Provocări privind definirea unui proiect național de intelligence

drd. Petrişor BĂDICĂ
Academia Națională de Informații *„Mihai Viteazul”*
petrisor_35@yahoo.com
George Răzvan ŞTEFAN
geo.stef.book@gmail.com

Abstract

Intelligence reform must be seen as a dynamic process allowing the transition to the creation of coalitions of change inside the organizations and a networked management, with multiple decision and cooperation levels where the emphasis will shift from information exchange to knowledge exchange. Basically, in the knowledge society, the distinction between intelligence and non-intelligence is a major challenge, as the geographical boundaries and jurisdictional limits are not the same anymore.

Keywords: synergy, strategic knowledge, early-warning, integrated intelligence, analysis corroborated, cooperation.

Era informațională şi provocările sale strategice

Abordarea comprehensivă şi multidisciplinară a mediului de securitate global şi a noilor realități geopolitice (nuanțate şi potențate de tehnologii şi capabilități informaționale), atât la nivelul forurilor academice sau de cercetare, cât şi la nivelul serviciilor de informații, facilitează, astăzi, înțelegerea vechilor amenințări reinventate de emergența noilor riscuri, complexitatea şi valența transnațională a acestora, sinergia[1] eforturilor şi varietatea mecanismelor de prevenire şi combatere, precum şi relevanța cunoaşterii strategice. Asigurarea unui cadru comun de cunoaştere, poate

[1] Sinergia – ca şi principiu de funcționare a unui sistem – reprezintă integrarea elementelor separate în vederea obținerii unor rezultate imposibil de atins dacă unitățile sunt autonome şi independente.

contribui la valorificarea potențialului tuturor actorilor implicați în ecuația securității naționale, fie că este vorba de servicii de informații, actori privați, centre academice sau de cercetare, think-tank-uri etc.

Cunoaşterea strategică şi era informațională

Dinamica schimbărilor din mediul operațional, în special a celor cu valențe şi nuanțe asimetrice sau transnaționale, aflate pe agenda serviciilor de informații, induce astăzi provocări complexe privind procesele de cunoaştere strategică, identificarea amenințărilor şi a consecințelor manifestării lor în planul securității individuale şi societale, individul devenind subiect al strategiilor de securitate națională pentru majoritatea statelor din spațiul euro-atlantic.

Interconectarea societăților şi dezvoltarea tehnologiilor moderne generează noi oportunități pentru inovație tehnologică şi creştere economică, dar şi noi provocări de securitate la nivelul unor actori independenți sau ai unor actori non-statali (grupări paramilitare, grupări teroriste în conivență cu rețele de crimă organizată transfrontalieră, mişcări de extremă dreapta / stânga, rasiste sau xenofobe etc.), în măsură să nuanțeze înțelegerea mediului de securitate, să determine incertitudini şi riscuri mai mari şi un viitor mai puțin predictibil, dar şi o serie de amenințări complexe şi imprevizibile care depăşesc frontierele geografice şi limitele organizaționale.

Cunoaşterea strategică devine *„(...) cheia elaborării unei hărți a intereselor şi stabilirii priorităților. Este cel mai important instrument în conştientizarea problemelor şi imprimarea unui caracter urgent pentru soluționarea acestora. Managementul şi decizia strategică necesită un anumit grad de împărtăşire a cunoaşterii*[2]*”*. Aşadar, în fața incertitudinilor în care operează serviciile de informații, putem afirma că obținerea avantajului informațional este în măsură să asigure reducerea gradului de incertitudine şi risc, în special prin utilizarea de către decidenți a informației ca instrument de putere națională. Acest lucru impune efort unificat din partea unor sisteme aliniate, flexibile, interconectate şi inovative, bine instruite şi dotate, provenite atât din zona guvernamentală, cât şi a actorilor

[2] G. C. Maior – Conferința susținută în cadrul Seminarului regional, *O abordare sinergetică a cunoaşterii strategice în Reginea Extinsă a Mării Negre*, organizat în cooperare cu Universitatea Harvard în perioada 04-06.04.2011.

privați sau a societății civile, în măsură să asigure adoptarea unor „modus operandi" sau a unor viziuni de tipul „managementului de rețea" şi care aderă la o cultură organizațională adaptată realităților mediului oprațional. Din ce în ce mai pregnant suntem martorii implementării unor concepte precum *„cooperare interinstituțională"*, *„need to know vs. need to share"*, *„intelligence sharing"*, *„parteneriat în domeniul intelligence"* în strategiile de securitate, în definirea politicilor de reformă şi educație, în doctrinele şi studiile de intelligence, cu semnificația scopului promordial de eficientizare a coordonării şi schimbului de informații la nivel național şi a cooperării în format internațional, fără a pune în pericol resursele şi metodele utilizate în atingerea obiectivelor de securitate asumate.

În contextul societății informaționale, amenințările sunt din ce în ce mai greu de identificat, lucru care determină provocări complexe privind modalitatea de contrucție şi identificare a responsabilităților, rolurilor şi misiunilor instituțiilor îndrituite să asigure securitate națională, în special a comunității de informații. Philip Bobbitt[3] prezintă antinomiile cunoaşterii create de actualele modele de securitate, care influențează rolul activității de intelligence: public *versus* privat; securitatea națională *versus* securitatea internațională; servicii de informații *versus* instituții responsabile cu aplicarea legii; surse secrete *versus* surse deschise; culegere de informații *versus* analiză; producție *versus* consum de intelligence.

Pe acest fond, ***competitivitatea în intelligence determină obținerea avantajului informațional***, fiind influențată de următorii factori[4]:

- comprimarea timpului de reacție, respectiv de prelucrare a datelor;
- capacitatea de interpretare sau integrare a datelor cu accent pe analiza multisursă şi abordarea multidisciplinară a problemelor de interes strategic;
- forma şi metodologia corespunzătoare produselor informative prin utilizarea unor metode şi tehnici analitice în varii situații, permițând eliminarea eşecului analizei din cauza subiectivismului specialiştilor implicați.

[3] P. Bobbitt – *Terror and Consent. The Wars for the Twenty- First Century*, Penguin Books, Londra, 2008, pp. 290-230.

[4] Ciobanu C. – *Rolul procesului de intelligence strategic în gestionarea noilor provocări ale mediului internațional de securitate*, referat Teză de doctorat, Bucureşti 2011.

Cunoaşterea strategică implică înțelegerea comprehensivă a fenomenelor cu implicații asupra securității, sens în care modelele de analiză multisursă sunt definitorii şi implică participarea tuturor resurselor informaționle ce pot genera cunoaştere la nivel național. Astăzi, riscurile şi amenințările sunt tot mai complexe, interdependente şi depăşesc prin natură şi profunzime granițele naționale, acest lucru implicând angajarea unor formate de cooperare internațională şi schimburi de informații. Reiterăm faptul că, nu putem aborda procesele cunoaşterii strategice fără a evidenția rolul cooperării în vederea schimburilor analitice în cadrul unor parteniate internaționale, în special pe zona noilor riscuri, asimetrice: criminalitatea cibernetică, terorismul, dezastrele naturale, problemele de mediu, securitatea energetică etc.

Nevoia de a asigura factorilor de decizie cunoaştere strategică este relevată şi de adj. dir. SRI, Ion Grosu, sens în care acesta evidențiază faptul că *„(...) dinamismul extrem al mediului de securitate creşte probabilitatea evenimentelor neprevăzute şi extinde importanța previziunilor strategice, a identificării riscurilor şi oportunităților, a analizei şi avertizării*[5]*”.*

Provocări strategice la adresa securității naționale – riscuri noi şi oportunități de transformare a intelligence-ului

Incertitudinea îşi are izvorul în lipsa de predictibilitate. În societatea secolului XXI, provocarea pentru intelligence şi, implicit, pentru cunoaşterea strategică o reprezintă modul de integrare a opțiunilor politice, economice, sociale, istorice şi culturale, sociale şi informaționale, instrumentele care asigură integrarea, precum şi relevanța posibilelor referințe legate de ritmul, intensitatea şi gradul de certitudine al vulnerabilităților şi riscurilor viitoare.

