Maciej Marczyk

Wojskowe sieci teleinformatyczne na potrzeby kierowania reagowaniem kryzysowym

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 3, 61-70

2013

Maciej MARCZYK
Akademia Obrony Narodowej

WOJSKOWE SIECI TELEINFORMATYCZNE NA POTRZEBY KIEROWANIA REAGOWANIEM KRYZYSOWYM

Wstęp

Rozwój ekonomiczny świata, globalizacja i postęp techniczny szczególnie w dziedzinie informatyzacji większości obszarów funkcjonowania człowieka powoduje znaczny wzrost zagrożeń dla niego samego i otaczającej go rzeczywistości. Jest to związane m. in. z powszechnym używaniem materiałów i środków zawierających substancje niebezpieczne dla zdrowia i życia ludzkiego, czy też z wymianą i bezpieczeństwem informacji ważnych dla danej społeczności, narodu czy państwa.

Coraz bardziej zauważalne są zaburzenia klimatu powodowane m.in. zjawiskiem globalnego ocieplenia. Gwałtowne zjawiska przyrodnicze takie jak ulewy i huragany stwarzają zagrożenia dla ludzi i infrastruktury aglomeracji miejskich.[1] Gwałtowny wzrost liczby ludności, zwiększenie populacji mieszkającej w miastach oraz uzależnienie ludzi w nich żyjących od dostaw wody, żywności i energii stwarza poważne zagrożenie związane z ewentualnymi awariami infrastruktury technicznej. Duże uzależnienie gospodarki światowej od systemów teleinformatycznych sprzyja działaniom hakerskim czy cyberterrorystycznym.

Należy jednocześnie zauważyć, że wraz z rozwojem cywilizacyjnym nastąpił szybki rozwój narzędzi i technologii wspomagających człowieka w walce z zagrożeniami. Było to szczególnie widoczne w ostatnich latach XX wieku oraz na początku nowego stulecia, w którym to okresie nastąpił szybki rozwój technologii informatycznych, w tym teleinformatycznych systemów wspomagania zarządzania i dowodzenia. Posiadanie i wykorzystanie odpowiednich narzędzi, zdolnych do przechowywania, przetwarzania i przesyłania danych daje nowe możliwości i wprowadza w każdą działalność człowieka nową jakość. Ich wykorzystanie w zarządzaniu kryzysowym przyczyni się do niwelowania skutków potencjalnych zagrożeń i katastrof i bezpieczeństwa infrastruktury krytycznej państwa.

Należy przypuszczać, że siły zbrojne, a w dużej mierze wojska lądowe będą miały znaczący udział w zapobieganiu skutkom różnego rodzaju katastrof. Będą one ważnym ogniwem realizującym proces kierowania reagowaniem kryzysowym. Z tego względu muszą być zdolne do realizacji wybranych etapów reagowania kryzysowego przy jednoczesnej możliwości współpracy z organami rządowymi i samorządowymi państwa. Z powyższego wynika, że należy podjąć kroki zmierzające do określenia przydatności posiadanych przez wojska lądowe systemów i sieci teleinformatycznych w zakresie kierowania reagowaniem kryzysowym, a także określenie możliwości wykorzystania publicznych systemów i technologii w zakresie transmisji danych i mowy.

[1] Np. huragany tsunami w USA i w Japonii.

Wojskowe sieci teleinformatyczne w zarządzaniu kryzysowym

Koncepcja organizacji łączności na potrzeby zarządzania kryzysowego powinna opierać się na założeniach związanych z uniezależnieniem się od warunków środowiskowych prowadzonych operacji kryzysowych. Można wykorzystywać infrastrukturę teleinformatyczną w obszarze działania, jednakże należy liczyć się z jej awaryjnością lub niedostępnością w wyniku uszkodzeń, jakie zostały dokonane w toku wcześniejszych działań. Podstawowym elementem, jaki należałoby zagwarantować, jest doprowadzenie do wdrożenia mechanizmów umożliwiających tworzenie i udostępnianie pełnego zobrazowania sytuacji obszaru operacji i realizacji nowoczesnych usług łączności i informatyki. Takie rozwiązanie pozwoli stworzyć sieć teleinformatyczną, charakteryzującą się szybkością wymiany informacji (danych) i jednocześnie umożliwiającą łatwe określenie autora i odbiorcy informacji.

