UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I“
Centrul de Studii Strategice de Apărare şi Securitate

Proiectul: CEEX-M1-4044-GESTIONARE CF-16/2006
„SECURITATEA SISTEMELOR ŞI ACȚIUNILOR MILITARE ŞI CIVIL-MILITARE ÎN GESTIONAREA CRIZELOR ŞI CONFLICTELOR ARMATE“

Etapa 1. ***Dezvoltarea unei baze de date şi a unei metodologii de analiză a crizelor şi conflictelor armate*** *pentru: cunoaşterea şi aprofundarea fenomenului crizelor şi conflictelor armate*

DEFINIREA CRIZELOR ŞI CONFLICTELOR ARMATE ÎN NOUA CONFIGURAȚIE A FILOSOFIEI ŞI FIZIONOMIEI NAȚIONALE ŞI INTERNAȚIONALE DE REȚEA

- studiu -

Termen: 29 septembrie 2006

BUCUREŞTI
- 2006 -

ECHIPA DE CERCETĂTORI

1. General prof. univ. dr. MUREŞAN MIRCEA, conducător de proiect
2. General de brigadă (r) dr. CS I VĂDUVA GHEORGHE, director de proiect
3. Colonel (r) dr. CS I MOŞTOFLEI CONSTANTIN, executant
4. Colonel (r) dr. CS I DOLGHIN NICOLAE, executant
5. Colonel (r) dr. CS I ALEXANDRESCU GRIGORE, executant
6. Colonel (r) dr. CS II PETRE DUŢU, executant
7. Colonel (r) CS POPA VASILE, executant
8. Cercetător ştiinţific drd. SARCINSCHI ALEXANDRA, executant
9. Cercetător ştiinţific drd. BĂHNĂREANU CRISTIAN, executant
10. Cercetător ştiinţific drd. DINU MIHAI, executant
11. Locotenent colonel dr. ENACHE DORU, executant
12. Cercetător ştiinţific drd. RĂDUICĂ GEORGE, executant
13. Cercetător ştiinţific drd. MĂLESCU SIMONA-VALENTINA, executant
14. VLADU CORINA, executant
15. CUCU IRINA, executant
16. ATANASIU MIRELA, executant
17. Locotenent RĂDUICĂ SORINA, consilier juridic, executant
18. MIHAI DOINA, executant

CUPRINS

ARGUMENT

Crizele şi conflictele armate fac parte din viaţa societăţii omeneşti, sunt expresii ale complexităţii şi imperfecţiunilor acesteia. Au cauze dinamice şi complexe şi, la rândul lor, sunt sau devin cauze, la fel de dinamice şi de complexe, pentru alte fenomene şi procese care ţin de viaţa oamenilor, a comunităţilor omeneşti, de tot ceea ce presupune muncă, efort, creaţie, înfăptuire şi efect al activităţii omeneşti, sistem şi proces. Crizele nu sunt doar desfăşurări lineare, nici simple disfuncţii. Ele au fost, sunt şi, probabil, vor fi totdeauna tensiuni complicate, acumulări în labirint, revărsări sau desfăşurări multiforme, de regulă nelineare şi chiar haotice, tot atât de diversificate şi de complexe cum este însăşi societatea care le generează, le gerează şi le adăposteşte.

Uneori, crizele şi conflictele armate sunt privite şi tratate ca o fatalitate. Ne este dat să le trăim şi trebuie să le trăim, nu avem ce face. Li se dă, implicit, aura de fenomene ce depăşesc oamenii şi voinţa acestora, precum cutremurele, inundaţiile, revărsările de ape, avalanşele, uraganele... Alteori, sunt considerate disfuncţii datorate imperfecţiunilor şi greşelilor omeneşti, pe care trebuie să le suportăm şi să le plătim cu toţii, în virtutea acelui *e pluribus unum*, a solidarităţii umane la bine şi la greu. De foarte multe ori, sunt considerate şi deficienţe, lipsuri, scăderi drastice, neîmpliniri.

Crizele şi conflictele armate sunt privite şi ca un rău necesar, sau ca un exces de rău, ca un efect de rău sau ca o invazie dramatică a răului, precum invaziile repetate şi intempestive de lăcuste de odinioară, ca o revărsare a acestuia peste viaţa şi liniştea oamenilor şi a spaţiului lor de viaţă şi de muncă. Crizele mai pot fi privite şi ca implozii ale societăţii omeneşti, ca surpări şi reaşezări de structuri, relaţii şi sisteme.

Dar crizele mai au şi o altă latură foarte importantă. Ele sunt treceri la limită, dincolo de limită, generate de atingerea unui nivel maxim de funcţionalitate a unui sistem (proces) şi de necesitatea transformării radicale a acestuia, trecerii lui la o altă calitate, la o altă stare, sau înlocuirii lui cu un alt sistem (proces).

Desigur, toate acestea şi multe alte modalităţi de a privi, cunoaşte, înţelege şi defini crizele şi conflictele armate rămân, într-un fel, simplificate şi chiar exterioare nu doar fenomenului care le incumbă, ci şi esenţei acestuia. Crizele nu pot fi detaşate sau separate cu uşurinţă de mediul în care se produc, fie chiar şi numai pentru a fi studiate, şi, de aceea, rareori ele pot fi înţelese în toată profunzimea, amplitudinea şi implicaţiile lor şi, pe această bază, soluţionate la timp şi complet. De cele mai multe ori, efectele depăşesc cauzele, prin incertitudini şi desfăşurări haotice, greu de înţeles şi de controlat, iar lanţul determinărilor se rupe în multe locuri şi nu se mai lasă refăcut. Ce s-a distrus rămâne totdeauna distrus. Dar oamenii au capacitatea şi vocaţia sisifică de a o lua totdeauna de la capăt. Crizele şi conflictele armate le tulbură viaţa, le dezgolesc caracterele malefice şi provizoratele, tarele şi vulnerabilităţile, dar tot ele îi determină pe oameni să-şi reconstruiască mereu mediul, ca furnicile pământului sau ca entităţile Universului.

Crizele şi conflictele armate sunt efecte de distonanţă şi de falie ale insecurităţii sistemelor şi proceselor şi, la rândul lor, devin cauze, sisteme şi procese generatoare de insecuritate. Cu cât ele sunt mai numeroase, mai complexe şi mai greu de gestionat, cu atât insecuritatea sistemelor şi proceselor este mai accentuată. De unde rezultă, la o primă analiză, că a securiza sistemele şi procesele umane presupune, înainte de toate, a controla, a gestiona şi, mai ales, a dezamorsa crizele şi conflictele armate. Or, după cum bine se ştie, acest obiectiv permanent al activităţii omeneşti – realizarea securităţii şi securizării sistemelor şi proceselor, întrucât totdeauna oamenii au avut şi vor avea

nevoie de securitate – nu poate fi niciodată realizat pe deplin. Totdeauna va exista un grad mai mare sau mai mic de insecuritate, generat tocmai de dinamismul complex al vieții, activității oamenilor, al configurării şi reconfigurării continue a societății omeneşti, din care crizele şi conflictele fac parte intrinsecă.

Securitatea este o stare dinamică de protecție şi siguranță a sistemului (procesului) şi, deci, o condiție a funcționării sistemului sau a desfăşurării procesului respectiv. Insecuritatea provine din imposibilitatea menținerii unei astfel de stări totdeauna în parametri optimi, care să asigure stabilitatea şi funcționalitatea sistemului în orice condiții.

Starea de securitate maximă este o stare ideală. Ea nu se poate realiza niciodată, întrucât sistemul (procesul) se află într-o strictă dependență de condițiile concrete (şi chiar de condițiile inițiale) şi variază în funcție de aceste condiții. Există o mulțime de factori care influențează starea sistemului şi, implicit, şi starea lui de securitate. Unii sunt de natură internă, alții sunt exteriori. Totdeauna aceşti factori acționează în mod complex, unii sporind vulnerabilitățile sistemului, alții amplificând pericolele şi amenințările la adresa lui. Se poate realiza doar un maximum posibil de securitate a sistemului sau procesului în condițiile date.

Criza, ca şi conflictul armat şi războiul, face deci parte din viața oamenilor, a societății omeneşti. Ea reprezintă un moment (o perioadă) sau o succesiune lineară sau haotică de disfuncționalități în evoluția societății, care necesită soluții viabile, menite să asigure o schimbare, o reconstrucție sau o revitalizare a sistemelor şi proceselor deteriorate. Cauzele crizelor sunt complexe, iar rezolvarea lor ține de funcționalitatea socială, de filosofia şi fizionomia de sistem şi de proces, dar şi de o nouă filozofie a interdeterminărilor, filosofia de rețea. Această filozofie nu schimbă esența fenomenului crizelor şi conflictelor. Aduce însă elemente noi, unele favorabile procesului de cunoaştere şi de influențare a traiectoriei lor, altele defavorabile, generatoare de noi vulnerabilități, de noi pericole şi chiar amenințări. Deşi crizele şi conflictele au fost analizate în mod riguros, nu se cunosc şi, mai ales, nu se pot prevedea în totalitate şi în mod oportun toate cauzele care le generează, nici măcar cele esențiale.

Nici o societate omenească, din câte se cunosc până acum, nu s-a dezvoltat şi nu se dezvoltă linear. Viața unei societăți cunoaşte momente simetrice, care evoluează ca într-o oglindă, într-o arhitectură complementară, dar şi momente disproporționate, disimetrice, care fie se anulează reciproc, fie se amplifică reciproc, sporind gradul de insecuritate fizică şi socială. Majoritatea momentelor în dinamica socială sunt însă asimetrice, cu evoluții rapide şi stagnări, progrese şi regrese, dar care se compensează reciproc, situații normale, dar şi anormalități, schimbări bruşte, de cele mai multe ori dramatice, crize şi conflicte. Omenirea se luptă cu ele de la începutul existenței sale şi, probabil, această luptă va fi dusă până în ultima clipă a existenței umane. De aici nu rezultă că fenomenul crizelor şi conflictelor reprezintă neapărat o fatalitate, că oamenii sunt complet neputincioşi în fața lui şi trebuie să se resemneze, ci doar o realitate socială, politică, economică, informațională, militară etc. de care trebuie să se țină seama şi care poate fi şi trebuie să fie, în limita posibilului, controlată, ameliorată şi chiar prevenită.

Este posibil ca oamenii să nu mai fie victime inconştiente şi, adesea, indiferente ale crizelor, conflictelor şi războaielor, ci să folosească aceste fenomene şi aceste procese pentru a-şi ameliora propria condiție, a-şi securiza sistemele acționale şi procesele, pentru a grăbi procesele de modernizare şi a prelungi perioadele de prosperitate şi de stabilitate. Deja omenirea şi-a format unele abilități în ceea ce priveşte gestionarea crizelor şi conflictelor, inclusiv a conflictelor armate, şi, deşi nu a reuşit să rezolve nici măcar în parte problema conflictualității, a realizat, totuşi, paşi importanți

în prevenirea unor crize şi conflicte militare de mare amploare, cum ar fi cele de mare risc, aşa cum sunt cele ce se bazează pe întrebuințarea armelor de distrugere în masă (ADM) şi a altor mijloace.

Tratatele şi acordurile privitoare la asigurarea păcii şi securității planetei, la neproliferarea ADM, la interzicerea minelor şi altor mijloace de distrugere a ființei umane, la controlul armamentelor, activitatea ONU şi a altor organizații de securitate constituie expresii ale efortului omenirii de a pune sub control fenomenul crizelor şi conflictualității. Din păcate, fenomenul evoluează, iar măsurile de securitate economică, socială şi militară țin cu greu pasul. Vulnerabilitățile cresc o dată cu dezvoltarea societăților, simetric cu pericolele şi amenințările, astfel încât putem spune că cu cât o societate este mai dezvoltată şi mai sofisticată, cu atât ea devine mai vulnerabilă. Chiar dacă se cunoaşte foarte bine această relație, este foarte greu de gestionat realitățilr şi, mai ales, vulnerabilitățile. Mereu apar altele noi, de cele mai multe ori, în mod aleator, greu de anticipat şi de contracarat. Cu toate acestea, fenomenul crizelor şi conflictelor trebuie studiat, analizat, înțeles şi pus sub control. Toate instrumentele cunoaşterii pot fi folosite, într-o formă sau alta, pentru analiza, înțelegerea şi soluționarea crizelor şi conflictelor. Chiar dacă rezultatele nu vor fi totdeauna spectaculoase, ele nu vor lipsi. Studiind fenomenologia şi filosofia crizei, omenirea nu are decât de câştigat. Este şi rămâne cea mai mare provocare a tuturor timpurilor.

CAPITOLUL 1
FILOSOFIA ŞI FIZIONOMIA DE REŢEA

Sistemele şi procesele, cu toate determinările, cauzele şi efectele care le însoţesc, le definesc şi le generează, sunt interdependente. Au fost totdeauna aşa, dar nu totdeauna interdependenţele au avut aceeaşi configuraţie, chiar dacă totdeauna au avut aceleaşi principii şi aceeaşi filozofie. Pe măsură ce societatea omenească evoluează informaţional, tehnologic şi social, complexităţile se multiplică, iar interdependenţele sporesc. Într-un fel, entropia acestor sisteme şi procese creşte, pentru că şi nedeterminările cresc – totdeauna, în cadrul sistemelor şi proceselor haotice, indeterminările sunt mari, tind către limita maximă –, iar fenomenele se multiplică şi se complică. În pofida globalizării (care înseamnă, în primul rând, globalizare a informaţiei, prin amplificarea şi multiplicarea reţelei, apariţia reţelelor de reţele şi a unor mulţimi de microreţele), indeterminările nu se diminuează, ci, dimpotrivă, cresc, de unde rezultă că şi entropia creşte (informaţia fiind nedeterminare înlăturată), iar dinamismul şi complexitatea sistemelor şi proceselor se amplifică.

1.1. O nouă realitate structurală şi funcţională

Noua epocă deschisă după spargerea bipolarităţii politice, se caracterizează, între altele prin realităţi şi efecte contradictorii, chiar conflictuale, cu schimbări bruşte şi evoluţii nelineare şi imprevizibile. Reţeaua oferă posibilitatea circulaţiei rapide a datelor şi informaţiilor, dar acest lucru nu este totdeauna benefic. Este adevărat, oricare om de pe planetă, care are un televizor conectat la un cablu de reţea sau dispune de un calculator cuplat la Internet, poate afla, la orice oră din zi şi din noapte, ce se petrece în lume, dar cu o singură condiţie: să ştie să se descurce în păienjenişul de date şi informaţii, să ştie adică ce să caute şi cum să caute. Din păcate, reţeaua este un suport din ce în ce mai stabil şi mai extins, foarte eficient nu numai pentru informaţie, ci şi pentru dezinformare, pentru de tot felul de date şi chiar de informaţii care îl pot intoxica nu doar pe un neavizat, ci chiar şi pe un specialist în domeniul informaţiilor.

