SECURITATEA TEHNOLOGICĂ EMERGENTĂ

EMERGING TECHNOLOGICAL SECURITY

Colonel (r.) prof. univ. dr. ing. Eugen SITEANU*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)

***Rezumat**: Un domeniu nou de mare actualitate al securităţii este securitatea tehnologică.*

Securitatea tehnologică reprezintă un domeniu emergent care se impune astăzi pe scena internaţională; ea a devenit un instrument comun şi totodată o ţintă pentru puterile rivale.

***Cuvinte cheie**:securitate tehnologică, scenă globală, domeniu emergent, tehnologie disruptivă, ştiinţă.*

***Abstract**: A hot new area of security is technological security.*

Technological security is an emerging field that is imposing itself on the international scene today; it has become both a common tool and a target for rival powers.

***Keywords**: technologycal security, global scene, emerging field, disruptive technology, science.*

Astăzi se vorbeşte frecvent despre noua abordare „a tehnologiei ca ameninţare şi arie individuală de securizare”[1].

Securitatatea tehnologică este tratată în următoarele documente strategice americane: Annual Threat Assessment of the US Intelligence Community (aprilie 2021); America's Place in the World (februarie 2021); A Foreign Policy for the American People (martie 2021); Analiza prospectivă Global Trends 2040. A more contested world, a National Intelligence Council (martie 2021). De asemenea şi în trei documente ale NATO este dezbătută problema securităţii tehnologice (The Secretary General Annual Report 2020; Evaluarea experţilor NATO 2030: United for a New Era, 25 noiembrie 2020; Analiza specifică pe noile tehnologii NATO 2030: new technologies, new conflicts, new partnerships, februarie 2021, NATO), precum şi în două documente ale UE (Cartea lui Joseph Borell Fontelles, European Foreign Policy in Times of Covid 19, Luxembourg, Publications Office of the European Union, 2021 şi studiul The geopolitical implications of the Covid 19 pandemic).

Totodată acest subiect este dezbătut şi în două documente britanice (Strategia integrată până în 2030 - Global Britain in a Competitive Age. The Integrated Review of Security Defence, Development and Foreign Policy şi strategia militară Defence in a competitive age, Ministry of Defence).

---

* Membru corespondent al Academiei Oamenilor de Ştiinţă din România, Secretar Ştiinţific al Secţiei de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, membru titular al Comitetului Român de Istoria şi Filosofia Ştiinţei şi Tehnicii (CRIFST) al Academiei Române, esiteanu@yahoo.com.

[1] Barry Buzan, „Popoarele, statele şi frica”, Editura Cartier, Chişinău, 2014, pp. 112-131.

Exprimările din aceste documente strategice se referă la unele concepte și nuanțe de interpretare a securității tehnologice - dovada faptului că acest concept este în dezvoltare, nefiind deocamdată definitivat. În documentele menționate se întâlnesc sintagme și concepte precum: tehnologia disruptivă și emergentă, putere științifică, dominație tehnologică, supremație tehnologică, superioritate tehnologică, leadership tehnologic, avantaj tehnologic, strategie tehnologică, schimbare, tranziție tehnologică, dezvoltare tehnologică, putere științifică și tehnologică, superputere științifică și tehnologică, efectele adverse ale tehnologiei etc.

Incontestabil, schimbarea tehnologică rapidă transformă știința și tehnologia „într-o formă de măsurare a puterii”[2].

