

SRI ÎN ERA INFORMAȚIONALĂ

Viziunea Strategică 2011-2015

Mesajul directorului Serviciului Român de Informații

Intrarea lumii în secolul XXI a fost marcată de efectele celui mai dramatic atentat terorist, de temerile generate de „virusul mileniului”, amplitudinea crizei economice, emergența unor crize energetice în Europa și a unor crize alimentare în lume, într-un cuvânt, de multiplicarea amenințărilor asimetrice și atipice la adresa securității statelor și cetățenilor.

Extinderea tipologiei riscurilor, sub presiunea erei informaționale, a condus la accentuarea incertitudinii asupra viitorului securității europene și euroatlantice. 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 și periculoase și astăzi, dezvoltarea tehnologică fără precedent și 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 și acționale în rețelele informatice determină noi forme de coagulare a securității prin care noile riscuri le modelează și le transformă pe cele clasice.

Expansiunea lumii virtuale a condus la emergența unei noi dimensiuni a puterii statale, „puterea digitală”, cu efecte pe termen lung asupra cunoașterii strategice și acțiunilor statului în plan național și internațional. De asemenea, individul a dobândit noi instrumente de acțiune, prin intermediul accesului la baze de date și rețelele informatice, instrumente prin care poate influența în mod direct exercitarea puterii în plan intern sau internațional. Recurența revoluțiilor „facebook” sau „twitter” din Europa până în Orientul Mijlociu demonstrează impactul acestor instrumente virtuale asupra regimurilor politice, impact de neimaginat acum mai puțin de un deceniu.

Formele de evoluție a „puterii digitale” vor reprezenta, în egală măsură, oportunități de dezvoltare, dar și vulnerabilități și provocări la adresa securității, iar gestionarea acestora va fi determinată de capacitatea de accesare, decelare și utilizare a informației.

Se profilează, astfel, un nou front de acțiune al serviciilor de informații, care modifică responsabilitățile tradiționale, dar extinde și conceptele securității cu o dimensiune complet nouă, cea a securității cibernetice. Abundența și caracterul nestructurat al informațiilor specifice secolului XXI constituie în prezent o provocare cel puțin la fel de serioasă ca lipsa sau caracterul limitat al informațiilor disponibile în trecut. În acest context, capacitatea de a colecta, procesa, analiza și disemina informațiile este cu atât mai importantă pe termen mediu și lung, iar calitatea produsului de intelligence va fi fundamental determinată de abilitatea de integrare a informațiilor obținute din toate categoriile de surse, HUMINT, SIGINT, IMINT, OSINT etc., prin exploatarea progresului tehnologic ca multiplicator al eficienței sau liant al metodelor de acțiune clasice și moderne.

Cunoașterea este esențială în susținerea, în timp real, a procesului decizional pentru asigurarea competitivității statului și promovarea intereselor naționale. Capacitatea de a înțelege trecutul și prezentul și de a le evalua în profunzime semnificațiile și implicațiile este



fundamentală pentru anticiparea viitorului. Cunoașterea strategică este determinată de calitatea informației furnizate de serviciile specializate, iar aceasta este rodul unor activități susținute de planificare, colectare, analiză și diseminare care sunt influențate pe toate dimensiunile ciclului de intelligence de revoluția tehnologică.

Această Viziune Strategică își propune să identifice modul în care Serviciul Român de Informații trebuie să răspundă provocărilor contemporane determinate de era informațională și să-și consolideze performanța operațională și analitică prin utilizarea noilor instrumente cibernetice. Scopul său nu este de a genera o restructurare de amploare, ci de a direcționa viitoarele transformări ale Serviciului în direcția asimilării „puterii digitale” ca parametru indispensabil al muncii de informații.

Dezvoltarea profesiei de ofițer de intelligence este indisolubil conectată schimbărilor actuale care necesită integrarea instrumentelor informatice în activitatea curentă, comunicarea rapidă prin platforme de lucru colaborative, consolidarea cooperării între analiști și operativi, aplicarea unor noi standarde de performanță profesională. În acest context, dacă Viziunea 2007-2010 a fost în primul rând un document destinat transformării Serviciului, noua Viziune 2011-2015 se adresează transformării profesiei și se orientează cu precădere pe resursa umană, pe îmbunătățirea activității ofițerilor care servesc cu loialitate și dedicație această instituție.

