



CENTRUL DE EXCELENȚĂ

OSINT

Nr. 14/2022



TEHNOLOGIILE EMERGENTE

PLUSVALOARE PENTRU
ACTIVITATEA DE INTELLIGENCE

EMERGING TECHNOLOGIES

ADDED VALUE TO THE
INTELLIGENCE ACTIVITY



Materialul își propune să evalueze modul în care Inteligența Artificială/ IA influențează și forțează, chiar, schimbări în tot mai multe domenii de activitate: de la sănătate și educație la intelligence. Oportunitățile oferite de IA creează contextul pentru o competiție între mari actori statali, precum și între domeniul public și cel privat, dar și apariția unor dileme de ordin etic sau legal pentru societate.

This paper aims to assess how artificial intelligence/ AI influences and even forces shifts in more and more domains: from health and education to intelligence. The opportunities presented by AI create the context for a competition among major state actors, as well as between public and private sectors, while generating some ethical or legal dilemmas for the society.

EVOLUȚIILE TEHNOLOGICE – ÎNTRE BINECUVÂNTARE ȘI BLESTEM

Până în prezent, omenirea a fost martora a trei revoluții industriale alimentate de nevoia și dependența perpetuă a indivizilor de evoluție și de îmbunătățire a modului de viață. În linii mari, revoluțiile industriale au condus la înlocuirea producției manuale cu cea bazată pe mașini, aceste evoluții având, în general, scopul de a genera schimbări fundamentale la nivel organizațional, funcțional și relațional, dar și transformări calitativ superioare.

Prima Revoluție Industrială a adus cu sine mecanizarea proceselor de producție, cea de-a doua a facilitat producția în masă, iar cea de-a treia a deschis calea spre automatizarea producției. Cea de-a patra etapă aflată în derulare – tranziția de la digitizarea simplă la inovarea bazată pe combinarea de tehnologii – a început să prindă contur odată cu interconectarea a milioane de persoane prin dispozitive mobile, cu putere de procesare, capacitate de stocare și acces la cunoștințe fără precedent. Aceste oportunități au fost și sunt permanent amplificate, în principal, de patru dintre evoluțiile tehnologice emergente¹ – Internetul mobil de mare viteză, inteligența artificială și automatizarea, analiza *big data* și tehnologia *cloud*² – fiind evident faptul că procesul de colectare și analiză a datelor reprezintă o caracteristică esențială a fiecăreia dintre acestea³.

Printre elementele care diferențiază noua eră, denumită A Patra Revoluție Industrială, 4IR sau Industria 4.0, de celelalte perioade se numără: modul în care echipamentele *hardware*, *software* și conectivitatea sunt reconfigurate și integrate, colectarea și analiza unor cantități vaste de date, interacțiunea fără impedimente dintre dispozitivele inteligente și estomparea graniței dintre dimensiunile fizice și virtuale ale procesului de producție⁴.

La nivel social, noile tehnologii și platforme facilitează interacțiunea cetățenilor cu guvernele, dar și controlul acestora asupra populației, bazat pe sisteme de supraveghere și abilitatea de a controla infrastructura digitală. În raportul furnizor – beneficiar, evoluțiile tehnologice au efecte asupra așteptărilor clienților, îmbunătățirii produselor, inovării colaborative și formelor organizaționale. Cu cât mașinile colectează mai multe date despre consumatori, cu atât mai bine le pot anticipa nevoile și pot acționa în numele acestora. Într-o societate în care datele joacă rolul de monedă în plan digital, furnizorii trebuie să asigure însă confidențialitatea și securitatea informațiilor clienților și să recurgă la transparență în privința modului în care utilizează datele personale⁵.

TECHNOLOGICAL DEVELOPMENT – BETWEEN BLESSING AND CURSE

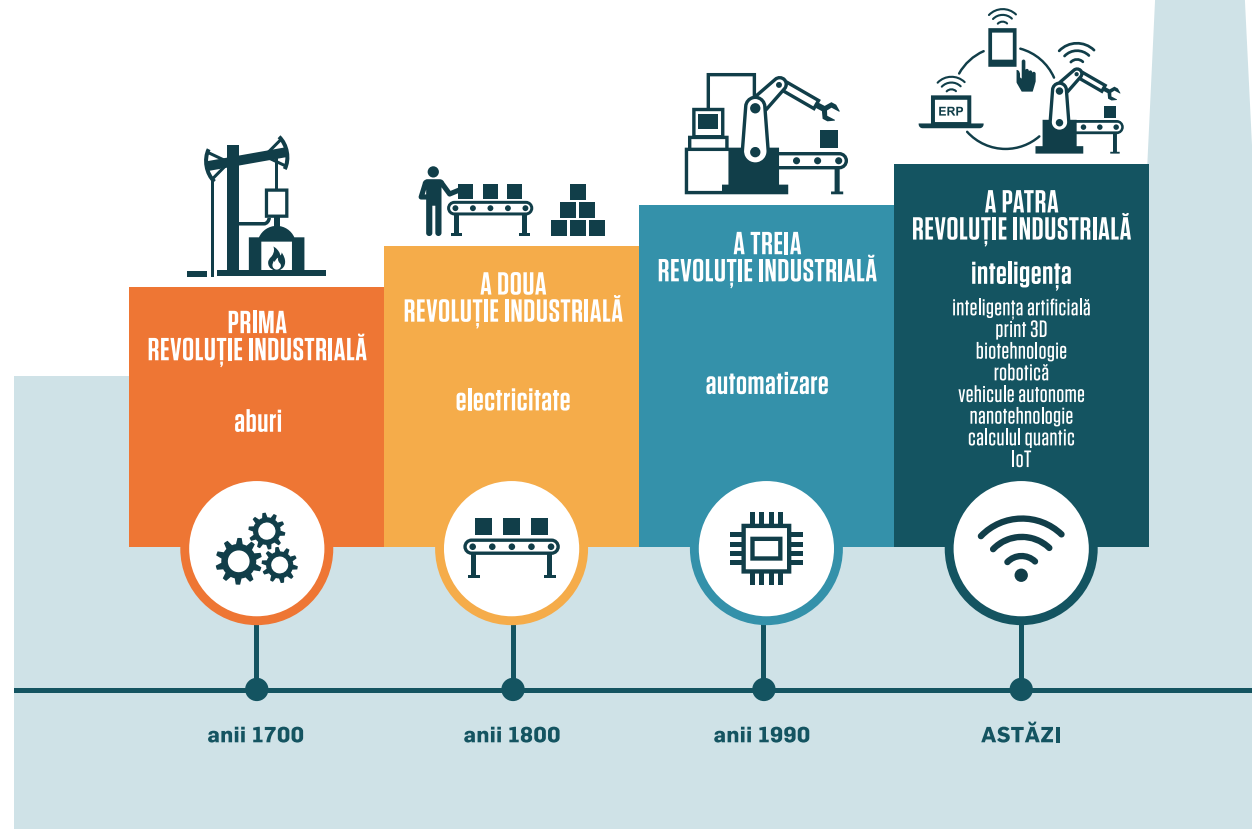
Until now, humankind has witnessed three industrial revolutions fueled by the continuous need and dependency of the individuals on evolution and on improving their lives. Basically, industrial revolutions led to the replacement of manual labor by machine-based production, developments generally aiming to produce fundamental changes at organizational, functional, and relational levels, as well as quality improvements.