Dincolo de aceste concepte și nuanțe, de interpretări și de „abordarea tematicii securității tehnologice, există o convergență deosebită a abordărilor, care se bazează pe câțiva piloni”[3]:

1) atât știința, cât și tehnologia sunt multiplicatori și referențiali de putere;

2) există azi o competiție a accesului la tehnologie ce conduce la conflicte/războaie, la posibilități mai mari de dezvoltare, precum și la dezvoltări de nișă ale țărilor care participă la reașezarea ierarhiei globale;

3) tehnologia nu reprezintă doar un avantaj care crează oportunități, ci poate fi și un dezavantaj, o vulnerabilitate și o sursă de amenințări la adresa securității omenirii;

4) tehnologia nouă crează alianțe în scopul schimbului tehnologic și constrângeri și limitări în ceea ce privește accesul la tehnologie;

5) a apărut un nou spațiu comun al avantajelor tehnologice vizate de referirea la securitatea tehnologică și anume: IT&C, AI, nanotehnologii, biotehnologii, big data, tehnologia spațială și cyber etc.;

6) nu există încă norme și limitări etice pentru noile tehnologii care ar putea deveni distructive;

7) goana după noile tehnologii ar putea însemna și goana după arma supremă pentru dominarea omenirii.

Rusia și China trebuie să fie luate în considerare cu unele nuanțe și diferențe între acești doi actori în ceea ce privește gradul de pericol implicat.

În continuare vom aduce câteva argumente pentru o securitate tehnologică a lumii.

Documentele strategice precedente evidențiază principalele evoluții globale care evocă perspectivele care impun definirea securității tehnologice.

Secretarul de stat al Apărării Regatului Unit, Ben Wallace, a declarat că puterea științifică a UK va susține avantajul strategic al UK. Iată de ce UK a adoptat deja o Strategie pentru știință și tehnologie (2020) și o Strategie industrială pentru apărare și securitate. Scopul acestora constă în

[2] Iulian Chifu, „Reconfigurarea securității și a relațiilor internaționale în secolul 21”, Volumul IV, *Războiul de agresiunea pe scară largă în Ucraina, în plin secol 21*, Editura Rao, București, 2023, p. 49.
[3] *Ibidem*, p. 49.

folosirea componentei tehnologice de vârf pentru construirea „capabilităților câștigătoare pentru viitoarele bătălii militare pentru a se adapta la amenințările globale generate, folosind tehnologii avansate”[4].

Și secretarul de stat Anthony Blinken a desemnat printre prioritățile politicii externe americane „*asigurarea leadership-ului în domeniul tehnologic: Puterile majore ale lumii concurează pentru a dezvolta și desfășura noi tehnologii (...) Dorim ca America să mențină avantajul tehnologic și științific*”[5].

Joe Biden a cerut numirea în Departamentul Securității Naționale a unui nou „adjunct responsabil pentru coordonarea componentei cibernetice și de tehnologii emergente și lansarea unei inițiative urgente pentru a îmbunătăți capabilitățile, pregătirea și reziliența în spațiul cibernetic”[6].

De asemenea și Boris Johnson a specificat apariția programului de modernizare în scopul acoperirii noilor domenii, cibernetic și spațial, pentru echiparea forțelor armate cu tehnologie de vârf[7]. El a declarat că UK „*va deveni o Superputere Științifică și Tehnologică în 2030*” și se va transforma „*într-un hub pentru servicii globale, digitale și de date, investind în una dintre cele mai importante avantaje de forță, tehnologiile digitale, dar și prin atragerea investițiilor*”[8].

În ceea ce privește securitatea tehnologică, NATO Allied Command Transformation „ a lansat o foaie de drum pentru Tehnologiile Emergente și Disruptive încă din 2018 pentru a evalua impactul evoluțiilor rapide și a revoluțiilor în domeniul tehnologiei”[9].

Studiul National Intelligence Council al SUA „Global trends 2040” a introdus tehnologiile disruptive la capitolul provocărilor globale, dar și „conceptul de supremație tehnologică prin dezvoltare, prin transformarea experiențelor umane și a capabilităților și aplicațiilor, adoptarea rapidă a acestora și prin crearea unor noi tensiuni și rupturi între diferiții actori pe baza competiției pentru această supremație”[10].

În acest scop se impune leadership-ul tehnologic întrucât aceia care investesc acum în tehnologii de vârf vor fi liderii tehnologici în anul 2040. Numai coordonarea și conlucrarea între guverne și corporații private poate asigura o competiție cu șanse reale de reușită contra economiilor centralizate de stat.

