SPĂLAREA BANILOR ŞI FINANȚAREA TERORISMULUI VERSUS MANAGEMENTUL ŞI PROTECȚIA INFRASTRUCTURILOR CRITICE

MONEY LAUNDERING AND FINANCING TERRORISM VERSUS THE MANAGEMENT AND PROTECTION OF CRITICAL INFRASTRUCTURES

Mircea Constantin SCHEAU*

Este analizat impactul Spălării Banilor şi al Finanțării Terorismului în contextul Managementului şi Protecției Infrastructurilor Critice Naționale şi Internaționale. Modalitățile globale de abordare a fenomentului, raportarea la măsurile comune şi particularizarea acestora în funcție de realitățile socio-economice ale fiecărei comunități. Poziționarea instituțiilor financiar-bancare în adoptarea măsurilor imediate şi pe termen lung. Metode şi Fluxuri de prevenire şi contracarare urmate de un exemplu concret.

Cuvinte-cheie: *bani; terorism; metode; reglementări.*

The impact of Money Laundering and Financing Terrorism is analyzed in the context of Management and Protection of National and International Critical Infrastructures. Global ways of approaching the phenomenon, reporting to common measures and their particularization according to the social-economical realities of each community. The positioning of the financial- banking institutions to adopt immediate and long term measures. Methods and Flows to prevent and counteract followed by a practical example.

Keywords: *moneys; terrorism; methods; regulations.*

* Manager Regional Vânzări – Regiunea de Sud, B.C.R. S.A.; e-mail:mirceaconstantin.scheau@bcr.ro

Introducere

Spălarea banilor şi Finanţarea terorismului nu este un subiect nou. Aş putea spune că rădăcinile se regăsesc adânc în istorie. Metodele se constituie într-un segment de reguli dintre cele mai atipice dată fiind evoluţia şi adaptarea lor în funcţie de luptă de apărare şi/sau atac ce se dorea a fi iniţiată/desfăşurată/susţinută. Este dificil să le numim reguli. Poate singura regulă unanim recunoscută era şi este şi acum „Fără reguli". Tot ceea ce nu se încadrează într-un tipar apriori stabilit poate fi considerat la un moment dat terorism. Societatea modernă a impus ajustarea strategiilor de depistare şi combatere a spălării banilor şi finanţării terorismului. De aceea am ales această temă ca şi punct de pornire a unei analize ulterioare mai detaliate.

Repere şi caracteristici

Ca şi prim pas încercăm să caracterizăm Infrastructurile Critice Naţionale şi Europene şi să precizăm care sunt reperele fundamentale ale acestora. De aceea, subliniem că modalităţile de abordare a protecţiei infrastructurilor critice diferă de la o ţară la alta, de la o organizaţie la alta, însă se pot identifica elemente comune, măsuri întreprinse până în prezent, funcţii şi responsabilităţi compatibile. În literatura de specialitate, sunt unanim acceptate două axiome în analiza acestui domeniu:

- în mod practic, este imposibil să se asigure protecţia integrală a unei infrastructuri critice;
- nu există o soluţie unică, universală pentru rezolvarea acestei probleme.

Specialiştii oferă următoarele moduri de abordare a protecţiei infrastructurilor critice:

- protecţia infrastructurilor critice din plan economico-social, în cadrul căruia este necesară o abordare sistemică/integrată a tuturor punctelor/nodurilor vulnerabile, pe suportul unor hărţi de risc, şi conexiunilor acestora;
- protecţia infrastructurilor critice informaţionale, care ia în considerare numai securitatea conexiunilor IT şi soluţiile de protejare a acestora, competenţele protecţiei fizice a celorlalte infrastructuri fiind disipate între diverse organisme de stat sau private;
- asigurarea funcţionării neîntrerupte a reţelelor IT şi a elementelor fizice ale infrastructurilor critice. În acest caz, protecţia fizică reprezintă o componentă a sistemului naţional de protecţie civilă. În prezent, se încearcă o cooperare cât mai strânsă între sectorul public şi cel privat pentru atingerea unui grad cât mai înalt de protecţie a infrastructurilor critice. La nivel de planificare strategică însă, cooperarea este aproape inexistentă. Acest tip de abordare a fost denumită generic „all hazards approach" (abordarea tuturor riscurilor);

- realizarea unui sistem minim obligatoriu de protecţie a sistemului de guvernare şi a anumitor organisme statale, vitale. Acest mod de tratare este mult mai puţin răspândit, ia în considerare numai protecţia sistemului de guvernare şi protecţia anumitor organisme statale. În opinia specialiştilor, protecţia infrastructurilor critice este un atribut atât al structurilor militare, al instituţiilor civile şi, nu în ultimul rând, al sectorului privat, în calitate de principal beneficiar al serviciilor deservite de infrastructuri critice. Cadrul legal actual din România nu prevede competenţe pentru structurile militare în domeniul protecţiei infrastructurilor critice. În noul pachet de legi ale securităţii sunt încercări de a oferi competenţe în domeniu Serviciului Român de Informaţii. Abordarea studiului protecţiei infrastructurilor critice este foarte complexă, din cauza relaţiilor de interdependenţă şi dinamicii acestora. O variantă de tratare a problematicii ar putea cuprinde şapte etape: analiza de sector, analiza interdependenţelor, analiza de risc, analiza ameninţărilor, analiza vulnerabilităţilor, analiza consecinţelor şi analiza sistemului.

