Provocări privind Comunitatea Națională de Informații modernă. Repere privind definirea strategiei de sharing

drd. Petrişor BĂDICĂ
Academia Națională de Informații *„Mihai Viteazul”*
petrisor_35@yahoo.com

Abstract

The intelligence community is expressed in the context of the informational society and in the awarness of an intelligence organization. The security's multidisciplinar character imposes the existence, at the level of the intelligence structures, a macro-management project reflected within the infomational/security reports in order to identify and to control the insecurity sources. Details as corroborating joint capabilities, activating the cooperation structures within NATO and EU, being aware of the already “learnt lessons” and using the best practices, are able to ensure the efficiency and the efficacy to the answer measures as regards some critique events, as well as to include a minimal level of protection for all the states. Romania and SRI (The Romanian Intelligence Service) are actively involved in ensuring the European security space by being aware of the following details of interest: operational environment, the coordination of the national efforts and activities, namely the intelligence exchange with the liaison services and with the NATO intelligence structures.

Keywords: the intelligence community, decision-making, strategical awareness, informational revolution, capabilities, integrated system, sinergy and intelligence exchange; sharing.

Provocările lumii globalizate – cunoaştere prin intelligence

În contextul dezbaterii internaționale privind gestionarea marilor provocări ale lumii globalizate (*cristalizarea unor noi poli de putere, amplitudinea crizei economice, emergența unor crize alimentare în lume, creşterea numărului populației, concurența acerbă pentru resurse, alte amenințări asimetrice şi atipice*), activitatea serviciilor/comunităților de informații se modelează/remodelează în acord cu dinamica mediului de securitate, potențată de „oportunitățile” erei informaționale şi aplicarea pe scară largă a noilor tehnologii.

Aprofundarea Viziunii 2011 – 2015 „SRI în era informațională" conduce la identificarea unui demers legitim privind necesitatea unui proces continuu de transformare a serviciilor naționale de informații, între care Serviciul Român de Informații (SRI) reprezintă un exemplu asumat în fața comunității internaționale, lucru reliefat prin provocarea lansată de directorul instituției, dl. ambasador George – Cristian Maior către specialiști în domeniul securității şi către societatea civilă: „*...Cine va fi viitorul inamic cu care ne vom confrunta? Hackerul care sparge coduri de securitate, teroristul cu acces la arme biologice, rachetele cu încărcătură nucleară lansate de un stat proliferant, spionul care poate influența decizia politică într-un stat? Dincolo de riscurile clasice, la fel de prezente şi periculoase şi astăzi, dezvoltarea tehnologică fără precedent şi formarea unor comunități virtuale într-un spațiu cibernetic fără frontiere a creat practic o nouă dimensiune de putere, un nou câmp de luptă în care trebuie să acționăm. Mai mult, migrarea continuă a resorturilor decizionale şi acționale în rețelele informatice determină noi forme de coagulare a securității prin care noile riscuri le modelează şi le transformă pe cele clasice*[1]".

Utilizarea resurselor generate de „puterea digitală" în problematica securității a devenit o necesitate care modifică esențial modelele de acțiune acceptate şi uzitate de serviciile de informații, ele însele devenind facilitatoare şi purtătoare a nevoii de schimbare/transformare, în special prin utilizarea produselor „lumii virtuale" („Facebook", „Twitter" etc.), accesul la baze de date şi rețele informatice interconectate, lucruri menite să asigure cunoaşterea strategică într-o nouă paradigmă şi să participe la exercitarea puterii statului în plan intern şi internațional, într-o nouă formulă de acțiune.

România este conexată proceselor şi evenimentelor internaționale într-o manieră activă, pragmatică şi funcțională, fiind indisolubil legată de realizarea „*obiectivelor naționale de securitate, gândite să se desfăşoare în limitele matricei de securitate şi în spitirul ideii de bună guvernare*[2]".

Pe acest fond, dezbaterea ideii de implementare a proceselor de reformă, pe modelul asumat şi implementat de SRI, trebuie extins la nivelul tuturor instrumentelor de putere cu valențe informative ale României, iar specialiştii în domeniul securității trebuie să răspundă cât mai curând unei noi provocări: *„care este viziunea transformării Comunității Naționale de Informații Moderne (CNIM) în contextul mediului operabil de securitate al secolului XXI?"*. Iar reperele unui astfel de demers cu valențe naționale vor putea fi identificate în contextul abordărilor ce urmează....

[1] * * * – *Viziunea 2011-2015 „SRI în era informațională",* Bucureşti, 2010.
[2] * * * – *Strategia Națională de Apărare*, Bucureşti, 2010.

Fie că vorbim de spațiul euro-atlantic sub impactul crizei financiare, fie că suntem dispuşi să aprofundăm spațiul MENA (nordul Africii şi zona Orientului Mijlociu) sau să supunem analizei provocările Asiei Centrale şi ale principalilor actori cu valențe geopolitice şi geostrategice din zona Asia – Pacific, la care adaugăm procesele de redefinire a relațiilor de putere şi „dosarul iranian", un lucru este cert: lumea globalizată[3] va trebui guvernată într-o nouă paradigmă prin management superior care răspunde provocărilor de securitate şi prin redefinirea relațiile de putere.

Reaşezarea mediului de securitate a generat transformarea conceptului de securitate tradițional (în sensul înlocuirii acestuia cu un demers focalizat nu pe „național" ci pe „securitatea umană") şi o dinamică considerabilă a direcției şi modalităților de manifestare a amenințărilor la adresa securității statelor. Privit ca un proces complex de analiză a dinamicii mediului de securitate şi luând în considerare emergența unor noi actori şi amenințări care pot influența evoluțiile acestuia, cercetarea atitudinilor la nivel global relevă o tendință de avânt a antiamericanismului, în special în lumea musulmană, aceasta considerând că sistemele economice de pe piața liberă şi democrația în stil occidental pot funcționa la fel de bine în țările lor, pe baza valorilor consacrate, precum libertatea expresiei, libertatea presei, sistemele politice multipartide şi tratatementul egal în fața legii.

Într-un asemenea context, deşi realizat în anul 2004 pe baza consultării unor experți nonguvernamentali din întreaga lume, *proiectul 2020* al Consiliului Național de Informații al SUA, prezintă o serie de „certiduni/incertitudini relative" care marchează peisajul global în perspectiva deceniului următor, în măsură a influența evenimentele mondiale. Câteva dintre acestea[4]:

- ***certitudini relative***: globalizarea reversibilă şi mai puțin occidentală; creşterea cantitativă şi geografică a economiei mondiale, precum şi a numărului firmelor globale şi facilitarea noilor tehnologii; ascensiunea Asiei şi apariția unor noi puteri economice de mijloc; îmbătrânirea populației în puterile mondiale existente; puterea în creştere a actorilor non-statali şi potența islamului politic; îmbunătățirea posibilităților armelor de distrugere în masă (WMD) în unele state; arcul de instabilitate Orientul Mijlociu, Asia şi Africa; improbabilitatea escaladării conflictului dintre marile puteri într-un război total; problemele de mediu şi cele etice, etc;

[3] Privită ca o interconectare reflectată în fluxuri extinse de informații, tehnologie, bunuri, servicii şi de oameni.

[4] * * * – *Lumea în 2020 – O schiță a viitorului global prezentată de Consiliul Național de Informații al SUA*, Editura Cartier, Ed. I, 2008.

• ***incertitudini cheie***: dacă globalizarea va reduce numărul economiilor rămase în urmă, în ce măsură ţările asiatice vor stabili „noile reguli ale jocului"; rezolvarea sau continuarea crizelor financiare; măsura în care conectivitatea globală provoacă guvernele şi generează crize; abilitatea Uniunii Europene (UE) şi a Japoniei de a-şi adapta forţa de muncă, sistemele de asistenţă socială şi integrarea populaţiei de emigranţi; dacă UE devine o superputere; impactul religiozităţii asupra unităţii statelor şi a potenţialului de conflict; dezvoltarea ideologiei fundamentaliste de tip jihad; ambiguitatea numărului şi capacităţilor nucleare în lume şi incertitudini legate de abilitatea teroriştilor de a obţine arme WMD; abilitatea de controla punctele importante şi competiţia pentru resurse; măsura în care noile tehnologii creează sau rezolvă dilemele etice.

Cadrul noii agende de securitate, în opinia experţilor americani, reliefează faptul că „securitatea naţională globală[5]" este un mit, fiind necesară clarificarea priorităţilor şi strategiilor de securitate, precum şi modificarea acesteia în condiţiile unor „vulnerabilităţi cu care ne confruntăm astăzi", în cadrul unor posibile scenarii ale căror consecinţe ar putea fi una din cele „patru lumi potenţiale[6]" caracterizate de:

• ***temperarea motoarelor de dezvoltare (Stalled Engines)*** – creşterea riscului conflictelor interstatale, în cel mai sumbru scenariu posibil, în condiţiile unei retrageri a puterilor SUA pe propriul teritoriu şi ale întârzierii procesului de globalizare;

• ***fuziune (Fusion)*** – în scenariul cel mai plauzibil, China şi SUA colaborează într-o varietate de probleme, conducând la o cooperare globală;

• ***explozia inegalităţilor (Gini – Out – of – the - Bottle)*** – în care unele state devin mari câştigători, în timp ce altele eşuează, generând tensiuni sociale, în condiţiile unei cedări parţiale a SUA în afacerile globale;

• ***nonstatalitate (Nonstate World)*** – influenţată de noile tehnologii, actorii non-statali preiau conducerea în gestionarea provocărilor globale.