Un alt argument pentru necesitatea securității tehnologice vine de la amenințările care au legătură cu noile tehnologii, iar cea mai mare

---

[4] *Ibidem*, p. 50.
[5] Anthony Blinken, „A Foreign Policy for the American People.”, disponibil la https://www.state.gov/a-foreign-policy-for-the-american-people/, accesat la 27.02.2024.
[6] America's Place in the World, disponibil la https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/, accesat la 27.02.2024.
[7] Iulian Chifu, *op. cit.*, pp. 51-52.
[8] *Ibidem*, p. 52.
[9] *Ibidem*.
[10] *Ibidem*, p. 53.

amenințare o constituie pierderea avantajului strategic prin știință și tehnologie.

Regatul Unit (UK) „își asumă o poziție activă și în domeniul studiilor prospective, pentru a participa la definirea ordinii internaționale a viitorului”[11].

Printre amenințările legate de securitatea tehnologică sunt comportamentele agresive în spațiul cosmic și în cel cibernetic, folosirea lipsită de etică a tehnologiilor etc.

Principala amenințare vine dinspre Rusia și China, țări care investesc în dezvoltare pentru a detrona Occidentul prin transferul tehnologic ilegal și furtul de proprietate intelectuală pentru a declanșa noi atacuri cu rachete hipersonice și operațiuni hibride. Tehnologiile de vârf (noi) vor schimba natura războiului și vor juca un rol esențial în spațiul cosmic, iar noile amenințări vin în special dinspre tehnologia de vizualizare modernă, cea de IT&C și utilizarea tehnologiilor emergente în operațiuni hibride.

Alte amenințări sunt cele la adresa protecției vieții private, la adresa democrației și securității lumii. De aceea „salvgardarea securității naționale înseamnă astăzi investițiile în capabilități tehnologice”[12].

Comunitatea de intelligence a SUA, evaluând amenințările, a menționat și amenințările cibernetice la adresa drepturilor omului. Nu trebuie uitate nici amenințările percepute la limitarea libertății de opinie de către marile corporații tehnologice.

Comisia AFET a Parlamentului European a elaborat un studiu privind normele și standardele în domeniul Artificial Intelligence (AI) și folosirea Big Data explicând că „China, Rusia și SUA s-au grăbit să aplice capitalismul sălbatic în materie de date și să perfecționeze tehnologia represivă”[13].

Este posibilă amenințarea unor noi tensiuni și rupturi în și între societăți, industrii și state deoarece în următoarele două decenii tehnologia urmează să transforme și să îmbunătățească experiența umană și capabilitățile în domeniul îmbătrânirii, schimbărilor climatice și măririi productivității[14].

Dominația tehnologică se manifestă în primul rând prin rivalitatea/concurența SUA-China, însă în această competiție se vor adăuga unele companii private cu viziune strategică și resurse enorme.

La amenințările actuale, NATO a invocat tehnologiile emergente și disruptive care se impun ca relevante, revoluția tehnologică și schimbările

---

[11] Ministry of Defence, Defence in a competitive age, disponibil la https://www.gov.uk/-government/publications/defence-in-a-competitive-age, accesat la 27.02.2024.

[12] Anthony Blinken, A Foreign Policy for the American People, disponibil la https://www.state.gov/a-foreign-policy-for-the-american-people/, accesat la 27.02.2024.

[13] European Parliament, The geopolitical implications of the Covid-19 pandemic, disponibil la https://www.europarl.europa.eu/RegData/etudes/STUD/2020/603511/EXPO_STU-(2020)603511_EN.pdf, accesat la 28.02.2024.

[14] National Intelligence Council, Global Trends 2040. A more contested World, disponibil la https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf, accesat la 28.02.2024.

pe termen mediu și lung (produsul dezvoltării și difuzării tehnologiilor, acesta fiind un proces lung și complex care necesită investiții suplimentare). În ceea ce privește păstrarea avansului tehnologic, evaluarea NATO cuprinde „două obiective: 1) păstrarea leadership-ului pentru cea de-A Treia Revoluție industrială și consolidarea leadership-ului pentru cea de-A Patra Revoluție Industrială, care va urma”[15].

