DOMENIUL CIBERNETIC- ASPECTE CU IMPACT IN EVALUAREA STĂRII DE SECURITATE A STATELOR

CYBER DOMAIN – ISSUES IMPACTING THE ASSESSEMENT OF STATES' SECURITY

CS II dr. Mihai-Ştefan DINU [*]

Rezumat: *Impactul tehnologiei informației manifestat în primele două decenii ale mileniului trei asupra majorității activităților umane precum și diversificarea acestor activități în spațiul cibernetic creat de utilizarea pe scară din ce în ce mai masivă a acestor tehnologii a condus nu numai la apariția unor efecte benefice, ci și negative, ceea ce a diversificat discuțiile din cadrul studiilor de securitate, amenințările de natură cibernetică diversificându-se și amplificându-se pe măsură ce spațiul cibernetic a fost adăugat mediilor strategice, sau domeniilor operaționale clasice. Această lucrare își propune să schițeze reperele actuale ale evaluării securității naționale a statelor, în contextul mai larg al modului de interacțiune a acestora în cadrul comunității internaționale și în directă relaționare cu beneficiile și neajunsurile create de dezvoltarea spațiului cibernetic, de la putere la amenințare cibernetică, via moduri de comportament în spațiul cibernetic.*

Cuvinte cheie: *cibernetic, securitate națională, securitate cibernetică, strategii, drept.*

Abstract: *The impact of information technology manifested in the first two decades of the third millennium on most human activities, as well as the diversification of these activities in cyberspace created by the use of these technologies on an increasingly massive scale, led not only to the appearance of beneficial, but also negative effects , which has diversified the discussion within security studies, with cyber threats diversifying and amplifying as cyber space has been added to strategic environments, or classic military operational domains. This paper aims to outline the current referential of the states' security assessment, in the wider context of how they interact within the international community and in*

[*] Membru asociat al Academiei Oamenilor de Știință din România, Cercetător ştiinţific gr. II, în cadrul Facultăţii de Securitate şi Apărare a Universităţii Naţionale de Apărare „CAROL I", mihaistdinu@yahoo.co.uk

direct relation to the benefits and deficiencies created by the development of cyberspace, from power to cyber threat, via diverse postures in cyberspace.

Keywords: *cyber, national security, cyber security, strategies, law.*

1. Introducere

În perioada ce a urmat Războiului Rece, în perioada de renaștere a studiilor de securitate odată cu dezvoltarea domeniului în mediul academic, majoritatea specialiștilor în domeniu erau de acord că scena internațională este supusă unor transformări care determinau trecerea către o nouă ordine mondială. Modul în care se făcea această trecere arăta fără echivoc că puterea militară rămânea un element central al politicii internaționale, iar scena internaţională devine astfel, după părerea lui Zbigniew Brzezinski *marea tablă de şah*[1] în care actorii acţionează frecvent prin relaţiile de putere spre atingerea intereselor naționale De o importanţă majoră în proiectarea unor politici de securitate eficiente, puterea este rezultatul unei combinaţii de capacitaţi care derivă din surse interne sau externe, ca rezultat al relaţiilor internaţionale. În general, sunt acceptate ca surse esenţiale de putere sursele naturale, sursele socio-psihologice şi sursele sintetice[2]. S*ursele sintetice*, derivă din celelalte două categorii, reflectând abilitatea statului de a-şi întrebuinţa sursele naturale şi sociopsihologice pentru afirmarea puterii. Practic, sursele sintetice de putere sunt constituite de resursele industriale, financiare, tehnico-ştiinţifice şi militare, resurse care dau de asemenea și nivelul *puterii cibernetice* a unui stat, în funcţie de evoluţia gestionării relaţiilor dintre sursele naturale și cele socio-psihologice pot exista implicaţii asupra securităţii statului respectiv, în sensul menţinerii sau degradării stării acesteia. Iată, așadar, că avansul tehnologic a condus către o expansiune a clasicei *mari table de șah* de la sfârșitul mileniului al doilea prin intermediul *spațiului cibernetic*, care astăzi poate fi considerat un domeniu global de interacțiune umană.

[1] Zbigniew Brzezinski, Marea tablă de șah – supremația americană și imperativele sale geostrategice, Univers Enciclopedic, București, 2000

[2] Walter S. Jones, *The logic of International Relations*, Longman, New York 1997, p. 202.

2. Puterea cibernetică a statelor

Cel mai simplu reper în definirea puterii cibernetice este acela formulat de Daniel T. Kuehl care vede puterea cibernetică prin prisma comportamentului statelor în relație cu alte state *„abilitatea de a utiliza spațiul cibernetic pentru a crea avantaje și a influența evenimentele în toate mediile operaționale și între instrumentele de putere”*[3]. Un an amai târziu, Joseph S. Nye Jr, propune o abordare similară a puterii cibernetice, definind-o drept *„abilitatea de a obține rezultatele dorite prin utulizarea resurselor informaționale interconectate electronic în domeniul cibernetic”*[4], menționând critic și definiția menționată anterior, precizând însă că puterea cibernetică poate fi folosită în scopul atingerii obiectivelor în spațiul cibernetic sau se pot folosi intrumente cibernetice pentru a atinge obiectivele dorite în alte domenii din afara spațiului cibernetic[5].