În ţara noastră, problematica infrastructurii critice a devenit subiect de amplă dezbatere în ultimii ani – în contextul admiterii în NATO şi UE şi al adeziunii României la strategia partenerilor euroatlantici de prevenire şi combatere a terorismului internaţional – contrar, însă, realităţilor naţionale, determinate de situaţiile cu grad ridicat de criticitate, produse, mai ales în ultimii doi ani, ca efect al manifestării unor fenomene meteorologice extreme, de altfel previzibile în contextul evoluţiei procesului de încălzire globală şi mutaţiilor climaterice produse. Până în prezent, însă, nu a fost formulată o definiţie unanim acceptată. Mai mult, disputele frecvente pe marginea acestei probleme sunt legate de stabilirea diferenţei specifice a noţiunilor „infrastructură strategică” şi „infrastructură critică”.

Privind protecţia infrastructurilor critice în Uniunea Europeană putem spune că întregul spaţiu euroatlantic şi-a redimensionat politica şi strategia cu

privire la securizarea infrastructurilor critice. Problematica infrastructurilor critice se află în atenţia autorităţilor europene. Infrastructurile critice sunt, potrivit unei definiţii europene, „instalaţiile fizice şi tehnologice ale informaţiei, reţelele, serviciile şi activele care, în caz de oprire sau de distrugere, pot să producă incidente grave asupra sănătăţii, securităţii sau bunăstării economice a cetăţenilor sau activităţilor guvernelor statelor membre”.

Atentatele de la 11 septembrie 2001 au avut un impact considerabil, nu doar în Statele Unite, ci asupra întregului context de securitate pe plan internaţional. Modul de concepere a relaţiilor internaţionale, paradigma de securitate, percepţia riscurilor şi definirea metodelor de prevenire şi combatere a acestora s-au modificat fundamental. Se poate vorbi de o epoca “post-11 septembrie”. Atentatele de la 11 septembrie nu au constituit un eveniment singular şi izolat, ele reprezentând din păcate doar începutul unei serii de acte teroriste de amploare (Madrid, Londra, Sharm el Sheikh). Rezultatul este că, în prezent, ne aflăm într-un „război împotriva terorii”, cu atât mai dificil şi mai complex cu cât este unul neconvenţional.

- Ce este terorismul?
- Cine finanţează actele de terorism?
- Care este circuitul fondurilor utilizate de către grupările teroriste?

Iată câteva dintre întrebările la care specialişti din întreaga lume încearcă să ofere un răspuns. Este dificil de clasificat dar cu siguranţă se pot prezenta câteva elemente definitorii:

- este un act de violenţă;
- are un scop sau o motivaţie politico-ideologică;
- ţintele vizate sunt membri ai populaţiei civile;
- caută să intimideze o audienţă, mizând pe crearea terorii în rândul acesteia.

Sursele de finanţare a terorismului includ:

- State-sponsori ai terorismului: sprijinul financiar acordat de către state sau organizaţii cu o infrastructură suficient de mare să colecteze şi să facă disponibile fondurile către organizaţia teroristă;
- Surse legitime (licite): organizaţii caritabile, afaceri legitime utilizate drept acoperire;
- Surse criminale (ilicite): afaceri ce implică droguri, răpiri, lanţuri de prostituţie, fraude cu carduri de credit etc.

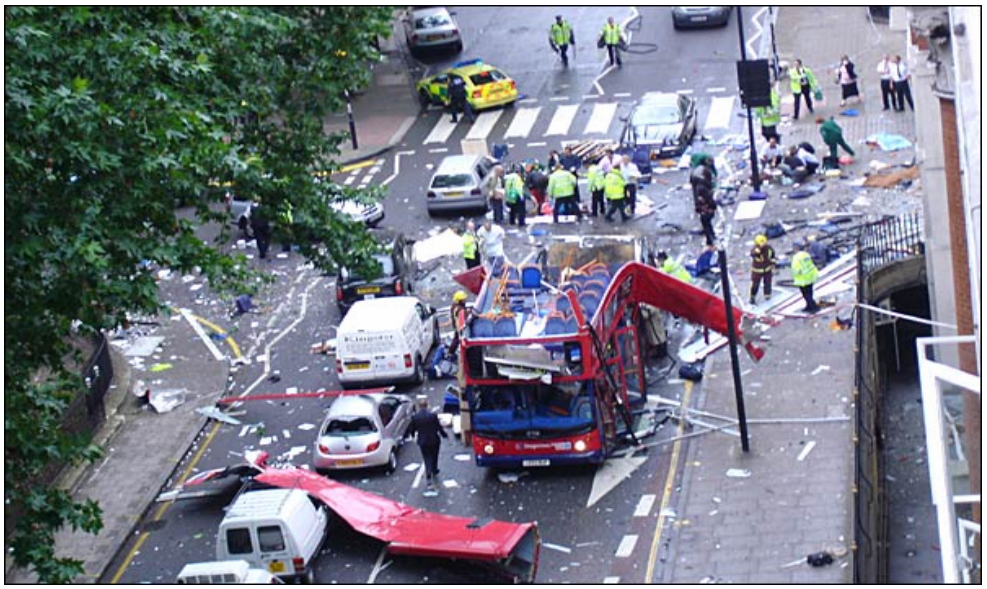
Cum realizează grupurile teroriste circuitul banilor?