„Combinația dintre vechile şi noile amenințări ridică tot mai multe probleme pentru comunitățile de informații[6]*”* – relevă directorul SRI în vol. *„Cunoaşterea strategică în zona extinsă a Mării Negre”*. Întărim această idee iterând necesitatea edificării unei noi comunități a celor care pot facilita

[5] I. Grosu – Cuvânt de încheiere, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Ed. RAO, București, 2011, p. 250.

[6] G. C. Maior – *De la intelligence la politici – rolul cunoaşterii strategice în asigurarea securității în zona Mării Negre*, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 25.

cunoaşterea strategică, în care societatea civilă, centrele academice şi de cercetare, resursele de intelligence privat, alături de serviciile de informaţii, pot furniza soluţii la problemele fundamentale ale securităţii naţionale.

Dacă reflectăm asupra reperelor / problemelor generate de mediul de securitate actual, analiştii de intelligence atrag atenţia asupra necesităţii unui management superior pentru gestionarea / controlul acestora, proces în care responsabilităţile nu pot reveni numai unui singur stat, ci reprezintă efortul sinergetic al întregii comunităţi internaţionale. Între **fenomenele şi provocările care vor influenţa mediul de securitate la nivel global**, amintim[7]:

- *apariţia şi consacrarea unor actori internaţionali non-statali importanţi*, care se raportează la alte valori decât cele naţionale, capabili să gestioneze domeniile şi sectoarele emblematice ale puterii, precum economia şi finanţele, resursele energetice, tehnologiile ultraperformante etc.;
- *prezenţa recesiunii economice mondiale,* în măsură să crească fragilitatea situaţiilor de securitate în câteva regiuni cheie;
- *globalizarea ireversibilă* care tinde să devină mai puţin occidentală şi care va genera imense convulsii economice, culturale, politice (guvernele slabe, economiile rămase în urmă, extremismul religios vor asigura condiţiile perfecte pentru conflicte interne în anumite regiuni);
- *fragmentarea politică internă*, evocând, aici, exemplul statelor care au suportat evenimente sociale în zona islamică şi, în care, opoziţia nu se manifestă ca o alternativă consacrată, lucru ce poate avea implicaţii sociale şi politice deosebite în plan regional sau internaţional;
- *manifestarea de noi forme de politici de identitate concentrate asupra convingerilor religioase* (islamul politic poate coaliza grupări etnice şi naţionale, existând posibilitatea creării unei autorităţi dincolo de graniţele naţionale);
- *problema sărăciei* sub aspecte de continuare/extindere, având în vedere şi potenţiala criză alimentară semnalată de experţi internaţionali în domeniu;
- *concurenţa acerbă între state şi corporaţii multinaţionale*, creşterea numărului firmelor globale care facilitează răspândirea noilor tehnologii;

[7] http://cssas.unap.ro/ro/pdf_studii/amenintari_la_adresa_securitatii.pdf., accesat la 10.10.2012.

- *ameninţările transnaţionale* complexe venite din partea terorismului, crimei organizate şi proliferării WMD;
- *problemele de mediu, cele etice* (alimente modificate genetic, securitatea datelor, cercetarea materialului biologic, senzorii ascunşi, dispozitivele biometrice) şi de natura *asigurării resurselor energetice*;
- *statele instabile şi zonele necontrolate* – zone sigure pentru organizaţii teroriste şi criminale, potenţialul acces la ADM[8] şi cauzatoare de foamete, genocid şi degradarea mediului;
- *îmbătrânirea forţei de muncă*;
- *reînvierea şi extinderea naţionalismului* şi a tot ce este asociat acestuia;

Alături de acestea, în plan naţional, ***Strategia de Apărare identifică următoarele riscuri şi ameninţări la adresa României***[9]:

- extinderea modalităţilor de manifestare a fenomenului terorist în plan internaţional, prin diversificarea bazei de sprijin şi recrutare, precum şi apariţia unor noi riscuri generate de radicalizare religioasă, terorism cibernetic sau propagandă la nivel virtual;
- proliferarea armelor de distrugere în masă, precum şi dezvoltarea programelor de rachete balistice;
- criminalitatea organizată (cu caracter naţional, dar şi transfrontalier), cu un ridicat potenţial de adaptare şi capacitate de acţiune crescută în contextul crizei economice; insecuritatea publică şi personală; traficul de doguri
- fragilitatea sistemului financiar internaţional;
- spionajul şi alte acţiuni ostile ale unor servicii de informaţii, activităţile şi preocupările informative ale unor actori non-statali orientate spre influenţarea actului decizional, inclusiv a deciziei politice, a mass-mediei sau a opiniei publice;
- proliferarea unor manifestări radicale, iredentiste sau extremiste care pot afecta drepturile şi libertăţile cetăţenilor, coeziunea socială sau relaţiile interetnice;
- degradarea mediului înconjurător şi dezastrele naturale, inclusiv cele generate de schimbările climatice etc.

[8] Formularea vizează armele de distrugere în masă, care pot fi de natură nucleară, bacteriologică, chimică, radiologică.
[9] *** – Strategia de Apărare a României, Bucureşti, 2010, cap. 6.1.

În contextul provocărilor societății informaționale, așteptările privind evoluția **principalelor riscuri și amenințări în atenția intelligence-ului românesc** pot fi nuanțate astfel[10]:

- **terorismul internațional** – va genera expectații pe fond fundamentalist sau extremist, pe o logică operațională potențată de accesul facil la informație, viteză de acțiune sporită, posibilități generoase de tranzitare a frontierelor naționale şi utilizarea spațiului cibernetic drept interfață pentru prozeletism, propagandă, radicalizare, planificare şi coordonare de atacuri de amploare. Teroriştii vor miza pe o combinație a metodelor clasice, convenționale, cu acțiuni premergătoare în spațiul virtual, lucru ce conduce la ideea că originalitatea acestora constă în adaptarea conceptelor operaționale la strategiile / eforturile antiteroriste, precum şi în disponibilitatea pentru obținerea de agenți chimici / biologici sau componente nucleare capabile să provoace dezastre de amploare sau pentru lansarea unor atacuri în plan cibernetic asupra rețelelor informatice importante.
- **criminalitatea organizată transfrontalieră** – poate genera insecuritate pe fondul utilizării tehnologiei informaționale pentru obținere de profit ilegal, lucru ce poate conduce la specializarea grupurilor ce acționează în spațiul virtual, care pot „închiria" anumite servicii (contra unor sume importante) pentru lansarea unor atacuri devastatoare asupra unor ținte facile sau coordonarea unor operațiuni ilegale de trafic de droguri, contrabandă cu produse puternic accizate şi contrafăcute, spălare de bani, cu păstrarea confidențialității şi ștergerea oricăror urme, potrivit regulilor cunoscute ale grupărilor criminale. În conexiune cu interesele terților, inclusiv a unor grupări teroriste, tehnologia potențează mişcările operaționale ale crimei organizate încât diferența dintre vulnerabilitate şi pericol este dată de relevanța informațiilor obținute şi rapiditatea adoptării contramăsurilor active.
- **spionajul** – va contribui la definirea şi apărarea intereselor de securitate ale statelor, pe toate componentele sale, lucru ce va angaja resurse tehnologice importante şi va valida / perfecționa metode şi angajamente diverse, inclusiv în spațiul cibernetic. Obținerea de informații secrete utilizând rețelele informatice sau accesarea / diseminarea acestora prin acțiuni tip „Wikileaks" vor face parte din arsenalul serviciilor de intelligence. Tot o oportunitate operațională este generată de procesul globalizării, eonomice în principal, prin modalități disimulate de acoperire a intențiilor / preocupărilor de

[10] www.sri.ro/ce-facem/ce-facem.html, accesat la 10.10.2012.

culegere de informații sau prin utilizarea unor actori non-statali pentru acest scop sau pentru influențarea unor decizii strategice.