Odată cu dezvoltarea reţelelor, au apărut, au evoluat, s-au complicat şi multiplicat fel de fel de abilităţi, de la cele care ţin de constituirea şi gestionarea reţelelor, până la cele care urmăresc vulnerabilizarea acestora sau folosirea lor în fel de fel de scopuri. Reţelele evoluează, proporţional, în oglindă, de o parte şi de alte a unei axe, ducând cu ele tot ce are mai bun şi mai rău omenirea. Reţelele nu sunt selective, nu sunt purificatoare. Ele constituie doar un suport. Şi, aşa cum, de veacuri, hârtia suportă orice, şi ele suportă orice, cu condiţia să poate fi transpus în acel semnal purtător de informaţie specific reţelei. De aceea, cu o minimă pregătire în ceea ce priveşte folosirea unui calculator, alcătuirea unui site, introducerea unor date, obţinerea unui cont şi a unei parole, dar chiar şi fără acestea, oricine poate intra în reţea şi beneficia de ceea ce oferă aceasta.

De aici nu rezultă neapărat că crizele şi conflictele armate se constituie şi se transmit de-acum prin reţea sau că reţelele ar constitui noi cauze pentru crize şi conflicte. Rezultă doar o realitate care influenţează semnificativ şi domeniul crizelor şi conflictelor armate. Este evident că, la acest nou început de secol şi de mileniu, reţelele există, că ele reprezintă realităţi complexe, bazate îndeosebi pe interacţiuni şi efecte. La rândul lor, ele amplifică interacţiunile şi induc un efect special, care influenţează

semnificativ dinamica tuturor sistemelor şi proceselor sociale şi nu numai – *efectul de reţea*.

1.1.1. Efectul de reţea

Efectul de reţea se bazează pe accelerarea circulaţiei informaţiei, pe amplificarea explozivă a fluxului informaţional, pe facilitarea actului comunicării, dar şi pe capacitatea reţelelor de a asimila, de a se multiplica, de a influenţa, de a schimba filozofia relaţiilor sociale, adică viaţa oamenilor şi a entităţilor omeneşti, de a descoperi, a acapara, a extinde[1], şi, în acelaşi timp, a ascunde şi a vulnerabiliza. Efectul de reţea este similar cu fulgerul sau cu trăsnetul. Creează şi degajă uriaşe energii, dar şi uriaşe distrugeri. Siguranţa sistemelor şi proceselor sporeşte într-un sens şi de degradează în altul.

Puterea reţelei este imensă. Ea creşte pe măsură ce reţeaua se extinde, fiind direct proporţională cu numărul de noduri. Cu alte cuvinte, cu cât o reţea are mai multe noduri, cu atât este mai stabilă, mai puternică şi mai sigură. Chiar dacă redundanţa creşte, o dată cu ea cresc şi siguranţa şi stabilitatea. Spre exemplu, reţelele de transmisiuni, funcţionează şi în cazul în care o mare parte dintre noduri sunt distruse. Rutarea se face în mod automat. Informaţia este automat dirijată pe canalele neafectate, astfel încât ea să ajungă rapid la destinaţie. Evident, în aceste cazuri puterea reţelei scade, aşa cum scade şi capacitatea ei, dar ea, totuşi, funcţionează.

$$P_r = N_r^2$$

Unde P_r este puterea reţelei, iar N_r numărul nodurilor de reţea. $P_r = N_r^2$

Efectul de reţea este generat, pe de o parte, de puterea reţelei şi, pe de altă parte, de aria de cuprindere a reţelei, de capacitatea ei de a asimila rapid orice element, de a modela mediul în care acţionează şi de a se adapta la condiţiile lui. Comportamentul reţelei în raport cu mediul în care se dezvoltă este unul de asimilare a acestui mediu şi de acomodare la condiţiile lui, dar nu supunându-se lui, ci transformându-l. În acest sens, reţeaua distruge. Distruge şi înlocuieşte, nu lasă nimic gol. Cu alte cuvinte, reţeaua creează o altă realitate, o nouă realitate, deosebită de ceea ce există. Este o realitate de reţea, o realitatea virtuală, în care dependenţa, interdependenţa şi securitatea devin reguli stricte de funcţionare. Pentru a funcţiona, reţeaua trebuie să fie stabilizată şi securizată. Dar o reţea nu poate fi niciodată securizată complet. Totdeauna vor exista vulnerabilităţi generate de funcţionarea reţelei, de raporturile ei cu mediul sau cu alte reţele, de variaţia condiţiilor concrete. Aceste vulnerabilităţi vor fi exploatate de alte reţele concurente, de inamicii reţelei şi de toţi cei care sunt angajaţi, într-o formă sau alta, în continua bătălie a lumii pentru resurse, pieţe, putere, supremaţie şi influenţă. Propriu-zis, în acest război permanent al omenirii cu sine, mai exact, cu acele entităţi,

[1] 92 / **57 Network effect / Effet de réseau / Efecto de red /Efectul de retea. „**Efectele de reţea apar atunci când valoarea unui produs creşte, pentru un utilizator, cu numărul de utilizatori ai aceluiaşi produs sau ai unor produse compatibile. Economiştii vorbesc despre acest fenomen ca despre „externalitatea" reţelei, deoarece, atunci când se ataşează consumatori suplimentari la reţeaua consumatorilor existenţi, aceştia au un impact „extern" benefic pentru consumatorii care sunt, deja, membri ai reţelei" (http://www.competition.ro/publicatii/ GlosarUE).
A se vedea şi http://www.kinecto.ro/new/Resurse/dictionar-de-termeni/web-communication.shtml „**Efectul de reţea" (Network effect)** = fenomenul prin care un serviciu devine cu atât mai valoros cu cât este folosit de mai multe persoane; numărul mare de utilizatori încurajează înscrierea de utilizatori noi (de exemplu, un forum este cu atât mai util cu cât este accesat de mai mulţi utilizatori)."

sisteme şi procese care devine incompatibile între ele şi generează dezordine, şi conflictualitate, rețeaua nu se constituie în parte beligerantă. Rețeaua nu este decât un suport, un mijloc, dar un mijloc care se extinde şi se multiplică, facilitând circulația rapidă a informației, comunicarea, transportul, transmiterea de date şi de imagini, circulația mărfurilor, dar şi a tot felul de efecte.

Există rețele ale diferitelor entități care se pot afla în relații de colaborare, de parteneriat, de concurență sau în război, dar există şi rețele care acoperă întreaga planetă, cum ar fi, spre exemplu Internetul, care pot fi folosite de toată lumea.

Efectul de rețea se face simțit nu doar în circulația mărfurilor, a informației, a trenurilor, avioanelor şi, în viitor, şi a navetelor cosmice, ci şi în dimensionarea, configurarea şi reconfigurarea crizelor şi conflictelor armate, a războiului şi altor fenomene complexe care însoțesc şi definesc omenirea şi conflictualitatea ei permanentă. Rețeaua aduce noi dimensiuni şi elemente specifice în dinamica acestor fenomene şi procese, dintre care cele mai importante ar putea fi:

- circulația rapidă a informației, ceea ce conduce la o cunoaştere mai precisă şi oportună a cauzelor, determinărilor, implicațiilor şi efectelor crizelor şi conflictelor, inclusiv ale conflictelor armate şi războaielor;
- accelerarea fenomenelor şi proceselor generatoare de crize şi conflicte, dar şi a celor care estompează, frânează sau dezamorsează crizele şi conflictele;
- inducerea şi radierea efectului de criză şi a celui de conflict;
- diminuarea şi chiar estomparea efectului de criză şi a celui de conflict.

Rețeaua interconectează componentele sistemice şi procesuale ale unei crize, optimizând dinamica lor. În aceeaşi măsură, rețeaua conectează şi crizele între ele. În acest fel, în funcție de o mulțime de factori, efectul de criză poate fi diminuat sau amplificat.

Rețeaua dezvoltă, intensifică şi amplifică un sistem dinamic complex de relații bazate pe efecte, micşorând semnificativ ecartul dintre cauză şi efect, dintre acțiune şi rezultatul acesteia, dintre subiectul acțiunii şi obiectul acesteia, dintre proiect şi execuție, dintre producție şi consum, dintre scop şi mijloc.

Rețeaua nu schimbă actorii. Îi scoate însă din turnul lor de fildeş sau din sistemele tradiționale de protecție şi îi obligă să suporte efectul de rețea, sau cel puțin să țină seama de el. De acum înainte, nimeni nu va mai putea eluda efectul de rețea. Se vor găsi însă mijloace şi strategii adecvate pentru folosirea lui la maximum în avantaj propriu.

1.1.2. Efectul de criză

Efectul de criză poate fi definit ca impact direct sau mediat al crizei asupra altor domenii care nu sunt direct afectate de criză. O criză este ca o furtună, ca un uragan. Distruge, în proporții mai mari sau mai mici, tot ce întâlneşte în cale, dar, în acelaşi timp, provoacă dezechilibre semnificative pe o arie foarte mare, induce şi o stare de teamă, de nesiguranță, bulversează producția, prețurile, diminuează siguranța oamenilor şi instituțiilor, sporeşte vulnerabilitățile şi creează un câmp propice recrudescenței pericolelor şi amenințărilor.

Efectul de criză este ca o undă (este o undă) care se propagă în toate direcțiile, afectând, într-o măsură mai mare sau mai mică, tot ce poate avea tangență atât cu procesul sau cu sistemul care a declanşat sau din care s-a declanşat criza, cât şi cu sfera de manifestare a acesteia şi, evident, cu conținutul ei. Efectul de criză se manifestă ca o reacție în lanț. Criza prelungită din Orientul Mijlociu şi cea din Orientul Apropiat induc efecte dintre cele mai grave, care se manifestă pe o arie foarte largă, începând cu recrudescența fenomenului terorist, mai ales a terorismului islamic, şi continuând cu fluctuație prețului petrolului, cu influențarea piețelor şi strategiilor de piață, a relațiilor

financiare şi chiar cu declanşarea sau stimularea unui adevărat război financiar. Din această perspectivă, spre exemplu, o parte dintre țările arabe, mai ales cele producătoare de petrol, vor acumula, probabil, cantități mari de devize, putând produce o adevărată criză a dolarului. Oricum, efectele crizelor multiple şi greu de gestionat, chiar negestionabile din Orientul Mijlociu şi din Orientul Apropiat (pentru că toate acestea sunt legate între ele) se extind în mod haotic asupra relațiilor internaționale, bulversând grav nu doar o economie construită pe un suport energetic extrem de „fluid“ şi greu de înlocuit, cum este petrolul, ci şi securitatea, în general, şi securitatea energetică, în special, a tuturor țărilor lumii.

Interdependențele sunt atât de mari, încât nici o țară din lume nu poate eluda efectul crizelor şi îndeosebi efectul crizelor energetice. Evident, nu există crize energetice în sine, ci crize energetice generate de un fenomen politic complex, măcinat de un sistem de strategii şi de bătălii (câştigate, pierdute sau în plină desfăşurare, fiecare cu efectele ei) pentru resurse, pentru piețe, pentru supremație şi, evident, pentru realizarea şi menținerea unui mediu strategic care să asigure prevenirea războiului şi realizarea unor capacități de acțiune şi de reacție ante-criză, în timp de criză şi post-criză. Rețeaua favorizează acest lucru, dar, în acelaşi timp, prin *efectul de rețea*, amplifică, în proporții, greu de estimat şi de controlat, efectul de criză.

JM Guillery[2] scrie că „există crize care se nasc dintr-o pură revelație mediatică.“ O revistă, intitulată „Jurnalul de Duminică“, a publicat, pe patru coloane, în susul paginii, un titlu şocant: „Alertă la Montparnasse. Amiantă. Trebuie luate măsuri de urgență în imobilul unde lucrează 5000 de oameni. Două scenarii în studiu arată că evacuarea liniei ar dura… trei ani!“[3]

Toate publicațiile şi agențiile de presă au preluat şi publicat conținutul acestui articol. În 24 de ore, *efectul de criză* s-a produs. Patrick Lagadec numeşte acest fenomen „efectul Larsen“[4] O astfel de ştire, preluată şi amplificată, declanşează scandalul. De fapt, nu este nimic nou. Turnul Montparnasse, ca mai toate clădirile construite în acea epocă, conține amiantă (azbociment).

Nimeni un are o evidență clară a acestor clădiri sau, în orice caz, dezamiantarea acestora ar dura foarte mult şi ar costa enorm. Dar, dezvăluirile jurnalului au produs multă panică. Patologiile legate de azbociment sunt responsabile de 3000 de morți pe an şi se estimează că şi de 50.000-100.000 decese până în 2025.

Efectul de criză este rapid şi şocant. El trece însă foarte repede, chiar mai repede decât criza care l-a produs. Lasă însă urme greu de şters.

1.1.3. Presiuni şi vulnerabilități

Într-un fel, rețeaua, prin *efectul de rețea*, ajută la depresurizarea zonelor grav tensionate. Difuzarea rapidă a informațiilor de stare este benefică pentru metasistem, în sensul că, datorită accesului la informație în timp real (sau în timp util), se crează condiții pentru a fi luate măsuri care să ducă la rezolvarea oportună a situațiilor care au facilitat producerea crizei sau care întrețin cauzele generatoare de crize şi conflicte. Rețeaua are funcția unor vase comunicante (cu noduri de distribuție şi de optimizare), dar ea nu poate rezolva, prin această calitate, toate problemele care se ivesc cu rapiditate sau ca urmare a unor acumulări în timp, într-un loc sau în altul. Măreşte însă

[2] http://www.gestiondecrise.com/amiante_gestion_crise.htm
[3] http://www.gestiondecrise.com/amiante_gestion_crise.htm
[4] Microfonie. Efect de feedback electroacustic intre microfon si amplificator. Oscilații a căror amplitudine atinge foarte repede valori maxime. Se prezintă sub forma unui şuierat strident, caracteristic.

interacțiunile şi facilitează *cunoaşterea rapidă a problemelor*, ceea ce este esențial în gestionarea crizelor şi conflictelor.

Rețeaua creează o situație nouă, în coordonate noi, multidimensionale, care impun abordări noi, flexibile şi oportune. Această nouă situație poate fi caracterizată prin:

- sporirea cantității de informație despre zona sau despre zonele în criză, aceasta definindu-se pe un procent mai mare de nedeterminări înlăturate şi, prin urmare, prin reducerea incertitudinilor;

- creşterea proporțională a posibilității de dezinformare, ceea ce duce la crearea unor noi tipuri de incertitudini, a *incertitudinilor orizontale* sau a *incertitudinilor de rețea*;

- crearea unor presiuni concurențiale noi, altfel configurate, care pot fi disipate în toată rețeaua şi, la momentul potrivit, concentrate acolo unde se consideră că este necesar[5];

- formarea, în cadrul rețelei, a unor noduri sau elemente care pot crea perturbații, instabilitate şi chiar crize şi conflicte în spațiul virtual, dar şi în cel real;

- vulnerabilizarea sistemelor şi/sau proceselor prin flexibilizarea incertitudinilor;

- posibilitatea apariției, inducerii şi proliferării unor efecte negative de rețea.

Rețeaua creează, deopotrivă, un sistem de presiuni continue asupra utilizatorilor şi mediului ambiant, în sensul restricțiilor şi regulilor ce se cer urmate şi în cel al vulnerabilităților ce se cer depistate şi reduse sau acoperite, dar şi un spațiu extins de comunicare şi de acțiune.