- Prin intermediul formal al sistemului bancar.

Tot mai multe instituţii bancare iau o atitudine preventivă şi completează din ce în ce mai multe Rapoarte de Tranzacţii Suspecte (RTS) cu privire la ceea ce se consideră a fi „activitate suspectă” referitoare la clienţi.

- Prin canale non-formale care implică transferuri prin intermediul sistemului „hawala”. Acest sistem este utilizat în aproape tot Orientul Mijlociu de multă vreme şi se bazează pe încredere, precum şi pe asigurarea anonimatului, deoarece toate operaţiunile nu se realizează pe hârtie. Utilizatorii unui astfel de sistem transmit banii peste graniţe fără a-i transfera în mod fizic. În fapt, principala caracteristică a Hawala este „compensarea”, deoarece persoanele implicate sunt asigurate că în contul respectiv se vor depune bani (sau în alte cazuri, se transmit bunuri) ce vor fi returnaţi printr-o tranzacţie reversibilă viitoare.
- Prin folosirea sistemelor electronice de plăţi (e-cash, smart – carduri, etc.).
- Prin contrabanda cu numerar (prin curieri sau prin încărcături cu numerar).

Ulterior atacurilor cu bombe din Londra din 7 iulie 2005 au fost reconsiderate aspectele cu privire la finanţarea terorismului, oferindu-se o nouă viziune asupra finanţării terorismului. Cele patru explozii au fost comise de către persoane cu cetăţenie britanică crescuţi şi educaţi în Marea Britanie, spre deosebire de Madrid şi New York, cazuri în care teroriştii erau de origine arabă. În plus, costurile exploziilor din Londra s-au ridicat până la suma de 2.000 USD spre deosebire de atacurile din Statele Unite a căror finanţare a fost de cca. 500.000 USD. Recentele investigaţii arată faptul că multe atacuri sunt finanţate în prezent cu sume mici.



S-a dedus faptul ca în foarte multe cazuri sursele de finanţare a actelor de terorism provin din afaceri legitime şi instituţii de tip non-guvernamental şi prin intermediul acţiunilor caritabile. Grupurile teroriste combină adesea fondurile obţinute din surse legitime cu cele din surse ilicite. Încercând să construim relaţia dintre spălarea banilor şi finanţarea terorismului s-a concluzionat de către organismele internaţionale ca finanţarea terorismului este diferită faţă de clasica spălare a banilor:

- În cazul spălării banilor, veniturile activităţilor ilicite sunt spălate sau stratificate prin mijloace care le fac să pară legale, iar scopul final este, de obicei, câştigarea unor cantităţi mai mari de bani. Prin finanţarea terorismului, sursa de fonduri sau de finanţare este adesea „legitimă", iar scopul final nu este în mod obligatoriu atragerea de mai multe fonduri, ci mai degrabă atingerea obiectivelor vizate de către gruparea teroristă. De aceea, primul pas care trebuie făcut în combaterea spălării banilor şi a finanţării terorismului este impus de cunoaşterea metodelor şi identificarea potenţialelor surse.

Clasificare şi concept

Strategia ulterioară va ţine cont de anumite particularităţi de implementare şi ea începe cu prezentarea premiselor, a căilor de construcţie şi a priorităţilor şi se dezvoltă apoi în jurul identităţii europene şi euro-atlantice a României, a securităţii interne pentru a se încheia cu evidenţierea rolului şi a responsabilităţilor pe care diverşi actori îl au în construcţia şi asigurarea securităţii naţionale. Apreciabilă ca