- **securitatea economică** – rămâne un deziderat greu de apărat în condițiile interconectărilor transnaționale şi a evoluțiilor tehnologice majore. Dezvoltarea societății informaționale potențează ritmul schimbărilor economice, importanța informației strategice şi nevoia de protecție a acesteia, sens în care sunt necesare strategii de cunoaştere, prevenire şi diminuare a riscurilor şi vulnerabilităților ce țin de funcționalitatea, stabilitatea şi reziliența infrastructurilor critice.
- **apărarea ordinii şi valorilor constituționale** – va fi provocată de evoluția tehnologică prin influențarea proceselor de conducere/coordonare în planul dezvoltării societale, alterarea deciziilor autorităților publice şi limitarea / îngrădirea accesului cetățenilor la serviciile publice. Securitatea cetățeanului, limitarea actelor de prozeletism pe fond religios sau extremist, precum şi apărarea libertăților constituționale împotriva riscurilor generate de utilizarea ilegală a tehnologiei pentru interceptarea comunicațiilor şi violarea spațiului vieții private trebuie să fie atent evaluate şi gestionate de serviciile de informații în scop de cunoaştere, prevenire, protecție şi contacarare.
- **amenințarea cibernetică** – relativ nouă în peisajul amenințărilor tradiționale, nuanțează fenomenele de cunoaştere strategică şi solicită efort unanim, coordonat şi integrat al structurilor cu atribuții în domeniul securității naționale pentru luarea sub control şi gestionare adecvată. Colectivitatea devine tot mai interdependentă de sistemele de informații şi comunicații şi integrează din ce în ce mai mult rețele de baze de date, accentuând astfel efectele riscurilor specifice erei informaționale asupra comunității şi societății româneşti.

Pe acest fond al identificării noilor riscuri şi amenințări, indisolubil legate de securitatea națională, **este necesar să înțelegem spiritul următorilor factori în definirea intereselor naționale:**

- interesele noastre economice, conexiunile culturale şi familiale sunt pretutindeni în lume, sens în care va trebui să generăm puternice relații de parteneriat cu țările respective;

- asigurarea fluxurilor vitale de energie, resurse şi capital trebuie să se realizeze într-un mediu securizat;

- asigurarea securității naționale se realizează prin parteneriate cu alte țări;

- poziția geografică înscrie România pe axul migrației ilegale şi a altor amenințări asimetrice, cu relevanță pentru securitatea Europei şi a spațiului euro-altlantic;

- securitatea internă nu poate fi disociată de securitatea împotriva amenințărilor venite din exteriorul țării.

În tot acest demers academic este de reliefat faptul că la nivelul comunității de informații, pe baza studiilor şi analizelor privind viitorul intelligence, *au fost identificate o serie de premise care contribuie şi energizează procesele de transformare*, iar dacă ne referim la contextul actual al societății informaționale şi la fenomenele care vor influența mediul de securitate în perioada următorilor ani, putem concluziona că acestea sunt indisolubil legate de[11]:

▪ *competiția între agențiile de informații, mediul de afaceri şi societatea civilă*, pe fondul circulației rapide a informației şi trecerii valorii ei de la dreptul de proprietate la valoarea analizei acesteia (putem vorbi de o „privatizare a intelligence-ului" care nu poate fi controlat sau limitat de stat);

▪ *dificultatea definirii adversarilor*, unii actori considerați mai puțin importanți ajungând să influențeze agenda politică a statelor (ONG-uri, grupări teroriste, grupări paramilitare în entități secesioniste ce dispun de armate private, amenințările clasice din zona spionajului transpuse prin racolarea de politicieni, oficiali guvernamentali şi influențarea deciziei politice etc.);

▪ *dinamica tot mai mare a fluxurilor de bunuri, persoane, mobilitatea rețelelor teroriste sau de crimă organizată, crearea mediului virtual de manifestare a unor riscuri* (terorismul cibernetic, autoradicalizarea pe internet, furtul de informații clasificate, rețele de contacte şi forumurile de discuții ale unor organizații radicale);

▪ *extinderea plajei securității naționale* asupra unor fenomene puțin studiate în zona serviciilor de intelligence: crizele economice sau alimentare, pandemiile, competiția pentru resursele energetice, vulnerabilitățile infrastructurilor critice, schimbările climaterice;

▪ *viteza de circulație a informațiilor* – informațiile secrete devin mâine publice, informația strategică îți pierde valoarea pentru procesul de luare a deciziilor dacă nu este utilizată oportun, media publică devine o sursă de informații mai rapidă decât serviciile sau chiar o sursă pentru acestea;

[11] G. C. Maior, *Un război al minții. Intelligence, servicii de informații şi gândire strategică în sec. XXI*, Editura RAO, Bucureşti, p. 132.

▪ *accentuarea „prăpastiei" cognitive dintre analistul de intelligence şi factorul de decizie*, în contextul actual al globalizării şi al accesului facil la informația din surse deschise.

Un proiect național, integrat şi interconectat de intelligence – între viziune şi sinergie

Un sistem de securitate națională consolidat, obiectiv al Strategiei de Apărare a României, poate fi atins prin construirea şi menținerea unei stări de echilibru şi de eficiență în funcționarea sistemului de instituții naționale implicate în atingerea țelurilor comune, ecuație în care serviciilor şi structurilor departamentale de informații le sunt atribuite roluri vitale. Acesta trebuie să răspundă actualelor nevoi de dezvoltare a țării şi a necesității afirmării internaționale, în special la nivelul Alianței Nord-Atlantice şi Uniunii Europene, în cadrul matricei de securitate care cuprinde[12]:

- relația securitate – prosperitate – identitate;
- conceptul multidimensional de securitate;
- echilibrul între stat şi individ ca beneficiari ai securității naționale;
- conducere politică şi control democratic în gestionarea integrată a securității;
- gestionarea integrată a securității;
- ideea de comunitate de securitate[13].

În fața acestor provocări şi în contextul mediului de securitate modern, caracterizat de o dinamică înaltă, varietate, neuniformitate şi de ambiguitatea cauză – efect, întrebarea fundamentală ce rezidă din analizele comunității academice şi de cercetare este: ce tip de arhitectură de intelligence trebuie construită astfel încât aceast să răspundă noilor provocări?

[12] * * * – *Strategia de Apărare a României*, București, 2010

[13] Potrivit Strategiei de Apărare, ***conceptul are două valențe: valența națională*** – constă în gestionarea integrată a apărării țării, în cadrul căreia, plecând de la un scop comun, instituțiile statului de completează şi se sprijină reciproc (cerința este dată de caracterul multidimensionalal problemelor de securitate); ***valența internațională*** – este dată de gestionarea multilaterală a securității, care se realizează prin cooperare în cadrul organizațiilor internaționale sau a unor coaliții.

Obiective de intelligence național şi provocări ale schimbării

Viziunea unui proiect național de intelligence se conturează în jurul ideii generoase de a asigura cadrul proporțional de răspuns riscurilor de securitate şi oportunităților de promovare a intereselor naționale care să permită societății româneşti să funcționeze eficient, în condiții de siguranță şi într-un mediu operațional sigur. Acest lucru implică introducerea în problematica de cercetare a nevoii de răspuns la provocările privind contruirea unor capacități adecvate de adaptare, anticipare şi răspuns, precum şi de generare a soluțiilor naționale de adaptate a actualelor construcții de securitate în jurul valorilor de sinergie, competitivitate, eficiență, eficacitate, flexibilitate, predictibilitate. Totodată, considerăm că în cadrul proceselor de autotransformare a instituțiilor (obiectiv permanent în atenția organizațiilor performante), trebuie acordată o mai mare importanță dezvoltării capacităților organizaționale pentru a stabili o cultură instituțională adecvată şi organisme robuste, dinamice şi adaptabile.

