

Bogdan Stachnik

Modernizacja infrastruktury IT w NCIA dla NATO

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii
Obrony Narodowej nr 3(7), 113-122

2013

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach
dozwolonego użytku.

AUTOR

mgr inż. Bogdan Stachnik

Stachnik@gmail.com

MODERNIZACJA INFRASTRUKTURY IT W NCIA DLA NATO

Współcześnie, niezwykle szybko następują zmiany w infrastrukturze teleinformatycznej. Jest to wynik ewolucji rozwiązań technicznych i technologicznych. Wszystkie organizacje i instytucje chcąc zachować konkurencyjność i nowoczesność, starają się nadążyć za rozwojem IT i sprostać wyzwaniom oraz potrzebom przyszłości. Sojusz Północnoatlantycki, rozumiejąc rangę i znaczenie teleinformatyki, dokonuje okresowych analiz i ocen stosowanych rozwiązań, technologii a także nowoczesności technicznej systemów teleinformatycznych przez wyspecjalizowane agendy własne lub powołane do tego doraźnie instytucje zewnętrzne.

W grudniu 2012 roku przedstawiono analizę dokonaną przez niezależne Konsorcjum NCOIC¹ (z ang. *Network Centric Operations Consortium*) oraz NCIA² (z ang. *NATO Communication and Information Agency*) dotyczącą infrastruktury systemów teleinformatycznych³ w NCIA. Analiza ma na celu ocenę wydajności systemów teleinformatycznych, zapewnienie utrzymania określonych standardów bezpieczeństwa oraz efektywniejszego wykorzystania istniejącego sprzętu. Warto zauważyć, że Agencja NCIA jest organizacją, która dostarcza większości usług informatycznych koniecznych do pracy struktur dowództwa NATO. W trakcie analizy określono trzy główne problemy w obecnym obszarze IT:

- brak redundancji⁴ ważnych węzłów;
- limitowana ochrona w razie awarii;
- cyberbezpieczeństwo⁵ w okrojonym stanie.

¹ NCOIC – konsorcjum, które przeprowadziło ocenę IT dla agencji NCIA. Zob., <https://www.ncoic.org/home/>.

² Agencja NCIA utworzona w lipcu 2012 r. z kilku poprzednich agencji NC3A, NCSA, NACMA zajmująca się dostarczaniem usług informatycznych dla struktur NATO. Zob., <http://www.ncia.nato.int>.

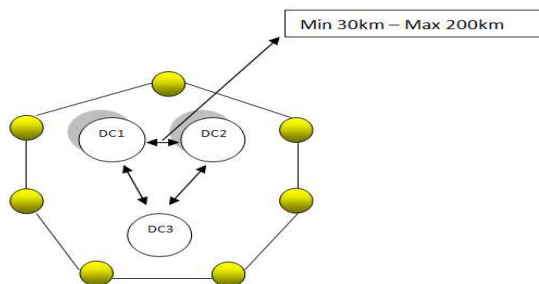
³ System informatyczny jest zbiorem powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. System informatyczny uznaje się zazwyczaj za wyodrębnioną część systemu informacyjnego, w którym do przetwarzania danych zastosowano środki i metody informatyczne, a zwłaszcza sprzęt i oprogramowanie komputerowe. Zob., J. Antczak, *Informatyczne systemy wspomagania zarządzania*, AON Warszawa 2011, s. 149.

⁴ Redundancja w pojęciu dodatkowego składowania danych jako kopii zapasowej.

Wyniki przeprowadzonych analiz wskazują, że istniejąca infrastruktura IT jest trudna do zaakceptowania do dalszego utrzymywania i rozwoju ze względu na liczne mankamenty, a także nie spełnia wymagań stawianych obecnym i przyszłym operacjom wojskowym prowadzonym przez państwa sojuszu Północnoatlantyckiego. Warto wymienić tutaj kilka kluczowych czynników powodujących niedomagania systemów. W obecnej sytuacji są to:

- 30 centrów IT w różnych lokalizacjach;
- 2582 serwerów różnych firm – 250 typów;
- 1400 osób do obsługi;
- różnorodność oprogramowania, brak rozwiązań *enterprise*⁶;
- wykorzystanie mocy obliczeniowej sprzętu na poziomie 10% (max 30%);
- obciążenie sieci telekomunikacyjnych na poziomie 7%.