Privitor la analiza actuală a securităţii europene, criza financiară a indus riscul amplificării stării tensionate şi al reducerii sprijinului opiniei publice pentru instituţii. Există ***cinci chei de dinamică*** în mediul economic post-2008, ale căror rezultate vor influenţa decisiv viitorul UE, în particular şi cel al statelor dezvoltate la nivel global:

---

[5] *Idem*.

[6] Potrivit studiului elaborat Consiliului Naţional de Informaţii al SUA intitulat „*Global Trends 2030: An Alternative World*" (2013) care identifică tendinţele şi factorii capabili să schimbe radical lumea în următorii 15 - 20 de ani.

- ***încetinirea dezvoltării economice*** – pe fondul restrângerii masive a activităților private şi publice, cu efecte imediate (reducerea consumului individual, a investițiilor şi diminuarea cheltuielilor bugetare, urmare a programelor de austeritate);
- ***regresul mobilității sociale sau inversarea bruscă a mobilității sociale şi lipsa unor perspective pozitive pentru populație***;
- ***conflictele între generații*** – pe fondul trendului existent de îmbătrânire a populației europene;
- ***populismul, protecționismul, izolarea, naționalismul*** – determină tensiuni economice şi sociale; declinul consumului şi supradimensionarea organizațională au generat instincte de protecționism; războaiele comerciale şi cele de schimburi valutare sunt „anticamera" naționalismului agresiv şi a xenofobiei;
- ***reechilibarea forțelor de putere*** – la nivelul guvernanței globale, influența Europei este în scădere.

În acest context, Europa trebuie să asigure securitatea cetățenilor săi prin sinergia eforturilor naționale în 4 domenii prioritare: dezvoltarea cooperării împotriva terorismului şi a crimei organizate; instituirea unor capacități europene de protecție civilă; coordonarea apărării împotriva atacurilor informatice; securizarea aprovizionării cu energie şi cu materii prime strategice. Pentru Europa economică 2020, Institutul Bertelsmann a propus trei priorități de dezvoltare:

- ***dezvoltarea inteligentă*** – extindere şi economie bazate pe cunoaştere şi inovație;
- ***dezvoltare sustenabilă*** – promovarea unei economii mai competitive, bazată pe mai multe resurse, inclusiv cele „verzi";
- ***dezvoltare inclusivă*** – asumarea unei economii cu un grad ridicat de ocupare a forței de muncă şi a unei coeziuni sociale şi teritoriale.

În contextul acestor abordări, domeniile de confruntare informațională în atenția intelligence-ului, rezultate din evaluările cu privire la amenințările la adresa securității naționale şi globale şi identificate la nivelul principalelor comunități de informații, sunt:

- ***apărarea cibernetică***[7] – suntem într-un „război rece cibernetic", fiind posibil ca această dimensiune să o egaleze şi să o depăşească pe cea reprezentată de terorism, în viitorul apropiat;

[7] Potrivit Raportului Congresului SUA/31.01.2012, pierderile din spionajul cibernetic sunt de aproximativ 300 mlrd. dolari, iar atacurile îndreptate împotriva sistemelor publice, zilnice. DNI a solicitat Congresului să reautorizeze *Foreign Intelligence Surveillance Act*, document „crucial" pentru colectarea de informații şi să adopte un proiect de lege care să includă schimbul de informații între autoritățile guvernamentale şi sectorul privat. Directorul FBI a reiterat importanța schimbului de informații, precizând că *National CyberTask Force* include 20 de agenții SUA, dar că există încă diferențe de abordări între autorități, la nivel statal.

- ***terorismul*** – în următorii 2-3 ani se va realiza faza critică de tranziție în privința amenințării teroriste, în special din partea Al-Qaida şi a altor organizații incluse în „mişcarea jihadistă globală". Un risc semnificativ îl reprezintă extremismul homegrown, provenind de la indivizi izolați sau grupări mici inspirate de ideologia Al – Qaida, fără a fi asociate în mod formal cu această rețea;
- ***proliferarea WMD*** – prin demersul statelor-națiune de a dezvolta, obține şi a/sau prolifera WMD sau materiale şi tehnologii ce pot contribui la consolidarea programelor nucleare deja existente;
- ***spionajul*** – pe fondul dezvoltării, în mod constant, de către serviciile străine de metode şi tehnologii care pun la încercare capacitățile autorităților şi sectorului privat de a proteja securitatea națională, sistemele informaționale şi infrastructura. Cele mai mari riscuri pe acest palier vor include în perioada următoare: spațiul cibernetic, amenințări din interior prin diseminarea neautorizată de informații clasificate; acțiunile unor state precum China, Rusia, Iran;
- ***dimensiunile asimetrice ale confruntării informaționale, obiective ale comunității de informații.***

Există o certitudine relativă: fenomenele de amenințare identificate ca ținte prioritare ale activităților de culegere de informații sunt interpătrunse profund[8]. Fiecare pot să interacționeze cu altele, cu evoluții din zone geografice îndepărtate, cu tendințele economico-financiare de importanță globală şi până la evenimente cu cauze naturale, înregistrând accelerări periculoase şi evoluții a căror rezultate sunt imprevizibile.

În fața acestor viziuni/previziuni privind lumea globalizată, considerăm că, în societatea informațională şi a cunoaşterii, este nevoie de inovație majoră în abordarea globală a intereselor de securitate. O evaluare sintetică a noii ordini mondiale şi a sistemului de relații internaționale din sfera puterii conduce la concluzia existenței unei schimbări globale în optica principalilor actori ai scenei politice mondiale, în sensul afirmării interesului general pentru stabilitate la nivel global, în contrast cu vechea ordine bipolară, în care interesul uneia dintre părți era destabilizarea celeilalte părți şi „schimbarea polarității" ordinii mondiale.

[8] *** – *Raport privind politica de informații pentru securitate Italia*, dezbătut în cadrul Parlamentului Republicii/2010.

Regândirea paradigmei de intelligence – o comunitate de informații integrată, colaborativă, inovativă

În contextul relațiilor internaționale actuale şi a complexității mediului de securitate, existența şi funcționalitatea Comunității de Informații, *„urechile şi ochii democrației*[9]*”* – reprezintă o necesitate obiectivă. Amenințările şi vulnerabilitățile sunt dimensiuni umane şi tehnologice ale culturii noastre, iar evaluarea acestora reprezintă o sarcină continuă în cadrul procesului de management al riscului. Pentru abordarea acestora, serviciile de informații trebuie să adopte măsuri riguroase, standarde şi practici specifice fiecărui tip de amenințări şi să treacă la identificarea oportunităților de exploatare[10].

Mesajul directorului SRI exprimat în Viziunea 2011 – 2015 este edificator: *„Formele de evoluție a ‹‹puterii digitale›› vor reprezenta, în egală măsură, oportunități de dezvoltare, dar şi vulnerabilități şi provocări la adresa securității, iar gestionarea acestora va fi determinată de capacitatea de accesare, decelare şi utilizare a informației. Se profilează, astfel, un nou front de acțiune al serviciilor de informații, care modifică responsabilitățile tradiționale, dar extinde şi conceptele securității cu o dimensiune complet nouă, cea a securității cibernetice*[11]*.”*

Interconectarea generală presupusă de procesul de globalizare îngreunează considerabil identificarea corectă a amenințărilor, precum şi organizarea efectivă a măsurilor de prevenire şi combatere a acestora. Comunitatea națională de informații actuală trebuie să asigure continuarea proceselor de reformă, exercitate disparat la nivelul unor servicii de informații, printr-un efort comun (mecanismul „lecțiilor învățate” poate asigura un suport eficient), în baza unor repere generale:

- ***implementarea principiilor integrării, inovării, colaborării*** – ca principii de bază ale instituțiilor de intelligene reformate;

---

[9] Expresia aparține primului preşedinte al SUA, George Washington, cel care a definit simplu şi la obiect rolul unei comunități informative: „Munca acestora [a serviciilor de informații şi contrainformații - n. n.], fie că o recunoaştem sau nu, reprezintă urechile şi ochii democrației. Altfel, cum vom putea apăra ceea ce clădim dacă nu cunoaştem la vreme de unde vine primejdia şi care sunt forțele de care ea dispune?”

[10] * * * – *National Counteintelligence Strategy*, SUA, 2009.

[11] Amb. G. C. MAIOR – prezentare *Viziunea Strategică 2011 – 2015 „SRI în era informațională”*, accesată pe adresa www.sri.ro

- ***asigurarea binomului de colaborare intelligence-comunitate socială***, individul fiind subiect al strategiei de securitate națională;
- ***redefinirea Comunității de Informații – în parametrii funcționali ai unei organizații de intelligence*** (demersul SRI poate fi utilizat ca model organizatoric şi operațional) – în măsură să asigure strategii „*SMART*" privind funcționalitatea acesteia în integralitatea sa;
- ***crearea unor valori adăugate acțiunilor/operațiunilor informative pe criterii de eficiență/eficacitate,*** în special prin instituirea unor practici moderne de management şi prin participarea mediului academic şi societății civile la definirea obiectivelor de securitate, respectiv la validarea rezultatelor obținute;
- ***dezvoltarea integrată a capacităților de detectare şi analiză a amenințărilor***, prin contracararea proceselor şi nu a subiecților.

