OPERAŢIILE INFORMAŢIONALE SPECIFICE SISTEMULUI NATO DE RĂSPUNS LA CRIZE

SPECIFIC INFORMATION OPERATIONS OF NATO CRISES RESPONSE SYSTEM

Mr.drd. Cristian ICHIMESCU*

Sistemul NATO de răspuns la crize are nevoie de planificarea și executarea operațiilor informaționale pentru a controla și a domina mediul informațional de confruntare. Pentru aceasta, elementele fundamentale (obiective, activități, audienţe ţintă şi efecte), ce caracterizează fiecare domeniu specific operațiilor informaționale, necesită să fie coordonate, sincronizate şi prioritizate indiferent că vorbim despre operaţii de tip articol 5 de apărare colectivă, fie de operaţii non-articol 5 de răspuns la crize. Componentele complementare ale Sistemului NATO de răspuns la crize: opțiunile preventive, măsurile de răspuns la crize, contrasurprinderea, stările de alertă de securitate NATO și contraagresiunea pot fi relaționate cu anumite domenii ale operațiilor informaționale. Se poate observa că în cazul măsurilor de răspuns la crize, a contrasurprinderii și a contragresiunii toate domeniile operațiilor informaționale pot fi utilizate în timp ce în cazul opțiunilor preventive și a stărilor de alertă de securitate NATO doar o parte a acestor domenii pot fi puse în valoare.

NATO Crisis Response System needs planning and execution of Information Operations to control and dominate the information environment of confrontation. For this, the fundamental elements (objectives, activities, target audiences and effects) that characterize each specific field of Information Operations, need to be coordinated, synchronized and prioritized whether we speak of Article 5 collective defense operations or non-Article 5 crisis response operations. Complementary components of the NATO Crisis Response System: Preventive Options, Crisis Response Measures, Counter Surprise, NATO Security Alert States and Counter Agression can be related to specific domains of Information Operations. It can be seen that in case of Crisis Response Measures, Counter Surprise and Counter Agression all domains of Information Operations can be used while in the case of Preventive Options and NATO Security Alert States only some of these domainss can be valued.

Cuvinte-cheie: operaţii informaţionale; Sistemul NATO de răspuns la crize.

***Keywords**: Information Operations; NATO Crises Response System.*

Operaţiile informaţionale (Information Operation Info Ops) sunt prezente în spaţiul de luptă modern şi în toate operaţiile în curs de desfăşurare ale NATO. Aceste operaţii se concretizează într-un cumul de activităţi informaţionale realizate de un număr de zece domenii[1] nominalizate de NATO în AJP-3.10, *Allied Joint Doctrine for Information Operations* (Doctrina Aliată Întrunită pentru Operaţii Informaţionale).

Sistemul NATO de răspuns la crize (NATO Crises Response System – NCRS) este acel sistem din cadrul organizaţiei Nord-Atlantice responsabil de asigurarea stării de pregătire şi sprijin în vederea realizării prevenirii conflictelor şi a managementului crizelor prin implicarea organizaţiei în operaţii de tip articol 5 şi non-articol 5.

Această analiză pleacă de la ipoteza utilizării tuturor celor zece domenii ale Info Ops de către NCRS în scopul îndeplinirii scopului fundamental a NATO de a proteja libertatea şi securitatea tuturor membrilor săi prin mijloace politice şi militare. Se demonstrează această ipoteză plecând de la necesitatea *coordonării, sincronizării şi prioritizării* între elementele fundamentale (obiective, activităţi, audienţe ţintă şi efecte) ce caracterizează domeniile Info Ops. Apoi se prezintă succint *componentele NCRS* şi se detaliază pentru fiecare dintre *domeniile specifice* Info Ops, obiectivele, activităţile, audienţele ţintă şi efectele, precum şi acele componente ale NCRS în care se poate utiliza domeniul specific al operațiilor informaționale.

