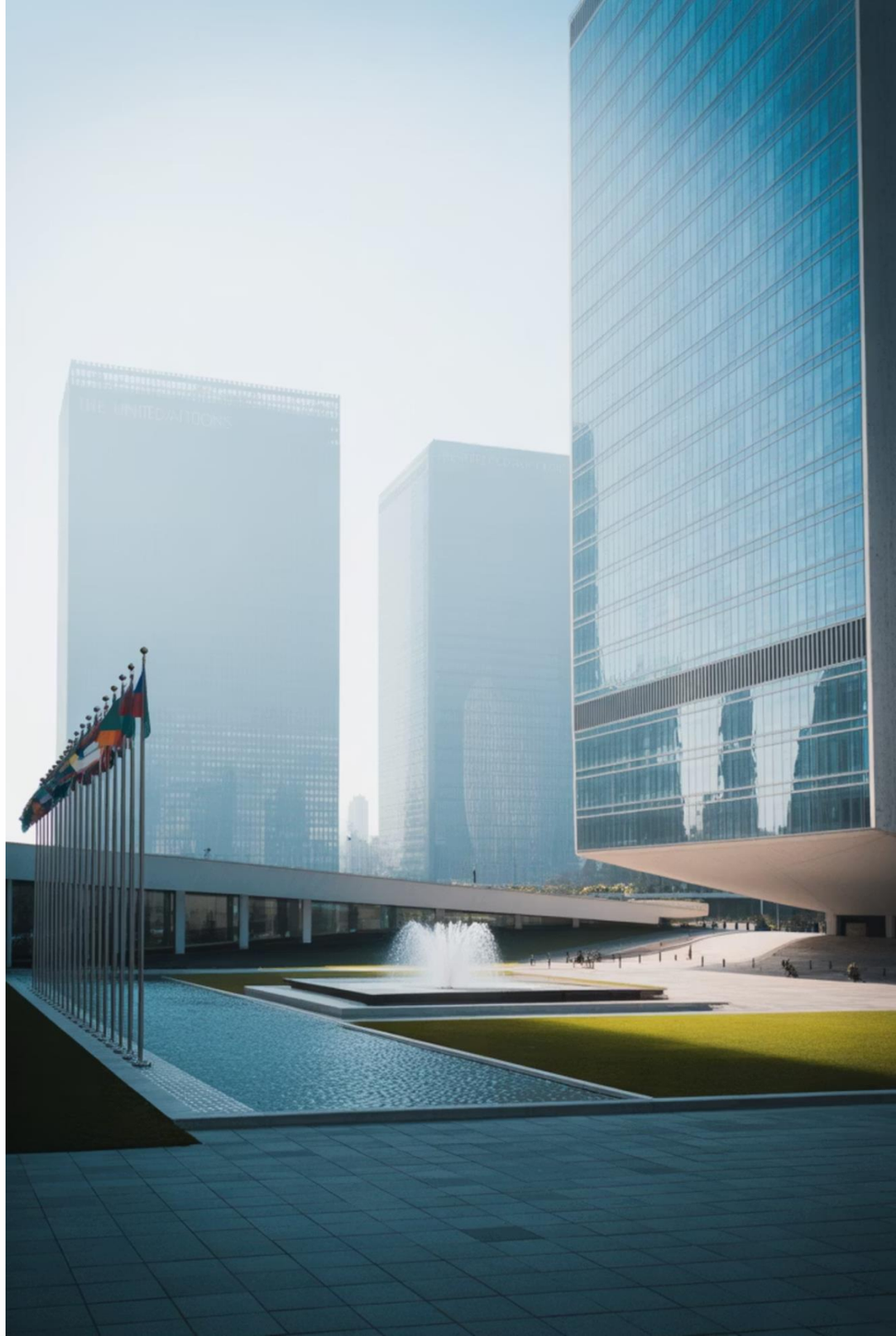
Arhitectura sistemului de guvernanță globală în secolul XXI-lea: provocări și tendințe pentru mediul internațional de securitate

Prezentare elaborată de **Dr. Busuncian Tatiana**, conferențiar universitar

Chișinău, 2025



Structura cursului

1 **Guvernare și guvernanță: delimitarea guvernanței globale**

Concepte fundamentale, actori principali și evoluția sistemului internațional

2 **Surse și resurse de putere în guvernanța globală**

Analiză a elementelor care constituie puterea în contextul internațional actual

3 **Reconfigurarea ordinii multilaterale**

Transformări structurale la începutul secolului XXI
și impactul asupra securității globale