întindere, strategia se consideră a fi „un proiect naţional realist, îndrăzneţ şi pragmatic" care răspunde nevoii şi obligaţiei de protecţie a drepturilor şi libertăţilor fundamentale ale omului, valorilor şi intereselor naţionale vitale ca baze ale existenţei statului român. Este evidenţiată poziţia favorabilă a României conferită de calitatea de membru NATO şi al UE vis-à-vis de accelerarea dezvoltării economice şi sociale şi de contribuţia la menţinerea securităţii regionale şi globale. Pentru realizarea analizei comparative a strategiilor de securitate naţională a României, în contextul Strategiei Europene de Securitate, s-au fixat ca unităţi de cercetare sursele care au contribuit la generarea strategiilor respective, evoluţia în timp a strategiilor, structura documentelor care constituie documentele oficiale, elementele de conţinut ale strategiilor (cu focalizare pe câţiva factori cheie: valori şi interese, mediul de securitate cu ameninţări, riscuri, provocări la adresa securităţii naţionale, obiective al securităţii, căi de implementare a strategiei de securitate, strategii sectoriale, sisteme şi actori de securitate).

Prin analogie cu cele trei niveluri de analiză utilizate în relaţiile internaţionale – individual, statal (intern, naţional) şi sistemic (internaţional, global), am recurs la analizarea Strategiei de Securitate Naţională a României şi plasarea ei în contextul mediului regional de securitate din prisma ultimelor două niveluri. În relaţiile internaţionale, primul nivel de analiză caută explicaţiile evenimentelor internaţionale pornind de la indivizi, în al doilea nivel de analiză explicaţia este orientată în direcţia inside out, în sensul că structura şi procesele politice, economice şi sociale din interiorul statelor constituie cauza proceselor şi evenimentelor internaţionale, în timp ce la nivelul trei este acceptată o cauzalitate inversă, de tip out inside, sistemul internaţional fiind considerat drept cauza care determină comportamentul statelor, state care „nu acţionează ci reacţionează", după cum opina şi Kenneth N. Waltz în cartea sa „Omul, statul şi războiul".

Am căutat aşadar să identificăm cauzalităţile şi determinismele care provin din mediul şi evenimentele internaţionale (ca exemple: tendinţa de revenire la bi- sau chiar multipolaritate; competiţia între puteri în spaţiul euro-atlantic pentru redistribuirea rolurilor; adâncirea integrării în UE; dezvoltările recente din spaţiul Federaţiei Ruse; influenţa NATO, ONU, OSCE, etc.) şi care au generat construcţia actualei Strategii de Securitate a României (nivelul trei de analiză sau modul cum „reacţionează" România la stimulii mediului regional şi internaţional de securitate), dar si invers, adică să analizăm la ce influente şi efecte conduce Strategia de Securitate Naţională în plan geopolitic, ce aduce nou în relaţiile cu vecinii şi în evoluţia stabilităţii şi securităţii regionale.

„Spălarea banilor nu este nimic nou. Este la fel de veche precum este nevoia de a ascunde bogăţia cuiva de ochii prădători şi de mâini invidioase. Bineînţeles, spălătorii moderni de bani vor adopta tehnici mai sofisticate decât transportatorii de

bijuterii din India sau decât Cavalerii Templieri, dar *modus operandi* esenţial va fi acelaşi!" – Rider, 1993.

UE poate fi privită ca structura care a apărut în virtutea unui proces de integrare bazat pe tratate şi organizare internaţională şi ca o construcţie pe 3 piloni – unul integrativ şi doi interguvernamentali. În viziunea Curţii de Justiţie de la Luxemburg, UE este o organizaţie autonomă specifică ce cuprinde caracteristicile unei organizaţii internaţionale, dar depăşeşte structura organizatorică şi funcţională a acesteia. Forma actualizată a evoluţiei construcţiei comunitare, a fost începută în 1952, cu CECO, urmată în 1958 de CEE şi CEEA (EURATOM). Tratatul de la Maastricht (1992) a formulat conceptul de UE formată din cele 3 segmente: CE (CECO, CEE, CEEA) – la Maastricht nu era încă acceptată noţiunea de UE, UE – integrare politica si CE - integrare economica. Un segment este complet realizat UE fiind o uniune economică, care cuprinde o uniune vamală, are politici comune, are un federalism politic, o coordonare şi o uniune monetară (1999). Nu funcţionează însă legea preţului unic: în Germania plata/ora este aproximativ 26,6 euro, în Portugalia 5,1 euro, în Grecia 6 euro (acum probabil că este mai puţin). În context mondial, UE, SUA, Japonia s-au constituit într-o triadă de superputeri economice ceea ce a condus la naşterea unui nou concept al procesului de triadizare.