***Universitatea Națională de Apărare „Carol I”**
e-mail*: cristian.ichimescu@yahoo.com*

Coordonare, sincronizare şi prioritizare

Domeniile Info Ops pot crea cele mai bune efecte asupra audienţelor ţintă prin executarea unor activităţi informaţionale specifice în vederea îndeplinirii unor obiective clar stabilite. Elementele fundamentale OAAE (obiective, activităţi, audienţe ţintă şi efecte)[2], ce caracterizează fiecare domeniu specific Info Ops, necesită să fie coordonate, sincronizate şi prioritizate pentru a îndeplini scopul stabilit de către comandantul operaţiei. Indiferent că vorbim despre operaţii de tip articol 5 de apărare colectivă, fie de operaţii non-articol 5 de răspuns la crize, cuvintele-cheie care trebuie să caracterizeze relaţia dintre elementele fundamentale asociate fiecărui domeniu Info Ops sunt: *coordonare, sincronizare şi prioritizare*.

Coordonarea permite funcţionarea celor zece domenii amintite ale Info Ops prin scoaterea în evidenţă a elementelor comune acestor domenii şi activarea lor în timp ce elementele care le diferenţiază sau chiar care le pun în relaţie contradictorie nu sunt încurajate. Desigur, rolul esenţial în coordonare va fi jucat de toate structurile de tipul Comitetului de coordonare a operaţiilor informaţionale (Information Operations Coordination Board IOCB), ce se vor regăsi la nivelul eşaloanelor strategice şi operative. La nivel tactic, această coordonare va fi sarcina unui grup de coordonare a operaţiilor informaţionale sau a unor specialişti în acest domeniu.

Sincronizarea este componenta care va oferi soluţia la modul în care fiecare domeniu al Info Ops va răspunde secvenţial şi integrat la fiecare dintre elementele fundamentale OAAE la momentul şi locul potrivit. Vom avea astfel obiective care vor fi îndeplinite la un nivel tactic, de exemplu, prin lucrul în comun a doar o parte dintre domeniile Info Ops, pe baza unor activităţi informaţionale specifice care vor fi direcţionate către audienţele ţintă stabilite de către comandantul din teren. Cu cât vom urca mai sus, la nivelul operativ şi la cel strategic, cu atât sincronizarea pe orizontală şi verticală, în timp şi spaţiu, va fi esenţială între toate domeniile Info Ops pentru a obţine efectele dorite în concordanţă cu obiectivele stabilite.

Prioritizarea este un alt element important care trebuie să ghideze specialiştii în Info Ops când se discută despre modul cum se alocă resursele Info Ops în spaţiul de luptă la locul şi momentul dorit şi mai ales potrivit. Acest proces al prioritizării pe care specialiştii în Info Ops îl vor utiliza pe tot parcursul ducerii operaţiilor va însemna o clasificare a importanţei obiectivelor informaţionale, a activităţilor informaţionale, a audienţelor ţintă şi a efectelor produse asupra acestora, astfel încât să se îndeplinească misiunea propusă de către comandant şi să se atingă starea finală dorită.

Încurajarea coordonării, a sincronizării şi a prioritizării dintre domeniile Info Ops şi obiectivele, activităţile, audienţele ţintă şi efectele Info Ops se poate concretiza în acţiunea eficientă a Sistemului NATO de răspuns la crize în mediul informaţional în vederea controlării acestuia.

Componentele Sistemului NATO de răspuns la crize

Sistemul NATO de răspuns la crize conţine, în prezent, cinci componente complementare[3]: opţiuni preventive, măsuri de răspuns la crize, contrasurprinderea, stări de alertă de securitate NATO şi contraagresiunea. Deşi aparent denumirea sistemului face trimitere doar la operaţiile de răspuns la crize, deci specifice non-articol 5, NCRS acoperă prin componentele sale şi operaţiile de tip articol 5. Ceea ce va diferenţia, în cadrul NCRS, modul de acţiune la un atac împotriva unei ţări membre prin activarea articolului 5 din Tratatul de la Washington, de modul de acţiune la o situaţie de criză în spaţiul de interes al NATO va fi proporţia utilizării combinate şi complementare a componentelor NCRS.

Opţiunile preventive reprezintă prima componentă a NCRS şi constă într-o serie de posibile răspunsuri pe care Alianţa le are pregătite pentru situaţii de crize incipiente. Aceste opţiuni pot acoperi o plajă largă de opţiuni diplomatice, economice, militare, de control al armamentelor şi de informare prin intermediul mass-mediei în scopul de a reduce situaţia de criză. Opţiunile preventive prin componenta militară pot aduce un aport substanţial la intensificarea vigilenţei forţelor ţărilor membre NATO. În acest context, domeniile Info Ops care vor putea fi utilizate în cadrul opţiunilor preventive sunt: securitatea informaţiilor, inducerea în eroare, războiul electronic, angajarea liderilor cheie, operaţiile în reţele de calculatoare.