În fața noilor realități geopolitice şi a globalizării surselor de insecuritate, considerăm important faptul că în combaterea proceselor care generează amenințări la adresa securității naționale este necesară implementarea unei abordări integrate a activităților comunității de informații, precum şi capacitatea de a corobora şi evalua riscurile şi amenințările rezultate din activitățile serviciilor de informații străine, ale organizațiilor teroriste internaționale, ale structurilor de criminalitate organizată transfrontaliere, precum şi procesele din interiorul grupurilor sociale închise. Toate acestea presupun dezvoltarea unor capacități organizaționale de interpretare şi analizare a fluxurilor de informații şi stabilirea unor condiții de eficientizare a interacțiunii şi a schimbului de informații din interiorul şi exteriorul comunității. În fond, actualele transformări care au loc la nivelul organizațiilor de intelligence, SRI asigurând pionieratul în această direcție, *„... se concentrează asupra abordărilor sigure şi sistematice destinate identificării provocărilor şi oportunităților existente, aniticipării celor emergente, evaluării şi prioritizării obiective a acestora, comunicării eficiente cu factorii de decizie şi monitorizării problemelor critice*[14]*”*.

[14] I. Grosu, Cuvânt de încheiere, în vol. *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 250.

În contextul acestor procese, ***obiectivele serviciilor de informații trebuie să aibă în vedere dinamica actuală şi previzibilă a riscurilor, amenințărilor şi vulnerabilităților şi acestea vizează***[15]:

- cunoaşterea, prevenirea şi contracararea riscurilor, amenințărilor şi vulnerabilităților la adresa securității naționale, conform competențelor proprii, precum şi apărarea şi promovarea intereselor naționale, a valorilor şi obiectivelor naționale de securitate;
- fundamentarea deciziilor şi politicilor de apărare a țării prin creşterea calității produselor serviciilor de informații şi prin dialog constant cu beneficiarii;
- îmbunătățirea capacităților de avertizare timpurie privind evoluții potențial periculoase pentru România, în special apariția surprizelor strategice;
- contracararea acțiunilor de influențare subversivă a deciziilor politice şi strategice de către servicii de informații adverse;
- creşterea capacităților operative pentru: combaterea amenințărilor subsumate fenomenului terorismului, proliferării armelor de distrugere în masă, precum şi a riscurilor cibernetice; contracararea acțiunilor de spionaj şi influență a unor actori interni şi internaționali; combaterea crimei organizate transfrontaliere; protejarea intereselor economice de nivel strategic, în spcial în ceea ce priveşte consolidarea securității energetice a statului român;
- dezvoltarea parteneriatelor cu serviciile de informații aliate şi partenere;
- contribuții la dezvoltarea culturii de securitate prin extinderea dialogului cu societatea civilă.

Pe fondul deschiderii cercetării academice privind tranformarea intelligence-ului, în acord cu schimbările mediului de securitate, considerăm oportună impunerea în dezbatere a unui proiect integrat, coroborat şi legat în rețea, precum şi dezideratul funcționării comunității de informații în parametrii strategici prognozați, în baza principiilor de adaptabilitate, aliniere şi flexibilitate evocați de Viziunea 2015 a Comunității de Informații a SUA.

Având în vedere participarea instituțiilor de intelligence în cadrul unor formate parteneriale necesare abordării amenințărilor de securitate sau la promovarea intereselor naționale, evocând aici rolul

[15] *** – *Strategia de Apărare a României*, Bucureşti, 2010, cap. 7.

intelligence-ului militar în teatrele de operaţii din Afganistan şi Irak, considerăm că abordarea integrată a activităţii de intelligence se înscrie într-un demers legitim de reformă a întregului sector al politicilor de securitate naţională, vizând, din **perspectivă sinergetică**, **următoarele obiective**:

- compatibilizarea conceptuală şi acţională a instituţiilor cu atribuţii în domeniu cu structurile de informaţii şi securitate din spaţiul euro-atlantic;
- delimitarea clară a competenţelor structurilor componente ale comunităţii (misiuni, manageri de programe şi funcţii), eliminarea suprapunerilor şi paralelismelor structurale şi operaţionale prin proiectarea unor structuri suple, reformate, capabile să se adapteze imediat dinamicii situaţiilor operative, precum şi clarificarea zonelor de intersecţie a acestora;
- analiza strategică unitară a informaţiilor privind securitatea naţională;
- proiectarea şi derularea unor proiecte de securitate generate de dinamica mediului de securitate şi de necesitatea apărării/promovării intereselor naţionale;
- organizarea proceselor de cunoaştere strategică prin elaborarea unei strategii naţionale de intelligence, bazele programării şi planificării, dezvoltarea şi managementul planurilor anuale de implementare – conducând la realizarea progresului;
- proiectarea coerentă a acţiunilor şi operaţiunilor informative, inclusiv a celor interinstituţionale sau transnaţionale şi evaluarea obiectivă a rezultatelor acestora;
- asigurarea unitară a coordonării activităţilor ce vizează securitatea naţională, în zonele de competenţă ale structurilor desemnate ca autorităţi naţionale, precum prevenirea şi combaterea terorismului, domeniile CYBERINT, IMINT, GEOINT, SIGINT, OSINT – scurtând astfel ciclul de decizie operativă şi promovând astfel în numele comunităţii parteneriate public-privat cu entităţi care au potenţialul şi capabilităţile necesare asigurării reacţiei coerente şi integrate de cunoaştere, prevenire, contracare, protecţie şi promovare;
- inducerea unităţii de acţiune şi scop printr-o conducere puternică, angajare fermă şi profesionişti care pot energiza resursa umană la dispoziţie;
- inducerea ideii de creare a unei noi culturi organizaţionale;
- asigurarea de acţiuni eficiente şi comunicaţii aliniate pentru energizarea serviciilor, componente ale noii comunităţi de informaţii;

- creşterea gradului de interoperabilitate internă în domeniul intelligence-ului şi eliminarea concurenței neproductive între structurile comunității;
- activarea unor formate de cooperare interactive, atât la nivel național, cât şi inter-agenții, în numele şi interesul structurilor componente ale comunității (agenții / servicii din NATO şi UE, servicii partenere etc.);
- instituționalizarea schimbării prin succese imediate, măsurarea şi recompensarea performanței, îmbunătățirea proceselor de comunicare internă, cu beneficiarii legali şi de cooperare;
- evaluarea unitară a surselor de informare şi gestionarea eficientă a acestora;
- asigurarea feed-back-ului operațional cu beneficiarii legali ai produselor de intelligence, îmbunătățirea ciclului de informare şi implicarea acestora în definirea unei culturi operaționale în acest domeniu;
- optimizarea şi coordonarea Diplomației intelligence-ului;
- inițierea şi operaționalizarea de parteneriate public-privat pe proiecte de securitate, în interesul şi beneficiul structurilor informative membre a comunității;
- crearea Forumului Național de Securitate ca entitate activă de consultare în definirea politicilor ce vizează securitatea națională, valorificarea expertizei în domeniu, îmbunătățirea calității produselor de intelligence şi redefinirea relațiilor între producătorii şi beneficiarii acestor produse;
- crearea Centrului de Excelență în Intelligence şi a Academiei Naționale de Intelligence ca oportunități de formare, training, cercetare şi valorificare a intelligence-ului românesc;
- relaționarea cu structuri private de intelligence, în special pe zona de analiză de risc, tip STRATFOR, precum şi promovarea, în numele structurilor componente ale comunității a legislației în domeniul intelligence.

Abordări privind definirea unui proiect național de intelligence

Deziderat al politicii de securitate națională, edificarea unui sistem integrat de management al crizelor îşi păstrează relevanța şi importanța în societatea secolului XXI. Acesta reprezintă un demers asumat de statul român în măsură să asigure *„(...) un nivel optim de pregătire, planificare operațională şi funcționalitatea tuturor structurilor de decizie şi execuție cu*

responsabilităţi în domeniu, pentru gestionarea întregului spectru al crizelor interne sau externe[16]*"*. Parte a acestui sistem naţional, comunitatea de informaţii a României asigură ansamblurile funcţionale sinergice a tuturor elementelor sale componente, în măsură să genereze susţinerea deciziilor strategice în problemele fundamentale privind promovarea şi susţinerea intereselor naţionale, dar şi activarea mecanismelor de gestionare a riscurilor şi ameninţărilor transnaţionale şi asimetrice, în cadrul formatelor de cooperare la care România este parte.

