podłączenie różnych źródeł danych. Główne źródła to: baza danych IHS JANE's (baza danych, która przechowuje różnego rodzaju informacje w zależności od warunków geograficznych, pogodowych, np. szczegółowy opis pojazdu opancerzonego), MAJIIC (Multisensor Aerospace-ground Joint ISR Interoperability Coalition), TBD - (TEL DAT Battlefield Directory – dostarcza bezpośrednich usług, logiczny i precyzyjny sposób opisanie wszystkich zasobów ludzkich i hardware), JC3IEDM i C2IEDM (starsze i nowsze wersje modeli bazy danych MIP), IMS (System Zarządzania Informacją) - system bazy danych, który przechowuje informacje na temat pola walki, pliki, zdjęcia, głos i nagranie obrazu.





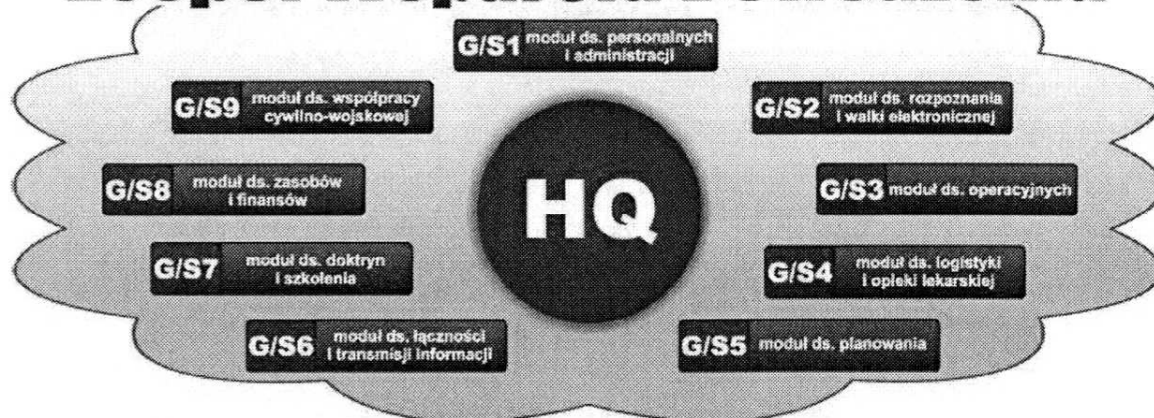
COMBINED ENDEAVOR 2011 i NATO CWIX 2011

Przykład ćwiczeń z wykorzystaniem HMS WEB PORTAL JAŚMIN na Combined Endeavor 2011 i NATO CWIX 2011 w Bydgoszczy – w ramach tych ćwiczeń występowały:

- 2 brygady w ramach komponentu lądowego;
- 8 podległych batalionów;
- HMS WEB PORTAL – umożliwiał współpracę w ramach polskich brygad (12 POL BDE) oraz współdzielenie informacji z innymi brygadami i batalionami bezpośrednio z poziomu przeglądarki internetowej – JCOP, JCHAT, MS OFFICE, P&O.

HMS WEB PORTAL JAŚMIN to system informacyjny, który spełnia wszelkie wymagania dowódców szczebla operacyjnego oraz taktycznego i z powodzeniem może wykorzystywać dane z systemów typu ISR.

Zespół Wsparcia Dowodzenia



Wsparcie dowodzenia jest realizowane poprzez dostarczenie odpowiednich narzędzi dla specjalistów zabezpieczających współpracę sekcji, jednostek i grup sztabu jak i współpracę z organizacjami cywilnymi.

Zobrazowanie pola walki jest możliwe z użyciem komputera z przeglądarką internetową, bez konieczności instalacji dodatkowego oprogramowania. Integracja z różnymi systemami pozwala zbudować obraz sytuacji operacyjnej.

Rozwiązanie może być użyte, jako wsparcie dla operacji ekspedycyjnych NATO lub jednostek bojowych Unii Europejskiej przeznaczonych głównie do użycia w operacjach cywilno-wojskowych, takich jak operacje kryzysowe.