În 2011, în lucrarea Future of Power, Nye revine asupra definirii puterii cibernetice abordată din punct de vedere a resurselor tehnice relaționate creerii, controlului și comunicațiilor în interiorul unei infrastructuri de informații electronice bazate pe computer, incluzând aici nu numai rețeaua de computere conectate la internet , ci și rețelele de intranet, tehnologiile celulare și comunicațiile satelitare.

Pe parcursul timpului definițiile derivate din tehnologia informației și securitatea sistemelor își fac din ce în ce mai mult loc în caracterizarea stării de securitate a statelor, cu observația că specificul definițiilor tehnice timpurii ale securității cibernetice se deosebesc în opinia noastră de definițiile securității naționale și pentru că definițiile securității informațiilor, de exemplu, aveau un domeniu de aplicabilitate mult mai mică, fiind limitate de componentele hardware ale unui sistem sau ale unei rețele locale, mai degrabă decât de granițele unui stat. Odată cu dezvoltarea rețelelor de calculatoare și acces facil la Internet, postura se schimbă drastic: frontierele geografice ale statului sunt depășite prin intermediul spațiului cibernetic, iar definițiile securității, indiferent că este vorba despre cea

[3] Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem, in Cyberpower and national security,* Potomac Books, Inc., Dulles, 2009, p.38

[4] Joseph S. Nye Jr, *Cyber Power,* Belfer Center for Science and International Affairs, Cambridge, 2010, p3.

[5] *Ibidem*, p. 4

naţională sau cea cibernetică, folosesc o terminologie comună: vulnerabilităţi, ameninţări, actori statali, actori non-statali, apărare, reziliență etc.

Astfel, Ralph Langner, specialist în apărare cibernetică şi cel care a decodat Stuxnet-ul, propunea o definiţie cuprinzătoare a puterii cibernetice din punct de vedere al unei capacităţi organizate a societăţii de a folosi tehnologia pentru supraveghere, exploit, operaţii subversive subminare şi coerciţie în caz de conflict internaţional. O societate ce îşi poate mânui la un nivel superior puterea cibernetică se poate angaja într-o serie de acţiuni în care să exploateze sau să submineze economic alte state, să culeagă informaţii de la nivel politic şi militar, să scoată din uz pe timp limitat sau nedeterminat capacităţile de luptă ale adversarilor, să saboteze infrastructura critică[6].

3. Posibile noi dimensiuni ale securităţii naţionale

Într-una dintre conferinţele anului 2016, avansam ideea necesităţii ca în analiza dimensiunilor securităţii să fie considerată dimensiunea *cyber (figura nr. 1),* dacă ţinem cont de aspectele menţionate în secţiunea anterioară a acestei lucrări, unde subliniam că buna funcţionare a unui stat, implicit starea de securitate a acestuia, este relaţionată infrastructurilor critice sectoriale şi, în principal, infrastructurii informaţionale critice.

În ceea ce priveşte nivelurile securităţii, credem că celor tradiţionale precum naţional, regional şi internaţional, trebuie să adăugăm unul specific societăţii informaţionale, nivelul virtual, cibernetic al securităţii, cu atât mai mult cu cât acest nivel, datorită naturii sale, le poate transcede pe cele trei tradiţionale, nivelul cibernetic nefiind caracterizat de limitări precum graniţele sau distanţele geografice.

[6] Ralph Langner, Cyber Power: An Emerging Factor in National and International Security, in Horizons No.8, Journal of International Relations and Sustainable Development 2016, pp. 206-207.