1. Abordări generale privind intelligence-ul strategic – de la avertizare timpurie la infodecizie

Pentru Comunitatea Națională de Informații Modernă, cunoaşterea – anticiparea constituie o nouă funcție strategică, o prioritate în politicile de securitate națională/aliate. Cunoaşterea garantează autonomia decizională şi permite păstrarea inițiativei strategice. Pe acest segment, CNIM trebuie să ofere atât factorilor de decizie, cât şi comandanților militari şi responsabililor pe linie de securitate internă/civilă, posibilitatea de a dispune cât mai repede de elementele de previzionare şi de prospectivă a acțiunilor, prin furnizarea produselor informaționale rezultate din analiza şi integrarea multisursă a informațiilor obținute de serviciile de informații într-o formă adaptată, care să permită adoptarea infodeciziilor de securitate.

Aşadar, relația dintre cunoaştere şi decizie reprezintă un factor fundamental în dezvoltarea intelligence-ului. Altfel spus „...c*unoaşterea strategică presupune mai mult decât o simplă informare a politicianului şi decidentului cu privire la anumite evoluții, şi se referă la construirea unor relații de cooperare în care serviciile de informații să fie capabile să transmită unda de cunoaştere necesară pentru dezvoltarea de către aceştia a unor strategii de securitate*[12]".

[12] MAIOR, George, Cristian, *Cunoaştere şi decizie: consumatorii şi paradoxurile politizări intelligence în secolul XXI*, în vol. *"Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI*", Ed, RAO, Bucureşti, 2010, pag. 54.

În acest context, informația pentru securitate furnizată de CNIM asigură funcția de avertizare timpurie şi suportul necesar „*... evitării surprinderii strategice, fundamentarea corectă a deciziilor şi viteza adecvată de reacție, precum şi capacitatea de acțiune pro-activă, în scopul îndeplinirii noilor tipuri de misiuni*[13]" Rolul primordial al intelligence-ului este preponderent acela de a selecta informații de avertizare asupra situațiilor/evoluțiilor ce devin dezirabile, sens în care CNIM impune acestei activități un pronunțat şi cuprinzător caracter anticipativ-preventiv. Informațiile şi avertizările strategice trebuie să vizeze cu predilecție tendințele şi evoluțiile generate de mediul de securitate pentru ca factorii de decizie să poată descuraja, preveni sau răspunde eficient unor amenințări şi să beneficieze de pe urma oportunităților create. O prioritate esențială revine intelligence-ului militar din teatrele de operații şi care constă în „*responsibility to provide*", sens în care este necesară o cooperare strânsă cu partenerii, într-un mediu operațional din ce în ce mai integrat.

Pe aceste considerente, opinăm că un sistem național de intelligence competitiv trebuie să furnizeze cadrul adecvat pentru avertizarea timpurie şi preziune strategică[14]. Termeni precum „scanarea orizontului" (*horizon scanning*), „scanarea mediului" (*environmental scanning*) sau „scenarii alternative ale viitorului" (*alternative futures*) sunt asociați eforturilor de intelligence strategic. Scopul unor astfel de demersuri îl reprezintă *necesitatea avertizării strategice asupra pericolelor posibile* (crize, conflicte, negocieri, încheierea unor acorduri şi tratate internaționale, apariția şi dezvoltarea unor fenomene de natură a periclita securitatea economică şi financiară a statului, stabilitatea socială şi etnică, starea de sănătate sau alertele de mediu etc.) sau *a unor demersuri statale sau non-statale de penetrare a secretelor naționale sau ale organizațiilor de securitate din care țara face parte*. Pe acest fond, considerăm că, cel mai adesea, confruntarea în secolul societății cunoaşterii are loc în planul activității informative[15], iar în acest sens informația integrată furnizată de structurile de intelligence are valoare strategică pentru decidenți.

Nu în ultimul rând, CNIM trebuie să acorde importanța necesară consolidării dimensiunii psihologice a capacității de reacție la nivel național, care constă în rezistența populației în perioade de incertitudine

[13] *** – *Strategia de Securitate Națională, Bucureşti*, 2007, pag.
[14] VASILE Păun, *Puterea informațională*, Editura Tritonic, București, 2005, pag.122.
[15] Vezi VLĂDUȚESCU Ştefan, *Informația de la teorie către ştiință*, Editura Didactică şi Pedagogică, București, 2002, pag. 208.

şi instabilitate şi în menţinerea unei stări de normalitate. Este vital modul de comunicare în timpul unor situaţii de criză fără a alarma populaţia. Totodată, avertizarea timpurie şi previziunea strategică trebuie să determine intenţiile şi capabilităţile reale ale adversarilor, acordând o atenţie sporită identificării acţiunilor deliberate de manipulare şi dezinformare[16].

În acest context, trebuie să menţionăm că eforturile de dezvoltare în plan naţional/aliat a unor sisteme de avertizare timpurii trebuie să se concentreze pe asigurarea expertizei necesare prin 3 tipuri de avertizare[17]:

- ***early alerting*** – care prevesteşte evenimentele iminente sau incipiente, cea mai utilizată în zilele noastre, în special în spaţiul mass-media;
- ***early warning*** (sau, într-o altă accepţiune – tactical warning), care, plecând de la trenduri identificate prin monitorizarea unui set de parametri, poate oferi indicii cu privire la evoluţii de interes pe termen scurt şi mediu;
- ***strategic warning***[18], care, combinând datele obţinute în baza monitorizării consecvente a elementelor critice din punctul de vedere al problematicilor de securitate abordate cu expertiza senior analistului, oferă perspective şi scenarii de evoluţie pe termen lung.

OSINT reprezintă platforma ideală care poate integra toate exigenţele unui sistem de strategic warning.

Elaborarea unor forme eficiente de contracarare a ameninţărilor asimetrice[19] reprezintă o provocare şi obiectiv a CNIM reformate, iar o posibilă soluţie poate fi elaborarea şi actualizarea constantă a modelelor ameninţărilor asimetrice, a mecanismelor de evaluare de risc şi a unui sistem eficient de criterii de identificare timpurie a ameninţărilor şi de definire a potenţialului putătorilor de ameninţări.

---

[16] I. NIŢU, *Evitarea surprizei strategice şi avertizarea timpurie. Dificultăţile prognozei într-o eră a incertitudinii*, în vol. G. C. MAIOR, *Un război al minţii. Intelligence, servicii de informaţii şi decizie politică*, Editura RAO, Bucureşti, 2010, p. 130.

[17] C. IANCU, A. VASILESCU, *OSINT în era noilor ameninţări globale - strategic warning*, articol, Sesiunea de comunicări ştiinţifice a Academiei Naţionale de Informaţii „Mihai Viteazul, Bucureşti," 2010.

[18] Dintre toate definiţiile clasice ale strategic warning, cea mai aproape de rolul actual pe care poate să îl deţină în ansamblul intelligence considerăm că a fost oferită de Jack Davies, respectiv: „percepţia analitică oportună şi comunicarea efectivă către factorii de decizie a schimbărilor importante ale nivelului ori caracterului ameninţărilor la adresa securităţii naţionale ce necesită reevaluarea capacităţii statului de a înlătura ori limita consecinţele". Obiectivul final? Bineînţeles că „scopul acestei acţiuni este prevenirea surprizei strategice".

[19] Potrivit Conceptului SANS – agenţia de informaţii interne a Bulgariei, 2012.

2. Elemente de structuralitate şi funcţionalitate ale Comunităţii Naţionale de Informaţii Modernă

Întregul proces de analiză a proceselor de reformă în intelligence reliefează capacitatea de adaptabilitate a structurilor de informaţii la contextul politic şi social existent la nivel naţional/aliat, nuanţele fiind induse de apartenenţa sau nu a comunităţilor de informaţii la diferite organizaţii internaţionale de securitate cu valenţe regionale sau globale (NATO, UE, Organizaţia Tratatului de Cooperare de la Shanghai etc.), precum şi interferenţele cu zonele/fluxurile de instabilitate care generează ameninţări asimetrice/atipice.

Caracteristica principală a proceselor de reformă ale CNIM o reprezintă trecerea la un nou model organizatoric şi operaţional, capabil să asigure misiunea primordială, prevenirea manifestărilor riscurilor şi ameninţărilor, sau, în cazul producerii, limitarea urmărilor acestora la un nivel acceptabil pentru societate. Identificăm aici o nevoie acută de cooperare/colaborare, de realizare, în principal, a sinergiei resurselor informaţionale la dispoziţia serviciilor de informaţii şi nu în ultimul rând, acceptarea ideii că fără o relaţionare externă cu celelalte comunităţi sau organizaţii internaţionale misiunile de cunoaştere, prevenire, protecţie şi contracarare aflate pe agenda acestora sunt greu de realizat.

O construcţie modernă de intelligence, structurată, condusă şi operaţionalizată conform unui proiect optimizat pentru societatea informaţională şi a cunoaşterii este Comunitatea Naţională de Informaţii Modernă – Organizaţie de intelligence. Acest proiect integrat şi interconectat global răspunde eficient vechilor ameninţări şi asimilează noi misiuni aflate/solicitate pe/prin agenda serviciilor de informaţii care depăşesc domeniul securităţii naţionale sau zonele de expertiză ale acestora. O provocare majoră o reprezintă delimitarea competenţelor serviciilor de informaţii şi nevoia de coordonare unitară a întregii arhitecturi de intelligence într-o nouă paradigmă care valorifică sinergiile existente, expertizele specifice şi acoperirea globală a problemelor de interes.