The First Industrial Revolution entailed the mechanization of production, the Second one facilitated mass production, and the Third opened the way towards automated production. The ongoing Fourth stage – the transition from the basic digitalization towards innovation based on a fusion of technologies – began to take shape with the interconnection of millions of people through mobile devices with unprecedented processing power, storage capacity, and access to knowledge. These opportunities have been permanently amplified mainly by four of the emerging technology breakthroughs¹ – high-speed mobile Internet, artificial intelligence and automation, big data analytics, and cloud technology² – and it is obvious that the process of data collection and analysis is an essential feature of each one of them³.

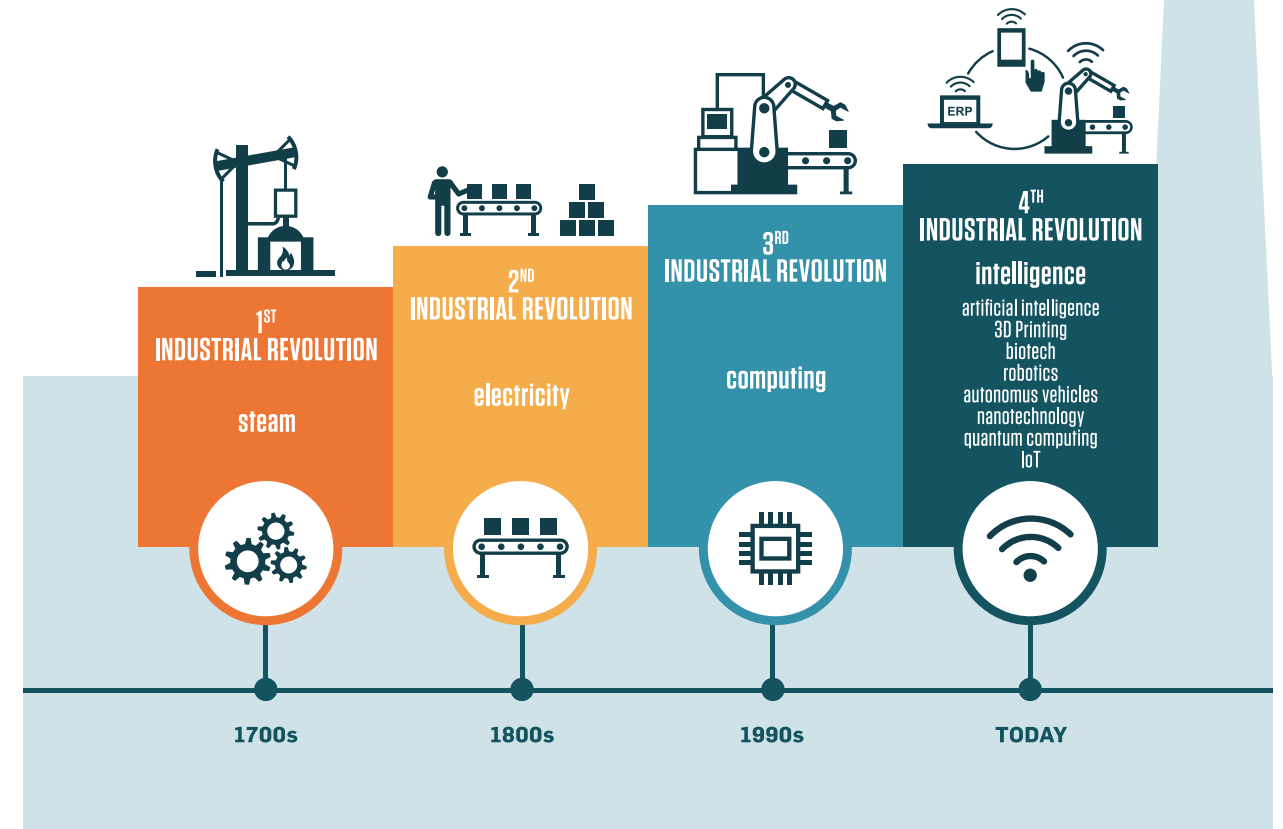
Some of the elements that differentiate the new era, called The Fourth Industrial Revolution, 4IR, or Industry 4.0, from the other periods are: the way in which hardware, software, and connectivity are reconfigured and integrated, the collection and analysis of large data volumes, the unimpeded interaction between smart devices, and the blurred line between the physical and virtual components of the production process⁴.

At the social level, the new technologies and platforms facilitate the citizen-government interaction, as well as governments' control over the population, based on surveillance systems and on the ability to control digital infrastructure. In the relation between the supplier and the beneficiary, technological developments produce effects on customer expectations, on product improvement, on collaborative innovation, and on organizational forms. The more data the machines gather about the consumers the better they can anticipate their needs and act on their behalf. In a society where data plays the role of digital currency, suppliers must also ensure the confidentiality and the security of customer data and show transparency about the way they use personal information⁵.

A PATRA REVOLUȚIE INDUSTRIALĂ



THE FOURTH INDUSTRIAL REVOLUTION



A Patra Revoluție Industrială va avea, de asemenea, implicații la nivel identitar și al aspectelor conexe, precum confidențialitatea, simțul proprietății, obiceiuri de consum, timpul dedicat activităților personale și recreative, dezvoltarea carierei și a competențelor, dezvoltarea de relații interpersonale.

În plan securitar, 4IR ar putea avea efecte atât asupra securității naționale și internaționale, cât și a naturii și probabilității conflictului. Conflictele hibride au estompat distincția dintre război și pace, combatant și non-combatant, violență și non-violență. În același timp, evoluțiile din domeniul tehnologic generează potențial pentru reducerea dimensiunii și impactului actelor violente prin dezvoltarea unor noi modalități de protecție sau prin creșterea preciziei în procesul de *targeting*⁶.

Klaus Schwab, fondator al Forumului Economic Mondial, a avertizat că modul în care este înțeleasă și integrată noua revoluție constituie cea mai mare provocare, având în vedere accentul pus pe inteligență artificială, *big data* și robotică, dar și pe normalizarea procesului de însușire și integrare a componentelor aparținând acestor tehnologii⁷.

A Patra Revoluție Industrială este adesea asociată conceptului de Inteligență Artificială/ IA și, în prezent, se axează pe evoluția sistemelor de tip *machine learning*. Odată cu Industria 4.0, IA nu mai înseamnă doar captarea de cunoștințe explicite, ci replicarea de cunoștințe în mod intuitiv prin recunoașterea de *pattern*-uri și utilizarea algoritmilor de date și învățare pentru a produce rezultate și a lua decizii cu intervenție minimă din partea factorului uman⁸. IA este o caracteristică a computerelor care „gândesc asemenea oamenilor” și are utilizări de la operarea funcției *autocorrect* de pe telefoanele mobile la identificarea de *pattern*-uri în cantități uriașe de date nestructurate⁹.

Furthermore, the Fourth Industrial Revolution will affect human identity and related issues, such as privacy, sense of ownership, consumption habits, time for personal and leisure activities, career and skills improvement, and development of interpersonal relationships.