Nowoczesną sieć teleinformatyczną powinna charakteryzować: globalizacja, interoperacyjność, ekonomiczność oraz łatwość zarządzania i obsługi.

Usługi w sieci teleinformatycznej powinny obejmować:

- stałą obserwację sytuacji na obszarze objętym kryzysem;
- możliwość stałej wymiany informacji;
- wymianę poczty elektronicznej;
- dostępność usług sieciowych oraz serwisu informacyjnego;
- możliwość komunikacji poprzez komunikatory;
- VoIP (ang. *Voice Over Internet Protocol*) technologię, której głównym założeniem jest integracja ruchu telefonicznego z transmisją danych.

Ze względu na znaczne zapotrzebowanie osób funkcyjnych w zarządzaniu kryzysowym na przesyłanie dużych ilości informacji, podstawową osnową rozległych sieci teleinformatycznych w procesie kierowania (wojskowej sieci szkieletowej) będzie sieć radioliniowa uzupełniana siecią kablową i siecią satelitarną. Sieci te powinny być przypisane do obszaru działań (obszaru realizacji zadań przez komponent wojskowy), a nie do poziomu na jakim występują. Głównym zadaniem sieci wojskowych będzie zapewnienie odpowiedniego poziomu usług teleinformatycznych wszystkim organom kierowania (decyzyjnym) realizującym swoje zdania w obszarze, na którym sieć szkieletowa jest rozwinięta oraz przechowywanie i udostępnianie informacji uprawnionym organom kierowania.

Następnym komponentem rozległych sieci teleinformatycznych, zapewniającym łączność w ruchu na dużych odległościach, ale o mniejszych możliwościach transmisyjnych, są sieci radiowe KF i UKF budowane przy zastosowaniu radiostacji krótkofalowych i ultrakrótkofalowych. Sieci radiowe UKF i KF będą wykorzystywane na zasadach aktualnie obowiązujących w celu zapewnienia łączności dublującej oraz transmisji ograniczonych ilości danych na potrzeby systemów zarządzania polem walki. Sieci radiowe UKF i KF stanowią sprawdzone i niezawodne sposób wymiany informacji, jednakże charakteryzują się ograniczoną przepustowością i małą ilością świadczonych usług teleinformatycznych. Przy dużej ilości posiadanych na wyposażeniu komponentu wojskowego radiostacji UKF i KF rezygnacja z tego środka łączności wydaje się niecelowa.

Badania wykazały, że oddzielnym komponentem sieci teleinformatycznych organizowanych na potrzeby procesu zarządzania kryzysowego będą lokalne sieci teleinformatyczne pododdziałów wykorzystujące szerokopasmowe sieci radiowe pracujące w trybie ad hoc, sieci radiowe pakietowe oraz sieci radiodostępowe (radiowe).

Ostatnim elementem sieci teleinformatycznych będą lokalne sieci teleinformatyczne stanowisk dowodzenia (SD) i punktów kierowania (PK). Sieci te mogą być tworzone zarówno w oparciu o środki kablowe (sieci kablowe), jak również środki radiowe (sieci radiowe szerokopasmowe o ograniczonej mocy oraz radiodostępowe pracujące w oparciu o protokoły rodziny 802.11).

Elementy składowe wojskowych sieci teleinformatycznych organizowanych na potrzeby kierowania w operacji kryzysowej przedstawiono na rysunkach 1 i 2.

W strukturze wojskowych sieci teleinformatycznych dla potrzeb zabezpieczenia relacji kierowania operacją powinny funkcjonować następujące elementy:

- węzły teleinformatyczne: sieciowe, dostępowe i stanowisk dowodzenia (PK);
- linie teletransmisyjne: międzywęzłowe, dowiązania, bezpośrednie i abonenckie.

