NOI PROVOCĂRI ÎN LINIA ÎNTÂI A ACTIVITĂŢII DE INTELLIGENCE – PERSPECTIVA UNUI PRACTICIAN

Florian COLDEA*

Abstract

This century has come with different types of challenges in security matters that set a new security agenda for multiple fields, including intelligence. We all live in a growingly complex IT ecosystem, where the availability of the technology is pushed to lower levels, the security of information is fragile, and the citizens change the ways they communicate with one another and with states and governments. The technology-related change is affecting the intelligence agencies ability to deal with some of the most important threats, ranging or coming from the cyber arena, hybrid warfare, large scale migration flows, terrorism, counterespionage and other. Tackling these phenomena is not an easy task for the intelligence field requiring a comprehensive and reinforced cooperative approach, mutual support and assistance, doubled by the responsibility at state levels in decision making.

Keywords: challenges, gaps, security agenda, technology, innovation, way forward.

Introducere

Problema. Secolul al XXI-lea se caracterizează printr-o serie de provocări diverse în materie de securitate cărora trebuie să le facem faţă. Începând cu „vechea" problemă a Y2K din 2000, continuând cu ansamblul de comploturi teroriste de impact din mai multe oraşe occidentale, seria de dezastre legate de diverse fenomene naturale sau migraţia la scară largă, şi până la problemele de securitate majore determinate de „lumea virtuală", toate acestea ne duc cu gândul la faptul că oamenii, statele şi societăţile se confruntă cu o nouă agendă de securitate, fundamental diferită faţă de ceea ce am experimentat în secolul al XX-lea, şi caracterizată prin ceea ce numim setul de ameninţări „îngheţate".

Situaţii specifice. Noua agendă de securitate şi provocările la care aceasta se raportează cunosc o serie de aspecte comune. În mare parte din

* Serviciul Român de Informaţii.

cazuri, amenințarea este direct legată de informație (Jouini, Rabai și Aissa, 2014), așa cum am văzut în toate cazurile de atacuri cibernetice împotriva statului sau a sistemelor informatice deținute de actori din mediul privat. Astfel, observăm că, printre altele, liderii sau responsabilii cu gestionarea crizelor au nevoie de informație critică pe care nu o pot obține în lipsa unei infrastructuri instituționale sau organizaționale solide (Suchan, 2002).

De asemenea, o altă categorie de provocări solicită un amestec complex de informații secrete (provenite fie din surse umane, fie din surse tehnice) și date deja disponibile, dar care nu au fost încă integrate într-un sistem de intelligence viabil (Delaforce, 2013).

Întâlnirea oamenilor și a administratorilor cu tehnologia

Avansul tehnologic din prima parte a secolului al XXI-lea a schimbat fundamental modul în care cetățenii comunică atât între ei, cât și cu statele și guvernele lor. Aceasta a determinat o schimbare evidentă a caracterului relațiilor sociale în societățile moderne, a modelelor de comerț, a relațiilor dintre cetățean și stat (Goldsmith & Crawford, 2014). Omniprezența și disponibilitatea tehnologiei transformă fața securității și a intimității, ceea ce solicită profesioniștilor din activitatea de intelligence să înțeleagă tendințele actuale dacă doresc să răspundă noilor provocări.

Dată fiind **facilitarea proceselor de colectare tehnică și stocare** la nivelul mai multor departamente guvernamentale, numărul bazelor de date privind populația a înregistrat o creștere în ultima vreme, punând la dispoziția agențiilor de informații și a agențiilor angajate în asigurarea securității sau în livrarea unui anumit serviciu în acest sens, o cantitate considerabilă de informații sensibile. **Aceste agenții nu sunt doar cele din domeniul informațiilor și al poliției** – așa cum majoritatea persoanelor cred, ci includ, de asemenea, administrația locală și autoritățile însărcinate cu colectarea taxelor. Aceasta reprezintă o extindere a puterilor oferite agențiilor fără atribuții în domeniul securității și activității polițienești.