Măsurile de răspuns la crize reprezintă convenţii pe care statele membre ale NATO sunt solicitate să le îndeplinească în anumite situaţii de criză. Aceste măsuri se pot, uneori, concretiza

în acțiuni pe care anumite instituții naționale sau comandamente trebuie să le execute. Măsurile de răspuns la crize nu au caracter obligatoriu pentru statele membre, ele putând căpăta anumite nuanțe, tendințe și evoluții decise de statul în sine, de legislația națională și de modul de punere în aplicare a anumitor proceduri specifice instituțiilor din sistemul de apărare național. Gama largă de acțiune a măsurilor de răspuns la crize acoperă domenii diverse, cum ar fi: operații specifice forțelor terestre, aeriene, navale, operații informaționale (în toate cele zece domenii), protecția forței, logistica, infrastructura critică etc.

Contrasurprinderea este următoarea componentă a NCRS. Ea se referă la acţiunile de apărare civile şi militare[4] ce se iau în cazul unui atac. Această componentă nu este de nivelul măsurilor de răspuns la crize prezentate mai sus, care presupun măsuri luate din timp. Contrasurprinderea presupune, deci, o acțiune de tip reacție militară și civilă la un atac al unui adversar. Luând în considerare acest lucru, se estimează că toate domeniile Info Ops vor putea fi utilizate în cadrul contrasurprinderii.

Stările de alertă de securitate NATO constau în măsuri antiteroriste şi antisabotaj[5] luate de statele membre NATO. Aceste stări nu reprezintă o componentă în sine a NCRS, însă sunt incluse pentru a asigura similitudinea stărilor de alertă de securitate la nivelul tuturor statelor membre ale Alianței. La nivelul acestor stări de alertă, se poate estima că următoarele domenii ale Info Ops ar putea fi utilizate: operațiile psihologice, prezența, profilul şi postura trupelor, angajarea liderilor cheie, război electronic și operațiile în rețelele de calculatoare.

Contraagresiunea reprezintă trecerea la autorizarea angajării forţelor armate a statelor membre NATO împotriva unui adversar ce atacă un stat membru al Alianței. Această componentă poate crea efecte anterior activării articolului 5. Prin natura efectivă de angajare a forțelor armate, rezultă că se pot utiliza pe timpul contraagresiunii toate domeniile Info Ops, în funcție de starea finală dorită de către comandantul forțelor proprii și de modul în care unul sau altul dintre domeniile Info Ops răspund mai bine îndeplinirii acestei stări.

Domeniile operaţiilor informaţionale specifice Sistemului NATO de răspuns la crize

Domeniile operaţiilor informaţionale identificate în documentele NATO ce reglementează Info Ops sunt: operațiile psihologice, prezența, profilul şi postura trupelor, securitatea operaţiei, securitatea informaţiilor, inducerea în eroare, războiul electronic, distrugerea fizică, angajarea liderilor cheie, operaţiile în reţele de calculatoare, cooperarea civili - militari.

Întrebarea firească ce apare este: „În ce măsură domeniile enumerate mai sus răspund componentelor complementare ale NCRS?”. Pentru aceasta, se pot analiza pe fiecare domeniu al operaţiilor informaţionale obiectivele, activităţile, audienţele ţintă şi efectele specifice şi cum acestea se vor ataşa uneia sau mai multor componente specifice NCRS.

Operaţiile psihologice au ca obiectiv principal influenţarea percepţiilor, a atitudinilor şi a comportamentelor audienţelor ţintă pentru a îndeplini, în final, misiunea stabilită de către comandant. Un alt obiectiv important, în special în lumina acţiunii comune în cadrul Sistemului NATO de răspuns la crize, este coordonarea cu celelalte domenii ale Info Ops pentru a obţine efectele dorite asupra audienţelor ţintă. Activităţile preponderente specifice PSYOPS vor fi de tipul activităţilor de influenţare şi activităţilor îndreptate împotriva conducerii şi capacităţii de comandă. Audienţele ţintă specifice operaţiilor informaţionale pot fi: adversarul şi populaţia ostilă. Efectele pe care operaţiile psihologice le pot produce sunt: influenţarea capacităţii de decizie a liderilor forţelor adversarului şi insuflarea incapacităţii de a lupta pentru forţele acestora; motivarea adversarului pentru a dezerta; câştigarea adeziunii populaţiei locale ostile.