4 **Provocări la adresa arhitecturii sistemului de guvernanță globală**

Identificarea și analiza amenințărilor contemporane la nivel global

5 **Tendințe strategice ale organizațiilor internaționale**

Direcții de acțiune pentru consolidarea securității globale în secolul XXI

Obiective de referință

- Analizarea arhitecturii instituționale a sistemului de relații internaționale
- Înțelegerea conceptelor specifice proceselor de guvernanță la nivel internațional
- Explicarea guvernanței globale prin prisma conceptelor, principiilor și actorilor internaționali
- Evaluarea impactului guvernanței politice globale în gestionarea inegalităților sociale

Transformări majore în mediul contemporan de securitate

Evenimente determinante pentru configurația actuală:

Sfârșitul Războiului Rece
A restructurat fundamental relațiile internaționale și dinamica de putere globală

Evenimentele de la 11 septembrie 2001
Au reorientat prioritățile de securitate către combaterea terorismului internațional

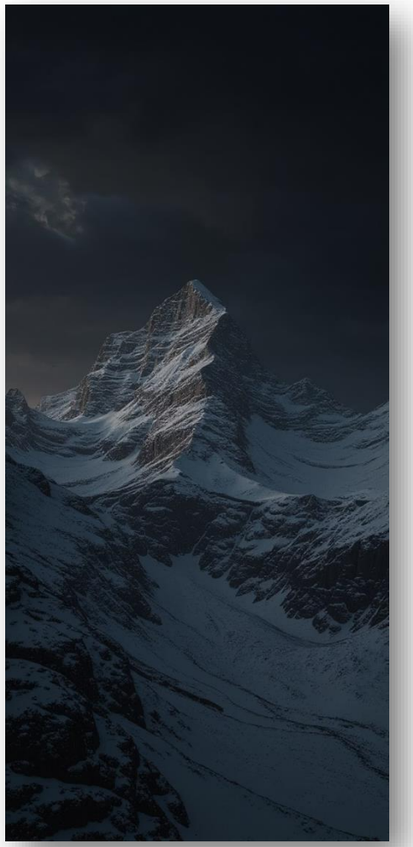
Secolul al XXI-lea se caracterizează printr-un mediu de securitate din ce în ce mai **fluid și flexibil**, cu multiple posibilități de evoluție, dependent de interesele actorilor statali și non-statali de pe arena internațională.

- Globalizarea și interconectarea economică și informațională
- Terorismul internațional și rețelele transnaționale
- Proliferarea armamentelor convenționale și neconvenționale
- Violența etnică și religioasă în diverse regiuni
- Probleme globale: sărăcie, foamete, educație deficitară, probleme de sănătate

Guvernare și guvernanță: delimitarea guvernanței globale

Conceptul de guvernanță globală

Guvernanța globală reprezintă **totalitatea proceselor și instituțiilor** formale și informale care ghidează și reglementează activitățile transfrontaliere, implicând actori statali și non-statali, în contextul unei lumi tot mai interconectate.



Evoluția amenințărilor după 2001

Războiul global împotriva terorismului a transformat fundamental mediul de securitate, generând noi tipare de cooperare internațională și reconfigurând prioritățile strategice ale actorilor globali.

> Principalele provocări ale mediului contemporan de securitate includ: globalizarea, terorismul, proliferarea armelor, violența etnică și religioasă, sărăcia, foametea, degradarea educației și sănătății.

Globalizarea terorismului impune statelor **noi nevoi de politici de securitate și apărare comune**, în contextul extinderii fără precedent a fenomenului terorist.

Confruntări militare și focare de conflict la nivel global

Campaniile militare din ultimul deceniu

- Campaniile din Irak și Afganistan, conduse de coaliții internaționale sub conducerea SUA
- Caracter **profund asimetric** al conflictelor
- Generarea de noi probleme de securitate fără soluții viabile în prezent