Procesele de reformă desfăşurate la nivelul statului român, într-o perioadă de sensibilitate extremă, sugerează ideea luării în considerare a unei analize obiective asupra „realităţii" în care funcţionează serviciile de informaţii în vederea adaptării acestora la mediul operaţional în care funcţionează (organizatoric, operaţional, doctrinar, cultural etc.), evaluării şi valorificării „lecţiilor învăţate" rezultate din practici similare de reformă desfăşurate în statele din comunitatea euro-atlantică (SUA, Marea Britanie, Spania, Germania), inclusiv din Europa Centrală şi de Est[17], respectiv a identificării unor „modele ale schimbării" bazate pe alinierea strategiei – organizării – performanţei operaţionale – logisticii.

Pe acest fond, **în plan naţional**, la nivelul Serviciului Român de Informaţii a fost nevoie de o viziune strategică care a vizat procesele de transformare instituţională şi modernizare structurală şi prin care au fost redefinite misiunile, obiectivele majore şi priorităţile strategice în domeniu, asigurându-se astfel evitarea surprizelor strategice şi şocurile care ar fi putut afecta evoluţia societăţii româneşti, urmată de o nouă **Viziune 2011-2015**, ancorată în ideea implementării capabilităţilor tehnice şi tehnologice necesare generării unui răspuns adecvat, corespunzător provocărilor generate de era informaţională. Trebuie să recunoaştem că necesitatea generalizării proceselor de reformă instituţională este evidentă pentru întregul sector de intelligence românesc, în acord cu nevoile de securitate ale statului român, adaptate secolului XXI.

În sensul celor prezentate, considerăm că sinergia intelligence-ului românesc vizează primordial gestionarea confruntării informaţionale prin cooptarea actualelor structuri de informaţii într-un nou proiect de

[16] * * * – *Strategia Naţională de Apărare*, Bucureşti, 2010, p. 27.

[17] Relevante sunt procesele de modernizare desfăşurate în Bulgaria (2010 – crearea Agenţiei de stat pentru Securitate Naţională) sau reformarea Comunităţii de Informaţii a Ungariei (2012).

intelligence care să le aducă la o singură referință, concepție şi resursă unică şi care trebuie să răspundă oportun, proporțional şi coordonat în domeniile:

- confruntării de comandă şi control;
- confruntării pentru supremație informațională;
- confruntării electronice;
- confruntării psihologice;
- pirateriei informaționale;
- informațiilor economice;
- confruntării pentru controlul spațiului cibernetic.

În opinia specialiştilor din domeniu, modelarea şi edificarea unui proiect de intelligence nu ține exclusiv de generarea unor restructurări de amploare ci de direcționarea viitoare a transformării tuturor actorilor implicați în activitatea de intelligence, într-o nouă paradigmă, prin asimilarea „puterii digitale" ca parametru indispensabil al activității operaționale, prin identificarea mecanismelor de utilizare eficientă a resurselor informaționale, pe platforme colaborative, politici de securitate şi adoptarea culturii schimbului de informații, prin o mai bună utilizare a fondurilor financiare pe proiecte de securitate comune şi priorități operaționale, respectiv printr-o mai bună coordonare şi evaluare obiectivă a performanțelor, în context sistematizat şi standardizat.

Într-o abordarea sistemică, comunitatea de informații trebuie să aibă caracteristicile unui sistem deschis, cu granițe imperceptibile şi dependență informațională în mediu, o organizație robustă, puternică, dinamică adaptabilă la schimbările de mediu, cu niveluri ridicate de monitorizare şi control.

În sensul celor prezentate, directiva fundamentală privind definirea unui proiect național o constituie realizarea unei comunități de informații, integrată şi colaborativă, bazată pe servicii mutuale, operațiuni centrate pe misiune, management integrat al acestora, angajare de resurse, oameni şi tehnologii ale căror limite depăşesc pe cele generate separat de servicile de informații care compun actualmente comunitatea.

Cu alte cuvinte, în plan operațional, considerăm că o construcție națională de intelligence trebuie să fie activă, adaptabilă şi integrată, în măsură să asigure avantajul decizional şi realizarea următoarelor obiective:

- construirea unor capacități integrate pe baza utilizării tehnologiilor informaționale şi a platformelor colaborative pentru a

răspunde întregii game de provocări de securitate şi a susține noi misiuni introduse pe agenda serviciilor de informații;

- definirea unui model de intelligence orientat către beneficiarii informaților de securitate naționale şi operaționalizarea raporturilor cu aceştia într-o nouă paradigmă;
- îmbunătățirea capacităților şi capabilităților de „early warning" şi de previziune strategică, România fiind conexată la problemele globale ale securității, iar actualmente interesele naționale se apărără şi în Afganistan;
- edificarea unor proiecte naționale informative la care să participe pe lângă angrenajul instituțional şi alți actori care pot furniza expertiză, inclusiv elemenete de intelligence privat, concentrarea pe misiuni, conexarea tuturor posibilităților de colectare de informații (HUMINT, SIGINT, GEOINT, CYBERINT, MASINT, ELINT etc.) şi schimbul de informații în timp real;
- edificarea şi definirea unei culturi organizaționale adaptate cerințelor mediului informațional al secolului XXI, precum şi dinamizarea schimbului de informații prin definirea strategiei de sharing, sectorial şi la nivelul comunității;
- integrarea elementelor strategice de inteligence – capital uman, training, resurse, cercetare, tehnologie şi politici de inovare, sprijin logistic;
- schimbarea fundamentală a leadership-ului în ceea ce priveşte orientarea tradițională centrată pe serviciu către un nou stil bazat pe colaborarea între servicii şi către experiență interdisciplinară.

Suntem conştienți că întotdeauna vor fi activate puncte de vedere privind impedimentele şi limitările unei noi construcții (majoritatea țin de rezistența la schimbare, de ordin intern şi cultural, de existența zidului birocratic, sau de lipsa de încredere), însă, constatăm că atunci când există voință şi disponiblitate, chiar fără nuanțe gen ordine precise, concise, inovatoare, lucrurile se schimbă, pentru că natura umană a ofițerilor de informații şi disponibilitatea acestora de a răspunde unor provocări generate de realitatea pe care o cunoasc şi o înțeleg foarte bine, excede granițelor organizaționale (schimbarea este îmbrățişată din start), în ecuație exemplul concludent fiind **Serviciul Român de Informații**. Lucrurile se complică uşor atunci când avem în vedere proiectarea unui angrenaj în care actualele servicii de informații / structuri departamentale trebuie să funcționeze într-o altă arhitectură în care suprapunerile operaționale, alocarea resurselor în raport cu rezultatele aşteptate şi misiunile acestora vor trebui redefinite.

Domenii de expertiză şi paradigme ale schimbării

Definirea unui proiect național de intelligence trebuie să aibă ca obiectiv fundamental sinergia resurselor informaționale aflate la dispoziția statului român (interne, externe, militare, de intelligence privat) în vederea abordării integrate a riscurilor de securitate, fiind în măsură să genereze o gestionare superioară a tuturor resurselor, practici uniforme şi eficiente de atragere, formare şi dezvoltare a capitalului uman, calitatea înaltă a analizelor şi nivel ridicat de satisfacție a beneficiarilor. Totodată, va trebui să rezolve lipsa de unitate în înţelegerea şi aplicarea unui set de concepte şi principii – doctrina operațională, concretizate prin:

- definirea funcțiilor de bază ale intelligence-ului;
- managementul resurselor pe bază de criterii uniforme;
- perfecționarea unitară a managementului de nivel middle-management şi top management;
- practica uniformă în cadrul comunității.

Totodată, o doctrină operațională este necesară pentru a stabili prioritățile curente şi a stabili echilibrul între cerințele adesea în competiție (*flexibilitate şi eficiență*; *oportunitate temporală şi acuratețea informației*; *extindere analitică şi adâncime analitică*; *capacitate de reacție şi nevoia de experimentare şi dezvoltare a unor „schimbări pilot" într-un sistem de intelligence)*. Aceasta trebuie să se reflecte şi în practica operațională zilnică prin importul unor metode şi sisteme validate în alte domenii, reflectând la nivel macro nevoia de management al schimbării, pe anumite paliere adaptat procedurilor din mediul privat sau chiar modului în care adversarii îşi schimbă permanent modul de acțiune pentru a nu fi contracarați.