În context, filosofia managerială amintită mai sus implică viziune, misiune, strategie, politici, reguli şi proceduri care generează în final o nouă cultură organizaţională. Totodată, operaţionalizează noi concepte care facilitează lucrul integrat şi schimburile de informaţii în format bi-/multilateral, precum şi realinierea misiunilor şi responsabilităţilor Comunităţii şi a entităţilor informative componente.

CNIM este rezultatul revoluţiei în intelligence, respectiv al revoluţiei OSINT, procese care au generat un impact deosebit asupra managementului

şi activităţii serviciilor de informaţii, şi care sunt în măsură să asigure orientarea unitară a activităţii de informaţii spre realizarea unor scopuri comune care, în viziunea SUA[20], vizează:

- ***promovarea de politici pertinente de securitate naţională***: presupune monitorizarea şi evaluarea continuă a climatului internaţional de securitate pentru a avertiza factorii de decizie cu privire la ameninţări şi a-i informa cu privire la oportunităţi;
- ***susţinerea acţiunilor eficiente pentru securitatea naţională*** – prin furnizarea de informaţiii care pot conduce la acţiuni de sprijin a toate nivelurile;
- ***furnizarea unor capacităţi echilibrate şi în continuă dezvoltare*** – care susţin diversitatea competenţelor unice ale CI, integrarea capacităţilor pentru valorificarea sinergiilor şi sprijinul noilor misiuni şi concepte;
- ***acţiune integrată ca o singură echipă*** – implică angajarea de echipe colaborative ce sprijină întreaga gamă de capacităţi ale CNIM pentru a realiza cerinţele beneficiarilor.

Din analiza celor prezentate, CNIM este organizaţie de intelligence centrată pe reţea, iar acest lucru presupune:

- ***infrastructură comună de informaţii*** bazată pe cultura schimbului de informaţii şi susţinută de diferite servicii[21] prin care se asigură accesul unitar la toate datele şi produsele de intelligence, mijloacele şi bazele de date ale serviciilor de informaţii;
- ***arhitectură unificată construită în jurul unui punct focal comun***, bazat pe o singură reţea în centre care facilitează accesul la comunicaţii;
- ***menţinerea unui vârf tehnologic***, cu servicii interoperabile pentru toate sistemele de informaţii, standarde uniforme şi interfeţe comune;
- ***integrarea componentelor vitale şi eliminarea diferenţelor organizaţionale***;
- ***implementarea unor practici moderne*** pe linia asigurării resurselor umane, cu asumarea diferitelor roluri în carieră şi a unor competenţe şi calificări înalte;
- ***aplicarea unor programe de dezvoltare*** pentru conducere, sisteme de evaluare a performanţelor şi o structură de stimulente unitare la nivelul Organizaţiei;

[20] Strategia Serviciilor Naţionale de Informaţii a SUA, trad., Bucureşti, 2009, pag. 7.

[21] Includ: servicii de comunicare (e-mail, directoare, catalogare, colaborare); servicii de date (solicitări şi căutări, etichetare, extragere, păstrare); servicii de securitate (control acces, auditare, monitorizare); servicii analitice (portaluri, exploatare date, vizualiaze, simulare, modelare).

- ***regândirea funcției securității/protecției*** şi dezvoltarea de proiecte comune a tuturor celor implicați pe această linie;
- ***dezvoltarea de proiecte comune interagenții***, cu echipe dinamice cu susținerea tuturor resurselor tehnice moderne;
- ***utilizarea cercetării şi dezvoltării noilor tehnologii pentru avantaj competitiv;***
- ***dinamizarea funcței inovației*** prin îmbunătățirea calității actului de conducere, alinierii organizaționale şi a resurselor.

Contextul general de remodelare a arhitecturilor naționale de intelligence a fost nuanțat de evoluțiile geopolitice şi de evenimentele cu impact strategic major care, în unele cazuri, au fost atribuite unor eşecuri operaționale – legate de incapacitatea de cunoaştere şi prevenire, deficiențelor organizatorice – primordiale fiind lacunele privind schimburile de informații şi rezistența întâmpiată pe parcursul proceselor de reorganizare şi reformă.

În context, sunt 4 domenii asupra cărora CNIM şi serviciile de informații trebuie să-şi adapteze abordările[22] în ceea ce priveşte:

- culegerea de informații şi utilizarea acestora – provocată de explozia informațională;
- coordonarea națională şi cooperarea între serviciile de informații, precum şi cu alți actori ai sectorului de securitate;
- schimburile de informații cu organizații internaționale şi cu alte țări;
- acceptabilitatea şi recunoaşterea/aprecierea publică.

Funcționalitatea CNIM într-o paradigmă adaptată secolului XXI, pe baza principiilor integrării, colaborării şi inovării, este în măsură să genereze soluții de răspuns la constelația de vechi amenințări reinventate prin noile riscuri, în special prin:

- asigurarea unei viziuni corecte asupra lumii actuale, complexității şi dinamicii acesteia;
- operaționalizarea Organizației de Intelligence prin identificarea rolurilor şi responsabilităților, stabilirea drepturilor decizionale şi stabilirea leadership-ului la nivelul CNIM;
- coordonarea şi integrarea agențiilor/serviciilor de informații componente ale Organizației de intelligence, ce facilitează irelevanța delimitării între serviciile civile şi militare de informații (reacțiile trebuie să implice activități de informații interconectate);

[22] DCAF Backgrounder, *Contemporary Challenges for the Intelligence Community*, nr. 3/2006, Geneva, pag.3.

- corelarea nivelului riscurilor şi ameninţărilor cu obiectivele şi priorităţile activităţii de informaţii, stabilite multianual;
- planificarea integrată a cerinţelor operaţionale şi a managementului resurselor alocate, potrivit necesităţilor actuale şi priorităţilor viitoare cu privire la bugete, achiziţii şi operaţiuni;
- dezvoltarea de proiecte de securitate comune, inter-agenţii, cu echipe şi management performante;
- asigurarea feed-back-ului între conducerea CNIM şi a agenţiilor/ serviciilor de informaţii pentru înţelegerea planurilor şi a priorităţilor operaţionale, precum şi instituirea unui proces de evaluare anuală a performanţelor manageriale şi personale;
- transparenţa organizaţională privind misiunile, responsabilităţile, respectarea drepturilor şi libertăţilor fundamentale ale omului, implicarea în definirea, implementarea şi susţinerea educaţiei şi culturii de securitate;
- valorificarea trend-urilor tehnologice şi dezvoltarea revoluţiei IT necesare fundamentării avertizărilor cu privire la ameninţările viitoare şi prevenirii decidenţilor asupra oportunităţilor strategice.

3. Integrarea intelligence-ului – obiectiv şi oportunitate

Integrarea intelligence-ului reprezintă un obiectiv strategic al CNIM pentru că astfel sunt create mecanismele şi procesele de guvernanţă care să alinieze strategic Comunitatea la priorităţile şi obiectivele naţionale de securitate. Integrarea asigură eficienţa atunci când informaţiile furnizate de CNIM în ansamblul său, asigură infodecizia şi crează avantajul informaţional în relaţie cu competitorii.

Raţionamentele pentru înţelegerea CNIM integrată în societatea informaţională şi a cunoaşterii sunt legate de evoluţiile din mediul global şi de crearea de noi oportunităţi:

- o misiune integrată susţinută prin intelligence este mai puţin caracterizată prin profunzimea diviziunii specifice între beneficiarii de anvergură naţională şi tactică, diplomatică, de informaţii politice, economice şi militare, aceastea fiind legate indisolubil una de cealaltă;
- tehnologia informaţiei oferă posibilitatea unui intelligence mai închegat, ceea ce determină capacitatea unui sistem unificat în contrapondere cu infrastructurile individuale asociate disciplinelor de intelligence.

Viziunea[23] privind CNIM înglobează deopotrivă problemele legate de politici şi reglementare, ca şi relaţiile cu beneficiarii naţionali - în acord cu orientările statului pe linia aspectelor politice, juridice şi de securitate, recunoscând, totodată, posibilităţile de abordare integrată a managementului şi funcţiilor informaţiei (incl. „exigenţele, obiectivele, culegerea, exploatarea, etichetarea, exploatarea, arhivarea, coroborarea şi analiza" şi, de asemenea, „comunicaţiile, infrastructurile, politicile şi procedurile").

Resursele naţionale, inclusiv de tehnologia informaţiei, sunt în măsură să sprijine, atât la nivelul abordărilor conceptuale, cât şi al proceselor curente, ideea de comunitate de informaţii integrată, capabilă să genereze produse informaţionale personalizate pentru eficienţa infodeciziilor privind securitatea naţională/aliată. Pe acest fond, sunt importante două abordări care să fundamenteze şi să sprijine proiectul CNIM:

- ***Comunitatea poate implementa sisteme definite prin instituţii individuale*** (agenţii/ servicii de informaţii), în cadrul disciplinelor lor specifice, infrastructurilor şi programelor – lucru care se bazează pe procese proprii fiecărei agenţii şi organizări de achiziţii şi de practici specific.
- ***Comunitatea finanţează arhitectura, integrarea capacităţilor şi tehnologiilor*** în cadrul unor discipline şi infrastructuri unificate.