Printre presiunile create şi exercitate de rețea s-ar putea situa şi următoarele:

- extinderea nelimitată a spațiului informației şi al comunicării (în mod implicit şi a ofertei informaționale), dar, în acelaşi timp, şi restricționarea accesului;

- crearea unor puternice presiuni de rețea, atât la nivelul individului (concretizată într-o dependență numită, între altele, şi „sindromul Internet", deşi rețea nu înseamnă numai Internet), cât şi la nivelul instituțiilor, administrației, organizațiilor şi organismelor internaționale şi altor structuri naționale şi internaționale;

- crearea şi accentuarea interdependențelor;

- impunerea de standarde;

- crearea unui conflict major între monopolul de rețea şi tendința firească de multiplicare şi proliferare a rețelelor;

- creşterea redundanței canalelor de comunicații, ceea ce, pe de o parte, duce la o mai bună stabilizare a acestora şi, pe de altă parte, la înstufarea datelor, imaginilor şi informațiilor, deci la intoxicare informațională;

- facilitatea manipulării şi creşterea „efectului de manipulare";

- generarea şi facilitarea extinderii unui nou tip de piraterie – pirateria informațională;

- generarea şi facilitarea extinderii cyberterorismului;

- amplificarea „efectului de criză".

Vulnerabilitățile sunt strâns legate de aceste presiuni şi se referă, în principiu, la:

- sensibilitatea programelor şi bazelor de date şi posibilitatea spargerii codurilor şi parolelor, deci a accesului neautorizat;

- dependența de surse de energie şi, deci, vulnerabilitatea la acestea;

[5] O astfel de concentrare a efectelor poate fi dirijată de cei care au capacitatea, posibilitatea şi interesul să o facă. Şi, de cele mai multe ori, lucrurile aşa se produc. Trebuie avute totuşi în vedere şi situațiile de concentrare spontană şi, adesea, haotică, deci necontrolabilă, a efectelor, ceea ce sporeşte şi mai mult, deopotrivă efectul de criză şi efectul de rețea, prin cumularea intempestivă a acestora.

- complicarea programelor şi vulnerabilitatea lor încă mare atât la cyberpiraterie, cât şi la atacuri ale hackerilor;

- costul destul de mare al programelor de securitate şi schimbarea lor foarte rapidă;

- competiția deschisă şi foarte intensă dintre programele de securitate şi activitatea hackerilor şi altor inamici ai rețelei sau car vor pur şi simplu să utilizeze rețeaua în folosul lor.

Vulnerabilitățile, ca şi abilitățile şi elementele de putere ale rețelei, sunt dinamice. Ele evoluează odată cu sistemele, procesele şi programele şi, pe măsură ce unele dispar, altele apar. Niciodată nu vom putea spune că rețelele de informații, de comunicații şi de relații internaționale, precum şi cele economice, politice, sociale, culturale etc. sunt complet şi pentru totdeauna securizate. Pe măsură ce ele se dezvoltă, se amplifică şi vulnerabilitățile lor, apar altele noi, se complică şi se sofistichează sistemele de acces şi de siguranță, se măresc şi se diversifică presiunile, provocările, pericolele şi amenințările, iar riscurile (asumate, impuse sau conjuncturale) devin din ce în ce mai numeroase şi mai greu de gestionat. Siguranța şi securitatea sistemelor şi proceselor, în condițiile filosofiei şi fizionomiei de rețea devin forte costisitoare.

1.1.4. Provocări, pericole, amenințări, riscuri specifice

Deşi, în general, lumea devine şi mai prosperă – cel puțin, acea parte a lumii care are acces la înalta tehnologie şi la tehnologia informației şi, evident, cea care creează aceste tehnologii –, pericolele continuă să existe şi chiar să evolueze pe coordonate şi direcții complexe şi imprevizibile.

Provocările, pericolele, amenințările şi legat de acestea, riscurile specifice – asumate, întâmplătoare sau impuse – sunt legate de evoluția şi caracteristicile societății omeneşti şi de fiecare componentă şi acțiune a ei. Ele se află şi se dezvoltă, cresc şi descresc, apar şi dispar în fiecare domeniu de activitate şi vizează tot ce ține de societatea omenească şi de acțiunile oamenilor şi comunităților. De aceea, ele nu vor putea fi niciodată nici pe deplin cunoscute, nici pe deplin eradicate, nici pe deplin gestionate. Totdeauna va exista o competiție, va exista chiar o luptă între mulțimea provocărilor, pericolelor, amenințărilor şi riscurilor implicite (asumate, întâmplătoare sau impuse) şi modalitățile şi acțiunile concrete de securizare a sistemelor şi proceselor.

Pentru a deveni *amenințare*, pericolul are nevoie de un vector, trebuie adică „transportat". Rețeaua este mai mult decât un vector, este un suport al oricărui tip de transport şi al oricărui tip de vector care respectă exigențele fluxului de rețea.

Amenințarea are o destinație, vizează ceva, este orientată, este, deci, un pericol cu destinație, un pericol orientat. Desigur, ea poate fi şi un simplu *avertisment*. Avertismentul nu este însă amenințare. Mai exact, avertismentul poate fi un fel de amenințare condiționată.

Riscul este o atitudine față de un pericol sau de o amenințare. El se asumă, se impune, se asociază, conştient, responsabil sau, dimpotrivă, în mode aleator, colateral, intempestiv. *„Nu există reguli pentru aprecierea riscului, aşa cum nu există nici pentru alegerea unei soluții bune; aprecierea riscului este o chestiune de inteligență, dar şi de cunoaştere şi de experiență."*[6] De aceea, identificarea pericolelor[7], amenințărilor[8] şi

[6] **www.stratisc.org** François Caron, L'APPRÉCIATION DU RISQUE MILITAIRE.

[7] *Pericolul* reprezintă o primejdie, adică o situație care poate duce la degradarea unui sistem sau proces, la distrugerea unei entități. El însuşi este, de altfel, un efect al degradării unui sistem sau proces.

[8] *Amenințarea* semnifică o acțiune ostilă, cu scopul de a intimida. Ea poate fi exercitată în mod direct de cel care amenință sau poate fi percepută ca atare de cel care se consideră amenințat. Ecartul dintre o

riscurilor[9], ca şi a provocărilor[10], sfidărilor[11] şi tensiunilor[12], rămâne o chestiune cu un grad înalt de subiectivitate, acest proces situându-se undeva, la graniţa dintre obiectiv şi subiectiv, ca o construcţie dinamică şi flexibilă între aceşti doi poli importanţi ai cunoaşterii.

În actualele condiţii ale evoluţiei societăţii omeneşti, mai ales ca urmare a dezvoltării, fără precedent a reţelelor economice, politice şi informaţionale, evaluarea riscurilor, ameninţărilor, provocărilor, sfidărilor şi tensiunilor, în măsura în care acestea sunt identificate[13], este absolut necesară.

O primă grilă ar putea fi constituită din identificarea *parametrilor de impact* şi constă dintr-o evidenţiere a efectelor previzibile (în plan economic-financiar, politic, social, demografic, cultural şi militar) privind securitatea naţională a sistemelor şi proceselor (securitate economică, socio-culturală şi militară), adică a înlănţuirii cauzelor şi efectelor. (Anexa nr. 1).

O altă grilă poate fi folosită pentru identificarea şi evaluarea *parametrilor de proximitate* şi ar cuprinde un sistem de analiză şi evaluare a riscurilor în funcţie de timp (diagramă de timp).

Cea de a treia grilă se constituie într-o modalitate de evaluare a *parametrilor de asumare* (provocare) şi, în consecinţă, a riscurilor de asumare, mai exact, a riscurilor reacţiei.

Ar fi posibil şi un model matematic de evaluare a riscurilor, deşi s-ar putea ca un asemenea model să nu fie chiar foarte util. Riscurile, ca pericole conştientizate, impuse, aleatoare sau posibil a fi asumate[14], au cauze, determinări şi implicaţii complexe şi o dinamică foarte mare, în care factorul subiectiv joacă un rol important. De aici şi dificultatea unei analize cantitative şi calitative bazată pe modele matematice. *„Cei care pretind să încredinţeze unui model matematic, oricât de elaborat ar fi el, aprecierea riscului şi inteligenţei artificiale, sarcina elaborării deciziei pornind de la date exclusiv obiective, cred că se pot proteja împotriva erorilor datorate subiectivismului; dar nu vor ajunge niciodată la o corectă apreciere a riscului de vreme ce subiectivul face parte integrantă din acesta.“* [15]

Totuşi, trebuie să subliniem că şi subiectivul poate şi trebuie să fie, în anumite condiţii, analizat şi evaluat.

---

realitate (acţiune) şi perceperea ei ca ameninţare este foarte mic şi greu de identificat. De aceea, în relaţiile dintre state, problematica ameninţării şi a percepţiei acesteia ca atare este foarte sensibilă.

[9] Prin *risc* se înţelege o primejdie (pericol) căreia i se poate evalua (măsura), până la un anumit punct, eventualitatea, care poate fi mai mult sau mai puţin previzibilă (DICTIONAIRE DE LA LANGUE FRANCAISE. Encyclopedie, noms communns, noms propres, 1995)

[10] Provocarea semnifică o suită de gesturi, de realităţi sau de acţiuni îndreptate împotriva cuiva cu scopul de a produce o reacţie. Există şi aici o mare sensibilitate între provocarea ca atare şi percepţia ei. De aceea, în multe privinţe, provocarea nu este doar acţiunea de a provoca, ci mai ales înaelegerea (considerarea, analiza, calificarea) acesteia ca provocare.

[11] *Sfidarea* este, deopotrivă, provocare prin ignorare, adică o ignorare care provoacă, dar şi atitudine care ignoră. Sfidarea este o ignorare orientată, adesea ameninţătoare.

[12] Prin *tensiune*, în sensul acestui studiu, înţelegem o stare de încordare care induce teamă, nesiguranţă şi neîncredere şi determină, în cele mai multe cazuri, reacţii.

[13] Identificarea provocărilor, sfidărilor, pericolelor, ameninţărilor şi a riscurilor asociate acestora revine, deopotrivă, unor structuri specializate, cum ar fi, spre exemplu, serviciile de informaţii, compartimentele de analiză şi de evaluare din fiecare sistem sau proces, dar şi fiecărei instituţii şi fiecărui om în parte. Trăim într-o lume a interdependenţelor. De aceea, nu numai procesele şi acţiunile care duc la progres se intercondiţionează, ci şi cele care duc la degradarea şi distrugerea sistemelor şi proceselor, a calităţii vieţii, a relaţiilor internaţionale, a păcii şi securităţii.

[14] În cele din urmă, *riscul* este un comportament (asumat sau impus) faţă de un pericol conştientizat sau de o ameninţare înţeleasă ca atare.

[15] **www.stratisc.org** François Caron, L'APPRÉCIATION DU RISQUE MILITAIRE.

Există câteva mari categorii de provocări, pericole, amenințări şi, în consecință, de riscuri asociate, asumate, impuse sau aleatoare. În cadrul temei acestui referat, eu propun următoarea clasificare:

a) provocări, tensiuni, pericole şi amenințări care privesc întreaga lume (ființa umană, în general);
b) provocări, tensiuni, pericole şi amenințări centrate pe diferite regiuni;
c) provocări, tensiuni, pericole şi amenințări transfrontaliere;
d) provocări, tensiuni, pericole şi amenințări interne (care vizează statele);
e) provocări, tensiuni, pericole şi amenințări la adresa securității proprietății;
f) provocări, tensiuni, pericole şi amenințări la adresa ordinii de drept;
g) provocări, tensiuni, pericole şi amenințări la adresa persoanei.

Din categoria a) fac parte îndeosebi:

- proliferarea armelor de distrugere în masă, a sistemelor de arme, a armelor geofizice i cosmice;
- încălzirea planetei, seceta, fenomenele meteorologice, cosmice şi cele care țin de geofizică;
- sărăcia şi malnutriția;
- lipsa apei potabile;
- împuținarea resurselor;
- proliferarea maladiilor distructive (cancer, SIDA, bolide malnutriție etc.);
- terorismul;
- traficul de droguri, de arme şi de carne vie;
- criminalitatea transfrontalieră.

În categoria b) pot fi situate pericolele şi amenințările specifice diferitelor regiuni, dintre care:

- programele nucleare sau chimice, biologice, radiologice şi nucleare (CBRN);
- lipsa apei potabile;
- deşertizarea unor teritorii întinse;
- catastrofele naturale;
- diferendele etnice;
- terorismul;
- gravele probleme de frontieră;
- sărăcia şi malnutriția;
- regimurile dictatoriale;
- războaiele civile;
- gherila.

Categoria c) se referă mai ales la acele provocări, tensiuni, pericole şi chiar amenințări care nu țin seama de entitățile statale, ci urmează acele coridoare strategice ale traficanților, rețelelor mafiote, spălării banilor, crimei organizate etc. Dintre acestea, cele mai importante ar putea fi:

- emigrația clandestină;
- rețelele violente mafiote, de crimă organizată, de spălare a banilor etc.;
- terorismul transfrontalier, îndeosebi cel sinucigaş;
- rețelele locale de traficanți;
- rețelele locale transfrontaliere de distribuire a drogurilor;
- rețelele transfrontaliere de prostituție;
- rețelele transfrontaliere ale economiei subterane şi crimei economico-financiare.

În consonanță cu provocările, tensiunile, pericolele şi amenințările globale, regionale, transfrontaliere etc, se dezvoltă şi cele interne, cele din categoria d). Deocamdată, nici un stat din lume nu a reuşit să rezolve aceste probleme, care proliferează odată cu noua filozofie şi fizionomie de rețea. Cele mai importante dintre provocările, tensiunile, pericolele şi chiar amenințările care afectează statele sunt, în opinia noastră, următoarele:

- distrugerea unităților economice naționale;
- diferendele etnice;
- corupția;
- rețelele de distribuție a drogurilor;
- economia subterană;
- rețelele şi găştile de cartier;
- lipsa acută a locurilor de muncă;
- rețelele de prostituție;
- crima organizată;
- spălarea banilor.

Există o serie de provocări, tensiuni, pericole şi amenințări, cele din categoria e), care afectează securitatea proprietății. Printre cele mai importante dintre acestea, în etapa în care ne aflăm, ar putea fi şi următoarele:

- inconsistența legislației care reglementează proprietatea sau neconcordanța dintre diferite reglementări;
- dificultatea revenirii de la proprietatea de stat şi obştească la proprietatea privată;
- corupția funcționarilor de stat şi altor persoane;
- problemele nesoluționate cu privire la punerea în posesie şi la acordarea titlurilor de proprietate;
- calamitățile şi dezastrele naturale;
- infracționalitatea încă ridicată cu privire la proprietate.

Din categoria f), cele mai frecvente provocări, tensiuni, pericole şi amenințări la adresa ordinii de drept se referă la:

- bulversarea economiei naționale şi creşterea gradului de nesiguranță socială;
- migrația masivă a forței de muncă spre țările din Vestul Europei, cu toate consecințele care decurg de aici;
- fluctuația foarte mare de bunuri, persoane şi servicii;
- proliferarea economiei subterane;
- criminalitatea economico-financiară ridicată;
- nesiguranță socială.