Principalele domenii de expertiză integrată şi reperele de analiză la nivelul acestora sunt:

- **procesele de „early-warning" şi de previziune strategică:**

- extinderea şi dezvoltarea sistemelor de averizare timpurie şi prognoză;

- asigurarea capabilitării de a preveni protrivit principiului **„responsability to provide"**;

- adoptarea unor politici anticipative la nivelul analizei strategice şi proceselor de prognoză generate la nivelul comunității sau în urma unor procese paralele de prognoză civile derulate în parteneriat cu comunitatea de informații (există subiecte pentru care sursele deschise sau nesecrete vor fi unice şi suficiente să genereze indicatori de avertizare);

- dezvoltarea capacității de reacție la nivel național prin managementul riscului – dată de valoarea anticipării strategice şi preavertizării adecvate a transformărilor din punct de vedere al nivelului şi tipului amenințării cu care se confruntă societatea, în probleme sensibile precum anticiparea proliferării tehnologiei chimice, biologice, radiologice sau a celei utilizate în atacuri cibernetice;

- consolidarea dimensiunii psihologice a capacității de reacție la nivel național, care constă în rezistența populației în perioade de incertitudine şi instabilitate şi în menținerea unei stări de normalitate (este vital modul de comunicare în timpul unor situații de criză fără a alarma populația);

- implicarea unui intelligence adaptativ, prin extinderea „rețelelor de senzori" capabili să detecteze „semnalele slabe" şi alți indicatori ai riscurilor emergente de securitate;

- realizarea unor obiective precum: **dezvoltarea expertizei** – prin stabilirea tematicilor, profunzimea şi calitatea analizelor strategice, în special în domeniile economic, energetic şi al reuserselor naturale, tehnologiei non-militare etc; **extinderea cooperării** – vizând abordări strategice cu importante centre externe de expertiză şi informații; **eficientizarea colaborării** – prin dezvoltarea şi implementarea noilor tehnologii şi capacități pentru intensificarea contactelor şi prin promovarea, culturii analizei strategice, tactice şi operaționale solide; **dezvoltarea aptitudinilor lingvistice** – pe linia intensificării cantității şi fluenței capacităților privind limbile străine.

➢ **intelligence integrat şi analiză coroborată:**

- menținerea excelenței în domenii separate şi depăşirea actualelor abordări lineare, bazate pe servicii de informații / departamente de informații, într-un nou model bazat pe misiune, care sincronizează culegerea de informații, amplifică colaborarea în chestiuni analitice în timp real şi diversifică strategia de parteneriat;

- integrarea noilor tehnologii şi procese;

- îmbunătățirea vitezei de culegere şi analiză a informațiilor prin reducerea nivelurilor verticale şi clarificarea autorității misiunii;

- impulsionarea inovației prin diversitate şi schimb de idei;

- asigurarea caracterului complet prin valorificarea expertizei de nişă;

- reducerea suprapunerilor / duplicării printr-o mai bună coordonare;

- conducere fermă, reconceptualizare a proceselor de organizare, pregătire şi operare;

- alocarea / realocarea dinamică a ciclului informațional şi evidențierea rolul pregnant al culegerii de informații din surse deschise;

- generarea: abilității de a realiza penetrări adânci şi persistente ale țintelor vizate; punerii accentului pe echipe multi-agenții care folosesc strategii „multi-INT" de culegere de informații; utilizării profesioniştilor care vorbesc limbi străine şi cunosc cultura în care operează; arhitecturii integrate de procesare, exploatare şi diseminare a informațiilor de securitate către beneficiarii legali; modernizării sistemului de culegere care să faciliteze vigilența generală asupra stării senzorilor şi alinierea tuturor mijloacelor de culegere, pentru a răspunde cerințelor beneficiarilor informațiilor de securitate națională;

- crearea plusvalorii față de suma cunoaşterii individuale existente la nivelul structurilor ce compun comunitatea;

- remodelarea ciclului tradițional al activității de informații pentru ca modelul de analiză a informațiilor să răspundă schimbărilor rapide ale mediului de securitate şi, pe acest fond, necesităților de informare ale beneficiarilor;

- definirea unui nou tip de abordare a produselor de intelligence în care accentul se va comuta de la aspectele individuale la operațiuni în colaborare;

- eficientizarea şi optimizarea întregului ciclu informațional, precum şi la îmbunătățirea relației dintre ofițerii operativi şi analişti implicați în procesul de culegere, prin: evaluarea rapoartelor disponibile în proiectele de securitate, pe baza certificatelor de securitate care dau drept de acces celor implicați în acestea; validarea / revizuirea propunerilor analiştilor pentru noi culegeri de informații în colaborare; etichetarea şi păstrarea informației în medii securizate; promovarea cunoaşterii la nivelul comunității, generând îmbunătățirea calității cererilor de culegere de informații, cât şi gradul de sofisticare a judecăților analitice; adaptarea produselor şi serviciilor transmise către beneficiari la nivelul nevoilor în creştere de informație actuală şi analiză pertinentă, în mod personalizat; implicarea în timp real a comunității de analiză integrată în clarificarea nevoilor în schimbare ale beneficiarilor;

➢ **culegere de informații din surse deschise:**

- implementarea proceselor de analiză multisursă şi multidisciplinară care reuneşte componentele de intelligence strategic în ansamblul lor;

- dezvoltarea programelor de *„outsourcing"* în domeniul analizei, *„privatizarea evaluării"* prin expertiză oferită de unele firme private în analiza riscurilor globale (tip „STRATFOR"), realizarea de rețele neoficiale

de distribuție a informațiilor din surse deschise sau companii care permit accesul, contra cost, în mediul virtual, la analizele şi evaluările lor, precum şi firme care oferă produse de competitive intelligence, business intelligence sau derivate ale acestora;

- îmbunătățirea capacităților de culegere / diseminare a informațiilor din surse deschise, coroborarea cu date obținute prin metode secrete sau generate de o rețea de experți externi, stabilindu-se astfel relevanța acestora pentru agenda beneficiarilor şi înțelegerea clară a situației de securitate;

- îmbunătățirea comunicării între beneficiarii, analiştii, ofițerii operativi şi sursele deschise utilizând tehnologia informațional.

➢ **tehnică, tehnologie şi inovație:**

- operarea pe o bază comună inter-servicii de intelligence şi securitate / inter-agenții, în problemele fundamentale ale securității naționale;

- crearea unor zone sigure de spațiu virtual pentru dezbatateri de grupul de analişti şi dezvoltarea altor modalități de creare şi conectare a unor centre analitice virtuale ale serviciilor componente ale comunității ce utilizează tehnologii avansate de securitate;

- utilizarea capabilităților cibernetice pentru consolidarea performanței operaționale şi a capabilităților analitice;

- trecerea arhitecturii informaționale de la modelul bazat pe discipline specifice privind culegerea de informații, analiza şi diseminarea lor, către o arhitectură unificată care permite utilizatorilor finali accesarea şi exploatarea informațiilor cu ajutorul serviciilor care includ: servicii de comunicare (e-mail, directoare, catalogare, colaborare), servicii de date (solicitare, căutări, etichetare, extragere, păstrare), servicii de securitate (înregistrare utilizator individual, control acces, monitorizare, auditare), servicii analitice (portaluri, exploatare date, vizualizare, modelare, simulare);

- reconceptualizarea fundamentală a politicilor de achiziție inovatoare, bazate pe performanță, şi a practicilor pentru achiziția de capacități logistice pentru a pune accent pe adaptare, viteză şi agilitate;

- dezvoltarea activității de cercetare, dezvoltare şi aplicare a noilor tehnologii produse din resurse interne, însă aceste programe trebuie să asigure avantaj competitiv, inovații, tehnologii disruptive, toleranță înaltă pentru risc şi eşec şi rapidă tranziție către ofițerii de informații;

- crearea unei culturi a inovației în intelligence – implică alinierea abordărilor teoretice fundamentale (concepte, tehnologie, doctrine), cu

îmbunătățirea actului de conducere, structurarea organizațională şi resursele la dispoziție.