Operaţiile psihologice, ca parte integrantă a Info Ops, pot fi utilizate de Sistemul NATO de răspuns la crize în cadrul măsurilor de răspuns la crize, a contrasurprinderii, a stărilor de alertă de securitate B, C şi D şi, în mod prioritar, în cazul contraagresiunii.

Prezenţa, profilul şi postura trupelor reprezintă un alt domeniu al operaţiilor informaţionale care poate aduce o contribuţie importantă Sistemului NATO de răspuns la crize. Obiectivele principale care sunt îndeplinite de acest domeniu sunt: transmiterea unei imagini publice a forţei proprii; postarea unei atitudini care identifică pozitiv forţele, militarii şi comandanţii proprii. Pentru a îndeplini aceste obiective, activităţile specifice vor fi de tipul activităţilor de influenţare, activităţilor de protecţie, precum şi a activităţilor îndreptate

împotriva conducerii şi capacităţii de comandă. Audienţele ţintă specifice PPP sunt: adversarul, aliaţii şi populaţia locală. Efectele pe care prezenţa, profilul şi postura trupelor le obţin sunt: motivarea pozitivă a acţiunilor aliaţilor, câştigarea încrederii populaţiei locale în vederea susţinerii forţele proprii şi demotivarea adversarului.

Prezenţa, profilul şi postura trupelor este un domeniu al Info Ops care poate fi regăsit în toate componentele NCRS, cum ar fi: opţiunile preventive, măsurile de răspuns la crize, contrasurprinderea, stările de alertă de securitate NATO şi contraagresiunea.

Următorul domeniu al Info Ops este *securitatea operaţiei.* Prin acest domeniu, operaţiile informaţionale pot îndeplini două obiective: să identifice acele informaţiile despre forţele proprii pe care adversarul nu trebuie să le cunoască şi să protejeze informaţiile care pot conduce forţele proprii la victorie. Aceste obiective pot fi realizate, în special, prin intermediul unor activităţi de protecţie informaţională. Audienţele ţintă ale securităţii operaţiei sunt: forţele proprii, în special, şi aliaţii; şi adversarul. Efectele utilizării acestui domeniu sunt: acţiunile forţelor proprii sunt protejate faţă de acţiunile de spionaj ale adversarului; nivelul de securitate al protecţiei informaţiilor nu permite accesul adversarului la acestea.

Securitatea operaţiei este esenţială pentru Sistemul NATO de răspuns la crize în toate componentele sale şi, în special, în contraagresiune, contrasurprindere şi în măsurile de răspuns la crize.

Securitatea informaţiilor este un alt domeniu al Info Ops care se regăseşte la nivelul Sistemului NATO de răspuns la crize. Obiectivele pe care securitatea informaţiilor le are în atenţie sunt: asigurarea securităţii personalului şi securităţii fizice; asigurarea securităţii documentelor şi securităţii industriale; asigurarea securităţii sistemelor informatice şi de comunicaţii. Activităţile specifice care sunt asociate INFOSEC sunt similare celor ale securităţii operaţiei fiind deci prioritare activităţile de protecţie informaţională. Având în vedere aceste activităţi, audienţele ţintă vor fi reprezentate, în mare măsură, de forţele proprii şi de aliaţi şi, în mai mică măsură, de adversar. Efectele cele mai consistente pe care securitatea informaţiilor le aduc în cadrul efectelor produse, în general, de domeniile Info Ops sunt: adversarul nu are acces la informaţiile din reţele de comunicaţii şi schimb de date ale forţelor proprii; păstrarea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi non-repudierii informaţiilor printr-un sistem de control organizat şi printr-o educaţie preventivă permanentă a personalului forţelor proprii.

Securitatea informaţiilor este importantă pentru Sistemul NATO de răspuns la crize, în special, în cadrul componentelor de opţiuni preventive, de contraagresiune şi contrasurprindere şi punerea în aplicare a măsurilor de răspuns la crize.

