Arhitectura sistemului de guvernanță globală în secolul XXI-lea: provocări și tendințe pentru mediul internațional de securitate

Busuncian Tatiana
Dr., conferențiar universitar

Chișinău
2024

Conținuturi; Obiective de referință; Termeni-cheie

Conținuturi:

1. Guvernare și guvernanță: delimitarea guvernanței globale.
2. Surse și resurse de putere în guvernanța globală.
3. Reconfigurarea ordinii multilaterale la înc. sec. XXI și impactul său asupra mediului de securitate global.
4. Provocări la adresa arhitecturii sistemului de guvernanță globală în sec. XXI.
5. Tendințe strategice ale organizațiilor internaționale de securitate pentru consolidarea securității globale.

Obiective de referință:

- să analizeze arhitectura instituțională a sistemului de relații internaționale şi a funcționării acesteia în sec. XXI.
- Să cunoască conceptele specifice proceselor de guvernanță la nivel internațional.
- Să explice guvernanța internațională/ globală prin prisma conceptelor, principiilor, actorilor care activează la nivel internațional, a temelor aflate pe agenda internațională, a evoluției și provocărilor la adresa ordinii globale.
- Să evalueze impactul guvernanței politice globale în gestionarea inegalităților sociale și sărăciei la nivel global.

Mediul contemporan de securitate este rezultatul transformărilor determinate de două evenimente majore, sfârşitul Războiului Rece şi evenimentele de la 11 septembrie 2001, care au produs schimbări radicale în cadrul relaţiilor internaţionale.
O serie de fenomene complexe cum ar fi globalizarea, terorismul internaţional, proliferarea armamentelor, violenţa etnică şi religioasă, criminalitatea organizată, problemele populaţiei şi altele, se constituie în provocări majore ale mediului contemporan de securitate.

La începutul secolului al XXI-lea, mediul de securitate internațional înregistrează ca principală amenințare terorismul, reconsiderarea strategiilor şi politicilor naționale de securitate după atentatele de la 11 septembrie 2001, fiind direct conectate asupra identificării celor mai viabile soluții de prevenire şi combatere a acțiunilor teroriste. Astfel, terorismul, prin modul său de manifestare, se transformă într-un fenomen global al mediului de securitate internațional.

Secolul al XXI-lea este marcat de transformări profunde ale mediului de securitate, devenit din ce în ce mai fluid şi flexibil, cu posibilităţi multiple de evoluţie, în funcţie de predominanţe, tendinţe politice şi economice şi în special, de interesele principalilor actori statali şi non statali de pe arena internaţională.

Guvernare și guvernanță: delimitarea guvernanței globale
Contextul amenințărilor cibernetice

După 2001 războiul global împotriva terorismului, a cuprins întreaga lume şi a produs schimbări profunde în cadrul mediului de securitate. Printre provocările mediului contemporan de securitate evidențiem: globalizarea; terorismu, proliferarea armelor; violența etnică și religioasă; probleme majore ale populației (sărăcia, fometea, degradarea educației, bolilor, etc.

Secolul al XXI-lea este marcat de transformări profunde ale mediului de securitate, devenit din ce în ce mai fluid şi flexibil, cu posibilităţi multiple de evoluţie, în funcţie de predominanţe, tendinţe politice şi economice şi în special, de interesele principalilor actori statali şi non statali de pe arena internaţională. Sfârşitul „războiului rece”, îndeosebi după 1991, scoate în evidenţă o multitudine de conflicte etnice care se declanşează cu o violenţă deosebită. De regulă, problemele etnice scot la iveală probleme fundamentale pe fondul unei descreşteri economice şi implicit cu scăderea nivelului de trai al populaţiei. Atât libertăţile sociale, cât şi cele politice ale omului nu pot exista în lipsa libertăţilor economice şi doar dezvoltarea concomitentă a lor poate duce la un rezultat pozitiv.

