Securitatea Internațională în era tehnologiilor emergente

Autor: T. Busuncian
Dr., conferențiar universitar

Chișinău 2026

Conținuturi; Termeni-cheie

Conținuturi:

1. Noile tehnologii emergente -riscuri și vulnerabilitățiI la adresa securității internaționale.
2. Competiția dintre marile puteri în domeniul noilor tehnologii emergente și implicațiile pentru mediu de securitate internațional;
3. Noile tehnologii și securitatea internațională: efecte și evoluții;
4. Răspunsul multidimensional internațional la provocările emergente

Termeni-cheie: tehnologii emergente, securitate internațională, riscuri, amenințări și vulnerabilități în era digitală, inteligență artificială, securitate cibernetică etc.

Noile tehnologii emergente -riscuri și vulnerabilității la adresa securității internaționale

Înțelegerea securității internaționale și a tehnologiilor emergente este esențială pentru a naviga în lumea contemporană plină de provocări și oportunități. Securitatea internațională se referă la eforturile de menținere a păcii și a stabilității la nivel global, abordând amenințări precum conflictele armate, terorismul, proliferarea armelor de distrugere în masă și securitatea cibernetică.

Pe de altă parte, tehnologiile emergente includ inovațiile și progresele tehnologice recente care pot influența semnificativ domeniul securității internaționale, cum ar fi inteligența artificială, biotehnologia, securitatea informației și

Soluția la sarcina complexă de a asigura securitatea ar trebui să preia un caracter complet nou, în raport cu metodele și mijloacele tradiționale de securitate a informațiilor. Securitatea informațională necesită crearea de noi tehnologii integrate pentru stocarea și protejarea resurselor informaționale, dezvoltarea suplimentară sau îmbunătățirea schemelor și procedurilor organizaționale existente menținerea integrității resurselor informaționale, instruirea personalului specializat pentru soluții la provocări.

Statele din Europa de Est, Federația Rusă și alte țări cu o pondere considerabilă în sectorul informațional, la fel acordă o importanță deosebită asupra subiectului securității informaționale. Se poate menționa nivelul ridicat al activității serviciilor de informații în contextul rivalităților dintre state, la început în perioada războiului rece, iar mai târziu, odată cu procesul de globalizare și în domeniul informațional.

Prin sintagma securitate informațională se are în vedere protecția persoanei, societății și a statului, a drepturilor și intereselor acestora în domeniul informațional. Aceste aspecte sunt stipulate, de altfel, și în Constituția Republicii Moldova și alte legi, privind drepturile și interesele ce țin de căutarea, primirea, transmiterea, răspândirea, formarea, prelucrarea, păstrarea, utilizarea și protecția informației.

În prezent, la nivel internațional se vehiculează mai mulți termeni similari, cum ar fi:

- securitatea informației;
- securitatea informațională;
- și securitatea cibernetică.

Dar pot oare aceste concepte să se substituie unul pe altul sau sunt diferite? Și la nivel național multă lume întâmpină dificultăți majore în ce privește înțelegerea și aplicarea corectă a acestor concepte, care, în funcție de context, uneori pot fi considerate ca sinonime, alteori pot fi diferite, inclusiv ca sarcini, funcții, impact, arie de acoperire etc. Cercetările în domeniu urmăresc să ducă o mai bună înțelegere și conștientizare a terminologiei, fiind utilă pentru persoanele implicate în activități educaționale (elevi, studenți, profesori, doctoranzi), pentru cei angajați în activități informaționale și/sau de securitate a informației.

Securitatea informațională – al treilea val în dezvoltarea omenirii – constituie rezultatul procesului de informatizare de o mare amploare și de o aprofundare perpetuă ce se manifestă ca una din legitățile progresului social și a celui tehnico-științific.

Termeni cheie în securitatea informațională

Securitatea informației:

Protecția datelor și a sistemelor informatice împotriva accesului neautorizat, modificării sau distrugerii.