Osiągnięcie takiego stanu sieci teleinformatycznych, jakiego wymagają współczesne uwarunkowania, będzie możliwe dzięki właściwej organizacji i zastosowaniu nowoczesnych, zaawansowanych technologicznie urządzeń. Współczesne sieci teleinformatyczne powinny mieć strukturę wieloboczną, którą tworzą węzły teleinformatyczne sieciowe odpowiednio rozlokowane względem elementów ugrupowania bojowego i połączone między sobą liniami teletransmisyjnymi o dużej przepływności, węzły teleinformatyczne dostępowe zapewniające dostęp do sieci szkieletowej sieciom teleinformatycznym pododdziałów i sieciom teleinformatycznym stanowisk dowodzenia oraz węzły teleinformatyczne stanowisk dowodzenia.[2]

Z praktyki działania elementów wsparcia dowodzenia wynika, iż w czasie pokoju wykorzystywane są usługi teleinformatyczne świadczone przez węzły łączności stacjonarnego systemu łączności SZ RP (CWT SZ RP, RWT, WŁ). Natomiast w okresie kryzysu i wojny,[3] pododdziały łączności i informatyki będą rozwijały mobilne węzły teleinformatyczne. Sytuacja kryzysowa powoduje użycie wszystkich możliwych sposobów dla wzmocnienia wojskowych sieci teleinformatycznych, czyli także realizację zadań przez stacjonarne oraz mobilne elementy wojskowego systemu łączności.

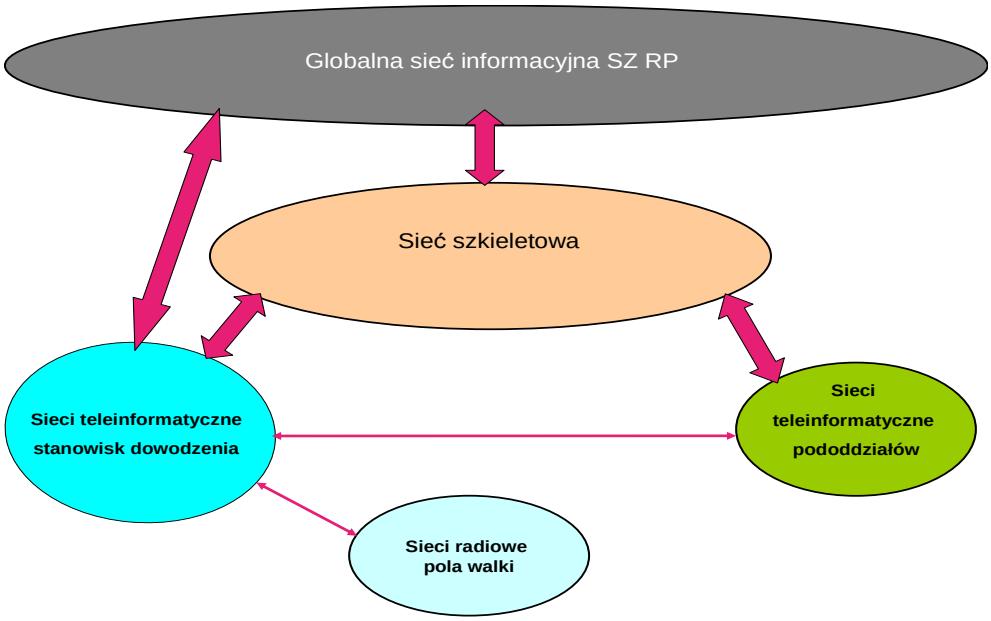
W strukturze techniczno - funkcjonalnej wojskowej sieci teleinformatycznej organizowanej na potrzeby procesu zarządzania kryzysowego będą występowały różne rodzaje linii teletransmisyjnych: linie międzywęzłowe, bezpośrednie, dowiązania oraz abonenckie.

---

[2] Zob. P. Dela, *Sieci teleinformatyczne w procesie dowodzenia komponentem wojsk lądowych*, Rozprawa habilitacyjna, ZN AON. Warszawa 2012

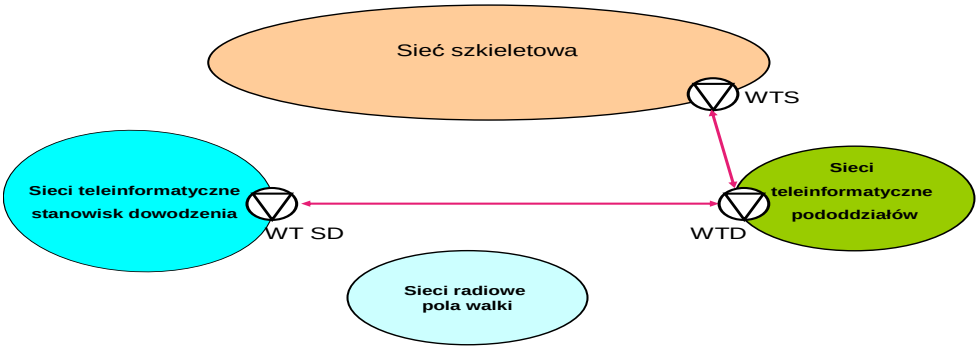
[3] Potwierdzają to ćwiczenia wojskowe organizowane w SZ RP.