Utilizarea datelor de către diverse autorități naționale a determinat îngrijorări considerabile în rândul multora dintre apărătorii dreptului la viața socială și intimă a persoanei, în cadrul informațiilor cu caracter privat aflându-se datele obținute cu ajutorul tehnologiei biometrice, imagini, transferuri de bani, istoricul medical, etc. Însă scurgerile de informații și colectarea acestor date de către sectorul privat (alături de utilizarea pe care o poate da acestor date), precum și numărul punctelor de acces de unde datele pot fi accesate ilegal de către adversari reprezintă o cauza diferită și de mare îngrijorare.

Pe scurt, dacă disponibilitatea şi utilitatea tehnologiei sunt aduse tot mai aproape de individ, în mod contrar, cunoaşterea necesară pentru securizarea informaţiei nu urmează aceeaşi direcţie, sau cel puţin nu cu aceeaşi viteză. În acest mod, securitatea informaţiei este din ce în ce mai fragilă, direct proporţională cu utilitatea care îi este dată de către state şi, implicit, de către sectorul privat.

Prezenţa întregii infrastructuri tehnologice creează ceea ce am putea numi un „ecosistem", în esenţă, un sistem de operare 24/7 în cadrul căreia servere, reţele şi aplicaţii pe mobil trimit şi primesc date către/de la alte servere, reţele şi aplicaţii – sperând că toate sunt de interes pentru state, companii sau alte persoane şi clienţi pe care acestea îi servesc.

Statele pierd monopolul deţinut asupra tehnologiei: provocarea decalajului

Ultimul deceniu s-a caracterizat prin trecerea la o paradigmă a tehnologiei, generată de creşterea exponenţială a bugetelor pe care actorii privaţi le dedică progresului tehnologic – atât pentru dezvoltarea, cât şi pentru integrarea acestuia în rândul activităţii zilnice de business – şi astfel, lăsându-i în urmă pe cei care ocupau locul întâi cu ceva ani înainte: actorii statali. **A devenit clar că statele nu mai sunt principalele motoare ale dezvoltării tehnologice**, iar instituţiile trebuie să se adapteze pentru a putea ţine pasul cu ritmul impus în prezent de către actorii privaţi şi să răspundă la aşteptările în schimbare ale societăţii. Această diferenţă între avansul tehnologic şi capabilitatea statului reprezintă o vulnerabilitate nouă şi strategică prin faptul că provoacă abilitatea instituţiilor de a folosi ultimele progrese în domeniul tehnologiei, chiar şi în situaţii majore de criză.

Andrew Parker, directorul general al MI5, subliniază că „provocarea critică, şi chiar cronică, am putea spune, căreia trebuie să-i facem faţă, vine din însăşi schimbarea tehnologică" (Adresa din 8 ianuarie 2015). Altfel spus, schimbarea determinată de tehnologie ne afectează abilitatea de a trata corespunzător unele dintre cele mai importante ameninţări.

Acest lucru nu este însă o surpriză: abilitatea de a accesa discuţiile purtate între teroriști este vitală pentru capacitatea agenţiilor de intelligence de a menţine nivelul de siguranţă a ţărilor ai căror cetăţeni sunt. Internetul a schimbat şi continuă să schimbe un număr foarte mare de aspecte din viaţa noastră – în foarte multe dintre aceste cazuri în bine, revoluţionând comerţul şi comunicaţiile, lărgind gama de opţiuni în diverse domenii şi facilitând accesul la informaţie pentru noi toţi. Dar, în acelaşi timp, aşa cum am arătat

în exemplele de mai sus, internetul a oferit de asemenea teroriştilor aceleaşi avantaje şi oportunităţi (Weimann, 2004).

Toate virtuţile recunoscute ale internetului – accesul facil, absenţa reglementării sau prezenţa acesteia într-o formă minimală, potenţiala audienţa în creştere la nivel global sau fluxurile rapide de informaţii – au fost deviate astfel încât să poată lucra în avantajul grupurilor determinate să folosească teroarea asupra societăţilor pentru a-şi putea atinge obiectivele. În aceste zile, toate grupările teroriste active şi-au stabilit prezenţa pe Internet, de multe ori de-o manieră foarte dinamică prin intermediul unor site-uri web, grupuri şi reţele au apărut deodată, acestea modificându-şi frecvent forma şi dispărând apoi dintr-o dată prin schimbarea adresei, dar păstrând conţinutul similar sau membrii. Aceste canale sunt folosite pentru răspândirea propagandei, pentru radicalizarea indivizilor uşor impresionabili, pentru aranjarea călătoriilor, pentru transferul banilor. Dar cei mai mulţi le folosesc pentru comunicare, pentru planificare şi organizare; practic, folosesc aceleaşi instrumente de comunicare ca restul oamenilor.