Tendințe de insecuritate în secolul XXI

Confruntări între marile puteri
Pentru supremație și resurse

Acțiuni ale actorilor nonstatali
Din sfera terorismului și criminalității

Conflicte de viziune
Între globalizare forțată și suveranitate națională

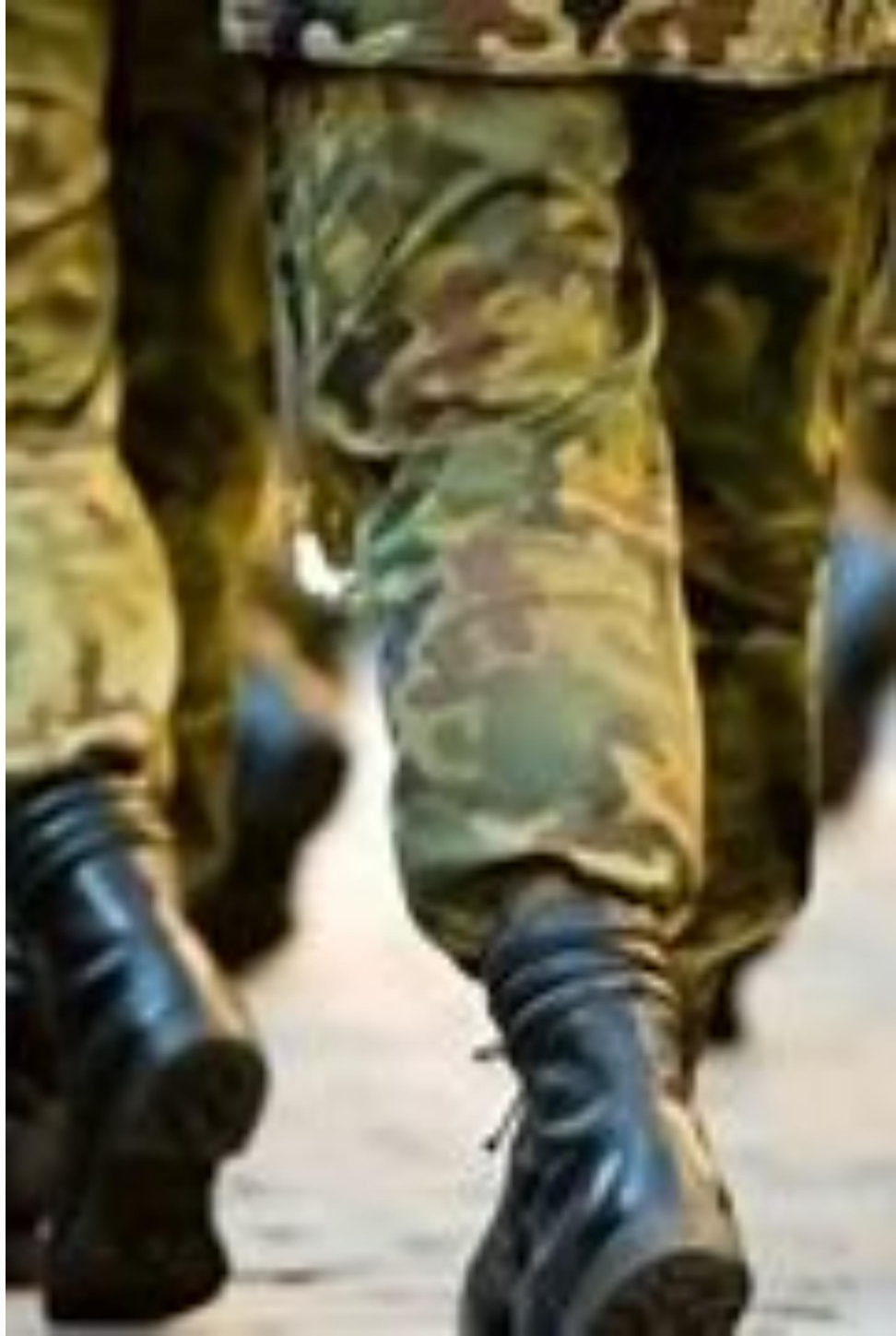
Tensiuni și focare de conflict

Conflicte latente și înghețate

Kosovo, Bosnia-Herțegovina, Cipru, Orientul Mijlociu, Transnistria, Caucazul de Nord și de Sud, Peninsula Coreea, Kashmir

Conflicte în desfășurare

Ucraina, Orientul Mijlociu, cu consecințe și finalitate încă greu de anticipat



Impactul asupra mediului de securitate global

Dimensiunile impactului conflictelor asupra securității globale

Caracter asimetric

Conflictele recente au demonstrat un caracter profund asimetric, generând probleme de securitate fără soluții viabile în prezent

Coaliții multinaționale

Tendința de formare a unor coaliții largi de state pentru combaterea amenințărilor globale

Anihilarea rețelelor teroriste

Eforturi concentrate pentru eliminarea infrastructurilor teroriste și stabilizarea regiunilor afectate