Taki stan rzeczy przyczynił się do opracowania nowego planu, który obejmuje utrzymanie trzech głównych centrów IT do świadczenia usług teleinformatycznych oraz od siedmiu do dziesięciu mniejszych węzłów do utrzymania istniejących elementów dowodzenia w strukturach NATO (rys. 1.). Liczba węzłów wraz z ich lokalizacją zostanie ostatecznie zatwierdzona w pierwszym półroczu 2013. W analizie przedstawiono również kluczowe założenie nowego systemu teleinformatycznego, w którym występują kontrolery domen DC1⁷, DC2, DC3. Ważnym elementem jest, aby dwa węzły DC1 oraz DC2 nie były oddalone od siebie dalej niż 200 km i nie bliżej jak 30 km w celu zapewnienia wydajnej replikacji najważniejszych danych.



Źródło: opracowanie własne.

Rys. 1. Ogólna idea przyszłego rozlokowania głównych węzłów teleinformatycznych w NCIA 2013

⁵ Ochrona zasobów w cyberprzestrzeni. Zob., http://en.wikipedia.org/wiki/Proactive_Cyber_Defence.

⁶ Przedsiębiorstwo jak całość (np. licencjonowanie oprogramowania w sposób wielo-stanowiskowy).

⁷ DC1 – kontroler domeny (z ang. *Domain Controller*).
Zob., [http://technet.microsoft.com/en-us/library/cc786438\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786438(v=ws.10).aspx).

Jednocześnie takie rozwiązanie stwarza możliwość zabezpieczenia kopii najważniejszych informacji w dwóch lub wielu różnych miejscach w razie awarii lub zagrożeń spowodowanych np. działaniami militarnymi (z ang. *disaster recovery*⁸). Węzły DC1 i DC2 mają mieć lokalizację w północnej części Europy i nie zostało jeszcze określone ich docelowe miejsce. Węzeł DC3 będzie zlokalizowany w miejscowości Lago Patria (Neapol we Włoszech). Równocześnie nowy plan obejmuje redukcję personelu z 1400 osób do 800 osób. Taka reorganizacja pozwoli na wydajniejszy system informacyjny⁹ dla nowych obszarów zadań. Kolejnym planowanym rozwiązaniem jest zastosowanie przetwarzania w chmurze¹⁰ (z ang. *cloud computing*) przy użyciu 40 lub 80 serwerów na węzeł, w zależności od potrzeb na moc obliczeniową (przydzielaną dynamicznie¹¹) do zapewnienia realizacji nowych zadań.

Dla zapewnienia separacji sieci o różnej klasyfikacji NCIOC proponuje rozdzielenie sprzętowe i aplikacyjne sieci komputerowych przy zastosowaniu dla sieci klasyfikowanych urządzeń kryptograficznych. Możliwym rozwiązaniem jest też podniesienie klauzuli istniejącej jawnej sieci komputerowej-NU (z ang. *NATO Unclassified*) do wyższej klauzuli, np. zastrzeżonej-NR (z ang. *NATO Restricted*) w przypadku spełnienia określonych wymogów bezpieczeństwa, narzuconych przez dokumenty normatywne NATO. Podobne rozwiązanie zostało zaproponowane przez agencję NCIA, gdzie przedstawiono użycie technologii wirtualnych routerów¹² i ścian ogniowych¹³, za pomocą których odseparowano by części sieci jawnej od klasyfikowanej. Takie rozwiązanie pozwala na kontrolowaną wymianę danych pomiędzy sieciami przy spełnieniu zasad właściwej ochrony danych. Największą zaletą jest porzucenie idei dublowania sprzętu przy wykorzystaniu elementów bram¹⁴. Dzisiejsze zawansowane technologie użyte w urządze-

⁸ Zabezpieczenie szybkiego odzyskania danych, przywrócenia infrastruktury teleinformatycznej w oparciu o uprzednio przygotowany plan na wypadek awarii. Zob., <http://www.computerbusinessresearch.com/Home/enterprise-architecture/disaster-recovery>.