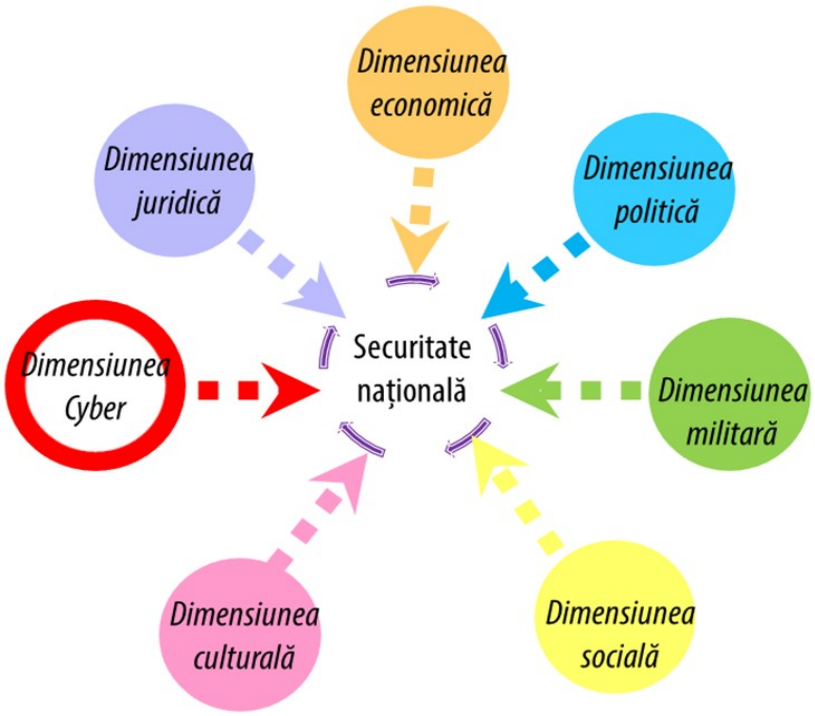

Figura nr. 1. Dimensiuni ale securității naționale

Deși poate părea surprinzătoare, prezența dimensiunii juridice în ansamblul dimensiunilor securității, aceasta capătă sens, în cadrul specific al surselor de insecuritate specifice societății informaționale, cu atât mai mult cu cât în secțiunea anterioară a lucrării noastre au existat definiții care au abordat securitatea din punct de vedere al comportamentului statelor în relație cu alte state.

Existența acestor definiții ne conduc către reconsiderarea dimensiunii juridice, a dreptului, în domeniul cyber, pentru că dreptul nu reprezintă altceva decât totalitatea normelor juridice elaborate sau recunoscute de puterea de stat, care au ca scop organizarea şi disciplinarea comportamentului subiectelor de drept în cadrul celor mai importante relaţii din societate, conform valorilor sociale ale societăţii respective, stabilind

drepturi şi obligaţii juridice a căror respectare este asigurată, la nevoie, de forţa coercitivă a statului.

4. Modelul ITU de evaluare a securității cibernetice a statelor

Securitatea națională, la fel ca și cea cibernetică are un domeniu de aplicare care cuprinde toate industriile, toate sectoarele, atât pe verticală, cât și pe orizontală. Pentru a spori dezvoltarea capacităţilor naţionale, forțele politice, economice şi sociale, prin organele în drept, instituții de învățământ, ministerele, operatorii din sectorul privat, prin parteneriatele public-privat și cooperare intra-statală, e nevoie de o aplicare unitară a legii la nivelul fiecărui stat în parte.

The International Telecommunication Union, agenție a ONU specializată în tehnologii ale informației și comunicațiilor a avansat o serie de criterii privind securitatea cibernetică în funcție de capacitățile cibernetice ale unui stat. Aceste capacități sunt evaluate în următoarele domenii:

- juridic;
- tehnic;
- organizațional;
- creșterea capacităților;
- cooperare.

Domeniul juridic include măsurile legale ce autorizează un stat național să instituie mecanisme de răspuns de bază prin investigarea și urmărirea penală a infracțiunilor și impunerea de sancțiuni pentru nerespectarea sau încălcarea legii. Un cadru legislativ stabilește baza minimă de comportament pe care se pot construi capacități suplimentare de securitate cibernetică. În esență, obiectivul este de a avea suficientă legislație în vigoare pentru a armoniza practicile la nivel regional/internațional și pentru a simplifica lupta internațională împotriva criminalității cibernetice. Contextul juridic este evaluat pe baza numărului de instituții și cadre juridice care se ocupă de securitatea cibernetică și criminalitatea cibernetică.

Domeniul tehnic trebuie să țină seama de faptul că tehnologia este frontiera principală de apărare împotriva amenințărilor cibernetice. Aici trebuie să se aibă în vedere:

- utilizarea echipelor de răspuns la situații de urgență sau incidente computerizate;
- cadrul de implementare a standardelor;
- mecanisme tehnice și capabilități implementate pentru a aborda spam-ul
- protecția online a copiilor etc.

Fără abilități tehnice adecvate pentru a detecta și a răspunde atacurilor cibernetice, statele rămân vulnerabile în fața amenințărilor cibernetice. Dezvoltarea și utilizarea eficientă a tehnologiilor informației și comunicațiilor nu poate fi corect direcționată decât într-un mediu de securitate solid si bine reglementat. Prin urmare, statele trebuie să standardizeze criterii de securitate minimă acceptate și scheme de acreditare pentru aplicații. Aceste eforturi trebuie să fie sinergizate sub un organism național cu scopul de a trata incidentele cibernetice, entități guvernamentale cu autoritate și a unui cadru național de supraveghere, avertizare și răspuns la incidente. Elementele tehnice sunt evaluate pe baza numărului de mecanisme practice pentru a face față securității cibernetice.