Toate cele de mai sus afectează şi persoana cetățeanului. Cele mai frecvente provocări, tensiuni, pericole şi amenințări la adresa persoanei, din categoria d), se referă la:

- creşterea gradului de înstrăinare şi de alienare a persoanei;
- lipsa acută a mijloacelor de subzistență;
- nesiguranța locului de muncă;
- nesiguranța străzii;
- corupția masivă şi omniprezentă;
- criminalitatea crescută;
- migrația;
- presiunile diferitelor instituții, firme şi mecanisme;
- diferendele etnice;

- terorismul;
- calamitățile.

Natura provocărilor, pericolelor, amenințărilor şi a riscurilor legate de acestea

Natura şi sfera de cuprindere a provocărilor, pericolelor, amenințărilor şi, evident, a riscurilor asumate sau impuse, care afectează securitatea națională şi internațională, poate fi identificată în funcție de:

- domenii de activitate;
- entități comunitare şi religioase, dar şi de altă natură;
- arie geografică;
- timp (durată);
- volum;
- importanță (interes, gravitate);
- probabilitate.

În funcție de domeniile de activitate, provocările, pericolele şi amenințările ar putea fi:

Economice

Interne

- Degradarea, ineficiența, scăderea drastică a producției sau subminarea unor ramuri ale economiei naționale;
- Proliferarea economiei subterane;
- Prejudicierea unor sectoare de importanță strategică (industria de apărare);
- Nesiguranța proprietății;
- Devalorizarea monedei naționale;
- Slăbirea sistemului bancar;
- Creşterea datoriei publice;
- Neîncrederea populației în sistemul bancar;
- Politici economice nerealiste şi neadecvate împrejurărilor, exigențelor momentului şi specificului românesc.

Externe

- Blocarea creditelor externe;
- Blocarea accesului la sursele de materii prime deficitare pentru economia națională;
- Blocarea accesului la tehnologii moderne;
- Diminuarea piețelor de desfacere;
- Globalizarea economică pe un fond național incapabil de adaptare;
- Regionalizarea tendențioasă;
- Neintegrarea economică oportună în Uniunea Europeană (integrarea fără ca economia să fie pregătită în mod corespunzător pentru acest efort);
- Contrabanda, traficul ilegal de mărfuri.

Sursele principale ale acestor provocări, pericole, amenințări şi riscuri de natură economică se află în imposibilitatea armonizării tuturor componentelor domeniului, în dificultatea relaționării componentelor, factorilor interni şi internaționali, în realitățile complexe, cu desfăşurări bruşte şi, de aceea, haotice, în interesele diferite, dar şi în complexitatea dimensionării şi redimensionării unor politici economice şi sociale realiste, concrete şi eficiente pe termen lung. De asemenea, lipsa unei strategii economice adecvate şi pe termen lung, pe termen mediu şi pe termen scurt, care să pună

în operă o decizie de politică economică bine elaborată, conjugată cu instabilități politice, sociale şi cu numeroase împrejurări economice nefavorabile, atât interne, cât şi externe, cu numeroşi factori aleatori, precum şi incapacitatea sistemului financiar bancar de a se adapta rapid cerințelor economice, îndeosebi cerințelor pieței constituie provocări, pericole şi chiar amenințări la adresa securității economice şi nu numai. Aceste împrejurări pot fi şi sunt folosite de anumite forțe economice care se adaptează rapid situațiilor confuze, profitând de ele pentru a înlătura concurența şi a câştiga noi piețe. Pot fi însă folosite şi de cei care urmăresc destabilizarea țării sau a zonei şi realizarea unor obiective mult mai mari decât simplul profit economic.

Astfel de pericole şi amenințări afectează grav securitatea economică a țării noastre, a oricărei țări şi influențează în mare măsură şi celelalte surse de pericole, amenințări şi, în consecință, de risc din domeniul politic, social, cultural, informațional şi militar.

Sursele de provocări, pericole şi amenințări din acest domeniu sunt greu sesizabile, întrucât sunt înstufate şi implicite. Manifestarea lor este ascunsă şi, adesea, perversă, întrucât o parte dintre acestea nu sunt cognoscibile, adică uşor de înțeles. Şi chiar dacă identificarea lor nu ar pune probleme deosebite, manifestarea lor îmbracă toată gama de acțiuni, de la cele directe la cele cu efect întârziat. Spre exemplu, privatizarea trebuie să aibă efecte pozitive în dinamizarea economiei şi prevenirea riscurilor majore de natură economică. În realitate, modul cum s-a efectuat şi cum şi se efectuează, în loc să ducă la creşteri economice, a dus şi duce în continuare la situații confuze, la fraude şi distrugeri care au afectat şi afectează grav situația economică a țării.

Se continuă marile discrepanțe între grupările de interese politice şi strategice, care seamănă confuzie şi probleme globale antinomice. Din această perspectivă, cele mai frecvente şi mai probabile provocări, pericole şi amenințări la adresa securității şi apărării țărilor, coaliților şi alianțelor, care ar putea genera crize şi chiar conflicte armate ar putea fi:

Globale

- Proliferarea armelor de distrugere în masă şi a mijloacelor chimice, biologice, radiologice şi nucleare (CBRN), cu efecte în toate planurile şi mari riscuri;

- Adâncirea decalajelor economice, tehnologice şi informaționale, accentuarea sărăciei şi a faliilor strategice între lumea bogată şi lumea săracă, între Orientul Mijlociu şi Occident, între diferite categorii de interese, care generează totdeauna concurență, bătălii pentru resurse şi pentru piețe, crize şi conflicte;

- Proliferarea conflictualității frontaliere sau ce ține de frontiere, acces la resurse, poziții geostrategice şi teritorii, care se exprimă mai ales în efortul politic disperat al unor entități etnice mai mari sau mai mici de recunoaştere internațională şi de constituire a unor state politice în arealul pe care-l consideră că le aparține de drept;

- Proliferarea conflictualității interetnice, interrasiale, interreligioase care generează conflicte confesionale, rasiale şi sociale, atât interne (între religiile de bază şi diferite secte, între rase), cât şi între diferite interese care capătă conotații religioase, rasiale sau sociale. Acest tip de conflictualitate duce la fundamentalism religios, de tipul fundamentalismului islamic, dar nu numai, întrucât aproape fiecare religie are şi o latură care exacerbează doctrina (fundamentalismul, ca şi islamismul, este de sorginte politică), la conflict rasial şi la conflicte sociale grave;

- Dezvoltarea grupărilor şi rețelelor teroriste şi posibilul acces al acestora la unele mijloace CBRN şi la unele sisteme perfecționate de arme, precum şi la alte categorii de mijloace, inclusiv psihologice şi mediatice;

- Dezvoltarea altor tipuri de provocări, pericole şi ameninţări disimetrice (disproporţionate) şi asimetrice (exploatarea vulnerabilităţilor reciproce), care menţin şi proliferează, până la saturaţie (anxietate generală) o stare de tensiuni, de teamă şi de nesiguranţă individuală, socială, economică şi chiar politică.

Sursele principale ale provocărilor, pericolelor, ameninţărilor şi riscurilor asociate acestora (asumate, întâmplătoare sau impuse) sunt numeroase. Ele rezidă, în primul rând, în dezordinea lumii, în decalajele tehnologice imense, în confruntarea dintre interese – deci, dintre politici –, dintre concepţiile privind ordinea lumii, accesul la resurse, relaţiile dintre comunităţi, drepturile comunităţilor şi ale oamenilor.

Politice

Interne

- Instabilitatea sau confuzia şi promiscuitatea politică;
- Proliferarea extremismului sau a bătăliilor pentru putere şi influenţă;
- Criza de autoritate a instituţiilor puterii;
- Lipsa, insuficienţa sau neaplicarea corectă a legislaţiei democratice;
- Politici ascunse sau perverse de secesiune teritorială;
- Nedefinirea clară a interesului naţional;
- Proliferarea intereselor de grup.

Externe

- Tendinţe revizioniste, revendicări teritoriale din partea unor forţe (guverne, grupări politice, grupuri de interes etc.) din zona noastră de interes strategic;
- Presiuni externe în problema minorităţilor;
- Reinstalarea sferelor de influenţă;
- Deteriorarea imaginii României;
- Regrupări geopolitice, altele decât cele impuse de integrarea europeană.

Sursele principale ale acestor riscuri se află, în mare parate, în interesele contradictorii, în subiectivismul, lupta pentru putere şi lipsa unei moralităţi în viaţa politică. Astfel de surse nu sunt specifice doar României, dar ţara noastră este una dintre ţările grav afectate de confuzia şi promiscuitatea politică.

Astfel de realităţi se află în toată lumea şi cam în aceiaşi parametri. Situaţia complexă a trecerii de la o economie centralizată la o economie de piaţă, de la un regim politic autoritar la unul democratic, dar şi alte tipuri de desfăşurării şi schimbări care induc o stare de haos[16] constituie factor favorizant al proliferării acestor surse.

Ele se manifestă prin tot felul de acţiuni complicate, ascunse, viclene. Oricât de deschisă şi de ascuţită ar fi lupta politică, ea nu reuşeşte să dezvăluie dedesubturile confruntării. Ambiţiile, ameninţările şi maşinaţiunile politice au impus totdeauna acţiuni pe muchie de cuţit, adică un risc politic imens, concretizat în lupte politice care nu au nici limite, nici morală. Ele au distrus Roma antică, au falimentat democraţia grecească, au dus la căderea unor mari imperii; tot ele au dus şi la sfârtecarea teritorială a României în preajma celui de al doilea război mondial şi, în prezent, au întârziat cu mulţi ani redresarea ţării.

Informaţionale

Interne

- Lipsa de informaţii;
- Dezinformarea;
- Intoxicarea informaţională;

[16] Haosul este înţeles aici ca dezorganizare în vederea unei noi organizării, stare în care toate procesele sunt accelerate, intersectate, amestecate, confuze, greu de identificat, de analizat, de înţeles şi de susţinut.

- Manipularea informațională;
- Managementul defectuos al sistemelor de comunicare.

Externe

- Lipsa de informații;
- Dezinformarea;
- Intoxicarea informațională;
- Manipularea informațională;
- Managementul defectuos al sistemelor de comunicare.

Pericole şi amenințări specifice perioadei de trecere de la societățile industriale la cele de tip informațional

- Diminuarea unității economice a statului în favoarea rețelelor economice mondiale;
- Scăderea producției şi creşterea dependenței şi interdependenței economice, de unde şi haosul producției, concomitent cu constituirea şi reconstituirea centrelor de putere sau de superputere economică;
- Proliferarea perturbațiilor şi chiar a agresiunilor din sistemele informaționale;
- Constituirea unor puternice centre internaționale de influențare economică şi informațională;
- Intoxicarea, dezinformarea, individualismul;
- Pierderea controlului național asupra informației.

Sursele acestor provocări, pericole şi amenințări se află explozia informațională şi în faliile strategice care se creează între structurile de rețea, care se impun din ce în ce mai mult în actul comunicării, şi interesele sectare, în bătălia pentru putere, resurse, piețe şi supremație informațională ale unor comunități umane, instituții, grupări economice, politice. Aici intervin puternic şi grupările din lumea interlopă, din lumea traficanților şi crimei organizate.

Sociale

Interne

- Degradarea condiției socio-profesionale a cetățenilor, îndeosebi din țprile care nu se află în prima linie *high tech* şi *IT*;
- Şomajul;
- Exodul de inteligență;
- Degradarea stării de sănătate;
- Migrația internă;
- Perturbațiile demografice (îmbătrânirea populației, scăderea ratei natalității şi creşterea celei a mortalității, scăderea ratei populației active etc.);
- Sărăcirea (creşterea haotică a procentului cetățenilor ce trăiesc sub pragul de sărăcie);
- Nesiguranța socială.

Externe

- Emigrația în SUA, țările Europei Occidentale şi în cele ale UE;
- Destabilizarea demografică a regiunilor de falie, inclusiv a zonei balcanice;
- Globalizarea sărăciei (multiplicarea şi diversificarea polilor de sărăcie);
- Destabilizarea continuă a spațiului vechiului foaierului perturbator[17] şi mai ales a Orientului Mijlociu;
- Folosirea teritoriului național pentru refugierea unor grupuri etnice mai mari sau mai mici venite în mod ilegal din zonele de conflict.

[17] Vechiul foaier perturbator se întindea între Nordul Mării Caspice şi Manciuria şi se caracteriza prin invadarea spațiului european şi asiatic de către populațiile nomade războinice care se aflau aici.

Cauzele şi sursele acestor provocări, pericole şi ameninţări – în fapt, ale situaţiei care generează asemenea fenomene extrem de periculoase – se află în realităţile create de evoluţiile forţate, fără discernământ, deopotrivă, spre globalizare şi fragmentare, în memoria colectivă care depozitează umiliri, nedreptăţi şi fantasme ale istoriei. Balcanii de Vest, spre exemplu, nu sunt o zonă generatoare de tensiuni şi conflicte, ci o zonă care depozitează efectele dezastruoase ale unor falii strategice între marile imperii. Anihilarea acestora şi detensionarea zonei va dura, poate, sute de ani, cel mai probabil tot atât cât au durat şi imperiile care le-au creat, dacă nu chiar mai mult, în virtutea unei experienţe umane îndelungate potrivit căreia este nevoie de un timp dublu pentru a corecta o greşeală, o deprindere greşită, un reflex, o prejudecată sau un rău făcut.

Culturale

Interne

- Decăderea sistemului educaţiei naţionale;
- Deprecierea valorilor naţionale;
- Scumpirea actului de cultură;
- Multiculturalismul agresiv şi grăbit;
- Anticultura;
- Etnocentrismul;
- Xenofobia.

Externe

- Presiuni culturale (filme, cărţi, cântece etc.);
- Substituirea valorilor cu produse culturale de piaţă şi cu nonvalori;
- Globalizarea produselor culturale de piaţă în dauna culturii autentice;
- Proliferarea subculturii, nonculturii şi anticulturii;
- Iredentismul;
- Multiculturalismul agresiv, cultivat din interes.

Sursele acestor realităţi se află în perioada de haos în care se cufundă societatea omenească. Avem de a face nu cu o criză a culturii, ci cu o ofensivă a non-culturii, în dauna culturii autentice. În perioadele de haos există o bătălie pentru pieţe, pentru resurse, pentru supravieţuire şi, mai ales, pentru un loc cât mai bun în viitoarea reconfigurarea a structurilor de putere. În aceste condiţii, cine vinde mai mult devine mai puternic. Este deci normal ca, în astfel de epoci să se promoveze multiculturalismul, dar nu multiculturalismul autentic, care se realizează prin secole de convieţuire culturală, prin asimilare de valori care se unifică într-un edificiu important ce ridică civilizaţia planetei pe o treaptă superioară, ci amalgamul de produse culturale care nu pot intra în dialog, ci, cel mult, într-o vecinătate tensionată şi beligerantă, adică într-o confruntare. Or confruntarea între produsele culturale de piaţă nu înseamnă conflict între culturi, nici război al civilizaţiilor, ci doar o bătălie între vânzătorii de astfel de produse, lipsite de valoare, pentru a câştiga cât mai mulşi bani. Câştigul de bani nu are de-a face cu cultura, dar poate genera o concurenţă şi o conflictualitate teribilă. Pentru că de aici se câştigă foarte mult. Statele Unite ale Americii, spre exemplu, câştigă din exportul de astfel de produse culturale (filme violente, programe de televiziune, casete, CD-uri, muzică etc.) mai mult decât câştigă din exportul de armamente.