⁹ Wielopoziomowa struktura, która pozwala użytkownikowi danego systemu na transzormowanie określonych informacji wejścia na pożądaną informację wyjścia za pomocą odpowiednich procedur i modelu. Zob., J. Antczak, *Informatyczne...*, wyd. cyt., s. 149.

¹⁰ Zob., http://en.wikipedia.org/wiki/Cloud_computing.

¹¹ Wirtualizacja (rozwiązania z użyciem technologii wirtualizacji np. firm VMware lub Microsoft Hyper-V) pozwala na przydzielenie mocy obliczeniowej automatycznie lub manualnie w zależności od potrzeb.

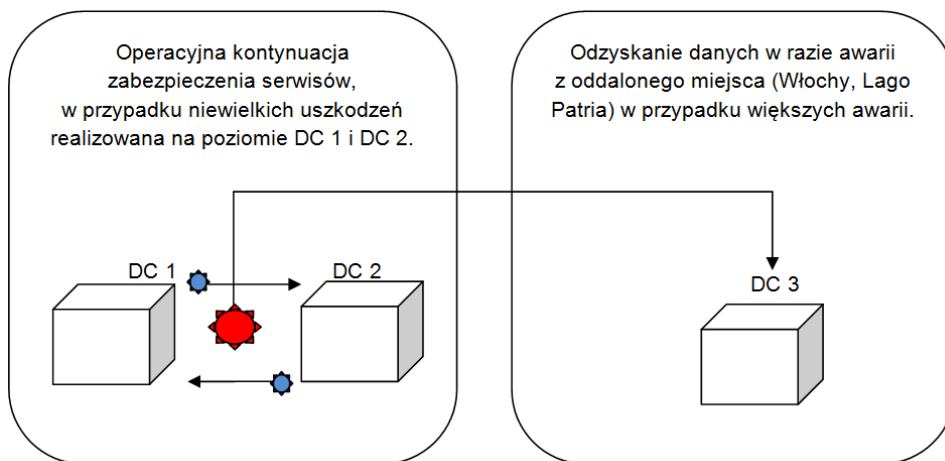
¹² Router to urządzenie służące do łączenia różnych sieci komputerowych.

¹³ Ściana ogniowa (z ang. *firewall*), termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepożądany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wpływem danych z sieci lokalnej na zewnątrz.

¹⁴ Urządzenia lub aplikacje nadzorujące przepływ danych pomiędzy systemami teleinformatycznymi.

niach takich firm jak CISCO lub Alcatel pozwalają na tworzenie tego typu rozwiązań. Jednak ciągle kwestią sporną pozostaje sfera zapewnienia bezpieczeństwa przepływu i wymiany danych pomiędzy sieciami. Sprawa wyboru ostatecznego rozwiązania pozostaje jeszcze nierozstrzygnięta wewnątrz agencji NCIA.

Kolejnym unowocześnieniem jest stworzenie scentralizowanego wsparcia serwisowego dla wszystkich usług teleinformatycznych świadczonych przez agencję NCIA. Projekt ma na celu redukcję personelu i wprowadzenie rejestracji wszelkiego typu incydentów oraz zgłaszanie potrzeb dla istniejących lub nowych usług (katalog usług NCIA) w oparciu o system zarządzany z jednego centralnego miejsca w Europie. Tego typu założenie opiera się na możliwości zdalnej pomocy technicznej wszystkim użytkownikom, niezależnie od lokalizacji. Dzisiejsze rozwiązania techniczne systemów operacyjnych pozwalają na realizację tego typu usług przy zachowaniu kontrolowanego, bezpiecznego dostępu do wszystkich komputerów w strukturach NATO. Wzięto także pod uwagę stworzenie zapasowego punktu obsługi klienta ze względu na potencjalne awarie głównego systemu, co odzwierciedla idea stworzenia punktów zapasowych DC 2 i DC 3.



Źródło: opracowanie własne.

