PROTECŢIA INFRASTRUCTURILOR CRITICE ÎN CONTEXT NA5CRO

CRITICAL INFRASTRUCTURE PROTECTION IN THE CONTEXT OF NA5CRO

PROTECTION DES INFRASTRUCTURES CRITIQUES DANS LE CONTEXTE DE NA5CRO

Lt.col.conf.univ.dr. Daniel ROMAN*

Complexitatea mediului operaţional contemporan este generată de multitudinea factorilor de influenţă, care, prin acţiunile sau stările de fapt ale acestora, dau acele puncte de echilibru sau de dezechilibru ale proceselor şi fenomenelor din sfera de securitate.

Incapacitatea naţiunilor de a gestiona problemele societale, în beneficiul populaţiei, creşte valoarea ameninţărilor la adresa infrastructurilor critice, iar componenta militară este solicitată să planifice şi să execute operaţii de răspuns la criză non Articol 5 (NA5CRO).

Determinările comportamentelor fiecărui factor de securitate politic, militar, economic, social, informaţional şi de infrastructuri pot fi analizate individual şi în funcţie de gradul de interdependenţă funcţională a rolului infrastructurilor care le susţin.

The complexity of the contemporary operational environment is generated by the multitude of factors of influence that, through their actions or states of affairs, provide those points of equilibrium or imbalance of the processes and the phenomena in the scope of security. In this context, the transition from normality to an inevitable state of crisis or war could be anticipated due to the changes in the "status parameters" of certain "responsible systems".

The failure of nations to manage societal problems for the benefit of the population increases the occurrence of threats to critical infrastructure, and the military component is required to plan and execute non-Article 5 crisis response operations (NA5CRO). This is a direct result of a comprehensive approach to the political, military, economic, social, informational and infrastructural security factors, which have a specific manifestation in a crisis or military conflict.

The determination of the behaviors of each security factor can be analyzed individually and depending on the degree of functional interdependence of the role of the infrastructures that support them.

La complexité de l'environnement opérationnel contemporain est le résultat d'une multitude de facteurs d'influence qui, par leurs actions ou leurs états réels, donnent ces points d'équilibre ou de déséquilibre des processus et des phénomènes dans le domaine de la sécurité.

L'incapacité des pays à gérer les problèmes sociétaux, au profit de la population, augmente l'effet des menaces pesant sur les infrastructures critiques, et la composante militaire est nécessaire pour planifier et mener des opérations de réponse aux crises ne relevant pas de l'article 5 (NA5CRO).

Les déteminations du comportement de chaque facteur de sécurité politique, militaire, économique, social, d'information et de l'infrastructure peuvent être analysées individuellement et en fonction du degré d'interdépendence fonctionnelle du rôle des infrastructures qui les soutiennent.

Cuvinte-cheie: securitate; criză; conflict militar; infrastructuri critice; NA5CRO; vulnerabilităţi.
Keywords: *security; crisis; military conflict; critical infrastructures; NA5CRO; vulnerabilities.*
Mots-clés: *sécurité; crise; conflit militaire; infrastructure critique; NA5CRO; vulnérabilité.*

Universitatea Națională de Apărare „Carol I”
e-mail*: danutroman2@yahoo.com*

Complexitatea mediului de securitate contemporan sub incidenţa NA5CRO

Pentru definirea stării de normalitate la nivelul unei societăţi, specialiştii din domeniul securităţii au identificat o serie de parametri descriptibili pe baza cărora sunt prezentate tendinţele de evoluţie viitoare a statului sau a unei regiuni, ca subiect de analiză de securitate distinct.

Din cauza modificărilor substanţiale şi a celor subtile din planul de securitate internaţional, lista parametrilor descriptibili reclamă ajustări permanente. Cunoaşterea situaţiei, ca fază distinctă a procesului de prevenire şi de contracarare a unei situaţii de criză, reprezintă un complex de activităţi desfăşurate permanent. Realizarea monitorizării, înregistrării rezultatelor şi interpretării acestora privind starea de fapt a unui stat sau a unei regiuni este responsabilitatea fiecărei instituţii cu atribuţii în domeniul securităţii, şi nu numai. Sub aspectul lucrului interinstituţional, construcţia „imaginii de ansamblu” privind cunoaşterea situaţiei reprezintă un atribut dificil de repartizat unui anumit factor de responsabilitate. Pentru aceasta, au fost desemnate acele instituţii care, în baza profilului acţional, formulează informări şi iau măsuri specifice din responsabilitatea fiecăreia privind menţinerea sectoarelor de securitate în parametri funcţionali.