Rysunek nr 1: Struktura wojskowych sieci teleinformatycznych organizowanych na potrzeby procesu kierowania operacją kryzysową – wariant.



Źródło: P. Dela, *Sieci teleinformatyczne w procesie dowodzenia komponentem wojsk lądowych*, AON. Warszawa 2012

Rysunek nr 2: Idea współpracy wojskowych sieci teleinformatycznych z innymi sieciami poprzez węzły teleinformatyczne tworzone na potrzeby procesu zarządzania kryzysowego – wariant.



Źródło: P. Dela, *Sieci teleinformatyczne w procesie dowodzenia komponentem wojsk lądowych*, AON. Warszawa 2012

Linie teletransmisyjne międzywęzłowe są rozwijane pomiędzy węzłami sieciowymi sieci szkieletowej. Sieć szkieletowa powinna być dowiązana własnymi środkami teleinformatycznymi, do co najmniej dwóch węzłów nadrzędnej sieci teleinformatycznej (sieci operacyjnej, sieci stacjonarnych resortowych, jak i publicznych). Do węzłów teleinformatycznych sieciowych powinny być dowiązywane węzły teleinformatyczne stanowisk dowodzenia i punktów kierowania elementów ugrupowania bojowego prowadzących działania na obszarze rozwinięcia sieci szkieletowej oraz węzły teleinformatyczne dostępowe. Linie teletransmisyjne bezpośrednie są organizowane z wykorzystaniem środków i urządzeń radiowych, radioliniowych, kablowych i środków satelitarnych.

Dla potrzeb przekazywania dużych zbiorów informacji w ramach stworzonego systemu dowodzenia istnieje potrzeba posiadania w sieciach teleinformatycznych określonego potencjału transmisyjnego. W sytuacjach, gdy stanowiska dowodzenia są rozwinięte i zespoły funkcjonalne działają w ramach tych stanowisk, wymagany potencjał jest zapewniony przez opisana wyżej sieć szkieletową. Jeżeli jednak stanowiska dowodzenia i punkty kierowania się przemieszczają lub poszczególne zespoły działają poza bazą, to istnieje potrzeba organizowania linii telekomunikacyjnych bezpośrednich o wymaganym potencjale transmisyjnym. Linie teletransmisyjne dowiązania determinowane są liczbą elementów ugrupowania bojowego wykonujących swoje zadania w obszarze rozwinięcia sieci szkieletowej oraz wyposażeniem węzłów teleinformatycznych w środki i urządzenia teleinformatyczne. Linie teletransmisyjne abonenckie występują na poziomie sieci teleinformatycznych stanowisk dowodzenia i punktów kierowania. Są rozwijane w celu zapewnienia wymiany informacji poszczególnym operatorom zarówno w ramach samej sieci lokalnej, jak i poprzez sieci rozległe, do których podłączone jest dane stanowisko dowodzenia, punk kierowania czy baza wojskowych sił zadaniowych.

Aby przyszłe siły zadaniowe uzyskały pełną zdolność do prowadzenia działań w operacji kryzysowej ich transformacja powinna zmierzać do wzrostu zdolności manewrowych wojsk i możliwości sieci teleinformatycznych, a także zintegrowania logistyki, rozszerzenia współpracy cywilno-wojskowej oraz bardziej efektywnego wykorzystania wojsk (zdolności w zakresie: systemów rozpoznania i wywiadu, prowadzenia działań w rejonach zurbanizowanych). Wszystkie te przedsięwzięcia zmierzają do osiągania przewagi informacyjnej, znacznego wzrostu możliwości prowadzenia działań autonomicznych czy wreszcie do uzyskania zdolności operacyjnych, pozwalających na przeciwstawianie się coraz nowszym zagrożeniom we współczesnych operacjach reagowania kryzysowego. Należy także zwrócić uwagę na możliwości współpracy sieci teleinformatycznych komponentu wojsk lądowych z innymi sieciami: publicznymi, komercyjnymi i resortowymi w czasie organizowania systemu zarządzania sytuacją kryzysową.