Rys. 2. Zabezpieczenie węzłów teleinformatycznych w przypadku awarii

W zakresie rozwiązań dla urządzeń końcowych – stacji roboczych (komputerów stacjonarnych) zarówno agencja NCIA, jak i konsorcjum NCIOC proponuje użytkowanie stacji roboczych typu desktop¹⁵ lub laptop¹⁶.

¹⁵ W popularnym znaczeniu stacja robocza to każdy komputer przeznaczony do bezpośredniej pracy (w odróżnieniu od serwera, który tylko udostępnia jakieś usługi). W szczególności w sieciach komputerowych mianem tym określa się każdy komputer, który

Wykorzystanie takiego rodzaju stacji pozwala na możliwości użycia pojedynczych komputerów niezależnie od jakichkolwiek problemów z siecią komputerową lub w wypadku przetwarzania danych w oparciu o model klient serwer¹⁷. Wzięto także pod uwagę wykorzystanie technologii VDI¹⁸, ale tylko dla wybranych lokalizacji. W szczególności tego typu rozwiązanie polecane jest dla lokalizacji stacjonarnych, gdzie przetwarzanie danych realizowane w jednym miejscu bez konieczności korzystania z zasobów zdalnych. Istotnym elementem jest posiadanie lub implementacja niezawodnej, wysoce przepustowej¹⁹, infrastruktury sieci komputerowej. Infrastruktura VDI bazuje na przetwarzaniu w chmurze. Wszelkiego rodzaju problemy w tym rozwiązaniu skupiają się na technologii wyświetlania danych na urządzeniu końcowym typu desktop – gruby klient²⁰, cienki klient²¹ lub zero klient²². Redukcja typów serwerów do dziesięciu umożliwi wydajniejsze zabezpieczenie wsparcia technicznego całego sprzętu. Zcentralizowany automatyczny system zarządzania w trzech centrach ze zintegrowanym NETOPS²³ i ochroną cybernetyczną (z ang. *Cyber Defence*) pozwo-

jest do tej sieci podłączony, a który nie służy wyłącznie do jej obsługi. Pokrywa się to z grubsza z terminem komputer osobisty.

¹⁶ Komputer przenośny, małych rozmiarów.

¹⁷ W informatyce – program komputerowy występujący w roli klienta wobec usług dostarczanych przez serwer. W znaczeniu potocznym, mianem *klienta* określa się również komputer lub hosta, na którym działa program w roli klienta. W konwencji nazw stosowanej dla programów z rodziny XFree86, *klientem* nazywa się maszynę, która stanowi źródło danych pobieranych przez serwer.

¹⁸ Wirtualna Stacja Robocza – VDI (z ang. *Virtual Desktop Infrastructure*) umożliwiająca wyświetlanie wyniku operacji przetwarzania danych z centrum przetwarzania (z ang. *Data Centre*) technika podobna do użycia starych terminali.

¹⁹ Przepustowość (pojemność kanału, ang. *throughput*) w telekomunikacji i informatyce – maksymalna ilość informacji (mierzonej w bitach), jaka może być przesyłana przez dany kanał telekomunikacyjny lub łącze w jednostce czasu (mierzonej w sekundach). Czasem potocznie nazywana jest błędnie *szybkością* (np. sieci komputerowej), ale ponieważ mówi o maksymalnej liczbie bitów w jednostce czasu, a nie zmianie fizycznego położenia w czasie, należy rozróżniać te pojęcia. Przepustowość mierzy się w bitach na sekundę (b/s – ang. *bits per second*) lub bajtach na sekundę (B/s, 8 b/s = 1 B/s) i ich krotnościach: kb/s, Mb/s, Gb/s, KB/s, MB/s itd. W praktyce spotykane są zarówno prefiksy dziesiętne (k = 1000, M = 1 000 000), jak i binarne (k = 1024, M = 1 048 576). Ze względu na tę samą jednostkę, przepustowość jest potocznie mylnie utożsamiana z przepływnością. Przepływność jest miarą natężenia strumienia informacji (danych), podczas gdy przepustowość jest cechą toru lub kanału telekomunikacyjnego.