un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre, care este esenţial pentru menţinerea funcţiilor societale vitale, sănătăţii, siguranţei, securităţii, bunăstării sociale sau economice a persoanelor, şi a cărui perturbare sau distrugere ar avea un impact semnificativ într-un stat membru, ca urmare a incapacităţii de a menţine respectivele funcţii”. Datorită algoritmului de nominalizare a infrastructurilor critice, respectiv de îndeplinire a criteriilor sectoriale, deducem faptul că fiecare componentă de securitate poate conţine, la un anumit moment dat, cel puţin o infrastructură critică. Din descrierea fiecărei infrastructuri, desemnată ca fiind critică, şi pe baza apartenenţei acesteia la un anumit domeniu de securitate, a conexiunilor acestuia cu alte domenii proprietare de infrastructuri critice, pot fi realizate scheme ale interdependenţelor dintre acestea.

În urma realizării legăturilor de interdependenţă dintre domeniile de securitate, rezultă o structură de securitate nouă, caracterizată printr-un grad de complexitate ridicat, cu o mărime de suprafaţă fizică concretă şi, sub aspect nematerial, mult mai greu de definit. Din natura relaţiilor dintre domeniile de securitate responsabile şi gradul de conectare al acestora, rezultă o serie de legături şi de noduri de conectare, care evidenţiază legăturile

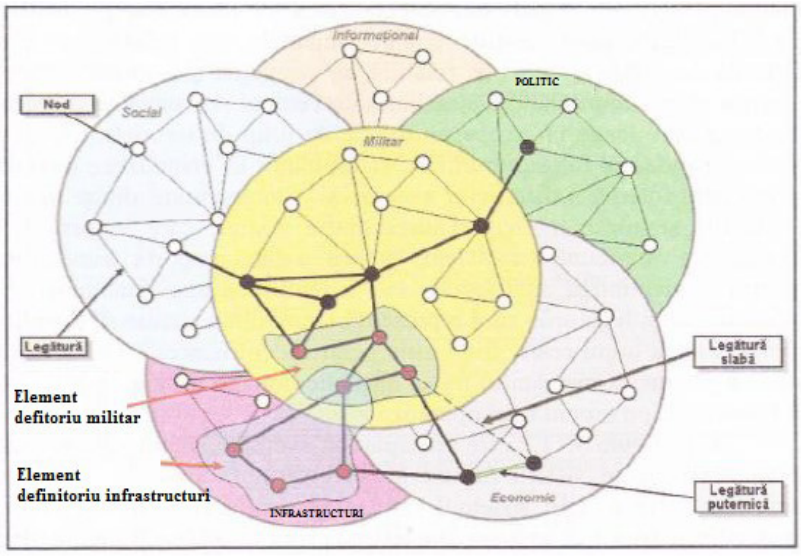

Fig. 1 *Variantă de reprezentare a interdependenţelor dintre domeniile de securitate cu proprietate asupra infrastructurilor critice*

Au fost identificate o serie de criterii în baza cărora sunt desemnate infrastructurile critice[1]. Aşa cum este definită în cadrul Directivei 114/2008 a Uniunii Europene, o infrastructură critică „*înseamnă* dintre elemente ca fiind definitorii pentru relaţiile de interconectare, ca în figura 1. Elaborarea unei perspective sistemice pe bază de reţea asupra relaţiilor dintre domeniile desemnate, cum ar

fi dintre proprietarii de infrastructuri critice, ne poate ajuta, ulterior, să identificăm raporturile de cauzalitate, efecte şi consecinţe, care stau la baza formării şi evoluţiei unei crize sau a unui eveniment negativ cu impact major.