Creșterea eficienței muncii de informații în societatea informațională depinde tot mai mult de credibilitatea și capacitatea noastră de a ne adapta unui prezent dinamic și unui viitor marcat de incertitudine. Suntem chemați să protejăm și să promovăm interesele cetățenilor, societății și statului român într-un mediu de securitate în care actorii și procesele s-au transformat în mod fundamental, în care puterea nu mai aparține entităților singulare, monadice, ci rețelelor, schimbului de informații, mobilizării civice și integrării suprastatale. Numai prin asimilarea, prin „internalizarea” acestor schimbări vom reuși să ne îndeplinim misiunea noastră fundamentală de cunoaștere, prevenire și contracarare a amenințărilor și să utilizăm ferestrele de oportunitate ale erei informaționale în susținerea intereselor naționale ale României în secolul XXI.

George – Cristian Maior

Viziune

Era informațională a indus schimbări profunde în evoluția riscurilor și în modul în care instituțiile statului trebuie să răspundă provocărilor și oportunităților create de revoluția tehnologică. Serviciile de informații trebuie să se adapteze acestor transformări ale mediului de securitate și să folosească în avantajul lor noile instrumente informaționale de acțiune pentru prevenirea și combaterea atât a riscurilor tradiționale de securitate, cât și a noilor amenințări cibernetice.

Noua concepție pornește de la premisa conform căreia cunoașterea reprezintă elementul central al dinamicii instituționale și competitivității necesare îndeplinirii misiunilor strategice ale Serviciului.

Accesul la informație este marcat de accentuarea competiției, în vreme ce utilizarea informației nu se poate realiza decât într-un mediu colaborativ, prin aplicarea principiului „need to share” ca fundament al accesului la cunoaștere. Succesele în era informațională vor fi potențate de modul în care această cunoaștere va fi construită și bazată pe cele mai relevante evoluții ale tehnologiilor avansate.

Creșterea performanței va consolida rolul Serviciului de autoritate națională în domeniile de responsabilitate, oferind oportunitatea poziționării sale ca principal furnizor de cunoaștere strategică în cadrul securității naționale.

Riscuri și oportunități în domeniul securității

Tendențele de evoluție ale securității naționale și internaționale pot fi reprezentate pe șase dimensiuni relevante.

O primă dimensiune a securității se manifestă în zona suveranității naționale și capacității de guvernare a statului în contextul evoluțiilor tehnologice specifice erei informaționale. Anvergura fenomenului de globalizare, consolidarea influențelor actorilor non-statali și evoluțiile accelerate ale inovării tehnologice, pe fondul accesului tot mai facil al tuturor categoriilor de utilizatori - state, entități non-statale sau indivizi - la produsele tehnologiei de vârf, constituie principalele repere ale dinamicii contextului de securitate actual. Diminuarea controlului statului asupra piețelor comerciale și ale muncii și competiția pentru acces la materii prime și resurse energetice se vor accentua în următorii ani. De aceea, va crește relevanța dimensiunii economice a securității pe fondul globalizării și al efectelor pe termen mediu și lung ale crizei financiare. Conflictele vor fi preponderent asimetrice și se vor desfășura nu numai în teatrele clasice de operațiuni, ci și în spații noi precum spațiul cosmic și mediul cibernetic. În această dimensiune, preocuparea pentru acces la tehnologii duale a actorilor statali și non-statali va cunoaște o continuă amplificare.

O altă dimensiune a securității va fi cea demografică, marcată de disparitățile dintre explozia demografică în statele sărace sau în curs de dezvoltare și fenomenul de îmbătrânire a populației din statele dezvoltate, cu efecte asupra fenomenelor migrației și exportului de insecuritate din diferite zone ale globului. Riscurile ecologice reprezintă o dimensiune din ce în ce mai prezentă pe agenda de securitate a statelor. Creșterea consumului și dezechilibrele în accesul la resurse, catastrofele naturale și schimbările climatice generează consecințe majore asupra vieții cetățenilor și funcționării societăților.

Dimensiunea științifică și tehnologică a securității este marcată de evoluții diverse, de la dezvoltarea nanotehnologiei și biotehnologiei, la robotica avansată sau energiile regenerabile. Viteza acestor evoluții reprezintă deopotrivă sursa și forța motrice a oportunităților de dezvoltare a societății informaționale bazate pe cunoaștere, dar și a unor provocări, riscuri și amenințări la adresa securității.

Accesul facil la aproape orice fel de date, volumul și viteza de propagare a informației, dar și rata ridicată de perisabilitate a acesteia au devenit realități ale lumii în care trăim. Odată cu liberalizarea fluxurilor de informații și comunicare, cunoașterea nu mai este generată de posesia informației, ci de utilizarea, diseminarea și împărtășirea acesteia, de configurarea unor canale de comunicare adecvate, de exploatarea interconectării la nivel de rețele în susținerea intereselor proprii.