²⁰ Rodzaj stacji roboczej, która może przetwarzać dane samodzielnie, niezależnie od innych urządzeń i aplikacji.

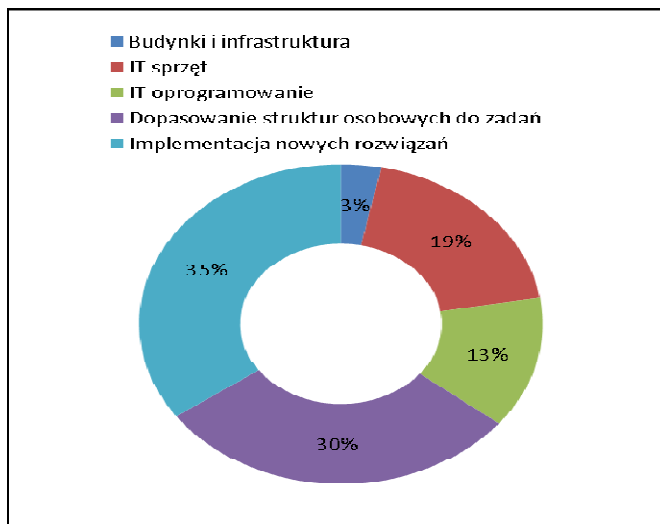
²¹ Rodzaj terminala/stacji roboczej, która posiada niewielkich rozmiarów aplikację umożliwiającą wyświetlanie wyniku przetwarzania danych w chmurze.

²² Monitor wraz ze zintegrowanym układem elektronicznym posiadającym aplikację umożliwiającą pobranie danych z określonego systemu teleinformatycznego.

²³ NetOps jest zdefiniowany jako rama operacyjna składająca się z trzech zasadniczych zadań, świadomości sytuacyjnej, dowodzenia i kontroli w oparciu o systemy teleinformatyczne oraz dowództwa jako organizacji. Te elementy razem zapewniają

li na dostarczenie właściwej informacji we właściwym czasie dla właściwych osób.

Konsorcjum NCOIC oszacowało wstępne koszty reorganizacji oraz długoterminowe plany przynoszące oszczędności z tytułu zmian. Roczne koszty utrzymania nowej organizacji spadną o połowę w kolejnych latach, w większości spowodowane będą redukcją etatów z 1400 do 800 w agencji NCIA. Na kolejnych rysunkach przedstawiono podział wydatków w przyszłości w oparciu o analizę NCIOC (rys. 3.) i NCIA (rys. 4.).

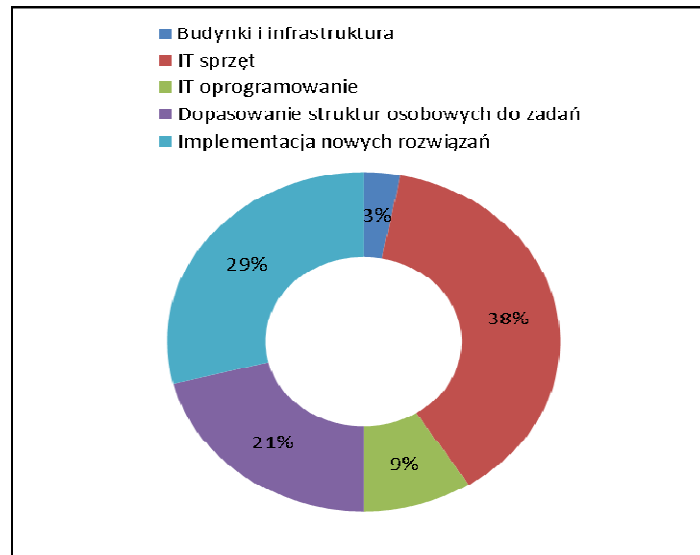


Źródło: prezentacja z NCIA grudzień 2012.