Ecologice

Interne

- Deteriorarea constantă a calităţii mediului;
- Catastrofe intenţionate sau provocate din neglijenţe;

- Accidente ecologice.

Externe

- Depozitarea unor deşeuri toxice pe teritoriul României;
- Calamităţi intenţionate sau provocate prin intervenţia în modificarea mediului;
- Subţierea stratului de ozon;
- Distrugerea ionosferei;
- Accidente ecologice.

Naturale (obiective)

- Cutremure, inundaţii, uragane, avalanşe şi alte calamităţi naturale;
- Încălzirea planetei, creşterea nivelului oceanelor, dezechilibre naturale;
- Fenomene geofizice dăunătoare pentru viaţa oamenilor şi a comunităţilor;
- Fenomene cosmice care afectează mediul de viaţă.

Cauzele acestor pericole şi ameninţări sunt în afara mediului social şi uman. Ele se află în faptul că pământul este o planetă activă, care continuă să se transforme. Însăşi viaţa este un produs al acestei activităţi a planetei, conjugată cu activitatea solară şi cu cea cosmică. Aceste cauze trebuie doar cunoscute. Astfel de pericole pot fi doar diminuate, în sensul că omul n-ar trebui să se aşeze în calea lor, ci să înţeleagă şi să respecte fenomenele naturale. Încă multe mii de ani de acum încolo vor fi tunete, trăsnete, inundaţii şi mari revărsări de ape, uragane, lunecări de teren, erupţii vulcanice, schimbări bruşte de climă etc. Aceste este mediul în care trăim şi el trebuie cunoscut, înţeles şi respectat, întrucât el este nu numai distrugător, ci şi generator de mişcare, de schimbare, de viaţă.

Tehnologice

Interne

- Degradarea (învechirea) patrimoniului tehnologic;
- Incapacitatea de a produce tehnologie modernă;
- Incapacitatea de a importa tehnologie modernă.

Externe

- Blocarea (limitarea) accesului la tehnologia modernă;
- Creşterea preţurilor tehnologiilor moderne;
- Incapacitatea sau imposibilitatea participării la realizarea (în cooperare cu statele dezvoltate) a tehnologiilor înalte.

Sursa acestor pericole şi ameninţări se află în atitudinea politică neadecvată, în arhitectura primitivă, neadaptată la condiţiile concrete a clasei politice, a legislaţiei, a relaţiilor internaţionale. Accesul la înalta tehnologie şi la tehnologia informaţiei nu este un drept, ci o construcţie care se realizează printr-un efort îndelungat pentru a pune în operă o politică atentă, inteligentă şi realistă.

Aceste tipuri de pericole şi ameninţări sunt implicite. Ele nu produc crize şi războaie şi nici nu agresează pe cineva. Creează însă decalaje imense, polarizează informaţia, cunoaşterea, bunurile materiale, civilizaţia şi chiar cultura. Societatea modernă produce nu doar o cultură tradiţională, bazată pe sute de ani de convieţuire, ci şi o cultură tehnologică, absolut necesară progresului. Valorile tehnologice şi informaţionale sunt absolut necesare în arhitectura unei societăţi, în construcţie echilibrului social şi a bunăstării. De fapt, una dintre cauzele fundamentale ale decalajelor, şi deci ale polarizării bogăţiei şi sărăciei o reprezintă falia sau faliile tehnologice. Datorită acestor falii, unele comunităţi se află în epoca Internetului şi a zborurilor cosmice, altele se află în epoca de piatră.

Militare

Interne

- Dezvoltarea fără precedent a armamentelor şi mijloacelor de luptă, îndeosebi a ADM, a vectorilor şi a sistemelor de arme foarte precise, precum şi a reţelelor I2SR şi C4.
- Crearea imaginii inutilităţii armatelor naţionale şi inducerea ideii că nu mai este nevoie de o astfel de instituţie, ci doar de armate profesioniste;
- Proliferarea ameninţărilor teroriste şi diversioniste;
- Posibila apariţie a unor tendinţe secesioniste prin violenţă;
- Sabotaje la obiective militare de importanţă strategică;
- Scăderea capacităţii de luptă a forţelor armate sub o anumită limită;
- Deteriorarea relaţiilor între structurile de forţă ale statului;
- Carenţe în pregătirea teritoriului, economiei şi populaţiei pentru apărare;
- Deteriorarea industriei de apărare;
- Lipsa (insuficienţa) unei legislaţii moderne şi clare în domeniul securităţii naţionale şi internaţionale;
- Neînţelegerea dimensiunilor şi modalităţilor actuale şi viitoare ale securităţii şi apărării, ca atribut naţional într-o strânsă determinare internaţionale, de coaliţie şi de alianţă;
- Eşuarea reformelor sistemelor militare şi civil-militare.

Externe

- Pericolul nuclear;
- Pericolul CBRN;
- Pericolul potenţial al unor agresiuni militare indirecte;
- Existenţa unor conflicte deschise, latente sau îngheţate în vecinătatea teritoriului naţional sau în zone de interes european şi euro-atlantic;
- Proliferarea armamentului neconvenţional;
- Pericolul folosirii altor arme de distrugere în masă;
- Proliferarea sistemelor de arme şi a strategiilor războiului non-contact, ale războiului disproporţionat, ale războiului preventiv şi ale războiului asimetric;
- Proliferarea armamentului cosmic şi a structurilor militare cosmice;
- Accentuarea decalajelor de potenţial militar;
- Blocarea accesului la tehnologii militare moderne;
- Crearea unor potenţiale conflicte între ţările care aparţin NATO şi unele dintre ţările din afara arealului Alianţei;
- Crearea unor potenţiale situaţii conflictuale între ţările din cadrul structurilor de securitate europene şi alte ţări;
- Apariţia unor posibile alianţe strategice opuse NATO.

Sursele acestor pericole se află în dinamica socio-militară, în conflictualitatea intereselor şi, deci, a politicilor şi strategiilor de punere în operă a acestora. Există încă numeroase puncte care se pot constitui în nuclee divergente între ţări sau între grupuri de ţări. Acestea ţin de dinamica intereselor, mai ales a intereselor economice şi politice, în termeni de putere, dominanţă şi influenţă. Parteneriatele strategice vizează tot aceşti parametri: puterea şi influenţa.

Strategiile de parteneriat, cele de alianţă şi coaliţie sunt impuse, pe de o parte, de universalizarea marilor pericole şi ameninţări nucleare, teroriste, de falii geopolitice şi geostrategice care pot fi oricând reactivate şi, pe de altă parte, de nevoie reconfigurării şi redimensionării raporturilor internaţionale în termeni de acces la resurse, la finanţare şi la marile pieţe.

Aceste determinări impun cooperarea şi colaborarea, evitare conflictelor armate şi a războaielor distrugătoare. Dar tot ele adâncesc decalajele, măresc faliile şi generează conflictualitate în întreg spectrul: simetric, disimetric şi asimetric.

Etnice

Interne

- Recrudescența presiunilor identitare ale unora dintre etnii;
- Acțiuni de autonomizare a diferitelor zone pe criterii etnice;
- Crearea unui suport economic, cultural, informațional şi internațional pentru o eventuală escaladare a diferendelor;
- Realizarea unor organizații (legale sau ilegale) care cultivă disensiuni între etnii sau creează presiuni generatoare de tensiuni şi conflictualitate;

Externe

- Presiuni exercitate de anumite grupuri, în numele unor organisme şi comunități, pentru fragmentarea (federalizarea) unor țări sau pentru acordarea unor autonomii teritoriale etnice;
- Presiuni exercitate de unele țări pentru protecția unor etnii din alte țări;
- Sprijinirea unor revendicări teritoriale;
- Sprijinirea acțiunilor de tip terorist (de către Al-Qaeda dar nu numai) efectuate de unele grupări etnice împotriva statelor din care fac parte.

Cauzele unor astfel de pericole şi amenințări rezidă, pe de o parte, în moşteniri istorice nefericite, în nedreptăți al istoriei, în falii lăsate de imperii şi neacoperite până azi şi, pe de altă parte, în decalajele economice foarte mari, în procesul frontierelor înghețat prin tratate şi convenții, dar, în realitate, neterminat sau neacceptat (în forma actuală) de unele dintre țările care se consideră frustrate sau nedreptățite de tratatele de pace şi de alte documente internaționale. Chiar dacă, în aceste condiții, când mai toate țările europene sunt preocupate de consolidarea unității continentului, de reuşita integrării europene, problemele frontierelor par desuete, dacă nu se au în vedere toate determinările şi implicațiile acestui proces complex şi permanent (procesul frontierei nu se încheie niciodată), acestea pot reveni spectaculos şi dramatic în tensiuni şi conflicte greu de rezolvat.

Religioase

Interne

Marea majoritate a populațiilor de pe continentul european sunt statornice din punct de vedre religios. Chiar dacă religia, odinioară, a creat cruciadele şi inchiziția, lucrurile s-au schimbat radical în zilele noastre. Religia face parte din civilizația modernă a continentului european şi din cea a continentului american şi ea cultivă armonia, încrederea, toleranța, cooperarea şi pacea. Cu toate acestea, în această epocă de foarte grele încercări pentru planetă, când peste 45 de milioane de oameni mor anual de foame şi de malnutriție[18], nici religiile nu rămân neafectate. Mai ales cele din zonele de falii profunde, sunt afectate de fundamentalism şi de alte pericole amenințări generatoare de tensiuni şi conflicte, atât în interiorul lor, cât şi în sfera socială, politică şi economică. Conflictul dintre şiiți şi sunniți, fundamentalismul islamic, fenomenul sectelor şi al terorismului de sorginte religioasă sunt doar câteva din realitățile care amplifică foarte mult conflictualitatea vremurilor în care trăim. Există, în acelaşi timp, şi unele acțiuni îndreptate împotriva unor fețe bisericeşti, probabil şi cu scopul de a slăbi încrederea populațiilor în biserică şi a adânci şi mai mult starea de haos care se află o

[18] http://www.iss-eu.org, L'Institut d"Etudes de Sécurité de l"Union Européenne, *Une Europe sure dans un monde meilleur. Stratégie européenne de Sécurité*, 2005, p. 6.

parte a planetei, îndeosebi regiunea Orientului Mijlociu şi Apropiat. eroare. Credința lor este statornică şi nu poate fi influențată prin strategiile de imagine.

Pericolele şi amenințările de sorginte religioasă sau pe suport religios :

- Acțiuni ale fundamentalismului islamic şi ale altor organizații religioase extremiste pentru fel de fel de revendicări, cele mai multe dintre acestea fiind de natură politică;

- Discuții şi chiar conflicte între biserici (catolici, greco-catolici, ortodocşi etc.) pe teme de patrimoniu;

- Acțiuni extremiste ale unor secte religioase etc.

Cele mai multe dintre pericolele şi amenințările de sorginte religioasă se desfăşoară în Orientul Mijlociu şi în Orientul Apropiat, dar ele pot fi întâlnite şi în Asia de Sud-Est, îndeosebi în Indonezia, în Japonia, în China, în țările din Asia Centrală, pe Valea Fergana, în Caucaz şi în multe alte locuri de pe planetă. Practic, nu există continent unde să nu se manifeste, într-o formă sau alte, extremismul religios.

Provocările, pericolele, amenințările şi riscurile asociate acestora mai pot fi analizate şi în funcție de alți factori, întrucât ele eu o durată şi o anumită frecvență (chiar dacă sunt aleatoare), se desfăşoară pe o anumită arie geografică, au anumite intensități şi generează efecte dintre cele mai complexe.

În funcție de timp:
- Prezente (asumate deja);
- Viitoare:
- Imediate;
- Apropiate;
- Pe termen mediu;
- Pe termen lung.
- Permanente.

În funcție de aria geografică şi spațială:
- Externe:
- Globale;
- Zonale.
- Interne;
- Cosmice
- Cyberspațiale.

În funcție de volum:
- Mici;
- Mari;
- Foarte mari.

În funcție de importanță (de interese, de gravitate):
- Vitale;
- Foarte importante;
- Importante
- Comune.

În funcție de probabilitate:
- Sigure (asumate);
- Previzibile (potențiale, probabile);

- Imprevizibile;
- Aleatoare.

După François Caron, elementul esențial al analizei riscurilor ține de ceea ce se numește de obicei „tendințe grele“, adică de acele elemente invariante sau puțin variabile în timp şi care sunt susceptibile de a fi totdeauna prezente în panorama politică şi strategică la termenul scadent[19]. De asemenea, în analiza unui pericol, a unei amenințări şi a riscului asociat acestora, noțiunea de gravitate este mai importantă decât cea de probabilitate. Importanța unui pericol (risc) nu se apreciază numai în funcție de efectele sale instantanee sau de cele care pot fi previzibile la un moment dat. Trebuie să se țină seama că un fapt aparent mărunt, de îndată ce începe să se deruleze, poate constitui o anumită primejdie pentru un sistem prin cumularea altor fapte, precum şi prin extensia propriilor sale efecte.

Nu se poate elabora o politică eficientă de reducere a vulnerabilităților dacă nu se ține seama de anumite pericole, pentru simplul motiv că nu se cunosc – ele sau efectele lor –, ci trebuie să se aibă în vedere toate pericolele cu care societatea se poate confrunta şi toate riscurile pe care şi le poate asuma la un moment dat. Nu se poate stabili un concept strategic de combatere a acestora, atâta vreme cât unele sau altele dintre ele sunt ignorate. Pericolul se concretizează atunci când apare o destabilizare, când găseşte punctul slab sau starea de inferioritate a celui amenințat. De cele mai multe ori, de-a lungul secolelor, avantajul care se preconiza sau se urmărea era de ordin teritorial. Acum se pare că balanța se înclină în favoarea unui câştig în plan economic, politic, cultural, în termeni de putere şi de influență etc. Aparent. Pentru că, în realitate, şi în condițiile în care se pare că aria geografică nu mai are mare importanță, lupta cea adevărată se dă tot pentru spațiu, chiar dacă el se exprimă mai mult în parametrii economici, politici (de putere şi de influență), culturali sau morali. Între etapa riscului virtual şi etapa concretizării lui, se situează etapa riscului potențial[20]. De fapt, analiza operează cu riscuri potențiale care au diferite grade de probabilitate, în funcție de care se stabilesc cele dintâi coordonate ale conceptului strategic.