Un model de CNIM valorifică preocupările deja validate din mediul privat, uziteată de tehnologiile informaţionale emergente în măsura în care acestea devin disponibile în vederea asigurării cerinţelor unei game diversificate de beneficiari. Acest model asigură autonomia continuă a compoentelor majore ale Organizaţiei de intelligence, crează noi procese manageriale, generează cunoştinţe şi permite un schimb de informaţii adaptat nevoilor şi provocărilor mediului de securitate.

CNIM trebuie să răspundă solicitărilor unui număr din ce în ce mai mari de beneficiari, preocupaţi de o gamă din ce în ce mai diversificată de probleme, iar acest demers nu poate şi realizat decât printr-o acţiune şi specializare comună, precum şi prin surprinderea schimbărilor complexe şi totodată subtile a relaţiilor între principalii actorii globali sau regionali de pe scena securităţii. Beneficiarii produselor de intelligence doresc o imagine completă asupra problemelor cu care se confruntă, în timp real, lucru ce face dificilă furnizarea expertizei tradiţionale dar facilitează procesele de cunoaştere prin colaborare şi schimb de informaţii, în manieră fiabilă şi constantă.

[23] Sunt evidenţiate astfel nevoia de integrare a funcţiilor intelligence-ului, conformitatea politicilor juridice, orientarea reglementărilor în baza nevoii de integrare şi o infrastructură de informaţii mai integrată.

Utilizarea noilor tehnologii, direcționate pe optimizarea modului de utilizare a resurselor corespunde viziunii CNIM: gestionarea şi integrarea funcțiilor informației şi intelligence-ului în sprijinul „modelului centrat pe beneficiar".

Capacitatea de integrare poate genera noi concepte de funcționare care vor dinamiza activitatea instituției de intelligence. Pot fi generate noi discipline mult mai cuprinzătoare decât cele actuale, precum şi o strategie națională integrată de securitate. Pe acest fond, pot fi create produse integrate de intelligence prin participarea, atât a decidenților, cât şi a instituțiilor abilitate, precum şi implementarea viziunii CIM cu ajutorul tehnologiei, abordării organizaționale şi integrării proceselor, fără a fi necesară combinarea infrastructurilor existente.

Cu toate acestea, importante impedimente la această integrare există. CNIM va trebui să le depăşească pentru a realiza viziunea liderilor Comunității, lucru ce presupune aplicarea rapidă a acesteia, pe fondul utilizării oportunităților tehnologice disponibile pentru realizarea integrării. Sunt necesare ajustări privind asigurarea cadrului legal, pentru promovarea intelligence-ului ca disciplină cu propriile norme privind funcționalitatea şi schimbul de informații. Relevante sunt:

- ***examinarea riguroasă a legilor existente şi identificarea reglementărilor şi normelor*** de punere în aplicare a Viziunii, cu identificarea autorităților responsabile pentru schimbare;
- ***identificarea misiunilor şi operațiunilor anuale***, model pentru a crea o Organizație de intelligence;
- ***adoptarea concepției şi utilizarea indicatorilor de performanță*** pentru adaptarea cadrului juridic, la nevoie, funcție de rezultatele de performanță.

Pe aceste coordonate, sunt evidente preocupările specialiştilor din zona intelligence-ului de a realiza integrarea resurselor necesare gestionării provocărilor din mediul de securitate, prin acțiune internă, națională, precum şi prin operaționalizarea formatelor de cooperare internațională.

În opinia specialiştilor americani sunt importante două schimbări în mediu pentru a justifica nevoia de integrare[24] a CNIM, precum şi crearea de oportunități puternice pentru realizarea integrării[25]:

[24] Intelligence-ul integrat are ca arie de manifestare sfera conducerii strategice a statului şi înglobează elemente de decizie, de planificare şi acționale.
[25] AFCEA International, *National Security and Horizontal Integration,* SUA , 2004.

• misiunile de astăzi sunt susținute prin diviziune între actorii de informații de nivel strategic sau tactic (diplomatici, politici, economici, militari etc.), ci prin integrarea eforturilor lor. Componentele sistemului sunt strâns legate unele de altele;

• tehnologia informației oferă oportunitatea unei mai strânse şi organice capabilități de intelligence, caracterizate prin unificarea valorilor, mai degrabă decât infrastructurilor individuale asociate în mod tradițional cu fiecare disciplină de informații (tehnologia informației permite managierea infrastructurilor disparate în mod uniform).

Integrarea inteligence-ului, poate conduce la noi şi colaborative procese capabile să asigure sprijinul decidenților/beneficiarilor, fiind posibilă datorită noii tehnologii. Impedimentele semnificative dau nu insurmontabile, pot fi abordate şi depăşite pentru a realiza această integrare.

Pe fond, o CNIM integrată presupune obținerea avantajului decizional beneficiarilor şi colaborarea în cadrul misiunilor, dar şi integrarea componentelor vitale ale Organizației – oameni, procese şi tehnologie. Noile generații sunt deschise la tehnologiile inovatoare, fiind produsele unei societăți informaționale, dar la fel de mult sunt atrase de misterele activității de intelligence. Una din provocările revoluționare a acestei culturi presupune trecerea uzualului *„ceea ce trebuie să ştie" („need to know")* la individuala *„responsabilitatea de a asigura" („responsability to provide")*, în scopul de a colabora şi a-i ajuta mai mult pe cei care au nevoie de informații.

4. Noile tehnologii în activitatea de intelligence

Argumentele legate de rolul şi necesitatea implementării noilor tehnologii în cadrul proceselor informaționale derulate la nivelul comunităților de informații țin indisolubil de creşterea cantității, surselor şi tipurilor de informații în atenție, de nevoia de coroborare de date disparate, disponibile între entități şi platforme colaborative, precum şi de analiza acestora în funcție de relevanța pentru beneficiari. Pe acest fond, în scopul eficienței şi performanței înalte, arhitecturile şi infrastructurile tehnice trebuie consolidate, procesele pentru fluidizarea securizării şi configurarea serverelor sau aplicațiilor trebuie automatizate.

Lucrurile simple astăzi vor fi complet integrate în platforme de comunicații multimedia mobile şi miniaturizate, într-o lume a Web n.0. cu funcții nenumărate. Ideea funcțiilor multiple este „*extrem de importantă, astăzi, instrumentele, echipamentele, rețelele sau organizațiile sunt ineficiente dacă nu sunt capabile să răspundă rapid unor funcții multiple.*

Răspunsul, indiferent dacă este văzut ca produs, decizie sau acțiune este construit pe date şi informații rafinate cognitiv[26]". Noile tehnologii produc mutații semnificative în zona misiunilor clasice ale serviciilor de informații.

CNIM evoluează în concordanță cu permanentele schimbări pe care mediul de securitate le înregistrează, în special, prin reinventare organizațională bazată de învățare şi adaptare. Afirmarea CNIM ca organizație integrată de intelligence implică şi preocupări de import a unor practici eficiente din sectorul privat, între care utilizarea centrelor de date comune şi de depozitare comună a datelor[27].

O altă necesitate stringentă pentru CNIM o reprezintă consolidarea şi dezvoltarea unei infrastructuri informatice comune, capabilă să susțină procesele de infodecizie, de cooperare în format intern şi conexiunea cu rețele partenere, precum şi interogarea rapidă şi eficientă a datelor necesare proceselor de analiză de informații[28].

Aplicațiile de tip web şi tehnologia informației remodelează întregul ciclu de intelligence, în sensul transformării acestuia într-un proces „target-centric[29]" cu obiectivul principal al realizării imaginii unei „ținte" informative pe care să o poată exploata oricare dintre participanții la proces, astfel încât fiecare dintre aceştia să poată extrage elementele de care are nevoie pentru îndeplinirea sarcinilor care le revin.

Un alt demers pentru relaționarea noile tehnologii-intelligence este dat de rolul programelor transformaționale tip Intellipedia, create pentru creşterea productivității, facilitarea colaborării, eficientizarea controlului managerial şi reducerea redundanței. Intellipedia reprezintă un element

[26] MAIOR, George Cristian, interviu în Revista Intelligence nr. 20, septembrie-octombrie 2011.
[27] Modelul este abordat la nivelul CI a SUA şi este prevăzut în Planul de 500 de zile elaborate la nivelul ODNI.
[28] Previziunile companiei de analiză de piață Gartner pentru anul 2012 privind tendințele tehnologice şi influențele comportamentelor viitoare, anticipează următoaree intrări: tablete mobile, aplicații şi interfețe grafice centrate pe dispozitive mobile, experiența utilizatorilor contextuală şi socială, internetul lucrurilor, mediile de distribuție software de tip app store/market place, aplicațiile analitice (de business sau de orice date istorice), cantitățile masive şi cerscânde de date (Big-Data), procesare In-Memory, serverele cu consum redus de energie, Cloud Computing.
[29] Construcția modelului se realizează în colaborare, în rețea, la care participă inclusiv beneficiarii. Relevanța constă în eficientizarea activității, pentru că o bună cunoaştere a țintei este esențială pentru operațiuni, atenuarea problemei de supraîncărcare a intelligence-ului modern, deoarece toți actorii conştientizează ceea ce este util pentru construirea modelului şi sunt implicați activ în acest sens.

relevant pentru contextul actual transnațional ce evoluează rapid, creând un mediu colaborativ ce ajută să nu se ajungă în situația în care informații critice ar putea fi pierdute în lanțul informărilor interagenții.