Rys. 3. Wydatkowanie budżetu przez agencję NCI w przyszłości (podejście NCOIC)

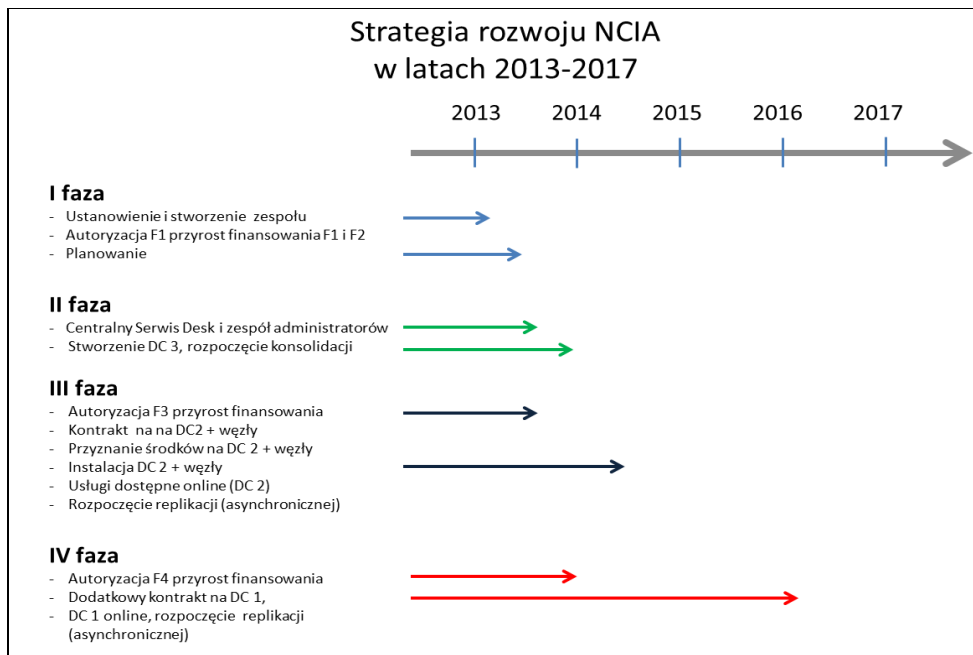
Nowe założenia finansowe powinny pokrywać wszelkie koszty modernizacji i zmian w kolejnych latach, pozwalając uzyskać środki finansowe z planowanych oszczędności. Takie uwarunkowanie poprawi, usprawni, a przede wszystkim wdroży nowy model zarządzania informacją w strukturach NATO. Przedstawiony plan ma na celu przygotowanie infrastruktury IT tak, aby mogła ona sprostać w nadchodzących latach wymogom prowadzenia wszelkiego rodzaju działalności struktur NATO.

przewagę informacyjną a zarazem powodzenie w operacjach. Zob. <http://en.wikipedia.org/wiki/NetOps>.



Źródło: prezentacja z NCIA grudzień 2012.

Rys. 4. Wydatkowanie budżetu przez agencję NCI w przyszłości (podejście NCIA)



Źródło: opracowanie własne.

Rys. 4. Strategia rozwoju NCIA w latach 2013-2017

Zatwierdzona strategia nowej agencji NCIA obejmuje 4 fazy rozwoju (rys. 5.):

- 1) planowanie, reorganizacja, nowa struktura zespołu;
- 2) optymalizacja, centralny service desk, podział obszarów pracy/wpływów dla specjalistów;
- 3) konsolidacja, instalacja, nowe usługi w porfolio agencji, replikacja węzłów;
- 4) kontrakt na nowy węzeł DC1, zakończenie wcześniejszych faz, ocena, wnioski.

Proces zmian został już uruchomiony i jest realizowany w NCIA. Dokonano już planowych modyfikacji wynikających z fazy pierwszej w całej organizacji. Agencja wzięła pod uwagę rzeczową ocenę konsorcjum NCOIC i własne analizy, co owocuje szybkimi zmianami w jej strukturze. Warto wskazać na wprowadzanie licznych poprawek do istniejących projektów i tempo postępu prac w obszarze centralizacji usług, zastosowania jednego standardu w przypadku dostarczania różnych serwisów dla odbiorców. Ważnym i najmniej zdefiniowanym obszarem pozostaje użytkowanie dedykowanego oprogramowania – FAS (z ang. *Functional Area Services*) na potrzeby Sojuszu. Kwestia ta będzie jeszcze wielokrotnie poruszana w trakcie dalszych prac na spotkaniach i konferencjach NATO. Celem jest ustalenie listy oprogramowania wspomagającego różne procesy (np. podejmowania decyzji na polu walki).