Construirea UE nu este privită cu simpatie de restul lumii care se opune. Procesele integrative de construire a blocurilor nu sunt o formulă de stabilitate şi de pace, ci poate chiar una dintre bazele războaielor economice. Dimensiunea protecţionistă a UE este reglată printr-un mecanism aproape natural, „de piaţă", în interferenţă cu celelalte organizaţii regionale, pe o scenă comună: OMC (fost GATT). Situată ca nivel al protecţiei practicate în apropierea SUA, dar peste nivelul Japoniei, UE se caracterizează printr-un nivel ridicat de protecţie comercială. Specialiştii vest-europeni nu sunt de acord cu aprecierile unora dintre partenerii lor comerciali, care se temeau că, după crearea pieţei interne unice, Comunitatea se va transforma într-o „fortăreaţă" comercială. Ei consideră că nivelul protecţiei comerciale practicate în prezent de UE este comparabil cu cel al

principalilor săi parteneri din ţările dezvoltate şi, în primul rând, SUA. Ca şi concluzie, UE este o grupare comercială şi politică, cel puţin deocamdată. Politica ei comercială este o formulă specială de multilateralism având acorduri cu fostele ţări AELS, ţările PECO şi acorduri cu ţări din America Latină.

Are, de asemenea, semnate acordurile MED, acordurile ACP şi convenţia de la Lomé, precum şi reglementările privind spaţiul transatlantic

Aceste acorduri sunt expresia noii diplomaţii comerciale a UE (UE a început să devină centrul sistemului comercial mondial şi încheie acorduri de la grupare la grupare).

Devenirea UE ca stat/putere politica este o problemă de viitor. În noul context creat s-a impus adoptarea unor măsuri comune care să preîntâmpine şi să răspundă agresiunilor economice infracţionale de spălare a banilor. S-a stabilit cadrul legislativ şi au fost constituite organismele care să pună în aplicare rezoluţiile stabilite prin standardele internaţionale: CDD, Comitetul de la Basel pentru supraveghere bancară, Grupul WOLFSBERG. Romania respectă toate aceste reglementări şi s-a aliniat politicii internaţionale în vederea prevenirii şi combaterii spălării banilor. Abordarea concretă a necesitat impunerea unei strategii bancare de recunoaştere a clientelei ce poate fi detaliată în câţiva paşi:

- Comportamentul clientului;
- Cerintele de raportare si de pastrare a inregistrarilor
- Spălarea banilor prin intermediul tranzacţiilor în numerar;
- Spălarea banilor folosind conturi bancare;
- Spălarea banilor folosind transferuri electronice bancare;
- Spălarea banilor folosind operaţiunile externe;
- Spălarea banilor prin intermediul operaţiunilor de credit;
- Spălarea banilor folosind tranzacţii legate de investiţii;
- Spălarea banilor folosind documentaţia de credit şi garanţii.

Spre deosebire de politica de securitate naţională care trebuie să ţină cont atât de planurile NATO, cât şi de noul bloc european ce-şi afirmă identitatea, politica monetară şi mai exact cea bancară se deosebeşte doar prin prisma caracteristicilor locale şi nu prin prisma celor globale.

Activitatea de informaţii cuprinde ansamblul acţiunilor şi operaţiunilor desfăşurate permanent de către componentele abilitate ale sistemului securităţii naţionale, pentru planificarea, căutarea, obţinerea, verificarea, prelucrarea analitică a datelor şi informaţiilor cu relevanţa în domeniu şi informarea factorilor de decizie, investiţi legal cu competenţa de realizare a securităţii infrastructurilor critice ori de aplicare a legii în domeniu. Scopul şi obiectul activităţii de informaţii, în acest caz, îl reprezintă cunoaşterea, anticiparea, prevenirea şi contracararea ameninţărilor la adresa „infrastructurilor critice". Aceasta este reglementată prin norme specifice, emise în baza şi pentru aplicarea legii şi se desfăşoară în secret, cu asigurarea protecţiei surselor, mijloacelor, metodelor şi tehnicilor utilizate. Informaţiile cu relevanţa pentru securitatea „infrastructurilor critice" se obţin prin valorificarea tuturor resurselor informaţionale existente, precum şi prin surse, mijloace şi metode specifice, create şi folosite sub autoritatea legii şi în conformitate cu imperativul protejării lor de orice fel de intruziuni ilegale. Complexitatea şi diversitatea „infrastructurilor critice", influenţa mediului de securitate, intern şi internaţional, marcat de provocări şi fenomene adeseori imprevizibile la adresa securităţii naţionale, regionale şi internaţionale impun desfăşurarea unei activităţi de informaţii cu un profund şi cuprinzător caracter anticipativ-preventiv. Nevoia de cunoaştere a situaţiei operative specifice „infrastructurilor critice" obligă factorii legal abilitaţi să constituie, să dezvolte şi adapteze capacităţi informative naţionale adecvate, să identifice răspunsuri şi soluţii viabile, necesare asigurării securităţii acestora, în consonanţă cu nevoile de securitate naţională şi ale aliaţilor. Activitatea de cunoaştere trebuie să permită identificarea disfuncţiilor şi vulnerabilităţilor, să estimeze riscurile, ameninţările şi tendinţele de evoluţie a fenomenelor perturbatoare la adresa infrastructurilor critice, să asigure controlul vectorilor şi mediilor de proliferare a crimei organizate, terorismului şi războiului informaţional, împotriva valorilor, intereselor şi/sau necesităţilor naţionale exprimate de acestea. Activitatea de informaţii pentru securitate presupune şi impune o legătură permanentă, pe de o parte, între factorii implicaţi în culegerea informaţiilor şi realizarea produselor informaţionale şi, pe de altă parte, cu beneficiarul sau utilizatorul acestora în cadrul sistemului de informare/raportare instituit potrivit legii. Priorităţile de informaţii se stabilesc în funcţie de valorile, interesele şi necesităţile de securitate şi apărare, protejate şi promovate, de caracteristicile mediului de securitate intern şi internaţional, de natura factorilor de risc şi ameninţărilor, de comenzile de informaţii ale