Din perspectiva factorului de securitate militar, au fost identificate acele situaţii care reclamă capabilităţi specifice structurilor militare ce trebuie să acopere nevoia de răspuns la o criză, dincolo de conceptul de „apărare colectivă”, aflat sub incidenţa Articolului 5 al Tratatului Atlanticului de Nord. Formulat prima dată în Conceptul Strategic 1991 şi reiterat apoi în Summitul de la Washington, din 1999, principalul pilon al NATO privind întrebuinţarea structurilor militare în operaţii de răspuns la crize, nonarticol 5 (NA5CRO), se referă la planificarea şi executarea altor tipuri de misiuni, care nu sunt cuprinse în Articolul 5, inclusiv cele care contribuie la prevenirea eficientă a conflictelor. Legăturile fizice sau nemateriale – cum ar fi cele din spaţiul cibernetic, dintre domeniile de securitate – generează implicaţii majore cu privire la protecţia infrastructurilor critice şi la cauze declanşatoare ale unei potenţiale crize sau la degenerarea în conflict militar a unui eveniment negativ cu impact major asupra mediului înconjurător sau asupra populaţiei. Astfel, misiunea militară a NA5CRO este concentrată pe contribuţia la managementul eficient al crizelor, încă din situaţiile în care nu este evidentă o ameninţare directă pentru naţiunile sau teritoriul NATO. Afectarea mediului de securitate poate fi realizată fie prin ameninţări directe sau indirecte, fie prin afectarea acelor infrastructuri, cum ar fi cele desemnate critice. Acest lucru implică o relaţie de cauzalitate biunivocă între statusul componentei militare şi cel al infrastructurilor critice. În cadrul NATO, participarea unor structuri militare la operaţii NA5CRO este condiţionată de îndeplinirea mai multor criterii[2], dintre care ne referim la:

- existenţa unor ameninţări la adresa păcii şi securităţii, recunoscută internaţional de către ONU, OSCE sau de alte organizaţii de securitate;
- existenţa unui proces legitim de reglementare politic, prin care să se încerce rezolvarea conflictului;
- producerea unor catastrofe de mari proporţii, care afectează în mod grav funcţionalitatea instituţiilor statului etc.

Din formularea criteriilor de realizare a intervenţiei militare NA5CRO, conform doctrinei la care m-am referit, rezultă acele situaţii în care este afectată în mod grav funcţionalitatea instituţiilor statului, natura factorilor destabilizatori şi a consecinţelor rezultate din acţiunile acestora. Războiul hibrid poate fi una dintre situaţiile în care forţele armate pot întâlni o gamă largă de adversari, diferiţi din punctul de vedere al intenţiilor şi al modurilor de acţiune al acestora. Adversarii pot desfăşura acţiuni convenţionale sau neconvenţionale, care, pentru a-şi îndeplini obiectivele, vor acţiona în orice fel de combinaţie, cum ar fi exploatarea efectelor unor calamităţi naturale (cutremure, tsunami, inundaţii etc.) sau a dezastrelor provocate de om (incendii, accidente industriale etc.). Din perspectiva situaţiilor la care m-am referit, precum şi a posibilităţii implicării componentei militare sub incidenţa NA5CRO, apariţia şi dezvoltarea unei potenţiale crize pot fi generate de însăşi natura legăturilor şi a nodurilor de reţea dintre domeniile de securitate, conform figurii 1. Deşi este realizată ca o reţea a condiţionărilor dintre elementele componente, eficienţa unei astfel de „reţele de securitate” nu poate fi explicată în termeni integratori din perspectiva legilor de guvernare ale acesteia. Acest lucru va fi greu de realizat, din cauza complexităţii elementelor componente şi a comportamentului imprevizibil al acestora, în situaţii de criză sau de materializare a unui eveniment cu impact major asupra populaţiei.

Aspecte ale NA5CRO privind protecţia infrastructurilor critice

Aşa cum au fost definite, infrastructurile critice reprezintă componenta vitală a unui stat sau a unui ansamblu de state, care, în orice împrejurare, trebuie protejate şi apărate cu prioritate. Sub aspectul protecţiei infrastructurilor critice, cauzele declanşatoare ale unui incident pot fi de natură dual, atât factori interni, cât şi factori externi. Din proiectarea şi punerea în funcţiune a oricărei infrastructuri, desemnată ca fiind critică, securitatea acesteia este asigurată de o serie de sisteme şi de măsuri de securitate.

Totuşi putem vorbi despre o dificultate a menţinerii coerente a unei infrastructuri critice, la parametrii de securitate proiectaţi iniţial. Acest lucru este confirmat de situaţiile care au avut loc şi care au afectat grav o serie de infrastructuri critice, considerate iniţial indestructibile. În

urma descrierilor legăturilor sistemice dintre componentele reţelei de securitate, structurile militare la nivel NATO sunt proiectate să răspundă deopotrivă atât solicitărilor de apărare colectivă pentru realizarea garanţiilor reciproce, prevăzute de Articolul 5, cât a celor prezentate conform NA5CRO.