O altă provocare pentru activitatea de intelligence o reprezintă new media. Dezvoltarea tehnologiei informației şi a comunicațiilor a facilitat extinderea Internetului şi apariția aplicațiilor Web 2.0, a căror implementare a condus la apariția new media. Numărul imens de website-uri corporate/ personale, bloguri, forumuri publice, popularitatea fără precedent a rețelelor sociale[30], dar şi creşterea exponențială a conținutului generat de utilizatori şi diversitatea limbilor şi a pachetelor în care este livrată informația sunt principalele caracteristici ale new media care reprezintă provocări pentru OSINT. Din această perspectivă, aproape fiecare etapă a procesului OSINT reprezintă o reacție şi o încercare de adaptare la dinamismul mediului online, fiind direct influențate de noile tehnologii şi de rapiditatea cu care sunt preluate şi dezvoltate de utilizatori. Legătura directă dintre evoluția Internetului (apariția Web 3.0 şi Web 4.0) şi dezvoltarea aplicațiilor asociate, precum şi orientarea media tradiționale către mediul online vor influența în mod decisiv procesul OSINT, atât în ceea ce priveşte mijloacele folosite, cât şi în privința consolidării rolului său în activitatea de intelligence.

Pentru eficiența exploatării eficiente a new media este necesară adaptarea metodologiei existente sau schimbarea profundă a acesteia şi elaborarea unor standarde noi în domeniu, care să răspundă avansului tehnologic. De asemenea, se impune nevoie cooptării/colaborării cu specialişti din mediul privat sau din sfera academică în elaborarea produselor OSINT, în cazul unor topicuri de nişă, abordate din ce în ce mai des în mediul blogurilor şi al publicațiilor online specializate. OSINT are un rol fundamental în direcționarea analizei multi-sursă. Pentru comunitatea tradițională de intelligence, OSINT rămâne doar o componentă a analizei multi-sursă. Pentru alte agenții guvernamentale, OSINT reprezintă prima sursă pe care o accesează şi pe care o consideră ca fiind o capabilitate strategică.

În ceea ce priveşte *software-ul social*, produs al revoluției informaționale, impactul a fost semnificativ asupra serviciilor de informații guvernamentale. Fără îndoială, difuzarea electronică facilitează şi accelerează

[30] Internet, bloguri, Facebook, Twitter, Youtube, Hi5. Sunt doar câteva cuvinte din mediul cibernetic şi al „noilor media". Rețele sociale virtuale reprezintă ultima generație de spațiu public mediat, spațiu de întîlnire şi interacțiune într-o zonă publică mediată de tehnologie (http://www.sociologie.ro/articol/8-17-Retele_sociale_in_internet.html).

procesul de inteligenţă. În cazul OSINT, software-ul a permis analistilor revizuirea produselor într-un mod relativ rapid, prin discuţii virtuale, contribuind la acurateţea îmbunătăţită a produsului şi mai mare calitate a acestora, depistarea erorilor şi corectarea acestora în orice etapă.

Revoluţia informaţională poate avea un efect mare, deoarece eficacitatea OSINT se împleteşte cu inovaţiile tehnologice. Dezvoltarea de servicii media la nivel mondial, explozia internet-ului şi evoluţia continuă a tehnologiei prin satelit face expunerea societăţilor globale „*mai largă şi mai multe informaţii deschise omniprezente*". Potrivit specialiştilor în domeniu OSINT se extinde treptat în zone care în mod tradiţional aparţin altor discipline, dar cu toate acestea nu poate înlocui activitatea HUMINT privind culegerea de informaţii clasificate.

Important, în lumea Web 2.0 ca software social, interacţiunile sunt multi-directionale, interactive şi iterative. Utilizarea software-ului social ca TIC este creativ şi colaborativ.

CNIM trebuie să fructifice fundamentele şi strategia generală pentru a asigura integrarea software-ul social în misiuni ce privesc securitatea naţională şi să beneficieze de pe urma colaborării participative rezultate utilizarea responsabilă a acestuia.

Repere privind definirea strategiei de sharing la nivelul comunităţii naţionale de informaţii modernă

În opinia specialiştilor americani, schimbul de informaţii reprezintă pentru Comunitatea de Informaţii a SUA o componentă tot mai importantă în procesului de realizare a securităţii naţionale. În acest sens, considerăm că şi în plan naţional, în conformitate cu principiile stabilite în Strategia de Securitate Naţională şi în Strategia de Apărare, serviciile de informaţii şi Comunitatea de Informaţii a României, în ansamblul său, trebuie să acţioneze pentru îmbunătăţirea schimbului de informaţii, promovarea unei culturi în această direcţie, implementarea de noi tehnologii, îmbunătăţirea politicilor şi procedurilor de angajament pe această linie, în timp real, relevant şi în toate direcţiile de interes pentru securitatea naţională.

1. Noi concepte în intelligence: need to know vs.need to share

În filosofia existenţei şi funcţionalităţii CNIM, înlăturarea barierelor politice şi tehnice, care altădată au făcut posibile evenimente cu implicaţii

strategice internaţionale, constituie o prioritate absolută, care trebuie tradusă astfel: informarea decidenţilor cu informaţii viabile, reale şi deconflictualizate – rod al implicării întregii comunităţi informative, schimburi permanente de informaţii între agenţiile de intelligence şi protejarea informaţiilor împotriva diseminărilor neautorizate, în acţiuni tip Wikileaks. Acest echilibru între cunoaştere/utilizare în comun şi eficienţa protecţiei informaţiilor este delicat şi dificil de realizat.

Pe fondul focusării asupra principiului *„need to know”*, sisteme complexe de gestionare a informaţiilor clasificate derulează investigaţii atente privind atribuirea accesului personalului agenţiilor la acestea, precum şi determinări pentru anumite persoane sau structuri care au nevoie să le utilizeze pentru îndeplinirea atribuţiilor lor. Chiar şi schimbul de informaţii a fost văzut ca fiind favorizator pentru unele riscuri privind sustragerea sau compromiterea informaţiilor. Diferite tipuri de abordări tehnice au fost identificate pentru a menţine securitatea informaţiilor partajate. O atenţie deosebită acestor abordări a fost reflectată în raportul din 2003 "*Task Force Foundation Markle pentru securitate naţională în era informaţională*", care a avut o influenţă importantă asupra abordării problemei privind schimbul de informaţii[31].

Există o măsură asupra căreia trebuie reflectată: principiul *„need to share*" este esenţial şi vital în toate domeniile de intelligence, fie că vorbim de prevenirea şi combaterii terorismului sau de eforturile pe zona de contrainformaţii sau de securitate cibernetică, deşi rolurile jucate de agenţiile/serviciile de informaţii sunt diferite. Eliminarea restricţiilor privind schimbul de informaţii este insuficientă, sens în care, în opinia noastră este nevoie de o structură organizatorică sub mandatul căreia să se realizeze acest deziderat, aceasta având un rol coordinator în stabilirea politicilor pe această linie şi autoritatea de a susţine programele comune ale organizaţiei de intelligence, inclusiv privind achiziţii publice de tehnologie finanţate prin programele strategice, precum şi capacitatea de a duce la îndeplinire următoarele obiective[32]:

- stabilirea de norme de securitate şi de proceduri uniforme;
- stabilirea de norme comune privind tehnologia informaţiei, protocoale şi interfeţe;

[31] Richard A. BEST Jr. (Specialist in National Defense), *Intelligence Information: Need-to-Know vs. Need-to-Share*, 2011, pag. 3.
[32] P. L. 108-458, section 1011; 118 Stat. 3650.

- asigurarea dezvoltării de sisteme de tehnologia informației care includ niveluri de securitate multiple şi capacități de integrare a informațiilor;
- stabilirea de politici şi proceduri ce vizează rezolvarea conflictelor între nevoia de a împărtăşi şi necesitatea de a proteja sursele şi metodele;
- elaborarea unei arhitecturi organizaționale pentru Comunitate şi asigurarea că elementele acesteia se conformează unei asemenea construcții;
- stabilirea de politici, proceduri şi tehnologii care să faciliteze legăturile între persoane, sisteme şi agenții guvernamentale sau de interes privat (instituții academice sau de cercetare, instituții de securitate sau de analiză private) pentru schimbul de informații/cunoaştere.

În viziunea SUA, crearea unui mediu comun a facilitat schimbul de informații între toate agențiile/serviciile de informații, concentrându-se nu numai pe agenții ci şi pe stabilirea politicilor şi a liniilor directoare coerente, precum şi a comunităților tehnologice în cinci mari domenii: apărare, informații, securitate internă, afaceri externe, aplicarea legii. În anul 2011, Corin R. Stone, a descris strategia cu trei componente pentru menținerea securității informațiilor în cadrul proceselor de sharing[33]:

- ***primul este accesul***: asigurarea că persoanele potrivite pot descoperi şi accesa rețele şi informații de care au nevoie pentru a-şi îndeplini atribuțiile, dar nu a celor de care nu au nevoie. Aceasta este o problemă complexă, centrată pe principiul „*need to know*";
- ***al doilea – protecția tehnică***: limitarea din punct de vedere tehnic a abilității de a deturna, manipula sau trasfera date, în special în volum mare (de ex. prin dezactivarea sau utilizarea discurilor mobile, CD, drivere, în rețelele securizate);
- ***al treilea – auditarea şi monitorizarea***: luarea de măsuri pentru a da garanția totală că accesul la informații acordat personalului este utilizat corect. Acest lucru implică monitorizarea şi auditarea utilizării sistemelor informatice clasificate pentru a identifica activitățile suspecte anormale şi urmărirea consecinţelor.