Globalizarea terorismului impune statelor noi nevoi de politici de securitate şi apărare comune şi puternice. Multitudinea atentatelor teroriste la începutul secolului al XXI-lea, denotă o extindere a terorismului fără precedent, până la globalizare.

Confruntările militare principale la nivel global din ultimul deceniu (campaniile din Irak și Afganistan) au avut ca dominantă constituirea unor coaliții de state, cu reprezentare mare la nivel planetar, care au acționat sub conducerea SUA, pentru a îndepărta de la putere regimuri nedemocrate, a anihila rețele teroriste și a sprijini funcționarea instituțiilor fundamentale ale statului. Ambele conflicte au avut un caracter profund asimetric, iar dezvoltarea acestora a generat alte probleme în planul securității, pentru care comunitatea internaţională nu are în prezent soluții viabile de rezolvare.

La nivel local și regional, există numeroase tensiuni și focare de conflict, de la cele latente și înghețate (Kosovo, Bosnia-Herţegovina, Cipru, Orientul Mijlociu, Transnistria, Caucazul de Nord și de Sud, Peninsula Coreea, Kashmir etc.), până la cele în desfășurare (Irak, Afganistan).

Tendințele de insecuritate se vor înscrie în aria confruntărilor dintre marile puteri, pretendente la supremație și resurse, în cea a confruntărilor dintre lumea civilizată și actori nonstatali din sfera terorismului, criminalității, economiei subterane, traficului de droguri și carne vie, precum și cea a luptei dintre adepții globalizării forțate și cei ai menținerii suveranității naționale, individualității și independentei entităților statale.

La fenomenele politice și sociale care au marcat ultimul deceniu, se pot adăuga cele cu manifestare recentă, aflate încă în desfășurare, războiul din Ucraina, Orientul Mijlociu, ale căror consecințe și finalitate sunt încă greu de anticipat.

Impactul asupra mediului de Securitate global

Confruntări militare la nivel global din ultimul deceniu (campaniile din Irak şi Afganistan) au avut ca dominantă constituirea unor coaliţii de state, cu reprezentare mare la nivel planetar, care au acţionat sub conducerea SUA, pentru a îndepărta de la putere regimuri nedemocrate, a anihila reţele teroriste şi a sprijini funcţionarea instituţiilor fundamentale ale statului. Ambele conflicte au avut un caracter profund asimetric, iar dezvoltarea acestora a generat alte probleme în planul securităţii, pentru care comunitatea internaţională nu are în prezent soluţii viabile de rezolvare.

Cauzele globalizării se găsesc în progresul tehnic, valoarea globală a informaţiei, caracterul transfrontalier al economiei, al sistemului educaţional, al relaţiilor sociale, în ofensiva frontierei democratice care depăşeşte frontierele politice limitate, sectariste şi, mai ales, totalitare. Politica democratică este cea care exprimă cel mai bine interesele democratice ale populaţiilor, ce devin globale, planetare. Dezvoltarea reţelelor globale determină o interdependenţă statală în anumite industrii. Pieţele financiare se globalizează. Apar alianţele strategice globale.

Efectele globalizării

1

Directiva NIS

Directiva se referă la securitatea rețelelor și a sistemelor informatice la nivel european și introduce norme obligatorii pentru statele membre.

2

Regulamentul GDPR

Regulamentul protejează datele personale și impune responsabilități clare asupra operatorilor de date.

3

Pachetul de măsuri privind securitatea cibernetică

Aceste măsuri vizează întărirea cooperării, sporirea rezilienței cibernetice și consolidarea capacității de răspuns la incidente în UE.

Colaborarea între statele membre UE în combaterea amenințărilor cibernetice

Echipe de răspuns la incidente

[illegible] cooperează [illegible]

Exerciții și conferințe

Exerciții periodice și conferințe internaționale facilitează schimbul de bune practici și dezvoltarea de expertiză în securitatea cibernetică.