As for the security environment, 4IR is likely to have an impact on both national and international security, and on the nature and likelihood of conflict. Hybrid conflicts have blurred the distinction between war and peace, combatants and noncombatants, violent and nonviolent acts. At the same time, technological developments engender a decrease in scale and impact of violent acts by developing new ways of protection or by increasing the accuracy of the targeting process⁶.

Klaus Schwab, the founder of the World Economic Forum, has warned that the biggest challenge is the way people understand and integrate the new revolution, given its emphasis on artificial intelligence, big data and robotics, as well as on the normalization of the process of mastering and incorporating aspects of these technologies⁷.

The Fourth Industrial Revolution is often associated with the concept of Artificial Intelligence/ AI and nowadays it focuses on the evolution of the machine learning systems. In the 4.0 Industry era, AI is no longer just about capturing explicit knowledge, but about intuitive replication of knowledge by pattern recognition and use of data and learning algorithms to produce results and make decisions with minimal human involvement⁸. AI represents a feature of computers that “think like humans” and has multiple uses, from powering the autocorrect function on mobile phones to pattern recognition in huge piles of unstructured data⁹.



În medii academice¹⁰ a fost lansată ideea ca *big data* și inteligența artificială să fie integrate sub o nouă denumire - *data intelligence*. Tehnologiile care au la bază inteligența artificială se răspândesc rapid la nivel global, companiile valorificându-le, de exemplu, pentru optimizarea proceselor analitice, în timp ce administrațiile locale recurg la acestea în vederea monitorizării blocajelor în trafic sau a contorizării *smart* a consumului energetic.

Avansul înregistrat, în ultimul deceniu, în domeniul IA este vizibil și în analiza de *intelligence*, tehnologiile care au la bază IA fiind deja folosite pentru a clasifica imagini și pentru a sorta volume mari de date, crescând astfel capacitatea analiștilor de a extrage informațiile de valoare. Utilizarea IA a fost determinată nu doar de creșterea capacității informatice și de noii algoritmi, dar și de explozia de date disponibile în prezent.

Un număr din ce în ce mai mare de state utilizează însă instrumentele avansate IA pentru supravegherea cetățenilor, în vederea îndeplinirii unor obiective politice - unele sunt legale (precum cele circumscrise zonei de prevenire și combatere a terorismului), altele sunt considerate a încălca drepturile omului sau la limita legalității. În prezent, tehnologiile IA sunt produse și comercializate, în proporție de 70%, de state precum Japonia, SUA, Coreea de Sud, China și Germania, estimându-se o extindere la nivelul tuturor națiunilor cu o economie avansată.

Consecințele utilizării IA, la nivel individual, se preconizează a fi multiple, în contextul unei „duble hibridizări” manifestate prin utilizarea la scară tot mai extinsă a tehnologiilor, respectiv prin asumarea unor comportamente umane de către mașinile care devin tot mai inteligente și necesare în sfera activităților cotidiene. Nu este exclusă concretizarea, într-un orizont de timp apropiat, a unor noi „modele de viață”, cu un nivel redus de consum, cu ajutorul roboților care vor desfășura activitățile cotidiene cele mai solicitante.

Aspectele problematice ale fenomenului hibridizării om - mașină constau în faptul că astfel de date sunt deținute, preponderent, de un număr restrâns de entități private, circumstanță care ridică probleme de acces și de partajare și constituie un punct de cotitură al secolului XXI, din perspectiva consecințelor asupra națiunilor.

IA rezolvă o serie de probleme, însă poate genera altele, de natură organizatorică, structurală ori de securitate a informațiilor. De exemplu, în plan militar și al operațiunilor de *intelligence*, unul dintre principalele aspecte de interes vizează posibila inversare a raporturilor de forță prin utilizarea IA.

The idea that big data and artificial intelligence should be merged into a new term – data intelligence – has been promoted in academic circles¹⁰. Technologies based on artificial intelligence are spreading rapidly worldwide, with companies leveraging them, for example, in order to optimize analytical processes, while local governments use them for monitoring traffic jams or smart metering energy consumption.

The progress of AI in the last decade is also noticeable in intelligence analysis, with AI-based technologies already being used to classify images and sort large amounts of data, increasing analysts' ability to extract valuable information. The use of AI has been fueled not only by the increase in computing capability and by the new algorithms, but also by the boom of currently available data.

However, an increasing number of states are using advanced AI tools to monitor their citizens in order to achieve political goals – some are legal (such as those related to preventing and countering terrorism), others are perceived as an infringement of human rights or considered to be operating on the fringes of the law. Nowadays, 70% of AI technologies are produced and traded by countries such as Japan, the United States, South Korea, China, and Germany and are expected to expand to all advanced economies.

The end results of using AI at individual level are expected to be manifold, in the light of a “double hybridization” marked by an increased use of technology, respectively human-like machines that are becoming more intelligent and necessary in daily activities. In the near future, it is conceivable to have new “life patterns” with a low level of consumption thanks to robots that will carry out the most demanding daily activities.

The challenge of human-machine hybridization is that data belongs mainly to a small number of private entities which generates access and sharing problems and represents a milestone of the 21st century in terms of consequences for every nation.

AI solves a number of problems, but it could also generate organizational, structural, and information security-related issues. For example, one of the main concerns at military and intelligence level is a potential change in the balance of power fueled by the use of AI.



IA – BRIGHT SIDES

În fața unor ofensive cibernetice tot mai sofisticate, se impune – pe lângă vigilență tehnologică și o sensibilizare a populației în sensul dezvoltării reflexelor adecvate de apărare – implementarea unor sisteme performante de monitorizare a infrastructurii IT, care să contribuie la detectarea eventualelor anomalii generate de acțiuni malițioase, înainte ca acestea să declanșeze o „apocalipsă a datelor”. O perspectivă salvatoare este recurgerea la inteligența artificială, aceasta participând la identificarea mutațiilor apărute la nivelul *software*-urilor malițioase¹¹.

IA poate contribui și la diminuarea eficienței dezinformării asupra securității internaționale. Instrumentele IA de detectare, analizare și eliminare a dezinformării ajută la blocarea conținutului nefavorabil și a roboților web. Printre acestea se regăsesc:

- *automated vetting* și detectarea știrilor false: entități precum *AdVerif.ai* scanează și detectează conținutul „problematic” prin utilizarea sistemelor de procesare a limbajului natural și *deep learning*;
- *trollbot detection & blocking*: modele de *machine learning* precum *Botometer API* oferă posibilitatea utilizării IA pentru identificarea și potențiala eliminare a *bots*; reducerea numărului de roboți ar putea sanitiza ecosistemul informațional, întrucât o serie de *political bots* sunt creați exclusiv în scopul amplificării dezinformării, propagandei și a știrilor false¹².

În mediul de afaceri, utilizarea IA a devenit deja o obișnuință, procesul decizional de la nivelul unor companii de top din segmentul financiar-bancar fiind asistat în mod pertinent și aplicat de IA (spre exemplu, sub aspectul identificării eventualelor inexactități și riscuri de fraudă ale clienților ca urmare a analizării datelor accesate pe surse private sau publice, interne sau externe). Astfel, activitatea anostă de înțelegere a contextului este reorientată către tehnologie, resursa umană putându-se concentra exclusiv pe valoarea adăugată.