O altă amenințare este aceea că tehnologiile emergente sunt neguvernate atât de legi și norme cât și de utilizarea lor agresivă și de riscul competiției care pot provoca conflicte/războaie.

Raportul World Economic Forum aduce în prim plan amenințările specifice despre relevanța globală și echitate. Accesul la tehnologia de vârf a unor state constituie o amenințare care ar putea mări distanța dintre aceia care au și cei care nu dețin resurse relevante[16]. Acest document prezintă riscuri economice ce se referă la efectele adverse ale tehnologiei, la fragilitatea economică și la diviziuni sociale care probabil vor crește. În raport se mai exemplifică unele amenințări cum ar fi de exemplu lărgirea faliei digitale dintre diverse țări ori în interiorul acestora și creșterea dependenței digitale, precum și accelerarea automatizării, manipularea și blocarea informației, diferențele de abilități și capabilități tehnologice între diferitele state[17].

În documentele NATO se prezintă „rolul semnificativ al spațiului cosmic ca domeniu operațional al Alianței, transferurile tehnologice în cadrul Alianței, tehnologia în comunicații și vizualizarea modernă”[18]. Și SUA notează AI, quantum computers, tehnologia energiilor curate, biotehnologia, nanotehnologia și telecomunicațiile generației viitoare (5G)[19].

UE reține securitatea cibernetică, dronele, siguranța rețelelor și tehnologia cuantică, precum și crearea unor surse alternative la cele din China în privința furnizării de tehnologie 5G[20].

Global Trends - varianta americană - notifică AI, biotehnologia, materiale și produse manufacturiere bazate pe nanotehnologie și crearea viitoarei lumi hiperconectate a viitorului. NATO menține în prim-plan AI, autonomie, robotică, big data, quantum computing, comunicațiile 5G și crearea unor domenii tehnologice noi. SUA vizează securitatea tehnologică cu câteva domenii: fundamentele care țin de tehnologia computerelor, construcția manufacturieră domestică - capacitatea de a produce computere

---

[15] Iulian Chifu, *op. cit.,* p. 56.

[16] World Economic Forum, The Global Risks Report 2021, disponibil la https://www.-weforum.org/publications/the-global-risks-report-2021/, accesat la 28.02.2024.

[17] Iulian Chifu, *op. cit.*, p. 57.

[18] NATO - 2030. United for a New Era, disponibil la https://www.nato.int/nato_static_-fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, accesat la 28.02.2024.

[19] President Joseph R. Biden, Interim National Security Strategic Guidance, disponibil la https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf, accesat la 28.02.02.2024.

[20] Iulian Chifu, *op. cit.*, p. 58.

acasă. Crearea standardelor tehnologiilor emergente e importantă ca și apărarea lanțurilor de furnizori critici de încredere și infrastructura tehnologică. NATO are ca obiectiv exploatarea tehnologiei noi și disruptive prin inovație, înbunătățirea datelor, AI, autonomia, sistemele hipersonice, tehnologiile cuantice, biotehnologiile etc. NATO a evaluat noile tehnologii şi impactul tehnologiilor disruptive asupra dezvoltării capabilităților NATO şi a analizat pregătirea pieței pentru a absorbi tehnologii critice (AI, viteza hipersonică, biotehnologiile, tehnologiile cuantice, telecomunicațiile 5G și 6G)[21].

Regatul Unit va deveni o putere cibernetică responsabilă și o putere științifică și tehnică globală, deoarece „schimbările tehnologice rapide fac ca știința și tehnologia să devină punct-reper care măsoară puterea în viitor”[22].