Cauzele multiple şi complexe care stau la baza izbucnirii unei situaţii de criză sau a unui conflict militar demonstrează existenţa dificultăţilor legislative pentru încadrarea acţiunii militare în cuprinsul sau în afara Articolului 5. Referitor la sistemul de securitate, la modul de operare al acestuia, se impun revizuiri legislative permanente care să coreleze acţiunile tuturor actorilor cu responsabilităţile din acest domeniu, inclusiv ale celui militar. Astfel, comportamentul fiecărei componente cheie a sistemului de securitate va influenţa decisiv comportamentul celorlalte componente de securitate, lucru care poate constitui provocarea sau alimentarea unei situaţii de criză.

În concepţia NATO, măsurile de management al crizelor asigură elementele necesare planificării şi execuţiei misiunilor specifice structurilor militare, în toate situaţiile. Existenţa infrastructurilor critice, desemnate în cadrul mai multor domenii instituţionalizate, determină o integrare operaţională a acestora şi includerea lor în sistemul de prevenire şi contracarare a conflictelor şi crizelor. În acest context, NATO declanşează şi desfăşoară procesul specific de management al crizelor, care cuprinde un spectru complet de măsuri ce asigură reacţia oportună şi coordonată a instrumentului militar. Acest proces specific de management al crizelor are şase faze succesive, corelate în cadrul Sistemului de Răspuns la Crize – NCRS (NATO Crisis Response System)[3] –, astfel:

- faza 1 – indiciile şi avertizarea despre o criză curentă sau potenţială;
- faza 2 – evaluarea dezvoltărilor sau reevaluarea unei situaţii de criză în desfăşurare, a potenţialului sau implicaţiilor acesteia asupra securităţii naţionale;
- faza 3 – elaborarea opţiunilor militare de răspuns, recomandate în sprijinul procesului de decizie a organelor naţionale abilitate;
- faza 4 – planificarea;
- faza 5 – executarea deciziilor şi directivelor organelor naţionale abilitate;
- faza 6 – tranziţia şi încheierea rolului în managementul crizei.

Parcurgerea coerentă a celor şase faze ale procesului de management al crizelor include atât componenta militară, cât şi celelalte instituţii cu atribuţii directe şi indirecte în sistemul de securitate. La declanşarea procesului de management al crizei, în faza 1, contribuie toate elementele de securitate desemnate, care sunt interconectate, după modelul de reţea prezentat în prima parte a articolului. Un aspect deosebit de important al acestei faze este dat de capacitatea de lucru sau de performanţa fiecărei componente de a identifica şi de a formula corect indicii reale şi de avertizare despre criză. Mă refer la faptul că, la nivelul fiecărei componente de securitate, pot apărea provocări la adresa valorilor esenţiale sau de percepţie privind nominalizarea crizei. Aceste percepţii pot avea la rândul lor impact diferit asupra factorului decident, pot chiar provoca ori alimenta o criză sau un conflict.

Una dintre situaţiile ipotetice declanşatoare de criză poate fi afectarea unei anumite infrastructuri critice de pe teritoriul unui stat sau al unei regiuni. Trebuie reamintit faptul că infrastructurile sunt acele elemente identificate, care realizează „suportul” real al societăţilor/statelor în ansamblul lor. În funcţie de rolul şi de anvergura acestora, infrastructurile sunt clasificate în: infrastructuri obişnuite, infrastructuri speciale şi infrastructuri critice.

Această clasificare pune accent pe rolul infrastructurilor şi importanţei acestora. Elementul distinctiv al infrastructurilor critice este acela că ele asigură funcţiile vitale ale unei societăţi, care, prin afectarea lor, ar produce pagube majore, astfel încât s-ar periclita buna desfăşurare a vieţii cotidiene. În funcţie de gradul de afectare al infrastructurilor critice, specialiştii în domeniu au identificat gradual mai multe praguri critice, peste care o societate nu îşi mai poate reveni la starea de normalitate. Modalitatea de traversare a unei situaţii de criză de către un stat sau o regiune poate fi clasificată în funcţie de gradul de afectare a infrastructurilor critice desemnate.

Prin urmare toate componentele de securitate ale unui stat sunt implicate în gestionarea situaţiilor infrastructurilor critice din zona de responsabilitate afectată. Componenta militară, datorită capabilităţilor sale privind apărarea şi puterea distructivă, este direct implicată în afectarea sau protecţia infrastructurilor critice, pe timp de pace, de criză sau de război.