Marile entități civilizaționale, provocări, pericole amenințări, riscuri

„Oamenii au fost impresionați, intrigați, ultragiați, speriați şi aduşi în stare de perplexitate de argumentul meu potrivit căruia dimensiunea centrală şi cea mai periculoasă a politicii globale pe cale de apariție va fi conflictul între grupuri ce aparțin de civilizații diferite“[21] spune Huntington chiar în prefața cunoscutei sale lucrări - „Ciocnirea civilizațiilor…“ – care a zguduit lumea. El citează, în continuare, în aceeaşi prefață, o frază care are valoarea de concluzie a cărții: „... ciocnirile dintre civilizațiile actuale reprezintă cele mai mari amenințări la adresa păcii mondiale, iar o ordine internațională bazată pe civilizații este cea mai sigură pază împotriva războiului mondial.“[22]

În continuare, ilustrul profesor de la Harvard împarte lumea în şapte sau opt civilizații: sinică, hindusă, japoneză, islamică, africană, ortodoxă, occidentală şi latino-

[19] www.stratisc.org/ , François Caron, L'APPRÉCIATION DU RISQUE MILITAIRE.
[20] Ibidem.
[21] Samuel P. Huntington, **CIOCNIREA CIVILIZAȚIILOR ŞI REFACEREA ORDINII MONDIALE,** Editura ANTET, 1998, p.11 (Titlu original: Samuel P. Huntington, 1997, **THE CLASH OF CIVILIZATIONS THE REMAKING OF WORLD ORDER**. Simon & Schuster).
[22] Ibidem

americană (aceasta din urmă poate fi însă integrată în civilizația occidentală). Fiecare din aceste civilizații are un stat-nucleu şi un grup de caracteristici.

În acelaşi timp, există un efort pentru realizarea unei noi ordini mondiale bazate pe multipolarism. Trecerea de la unipolarism la multipolarism presupune gruparea şi regruparea unor puteri regionale, fapt pentru care se vor crea noi echilibre şi, în acelaşi timp, noi adversități. Echilibrele se bazează pe parteneriate şi pe unitatea sistemelor de valori. Adversitățile, ca şi conflictualitățile, provin din confruntarea intereselor.

Conceptul fundamental al civilizației este cultura, iar conceptul fundamental al culturii este valoarea. Valoarea este confirmată de timp şi constă în tot ce a creat mai bun şi mai persistent omul, entitatea umană, comunitatea umană sau omenirea. Valorile nu sunt conflictuale. Ele se asamblează şi se armonizează în mari sisteme de valori. Iar sistemele de valori constituie cărămizile fiecărei civilizații şi ale civilizației universale. Valorile sunt fundamentele culturii şi ale civilizației. Sisteme de valori ridică civilizația mai sus, tot mai sus. Dacă există o unitate a lumii – şi, evident, o astfel de unitate există –, aceasta se bazează aproape în exclusivitate pe sistemele ei de valori.

Valorile se constituie în patrimonii. Aşadar, nu bătălia valorilor duce la crize, conflicte şi războaie, pentru că o astfel de bătălie nu a existat şi nu va exista niciodată, ci bătălia intereselor. Interesul este imboldul acțiunii, el împinge lumea înainte. Rezultatul acțiunii, confirmat de timp, poate deveni sau nu valoare. În această nouă confruntare, care nu este altceva decât o nouă fațetă a bătăliei intereselor, marile unități civilizaționale au un rol foarte important şi o responsabilitate imensă. Ele pot tempera ambițiile, vocațiile şi chiar interesele. Nu se ştie cine va ieşi învingător, se ştie însă că lumea nu este dispusă să accepte nici pierderile, nici câştigurile.

Deşi clasificarea pe care o face Huntington este restrictivă, simplificatoare şi chiar ofensatoare, ea ni se pare a fi destul de realistă (în sensul bătăliei intereselor unor entități politice pe suport civilizațional) pentru a-i putea asocia principalele riscuri cu care fiecare se confruntă. (Anexa nr. 2)

1.2. Configurația de rețea şi sporirea interdependențelor

Rețeaua introduce dimensiunea orizontală în relațiile interumane, în toate componentele lor. Orizontalitate nu înseamnă însă egalitate, ci doar posibilitate de comunicare, acces la informații şi transmitere rapidă a oricărui eveniment ce se petrece în rețea (evident, dacă nu există restricții). Oricum, restricțiile sunt mult mai puține şi mai puțin stresante decât imposibilitatea de a comunica. Rețeaua introduce însă o nouă dimensiune, extrem de importantă în dinamica sistemelor şi proceselor: interdependența. Nu este vorba, desigur, de o interdependență totală, ci doar de o interdependență în spațiul comunicării, al informației. Se pare că, astăzi, informația, ca nedeterminare înlăturată, devine din ce în ce mai mult, o funcție a rețelei. Bineînțeles, nu rețeaua creează informația. Ea doar o adăpostește şi o transmite.

1.2.1. Mutații produse de implementarea rețelelor

Informația face parte din această lume şi există în măsura în care lumea există şi are nevoie de informație, în sensul adâncirii cunoaşterii şi în cel al facilitării acțiunii. Fără informație, nu există nici viață, nici cunoaştere, nici acțiune, aşa cum nici informația nu poate exista decât în măsura în care, în calitate de funcție a sistemelor integrale vii, foloseşte inteligenței şi acțiunii umane. Spațiul în care viețuieşte, se generează, se regenerează, se transmite şi se înmagazinează informația se numeşte

cyberspațiu.[23] Cyberspațiul este, prin excelență un produs al rețelei. La această realitate virtuală au contribuit, deopotrivă, printre cei dintâi, medicul militar român Ştefan Odobleja, în lucrarea sa „La psychologie consonantiste“, şi Norbert Wiener, în „Cibernetica sau sistemele de comunicare la om şi maşină“, dar şi Shanon, cel care a creat aparatul matematic pentru analiza informației, între care şi celebra formulă a entropiei:

$$H_x = -x\sum_{i=1}^{n} p_{xi}.\log\ p_{xi}$$

Dar, acolo unde există informație, există şi conflict, există şi război, şi, în primul rând, un război al informației. Din care se nutresc toate celelalte. Iar acolo unde există război, există şi strategie. Rezultă că războiul informației se desfăşoară în cyberspațiu, iar strategia acestui tip de război am putea s-o numim, pentru a o distinge de celelalte strategii (terestre, navale, aeriene, economice, politice, sociale, de coaliție, de alianță, de globalizare, identitare etc.), cyberstrategie. Ea nu poate fi altceva decât o dialectică a voințelor care se confruntă în acest spațiu al rețelei virtuale pentru a-şi impune, unele altora, un anumit tip de comportament, pentru a gestiona o situație conflictuală sau pentru a realiza un anumit tip de dominanță strategică informațională.

Fără a se separa integral de strategiile care modelează celelalte tipuri de războaie sau de confruntări, cyberstrategia se limitează, totuşi, la cyberspațiu. Ea răspunde, bineînțeles, prin mijloace ştiințifice, pragmatice şi creative, unei politici sau unor politici privind cyberspațiul, dar rămâne tot atât de „pământeană“, de realistă sau de fantezistă, precum sunt sau pot fi respectivele politici. Nu există, deci, o singură cyberstrategie, ci atâtea tipuri de cyberstrategii câte tipuri de cyberpolitici se bat sau se zbat în acest nou spațiu, deopotrivă virtual şi real. Toate aceste cyberstrategii au însă comună *teoria cyberstrategiei*, care include un sistem coerent de teorii, principii, reguli şi norme cu care operează toată lumea şi care se constituie într-un limbaj ştiințific comun pentru a opera cu aceleaşi concepte şi cu aceiaşi termeni. *Cyberpractica* şi *arta cyberstrategică* țin însă de experiență şi, respectiv, de capacitatea de creație şi de construcție în spațiul virtual.

Cyberstrategia este un domeniu relativ nou al strategiei. Este, de fapt, o nouă strategie care, la fel ca oricare altă strategie, se compune dintr-o *cyberstrategie a forțelor* (marile corporații, entitățile din spațiul informațional, unități militare sau civil-militare speciale, care gestionează sistemele de comunicații, alte forțe, inclusiv hackerii şi cyberpirații), o *cyberstrategie a mijloacelor hardware şi software* şi o *cyberstrategie a acțiunilor şi operațiilor* care se desfăşoară în cyberspațiu.

Structura de rețea – îndeosebi de rețea informatică – a devenit esențială în societatea modernă. Toate relațiile economice, sociale, politice sunt dependente de această rețea informatică omniprezentă şi omnipotentă, care capătă din ce în ce mai mult o dimensiune mondială. Noua rețea – de fapt, noile rețele, pentru că există numeroase rețele şi nu doar una singură –, care se prezintă, deci, ca o *rețea de rețele*, creează în jurul ei un spațiul specific, deopotrivă virtual şi real – spațiul cibernetic sau *cyberspațiul*. Acest spațiu se cere identificat, localizat (chiar dacă este fluid şi flexibil), analizat, cunoscut, modelat şi securizat. Încă de la crearea sa, el este amenințat continuu, adăposteşte şi, în acelaşi timp, suportă numeroase atacuri: acces fraudulos la informație; atacuri informaționale (viruşi, viermi, bombe logice, troieni), spams-uri, email-uri bombe[24] etc., precum şi un sistem dinamic şi coerent de protecție împotriva acestor

[23] Gheorghe Văduva, *Cyberstrategia*, în *Gândirea militară românească*, nr. 2/2006
[24] www.smsi-territoires.net/article44.html , Olivier Itéanu, *Sauver la société de l'information*

atacuri şi de reacţii. Este însă timpul să fie concepute şi unele acţiuni preventive, care să diminueze şi chiar să anuleze, în anumite componente, ameninţarea din cyberspaţiu.

În 2002, Administraţia George W Bush publica o versiune provizorie a *Strategiei Naţionale de Securitate a Cyberspaţiului* (National Strategy to Secure Cyberspace). Ultima versiune fusese publicată sub Administraţia Clinton, în 2000. Cea de a doua versiune avea în vedere şi experienţa dramatică a atacurilor teroriste de la 11 septembrie 2001. Richard Clarke, la acea dată, consilier special al preşedintelui pentru securitatea cyberspaţiului, este cel care a coordonat elaborarea acestui document deosebit de important nu numai pentru Statele Unite, ci şi pentru Canada şi Mexic, adică pentru întreaga reţea de informaţii a Americii de Nord. Această strategie[25] s-a dorit a fi o interesantă foaie de parcurs în legătură cu ceea ce trebuie să facă industria, guvernul şi persoanele private pentru a asigura securitatea reţelelor.

Doua chestiuni sunt foarte importante în această strategie. În primul rând, toată populaţia ţării şi fiecare cetăţean consumator de informaţie în parte, şi nu numai guvernul, trebuie să-şi asume responsabilitatea securizării acelei părţi din cyberspaţiu care-i revine nemijlocit, întrucât problema ameninţărilor contra cyberspaţiului nu poate fi lăsată exclusiv în grija militarilor şi forţelor de ordine. Este una dintre marile mutaţii pe care le introduce reţeaua. În viziunea americană, universităţile, diverse sectoare ale economiei, proprietarii de infrastructuri esenţiale, ca şi cei ai reţelelor de distribuţie a electricităţii şi cei ai reţelelor de telecomunicaţii trebuie să-şi protejeze reţelele lor. În al doilea rând, ţara trebuie să treacă de la *paradigma ameninţării* la cea a *vulnerabilităţii*. Până la atacurile din 11 septembrie 2001, guvernul, şi doar guvernul, era acela care trebuia să semnaleze prezenţa pericolelor şi ameninţărilor şi să-i consilieze pe toţi cei vizaţi în ceea ce priveşte măsurile de securitate a reţelelor. Potrivit noii strategii elaborată în 2002, guvernul a trecut de la reglementări şi impuneri la a transfera (delega) tuturor americanilor „puterea de a-şi proteja propria lor parte din cybespaţiu". Pentru aceasta, guvernul şi asumat următoarele activităţi:

- să educe şi să sensibilizeze utilizatorii şi proprietarii de cyberspaţiu în legătură cu toate riscurile şi toate vulnerabilităţile posibile;
- să creeze noi tehnologii de securitate;
- să formeze specialişti şi mână de lucru cu înaltă calificare în domeniul cybersecurităţii;
- să promoveze sensul responsabilităţii particularilor, întreprinderilor şi sectoarelor de securitate la toate nivelurile, recurgând la forţele pieţei, partenariatelor sectoarelor publice şi private şi la reglementările legale necesare;
- să sporească cybersecuritatea federală, astfel încât aceasta să devină un model pentru celelalte sectoare;
- să stabilească mecanismele de prealertă şi de diseminare eficace a informaţiei sectoarelor publice şi private (şi între ele), pentru ca orice atac să fie descoperit imediat şi să se poată interveni eficient.

Iată o modalitate de pregătire a populaţiei pentru a face faţă celei mai periculoase crize şi celui mai periculos şi mai probabil dintre războaiele care se profilează la început de mileniu. Fără a se exclude şi alte tipuri de războaie – războiul terorist, războiul nuclear, războiul frontalier, războiul de gherilă, războiul mozaic, în general –, oamenii responsabili se gândesc la pregătirea naţiunii pentru un război al viitorului care, fără îndoială, va fi un cyberrăzboi. Nu neapărat un război al roboţilor, ci un război al computerelor, al reţelelor, al hackerilor, al societăţii informaţionale, cybernetice, epistemologice împotriva celor care-i contestă realitatea sau care o ameninţă şi o

[25] http://www.securecyberspace.gov

vulnerabilizează. Acest război deja a început, este în curs de desfăşurare şi se pare că nu va înceta niciodată.

Documentul a fost divizat în cinci secţiuni: utilizatorii la domiciliu şi micile întreprinderi; marile întreprinderi; sectoarele esenţiale, îndeosebi cele guvernamentale, sectoarele private şi universităţile; priorităţile naţionale; sectoarele de importanţă mondială. La fiecare nivel, au fost stabilite obiective strategice pentru toţi utilizatorii şi realizate programe, recomandări şi subiecte de dezbatere pentru a se realiza respectivele obiective. Documentul este însoţit, în anexe, de planuri concrete de protecţie a infrastructurilor esenţiale ale sectoarelor bancare şi financiare, energiei electrice, petrolului, gazelor, apei, transportului, îndeosebi a feroviar, informaţiei şi telecomunicaţiilor şi, bineînţeles, produselor chimice. Ele sunt publice şi pot fi consultate pe site-urile http://www.ciao.gov sau http://www.pcis.org.

Aceste planuri sunt puse în aplicare împreună cu Canada şi cu Mexic şi permit securizarea numeroaselor infrastructuri esenţiale (EI) comune de informaţii ale Americii de Nord.