➢ **asigurarea securității cibernetice:**

- dezvoltarea unui sistem de apărare prin cooperare în detecție şi analiză, cât şi prin implementarea măsurilor de limitare sau anulare a efectelor atacurilor;

- integrarea tehnologiilor destinate detecției şi blocării atacurilor cibernetice într-un spațiu delimitat cu cele destinate analizei comportamentului global al rețelelor, în scopul contruirii, cu costuri minime, a unui sistem centralizat de evaluare, raportare şi reacție la starea de securitate a rețelelor protejate;

- crearea unui sistem național de prevenire, identificare şi coordonare a apărării în cazul unor atacuri cibernetice, izolate sau masive, la adresa infrastructurilor informatice critice naționale şi, în perspectivă, europene, cu următoarele obiective: apărarea coordonată a infrastructurilor IT&C împotriva atacurilor cibernetice; protecția serviciilor societății informaționale europene disponibile prin mediul INTERNET; protecția împotriva scurgerilor de informații din interiorul instituțiilor publice şi a companiilor private; promovarea bunelor practici în domeniul protecției infrastructurilor informatice critice; dezvoltarea metodologiilor de cooperare cu scopul de a promova acțiuni comune între partenerii din mediile public şi privat în cadrul infrastructurilor informatice critice şi/sau al principalilor furnizori de rețele de telecomunicații; demonstrarea aplicabilității conceptelor enunțate în interiorul unor rețele cu acoperire națională;

- definirea strategiei de combatere – prin dezvoltarea şi standardizarea instrumentelor comune de identificare şi răspuns la incidente semnificative de securitate cibernetică din sectoarele public şi privat, în cadrul unor parteneriate public privat reale şi puternice.

➢ **securitate organizațională şi a operațiunilor:**

- redefinirea rolului securității / protecției prin adaptarea practicilor existente şi orientarea concordantă a acestora cu evoluția tehnologică şi eforturile personalului din instituțiile de intelligence;

- elaborarea unor standarde de securitate comune în parametri de eficiență impune monitorizarea permanentă a stării de securitate existente;

- atribuirea unui nou rol funcției securității prin: determinarea clasificării, monitorizarea şi conducerea întregului proces de dezvoltare a informațiilor clasificate, apărarea secretului;

- definirea şi consolidarea conceptului integrat de protecţie, brodat pe legislaţia internă privind protecţia informaţiilor clasificate sau pe cea generată la nivelul UE/NATO;

➢ **management resurse umane**:

- omogenizarea proceselor de formare şi perfecţionare, precum şi profesionalizarea prin sistematizarea cunoştinţelor privind fundamentele teoretice, metodologice şi tehnice în ansamblul comunităţii (trainig şi exerciţii aplicate; elaborarea politicilor şi doctrinelor în intelligence – HUMINT, OSINT, SIGINT, IMINT, GEOINT etc.; cercetare-dezvoltare şi experimentare în domenii de activitate; lecţii învăţate şi baze de date);

- generarea de programe de dezvoltare pentru conducere, sisteme de evaluare a performanţei şi o structură unitară de stimulente pentru întreaga comunitate;

- atragerea, dezvoltarea şi reţinerea unei forţe umane diverse, cu cunoştinţe tehnice, lingvistice şi culturale care să contribuie decisiv la realizarea obiectivelor misiunii, axate pe obţinerea de rezultate şi performanţe ridicate, capabile să furnizeze expertiza tehnică şi conducerea excepţională;

- corelarea proceselor de atragere, pregătire şi păstrare a unei resurse umane înalt calificate, creative şi adaptabile, inclusiv din mediul privat, mediul academic, cel al ONG-urilor şi think-tank-urilor, cu generarea unui sistem de recompensare a performanţei, promovare în carieră şi protecţie socială adecvată;

- definirea unui nou profil al ofiţerilor de intelligence, reflectate în documentele exclusive ce vizează ocuparea unor posturi: competenţe lingvistice excelente, cunoaştere excelentă a mediului cultural, bună stăpânire a naturii umane, capital anteprenorial şi centrat pe beneficiar, capabil de a combina cunoştinţele funcţionale şi expertiza cu cele de colaborare şi relaţionare, aptitudini de a juca diferite roluri în carieră şi nu posturi exclusive;

- promovarea profesiei în domeniul „intelligence" care să atingă un anumit nivel de expertiză, responsabilitate şi spirit corporatist şi să încorporeze practici formale şi structurate în politica de personal, fundamente în dezvoltarea unor exigenţe de încadrare stricte, programe susţinute de profesionalizare şi expertiză, un cod de etică strict, precum şi alte mecanisme care să permită pregătirea şi perfecţionarea cumulativă;

- adaptarea proceselor de instruire şi perfecţionare continuă a personalului operativ, integrându-se cunoştinţele IT în procedurile de lucru ale acestuia, pentru a fi asigurată valorificarea directă a componentei CYBERINT în fluxurile informaţionale specifice procesului de intelligence;

- definirea unor noi indicatori de performanţă în intelligence, orientaţi spre calitate şi nu pe cantitate, în proces un rol important revenind beneficiarilor, întrucât evaluarea finală a eficienţei derivă din capacitatea de a schimba şi influenţa mediul de securitate în interiorul căruia acţionează;

- redefinirea culturii organizaţionale care să valorizeze loialitatea şi grupul, fapt ce poate canaliza schimbarea în sistem.

➢ **promovare publică a activităţii de intelligence şi a culturii de securitate:**

- generarea la nivelul opiniei publice a unui nivel de încredere favorabil activităţilor / acţiunilor desfăşurate;

- consolidarea unui parteneriat operaţional prin care activitatea serviciilor de informaţii va fi validată de către cetăţean, acesta fiind convins că, **în toate împrejurările**, drepturile şi libertăţile fundamentale îi sunt apărate, că este protejat împotriva oricăror ameninţări şi că demersurile / activităţile comunităţii sunt permanent sub controlul său, prin mecanismele legale instituite;

- elaborarea unei strategii de promovare publică, valabilă pe durata ciclului de viaţă al strategiei de informaţii, precum şi derularea unor activităţi de promovare publică prin care să se realizeze conectarea societăţii civile la circuitul intern şi internaţional de forumuri academice şi instituţionale pe teme de securitate;

- iniţierea unei ***public diplomacy*** prin angrenarea resurselor partidelor şi organizaţiilor politice, organizaţiilor economice şi brand-urilor, ONG-urilor şi societăţii civile, grupurilor de interese, statului şi partenerilor statali poate fi o sursă de generare a proceselor care pot contribui la valorificarea cunoaşterii;

- instituirea şi funcţionarea optimă a unor canale de dialog şi consultare între instituţiile statului şi societatea civilă, în special cu mass-media;

- fundamentarea unei politici de educaţie pentru cultura de securitate care să asigure: promovarea dialogului şi comunicării între actorii publici; validarea misiunii sociale a diferitelor instituţii; promovarea unor noi concepte şi modalităţi de cooperare; identificarea unor formule concrete

de transfer de expertiză din sfera societății civile către instituțiile din sistemul securității naționale în domeniile de interes pe care cetățenii le asociază conceptului de securitate națională, precum şi a celor referitoare la valori, interese şi obiective de securitate națională;

- **relația cu beneficiarii de intelligence**

- îmbunătățirea interacțiunii instituționale cu beneficiarii informațiilor de securitate națională;

- dezvoltarea practicilor de diseminare/transmitere a produselor informaționale generând formate interactive, inclusiv interconectarea unei platforme tehnice de cooperare, prin care se realizează două lucruri importante: participarea beneficiarilor legali la definirea unor obiective privind securitatea națională; validarea / verificarea faptului că deciziile corespund realității dezvăluite de informații;

- elaborarea unor analize clare, transparente, obiective şi inteligente şi a unor informări sintetice care îmbină expertiza analitică cu relevanța ei pentru agenda publică, crearea unui dialog personalizat, interactiv, precum şi familiarizarea beneficiarilor legali cu ideea că intelligence-ul este o „sursă privilegiată";

- utilizarea unor tehnici sofisticate de depistare a nevoilor beneficiarilor şi de evaluare a performanțelor atinse de serviciile de informații;

- redefinirea relațiilor prin schimbarea accentului de la modelul centrat pe produs spre un model interactiv conduce la ştergerea distincției dintre producător şi consumator, iar prin angajarea prin *parteneriate între aceştia*, intelligence-ul poate defini acele **avantaje competitive** necesare cunoaşterii strategice;

- includerea societății civile în ecuația de securitate prin parteneriate cu agențiile neguvernamentale, think-tank-uri, academicieni, mass media şi alți reprezentanți, în vederea alertării reciproce cu privire la provocările securității naționale şi asigurării instituționalizării culturii de securitate la nivelul acestora.