Pe fond, preocuparea pentru asigurarea cadrului legal şi al reglementărilor care să faciliteze schimburile de infomații este specifică şi definitorie pentru existența şi performanța fiecărei construcții informative tip organizație de intelligence.

[33] Corin R. STONE, *Intelligence Community Information Sharing Executive, Office of the Director of National Intelligence, Statement for the Record before the Senate Homeland Security and Governmental Affairs Committee*, 2011.

Pe fond, la nivelul CNIM este necesară o nouă cultură de sharing, precum şi definirea modalităţile de realizare a schimburilor de informaţii - focusate pe mai multe componente:

- ***schimbul de informaţii la nivel naţional*** între serviciile de informaţii, componente ale Comunităţii şi celelalte agenţii de aplicare a legii, în format bilateral sau multilateral;
- ***schimburile de informaţii între elementele CNIM/agenţie de aplicare a legii şi o agenţie de informaţii internaţională*** (NATO, UE sau a altor organizaţii de securitate), în format naţional – internaţional (european, regional);
- ***schimburile de informaţii între diferite agenţii de informaţii internaţionale*** la care serviciile naţionale de securitate/agenţiile de aplicare a legi sunt elemente componente şi participante active.

Privitor la ultima modalitatea prezentată, la nivelul UE – în problematica terorismului, sunt necesare accentuarea schimburilor de informaţii între autorităţile de aplicare a legii prin eliminarea a două impedimente: compartimentarea informaţiilor şi lipsa unor politici clare privind canalele de informare. În acest sens, au fost identificate trei obiective diferite[34]:

- identificarea condiţiilor necesare pentru îmbunătăţirea accesului, utilizării şi schimbului de informaţi;
- introducerea unor reglementări legate de politicile de informaţii şi poliţia judiciare;
- menţinerea unui echilibru strict între respectarea drepturilor cetăţenilor şi creşterea responsabilităţilor statului în obţinerea şi utilizarea informaţiilor de către agenţiile de aplicare a legii.

O provocare strategică pentru CNIM este asigurarea controlului informaţiei[35]. Conceptul vizează asigurarea capacităţii factorilor de decizie şi a operativilor de a avea acces în timp util la informaţie şi de a o folosi într-un mod eficient, fiind fundamentat pe 4 piloni de bază:

- ***transmiterea informaţiei în timp util***, permiţând legătura între centrele de decizie şi cele de execuţie;

[34] Comunicatul Comisiei către Consiliul şi Parlamentul European din 16 iulie 2004: *Către îmbunătăţirea accesului la informaţii de către agenţiile de aplicare a legii* [COM (2004) 429 final].

[35] Conceptul iterează ca obiectiv garantarea, în condiţii normale, dar şi în perioade de criză, că toţi cei responsabili pe linia securităţii naţionale pot împărtăşi informaţii pertinente şi că factorii de deciziepot transmite la timp ordinele necesare.

• ***interoperabilitatea rețelelor de informare***, care optimizează circulația informației;

• ***protejarea informației sau securității sistemelor informatice***, permițând asigurarea confidențialității, disponibilității şi integrității sistemelor şi a informației;

• ***verificarea informației, a fiabilității şi a circulației adecvate a acesteia, precum şi valorificarea sa***.

În acest context, UE militează pentru asigurarea dinamizării schimburilor de informații la nivelul statelor, considerând că este necesar să se acționeze pe următoarele direcții:

• ***îmbunătățirea cooperării la nivel național şi al instituțiilor de securitate europene şi euro-atlantice*** – primordială în asigurarea sprijinului cu informații calitative a decidenților în vederea: formulării politicilor în domeniile securității, apărării şi externelor; asigurării sinergiei operațiunilor de intelligence; cooperării îmbunătăţite pentru o mai bună detectabilitate a amenințărilor de tip "nou"; generării unei mai mari transparențe şi responsabilități a serviciilor la solicitările societății civile şi a mass-mediei față de problemele securității colective;

• ***depăşirea problemelor politice privind schimbul de informații*** – pe fondul provocării că intelligence-ul se află la baza suveranității naționale. Analizele cost-beneficiu ale produselor de intelligence vor dinamiza mai mult schimburile național – național, iar în plan internațional, schimburile bilaterale decât cele multilaterale. Definirea termenilor relevanți trebuie extinsă: zonele de intelligence, terorism, securitate reprezintă cu totul altceva în zilele noastre, iar obiectivele, sursele şi metodele utilizate fac din procesul cooperării un aspect fundamental al eficienței operațiunilor;

• ***rezolvarea problemei încrederii privind schimburile de informații:*** pe fondul construcției „unei culturi de încredere şi cooperare";

• ***asigurarea coerenței organizaționale la nivelul comunității –*** generată de diversitatea organizațională (intelligence-ul unor state se bazează pe structuri militare datând din perioada Războiului Rece, nefiind reformate în acord cu provocările actuale) şi a procedurilor juridice privind schimburile de informații;

• ***elaborarea unui cadru legal adecvat care să faciliteze schimburile de informații –*** legislația privind protecția datelor este esențială pentru cooperarea europeană de informații, asigurând protecția vieții private a cetățenilor europeni; adoptarea unitară la nivel național a legislației în domeniul intelligence poate fi un factor multiplicator în creşterea încrederii şi amplificării schimburilor de informații în format național-UE/NATO;

• ***interoperabilitatea bazelor de date*** – în special prin asigurarea funcției „acces direct", pe baza principiului disponibilității, la bazele de date şi la combinarea acestora; indexarea unitară a informațiilor din bazele de date ale serviciilor naționale de informații şi conectarea sistemelor de comunicare între diferite instituții. Sunt necesare standarde comune pentru stocare, analiză şi schimburi de informații şi se poate acționa pe trei opțiuni[36]: fuzionarea sistemele existente într-un singur „Sistem Unic de Informații"; păstrarea sistemele independente şi crearea de noi sisteme; investigarea, armonizarea şi punerea în aplicare a formatelor de date şi a normelor respective de acces între diferitele sisteme;

• ***securitatea mijloacelor de comunicare – clasificare a informațiilor***: presupune implementarea unor soluții care dă diminueze standardele de clasificare a informațiilor, precum şi a elaborarea unor standarde comune pentru pentru stocarea de informaţii, analiza şi schimbul între serviciile competente.

CNIM are nevoie de informații calitative, obținute inclusiv în procesele de schimb de informații la nivel național sau al organizațiilor de securitate din care face parte, în atingerea obiectivului de a furniza securitate statului şi cetățenilor săi.

Promovarea unei strategii de sharing la nivel național este fundamentală în condițiile actualului mediu de securitate. Un astfel de demers, care pune accent pe satisfacerea nevoilor de securitate națională, este în măsură să asigure realizarea a 3 obiective:

• **consolidarea culturii privind schimbul de informații** prin accentuarea beneficiilor de informare activă şi schimbul de cunoaştere;

• **facilitarea schimbului de informații** prin utilizarea integrată şi concentrată a tehnologiei informației şi capabilităților tehnologice la dispoziție;

• **eficiența schimbului de informații**, în timp real.

Cultura de sharing trebuie să reprezinte o opțiune şi o parte a culturii fiecărei entități de informații național, lucru care va sta în atenția tuturor nivelelor de management şi leadership, în condițiile în care se respectă drepturile şi libertățile fundamentale ale omului şi nu se atentează la viața privată a cetățenilor, aşa după cum am văzut, deveniți subiecți ai Strategiei de securitate națională.

[36] Communication from the Commission to the Council and the European Parliament of 16 June 2004: Towards enhancing access to information by law enforcement agencies [COM (2004) 429 final].

Schimbul de informații poate conduce la un acces sporit şi rapid la noi surse de informații utile în procesul de manageriere a riscurilor, îmbunătățeşte cunoaşterea privind domeniile de activitate ale serviciilor, misiunile acestora, a operațiunilor şi procedurilor. Totodată, valorifică expertiza în cadul activităților derulate cu structurile partenere, furnizează cunoaştere privind capabilitățile şi limitările acestora pentru executarea misiunilor comune, asigură parteneriate de colaborare solide şi interacțiuni coordonate de cunoştințe în măsură să sinergizeze eforturile în direcția realizării obiectivelor de securitate națională.

Realizarea acestor deziderate se bazează pe o fundamentală „încredere" între entitățile componente ale comunității de informații. Această încredere rezultă din influența pe fiecare entitate o exercită în interiorul organizației şi rezultă din înțelegere, interacțiune şi experiențele pozitive obținute, atât la nivel organizațional, cât şi personal. Încrederea în schimbul de informații: scade lacunele de informare prin furnizarea de informații pertinente la nivel național; oferă contextul amenințărilor identificate, respectiv, facilitează răspunsuri la amenințări care depăşesc granițele organizaționale; consolidează colaborarea privind evaluarea de risc prin îmbunătățirea accesului la date şi analiză; ajută organizațiile să standardizeze procesele şi să alinieze obiectivele lor cu scopul comun.