Armonizarea legislației

Statele membre lucrează împreună pentru a armoniza legislația în domeniul securității cibernetice pentru a asigura un nivel ridicat de protecție în întreaga UE.

Mijloacele și instrumentele UE utilizate în lupta împotriva amenințărilor cibernetice

1 CERT-urile europene

Centrele regionale de răspuns la incidente cibernetice certifică și coordonează măsuri la nivel local pentru combaterea amenințărilor cibernetice.

2 Europol

Europol oferă sprijin tehnic și operațional pentru investigarea infracțiunilor cibernetice și întreprinde acțiuni de combatere a rețelelor criminale.

3 ENISA

Agenția Europeană pentru Securitate Cibernetică oferă asistență tehnică și promovează bune practici în securitatea cibernetică în UE.

Educația și conștientizarea privind securitatea cibernetică în UE

1

Programe educaționale

Se promovează învățarea despre securitatea cibernetică în școli și universități pentru a dezvolta competențe și conștientizare.

2

Kampanii de informare

Se desfășoară kampanii de informare pentru cetățeni și companii pentru a reduce riscul de căderi victime ale amenințărilor cibernetice.

3

Platforme de formare online

Există resurse și platforme de formare online pentru a învăța despre securitatea cibernetică și a obține certificări relevante.

Tendințe și provocări actuale în combaterea amenințărilor cibernetice în UE

Inteligenta artificiala și automatizarea

Amenințările cibernetice devin din ce în ce mai sofisticate, iar utilizarea inteligenței artificiale și a automatizării poate spori capacitatea de detectare și răspuns.

Cloud computing și IoT

Creșterea utilizării serviciilor cloud și a dispozitivelor Internet of Things (IoT) necesită măsuri suplimentare pentru protejarea datelor și a infrastructurii.

Colaborarea public-privat

O strânsă colaborare între întreprinderi și autorități este este crucială pentru a combate amenințările cibernetice și a asigura o protecție eficientă.

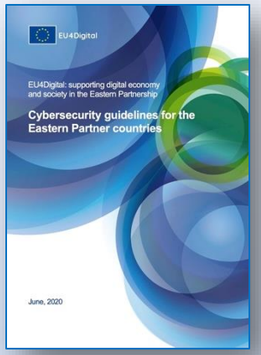
Concluzii:

- Modalitățile Uniunii Europene de a combate amenințările cibernetice reprezintă un pas semnificativ în direcția asigurării securității cibernetice într-un mediu tot mai interconectat și digitalizat.

- Abordarea UE, care se bazează pe colaborare, reglementare și cooperare internațională, reflectă necesitatea de a combate amenințările cibernetice la nivel global.

- Prin inițiative precum Directiva NIS, CERT-urile europene și investițiile în cercetare și dezvoltare în domeniul cibernetic, UE creează un cadru solid pentru prevenirea și gestionarea atacurilor cibernetice.

- În concluzie, abordarea UE în combaterea amenințărilor cibernetice reprezintă un efort concret de a proteja infrastructura digitală, datele și cetățenii europeni. Cu toate că provocările în domeniul cibernetic sunt în continuă evoluție, UE demonstrează angajamentul său pentru a rămâne la înălțimea acestor provocări prin promovarea securității cibernetice și colaborarea cu partenerii săi internaționali pentru a face față acestor amenințări la nivel global.



Bibliografie:

- **Securitatea cibernetică: în ce fel combate UE amenințările cibernetice : https://www.consilium.europa.eu/ro/policies/cybersecurity/**

- **Noua strategie de securitate cibernetică a UE**: https://dnsc.ro/citeste/noua-strategie-de-securitate-cibernetica-ue

- **Orientări privind securitatea cibernetică pentru țările partenere din est https://eufordigital.eu/ro/library/cybersecurity-guidelines-for-the-eastern-partner-countries/**

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