Însă schimbările pe care tehnologia şi piaţa le înregistrează riscă să ducă la închiderea zonelor în cadrul cărora ar trebui să avem acces pentru a opera. Locurile obscure din care aceia care doresc să ne facă rău, pot complota şi planifica, se multiplică. Astfel, noi toţi – statul, societăţile şi agenţiile – avem nevoie să menţinem acelaşi ritm şi să nu permitem diferenţelor tehnologice să devină noul teritoriu şi o sursă de ameninţări imposibil de abordat şi contracarat.

Schimbarea tehnologică şi cele mai importante ameninţări

Arena cibernetică. În prezent, un stick USB stricat sau virusat poate provoca mai multe prejudicii decât o bombă sau o rachetă. Ameninţarea cibernetică nu doar schimbă imaginea războiului, ci reprezintă, de asemenea, riscuri mari la adresa statelor şi a cetăţenilor.

Războiul cibernetic este un fenomen relativ nou, emergenţa sa justificându-se prin dependenţa crescândă faţă de infrastructura şi dotările cibernetice, dar şi prin costul scăzut al transformării acestui instrument menit să faciliteze munca şi comunicarea într-o armă cu un potenţial ofensiv ridicat. Există numeroase schimbări al paradigmei convenţionale privind câmpul de luptă, iar această abordare cibernetică pare să opereze o trecere de la mijloace la scop (Sharma, 2009) – un foarte bun motiv pentru a înţelege şi a fi în pas cu permanentele evoluţii care au loc zilnic în domeniul IT.

Dintr-o perspectivă profesională, aceste evoluţii în domeniul IT trebuie privite în raport cu o provocare deja existentă în domeniul securităţii,

iar în cadrul acestei perspective, este clar că acestea au devenit un nou declanşator atât pentru ameninţări vechi, cât şi pentru cele recent descoperite: spionaj, sabotare, dezinformare, energie etc. Există un consens clar că suntem martori la crearea unei noi „arene de confruntare" (Kostopoulos, 2008, pp. 165-169) – spaţiul virtual/cybernetic – caracterizat prin propriul tip de vulnerabilităţi, riscuri şi oportunităţi. Atacuri cibernetice au loc în fiecare minut peste tot în lume şi chiar dacă doar o mică parte au potenţialul de a aduce prejudicii securităţii naţionale, consecinţele lor deja s-au dovedit a avea potenţialul de a fi distrugătoare.

Pentru toate agenţiile de intelligence, este vital să ţină pasul cu transformările în această nouă arenă, să rămână competitive în abilitatea lor de a gestiona provocările ce se nasc chiar în acest nou context virtual. Serviciul Român de Informaţii şi-a extins cooperarea cu partenerii săi (atât la nivel naţional, cât şi internaţional) şi a creat Centrul Cyberint[1] pentru a creşte nivelul de protecţie şi pentru a facilita consolidarea rezilienţei necesare acestui nucleu de infrastructură critică al statului şi al societăţii deopotrivă, sisteme IT.

Dat fiind că doctrina în acest domeniu este într-o permanentă schimbare determinată de fiecare atac major sau „salt de broască" ce se înregistrează pe palierul tehnologiei, agenţiile de informaţii trebuie să acţioneze cu un set de norme flexibile şi adaptabile ce le conferă mai multă putere pentru a răspunde noilor ameninţări cibernetice, dar într-un cadru legal clar care nu expune cetăţenii, statele şi instituţiile.

Contraspionajul în era informaţională. Ritmul rapid înregistrat de avansul tehnologic a adus noi probleme şi oportunităţi pentru organizaţiile şi profesioniştii implicaţi în activităţi de contraspionaj. Există o cantitate incredibilă de informaţii deja disponibile pe internet şi relativ accesibile altor agenţii sau chiar indivizi „ambiţioşi", oferind posibilitatea de a accesa sau agrega informaţii secrete. Acum zece ani, un ziar a fost capabil de a crea o listă conţinând numele a mii de agenţi CIA, zeci de numere de telefon interne şi chiar mai multe facilităţi clasificate, adresele de domiciliu şi numele de acoperire, pur şi simplu prin scanarea bazelor de date comerciale disponibile on-line (Crewdson, 2006).