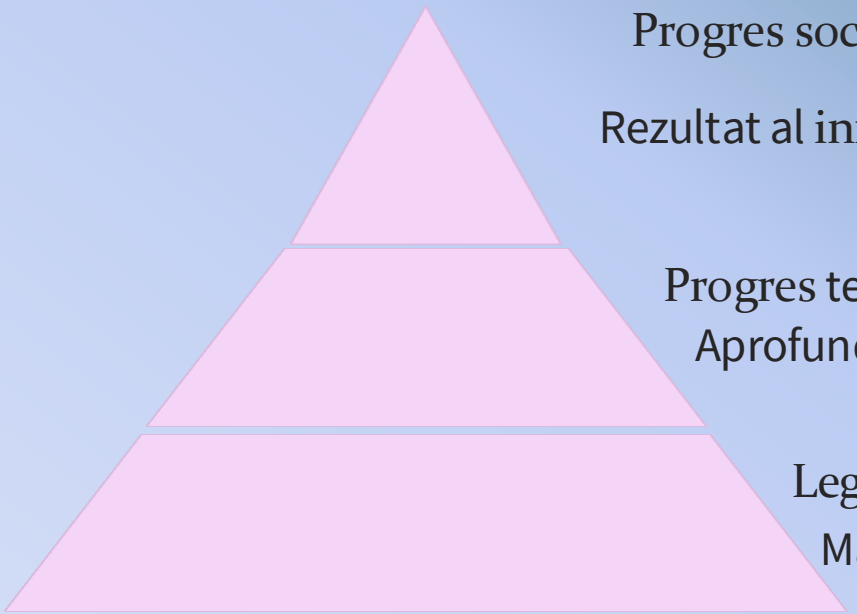
Securitatea cibernetică:

Focalizată pe protecția sistemelor, rețelelor și programelor digitale împotriva atacurilor cibernetice.

Securitatea informațională:

Concept mai larg care include și aspecte sociale, politice și economice ale securității în era informațională.

Securitatea Informațională - al treilea val în dezvoltarea omenirii



Progres social

Rezultat al informatizării la scară largă

Progres tehnico-științific

Aprofundare perpetuă a tehnologiilor

Legitimitate socială

Manifestare a dezvoltării societăţii

Securitatea informațională reprezintă o etapă crucială în evoluția societății, reflectând progresul tehnologic și social al umanității.

Securitatea informațională se studiază, tradițional, în termeni de amenințări și vulnerabilități, dar propune abordarea securității în sensul mai larg al termenului, ca o stare a unui subiect care se estimează neamenințat de un oarecare pericol sau gândește la mijloacele de a răspunde la pericol, dacă el poate deveni actual. Amenințările informaționale presupun influențe asupra sferelor informaționale care atentează la stabilitatea, securitatea națională și politică a statului. Agresiunile informaționale în lanț se pot constitui într-un război informațional, la care pot participa din umbră și serviciile specializate de informații din străinătate. Asigurarea securității informaționale presupune un efort comun între serviciile de informații, mediile academice și organizațiile neguvernamentale.

Exemplele în acest sens sunt numeroase: în contextul emergenței riscurilor la adresa securității cibernetice, un serviciu de informații poate fi eficient doar în cooperare cu zona privată, de business și de cercetare în materie de protecție a infrastructurilor informatice; evaluarea percepțiilor asupra unor evoluții geopolitice ar fi mai exactă în urma organizării unor dezbateri publice în domeniul analizei de risc; fundamentarea academică a domeniului.

Cum influențează tehnologiile emergente în securitatea internațională

Transformarea naturii conflictelor

Tehnologiile emergente estompează liniile dintre război și pace. Războaiele hibride, care combină tactici militare convenționale cu atacuri cibernetice, dezinformare și presiune economică, devin norma. Actorii non-statali, precum grupările teroriste sau hackerii, au acces la tehnologii care le permit să provoace daune semnificative, amplificând amenințările asimetrice. Conflictele se mută în spațiul cibernetic, unde atacurile pot viza infrastructura critică, instituțiile financiare sau chiar procesele electorale. Dronele și sistemele autonome permit războaie purtate la distanță, reducând riscul pentru propriile trupe, dar ridicând probleme etice complexe. Viteza cu care se desfășoară informațiilor.