Din această perspectivă, o platformă tip *cognitive search and analytics*, dotată inclusiv cu funcționalități de *image* și *voice recognition*, își poate dovedi utilitatea în combaterea activităților de spălare de bani, a atacurilor financiare, traficului sub toate formele lui ori chiar a terorismului, prin detectarea unor scheme de date „neobișnuite”, datorită algoritmilor de căutare predictivi și capacității intrinseci de cartografiere a conexiunilor între persoane, conturi, tranzacții și numeroase alte tipuri de date¹³.

AI – BRIGHT SIDES

Increasingly sophisticated cyberattacks require – besides technological alertness and public awareness by developing appropriate defense reflexes – high-performing systems for monitoring the IT infrastructure to support the detection of potential anomalies generated by malicious actions before they cause a “data apocalypse”. Artificial intelligence seems an appropriate solution as it may help detect mutations within malicious software¹¹.

AI may also help decrease the efficacy of disinformation on international security. AI tools for detecting, analyzing, and eliminating disinformation enable blocking of adverse content and web robots, and they include:

- automated vetting and fake news detection: entities such as *AdVerif.ai* scan and detect “problematic” content by using natural language processing and deep learning systems;
- trollbot detection & blocking: machine learning models such as *Botometer API* provide the possibility to use AI for detecting and potentially eliminating bots; reducing the number of robots is likely to sanitize the information ecosystem since a series of political bots are created solely to amplify disinformation, propaganda, and fake news¹².

In the business environment, AI is quite commonly used. Thus, in some of the top financial and banking companies, the decision-making process is relevantly and properly assisted by AI (for instance, to detect potential inconsistencies and risks of customer fraud following the analysis of data from public or private, internal or external sources). Therefore, the dull activity of comprehending the context is shifted towards technology, so that human resources can focus entirely on added value.

In this respect, a cognitive search and analytics platform, equipped with image and voice recognition features, may prove to be useful in fighting money-laundering, financial attacks, all forms of trafficking, and even terrorism through the detection of “unusual” data schemes, due to predictive searching algorithms and its inherent capacity to map connections among people, bank accounts, transactions, and many other types of data¹³.



IA – DARK SIDES

Dezvoltarea rapidă a IA comportă și riscuri. Pe fondul utilizării tot mai intense a sistemelor de inteligență artificială, experți în domeniu ai unor universități și companii de prestigiu din SUA¹⁴ au anticipat, încă din anul 2018, o serie de modificări majore în spectrul amenințărilor, în sensul:

- extinderii acestora (scăderea costurilor atacurilor prin utilizarea de sisteme IA în scopul îndeplinirii unor sarcini care, în mod obișnuit, ar implica inteligență, expertiză și activități umane; creșterea implicită a numărului de actori capabili să comită atacuri, a ratei la care pot comite astfel de atacuri, precum și extinderea setului de potențiale ținte);
- apariției unor noi amenințări (exploatarea vulnerabilităților sistemelor IA folosite de actorii pozitivi);
- schimbării caracterului tipic al amenințărilor (creșterea eficienței atacurilor și a dificultăților legate de atribuirea acestora autorilor reali)¹⁵.

Oricâte soluții pozitive ar putea oferi IA pentru securitatea IT, în egală măsură trebuie luată în considerare și posibilitatea utilizării acesteia de către infractorii cibernetici. Chiar dacă majoritatea nu își permite astfel de sisteme costisitoare, nu trebuie uitat că la originea atacurilor cibernetice se află, de multe ori, state și servicii de informații, în cazul cărora se poate pleca de la premisa că dispun de resursele necesare utilizării IA în scopuri ofensive.

Soluțiile bazate pe inteligența artificială pot prelua o serie de funcții în sprijinul atacatorilor statali, și anume: analiza și predicția vulnerabilităților; dezvoltarea de programe malițioase performante, dificil de detectat prin soluțiile de securitate bazate pe IA; identificarea țintelor *de facto* și recomandarea unor strategii de atac adecvate; derularea unor atacuri eficiente de tip *phishing* prin anticiparea comportamentului victimei. Altfel spus, inversarea funcțiilor pe care le oferă soluțiile IA pentru îmbunătățirea securității IT¹⁶.

IA nu afectează însă doar securitatea digitală, ci și pe cea fizică și politică. Utilizarea IA pentru comiterea de atacuri cu drone sau alte sisteme fizice (de exemplu, prin desfășurarea de sisteme autonome de armament) ar putea provoca o intensificare a amenințărilor asociate acestor atacuri. Este preconizată apariția unor noi tipuri de atacuri care să blocheze sistemele *cyber-fizice* (generând, de pildă, un *crash* al vehiculelor autonome) sau să implice sisteme fizice imposibil de teleghidat (de exemplu, mii de microdrone).

AI – DARK SIDES

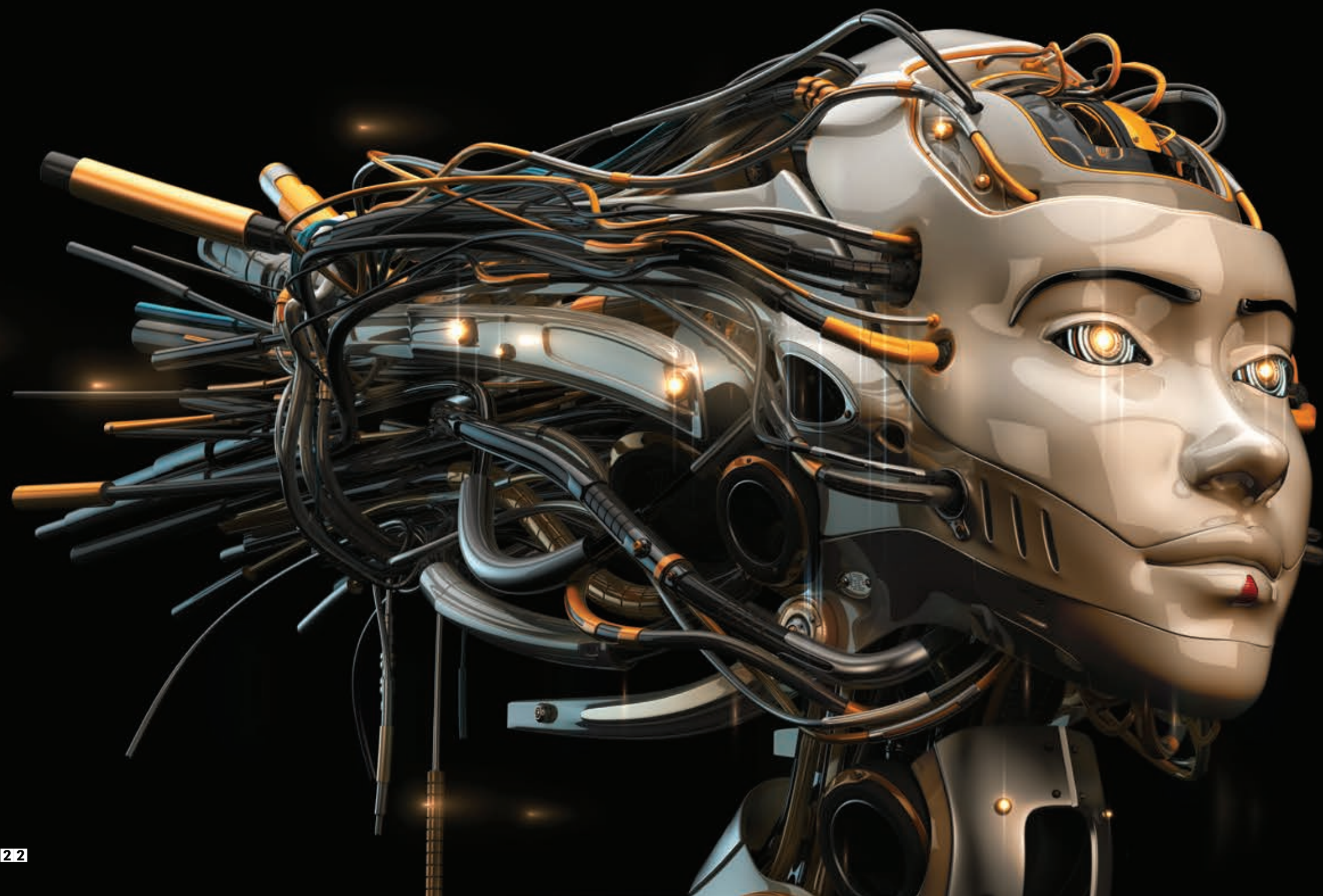
The fast AI development can also entail risks. As AI systems have been used more and more intensively, experts at top-notch US universities and companies¹⁴ anticipated, as early as 2018, major changes in security threats. These include:

- the expansion of threats (reducing the costs of attacks by using AI systems to perform tasks which would normally entail human intelligence, expertise, and actions; the increasing number of entities able to launch attacks and frequency of such attacks, as well as the expansion of the set of potential targets);
- the rise of new threats (exploiting the vulnerabilities of AI systems used by positive entities);
- the change in the typical character of threats (increasing attack efficiency and difficulties in finding the real perpetrators)¹⁵.

Despite all the solutions AI could provide for IT security, one should equally take into account that AI could also be used by cyber criminals. Although these expensive systems are not generally affordable, one should bear in mind that cyberattacks are mostly generated by states and intelligence agencies and, consequently, it can be assumed that such entities have the necessary means for using AI offensively.

AI-based solutions can carry several features beneficial to perpetrator states, namely: assessment and prediction of vulnerabilities; development of advanced malicious programs, difficult to trace by AI-based security solutions; detection of *de facto* targets and recommendation for proper attack strategies; running efficient phishing attacks by anticipating the victim's behavior. Shortly, a reversal of AI features used to strengthen IT security¹⁶.

AI does not affect only digital security, but also the political and physical safety. The use of AI to carry out attacks by drones or other physical systems (for example, by deploying autonomous weapon systems) could result in increased threats associated with these attacks. New types of attacks are expected to block cyber-physical systems (generating, for instance, a crash of autonomous vehicles) or to involve physical systems that cannot be remotely guided (for example, thousands of microdrones).



În ceea ce privește securitatea politică, exploatarea IA pentru îndeplinirea unor misiuni de supraveghere (analiza datelor în masă), persuasiune (propagandă țintită) și dezinformare (manipularea unor materiale video) ar putea genera extinderea amenințărilor asociate manipulării sociale și violării vieții private. În context, nu este exclusă apariția unor noi tipuri de atacuri care să profite de capacitatea îmbunătățită de analiză a comportamentului, stării psihice și convingerilor umane, în baza datelor disponibile. Aceste aspecte sunt deosebit de importante pentru statele autoritariste¹⁷.

IA joacă un rol tot mai relevant în cadrul ecosistemului informațional, prin eficientizarea și augmentarea propagandei. Printre principiile și tehnicile bazate pe IA și destinate diseminării propagandei și dezinformării se numără:

- exploatarea datelor comportamentale, prin selectarea acestora cu ajutorul *machine learning*; metadatale generate de utilizatorii unor platforme *online* – adesea pentru a obține o imagine a comportamentului consumatorilor pe componenta de *targeted advertising* – pot fi exploatare și în scopuri de propagandă;
- *pattern recognition & prediction*, prin utilizarea algoritmilor *machine learning* de pe platformele sociale, care ierarhizează conținutul preferat de utilizatori și produc mesaje adresate celor care manifestă deja o apetență pentru acestea;
- *agenda setting*, cu ajutorul roboților web, care cresc în mod artificial vizibilitatea unor conținuturi politice și influențează direcția dezbaterii publice;
- procesarea limbajului natural pentru orientarea sentimentului, prin intermediul unei metode sistemice de identificare, examinare și interpretare a conținutului emoțional în cadrul textului, în scopul construirii unei propagande eficiente;
- *deepfakes*, prin utilizarea unor sisteme IA capabile să genereze, în mod sintetic, vocea oricărei persoane, atât timp cât există un set extins de înregistrări cu vocea persoanei respective; acest lucru este tot mai des valabil și în cazul materialelor video¹⁸.

In terms of political security, the use of AI to carry out surveillance missions (mass data analysis), persuasion (targeted propaganda), and disinformation (manipulation of videos) could lead to the expansion of threats associated with social manipulation and privacy violation. In this context, new types of attacks that take advantage of the improved ability to analyze human behavior, mental state, and beliefs, based on available data, could be carried out. These aspects are particularly important for the authoritarian states¹⁷.

AI is playing an increasingly relevant role in the information ecosystem, by streamlining and increasing propaganda. Some of the principles and techniques based on AI and intended for the dissemination of propaganda and disinformation are:

- behavioral data exploitation, by machine learning selection; metadata generated by online platform users – often to get a picture of consumer behavior for targeted advertising – can also be exploited for propaganda purposes;
- pattern recognition & prediction, by using machine learning algorithms on social platforms, which rank the content preferred by users and produce messages addressed to those already interested in them;
- agenda setting, by using web robots which artificially increase the visibility of political content and influence the direction of public debate;
- natural language processing to target sentiment, by using a systemic method to identify, examine, and interpret the emotional content of the text in order to build an effective propaganda;
- deepfakes, by using AI systems capable of synthetically generating any person's voice, as long as there is an extensive set of recordings with that person's voice; this is increasingly common for videos as well¹⁸.



JAMES BOND *versus* CYBORG

În era inteligenței artificiale, spionii umani acționează într-un mediu tot mai ostil, tendința fiind de a fi parțial înlocuiți de *gadget*-uri de ultimă generație.

La fel ca în trecut, ei trebuie să rămână invizibili, însă acest lucru este tot mai dificil, pentru că adversarul este cu totul altul: în prezent, identitățile legendate și *well-told lies* nu prea mai sunt de ajutor, întrucât trebuie induse în eroare nu persoane, ci computere capabile să identifice o fizionomie într-o mulțime.

Efectele IA asupra activității serviciilor de informații sunt reflectate, de exemplu, prin provocările întâmpinate de *Central Intelligence Agency*/ CIA în procesul de adaptare la un mediu în care principalul inamic nu mai este un agent străin, ci o mașină.