China și Rusia sunt principalii competitori în domeniul tehnologic ai Occidentului. China ținteşte sectoarele tehnologice-cheie ale SUA, pe proprietarii de tehnologii militare și comerciale americani, dar și aliați, precum și instituțiile de cercetare asociate cu zonele apărării, energiei, finanțelor etc. Utilizând instrumente precum investiții publice, spionaj, furt pentru a-și dezvolta capabilitățile tehnologice, China urmărește să controleze domeniul tehnologic.

China urmărește să obțină controlul intern bazat pe tehnologie și expansiunea autoritarismului fundamentat pe tehnologie în lumea întreagă, precum și leadership-ul în unele tehnologii emergente până în anul 2030 pe baza resurselor și unei strategii comprehensive de a folosi tehnologie în scopul îndeplinirii obiectivelor naționale cum ar fi transferurile tehnologice forțate, culegerea de informații obligând toate entitățile chineze să împărtășească tehnologie și informații cu armata și cu serviciile de securitate. Astăzi, războiul comercial cu SUA ridică probleme dificile Chinei care nu-și poate menține componenta de tehnologii de vârf fără utilizarea tehnologiei americane.

Preşedintele Xi vrea să facă Armata chineză cea mai importantă forță tehnologică a lumii în anul 2049. Dar China nu a atins încă paritatea tehnologică cu Occidentul în tehnologii tradiționale (semiconductorii și vehiculele spațiale).

În schimb Rusia va exploata în curând unele tehnologii emergente și disruptive la nivel tactic și operativ, dar nu va avea acces la dezvoltări tehnologice strategice[23].

În concluzie, un domeniu nou al securității este securitatea tehnologică ce reprezintă un domeniu emergent care se impune astăzi pe scena internațională. Astăzi asistăm la o nouă abordare a tehnologiei ca amenințare și arie individuală de securitizare. Securitatea tehnologică este tratată într-o serie de documente strategice ale NATO, UE, SUA, Regatul Unit etc.

---

[21] *Ibidem*, pp. 59-60.
[22] *Ibidem*. p. 60.
[23] *Ibidem*. p. 63.

Securitatea tehnologică este un nou concept în plină dezvoltare nefiind încă definitivat. Dincolo de interpretări și nuanțe, abordarea conceptului securității tehnologice se distinge printr-o convergență deosebită a abordărilor care se bazează pe cei șapte piloni menționați în prezenta lucrare. De aceea, Academia Română și Academia Oamenilor de Știință din România trebuie să-și aducă aportul la dezvoltarea conceptului de securitate tehnologică bazată pe cei șapte piloni menționați în rândurile precedente.

BIBLIOGRAFIE

BUZAN B., „Popoarele, statele și frica", Editura Cartier, Chișinău, 2014;

BLINKEN A., „A Foreign Policy for the American People", disponibil la https://www.state.gov/a-foreign-policy-for-the-american-people/;

CHIFU I, „Reconfigurarea securității și a relațiilor internaționale în secolul 21", Volumul IV, *Războiul de agresiunea pe scară largă în Ucraina, în plin secol 21*, Editura Rao, București, 2023;

America's Place in the World, disponibil la https://www.whitehouse.gov/-briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/;

Ministry of Defence, Defence in a competitive age, disponibil la https://www.gov.uk/government/-publications/defence-in-a-competitive-age;

European Parliament, The geopolitical implications of the Covid-19 pandemic, disponibil la https://www.europarl.europa.-eu/RegData/etudes/STUD/2020/603511/EXPO_STU(2020)-603511_EN.pdf;

National Intelligence Council, Global Trends 2040. A more contested World, disponibil la https://www.dni.gov/files/ODNI/-documents/assessments/GlobalTrends_2040.pdf;

World Economic Forum, The Global Risks Report 2021, disponibil la https://¬www.-weforum.org/publications/the-global-risks-report-2021/;

NATO - 2030. United for a New Era, disponibil la https://www.-nato.int/nato_static_¬fl2014/¬assets/-pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf;

President Joseph R. Biden, Interim National Security Strategic Guidance, disponibil la https://¬www.-whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.