Modificarea balanței de putere

Tehnologiile emergente pot schimba raportul de forțe dintre state. Statele mici pot investi în capacități asimetrice, cum ar fi atacurile cibernetice, pentru a compensa dezavantajele militare convenționale. Competiția tehnologică dintre marile puteri, în special SUA și China, devine un factor determinant în peisajul geopolitic. Tehnologiile de supraveghere în masă oferă statelor instrumente puternice de control, dar ridică și probleme legate de drepturile omului și libertățile civile.

În legislația mai multor țări „securitatea informațională” este orientată spre:

Noi vulnerabilități

Dependența tot mai mare de sisteme tehnologice complexe creează noi vulnerabilități. Infrastructura critică, precum rețelele electrice, sistemele de transport și spitalele, devine expusă atacurilor cibernetice. Perturbarea acestor servicii esențiale poate avea consecințe devastatoare. Dezinformarea și manipulare online, facilitate de tehnologii precum deepfakes, pot destabiliza societățile și influența procesele politice. Amenințările biologice sintetice, create prin inginerie genetică, reprezintă un pericol major, greu de controlat și cu potențial pandemic.

Schimbări în strategiile de securitate

Statele trebuie să-și adapteze strategiile de securitate pentru a face față noilor amenințări. Rezilienta și adaptabilitatea devin esențiale. Investițiile în cercetare și dezvoltare tehnologică sunt cruciale pentru a menține un avantaj competitiv. Cooperarea internațională este necesară pentru a stabili norme și reglementări în spațiul cibernetic și pentru a combate amenințările transnaționale. Doctrinele militare trebuie actualizate pentru a integra noile tehnologii și tactici de război. Securitatea cibernetică devine o prioritate absolută.

Provocări pentru guvernare

Tehnologiile emergente ridică provocări complexe pentru guvernare. Este nevoie de noi cadre legale pentru a reglementa spațiul cibernetic, a controla armele autonome și a proteja datele personale. Dilemele etice legate de utilizarea inteligenței artificiale în domeniul militar și al supravegherii necesită o dezbatere publică amplă. Cooperarea internațională este esențială pentru a stabili standarde și a asigura un mediu digital sigur și stabil.

Oportunități pentru securitate

Tehnologiile emergente oferă și oportunități pentru îmbunătățirea securității. Inteligența artificială poate fi utilizată pentru a detecta amenințările mai rapid și mai eficient

Tendințe de viitor

Inteligența artificială, computația cuantică, biotehnologiile avansate, noile tehnologii spațiale și sistemele autonome vor continua să evolueze rapid, transformând profund peisajul securității internaționale. Este esențial să anticipăm aceste schimbări și să ne adaptăm continuu pentru a face față noilor provocări și oportunități.

Globalizarea afectează sistemul informațional într-o mulțime de aspecte precum utilizarea internetului de către publicul larg din lume, furnizorii globali de e-mail, rețele de socializare conectează întreaga lume. Sistemele informaționale au un rol important în globalizare prin influențarea diferitelor culturi prin intermediul internetului, unde economiile mari și țările dezvoltate beneficiază cel mai mult de acest lucru. Globalizarea a revoluționat managementul intern. De asemenea, a facilitat interacțiunea dintre țări, regiuni și continente, contribuind astfel la rentabilitate. Filosofia serviciilor de informare la fel a fost afectată ca rezultat a globalizării.

În cadrul societății informaționale, a estima puterea și viabilitatea sistemului de securitate națională fără a lua în considerare sistemele informaționale și modul de exploatare a informației:

Colectarea; protecția; transportul; managementul și împiedicarea accesului la informație - reprezintă un risc major.