CIA s-a pregătit peste 30 de ani pentru această tranziție de la oameni la computere, o dovadă în acest sens fiind documente guvernamentale din anul 1984, conform cărora un *AI Steering Group*, înființat în 1983, avea încă de atunci în competență transmiterea, către managerii CIA, a unor rapoarte lunare privind stadiul cercetării și dezvoltării IA.

Documentele respective, între timp declassificate, reliefează eforturile susținute întreprinse în cadrul comunității americane de informații în ceea ce privește sistemele de experți, procesarea limbajului natural (lingvistică computațională), *intelligent data base interfaces*, *image-understanding systems*, interpretarea semnalelor sau managementul datelor spațiale și geografice.

Totodată, în rapoarte este subliniată necesitatea instruirii agenților, a focusării pe susținerea dezvoltatorilor de IA atât din mediul profesional, cât și academic și a creării unui *open source AI clearinghouse* pentru agențiile guvernamentale.

CIA a anticipat, așadar, ceea ce urma să reprezinte tehnologia IA într-un moment în care cei mai mulți considerau inteligența artificială o pură ficțiune.

În prezent, cel puțin 30 de state dețin și folosesc tehnologii de supraveghere video, cu funcții de *video analytics* sau de analiză inteligentă, ceea ce înseamnă că instrumentele de *counterintelligence* au prioritate în jocul internațional „de-a v-ați ascunselea” al comunității globale de informații.

JAMES BOND *versus* CYBORG

In the age of artificial intelligence, human spies are operating in an increasingly hostile environment, with a tendency to be partially replaced by cutting-edge gadgets.

Just as in the past, they must remain invisible, but this is increasingly difficult because the adversary is completely different: currently, covert identities and well-told lies are no longer helpful as the ones to be misled are not people, but computers capable of identifying a face in a crowd.

The effects of AI on intelligence activities are reflected, for example, in the challenges faced by the Central Intelligence Agency/ CIA in adapting to an environment where the main enemy is no longer a foreign agent, but a machine.

The CIA has been preparing for more than 30 years for this transition from humans to computers, as evidenced by the 1984 government documents, according to which an AI Steering Group, founded in 1983, had since then the task to send monthly reports to CIA managers on the state of AI research and development.

Those documents, meanwhile declassified, highlight the constant efforts made within the American intelligence community in terms of expert systems, natural language processing (computational linguistics), intelligent data base interfaces, image understanding systems, signal interpretation, or spatial and geographic data management.

At the same time, the reports emphasize the need to train agents, to focus on supporting AI developers in both professional and academic fields, and to create an open source AI clearinghouse for government agencies.

Therefore, the CIA anticipated what AI technology would represent at a time when most considered artificial intelligence to be pure fiction.

Currently, at least 30 states have and use video surveillance technologies equipped with video analytics and intelligent analysis functionalities, which means that counterintelligence tools are a priority in the international “hide and seek” game of the global intelligence community.



Astfel, este foarte probabil ca, prin doar câteva progrese în domeniul GEOINT și al urmăririi prin sateliți, spionii umani să nu mai aibă nicio șansă în fața următoarei generații de IA¹⁹.

IA utilizată în anumite sarcini poate economisi timp pentru analiștii din domeniul *intelligence* și le poate îmbunătăți randamentul. Odată ce sarcini precum curățarea datelor, etichetarea sau recunoașterea șabloanelor vor fi îndeplinite cu ajutorul IA, analiștii vor putea aloca mai mult timp misiunilor exclusiv umane și vor colabora cu alți experți mai mult decât o fac în prezent.

Analiza din surse deschise bazată pe inteligență artificială, de exemplu, are un potențial imens pentru comunitățile de *intelligence*, deoarece instrumentele IA pot ingera volume mari de date din toate sursele disponibile și pot identifica tendințe și tipare care produc perspective valoroase pe care analiștii umani este posibil să nu le descopere²⁰.

*Institute for National Security Studies*²¹/ INSS preconizează că, cel puțin în următorul deceniu, sistemele IA vor continua să servească drept instrumente care pot face diferența între „important” și „irelevant” în fluxul de informații și pot detecta anumite anomalii, corelații și tipare care vor genera concluzii importante.

Conform INSS, inteligența artificială poate contribui la îmbunătățirea:

- activității analitice de rutină, prin: facilitarea procesării și folosirea optimă a volumelor mari de date; îmbunătățirea accesului analiștilor la informația originală; verificarea informației și identificarea falsurilor; identificarea de detalii, corelații, obiceiuri, tipare și anomalii; completarea și coroborarea datelor; reducerea erorii umane; îmbunătățirea continuității muncii de *intelligence*; gestionarea pupitrului de comandă (prin utilizarea unui asistent virtual precum „Siri” sau „Alexa”);
- procesului de realizare de produse analitice, respectiv: analize și evaluări ale informațiilor; reprezentări digitale ale informațiilor; alerte cu privire la modificările strategice ale cursului evenimentelor;
- integrării: în cadrul și între entitățile analitice; la nivelul unei comunități de informații; între agențiile de informații și entitățile operaționale și de planificare²².

Serviciile de informații și structurile de poliție au în vedere și *predictive policing*, în timp ce forțele armate întreprind demersuri în direcția implementării tehnologiilor IA pentru îmbunătățirea performanțelor echipamentelor militare, pentru a face față unor noi forme de desfășurare a războaielor.

Thus, it is very likely that, with only a few advances in the field of GEOINT and satellite tracking, human spies will no longer stand a chance against the next generation of AI¹⁹.

AI used in certain tasks can save time for intelligence analysts and improve their performance. Once tasks such as data cleaning, labelling or pattern recognition are accomplished by AI means, analysts will be able to spend more time on exclusively human missions and cooperate with other experts more than they currently do.

For example, AI-based OSINT analysis has a huge potential for intelligence communities, as AI tools can ingest huge volumes of data from all available sources and can identify trends and patterns which produce valuable perspectives that human analysts may not discover²⁰.

The *Institute for National Security Studies*²¹/ INSS predicts that, at least over the next decade, AI systems will continue to serve as tools that can differentiate between "important" and "irrelevant" within the information flow and detect certain anomalies, correlations, and patterns that will generate relevant conclusions.

According to INSS, artificial intelligence can contribute to the improvement of:

- the routine analytical activity by: facilitating processing and optimal use of big data volumes; improving analysts' access to the original information; verifying the information and identifying fakes; identifying details, correlations, habits, patterns, and anomalies; adding and corroborating data; reducing human errors; improving the continuity of the intelligence activity; managing the command desk (by using a virtual assistant such as "Siri" or "Alexa");
- the process of developing analytical products, such as: information analysis and assessment; digital representations of information; alerts on strategic changes in the course of events;
- the integration: intra and inter analytical entities; at intelligence community level; between the intelligence agencies and the operational and planning entities²².

Intelligence agencies and police structures act also towards predictive policing, while armed forces implement AI technologies to enhance the performance of the military equipment, in order to counter new forms of warfare.

Este luată în calcul inclusiv posibilitatea ca, în viitorul apropiat, statele să apeleze la sistemele IA în scopul elaborării propriilor strategii de politică externă.