Cauzele globalizării și impactul asupra securității

Progresul tehnic și valoarea globală a informației –
Accelerarea schimbului de informații și tehnologizarea societății

Caracterul transfrontalier al economiei –
Apariția piețelor financiare globalizate și a alianțelor strategice globale

Ofensiva frontierei democratice –
Expansiunea valorilor democratice dincolo de frontierele politice limitate

Interdependența statală –
Dezvoltarea rețelelor globale și creșterea interdependenței în diverse industrii

Efectele globalizării asupra securității cibernetice

Directiva NIS

Se referă la securitatea rețelelor și a sistemelor informatice la nivel european și introduce norme obligatorii pentru statele membre. Acest cadru legislativ reprezintă un pas important în consolidarea rezilienței cibernetice la nivel continental.

Regulamentul GDPR

Protejează datele personale și impune responsabilități clare asupra operatorilor de date. GDPR a revoluționat modul în care organizațiile publice și private abordează confidențialitatea și securitatea datelor personale în era digitală.

Pachetul de măsuri privind securitatea cibernetică

Aceste măsuri vizează întărirea cooperării, sporirea rezilienței cibernetice și consolidarea capacității de răspuns la incidente în UE. Implementarea acestora contribuie la o abordare coordonată a amenințărilor cibernetice.

Aceste reglementări europene reprezintă piloni esențiali în construirea unui **spațiu digital securizat** și în răspunsul la provocările cibernetice generate de globalizare. Ele formează baza pentru o abordare coordonată la nivel european a amenințărilor cibernetice tot mai complexe.

Colaborarea între statele membre UE în combaterea amenințărilor cibernetice

Echipe de răspuns la incidente

Statele membre cooperează prin **schimbul rapid de informații** și coordonarea acțiunilor împotriva atacurilor cibernetice. Aceste echipe specializate asigură primul nivel de apărare în fața amenințărilor cibernetice emergente.

Exerciții și conferințe

Exerciții periodice și conferințe internaționale facilitează **schimbul de bune practici** și dezvoltarea de expertiză în securitatea cibernetică. Acestea contribuie la consolidarea capacităților de răspuns colectiv.

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. Acest proces este esențial pentru o abordare coerentă la nivel european.

Colaborarea transfrontalieră reprezintă unul dintre cele mai eficiente instrumente în combaterea amenințărilor cibernetice, care prin natura lor depășesc granițele naționale și necesită un răspuns coordonat.

Mijloacele și instrumentele UE utilizate în lupta împotriva amenințărilor cibernetice

CERT-urile europene 1

Centrele regionale de răspuns la incidente cibernetice certifică și coordonează măsuri la nivel local pentru combaterea amenințărilor cibernetice. Acestea formează o rețea interconectată de expertiză și răspuns rapid.

- Monitorizare în timp real a amenințărilor
- Răspuns coordonat la incidentele majore
- Asistență tehnică pentru organizațiile afectate

Europol

Europol oferă sprijin tehnic și operațional pentru investigarea infracțiunilor cibernetice și întreprinde acțiuni de combatere a rețelelor criminale, reprezentând un pilon esențial în arhitectura de securitate cibernetică europeană. 2

- Coordonarea investigațiilor transfrontaliere
- Analiză criminalistică digitală avansată
- Combaterea fraudelor online și a criminalității informatice

ENISA

Agenția Europeană pentru Securitate Cibernetică oferă asistență tehnică și promovează bune practici în securitatea cibernetică în UE, contribuind la elaborarea politicilor și standardelor în domeniu. 3

- Elaborarea de ghiduri și standarde
- Organizarea de exerciții de securitate cibernetică
- Certificarea produselor și serviciilor digitale

ENISA Threat Landscape 2025. https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf

Educația și conștientizarea privind securitatea cibernetică în UE

Programe educaționale

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

- Curricule specializate în securitate informatică
- Programe de studii universitare și postuniversitare
- Competiții și hackathoane educaționale

Campanii de informare

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

- Materiale informative accesibile publicului larg
- Zile europene ale securității cibernetice
- Parteneriate cu mass-media pentru diseminare

Platforme de formare online

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

- Cursuri gratuite pentru dezvoltarea competențelor de bază
- Simulări de atacuri cibernetice și exerciții practice
- Certificări recunoscute la nivel european

Educația și conștientizarea reprezintă **prima linie de apărare** împotriva amenințărilor cibernetice, iar UE investește resurse semnificative în aceste domenii pentru a crea o cultură a securității cibernetice în rândul cetățenilor și organizațiilor.