Wojskowe sieci teleinformatyczne powinny mieć zdolność przyjęcia i obsłużenia dużej ilości użytkowników oraz elementów sieci, które powinny być łatwo identyfikowalne (co zapewnia adresacja IP) zarówno elementów wojskowych, jak i spoza resortu. Biorą pod uwagę technologie i protokoły wykorzystywane do budowy wojskowych sieci teleinformatycznych celowym byłoby skupienie uwagi na próbie integracji mobilnych sieci teleinformatycznych z globalną siecią Internet w celu umożliwienia dostępu dowódcy realizującego działania w operacji kryzysowej do szerokiego zaplecza zasobów sieciowych

w postaci baz danych rozproszonych na dużym obszarze, a także do innych elementów sieci, które dostarczają użytecznych informacji do prowadzenia działań np. danych o infrastrukturze telekomunikacyjnej danego obszaru. Ważne będą również organizacyjne i techniczne możliwości współdziałania sieci wojskowych z innymi wykorzystywanymi przez służby w ramach reagowania kryzysowego i kierowania tego typu operacją na obszarze kraju oraz infrastruktura teleinformatyczna dostępna dla wszystkich komponentów systemu.

Sieci wojskowe powinny gwarantować usługi na podobnym poziomie jak sieci publiczne czy komercyjne ale plusem tych sieci powinno być bezpieczeństwo przesyłanej informacji.

Usługi teleinformatyczne są obecnie najbardziej zaawansowanym komponentem struktury sieci teleinformatycznej. Komponent usług IT będzie się charakteryzował przede wszystkim zastosowaniem protokołu internetowego (IP wersja 6 i kolejne),[4] który tworzy wspólny, bezpieczny mechanizm transportowy dla wszystkich rodzajów informacji przesyłanych przez wszystkie media transmisyjne w sieciach teleinformatycznych. Usługi transportowe IP będą funkcjonować w środowisku, którego cechą jest wykorzystanie szerokiego zakresu usług transmisyjnych (transportowych) i konieczność wspierania różnych rodzajów jakości usług w celu spełnienia wymagań poszczególnych aplikacji. Obecne trendy w tej dziedzinie zwracają się ku rozwiązaniom polegającym na skupianiu uwagi na końcowych użytkownikach i dostarczaniu im zdefiniowanych usług teleinformatycznych. Stosowane do niedawna podejście systemowe, w którym najważniejsze było utrzymywanie systemów, a użytkownik był tylko „dodatkiem" do systemu, odchodzi w przeszłość.

Wnioski

Dostrzegając wagę problemu związanego z kierowaniem reagowaniem kryzysowym autor podjął się opisania ważnego problemu jakim są możliwości wykorzystania sieci teleinformatycznych wojskowych i ich współpracy z sieciami publicznymi na potrzeby zarządzania kryzysowego realizowanego przez SZ RP. Otrzymane wyniki badań pozwalają na stwierdzenie, że idealnym rozwiązaniem było by stworzenie jednego zintegrowanego zautomatyzowanego systemu informatycznego, który funkcjonował by we wszystkich służbach oraz podmiotach biorących udział w kierowaniu siłami i środkami podczas działań związanych z reagowaniem kryzysowym. Autor zdaje sobie jednak sprawę, że nie jest możliwe zastosowanie takiego rozwiązania, dlatego koniecznym jest:

- opracowanie koncepcji informatycznego wsparcia kierowania reagowaniem kryzysowym, która w pierwszym rzędzie zawierać będzie wymagania jakie taki system powinien spełniać;
- opracowanie i wdrożenie interfejsów umożliwiających bezkolizyjne przekazywanie informacji pomiędzy różnymi systemami informacyjnymi wszystkich podmiotów biorących udział w kierowaniu reagowaniem kryzysowym;

[4] IP wersja 6 ma umożliwić powstanie tzw. Internetu rzeczy (sprzęt AGD w ramach GRK, GO, chipy nowej generacji, kod kreskowy RFID), który ułatwi m.in. zabezpieczenie logistyczne i usprawni system zasilania grup.