Posibilitățile extinse ale prelucrării datelor prin intermediul inteligenței artificiale permit realizarea de prognoze cu privire la urmările unor decizii specifice de politică externă și evaluarea în timp real a efectelor acestora. Într-o oarecare măsură, acest lucru poate fi interpretat ca o extindere a analizei clasice de *intelligence*. Analiza automatizată cu ajutorul sistemelor IA face însă posibilă prelucrarea unor cantități mai mari de date și corelarea unor date de diverse tipuri și origini. Se preconizează, de exemplu, că astfel de sisteme vor fi utilizate, la un moment dat, pentru identificarea timpurie a crizelor, dar și în caz de pandemii sau în analiza fluxurilor migraționiste globale²³.

În rândul experților occidentali sunt evidențiate însă și limitele IA în domeniul *intelligence*.

Jo Cavan și Paul Killworth, ambii directori în cadrul *Government Communications Headquarters*/GCHQ, reliefează faptul că, deși sunt extrem de utile, instrumentele IA nu vor furniza serviciilor de informații capacitatea de identificare a unor soluții viabile de gestionare a avalanșei informaționale. Cei doi ofițeri ai GCHQ sunt de părere că nu vor exista alternative la: recrutarea de personal specializat; consolidarea parteneriatului cu mediile academice și industriale; actualizarea codurilor de etică, susținute de existența unei legislații solide și a unor dezbateri transparente²⁴.

Pentru Paula Kift, inginer în cadrul companiei americane *Palantir Technologies*, IA este supraestimată, rolul tehnologiilor constând în facilitarea, și nu în înlocuirea inteligenței umane. Spre deosebire de mașini, oamenii pot adopta decizii contextuale în scenarii în care ceva nu pare a fi corect. Din perspectiva acesteia, un sprijin real pentru serviciile de informații în gestionarea fluxurilor de date îl constituie inteligența augmentată²⁵, care le poate facilita analiștilor posibilitatea de a adopta decizii bazate pe date într-o manieră mai ținută, mai transparentă și mai responsabilă²⁶.

Potrivit lui Oskar Josef Gstrein, membru al *Data Research Centre* din cadrul *University of Groningen* (Olanda), IA este eficientă în a identifica pattern-uri empirice în punctele de date, însă comportă două deficiențe majore: (1) funcționează într-o manieră care nu este înțeleasă în totalitate de analiști, ceea ce generează probleme semnificative de responsabilitate; (2) este caracterizată de absența inerentă a raționamentului normativ (și, implicit, a conceptului de justiție)²⁷.

In the near future, states may turn to AI systems in order to develop their own foreign policy strategies.

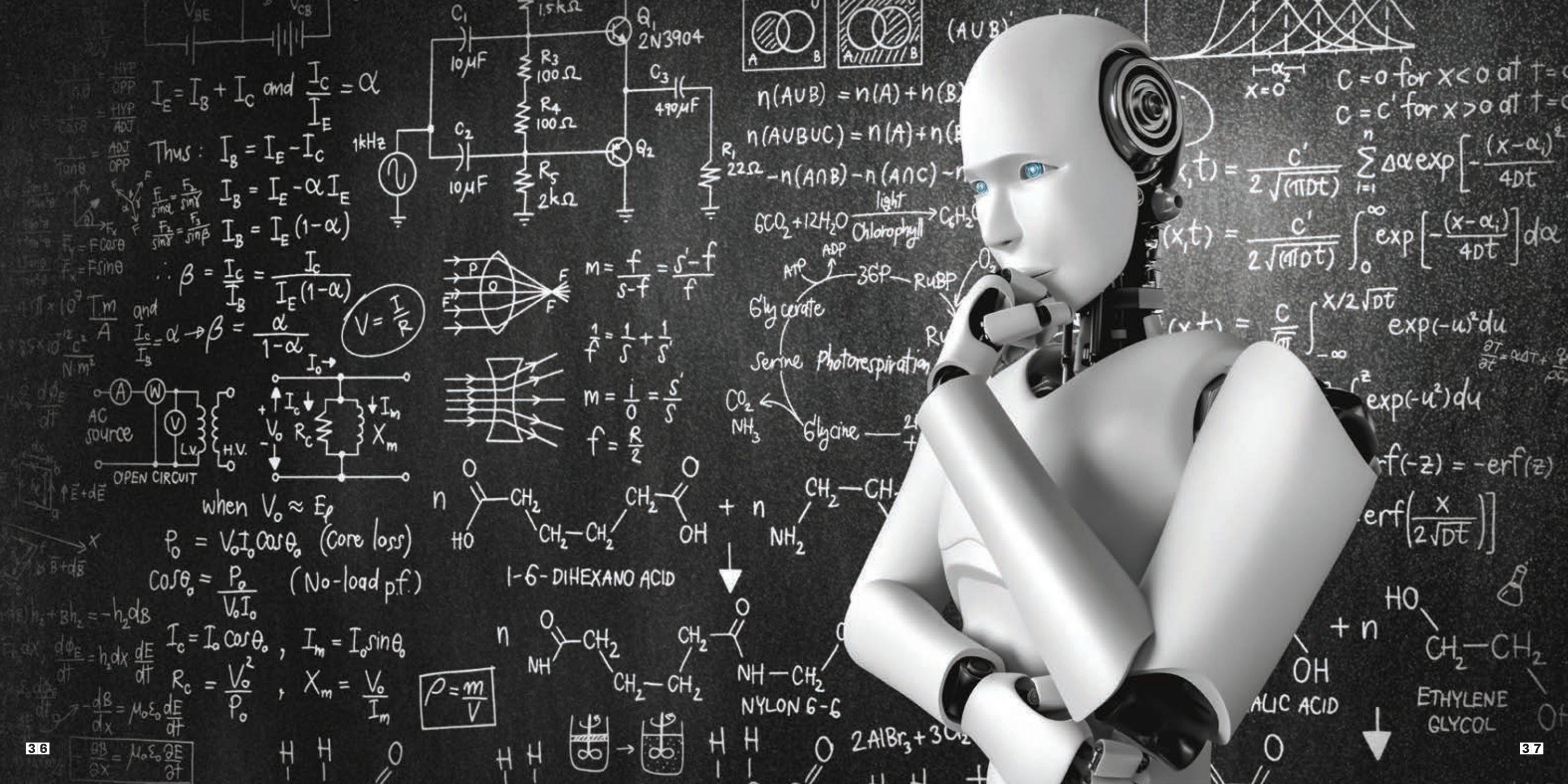
Extensive possibilities of data processing through artificial intelligence allow the development of forecasts on the outcomes of specific foreign policy decisions and real-time assessment of their consequences. To a certain extent, this may be regarded as an extension of traditional intelligence analysis. However, automated analysis based on AI systems makes it possible to process large amounts of data and to correlate data of different types and origins. For example, it is expected that such systems would be used at some point for early crisis detection and also in case of pandemics or for analyzing global migration flows²³.

However, some Western experts highlight the limitations of AI within the intelligence field.

Jo Cavan and Paul Killworth, both directors within the Government Communications Headquarters/GCHQ, emphasize that, useful as they may be, AI tools will not provide intelligence services with the ability to identify viable solutions for managing the huge information flow. The two GCHQ officers consider that there will remain no alternative to: recruiting specialized personnel; strengthening the partnership with academia and industry; updating the codes of ethics, based on a strong legislation and transparent debates²⁴.