Tendințe și provocări actuale în combaterea amenințărilor cibernetice în UE

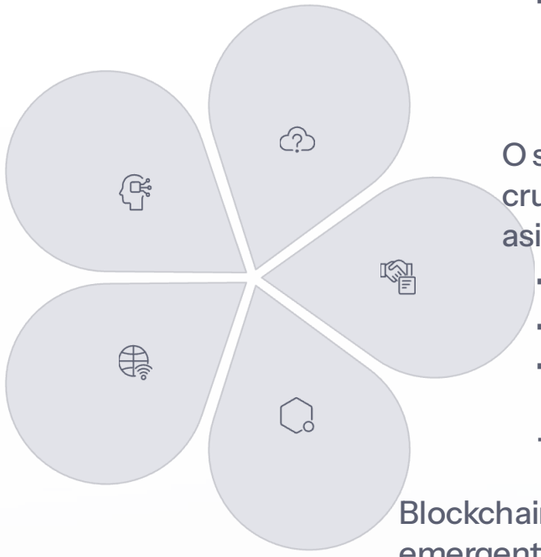
Inteligența artificială și automatizarea

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

- Algoritmi de detecție avansată a amenințărilor
- Sisteme autonome de răspuns la incidente
- Analiza predictivă a comportamentelor suspecte

Amenințări statale

Atacurile sponsorizate de state reprezintă una dintre cele mai sofisticate și persistente amenințări la adresa infrastructurilor critice și a instituțiilor strategice.



Cloud computing și IoT

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

- Securizarea dispozitivelor conectate
- Protecția datelor stocate în cloud
- Gestionarea riscurilor în ecosistemele complexe

Colaborarea public-privat

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

- Parteneriate strategice pentru securitate
- Schimb de informații despre amenințări
- Exerciții comune de simulare a atacurilor

Tehnologii emergente

Blockchain, criptografia cuantică și alte tehnologii emergente oferă noi oportunități pentru securizarea sistemelor, dar și noi provocări pentru specialiștii în securitate.

În contextul evoluției rapide a tehnologiei, UE trebuie să-și adapteze constant strategiile și instrumentele pentru a răspunde eficient la **peisajul amenințărilor în continuă schimbare**, menținând în același timp un echilibru între securitate și protecția drepturilor fundamentale.

Concluzii

Complexitate și dinamism

Sistemul de guvernanță globală în secolul XXI se confruntă cu o serie de provocări și tendințe care afectează mediul internațional de securitate, fiind caracterizat de o arhitectură complexă și în continuă schimbare.

Provocări multiple

Provocările sunt numeroase, de la terorism și proliferarea armelor până la amenințări cibernetice și schimbări climatice, necesitând abordări integrate și coordonate la nivel global.

Tendințe pozitive

Există tendințe pozitive, cum ar fi cooperarea multilaterală și implicarea actorilor non-statali în procesele de guvernanță globală, care pot contribui la gestionarea provocărilor contemporane.

Colaborare esențială

Este esențial ca statele, organizațiile internaționale și toți actorii relevanți să colaboreze pentru a construi un sistem de guvernanță globală mai eficient, capabil să răspundă provocărilor actuale și viitoare.

Arhitectura sistemului de guvernanță globală trebuie să evolueze pentru a asigura un **mediu internațional de securitate mai stabil și prosper**, adaptându-se la realitățile complexe ale secolului XXI.

Teme pentru lucrul individual

1 Arhitectura guvernanței globale în secolul XXI

O analiză a provocărilor și a tendințelor pentru securitatea internațională, cu accent pe transformările structurale și impactul lor asupra stabilității globale.

2 Provocări și tendințe în arhitectura sistemului de guvernanță globală

Implicații pentru mediul internațional de securitate, cu studii de caz relevante din diverse regiuni ale lumii.

3 Transformări în arhitectura guvernanței globale

Un impact asupra securității internaționale în secolul XXI, analizând rolul organizațiilor internaționale și al actorilor non-statali.

4 Evoluția sistemului de guvernanță globală

O analiză a provocărilor și a tendințelor pentru securitatea internațională, cu perspective istorice și previziuni pentru viitor.

5 Securitatea internațională în secolul XXI

O perspectivă asupra arhitecturii sistemului de guvernanță globală, examinând interacțiunea dintre dimensiunile politice, economice și sociale ale securității.

Lucrările vor fi elaborate utilizând minimum 10 surse bibliografice relevante și actuale, respectând normele academice de citare și redactare.