Inducerea în eroare este acel domeniu al Info Ops care se va orienta pe tot parcursul evoluţiei situaţiei de criză, de la pace până la război, pe crearea surprizei pentru adversar. Acesta va fi obiectivul fundamental, alături de componenta de incertitudine pe care orice acţiune sau inacţiune a forţelor proprii o poate produce asupra adversarului. Alături de această audienţă ţintă, mai face obiectul acestui domeniu al operaţiilor informaţionale şi populaţia ostilă. Activităţile ce vor conduce la inducerea în eroare sunt în prima fază de influenţare, apoi îndreptate împotriva conducerii şi capabilităţilor de comandă şi, nu în ultimul rând, au o componentă dezvoltată de protecţie informaţională. Efectele cele mai importante pe care le creează inducerea în eroare sunt: incapacitatea forţelor adversarului de a răspunde la locul şi momentul potrivit acţiunilor forţelor proprii; subminarea capacităţii de încredere în cadrul forţelor ce aparţin adversarului privind relaţia comandant-subordonaţi; crearea unei permanente impresii privind imposibilitatea adversarului de a previziona care sunt intenţiile şi acţiunile prezente şi viitoare ale forţelor proprii.

Pentru Sistemul NATO de răspuns la crize, inducerea în eroare va fi categoria de domeniu al Info Ops utilizată în cadrul componentelor de contraagresiune şi contrasurprindere şi desigur că poate fi utilizată şi în cadrul opţiunilor preventive. În plus, la punerea în aplicare a măsurilor de răspuns la crize, inducerea în eroare poate fi o opţiune pentru NCRS.

Războiul electronic (EW) este un domeniu esenţial al operaţiilor informaţionale. Obiectivele prioritare ale războiului electronic sunt: obţinerea superiorităţii în spectrul electromagnetic asupra adversarului; protecţia şi prevenţia împotriva acţiunilor adversarului în spaţiul electromagnetic. Activităţile care vor contribui la îndeplinirea obiectivelor menţionate mai sus sunt activităţile

de protecţie informaţională, activităţile de influenţare şi, desigur, activităţile îndreptate împotriva conducerii. Audienţele ţintă vor fi reprezentate de forţele proprii şi de către adversari sau alte forţe ostile care deţin capabilităţi de acţiune specifice EW. Efectele create de războiul electronic pot lua forma: interceptării şi bruierii emisiilor electromagnetice ale adversarului; protecţiei emiterii în spaţiul electromagnetic de către forţele proprii specializate.

Războiul electronic este un domeniu extrem de util pentru toate componentele Sistemul NATO de răspuns la crize şi, în special, pentru contraagresiune şi contrasurprindere. Desigur că EW poate fi utilizat la un nivel redus şi în cadrul opţiunilor de răspuns la crize şi apoi la o intensitate mai mare pe timpul măsurilor de răspuns la crize. În ceea ce priveşte stările de alertă de securitate NATO, în funcţie de fiecare stare şi de necesitatea utilizării EW, acesta se va utiliza treptat şi în concordanţă cu efectele dorite.

Distrugerea fizică este un alt domeniu care adaugă o cotă deosebită la capacitatea operaţiilor informaţionale de a crea efecte în spaţiul de luptă. Dualitatea obiectivelor realizate de acest domeniu se referă, pe de o parte, la atacarea directă a capacităţilor de comandă ale adversarului şi, pe de altă parte, la impactul psihologic[6] asupra adversarului. Pentru a îndeplini obiectivele distrugerii fizice, activităţile specifice vor fi, în special, de tip activităţi îndreptate împotriva conducerii şi activităţi de influenţare, iar în mod secundar vor fi şi de tip activităţi de protecţie. Audienţele ţintă specifice distrugerii fizice sunt adversarul şi alte forţe ostile prezente în spaţiul de luptă. Efectele acestui domeniu se pot orienta similar obiectivelor pe două direcţii: provocarea de daune materiale asupra punctelor de comandă şi centrelor de comunicaţii; reducerea voinţei adversarului de a continua lupta, neîncrederea în capacităţile proprii de apărare împotriva loviturilor forţelor proprii.

Distrugerea fizică va fi asociată, în special, următoarelor componente ale NCRS: contraagresiune şi contrasurprindere. În funcţie de decizia structurilor de comandă, distrugerea fizică poate fi utilizată în cadrul măsurilor de răspuns la crize.