- opracowanie środowiska informatycznego, które ujednolici dotychczasowe działania różnych organów i służb;
- opracowanie standardu informatycznego, który stanowić będzie podstawę formułowania w przyszłości specyfikacji sprzętowych i programowych;
- określenie harmonogramu działań koncepcyjnych oraz wdrożeniowych;
- oszacowanie kosztów związanych ze wszystkimi działaniami w tym zakresie oraz wskazanie źródeł ich finansowania.

Współpraca SZ RP z terenowymi organami administracji publicznej w ramach kierowania reagowaniem kryzysowym przy wykorzystaniu wojskowych sieci telekomunikacyjnych jest możliwa wtedy, gdy organa administracji publicznej zostaną w te środki wyposażone. Możliwości wykorzystania istniejącej infrastruktury teleinformatycznej jest tym większa im bardziej otwarte są te systemy. Badania wykazały, że podejście COTS (*ang. Commercial of the Shelves*), polegające na wykorzystaniu technologii komercyjnych w wojskowych systemach teleinformatycznych, w znacznym stopniu ułatwiło współpracę publicznych, resortowych i wojskowych systemów teleinformatycznych. Należy zauważyć jednocześnie, że obserwowany jest ciągły wzrost znaczenia technologii transmisji danych na niekorzyść klasycznych systemów telekomunikacyjnych.

Wprowadzenie takiego systemu opartego na funkcjonowaniu usług w ramach sieci teleinformatycznej jest procesem nieuniknionym, który należałoby wprowadzić w SZ RP i wykorzystywać do szkolenia i realizacji zadań przez pododdziały wojsk lądowych. Początkiem tego procesu jest wprowadzenie do użytkowania w SZ RP systemu JCATS i przetarg na platformę sieciocentryczną wsparcia dowodzenia nowej generacji (BMS).

Punkt kierowania działaniami w ramach Grupy Reagowania Kryzysowego (GRK) czy Grupy Operacyjnej (GO) powinien posiadać bezpośrednią bezpieczną łączność z przełożonym, podwładnymi, elementami współdziałającymi, militarnymi i niemilitarnymi po to, aby czuwać nad prawidłowym przebiegiem wykonywanych zadań. W sytuacjach kryzysowych posiadać powinien niezbędne narzędzia w postaci sił i środków teleinformatycznych, aby reagować na powstałe zagrożenia.

W ramach GRK i GO zadania powinni wykonywać najlepiej wyszkoleni żołnierze, profesjonalnie przygotowani do obsługi i użytkowania nowoczesnej techniki i sprzętu nie tylko produkcji krajowej. Każdy użytkownik sieci musi być profesjonalnym usługobiorcą, wyposażonym w środki dostępowe do sieci, a każdy budujący sieć specjalistą IT, profesjonalnym usługodawcą wyposażonym w systemy kontroli sieci i bezpieczeństwa przekazywanej w niej informacji. Właściwie rozwinięta sieć teleinformatyczna pozwoli na racjonalne zarządzanie elementami reagowania kryzysowego i skuteczną kontrolę nad nimi oraz właściwe sterowanie środkami przymusu bezpośredniego (działania wojskowe, otwarcie ognia), jeżeli zajdzie taka potrzeba.

Wyniki badań przedstawione w niniejszym artykule, dotyczące organizacji wojskowych sieci teleinformatycznych na potrzeby procesu zarządzania kryzysowego, uprawniają do sformułowania następujących wniosków:

- Wojskowe sieci teleinformatyczne wykorzystywane w procesie zarzadzania kryzysowego są częścią składową ogólnego systemu łączności danej operacji, ich głównym przeznaczeniem jest zapewnienie wymiany

informacji pomiędzy odpowiednimi organami decyzyjnymi oraz usprawnienie (przyspieszenie) procesu kierowania.

- Wojskowe sieci teleinformatyczne organizowane na potrzeby kierowania reagowaniem kryzysowym organizuje się, zapewniając kompleksowe wykorzystanie różnorodnych środków teleinformatycznych we wszystkich relacjach dowodzenia oraz sterowania środkami rażenia, współdziałania, powiadamiania, ostrzegania i alarmowania. Możliwości i struktura techniczno-funkcjonalna sieci powinna być znana podmiotom niemilitarnym i zależeć od przyjętego planu działania i zadań, jakie są stawiane przed sieciami w danej operacji.
- Wojskowe sieci teleinformatyczne są zbiorem kilku podsieci różniących się właściwościami, przeznaczeniem i rozmiarami, dostosowanych do spełniania funkcji współdzielenia i wymiany informacji w różnym zakresie, w zależności od zastosowanej techniki przekazu informacji. Poszczególne sieci nie są przypisywane do konkretnego poziomu dowodzenia, lecz do zadania, jakie muszą realizować i powinny realizować usługi niezbędne komponentom do przeciwdziałania sytuacjom kryzysowym.