beneficiarilor (utilizatorilor) legal abilitaţi, precum şi de resursele informaţionale disponibile sau care trebuie create. Analiza şi stabilirea priorităţilor de informaţii are în vedere diagnoza situaţiei operative, zonele de interes informativ, sursele de ameninţări în dinamica contextului geopolitic şi geostrategic, vulnerabilitatile, factorii de risc şi ameninţările exprimate prin intenţii, planuri, acţiuni care au ca scop: spionajul, sabotajul, subminarea economică sau politică a statului, democraţiei, ordinii constituţionale, subversiunea, periclitarea valorilor supreme garantate constiţutional, terorismul, criminalitatea organizată, periclitarea infrastructurilor informatice, agresiunile asupra sistemelor critice (transport, energie, comunicaţii, sisteme vitale pentru viaţă etc.) şi agresiunile asupra sistemului de comandă şi control al actului de decizie pentru securitate.

Anticiparea riscurilor, existente sau prognozabile, la adresa „infrastructurilor critice" şi a factorilor perturbatori, determină serviciile de informaţii, legal abilitate, să desfăşoare activitate preponderent preventivă, care să reducă, să înlăture şi să contracareze acţiunile surselor generatoare de riscuri, să creeze structuri şi să formeze personal specializat în acest sens. Prin capacitatea de cunoaştere, anticipare, prevenire şi contracarare a ameninţărilor la adresa „infrastructurilor critice", informaţia de securitate îşi întăreşte valoarea socială, pe care statul român o integrează patrimoniului său strategic şi o protejează, conform normelor legale şi reglementărilor internaţionale. În domeniul cunoaşterii disfuncţiilor, vulnerabilităţilor, factorilor de risc, ameninţărilor şi stărilor de pericol ce vizează „infrastructurile critice" şi, pe cale de consecinţă, starea de securitate naţională, un rol fundamental revine activităţii de căutare şi obţinere a informaţiilor relevante şi transmiterii/comunicării acestora factorilor legal abilitaţi să ia decizii de prevenire şi contracarare. Acest obiectiv se poate îndeplini dacă între structurile de informaţii legal constituite, instituţiile statului de drept, autorităţile publice, organizaţiile neguvernamentale, comunităţi şi cetăţeni există comunicare permanentă, în baza unui suport legal corespunzător, a unei responsabilităţi concrete, în raport de competenţe şi a unui control parlamentar eficient. Structurile de informaţii specializate au atribuţii legale pe linia căutarii, identificării, obţinerii şi furnizării de date şi informaţii exacte şi oportune despre vulnerabilităţi, factori de risc, ameninţări şi pericole la adresa „infrastructurilor critice" şi comunicarea lor factorilor abilitaţi în vederea luării deciziilor ce se impun.

În acest sens, ele sunt obligate:

- să-şi stabilească necesităţile operative, adapteze permanent dispozitivele şi modul de acţiune, în vederea identificării oportunităţilor şi ameninţărilor la adresa „infrastructurilor critice”;

- să formuleze propuneri de măsuri adecvate pentru cunoaşterea, prevenirea şi contracararea factorilor de risc şi ameninţărilor, sprijinind, în limitele prevăzute de lege, procesul de luare a deciziilor;

- să asigure un management eficient al resurselor informaţionale, îmbunătăţind cooperarea, conlucrarea şi colaborarea cu instituţiile din sistemul securităţii naţionale şi cu cele ale partenerilor externi;