Dacă, de regulă, tehnologia se presupune că facilitează distribuirea la scară mai mare şi mai rapidă a informaţiilor, rolul pe care activitatea de contraspionaj îl are este acela de a bloca accesul la resursele statului sau

[1] Vezi detalii pe http://www.sri.ro/cyberintelligence-en.html.

a agenţiilor de informaţii. Astfel, este foarte important ca activitatea de contraspionaj să se adapteze rapid la noile condiţii operative pe care era informaţională le presupune. Dar această responsabilitate nu aparţine exclusiv ofiţerilor/agenţiilor de informaţii: pe de o parte pentru că unii dintre aceştia nu au pregătirea tehnică pentru a asigura un nivel ridicat de securitate împotriva hackerilor calificaţi din toată lumea sau armatelor de hackeri, pe de altă parte deoarece majoritatea informaţiilor şi a agenţilor sunt vulnerabili din motive independente de responsabilitatea acestora, cum ar fi indexarea în mai multe baze de date administrative, instrumente de recunoaştere facială, proiectarea deficitară a securităţii infrastructurii IT critice etc.

Toate aceste provocări trebuie abordate la un nivel mai larg, de către stat sau chiar prin politici aliate, articulate într-o viziune care implică abordări integrate în ceea ce priveşte oamenii, procesele şi infrastructurile, o viziune care să ia în considerare ameninţările clasice la adresa vieţii oamenilor, precum şi ameninţările tehnice care se multiplică într-un ritm accelerat. Un nou ansamblu de programe integrate de gestionare a resurselor şi de formare este necesar, scopul fiind acela de a depăşi obstacolele organizatorice şi culturale actuale, care încă mai despart activitatea de contraspionaj de cea de intelligence alături de alte tipuri de activităţi relevante pentru rezultatele dorite. Tehnologiile moderne (şi, adesea, scumpe) sunt necesare pentru a spori ansamblul de acţiuni specifice domeniului contraspionajului. Nu în ultimul rând, există o nevoie vitală în cadrul întregului proces vizat, şi anume de a obţine şi menţine încrederea cetăţenilor că politicile noastre de contraspionaj sunt structurate şi implementate într-un cadru strict legal, înlăturând astfel orice suspiciune şi teamă.

Războiul hibrid. Acesta poate fi considerat o *nouă provocare*, însă, în realitate, principalele sale elemente nu reprezintă ceva cu adevărat nou (Wilkie, 2009). Pentru noi toţi, este evident că securitatea energetică a fost folosită şi înainte în calitate de armă politică, la fel cum modul în care manevrele militare convenţionale în combinaţie cu atacuri cibernetice puternice şi o propagandă în expansiune s-au răspândit pe toate canalele de media de tip nou. Însă, din punctul meu de vedere, această idee, care deşi „nu este în totalitate nouă", ar trebui să fie dezbătută în rândul teoreticienilor militari, dat fiind că, în prezent, conflictele devin tot mai complexe.

Deşi nu există nicio definiţie unanim acceptată, putem considera cu uşurinţă războiul hibrid ca fiind un „cocktail" sau un „amestec" de forţe militare clasice, insurgenţe, terorism, crimă organizată şi tehnologii avansate. Acest tip de război poate include violări ale legilor internaţionale, de multe ori

de către actori „privaţi", sprijiniţi de către state cu agende puse la îndoială. Toate aceste aspecte se pot manifesta în diverse variante şi, mai mult, oricare ingredient poate fi prezent sau absent în diferite etape ale războiului hibrid. **Se impune astfel întrebarea: există un element de noutate în ceea ce priveşte acest război hibrid?**

Putem afirma că în ultima vreme am asistat la folosirea elementelor componente ale războiului hibrid pe o scară largă şi de-o manieră mai coerentă. Iată ce reprezintă de fapt elementul de noutate: **amploarea şi elementul central**.