Domeniul organizațional cuprinde ansamblul măsurilor organizaționale: strategiile naționale, agențiile responsabile și evaluări de securitate cibernetică. Aceste măsuri organizatorice sunt indispensabile pentru implementarea corectă a oricărei inițiative naționale. Astfel, obiectivele strategice ample trebuie stabilite de statul național, împreună cu un plan cuprinzător în implementare, livrare și măsurare. Agențiile naționale trebuie să dețină responsabilitatea implementării strategiei și a cuantificării rezultatelor. Lipsa unei strategii naționale, a unui model de guvernanță și a unei autorități de supraveghere pot conduce la generarea unor situații conflictuale la nivel de roluri, responsabilități și proceduri, limitând eforturile de a obține o armonizare eficientă a dimensiunii securității cibernetice. Conform criteriilor ITU, structurile organizatorice sunt evaluate pe baza prezenței instituțiilor și strategiilor care implică dezvoltarea securității cibernetice la nivel național.

Creşterea capacităților este evaluată prin identificarea unor măsuri precum:

- campanii de conștientizare a publicului;

- existența unui cadru de certificare și acreditare a profesioniștilor în securitate cibernetică;
- cursuri de formare profesională în domeniul securității cibernetice;
- programe educaționale sau programe academice etc.

Creșterea capacităților este , în principiu, intrinsecă primilor trei piloni:juridic, tehnic și organizatoric. Securitatea cibernetică este abordată cel mai adesea dintr-o perspectivă tehnologică, dar există și numeroase implicații socio-economice și politice, astfel încât dezvoltarea capacităților umane și instituționale este esențială pentru a crește gradul de conștientizare, cunoștințe și know-how în sectoare, pentru soluții sistematice și adecvate și pentru a promova dezvoltarea unor profesioniști calificați. Consolidarea capacităților este evaluată de către ITU pe baza numărului de programe de cercetare și dezvoltare, de educație și formare și de profesioniști certificați și agenții din sectorul public.

Cooperarea este un factor important de evaluare având în vedere caracterul transfrontalier al acestui tip de infracțiuni din domeniul cybernetic. Infracțiunile cibernetice au devenit o problemă globală care nu ține cont de frontiere geografice. Prin urmare, combaterea infracțiunilor cibernetice necesită o abordare multistatală, cu mai multe părți interesate de limitarea fenomenului, cu contribuții din toate sectoarele și disciplinele. Măsurile în domeniul cooperării pot include:

- acorduri bilaterale și multilaterale;
- participarea forurilor/asociațiilor internaționale;
- parteneriate public-privat;
- acorduri inter-agenții).

Un grad ridicat de cooperare poate conduce la dezvoltarea unor capacități de securitate cibernetică mult mai puternice, ajutând la descurajarea amenințărilor cibernetice repetate și persistente și permițând o mai bună investigare, reținere și urmărire penală a actorilor rău intenționați. Cooperarea națională și internațională este evaluată de către ITU pe baza numărului de parteneriate, cadre de cooperare și rețele de schimb de informații.

5. Concluzii

Modelul de evaluare propus de ITU pe cele cinci dimensiuni, poate fi translatat în procesul de evaluare a securității naționale, dimensiunile clasice ale acesteia permițând evaluarea unor măsuri în domenii care ar trebui să fie prezente în fiecare moment de dezvoltare a activităților umane prin intermediul spațiului cibernetic. Dincolo de nivelul individual sau al comunității locale, realitatea comportamentului statului și a interacțiunii în spațiul cibernetic din ultimele două decenii a fost destul de diferit de modelul de război, atac catastrofal și constrângerea pe care se bazează strategia și politica cibernetică a multor țări. Cea mai mare parte a activității cibernetice sponsorizate de stat adversar a avut loc în afara conflictelor armate, și nu a fost desfășurată cu aplicare coercitivă, însă mediul de securitate regional instabil, poate permite oricând acțiuni disruptive ale statelor beligerante îndreptate asupra celor din vecinătatea imediată.

BIBLIOGRAFIE

BRZEZINSKI Z., *Marea tablă de șah – supremația americană și imperativele sale geostrategice*, Univers Enciclopedic, București, 2000;

JONES W. S., *The logic of International Relations*, Longman, New York 1997;

KUEHL D. T., *From Cyberspace to Cyberpower: Defining the Problem, in Cyberpower and national security,* Potomac Books, Inc., Dulles, 2009;

LANGNER R., „Cyber Power: An Emerging Factor in National and International Security", in Horizons No.8, Journal of International Relations and Sustainable Development 2016;

NYE Jr. J. S., *Cyber Power,* Belfer Center for Science and International Affairs, Cambridge, 2010.