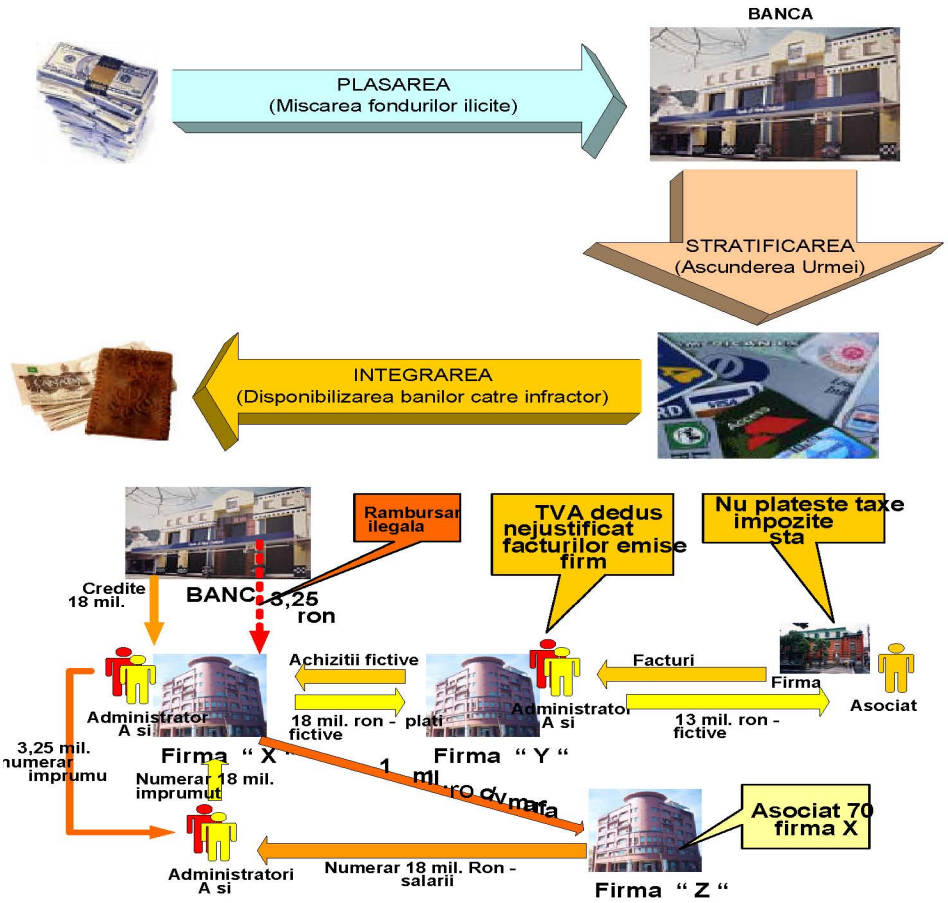
- să elaboreze evaluări şi analize complexe asupra stării de securitate a „infrastructurilor critice”, care să permită identificarea şi sesizarea ameninţărilor potenţiale asupra acestora, caracteristicile mediului de securitate, şi să propună măsuri adecvate pentru protejarea obiectivelor, valorilor fundamentale şi intereselor naţionale împotriva oricăror acţiuni ilegale.

- să furnizeze informaţiile de cunoaştere, anticipare şi prevenire a ameninţărilor la adresa securităţii „infrastructurilor critice” autorităţilor, instituţiilor şi organismelor însărcinate cu aplicarea legii, pentru fundamentarea şi determinarea deciziilor şi acţtiunilor necesare în fiecare situaţie.

Informaţia pentru securitatea infrastructurilor critice este componenta operaţională a informaţiei pentru securitatea naţională, definită în cadru doctrinar ca „produs analitic, rezultat al activităţii specializate de căutare, identificare, obţinere, prelucrare/procesare a datelor referitoare la disfuncţii, vulnerabilităţi, factori de risc, ameninţări, stări de pericol la adresa principiilor şi normelor politico-sociale statornicite prin Constituţie”.

Exemplu

Metodele sunt multiple. Voi încerca să abordez însă un exemplu clasic ce vizează utilizarea creditării pentru derularea de operaţiuni fictive în vederea obţinerii de rambursări ilegale de TVA de la bugetul de stat şi spălarea fondurilor obţinute prin retragerea acestora în numerar cu justificarea „restituire împrumut firmă“. În septembrie 2011, o grupare infracţională cu acţionariat cetăţeni străini şi care a prejudiciat bugetul statului cu mai mult de 4,5 milioane euro activând în domeniul imobiliar, a fost desfiinţată de către organele de combatere ale crimei organizate.



Clientul entităţii raportoare: firma X

Sediul social: oraşul Q

Persoane fizice şi juridice: firmele X,Y, Z şi administratorii A,B

Asociat extern : asociat African şi firma Fantoma

Descrierea tranzacţiei: creditare contului curent al firmei X cu suma 18 mil. ron – linie de credit, credit de stocuri sau credit de investiţii cu facturi proforme emise de firma Y. Pentru complicarea traseului de stratificare, ecuaţia poate fi completată cu alte noi firme. Achiziţii fictive de bunuri de la firma Y (în acest punct, instituţiile de verificare şi control – vama, garda financiară etc – au un rol foarte imprtant). Plăţi fictive în numerar ale firmei X către firma Y în valoare de 18 milioane ron. Acelaşi procedeu se derulează între firma Y şi firma Fantoma din

Africa pentru suma 13 mil. ron. Rezultă TVA dedus nejustificat aferent facturilor emise de firma Y. Firma Z care este acţionar cu 70% în firma X primeşte din partea firmei X 18 mil. Ron (c/v marfă) şi virează întreaga sumă în conturile personale ale persoanelor fizice A şi B (salarii) care împrumută persoana juridică X cu suma 18 milioane ron. Rambursarea ilegală de TVA în valoare de 3,25 mil. ron de la Stat către firma X se constituie la rândul ei în rambursare împrumut a firmei X către persoanele fizice A şi B.