Există numeroase alte recomandări conţinute în acest document cu privire la strategia de securitate a cyberspaţiului, între care se află şi următoarele:

- guvernul federal trebuie să efectueze o examinare completă a randamentului Programului Naţional de Siguranţă a Informaţiei (National Information Assurance Program (NIAP), în senul extinderii lui asupra tuturor achiziţiilor guvernamentale de tehnologie a informaţiei (IT);

- universităţile au obligaţia să stabilească unul sau mai multe centre de partajare şi analiză a informaţiei (ISAC) pentru a sesiza cyberatacurile şi vulnerabilităţile la acestea;

- sectoarele private trebuie să creeze astfel de centre de analiză şi partajare a informaţiei (ISAC), care să analizeze ecarturile pentru sectoarele tehnologiei şi ale R&D şi să stabilească practici sectoriale;

- furnizorii de servicii Internet (FSI) au obligaţia să adopte un „cod de bună conduită“ în materie de cybersecuritate;

- guvernul federal a instalat un sistem de alertă (Cyber Warning Information Network – CWIN) în centrele guvernamentale şi non-guvernamentale-cheie de operaţiuni de cybersecuritate, cu scopul de a analiza, avertiza şi coordona acţiunile în situaţiile de criză;

- toţi cei implicaţi, inclusiv comercianţii de material electronic şi de programe, au obligaţia să creeze un Centru de Operaţii de Reţea în Cyberspaţiu (Cyberspace Network Operations Center – Cyberspace NOC).

Impactul imediat al acestei strategii americane de securitate a cyberspaţiului l-a constituit sporirea atenţiei asupra Canadei şi Mexicului şi consolidarea, împreună cu aceste ţări, a mediului de securitate a cyberspaţiului. De aici nu rezultă că atacurile hackerilor şi cyberpirateria ar fi încetat, ci doar că au fost intensificate măsurile de cybersecuritate.

Din acest motiv, în SUA şi în Canada, ca şi în ale ţări, utilizarea neoficială a sistemelor informatice constituie o infracţiune foarte gravă care se pedepseşte cu cel puţin zece ani de închisoare.

Cele mai vulnerabile la aceste atacuri sunt întreprinderile mici şi utilizatorii particulari. Timpul acelui „eu sunt prea mic pentru a fi atacat“ a trecut.[26] Oricine poate deveni azi ţintă în cadrul războiului reţelelor sau al războiului în reţea. Nici marile întreprinderi sau marile organizaţii nu sunt scutite de aşa ceva. Dar, spre deosebire de marile corporaţii, întreprinderile mici sau acele organizaţii familiale, care trăiesc de azi

[26] www.smsi-territoires.net/article44.html, Olivier Itéanu, *Ibidem.*

pe mâine şi pentru care achiziționarea de calculatoare, de programe şi de licențe pentru fiecare calculator reprezintă un efort considerabil, nu dispun de strategii adecvate de securizare a sistemelor şi nici de acea cultură de securitate care se realizează în marile întreprinderi, în marile organizații naționale, internaționale sau transnaționale.

Mai mult, împotriva micilor utilizatori şi a întreprinderilor mici s-a declanşat un adevărat cyberterorism, pe de o parte, de către tot felul de profitori şi de speculanți şi, pe de altă parte, de anumite cercuri de interese şi chiar de autorități. De asemenea, în multe state, s-a elaborat o politică represivă fără nuanțe şi discernământ, care-i loveşte, bineînțeles, tot pe cei slabi în materie de securitate a cyberspațiului. Este vorba, între alții (dintre cei loviți), şi de operatorii de telecomunicații care trebuie să păstreze datele tehnice de conexiune timp de un an, altfel sunt pedepsiți cu închisoare. Nu se defineşte însă foarte exact care sunt aceste date şi ce înseamnă conservarea lor. Sunt vizați, de asemenea, şi utilizatorii care, dintr-o eroare, pot accesa informații pentru care nu au autorizarea necesară.

Cei care folosesc Internet-ul ca sursă de documentare ştiu ce înseamnă acest lucru. Legislația din domeniu a creat un adevărat hiat între „lumea numerică“ şi lumea reală. Se pare că legile din una nu sunt valabile şi în cealaltă. De aceea, una dintre prioritățile strategice ale acestei epoci este să se realizeze integrarea sau, mai bine-zis, reintegrarea celor două lumi, care, de fapt, sunt una şi aceeaşi. În acest sens, se impune un cod de conduită obligatoriu pentru toți cei care intră în rețea, dar şi găsirea unor modalități de depistare a „violatorilor de rețea“ din masa celor care nu doresc altceva decât să aibă acces, potrivit necesităților lor, la informație, în virtutea libertății informației şi dreptului de a fi informați.

Desigur, măsurile de securitate a cyberspațiului şi de siguranță a utilizatorilor autorizați sunt absolut necesare, întrucât la nivelul rețelelor mari (financiare, economice, de corporații, Internet etc.), fără un sistem drastic de securitate, s-ar crea o stare de haos. Dar de aici şi până la a sancționa cu zece ani de închisoare un utilizator care a intrat în rețea şi, aproape fără să-şi dea seama, a accesat sau a încercat să acceseze, sisteme informatice pentru care nu a fost autorizat, ar trebui să fie o cale lungă. Această cale nu există, întrucât rețelele sunt extrem de dinamice şi, în multe cazuri, foarte vulnerabile. Noii intrați în acest sistem, îndeosebi cei din țările care s-au aflat o jumătate de veac sub autoritatea comunistă, nu au avut timpul necesar pentru a-şi forma o cultură strategică şi informațională necesară filosofiei de rețea, adică o cybercultură. Pentru aceasta, va trebui să treacă un timp şi, poate, chiar o generație, dacă nu chiar două.

Chiar dacă nu suntem de acord cu o legislație atât de aspră, care poate fi aplicată fără discernământ în cazul accesului la informația din rețea, se pare că a sosit timpul punerii unei anumite ordini în rețea. Unii consideră însă că o astfel de ordine deja există, întrucât o rețea de tipul Internetului sau al rețelelor Kazza n-ar putea funcționa fără anumite reguli, fără o anumită disciplină de rețea.

Cui aparține dimensiunea creativă în acest imens domeniu care cuprinde întreaga planetă? Cine domină şi cine va domina arta cyberstrategică a începutului de veac? Marii creatori de programe? Hackerii? Pirații rețelelor? Marile şcoli de informatică? Marea finanță? Marile corporații cu interese mondiale, care domină lumea? Sau, într-un fel, toate acestea la un loc? Se va declanşa oare o competiție între ele pentru dominarea rețelelor?

E greu de dat un răspuns tranşant. Unii spun că, de fapt, îndeosebi, rețeaua Internet, dar şi alte rețele, nu reprezintă altceva decât o modalitate militară voită, planificată, experimentată şi foarte bine dirijată de gestionare a informației lumii, iar principalii ei beneficiari s-ar afla la Pentagon. Dacă ar fi aşa, probabil că evenimentele

de la 11 septembrie 2001 nu ar fi avut loc, sau, în orice caz, nu în sensul în care sunt cunoscute azi.

Noua fizionomie a relațiilor internaționale, definită pe o filozofie de rețea, care se prezintă a fi cu totul nouă şi încă destul de greu de înțeles în toate determinările sale, implică foarte multe elemente şi domenii imprevizibile. Este posibil ca cyberstrategia şi, respectiv, arta cyberstrategică, să cunoască mai multe niveluri de competențe şi de angajare, unele dintre ele situându-se foarte aproape de lumea reală, altele continuând mai departe gestionarea noului război de pe un teatru, deopotrivă, virtual şi real, numit cyberspațiu.

În 1999, un consultant pe probleme de securitate de la societatea Crypton din Ontario, Canada, a descoperit (cel puțin aşa a crezut) o poartă ascunsă în modulul de securitate Windows NT 4.0, program folosit de zeci de milioane de utilizatori de rețea profesionişti, care permitea Agenției Naționale de Securitate (National Security Agency – NSA) să decripteze, prin intermediul unei chei (NSAKEY), comunicațiile protejate. Desigur, unul dintre purtătorii de cuvânt ai lui Microsoft a dezmințit formal aceste afirmații, iar NSA, cum era şi firesc, i-a trimis pe toți curioşii spre Microsoft. (ZDNet 7.09.99). Problema însă rămâne, şi nimeni nu ştie dacă afirmațiile acestui consultant sunt sau nu pe deplin justificate. Ea ține, desigur, de confruntarea care există în cyberspațiu, de strategiile de acțiune şi de contraacțiune.

Cam în aceeaşi perioadă (deci înaintea atacurilor de la 11 septembrie 2001), un raport al unei comisii federale americane releva o amenințare teroristă majoră care consta în cyberatacuri asupra controlorilor aerieni şi într-o posibilă agresiune bacteriologică asupra oraşelor americane. Era un raport de 143 de pagini, rod al activității Comisiei Americane asupra Securității Naționale, compusă din 25 de experți, care avertiza că, în anii următori, americani vor fi din ce în ce mai vulnerabili, inclusiv la cyberatacuri.

Începând din 1999, au fost clonate de cyberterorişti milioane de pagini Web prin care cei ce navigau pe Internet erau deturnați spre site-uri cu conținut pornografic. În aceste site-uri Web, erau inserate comenzi care deschideau pagini porno şi dezactivate comenzile pentru ieşirea din acestea. Deci, cel care intra, fără voia lui, într-un astfel de site, nu putea ieşi decât dacă închidea calculatorul. Un terorism ieftin, aparent o glumă de prost gust. În realitate, era vorba de cu totul altceva. Era un atac psihologic, cu efecte foarte puternice în lumea americană, educată în spiritul unor valori foarte importante pentru Statele Unite. Or, prin pornografie, tocmai aceste valori erau vizate şi lovite. A fost o problemă extrem de complicată în Statele Unite, care nu a fost încă rezolvată pe deplin.

Departamentul Apărării, datorită unui laborator care a costat 15 milioane de dolari şi unei echipe formată din 80 de anchetatori, a încercat să oprească cyberpirații şi cyberspionii, să recupereze mai uşor fişierele şterse sau sustrase. Laboratorul a pretins că poate localiza precis cyberpirații, efectuând rapid căutări în zeci de milioane de documente şi reuşind să citească fişierele şterse de către proprietarii lor. În septembrie 1999, s-a făcut chiar o demonstrație prin care au fost recuperate informațiile de pe o dischetă făcută bucățele.

Un cyberpirat român – Mircea Harapu, de 23 de ani, din Timişoara – a fost deferit Justiției, în octombrie 2000, întrucât a încercat să escrocheze firma americană Zwirl Com din New York de suma de 5.000 de dolari. El a reuşit să intre în serverul firmei şi să sustragă unele date confidențiale. În SUA, astfel de infracțiuni se pedepsesc cu 15 ani de închisoare. În România, la vremea aceea, legislația era ca şi inexistentă. Fenomenul

face parte din sistemul infracţiunilor pe Internet şi constituie una dintre ameninţările majore ale acestui secol. Nu este însă cea mai periculoasă.

În 2003, spre exemplu, piraţii informaticieni au spart de mai multe ori codurile guvernului federal canadian, reuşind să acceseze reţelele Ministerului Apărării. Echipa de Reacţie la Incidentele Informatice (ERRI) a Ministerului Apărării a întocmit un raport în care se arăta că s-au petrecut 160 de asemenea incidente. Sistemele informatice federale canadiene, potrivit acestui raport, nu sunt vulnerabile numai la atacuri teroriste, ci şi la incursiunile serviciilor de informaţii străine. Este aproape imposibil să fie eliminate riscurile de piraterie în sistemele informaţionale, dată fiind evoluţia spectaculoasă a mijloacelor informatice accesibile spărgătorilor. Acelaşi raport semnala cinci cazuri de intruziune pentru „informaţii privilegiate“ în reţeaua Ministerului Apărării, ceea ce reprezintă cea mai gravă atingere posibilă printre cele şapte niveluri de violare pe care le definesc autorităţile canadiene. S-au semnalat, de asemenea, cinci cazuri de „acces limitat neautorizat“ şi 35 de tentative de infectare cu un virus, cu un vierme informatic sau cu un program nesolicitat, iar pe plan intern 110 cazuri de lipsă de securitate. Acestea sunt cazuri semnalate la 14 iulie 2004 de presa canadiană, datele provenind de la Centrul de securitate a telecomunicaţiilor, un organism ultrasecret al guvernului, însărcinat cu spionajul electronic şi cu protecţia sistemelor informatice federale[27].

Există, desigur şi alte modalităţi de a accesa anumite ordinatoare. FBI a reuşit să atragă în Statele Unite, la firma Invita, o întreprindere montată cu piese de ocazie, doi cyberpiraţi ruşi, promiţându-le posturi de consultanţi în securitatea informatică a acestei firme. Înainte de a fi arestaţi, li s-a cerut să demonstreze ce ştiu să facă. Li s-a pus la dispoziţie un ordinator a cărui tastatură era supravegheată. Fiecare apăsare de tastă era înregistrată. În acest fel, FBI a obţinut informaţiile şi parolele necesare pentru a avea acces la 250 gigaocteţi de date compromiţătoare asupra ordinatoarelor suspecte din Rusia. În timpul procesului, s-a discutat mult pe tema metodelor FBI, relevându-se şi alte cazuri – spre exemplu afacerea Mafiaboy – în care s-a colaborat cu autorităţile din ţara respectivă. Cei doi piraţi ruşi au fost acuzaţi de mai multe infracţiuni asupra întreprinderilor americane, fiind bănuiţi că ar fi sustras în jur de 300.000 de numere de cărţi de credit.

De-a lungul anilor, au apărut numeroase firme de securitate pe Internet, iar programele au fost dotate cu componente de securizare şi de protecţie a datelor mai simple sau mai sofisticate, care se reînnoiesc şi se complică de la an la an. În acest fel, numeroase atacuri ale cyberteroriştilor sunt prevenite şi stopate, dar unele, totuşi, reuşesc. Programele din ce în ce mai puternice, conexiunile de mare debit permit să se copieze ilegal, în doar câteva secunde, tot ce se doreşte a fi sustras şi cunoscut, inclusiv baze de date, proiecte de programe de modernizare şi dezvoltare, studii de marketing şi tot ce se mai poate spiona în domeniul economic, social, informaţional şi militar. Acestea îngreunează sistemele de securitate, dar ele nu încetează să ţină pasul şi să asigure, totuşi, o bună protecţie celor care apelează la ele.

Încă din octombrie 1998, Congresul american a elaborat o lege de copyright în domeniul numeric, care punea în aplicare tratatele semnate la Geneva în decembrie 1996 privind proprietatea intelectuală. Desigur, cei mai interesaţi în acest domeniu au fost şi au rămas producătorii şi proprietarii de soft-uri, îndeosebi în domeniul divertismentului (jocuri), şi mai puţin interesaţi oamenii de ştiinţă, bibliotecarii şi academicienii.

[27] http://fiweb.9online.fr/chronicnet61.htm.

În cyberspațiu, există un război continuu, cu mii de bătălii şi miliarde de confruntări. Am putea spune că niciodată, pe această planetă, nu a existat o confruntare mai complexă, mai violentă şi mai neiertătoare, precum cea actuală din cyberspațiu. E drept, acest cyberrăzboi nu produce, în mod nemijlocit, milioane de morți şi răniți, nu presupune ciocniri sângeroase cu sabia, cu aviația strategică sau cu rachetele Tomahawk. Bătăliile se desfăşoară, în primul rând, pentru controlul informației, pentru finanță şi putere. Beligeranții sunt, în primul rând, marile firme producătoare de hardware şi software, de jocuri şi alte produse de consum electronic şi informațional. Victimele sunt dependenții. Se ştie despre Sindromul Dependenței de Internet (SDI). El este deja în atenția specialiştilor şi, deocamdată, nu există un tratament pe măsură. Războiul clasic produce morți, răniți, traume psihologice şi pagube materiale. Impactul sângelui vărsat este puternic şi, de aceea, el este din ce în ce mai mult evitat în lumea civilizată. Dar lumea aceasta nu poate renunța nici la afaceri, nici la confruntare. La urma urmei, însuşi războiul, în epoca societății cunoaşterii, a societății cibernetice sau epistemologice, este privit şi tratat ca o afacere. Războiul bazat pe Rețea, noul concept fundamentat, dezvoltat şi aplicat de americani în ultimele războaie, mai ales în războiul din Irak din martie-aprilie 2003, este privit, evaluat şi dezvoltat ca o afacere, din perspectiva sistemelor dinamice complexe.