Un alt aspect privind protecţia infrastructurilor critice, în context NA5CRO, se referă la elaborarea şi punerea în aplicare a opţiunilor militare de răspuns. Managementul consecinţelor unor acţiuni militare în proximitatea fizică a unor componente economice sau a celor de securitate, desemnate infrastructuri critice, cuprinde relaţionarea şi realizarea lucrului colaborativ al tuturor instituţiilor şi actorilor implicaţi în gestionarea situaţiei de criză sau de conflict militar.

Caracteristicile identificate, specifice tipologiei de război hibrid, arată faptul că acţiunile militare şi cele de securitate nu pot fi abordate izolat. Într-o societate funcţională, instrumentele de putere naţională (diplomatic, informaţional, economic şi militar) sunt completate şi susţinute de celelalte componente societale: sistemul juridic, sistemul educaţional, structurile interne ale guvernării naţionale şi locale, sectorul comercial, sectoarele energetic şi de furnizare a apei potabile, instituţiile destinate asigurării bunăstării şi sănătăţii populaţiei. Deci formularea opţiunilor militare de răspuns implică, în funcţie de situaţie, soluţii atât adecvate Articolului 5, cât şi din domeniile NA5CRO.

Pentru susţinerea ambelor categorii de soluţii, componenta militară nu poate proiecta singură acţiuni fără suportul resurselor din economie (hrană, echipament, energie etc.). Studiile privind dependeţele critice ale tuturor componentelor de securitate, la nivelul unui stat sau al Alianţei, au demonstrat rolul incontestabil al infrastructurilor critice, cum ar fi: energie, finanţe, transporturi, cibernetică. În funcţie de particularităţile fiecărei infrastructuri critice, o parte este implicată fizic şi în mod direct, iar altă parte, imaterială, prin afectare din locaţii necunoscute şi de la mare distanţă, cum ar fi atacurile cibernetice.

Pentru exemplificare, managementul consecinţelor unui atac cibernetic simultan asupra componentelor de securitate, la nivelul unui stat sau al Alianţei, poate pune în pericol ireversibil statul sau regiunea. Includerea ori excluderea componentei militare în acest management al consecinţelor poate duce la o transformare radicală a geometriei reţelei de securitate, a legăturilor dintre elementele reţelei şi a importanţei nodurilor de decizie.

Prin urmare proiectarea măsurilor de prevenire a unei crize sau de evitare a unui conflict militar se referă la înţelegerea vulnerabilităţilor fiecărei componente de securitate. Vulnerabilităţile pot fi identificate doar în formularea şi în descrierea cât mai realistă a contextului în care ameninţările se pot materializa în evenimente negative cu impact major.

În figura 2 sunt reprezentate două situaţii ipotetice ale determinărilor privind afectarea componentei cibernetice. În baza managementului de risc, sunt reprezentate desfăşurări ale proceselor în flux normal/neafectate (căsuţele albe) şi cele