Conflictul ucrainean reprezintă ceea ce am putea numi oportunitatea „unui studiu de caz" pentru aceia interesaţi de acest tip de război. După cum a observat Clausewitz (1989, p. 593): „fiecare perioadă are propriul său tip de război, propriile condiţii de limitare şi preconcepţii specifice". Astfel, se poate afirma că, deşi războiul hibrid nu este ceva nou, profesioniştii din domeniul informaţiilor şi al securităţii trebuie să ia în considerare că modalităţile de manifestare ale acestuia devin din ce în ce mai sofisticate şi fatale, necesitând un răspuns pe măsură.

Aceasta poate însemna că în cadrul efortului de a actualizare a principiilor şi teoriilor războiului, trebuie să identificăm acele aspecte care încă rămân constante. În acest domeniu nu există un „ciclu" care conduce la un nou panaceu revoluţionar cu fiecare deceniu care trece, dar se înregistrează schimbări permanente şi incrementale care sunt inerente activităţii de gestionare a securităţii în ansamblul său. „Schimbări revoluţionare ale paradigmei" sunt mai puţin susceptibile de a se produce spre deosebire de ceea ce cred mulţi dintre participanţii la conferinţe pe acest subiect.

La nivelul Alianţei Nord-Atlantice, aşa cum am evidenţiat într-o altă lucrare (Coldea, 2015) – luând în considerare atacurile cibernetice care au lovit Estonia în 2007 – subiectul a fost discutat pentru prima data în ianuarie 2008 şi dezbătut mai departe cu ocazia Summit-ului NATO organizat la Bucureşti în Aprilie 2008.

Terorismul. S-a dovedit a fi un fenomen foarte dinamic pe mai multe niveluri, rămânând una dintre principalele ameninţări la adresa securităţii naţionale şi internaţionale – în special din cauza curbei schimbării pe care o traversează. Ceea ce credem că ştim la un anumit moment despre acest fenomen s-ar putea să nu fie potrivit pentru contracararea sa în viitor, deoarece dacă rădăcina care duce la manifestarea terorismului rămâne constantă, modul de acţiune, tacticile, structura şi organizarea sunt într-o continuă evoluţie. În aceasta constă permanenta provocare pe care terorismul

o reprezintă şi motivul pentru care acesta reprezintă principalul subiect de cercetare pentru mediul academic.

Evoluţia constantă a terorismului a împins acest fenomen sub umbrela conceptuală a ameninţării hibride, aşa cum este cazul evident al grupării „Daesh" şi al ambiţiilor sale de a se comporta precum „un stat" – dând naştere unor noi provocări pentru toate instituţiile statului şi pentru practicienii din domeniul securităţii. Un alt exemplu îl reprezintă numărul în creştere al luptătorilor străini şi a celor care se reîntorc în/din zonele de conflict, în special în Irak şi în Siria (*Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, decembrie 2014) – un flux nu doar al persoanelor, ci şi al abilităţilor militare şi al ideilor radicale, al fluxului logistic şi financiar, al celor care promovează terorismul şi chiar al celor care practică terorismul.

Pentru a pune lucrurile în perspectivă, într-o anumită măsură de-o manieră similară cu problema războiului hibrid, trebuie spus că problema luptătorilor străini nu este un fenomen nou. În secolele al XIX-lea şi al XX-lea, zeci de insurgenţi şi-au părăsit ţările, alăturându-se grupărilor ostile în calitate de luptători străini în multe războaie civile moderne, multe voci dându-l drept exemplu pe poetul englez Lord Byron, luptător străin în Grecia în 1820 (Malet, 2010, p. 101). Ceea ce este nou în zilele noastre este amploarea ameninţării pe care izbucnirea războiului civil şi a violenţei sectare din Siria, Irak, Libia şi alte ţări o reprezintă.

Abordarea acestor fenomene nu este uşoară, aşa cum a devenit tot mai clar în ultimii ani. Este nevoie de o abordare cuprinzătoare şi de cooperare, deoarece vorbim despre o problemă internaţională, mai degrabă decât una naţională, care poate fi abordată eficient numai prin eforturi comune ale mai multor ţări şi/sau agenţii. Am văzut că, după fiecare atac major (Paris 2015 şi 2016, Bruxelles 2015, etc.) normele juridice naţionale respective sunt actualizate, în principal prin încadrarea de noi infracţiuni teroriste. Aceasta este o reacţie comună şi previzibilă la ameninţarea tot mai mare, dar care poate crea, de asemenea, riscuri noi legate de lipsa unor standarde comune sau de diferenţe în ceea ce priveşte unele incriminări şi proceduri juridice în ţări distincte, dar supuse aceleaşi ameninţări.