Wnioski

Plan rozwoju agencji NCIA poprzez trzy założone fazy, tj. konsolidację, racjonalizację, optymalizację został zaaprobowany zaraz po utworzeniu NCIA 2012 roku. Rzeczowa analiza niezależnego konsorcjum NCOIC oraz agencji w grudniu tego samego roku wpłynęła na postęp prac nad wdrożeniem najważniejszych filarów nowej organizacji, tj. trzech węzłów bazowych oraz do dziesięciu węzłów mniejszego znaczenia, których zadaniem będzie zabezpieczenie świadczenia szeregu usług teleinformatycznych w rozmieszczonych ośrodkach, na terenie różnych państw, wchodzących w skład sojuszu. Warto zauważyć, że poprzedni plan utworzenia wielonarodowej sieci komputerowej (z ang. *Federal Multinational Network*) został podtrzymany i zmodyfikowany na potrzeby NATO. Podłączenie kolejnych narodowych węzłów teleinformatycznych państw członkowskich, odbywać się będzie poprzez rozwiązania na bazie różnego rodzaju mechanizmów (urządzenia lub rozwiązania programowe lub ich połączenie jako całość, z ang. *cross domain, gateway, diods, virtual router*) separujących ruch tylko w danym kierunku lub pozwalających na ruch w obie strony przy wybranych usługach z zakresu usług teleinformatycznych. To rozwiązanie pozwoli na

dzielenie się aktualną informacją w domenie NATO. Standardy dostępu do poszczególnych usług zostały określone w procedurach (z ang. *SOP, Standard Operation Procedures*) obowiązujących we wszystkich krajach członkowskich NATO. Aktualizacja procedur w czasie roku kalendarzowego pozwala na bieżące podążanie za rozwojem technologicznym między innymi w dziedzinie informatyki oraz dostosowaniu wymogów zabezpieczenia coraz to nowych usług związanych z bieżącymi konfliktami oraz wydarzeniami na świecie.

Bibliografia

1. Analiza Konsorcjum NCOIC przedstawiona w grudniu 2012 roku dla NCIA.
2. Analiza NCIA przedstawiona Głównemu Menadżerowi agencji NCIA.
3. <http://www.microsoft.com/pl-pl/server-cloud/ws2012/default.aspx>.
4. <http://www.ncia.nato.int>.
5. <http://www.vmware.com/solutions/>.
6. <https://www.ncoic.org/technology/activities/neer/>.
7. Umowa Świadczenia Usług teleinformatycznych pomiędzy instytucjami NATO a agencją NCIA – SLA (z ang. *Service Level Agreement*).
8. Wybrane opracowania oraz prezentacje dotyczące przekształceń agencji NCIA z sieci jawnej-NU (z ang. *NATO UNCLASSIFIED*).

IT INFRASTRUCTURE MODERNIZATION IN NCIA FOR NATO

Abstract: The article presents the latest development strategy of NATO Communication and Information Agency (NCIA) for 2013 – 2017 devised in order to provide the optimum Information and Communication Technology (ICT) systems' efficiency, rapid access to a wide range of information maintaining its proper protection and its fast authorized access in different parts of the world. The Joint Force Training Centre (JFTC) in Bydgoszcz has been conducting tasks basing on ICT systems provided by NCIA since 2009. Materials gathered by JFTC and NCIS present the problems of the Agency's reorganization which allows looking into in the future of planning, creating, modifying and developing of new ICT systems. At the same time, the article highlights an endless process of systems' improvement and development as well as the organization of people in teams that plan, implement, monitor and maintain the entire IT infrastructure presented.

Moreover, new tendencies in the use of cloud computing as well as developments regarding processing, storing and transmitting data basing on modern ICT hubs for NATO needs have been presented in a synthetic way.