Ceea ce se ştie se referă mai ales la confruntarea dintre marii producători de pe piața hardware şi software, iar bătălia se duce în principal pentru cucerirea sau dominarea acestor piețe de mii de miliarde de dolari. Dincolo de concurență şi de aceste bătălii fireşti, se află însă adevăratele dimensiuni ale strategiilor de dominare politică, economică, financiară, informațională şi, ca ultim suport al acestora, militară a lumii.

Când, la o masă de joc, jucătorii sunt de aceeaşi categorie, nimeni nu-şi pune probleme. Jocul este chiar interesant. Dar când un jucător devine mult prea puternic, atunci lucrurile se schimbă. Jucătorii nu mai pot părăsi masa, decât falimentați, în virtutea regulilor stabilite, iar cel puternic înghite totul până ce este şi el atacat din toate părțile. A fost cazul lui Napoleon Bonaparte. Regii europeni nu l-au iertat, întrucât nu făcea parte din lumea lor, iar când a devenit prea puternic, l-au lovit şi l-au distrus. Este şi cazul Microsoft. Arogantul Bill Gates a fost nevoit să demisioneze pentru a lăsa frânele unui amic de-al său de 30 de ani. În acest timp, s-a deschis un alt mare front, cel al Internet-ului. AOL, datorită supercapitalizării bursiere, cumpără Time-Warner, plătind acțiunile acesteia cu 71% mai mult decât valoarea lor reală. Pe planul producției materiale, are loc o reînnoire incredibilă a lui Apple, dar Intel este pe punctul de a marşa pe o nouă platbandă. Apare, prin anii 2000, un nou monstru în ceea ce priveşte comercializarea cărții electronice, Amazon.com.[28] Un acord amiabil (dar confidențial) se produce la începutul anului 2000 între Caldera (fondată de creatorul lui Novvell) şi Microsoft, valorând vreo 250 de milioane de dolari. Acest conflict este legat de o poveste uitată, cea a lui Gary Kyldall, primul în lume care a realizat, în 1973, un program de interfață între un lector de dischete cu un microordinator, Intelec-8, denumit de autor sistem de exploatare CP/M (Control Program/Microcomputer). Au loc o serie întreagă de negocieri între IBM, Digital Researche etc. Steve Balmer negociază cu Gates licența SCP-DOS, o clonă a lui CP/M pentru 50.000 de dolari şi îl angajează pe Tim Paterson pentru a adapta sistemul la IBM PC. Odată cu sistemul de operare MS-DOS 1.0, care costă 60 de dolari, apare şi sistemul DR-DOS, mult mai puternic, dar şi de patru ori mai scump. În 1984, este propusă o interfață grafică pentru PC, identică din punct de vedere vizual cu cea de pe Mac, dar cu unele modificări cosmetice, pentru a se evita un proces. Dar nu numai Microsoft s-a inspirat de la Apple. Ştim foarte bine că, în

[28] Lafactory.com, Francis Rozange, *La guerre de l'informatique*, jeudi 23 juin 2005.

această perioadă, a apărut şi Ventura Publisher Xerox. Acesta este, de altfel, şi primul program pe care l-a achiziționat Grupul de Presă al Armatei Române, în 1991, împreună cu editorul de texte WordStar şi cu care au fost realizate o parte dintre publicațiile noastre din acea perioadă. A urmat apoi editorul de text, sub MS-DOS, Windows 1.0, un program mediocru, prezentat de Microsoft prin anii 1990, apoi versiunea 3.0, ajunsă şi la Grupul de Presă al Armatei (GPA) prin 93, urmată de 3.1, după care s-a trecut la folosirea unor editoare de text şi programe de tehnoredactare mai noi, care nu erau produse de Microsoft.

În timpul acesta, Microsoft a făcut o publicitate imensă lui Windows 3.0. Firma a riscat atunci foarte mult pentru o interfață grafică care se vindea cu 40 de dolari. Gary Kyldall a fost un informatician genial, iar Bill Gates şi Steve Allen au avut calitatea de comercianți geniali.

A urmat Windows 95, care combina DOS cu o interfață grafică. DR-DOS intră în dizgrație, în timp de Caldera deschide un OpenDos, folosit în sistemele Linux. Caldera atacă Microsoft pentru următoarele patru probleme:

- în mod voit, Microsoft a făcut ca Windows 3.1 să fie incompatibil cu DR-DOS, refuzând să furnizeze lui Novell un beta care i-ar fi dat acestuia posibilitatea să asigure respectiva compatibilitate;
- a utilizat tehnici de concurență neloială, deturnând consumatorii de le DR-DOS;
- a combinat artificial Dos 7 cu Windows 4, pentru a realiza Windows 95, distrugând astfel concurentul;
- a combinat Windows 98 cu Internet Explorer;
- a impus constructorilor o licență pentru fiecare calculator vândut, chiar dacă se instala un alt sistem de operare decât cel furnizat de Microsoft (licență pe procesor).

A fost un proces de pomină. Departamentul pentru justiție relevă unele practici interesante în acest sens. Judecătorul Jackson, spre exemplu, ar fi acuzat Microsoft de a fi falsificat un video. Se fac unele demonstrații – inaccesibile celor neavizați în electronică –, pentru a se demonstra că suprimarea lui Internet Explorer din Windows 98 nu scade performanțele acestuia etc. În această capcană, a intrat chiar şi unul dintre martori, profesorul de economie Richard Shamlensee. Acesta a încercat să demonstreze că Windows nu reprezintă un monopol, întrucât se vede amenințat de tehnologii rivale. Fiind întrebat care sunt acestea, profesorul n-a fost în măsură să spună nici măcar una.

Bătăliile se continuă. Este interesant cazul AOL, o societate de difuzare a informației pe Internet. Inițial, a avut loc o fuziune de zece miliarde de dolari între AOL şi Netscape. Într-o vreme, aceasta a fost considerată, de unii naivi, o operațiune importantă. AOL a cumpărat apoi 55 la sută dintre acțiunile firmei Time Warner cu mai mult de 160 de miliarde de dolari. A rezultat un grup cu o capitalizare de 300 de miliarde de dolari. În fruntea lui AOL, se afla Steve Case, care putea deveni la fel de celebru ca Bill Gates. În 1995, Microsoft lansează propriul său serviciu on line: MSN, care nu este, totuşi, o reuşită. AOL înghite rapid Computerserve, o rețea destinată profesioniştilor, apoi, după cum s-a văzut, Netscape şi, în cele din urmă, uriaşa societate Time Warner.

Din acest moment, există două viziuni destul de fixiste, maniace chiar, asupra cyberspațiului: Bill Gates, care doreşte ca programele sale să fie prezente în fiecare casă şi Steve Case, care vrea ca AOL să fie în fiecare cămin. Începe o bătălie frontală. AOL Time Warner face parte din primele cinci mari societăți ale planetei. Microsoft a investit cinci miliarde de dolari în AT&T şi trei miliarde în diferite alte societăți de telecomunicații, pentru a profita de lansarea probabilă a Internet-ului de mare viteză. Trebuia deci să existe în SUA două categorii de abonați: abonații la AT&T, care primesc un conținut editat de Microsoft, şi abonații lui Time Warner, alimentați de

AOL. Astfel, un război care a început în cyberspațiu pătrunde şi în lumea reală. În acelaşi timp, se declanşează şi un alt război pustiitor: cel de la bursă. Aici există o dublă scală speculativă: una, în media, care se consideră a reprezenta o investiție pentru câştigarea de noi clienți, şi cealaltă, în lumea reală. „Băieții de aur" nu ştiu care scală trebuie aplicată. Cea a Internet-ului sau cea a lumii reale?

În ceea ce priveşte speculațiile la bursă – acolo unde se duce, în mare măsură, şi o parte din acest omniprezent cyberrăzboi –, lucrurile s-au schimbat radical față de ideea tradițională a acestei instituții, unde, adesea se păstrau zeci de ani pachete de acțiuni pentru a fi puse în vânzare la timpul potrivit. Filozofia de rețea schimbă complet şi filosofia de bursă. La un moment dat, *Amazon.com* avea pierderi cumulate la 600 de milioane de dolari, iar valoarea acțiunilor era ca şi inexistentă. Numai că, în condițiile actuale, acest lucru nu are prea mare importanță, întrucât totalitatea acțiunilor disponibile pe piață se schimbă la fiecare două săptămâni, iar această firmă dispune de cel puțin treisprezece milioane de acțiuni care se schimbă în fiecare zi.

Războiul informatic cuprinde toate sectoarele culturale şi media. Industria de discuri a fost afectată de recrudescența lui MP3, în timp ce editorii de cărți tipărite vor fi destul de repede înghițiți de cartea electronică. Cu atât mai bine. Vor fi astfel salvate o parte dintre pădurile planetei, ceea ce va însemna foarte mult, întrucât un copac produce oxigen pentru 40 de oameni, iar o carte se citeşte mult mai uşor pe un computer portabil (care, în viitor, se va afla la îndemâna fiecăruia) decât într-o mare bibliotecă!

Cyberrăzboiul marilor giganți are efecte şi pe plan material, adică în lumea reală. Apple câştigă, datorită Imac, un mic sistem, puțin costisitor, care permite conectarea facilă la Internet. Intel, care a fost obligat să realizeze un Pentium 2450, dotat cu un accelerator, capabil să ruleze orice aplicație, vizează deja reconversia sa, mai întâi prin crearea unor centre server destinate să conecteze marile întreprinderi la NET şi, poate, orientându-se spre Linux, întrucât Windows nu este, în viziunea sa, nici suficient de stabil, nici suficient de suplu. Bill Gates s-a retras pentru a medita la epoca de după PC. Microsoft nu va dispărea de pe piață, datorită, în primul rând, uriaşelor investiții în cablu şi satelit. Dar va mai rămâne el multă vreme un gigant în domeniul programelor? Rămâne de văzut, întrucât, de-acum, este vremea Internet-ului. Arta cyberstrategică, în această epocă de început, se prezintă ca o uriaşă arhitectură fluidă, flexibilă, fractală. Totul se află în mişcare, în devenire, reperele sunt şi ele mişcătoare, informația se globalizează, filosofia de rețea începe să domine şi să schimbe lumea. Esența ei rămâne însă aceeaşi. Arta cyberstrategică, la fel ca oricare artă, are menirea de a proiecta şi construi strategii, de a adopta strategii sau soluții strategice adecvate, inteligente şi surprinzătoare, într-o lume în care totul se mişcă. Ea aparține, după cum s-a văzut şi din aceste câteva sumare exemple, nu numai specialiştilor în informatică (poate, lor le aparține cel mai puțin), cât mai ales oamenilor politici care se află imediat în fața şi pe suportul „comercianților de informație", băncilor şi universului noilor interese care se confruntă, strategilor care visează la un altfel de război, sau care se tem de vechiul şi terorizantul război de atriție, dorind să transfere atrița în domeniul terorismului sau contraterorismului electronic şi informațional. În fond, şi aici există un inepuizabil câmp de bătaie, iar generalii generoşi în a-l pregăti şi modela n-ar trebui să lipsească.

1.2.2. Dinamica interdependențelor în cadrul rețelei

Există un management de criză şi în cadrul crizelor (dezastrelor) rețelelor şi bazelor informatice (*„systems failure"*)[29]. El se numeşte Business Continuity Management şi constă într-un pachet de măsuri (algoritm) care vizează crearea unor

[29] http://www.networkworld.ro/?page=node&id=1950

condiții pentru funcționarea optimă a unității (întreprinderii) în astfel de situații. Cele mai afectat companii în cazul unor astfel de crize şi dezastre informatice sunt cele din domeniul financiar, din telecomunicații, informatică şi administrație. Pentru a putea face față unor dezastre care ar afecta grav sistemele de stocare şi operare cu informații (cutremure, inundații, incendii, alte dezastre naturale, erori umane, terorism informațional etc.), trebuie realizate back-up-uri pentru toate informațiile, pe cât posibil, în locații cât mai îndepărtate, chiar la sute de kilometri. Desigur, acestea nu se realizează oricum, ci în urma unei analize de risc.

The Business Continuity Institute (BCI) si Disaster Recovery Institute International (DRII) din SUA au pus la punct un algoritm în 10 puncte prin care se vizează realizarea funcționării optime şi fără întreruperi a unei firme. Acesta constă în:

1. Desemnarea unui manager specializat în continuitatea afacerii şi în administrarea acestui proces.
2. Analiza vulnerabilităților, pericolelor şi amenințărilor, evaluarea riscului şi a modalităților de control al acestuia.
3. Identificarea proceselor critice şi determinarea impactului pierderilor asupra activității firmei.
4. Elaborarea unei strategii de busines continuity.
5. Stabilirea modului de operare în caz de criză.
6. Dezvoltarea soluțiilor de continuitate a proceselor, întrucât, de regulă, după identificarea cauzelor crizelor şi stabilirea măsurilor, se ignoră apariția unor noi disfuncții.
7. Conştientizarea si perfecționarea continuă a echipei care gestionează criza, în colaborare cu toate compartimentele şi îndeosebi cu IT.
8. Planificarea unor operații testate preventiv.
9. Menținerea unei legături permanente cu mediile de comunicare şi cu relațiile publice, având ca scop dinamica deosebită a crizelor din sistemul informatic şi schimbările bruşte, foarte greu de controlat, care por să survină aici.
10. Coordonarea activităților de depăşire a crizei cu cele ale autorităților din domeniul respectiv, mai ales când este vorba de informații secrete.

Una dintre cauzele cele mai frecvente, cu efecte forte grave în crizele şi dezastrele informaționale o constituie, deopotrivă, erorile umane şi/sau atacul hackerilor. Se apreciază că astfel de cauze generează dezastre informaționale de peste 2 miliarde de dolari pe an. Pentru recuperarea acestor pierderi, există un software ReVirt, elaborat de cercetătorii de la Universitatea din Michigan, care reconstituie căile urmate de hackeri odată cu distrugerea codurilor de siguranță.[30]

Acest program, pe de o parte, poate preveni accesul neautorizat la anumite date. În acelaşi timp, ReVirt poate reconstitui modul de operare al hackerilor. Acest program funcționează ca o „maşină virtuală" care ascunde sistemul de operare şi creează un tip „guest", asigurând astfel buna desfăşurare a aplicațiilor şi protecția reală a informațiilor.

[30] http://www.networkworld.ro/?page=node&id=1950