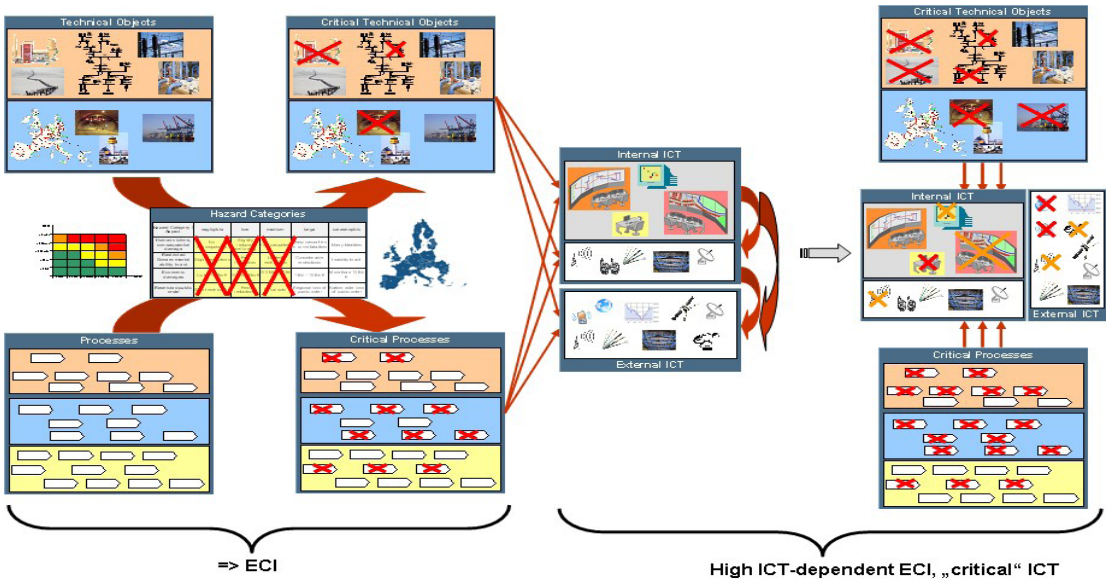

Fig. 2 *Reprezentare schematică a dependenţelor cibernetice normale şi a celor „critice”, la nivelul componentelor funcţionale ale unui stat sau ale unei regiuni*[4]

avariate (căsuţele bifate cu „x” roşu). Cauzele afectărilor pot fi multiple: întreruperi ale alimentării cu energie electrică, datorate cutremurelor, inundaţiilor etc. sau provocate, cum ar fi atacurile cibernetice.

Gradul consecinţelor unor astfel de afectări sunt apreciate în funcţie de natura componentelor de securitate avariate. Desigur, amploarea unor astfel de determinări este mult mai mare. De exemplu, pot fi înregistrate anumite afectări prin scoaterea din funcţiune a unor componente de securitate sau prin lipsa furnizării anumitor produse ori servicii.

O cu totul altă afectare este atunci când anumite componente de securitate sunt menţinute în lucru, dar deviate în direcţia obţinerii altor rezultate sau programate la alţi parametri de funcţionare, ceea ce poate duce la accidente industriale (explozia unei centrale atomoelectrice sau lansarea accidentală a unor rachete balistice).

Expertiza anumitor componente de securitate în domenii de interes comun, cum ar fi cel cibernetic, poate fi exploatată de toate elementele de securitate conectate la aceeaşi reţea colaborativă, despre care am vorbit anterior. În funcţie de situaţia creată, de afectarea anumitor infrastructuri critice, activarea componentei militare privind soluţionarea unei crize sau a anumitor secvenţe ale acesteia presupune incidenţa NA5CRO. Această incidenţă implică planificarea şi desfăşurarea operaţiilor de diverse tipuri, care reies din cadrul Articolului 5 şi care contribuie la prevenirea şi rezolvarea conflictelor, la managementul crizelor sau servesc scopurilor umanitare pentru îndeplinirea obiectivelor declarate ale Alianţei. Statele nu sunt obligate să ia parte la operaţii NA5CRO, potrivit documentelor politice/strategice ale NATO, care clasifică aceste operaţii ca operaţii în sprijinul păcii. Însă protecţia infrastructurilor critice reclamă obligativitatea părţilor deţinătoare de infrastructură critică să intervină, în situaţia unei afectări a stării de siguranţă a statului vecin sau a mai multor state (posibilitatea producerii unei pene majore de curent electric sau o explozie la o centrală atomo-electrică).

În acest context, NA5CRO, în privinţa protecţiei infrastructurilor critice, acoperă o gamă diversă de acţiuni militare, de la operaţii de sprijin, asociate în primul rând agenţiilor civile, la operaţii în sprijinul păcii, combaterea ameninţărilor asimetrice şi acţiuni de luptă (intervenţii contraterorismului). Într-o abordare mult mai cuprinzătoare, acţiunile NA5CRO, conduse de NATO, pot fi, printre altele, operaţii de extracţie, misiuni de sprijin în situaţii de urgenţă şi operaţii umanitare, căutare-salvare sau sprijin pentru operaţiile de evacuare a noncombatanţilor, operaţii de asigurare a libertăţii de navigaţie, de impunere a zonelor de interdicţie aeriană, a sancţiunilor şi a embargoului, de sprijin pentru misiuni de stabilizare şi de reconstrucţie, respectiv operaţii de impunere a păcii şi de contrainsurgenţă.