Streszczenie

Rozwój technologiczny na świecie, w szczególności dziedziny związane z przetwarzaniem i przesyłaniem informacji elektronicznej, przyniósł wiele zagrożeń, które mogą oddziaływać na społeczeństwa w postaci różnorodnych kryzysów. Mogą to być kryzysy wywołane m. in. działalnością terrorystyczną (cyberterroryzm), katastrofą ekologiczną czy też wrogim oddziaływaniem innego państwa (lub działalność hakerska pojedynczych jednostek czy instytucji).

Dostrzegając wagę problemu związanego z reagowaniem kryzysowym autor przedstawił w artykule możliwości wojska w dziedzinie szeroko pojętej teleinformatyki i wykorzystania wojskowych sieci łączności do kierowania działaniami w czasie sytuacji kryzysowej na terenie Polski. Autor podjął się analizy ważnego problemu jakim są możliwości sieci teleinformatycznych SZ RP na potrzeby kierowania (dowodzenia, zarządzania) reagowaniem kryzysowym realizowanym przez centra i organa kryzysowe naszego państwa.

Należy przypuszczać, że siły zbrojne, a w dużej mierze wojska lądowe będą miały znaczący udział w zapobieganiu skutkom różnego rodzaju katastrof. Będą one ważnym ogniwem realizującym proces kierowania reagowaniem kryzysowym. Z tego względu muszą być zdolne do realizacji wybranych etapów reagowania kryzysowego przy jednoczesnej możliwości współpracy z organami terenowymi państwa i samorządami. Z powyższego wynika, że należy podjąć kroki zmierzające do określenia przydatności posiadanych przez wojsko systemów i sieci teleinformatycznych w zakresie zarządzania kryzysowego, a także określenie możliwości wykorzystania wojskowych systemów i technologii w ramach bezpieczeństwa infrastruktury krytycznej Polski.

Summary

The technological development in the world, in particular in areas related to the transmission of electronic information, has brought a lot of risks that may affect the public in the form of a variety of crises. This can be caused among others

crises. terrorist activities (cyber terrorism), ecological disaster or hostile influence of another state (or hacker activity of single individuals or institutions).

Recognizing the importance of the problem of emergency response the author presented military capabilities in the field of IT and the wider use of military communications networks to direct the activities during a crisis situation on the Polish territory. The author undertook the analysis of an important issue what are the possibilities of IT networks Armed Forces for targeting (command, management) implemented by emergency response centers and emergency authorities of our country.

It is believed that polish army, and especially the armed forces, will have a significant part in preventing the effects of different types of disasters. They will be an important link in the process of implementing emergency response management. For this reason, they must be able to perform some steps of emergency response while allowing cooperation with the terrain of the state and local governments. It follows that you should take steps to determine the suitability held by the military systems and networks in the field of crisis management and to determine the possible use of military systems and technology within the security of critical infrastructure in our country.

Bibliografia

1. Dela P. i inni, *Kierunki zmian struktur organizacyjnych i wyposażenia pododdziałów dowodzenia wojsk lądowych w zakresie wsparcia informatycznego procesu dowodzenia*, AON. Warszawa 2008
2. Dela P., *Sieci teleinformatyczne w procesie dowodzenia komponentem wojsk lądowych*, Rozprawa habilitacyjna, ZN AON. Warszawa 2012
3. Janczak J. i inni, *Wykorzystanie mobilnych sieci teleinformatycznych na stanowiskach dowodzenia szczebla taktycznego*, AON. Warszawa 2008
4. Nowicki K. i inni, Sieci LAN, MAN i WAN – protokoły komunikacyjne, FPT. Kraków 2003
5. Ustawa z dnia 26.04.2007 r. *O zarządzaniu kryzysowym* (Dz.U. Nr 89, poz. 590)