Concluzie

Lucrarea s-a dorit a fi structurată pe câteva idei de identificare şi prevenire a spălarii banilor cu trimitere directă la combaterea terorismului în acord cu noile realităţi române şi europene. Infrastructurile Critice Naţionale şi Internaţionale pot să fie direct afectate de procesele în desfăşurare. Uniunea Europeană şi graniţele noi create au impus adoptarea de măsuri care să răspundă unitar în faţa ameninţărilor globale şi locale. Legislaţia în vigoare este continuu îmbunătăţită în aşa fel încât să ofere departamentelor de acţiune instrumentele necesare. Dacă în primul capitol s-a încercat o definire a axiomelor în analiza acestui domeniu coroborată cu prezentarea câtorva evenimente ce au determinat evoluţia ulterioară a studiului, în cel de-al doilea capitol s-au prezentat câteva potenţiale riscuri şi ameninţări la adresa infrastructurilor critice. Cel de-al treilea capitol încearcă să prezinte efectiv un studiu de caz a cărui generalizare poate să pună în lumină şi să reliefeze rolul şi locul protecţiei informaţiei în infrastructurile critice.

Ca o sinteză a celor prezentate mai sus, putem concluziona că eforturile de integrare în sistemele ce şi-au dovedit capacitatea de a se opune agresiunilor externe trebuie susţinute de toţi cei implicaţi în proiectele de apărare. Terenul pe care se desfăşoară ostilităţile este destul de accidentat, iar relieful îşi schimbă forma de mai multe ori în aceeaşi zi. Fără a încerca să intrăm în polemici inutile pe marginea competitivităţii lor, putem să spunem că multe dintre sistemele operaţionale de apărare se suprapun pe mai multe domenii de activitate şi pe mai multe arii. Mentalităţile sunt diferite, programatorii sunt diferiţi, zonele geografice sunt diferite. Cu toate acestea, globalizarea a condus la un proces de integrare a mentalităţilor. Comunicarea rapidă şi tranzacţiile comerciale între toate statele lumii a făcut ca informaţia să devină prima monedă de schimb – înaintea banului. Perisabilitatea ei este una dintre caracteristicile care-i conferă valoare. Menţinerea ei, protejarea, transmiterea şi recepţia ei nealterată sunt ţinta aşa-numitului „al treilea război mondial“.

BIBLIOGRAFIE

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

Chirlesan Georgeta, *Strategia de Securitate Naţională a României: studiu de caz şi reflecţii*

Myriam Dunn Cavelty, *Critical information infrastructure: vulnerabilities, threats and responses.*

Adrian V. Gheorghe, *Analiza de risc şi de vulnerabilitate pentru infrastructurile critice ale societăţii informatice – societate a cunoaşterii.*

Anghel Andreescu, *Motivaţia raţională a unui act iraţional – Terorismul suicidar.*

Stelian Arion, *Securitatea urbană şi protecţia infrastructurii critice*

Metoda Universalităţii Cranfield de evaluare a riscului la nivelul elementelor de infrastructură comunitară.

A*naliza modului în care organizaţiile teroriste îşi aleg ţintele,* editată de Ministerul Internelor şi Reformei Administrative

Radu Andriciuc, *Consideraţii privind protecţia infrastructurii critice,* Editura Ministerului Administraţiei şi Internelor, Bucureşti, 2009.

Sinteza documentara, *Utilizarea în scopuri teroriste a internetului*, editată de Ministerul Internelor şi Reformei Administrative.

O analiză a modului în care organizaţiile teroriste îşi aleg ţintele. Sinteza documentară – editată de Ministerul Internelor şi Reformei Administrative

Rizea Marian, *Protecţia infrastructurilor critice naţionale şi în spaţiul european,* 2010

*** Legea 535/2004 privind prevenirea şi combaterea terorismului

*** Strategia MAI de realizare a ordinii publice 2010

*** Strategia de securitate naţională a României 2007

*** Strategia de securitate naţională a României 2010

*** Strategia de securitate naţională a României 2010

*** Strategia europeană de securitate 2003 şi 2010

*** Ghidul privind abordarea comună în lupta împotriva terorismului 1986…2010

*** Strategia revizuită a Uniunii Europene privind lupta împotriva terorismul

*** Strategia revizuită a Uniunii Europene privind finanţarea terorismului

*** Directiva europeană privind Infrastructurile Critice 2008

*** Hotărârea guvernului privind Infrastructurile Critice 2010

Acte interne