Ceea ce se poate observa din multitudinea misiunilor care pot fi îndeplinite de către componenta militară, sub incidenţa NA5CRO, protecţia infrastructurilor critice se regăseşte în centrul de atenţie al acestor misiuni. Gestionarea unei situaţii de criză sau de conflict armat care scapă de sub control afectează în mod direct capacitatea de protecţie a infrastructurilor, indiferent de natura acestora, ceea ce poate duce la consecinţe dintre cele mai grave la nivel societal, cum ar fi abandonul total al teritoriului şi existenţa migraţiilor în masă ale populaţiilor către alte regiuni. Implicit, în acest caz, pot apărea suprapopulări ale regiunilor, care, asociate cu alte cauze, pot duce la conflicte, cum ar fi cele de natură etnică, culturală sau religioasă.

Concluzii şi propuneri

Subiectul protecţia infrastructurilor critice, în context NA5CRO, reprezintă punctul de plecare privind înţelegerea nevoii de redefinire a rolului fiecărei componente a sistemului de securitate. Printre ameninţările posibile, care reclamă operaţii de răspuns la criză ale componentei militare, se pot regăsi şi efecte ale fenomenelor naturale, cum ar fi cutremurele de pământ, inundaţiile, erupţiile vulcanice şi alte calamităţi naturale, precum şi dezastrele provocate de om, cum ar fi accidentele industriale, incendiile, poluările mediului de orice fel etc.

Efectele fenomenelor naturale la care m-am referit, prin afectarea gravă a infrastructurilor critice, pot fi cauze directe ale declanşării unei crize sau pot determina iniţierea de noi conflicte ori activarea celor îngheţate. Datorită rolului fundamental pe care îl au în societatea modernă, infrastructurile critice rămân ţinte potenţiale ale factorilor societali destabilizatori, cum ar fi organizaţiile teroriste, care, prin acţiunile lor, pot constitui, la un moment dat, cauza principală a unei crize sau a unui conflict militar.

Protecţia infrastructurilor critice, în context NA5CRO, se referă la modalitatea generală de abordare a acesteia, în toate fazele procesului specific de management al crizelor. Acest lucru este susţinut de faptul că toate componentele de securitate, şi nu numai, au sau pot avea în proprietate una sau mai multe infrastructuri critice desemnate. Afectarea acestor infrastructuri, indiferent de destinaţia lor, atrage după sine reacţii de afectare în lanţ şi a altor componente sau sisteme de securitate. Prin urmare este necesară aprofundarea raporturilor de influenţă a fiecărei componente de securitate, cu acele infrastructuri aflate în relaţii de condiţionare, indiferent de natura acestora (simple, speciale sau critice).

Exemplific situaţia instituţiilor Estoniei, în urma atacurilor cibernetice, din 2007, asupra infrastructurii informaţionale[5]. Respectivele atacuri cibernetice au afectat site-urile de Internet, sistemele de comunicaţii, domeniul bancar şi integritatea sistemelor informatice ale cetăţenilor, pagubele fiind estimate la zeci de milioane de euro. Prin urmare forurile competente în domeniul securităţii au demarat proceduri legislative specifice privind acţiunile în spaţiul cibernetic.

Într-o stare de fapt, apărarea cibernetică s-a constituit ca unul dintre domeniile comune ale tuturor componentelor de securitate, dar şi ca o reacţie imediată de protecţie a infrastructurilor critice, conform reprezentării din figura 2.

În urma dezvoltării conceptului de reţea integrată privind lucrul componentelor de securitate la nivelul unui stat sau de Alianţă, se impun noi modalităţi de transfer al autorităţii privind gestionarea unor situaţii de criză sau de conflict militar. Astfel, putem anticipa faptul că rolul infrastructurilor critice va creşte exponenţial, pe măsura afectării acestora şi a stabilirii nivelului existent de pagube materiale şi pierderilor de vieţi omeneşti.

Una dintre soluţiile identificate în acest sens constă în proiectarea şi operaţionalizarea acelor reţele de lucru colaborativ, în care sunt integrate toate componentele de securitate, indiferent de statutul acestora, privind proprietatea asupra infrastructurilor critice.

O altă direcţie de proiectare şi de realizare a infrastructurilor cu rol decisiv societal poate fi introducerea acestora în planurile de apărare şi de contracarare a acţiunilor de tip terorist. Acest lucru se impune, ca urmare a diversificării formelor şi mijloacelor de manifestare a fenomenului terorist (SUA, 11 septembrie 2001) sau în cazul erorilor acţiunilor militare, din zonele de conflict (Ucraina, Zborul 17 al Malaysia Airlines).