În acest context, nevoia consolidării cooperării internaţionale a devenit din ce în ce mai evidentă şi poate fi consolidată în perioada următoare printr-o abordare multi-disciplinară (incluzând domeniul juridic, de intelligence etc.). Niciunul dintre noi nu poate face faţă singur acestei ameninţări, astfel încât se impune nevoia cooperării strânse şi concrete.

Fenomenul imigraţionist. Numărul imigranţilor şi al refugiaţilor a crescut neaşteptat de mult în 2015, devenind rapid o temă de importanţă critică pe agenda europeană de politică şi securitate, punându-i pe decidenţi în situaţia de a se confrunta cu probleme cheie precum: impactul asupra ţărilor de tranzit şi a destinaţiilor finale (*Countries of transit ...*, 11 septembrie 2015), impactul asupra relaţiilor şi a solidarităţii între statele europene (Goldner Lang, 2015), măsura în care globalizarea acţionează precum un catalizator pentru dinamica accentuată a populaţiilor, rolul pe care instituţiile statului şi societatea civilă ar trebui să şi-l asume în acest context, etc.

Din perspectiva securităţii naţionale, principala greşeală pe care o putem face este aceea de a gândi şi de a aborda această problemă într-un cadru al securităţii ce intră exclusiv în competenţa statelor vizate, când de fapt avem de-a face cu o problemă pan-europeană cauzată de un ansamblu de conflicte şi instabilităţi manifestate de-a lungul întregii regiuni şi societăţi arabe.

Mai mult, dacă ţinem cont că la nivelul ţărilor europene, există probleme similare care fac obiectul politicilor şi al dezbaterilor care transced elementele distincte ce privesc securitatea naţională, identitatea şi etnia, criza imigranţilor este cu atât mai mult o preocupare de interes comun la nivelul Uniunii Europene, necesitând solidaritatea în rândul statelor membre sub forma ajutorului şi al asistenţei reciproce. Dacă dorim să avem o perspectivă de viitor, ţinând cont însă că nimeni nu ştie care vor fi tendinţele pe termen scurt sau mediu (fiind foarte probabil ca pe termen lung războaiele mici şi urbanizarea populaţiei la nivel global să menţină ridicat ritmul imigraţiei), trebuie să acceptăm că există o responsabilitate comună a statelor de a se ajuta pentru a gestiona această problemă şi pentru a proteja securitatea naţională şi regională.

Perspectiva „valurilor mari" de imigranţi generează noi riscuri, importante atât pentru instituţiile de implementare a legii, cât şi pentru serviciile de informaţii şi securitate. Aceste instituţii trebuie să-şi adapteze şi să-şi ajusteze resursele (umane şi financiare), fiind nevoite să opereze într-un cadru legal actualizat.

Concluzii sau căi de urmat

În ultimele decenii, ritmul schimbării tehnologice şi inovaţia au determinat neglijarea reglementărilor legislative. Acest decalaj se va adânci fără o serioasă actualizare a legislaţiei care să reglementeze toate aceste progrese tehnologice şi practicile asociate, şi fără o dezbatere liberă şi deschisă asupra gradului de supraveghere de către surse publice şi private. State şi societăţi deopotrivă trebuie să-şi adapteze reflexele la această lume

caracterizată de interdependenţă şi interacţiune în creştere inclusiv între domenii în aparenţă distincte precum terorismul şi sănătatea, precum şi între actori la prima vedere diferiţi precum indivizii, guvernul şi industria.

Provocarea centrală în acest context este înţelegerea modului în care putem construi capabilităţile statului, stabili şi sprijini existenţa şi acţiunea unor instituţii solide, bazate pe principii democratice, respectiv urmări îndeaproape profesionalismul, responsabilitatea şi integritatea acestora. Consider că este responsabilitatea noastră, în calitate de profesionişti în sfera activităţii de intelligence, să ţinem pasul cu aceste evoluţii rapide în cadrul actualului mediu volatil de securitate şi să propunem noi soluţii creative pentru a asigura şi a proteja securitatea cetăţenilor noştri.