Angajarea liderilor cheie este acel domeniu care identifică persoanele cele mai importante din rândul adversarului, a populaţiei locale, liderii religioşi, politici, informali etc. pe care liderii forţelor proprii ar trebui să-i cunoască şi să realizeze anumite contacte, întâlniri, schimb de opinii etc. Obiectivele acestui domeniu sunt: identificarea liderilor cheie; stabilirea contactelor cu aceştia şi influenţarea liderilor cheie în vederea apropierii acestora de obiectivele forţelor proprii. Activităţile angajării liderilor cheie vor cuprinde activităţi împotriva conducerii şi activităţi de influenţare prin: obţinerea unor informaţii despre liderii cheie; stabilirea unei modalităţi de contactare a acestor lideri; executarea unui plan de discuţii cu liderii cheie. Desigur că audienţele ţintă se vor concentra, în special, asupra adversarilor şi liderilor ostili, a liderilor influenţi din populaţia locală, precum şi a unor lideri indecişi cu putere de influenţă în zona de operaţii a forţelor proprii. Efectele pe care forţele proprii doresc să le obţină prin angajarea liderilor cheie sunt: influenţarea liderilor cheie, care sunt contactaţi în sensul susţinerii obiectivelor forţelor proprii; cunoaşterea, în detaliu, a personalităţii, a modului de gândire şi de acţiune a liderilor cheie; stabilirea unei reţele bazate pe relaţiile interpersonale şi interprofesionale dintre liderii cheie.

Calitatea deosebită a utilizării acestui domeniu în cadrul Sistemului NATO de răspuns la crize este dată de utilizarea angajării liderilor cheie în toate componentele NCRS şi pe toată perioada evoluţiei situaţiei de la criză la conflict. Vom regăsi, astfel, angajarea liderilor cheie la nivelul opţiunilor preventive, a măsurilor de răspuns la crize, a contrasurprinderii, a stărilor de alertă de securitate NATO şi a contraagresiunii.

Operaţiile în reţele de calculatoare sunt tipul de operaţii care a apărut odată cu creşterea dependenţei sistemului militar de sistemele de calculatoare, reţelele dintre acestea, a implicării utilizării calculatoarelor în toate activităţile militare de la luarea deciziilor până la punerea lor în practică. Obiectivele operaţiilor în reţele de calculatoare pot fi: atacul reţelelor de calculatoare ale adversarului; protecţia reţelelor proprii de calculatoare de acţiunile adversarului. Activităţile specifice ale operaţiilor în reţelele de calculatoare pot îmbina atât activităţile împotriva conducerii, cât şi activităţile de influenţare cu activităţile de protecţie informaţională. Audienţele ţintă specifice CNO pot fi: adversarii, ostilii, forţele proprii şi populaţia locală. Efectele care se pot obţine în urma utilizării operaţiilor în reţelele de calculatoare sunt: reţelele de calculatoare ale adversarului, care

sunt inutilizabile sau sub controlul forţelor proprii; infectarea cu diferite tipuri de viruşi a reţelelor secundare ce aparţin adversarului; accesarea unor baze de date ale adversarului, fără ca acest lucru să fie detectat; protecţia reţelelor de calculatoare proprii de influenţele exterioare a adversarilor.

Operaţiile în reţelele de calculatoare se pot utiliza la nivelul opţiunilor preventive, a măsurilor de răspuns la crize, a contrasurprinderii, a stărilor de alertă de securitate NATO şi a contraagresiunii. Nivelul de utilizare se va modifica în cazul fiecărei componente a NCRS, în funcţie de intensitatea situaţiei de criză sau de conflict şi de capacitatea forţelor de a implica integrat sau separat acest tip de operaţii cu alte domenii ale Info Ops.

Cooperarea civili - militari este un domeniu esenţial al Info Ops în punerea în practică a abordării cuprinzătoare specifice NATO. Cooperarea civili - militari se va orienta pe îndeplinirea următoarelor obiective: stabilirea şi îmbunătăţirea relaţiilor dintre forţele proprii şi componentele civile ale societăţii; sprijinirea de către forţele proprii a instituţiilor statului în vederea refacerii capacităţii acestuia de a asigura funcţiile de bază în sprijinul populaţiei locale. Activităţile specifice cooperării civili - militari vor fi cele de influenţare combinate cu cele de protecţie informaţională. Audienţele ţintă prioritare vor fi populaţia locală şi forţele proprii. În ceea ce priveşte efectele, care se vor obţine prin utilizarea cooperării civili - militari, acestea vor fi: funcţionarea mai bună a autorităţilor locale; populaţia locală care înţelege relaţia de succes dintre autorităţile locale şi forţele proprii, reţelele de alimentare cu apă, gaze, curent, canalizare etc. care funcţionează în urma parteneriatului dintre autorităţile locale şi forţele proprii.