Ca o consecinţă directă, apare necesitatea unei perfecţionări a programelor de formare şi pregătire a personalului specializat în domeniul acţiunilor NA5CRO, respectiv a ofiţerului de legătură pentru protecţia infrastructurilor critice. Acest lucru poate fi realizat prin implementarea unor programe comune de pregătire a specialiştilor din domeniul securităţii şi prin realizarea unei platforme de lucru colaborativ, destinată exclusiv generării şi testării vulnerabilităţilor şi riscurilor mai multor infrastructuri, în baza unor scenarii comune.

În încheiere, se poate aprecia faptul că protecţia infrastructurilor critice reprezintă o combinare a măsurilor şi a planurilor de apărare cu cele de contracarare/ofensive în toate domeniile de securitate, prin aplicarea metodelor şi mijloacelor adecvate, aflate sub incidenţa NA5CRO. Este de aşteptat, în acest sens, o transformare a măsurilor legislative şi o adaptare a acestora la nivelul tehnologiilor de ultimă oră, pentru contracararea noilor vulnerabilităţi şi ameninţări, rezultate din posibilităţile de agresiune şi de comitere a actelor de terorism sau a erorilor umane, din zona infrastructurilor critice desemnate.

NOTE:

1 Peter Gattinesi, colectiv, *JRC TECHNICAL REPORTS European Reference Network for Critical Infrastructure Protection, Luxembourg*, Publications Office of the European Union, ERNCIP Handbook 2017 edition, pp. 6-12.

2 Alexandru Rus, colectiv, *Doctrina privind participarea la operaţii de răspuns la crize non-articol 5*, Editura SMG, Bucureşti, 2013, pp. 9-10.

3 Liviu Şerban, colectiv, *Doctrina Armatei României*, Editura SMG, Bucureşti 2012, p. 73.

4 Stephan Gottwald, colectiv, *Final report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ITC Infrastructure*, Industrieanlagen-Betriebsgesellschaft (IABG), Berlin Office, 2011, p. 20.

5 https://www.cssp.ro/analize/2012/10/01/atacurile-cibernetice-din-estonia-2007/, accesat la 02.04.2018.

BIBLIOGRAFIE

*** *Ghidul Strategiei Naţionale pentru Apărare a Ţării pentru perioada 2015-2019*, document aprobat prin Hotărârea Consiliului Suprem de Apărare a Ţării nr. 128, din 10 decembrie 2015.

*** *Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor privind protecţia infrastructurilor critice de informaţie*, Bruxelles, 2009, http://ec.europa.eu/transparency/regdoc/rep/1/2009/RO/1-2009-149-RO-F1-1.Pdf

*** *Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora*, Bruxelles, 2008, http://ccpic.mai.gov.ro/docs/directiva114_RO.pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF

Alexandrescu Grigore; Văduva Gheorghe, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.

Drack Manfred, „Ludwig von Bertalanffy's early system approach”, in *Systems Research and Behavioral Science*, Volume 26, Issue 5, September/October 2009, http://journals.isss.org/index.php/proceedings52nd/article/viewFile/1032/322.

Gattinesi Peter, *JRC TECHNICAL REPORTS European Reference Network for Critical Infrastructure Protection*, Luxembourg, Publications Office of the European Union, ERNCIP Handbook 2017 edition.

Gottwald Stephan, colectiv, *Final report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ITC Infrastructure, Industrieanlagen-Betriebsgesellschaft (IABG)*, Berlin Office, 2011.

Robbins P. Stephen, *Organizational Theory: Structure, Design, and Applications, Prentice Hall*, New Jersey, 1990.

Rus Alexandru, colectiv, *Doctrina privind participarea la operaţii de răspuns la crize non-articol 5*, Editura SMG, Bucureşti, 2013.

Şerban Liviu, colectiv, *Doctrina Armatei României*, Editura SMG, Bucureşti 2012.

The White House, *Executive Order 13010: Critical Infrastructure Protection*, 15 July 1996, http://fas.org/irp/offdocs/eo13010.htm.

https://www.cssp.ro/analize/2012/10/01/atacurile-cibernetice-din-estonia-2007/

http://www.mediafax.ro/externe/sistemul-informatic-ale-unei-centrale-nucleare-din-sua-afectat-de-un-atac-cibernetic-16524844

http://intelligence.sri.ro/cyber-noul-domeniu-operational-nato/

https://www.recordedfuture.com/russia-ukraine-cyber-front/