Toate aceste provocări ar fi mai bine înţelese printr-un efort comun al decidenţilor, practicienilor, reprezentanţilor mediului academic astfel încât să putem dobândi o mai bună înţelegere a acestora, în vederea recomandării unor soluţii viabile. Această manieră de abordare a subiectelor dificile favorizează explorarea unei perspective şi a unor paradigme noi. Într-un moment în care cererea publică de informare şi transparenţă este mai mare ca oricând, trebuie să continue efortul nostru de căutare a unor noi modalităţi de gestionare a tuturor acestor interdependenţe.

Referinţe bibliografice:

1. Adresa din 8 ianuarie 2015 a directorului general al Serviciului de Securitate**,** *Andrew Parker, către Royal United Services Institute (RUSI) din Thames House*, accesibilă la https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html**.**
2. *Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, Global Center on Cooperative Security, Human Security Collective, and International Centre for Counter-Terrorism – The Hague, Policy Brief, December 2014.
3. Coldea, Florian, (2015), *Building national capabilities and countering hybrid threats: lessons learned*, Key Note Speech at NATO Advanced Research Workshop on *Countering Hybrid Threats: Lessons Learned from Ukraine*, Bucharest, 2015 September 28-29th.

4. *Countries of transit: meeting new migration and asylum challenges*, Council of Europe Committee on Migration, Refugees and Displaced Persons, Doc. 13867, 11 September 2015, accesibil la http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=22017&lang=en.
5. Crewdson, John, (March 12, 2006), *Internet Blows CIA Cover*, in Chicago Tribune, accesibil la http://articles.chicagotribune.com/2006-03-12/news/0603120396_1_agency-employees-or-operatives-cia-director-porter-goss-two-dozen-secret-cia.
6. Delaforce, Ruth, (2013), *Public and private intelligence: historical and contemporary perspectives*, în *Salus Journal*, Issue 1, Number 2, accesibil la http://www.salusjournal.com/wp-content/uploads/sites/29/2013/03/Delaforce_Salus_Journal_Issue_1_Number_2_2013_pp_21-39.pdf.
7. Goldner Lang, Iris, (2015), *The EU Financial and Migration Crises: Two Crises – Many Facets of EU Solidarity*, in E. Dagilyte & E. Küçük (eds.), *Solidarity in EU Law: Legal Principle in the Making*, Edward Elgar Publishing.
8. Goldsmith, Stephen, Crawford, Susan, (2014), *The responsive city. Engaging communities through data-smart governance*, San Francisco, Jossey-Bass.
9. Jouini, Mouna, Rabai, Latifa Ben Arfa, Aissa, Anis Ben, (2014), *Classification of Security Threats in Information Systems*, Procedia Computer Science, Volumul 32, pp. 489–496.
10. Kostopoulos, George K., (2008), *Cyberterrorism: The Next Arena of Confrontation*, Communications of the IBIMA 6(1), pp. 165–169, accesibil la http://www.ibimapublishing.com/journals/CIBIMA/volume6/v6n25.pdf.
11. Malet, David, (2010), *Why Foreign Fighters? Historical Perspectives and Solutions,* Published by Elsevier Limited on behalf of Foreign Policy Research Institute, Winter 2010**.**
12. **S**harma, Amit, (2009), *Cyber Wars: A Paradigm Shift from Means to Ends in The Virtual Battlefield: Perspectives on Cyber Warfare*, Proceedings 2009, NATO Cooperative Cyber Defence Centre of Excellence, accesibil la https://ccdcoe.org/sites/default/files/multimedia/pdf/01_SHARMA_Cyber_Wars.pdf.
13. Suchan, William, (2002), *The organizational information infrastructure maturity model*, AMCIS Proceedings, Paper 295, accesibil la http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1654&context=amcis2002.
14. Von Clausewitz, Carl, (1989), *On War,* Princeton University Press.

15. Wilkie, Robert, (2009), *Hybrid Warfare: Something Old, Not Something New*, în Air & Space Power Journal – Winter 2009, accesibil la http://www.airpower.maxwell.af.mil/airchronicles/apj/apj09/win09/wilkie.html.
16. Weimann, Gabriel, (March 2004), *How Modern Terrorism Uses the Internet*, US Institute of Peace, Special Report 116, accesibil la http://www.usip.org/sites/default/files/sr116.pdf.