Eforturile şi inițiativele ce pot fi lansate în direcția schimbului de informații trebuie să se orienteze, în principal, pe modelarea şi influențarea atitudinii, precum şi consolidarea aprecierii valorii acestui deziderat, concentrând eforturi pentru a integra pe deplin „sharingul" în cultura organizației, valorile şi evaluările interne.

Schimburile analitice şi participarea în cadrul unor „Joint Task Force", Centre de analiză în diferite domenii cu relevanță națională, îndeplinirea unor misiuni comune sunt repere de oportunitate pentru îmbunătățirea schimbului de informații şi a consolidării cunoştințelor instituționale în problemele ce vizează activitatea de informații.

Un alt reper al definirii strategiei de sharing îl reprezintă nevoia de a încuraja, a facilita şi extinde schimbul de informații eficient, prin eliminarea barierelor de comunicare şi facilitarea mijloacelor care pot conduce la realizarea ei. În realizarea acestui obiectiv, considerăm oportun şi necesar sprijinul întregii comunități în promovarea politicii de a genera perspective mai largi, proiecte individuale şi programe de impact asupra filosofiei fiecărui sistem şi activități desfăşurate.

Strategia de sharing trebuie să garanteze că, în toate împrejurările, entităţile informative ale comunităţii de informaţii asigură protejarea intimităţii, libertăţilor civile, precum şi alte drepturi legale ale persoanelor civile, să determine ca acestea să nu fie compromise, iar orice acţiune de verificare a aspectelor ce ţin de viaţa privată să fie realizată exclusiv pentru îndeplinirea unor obiective ce ţin de securitatea naţională, în cazuri bine documentate şi în virtutea procedurilor legale instituite.

Punerea în aplicare a Strategiei de sharing implică angajarea unor iniţiative tehnologice şi înlăturarea impedimentelor în schimbul de informaţii, iar în această direcţie, credem că, realizarea interconexiunilor cu diferite centre de fuziune ale actorilor implicaţi în realizarea securităţii naţionale, consolidează importanţa eforturilor instituţionale de gestionare şi schimb de informaţii sensibile, clasificate şi neclasificate.

Efectuarea unui schimb de informaţii eficient reprezintă scopul final al unei viitoare Strategii de Sharing pentru CNIM. Acesta are rolul de a consolida conceptul de securitate naţională în raport cu ameninţările şi riscurile generate de mediul de securitate. Creşterea eficienţei reprezintă rezultatul consolidării culturii schimbului de informaţii determinat prin motivaţiile însuşite, facilitarea schimbului, utilizarea abilă a capacităţilor tehnologice. Crearea unor relaţii puternice între componentele comunităţii este în măsură să genereze încredere sporită, să înlăture diferite bariere organizaţionale şi să permită comunicaţii îmbunătăţite, relaţii de cooperare deschise şi în timp real.

Schimbul de informaţii trebuie conştientizat şi în planul funcţionalităţii interne a fiecărei entităţi informative a comunităţii. Gradul de conştientizare asigură cunoaşterea mediului de lucru în care organizaţia funcţionează permanent, oferind contextul şi un sens al fiecărei ameninţări care operează sau are legătură cu mediul respectiv. Totodată, oferă managerilor o mai bună informare a managerilor pentru o mai bună aliniere a resurselor cu priorităţile în gestionarea ameninţărilor.

Redefinite, reperele unei strategii de sharing la nivelul CNIM pot fi:

- **asigurarea cadrului general** privind îmbunătăţirea responsabilităţilor şi siguranţei diseminării în cadrul comunităţii şi cu partenerii externi şi beneficiarii;
- **realizarea concentrării** atât pe aspectele de ordin tehnologic, cât şi pe problemele legate de politici, legalitate, aspecte culturale – considerate factori importanţi în realizarea progresului;

- **definirea scopurilor şi obiectivelor**[37] **–** repere în elaborarea proiectului strategiei (de ex.):

➢ ***optimizarea diseminării în cadrul comunității sau cu partenerii şi beneficiarii în scopul realizării avantajului deciziei – pp.*** identificarea, validarea şi adresabilitatea nevoilor de diseminare; managerierea relațiilor privind diseminarea în cadrul comunității, cu partenerii sau beneficiarii; identificarea, obținerea şi asigurarea informațiilor relevante atât în interiorul cât şi în exteriorul comunității pentru a îmbunătăți avantajul deciziei; controlul capabilităților beneficiarilor şi partenerilor asupra diseminării informației pe linia folosirii de către comunitate;

➢ ***maximizarea şi integrarea capabilităților comunității pentru descoperirea, accesul, reținerea, stocarea, diseminarea şi exploatarea informațiilor – pp.*** intelligence integrat, implementarea unei arhitecturi de date eficiente ce minimizează redundanța, acces autorizat;

➢ ***maximizarea şi integrarea capabilităților comunității pentru o informare securizată – pp.*** management interoperabil, acces autorizat al utilizatorilor, auditare şi monitorizare pe linia protecției informației, protecția comunității asupra amenințărilor interne sau externe;

➢ ***optimizarea diseminării concomitent cu protejarea libertăților cetățeneşti – pp.*** stabilirea şi armonizarea de politici, standarde şi procese ce vizează culegerea, accesul, folosirea, diseminarea şi protecția informațiilor, folosirea corectă a acestora în scopul protejării intimității, drepturilor şi libertăților civile; armonizarea politicilor, dezvoltarea şi implementarea standardelor pentru conectivitate IT, securitate şi interoperabilitate cu partenerii şi beneficiarii legali; stabilirea responsabilităților şi implementarea procedurilor pentru dezvoltarea şi managementul mediului informațional multi – agenții al comunității;

➢ ***promovarea unei culturi a diseminării informațiilor responsabilă – pp.*** identificarea principiilor fundamentale şi a valorilor pentru o diseminare responsabilă; integrarea principiilor şi valorilor în elementele de performanță ale comunității de informații; promovarea instruirii, celor mai bune practici, lecții învățate în instruire; recompensarea unei diseminări responsabile în cadrul managementului performant;

- implementarea principiului *„need to share”* în domeniul intelligence şi completarea acestuia cu principiul *„need to share”* în

[37] Un model de analiză poate fi oferit de Strategia de Sharing 2011-2015 a Comunității de informații a SUA.

domeniul capabilităților prin: abordare strategică de schimb de cunoaştere şi management, operaționalizarea de capacități de relaționare robuste, servicii de colaborare permanente, soluții integrate de e-learning, mijloace de vizualizare şi sisteme de management organizațional.

În loc de concluzii...

Comunitatea de informații a secolului XXI răspunde unor provocări şi niveluri ale riscurilor de securitate de o complexitate deosebită, interconectării acestora, pe o logică operațională ce implică eficiența activităților, parteneriate puternice cu societatea civilă şi centrele de cercetare/academice, cooperare/colaborare prin schimb de informații şi cunoaştere la nivel național şi internațional. Aceste construcții asigură sinergia resurselor informaționale necesare adoptării infodeciziei naționale în problemele fundamentale ale securității, aspectele de planificare, programare, bugetare integrate, coordonare a serviciilor de informații pe proiecte informative majore. Pe aceste coordonate, considerăm că problematica depăşeşte actualul cadru de organizare şi funcționare a comunității naționale de informații, constituindu-se într-o veritabilă direcție de cercetare avansată şi un argument al ipotezei lansate: Comunitatea națională de informații modernă – organizație de intelligence.

*

* *

Demersurile exprimate cu ocazia acestui demers academic generează şi impune ideea unei „abordări comprehensive şi multilaterale a securității, într-un cadru integrat european şi euro-atlantic[38]". Importanța creării, proiectării şi utilizării de rețele şi a diseminării informațiilor în cadrul unor parteneriate solide, liber consimțite la nivel național sau al structurilor de securitate din care România face parte, devin elemente fundamentale ale procesului de cunoaştere strategică, în măsură, pe fondul capacităților şi capabilităților tehnologice uzitate, să prevină şi să gestioneze amenințările la adresa securității naționale.

[38] I. GROSU – *Cuvânt de încheiere* al vol. Coord. G. C. Maior, S. Konoplyov – *Cunoaştere Strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 245.

Bibliografie

1. *** – *Doctrina informațiilor pentru securitate* – aprobată în ședința CSAT/23 iunie 2004;

2. *** – *Viziunea 2011 -2015, SRI în era informațională*, Bucureşti;

3. G. C. Maior, S. Konoplyov (coord.) – *Cunoaştere Strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011;

4. G. C. Maior (coord.) – *Un război al minții, Intelligence, servicii de informații şi cunoaştere strategică în secolul XXI*, Editura RAO, Bucurepti, 2010;

5. G. C. Maior – *Noul Aliat, Regândirea politicii de apărare a României la începutul secolului XXI*, Editura RAO, Bucureşti, 2009;

6. Viziunea 2015 a Comunității de Informații a SUA, Bucureşti, 2008;

7. * * * – *Lumea în 2020 – O schiță a viitoruluil global prezentată de Consiliul Național de Informații al SUA*, traducere, Editura Cartier, Ed. I, Bucureşti, 2008;

8. * * * – *US Intelligence Community – Strategic Intent for Information Sharing* 2011 – 2015;

9. * * * – *National Counteintelligence Strategy* , SUA, 2009;

10. Colecția publicațiilor Intelligence editate în perioada 2008-2012.