Cooperarea – factor multiplicator şi condiție esențială a succesului misiunilor de intelligence

Transformarea intelligence trebuie gândită şi în domeniul cooperării între serviciile de intelligence, prin instituționalizarea unei funcțiuni necesare pentru realizarea cooperării şi eliminarea birocrației şi a tradiționalei concurențe subiective în toate verigile întregului ciclu INTEL.

Astăzi, a devenit din ce în ce mai evident faptul că în definirea unor politici de securitate națională sau regională, pentru gestionarea amenințărilor vechi şi a noilor riscuri, *„... nici un servicu de informații nu poate fi eficient în absența unei cooperări strânse cu structuri naționale similare sau cu partenerii externi*[18] *”*.

Cooperarea eforturilor informative, schimbul de informații şi alte nevoi de cooperare se realizează astăzi prin protocoale, programe, proiecte ori operațiuni informative, cu specificația că terminologia specifică introduce alți doi termeni, **conlucrare** – referitor la activitatea din interiorul unui serviciu de intelligence, respectiv **colaborare**, care, alături de **cooperare**, se realizează în spațiul intern sau extern. Cooperarea în domeniul intelligence impune o nouă etapă în conlucrarea dintre serviciile de intelligence: deplasarea centrului de greutate dinspre schimbul de informații cu caracter de generalitate spre cooperarea pe cazuri şi acțiuni punctuale, ca modalitate de valorificare optimă a potențialului oferit de partenerii implicați.

În problematica colaborării / cooperării generate la nivelul comunității de informații, considerăm că acțiunile întreprinse pe această linie trebuie să vizeze:

- creşterea interconectivității între serviciile de intelligence pentru identificarea vulnerabilităților existente la limita de demarcare a mai multor sisteme (infrastructuri critice de securitate, întreruperea furnizării de energie, piețele financiare, schimbările climatice);
- construirea unei infrastructuri robuste de informații, bazată pe o cultură a schimbului de informații;
- trecerea accentului de la „schimbul de informații” la „schimbul de cunoaştere” 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;
- realizarea unor rețele secretizate virtuale între analiştii Comunității şi ai serviciilor de intelligence, cu acces la baze de date realizate pe probleme sau domenii.

[18] F. Coldea, Contribuția serviciilor de securitate la stabilitatea Regiunii Extinse a Mării Negre, în vol. *Cunoaşterea strategică în regiunea extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011, p. 225.

Propunerea noastră integrează şi o abordare care să valorifice beneficiile generate de expertiza şi sinergiile rezultate din amploarea şi profunzimea relaţiilor de parteneriat. Consolidarea unor parteneriate existente şi stabilirea unora noi cu entităţi private şi publice, interne şi externe pentru îmbunătăţirea accesului la sursele de informaţii şi asigurarea diseminării adecvate a produselor de intelligence, reprezintă o condiţie indispensabilă funcţionării comunităţii de informaţii în condiţii de eficienţă şi performanţă. Parteneriatele pot oferi soluţia pentru problemele transnaţionale ce depăşesc graniţele organizaţionale existente, iar această abordare trebuie să se circumscrie politicii naţionale comprehensive şi să fie implementată la nivelul întregii comunităţi prin intermediul politicilor ce definesc rolurile, responsabilităţile şi autorităţile.

Realizarea acestui obiectiv de consolidare a parteneriatelor, trebuie axat pe următoarele domenii:

- ✓ consolidarea relaţionărilor existente – prin informarea partenerilor despre ce înseamnă comunitatea de informaţii, capacităţile şi capabilităţile acesteia, precum şi conştientizarea beneficiilor oferite de parteneri;
- ✓ extinderea parteneriatelor – pentru a determina schimbul de informaţii şi colaborarea;
- ✓ stabilirea de noi parteneriate – prin construirea încrederii reciproce şi a unei înţelegeri comune în ceea ce priveşte nevoile, capacităţile şi misiunile realizate cu partenerii.

Îmbunătăţirea integrării şi schimbul de informaţii sunt menite să asigure managementul informaţiilor, practicile aferente scopului propus, sistemele şi arhitecturile informaţionale, pentru a răspunde responsabilităţii de a furniza informaţii şi date, protejându-le în acelaşi timp de riscul compromiterii. Tipul şi volumul datelor se dezvoltă exponenţial alături de viteza şi capacităţile de procesare a acestora, lucru care face ca întregul ciclu informaţional să se desfăşoare într-un cadru comprimat, iar schimbul de informaţii să se desfăşoare rapid, protejând, în acelaşi timp, sursele şi metodele şi respectând drepturile şi libertăţile fundamentale ale cetăţenilor.

*

* *

Societatea informaţională generează provocări şi oferă oportunităţi atât pentru comunitatea de intelligence, societatea civilă, cât şi pentru entităţile predispuse producerii de riscuri şi ameninţări la adresa securităţii

internaţionale. Securitatea este un bun al tuturor şi tocmai de aceea serviciile de informaţii trebuie să se adapteze permanent schimbărilor din mediul de securitate, să dezvolte parteneriate public-privat şi să ofere / importe expertiza mediului privat, mediului academic şi de cercetare sau a altor actori implicaţi în ecuaţia securităţii naţionale, de asemenea să contribuie substanţial la definirea şi aprofundarea educaţiei şi culturii de securitate.

Bibliografie

1. Constituţia României;
2. *** – *Doctrina informaţiilor pentru securitate* – aprobată în şedinţa CSAT/23 iunie 2004.
3. *** – *Strategia de Apărare a României*, Bucureşti, 2010.
4. *** – *Viziunea 2011-2015 „SRI în era informaţională”*, Bucureşti, 2011.
5. *** – *Viziunea 2015 a SUA – o organizaţie globală şi integrată de intelligence*, trad., Bucureşti, 2008.
6. *** – Consiliul Naţional pentru Serviciile de Informaţii (SUA) – *Tendinţe globale 2025: O lume transformată*, 2010.
7. *** – *Strategia serviciilor de informaţii a SUA*, 2009.
8. *** – *Strategia naţională de securitate: Implicaţii pentru comunitatea de informaţii a Marii Britanii*, 2008.
9. G. C. Maior (coord.) – *Un război al minţii, Intelligence, servicii de informaţii şi cunoaştere strategică în secolul XXI*, Ed. RAO, Bucureşti, 2010.
10. G. C. Maior, S. Konoplyov (coord.) – *Cunoaştere strategică în zona extinsă a Mării Negre*, Editura RAO, Bucureşti, 2011.
11. Z. Dumitru – *Respectarea drepturilor omului în activitatea serviciilor de informaţii*, Editura RAO, Bucureşti, 2007.
12. Colecţia publicaţiilor *Intelligence* editate în perioada 2008-2012.
13. Gheorghe, Ilie – *Securitatea mediului de afaceri*, Editura UTI PRESS, Bucureşti, 2006.
14. C. Ciobanu – *Rolul procesului de intelligence strategic în gestionarea noilor provocări ale mediului internaţional de securitate*, referat Teză de doctorat, Bucureşti, 2011.
15. Olivier, Forcade; Sebastien, Laurent – *Serviciile secrete – puterea şi informaţia secretă în lumea modernă* – Editura Cartier, Bucureşti, 2008.