Cooperarea civili - militari poate fi utilizată în următoarele componente ale Sistemului NATO de răspuns la crize: contraagresiune, contrasurprindere şi în cadrul a măsurilor de răspuns la crize.

Concluzii

Ipoteza de la care am plecat la începutul acestui articol a fost aceea a utilizării tuturor celor zece domenii ale Info Ops de către NCRS în vederea îndeplinirii scopului fundamental a NATO. Am demonstrat această ipoteză arătând necesitatea ca elementele fundamentale ale fiecărui domeniu al Info Ops (obiective, activităţi, audienţe ţintă şi efecte) să fie coordonate, sincronizate şi prioritizate pentru a putea vorbi despre eficienţă la nivelul Info Ops. Apoi am descris componentele Sistemului NATO de răspuns la crize şi am prezentat obiectivele, activităţile, audienţele ţintă şi efectele pentru fiecare dintre domeniile Info Ops. Apoi am dedus care ar putea fi componentele NCRS în care am utiliza domeniile respective. Conform analizei, se poate aprecia că domeniile Info Ops care vor fi utilizate în cadrul *opţiunilor preventive* pot fi: securitatea informaţiilor, inducerea în eroare, războiul electronic, angajarea liderilor cheie şi operaţiile în reţele de calculatoare. În cazul *măsurilor de răspuns la crize, contrasurprinderii* şi *contragresiunii*, toate cele zece domenii ale operaţii informaţionale pot fi utilizate. La nivelul *stărilor de alertă de securitate NATO*, următoarele domenii ale Info Ops ar putea fi utilizate: operaţiile psihologice, prezenţa, profilul şi postura trupelor, angajarea liderilor cheie, război electronic şi operaţiile în reţelele de calculatoare. Desigur că aceste deducţii pot fi susţinute sau infirmate de practica punerii în acţiune a componentelor NCRS, în funcţie de situaţia de criză specifică.

Indiferent că vorbim despre operaţii de tip articol 5 de apărare colectivă, fie de operaţii non-articol 5 de răspuns la crize, Sistemul NATO de răspuns la crize are nevoie de planificarea şi executarea operaţiilor informaţionale pentru a controla şi a domina mediul informaţional de confruntare.

NOTE:

1 Domeniile sunt: operaţiile psihologice (*PSYOPS Psychological Operations*), prezenţa, profilul şi postura trupelor, securitatea operaţiei (*Operation security OPSEC*), securitatea informaţiilor (*Information Security INFOSEC*), inducerea în eroare, războiul electronic, distrugerea fizică, angajarea liderilor cheie (*Key Leaders Engagement KLE*), operaţiile în reţele de calculatoare (*Computer Network Operation CNO*), cooperarea civili - militari (Civil-military Cooperation CIMIC).

2 Am descris aceste elemente într-un articol anterior, *Operaţiile informaţionale şi mediul informaţional global*, publicat în Buletinul Universităţii Naţionale de Apărare „Carol I” nr. 2/2016, aprilie - iunie, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2016, pp. 48 - 53.

3 *** SMG-103, *Doctrina Armatei României*, Bucureşti, 2012, p. 74.

4 *** AJP-01(D), *Allied Joint Doctrine*, 2010, p. 4-4.

5 *Ibidem*.

6 *** SMG/CO – 10.0., *Doctrina operaţiilor informaţionale*, Bucureşti, 2011, p. 30.

BIBLIOGRAFIE

*** AJP-01(D), *Allied Joint Doctrine*, 2010.

*** AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.

*** SMG-103, *Doctrina Armatei României*, Bucureşti, 2012.

*** SMG/CO – 10.0., *Doctrina operaţiilor informaţionale*, Bucureşti, 2011.

Ichimescu C., *Operaţiile informaţionale şi mediul informaţional global*, Buletinul Universităţii Naţionale de Apărare „Carol I” nr. 2/2016, aprilie – iunie, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2016.