Noile tehnologii și securitatea internațională: efecte și evoluții

Secolul XXI poate fi numit cu drepturi secolul Societății Informaționale, având în vedere schimbările semnificative în comportamentul și relațiile interumane generate de dezvoltarea tehnologiilor digitale. Indiferent de cât de des sau intens se utilizează tehnologiile moderne de comunicare, abilitățile individuale de comunicare rămân factori critici pentru succesul în diverse activități și procese

Începând cu anii ’50 ai secolului XX, dezvoltarea tehnologiilor informaționale și a mijloacelor de comunicare electronice, a reprezentat o revoluție în accesul la informație, oferind posibilități rapide și eficiente de colectare, stocare, organizare, procesare, prezentare și transmitere a datelor în format electronic, fără limite spațiale sau temporale. Schimbările respective au transformat ftotalment modul în care oamenii interacționează cu informația și cum aceasta este utilizată în diverse domenii ale vieții moderne.

Este important de menționat că rolul acestor tehnologii nu este să înlocuiască omul cu o „mașină cibernetică”, ci să faciliteze și să îmbunătățească activitățile umane prin automatizare și eficiență. Capacitatea de a accesa rapid și precis informații esențiale a devenit crucială în mediul contemporan, influențând sectoare variate precum educația, sănătatea, afacerile și guvernarea. În secolul XXI tehnologia informației și comunicațiilor s-a schimbat semnificativ, dezvoltând și implementând noi sensuri ale comunicației

Noile tehnologii și securitatea internațională: efecte și evoluții

- asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice;
- asigurarea securității spațiului informațional-mediatic;
- consolidarea capacităților operaționale;
- Eficientizarea procesului de coordonare internă și cooperare internațională în domeniul securității informaționale.

Concluzii:

Domeniul securității informaționale capătă proporții mondiale, iar cercetătorii tind spre definirea cât mai exactă a subiectului dat. Securitatea informațională ca parte componentă a sistemului național de securitate este o temă relativ nouă, însă vitală pentru asigurarea stabilității statale. Chiar și cele mai puțin dezvoltate state se ciocnesc cu subiectul progresului tehnologic, iar acest factor determină aprofundarea studiului în vederea teoretizării domeniului dat, astfel încât să nu devină periculos pentru instituțiile naționale sau internaționale și respectiv societatea civilă.

Problema securității informaționale este determinată nu doar numai de procesele de transformare, globalizare, regionalizare, dar și de criza globală, care înaintează problema încrederii în procesul de conlucrare într-o lume tot mai interdependentă și imprevizibilă. Ca rezultat al globalizării factorilor economici, politici și militari, al expansiunii rețelelor și sistemelor informaționale globale, guvernele lumii, instituțiile și organizațiile internaționale sunt nevoite să-și concentreze și mai mult eforturile spre asigurarea unei securități globale, pentru că la momentul actual riscurile și amenințările sunt tot mai mari, datorită efectului de propagare în lanț.

Concluzii:

În secolul XXI o multitudine de sectoare precum transporturile, sănătatea, energia, economia devin dependente de tehnologiile digitale pentru a-și asigura buna funcționare de zi cu zi. Digitalizarea oferă un șir de beneficii, sporind operativitatea cu care lucrurile se pot desfășura, dar în același timp expune societatea la riscuri și amenințări informaționale.

Până la apariția rețelelor globale, asigurarea securității sistemelor informaționale era o problemă de politică la nivel național, la momentul actual, la stabilirea strategiilor și politicilor de securizare a spațiului informațional trebuie luate în considerare și aspectele de compatibilizare și standardizare la nivel global.

Sarcini de autoevaluare

- Dezvoltați competențe în evaluarea riscurilor și vulnerabilităților asociate cu tehnologiile emergente;
- Dezvăluiți capacitatea de a gândi critic și de a evalua argumente complexe legate de utilizarea tehnologiilor în scopuri militare;
- Distingți contextul geopolitic global și a modului în care noile tehnologii influențează relațiile internaționale și echilibrul de putere;
- Analizați strategiile militare și de înțelegere a impactului tehnologiilor asupra securității naționale și internaționale.

Teme pentru lucrul individual:

- Impactul inteligenței artificiale (IA) asupra securității internaționale.
- Rolul organizațiilor internaționale în promovarea securității tehnologice.
- Impactul tehnologiilor emergente asupra conflictelor armate.
- Guvernanța tehnologiilor emergente și securitatea internațională.
- Impactul tehnologiilor emergente asupra securității umane.