Generalizarea utilizării inovării ca bază a evoluției societății, schimbarea cutumelor de difuzare a informației de la canale restrânse, ierarhice, pentru decizii puternic centralizate, la flexibilizarea și aplatizarea ierarhiilor, transformarea modurilor tradiționale de producție în întreprinderi și corporații virtuale capabile să reacționeze rapid la dinamica pieței și includerea efectivă a informației printre factorii de producție sunt repere relevante ce modifică substanțial perspectiva evoluțiilor economico-sociale contemporane.

În egală măsură, creșterea dependenței societății de tehnologie, în general, și de infrastructura și sistemele informatice și de comunicații, în particular, sporește vulnerabilitatea utilizatorilor în fața oricăror amenințări la adresa acestora. Atenția nu trebuie concentrată doar asupra noilor amenințări, ci și asupra modului în care acestea influențează riscurile și amenințările tradiționale (terorismul, spionajul, criminalitatea organizată, extremismul etc.) la adresa valorilor și intereselor de securitate ale României.

Impactul noilor tehnologii asupra misiunilor Serviciului Român de Informații

Includerea celor mai noi produse și tehnologii informatice în procesele specifice ale activității de intelligence reprezintă o prioritate a Serviciului pentru perioada următoare, nu ca scop în sine, ci ca instrument care să contribuie la realizarea misiunilor sale fundamentale:

Cunoașterea - extinderea riscurilor și disimularea acestora în forme de manifestare din ce în ce mai versatile, inclusiv informatice, solicită instrumente noi de identificare și înțelegere. Anticiparea dinamicii riscurilor, vulnerabilităților și amenințărilor presupune specializare și dezvoltare de capacități care să permită abordări adecvate naturii acestora și necesităților de fundamentare a deciziilor în domeniul securității naționale.

Prevenirea - spectrul de măsuri pentru limitarea manifestării riscurilor și amenințărilor la adresa securității naționale se multiplică atât intensiv prin utilizarea mijloacelor informatice în domeniile de acțiune clasice ale Serviciului, cât și extensiv, prin formularea răspunsului la noile amenințări cibernetice.

Protecția - securitatea cetățenilor români, a societății în ansamblu și a statului trebuie asigurată, în egală măsură, în spațiul fizic și virtual. Provocările sunt determinate de arhitectura celor două spații și de granița difuză dintre acestea, cu impact asupra responsabilităților instituțiilor statului. Întrepătrunderea dintre dimensiunile multiple ale securității necesită o analiză extinsă asupra valorilor naționale și modului în care vor trebui acestea protejate inclusiv în plan virtual.

Contracararea - sporirea și diversificarea gamei de operațiuni ostile care vizează sau utilizează noile tehnologii vor determina extinderea măsurilor de contracarare și creșterea gradului de intruziune a acestora în mediul virtual. În acest sens, vor fi necesare noi modele de răspuns integrat, individual sau în cadrul cooperării internaționale, precum și adoptarea unor principii de aplicare a proporționalității măsurilor de ripostă în mediul cibernetic.

Promovarea – identificarea și susținerea oportunităților de realizare a intereselor naționale și de afirmare a valorilor de securitate trebuie realizate prin valorificarea instrumentelor specifice erei informaționale. Noile resurse tehnologice trebuie orientate în sensul susținerii modalităților de lucru colaborativ și valorificării ferestrelor de oportunitate acționale și decizionale.

Prioritățile SRI pentru gestionarea provocărilor erei informaționale

Viziunea strategică „SRI în era informațională” se plasează pe o linie de continuitate cu demersurile de transformare instituțională inițiate în 2007. Documentul se adresează întregului spectru de domenii și activități ale Serviciului, cu accent pe schimbările determinate de era informațională asupra ciclului de intelligence, și urmărește trasarea direcțiilor majore de acțiune pentru consolidarea și extinderea proceselor și instrumentelor activității de intelligence în baza „**Viziunii Strategice 2007-2010**”.

Racordarea activității Serviciului la evoluțiile tehnologice este condiționată direct de prioritizarea alocării resurselor umane, materiale și financiare pe domenii și proiecte de interes. Integrarea noilor tehnologii trebuie să fie în strictă corelare cu nevoile instituționale în gestionarea riscurilor și oportunităților mediului actual de securitate. În egală măsură, noile tehnologii trebuie valorificate pentru îndeplinirea responsabilităților SRI de coordonator, contributor sau beneficiar în cadrul programelor naționale derulate sub egida Comunității Naționale de Informații, precum Sistemul Informatic Integrat, OSINT, CYBERINT, GEOINT sau IMINT.

Prioritățile activității Serviciului în perioada de referință a prezentei Viziuni sunt subsumate unor obiective strategice a căror realizare va asigura premisele adaptării în timp real la provocările și oportunitățile erei informaționale:

1. Capacitatea operațională în culegerea și valorificarea informațiilor

Dezvoltarea capabilităților de intelligence – prin utilizarea tuturor resurselor tehnologice disponibile – pentru asigurarea cunoașterii anticipative a evoluției riscurilor și integrarea informațiilor din surse multiple în produse informaționale relevante și oportune.

2. Tehnologia ca avantaj competitiv în intelligence

Realizarea unei infrastructuri integrate de comunicații și tehnologia informației și asigurarea instrumentelor tehnologice necesare pentru creșterea performanței activității pe toate componentele ciclului de intelligence și domeniile de activitate ale SRI.

3. Noi perspective asupra serviciilor de securitate

Integrarea celor mai moderne tehnologii, consolidarea metodelor de expertizare și îmbunătățirea determinărilor tehnico-științifice pentru asigurarea sprijinului acordat altor instituții naționale și internaționale.

4. Investiția în resursa umană

Adaptarea sistemului de management al resurselor umane la provocările și oportunitățile erei informaționale prin aplicarea unor criterii eficiente de performanță profesională și susținerea carierei și motivației individului în cadrul Serviciului.

5. Tehnologia ca facilitator al cooperării

Extinderea cunoașterii și anticipării evoluțiilor mediului de securitate și gestionarea în cooperare a riscurilor și amenințărilor la adresa intereselor naționale și a celor euro-atlantice.

6. Cercetarea științifică și dezvoltarea tehnologică

Asigurarea nivelurilor de cunoaștere și inovare necesare creșterii performanței activității de intelligence în cadrul unui sistem unitar de cercetare-dezvoltare.

7. Securitatea instituțională

Consolidarea sistemului integrat de protecție, incluzând componentele de securitate a personalului, fizică, procedurală, a operațiunilor și a legăturilor operative, prin utilizarea facilităților oferite de noile tehnologii.

8. Comunicarea publică în era informațională

Proiectarea unei imagini corecte a Serviciului și extinderea actului de comunicare prin promovarea rolului instituției în gestionarea problematicilor de securitate specifice erei informaționale.

Viitorul

Era informațională reprezintă debutul unei schimbări fundamentale a modului de gândire și acțiune la nivel statal, o revoluție a cunoașterii care influențează toate formele de manifestare a individului și societăților contemporane. Așa cum forțele armate au adoptat modelul operațiunilor de rețea (Network Centric), așa cum diplomația clasică se pliază în prezent pe noi abordări și relații cu actori non-statali relevanți, pe susținerea intereselor naționale prin investiția în educație și asistență de securitate, tot astfel domeniul intelligence va trebui să se adapteze transformărilor actuale printr-o dublă abordare:

1. Adaptarea proceselor și procedurilor la necesitatea reacției rapide și cunoașterii extinse prin noi modalități de acțiune și decizie în operațiuni și prin consolidarea capacităților analitice
2. Investiția în tehnologie ca resursă de modelare a sistemului instituțional și factor de multiplicare a puterii în plan informațional

Asemenea evoluții presupun descentralizarea și flexibilizarea deciziei operaționale, integrarea surselor în formularea unor scenarii de evoluție a riscurilor, dezvoltarea diplomației de intelligence și investiția consecventă în educație și cercetare, în formarea continuă a personalului propriu.

Tehnologia informației reprezintă o resursă fundamentală și un instrument inevitabil în creșterea eficienței și vitezei de reacție a Serviciului, a adecvării răspunsului la riscuri și amenințări complexe și a calității informării și analizei în susținerea deciziilor strategice ale statului. Interdependențele globale accentuează necesitatea dezvoltării cooperării externe care se va adânci în viitor, în contextul consolidării bazelor de date transnaționale, al extinderii schimburilor de informații și operațiunilor cu servicii din alte state, precum și în cadrul cooperării europene și euroatlantice.

Implementarea concepției strategice „SRI în era informațională” va asigura configurarea unor capacități informative și operaționale puternice și flexibile, care să permită îndeplinirea cu eficiență a misiunilor fundamentale ale Serviciului.