According to Paula Kift, engineer at the US company *Palantir Technologies*, AI is overrated, as the role of technology is to facilitate, not to replace human reasoning. Unlike machines, humans can make contextual decisions in scenarios where something seems wrong. From this point of view, for the intelligence services, augmented intelligence²⁵ is a real support in managing data flows, providing the analysts with the possibility to make data-based decisions in a more targeted, more transparent, and more responsible manner²⁶.

According to Oskar Josef Gstrein, member of the Data Research Centre within the University of Groningen (Netherlands), AI is effective in identifying empirical patterns in data points, but it has two major deficiencies: (1) it works in a manner that is not completely understood by analysts, which causes significant liability issues; (2) it is characterized by the absence of inherent normative reasoning (and, implicitly, the concept of justice)²⁷.



La rândul lor, experții de la *Deloitte Insights* atrag atenția că agențiile de *intelligence* care vor să obțină performanțe prin utilizarea IA pot întâmpina provocări precum:

- monopolizarea timpului analiștilor, în situațiile în care aceștia nu își clarifică prioritățile și modul în care IA se integrează în strategia lor de ansamblu ori nu evită investițiile în „tehnologii goale”, care folosesc IA fără să aibă acces la datele necesare;
- scepticismul analiștilor față de noile tehnologii, în cazul în care managementul nu se concentrează pe educarea angajaților și pe reconfigurarea activităților pentru o integrare perfectă a instrumentelor IA în fluxurile de lucru;
- încrederea, fără rezerve, în tehnologiile IA, existând riscul ca acestea să confirme concluzii preconcepute ale analiștilor, în detrimentul elaborării unei analize mai riguroase²⁸.

Deși tehnologiile emergente – IA, *advanced sensors*, *machine learning* (ML), *cloud computing*, *data analytics* – pot fi utilizate de serviciile de informații occidentale pentru îmbunătățirea activităților de colectare, procesare și exploatare a datelor în operațiuni, există și un revers al medaliei, când acestea sunt folosite de adversarii democrațiilor liberale. Aceleași instrumente tehnologice exploatate de agențiile occidentale de *intelligence* vor ajuta rivali străini în crearea unor *denied areas* pentru operațiuni, în detectarea, perturbarea și zădărnicierea (de exemplu, prin *deepfakes*) eforturilor serviciilor vestice, care se vor confrunta, probabil, cu o diminuare a abilității de a-și proteja ofițerii, operațiunile și informațiile clasificate, dar și a monopolului asupra capacității de colectare a acelor informații²⁹.

Experts from *Deloitte Insights* also point out that intelligence agencies which want to achieve performance by using AI may face challenges such as:

- monopolization of analysts' time, when they do not set their priorities straight and the manner in which AI fits within their overall strategy, or they do not avoid investments in "empty technologies" which use AI without having access to the necessary data;
- analysts' skepticism towards new technologies, if management does not focus on educating employees and on reshaping activities in order to perfectly integrate AI tools in the work flows;
- complete and unreserved confidence in AI technologies with the risk that they will confirm the presupposed conclusions of the analysts to the detriment of a more rigorous analysis²⁸.

Although emerging technologies – AI, advanced sensors, machine learning (ML), cloud computing, data analytics – can be used by Western intelligence services to improve the activities of data gathering, processing, and exploitation in operations, there is also a downside, when these are used by the adversaries of the liberal democracies. The same technological tools Western agencies use in operations will also help foreign rivals to create denied areas for operations, to detect, disrupt, and thwart (for example, through deepfakes) the efforts of the Western intelligence services, which will probably face a diminished ability to protect their own officers, operations, and classified information, and to maintain monopoly on the capability to collect that information²⁹.

DILEME DE ORDIN ETIC sau LEGAL

Deși inteligența artificială permite o analiză mult mai rapidă și obiectivă a datelor prin comparație cu capacitățile umane și, implicit, adoptarea unor decizii mai bine fundamentate, responsabilitatea pentru acestea este transferată, practic, unor sisteme computerizate, al căror *modus operandi* devine un fel de *black box*.

Necesitatea reglementării IA apare în momentul în care astfel de sisteme sunt folosite în domenii sensibile din punct de vedere politic și al respectării drepturilor fundamentale ale omului. În contextul utilizării sistemelor IA de către state, drepturile omului constituie un punct de plecare important, întrucât direcționează atenția către acele aplicații în cazul cărora folosirea inteligenței artificiale este strâns legată de constrângeri de ordin statal. Țări precum SUA sau Marea Britanie au introdus deja sisteme IA în activitatea structurilor de poliție: în cadrul *predictive policing* sunt realizate prognoze cu privire la locurile și momentele în care este preconizată comiterea unor acte infracționale, precum și la autorii acestora. De asemenea, în SUA sunt utilizate astfel de sisteme în sprijinul jurisprudenței, de exemplu pentru stabilirea unei sentințe. O accentuare a acestor evoluții se remarcă în China, unde guvernul analizează și sancționează comportamentul cetățenilor prin intermediul unui *Social Credit System*.

În mare parte neclar este însă dacă și, la nevoie, cum poate fi compatibilizată folosirea, de către state, a sistemelor IA cu normele drepturilor omului. Această problemă apare în special în ceea ce privește dreptul la un proces echitabil (Art. 14 din *International Covenant on Civil and Political Rights*/ ICCPR) sau dreptul la viața privată (Art. 17 din ICCPR).

Utilizarea militară a sistemelor IA intră cu prioritate în sfera dreptului umanitar internațional. Numeroase state investesc deja masiv în dezvoltarea de sisteme de armament autonome. Chiar și un transfer parțial al deciziilor privind aplicarea forței către sisteme IA ar pune în mod fundamental sub semnul întrebării mecanismele de protecție ale dreptului umanitar internațional.

O necesitate de reglementare există și în ceea ce privește utilizarea sistemelor IA de către întreprinderile private. Orientare în acest sens oferă, și de această dată, normele de drept internațional: statele sunt responsabile inclusiv cu protejarea drepturilor omului de încălcări ale acestora de către terți. Întrucât cele mai multe companii acționează în acest domeniu la nivel transnațional, măsurile naționale trebuie completate cu forme adecvate de reglementare internațională.

ETHICAL or LEGAL DILEMMAS

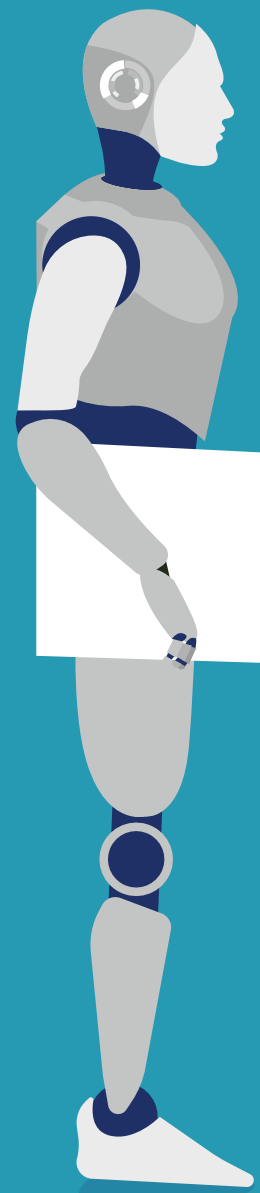
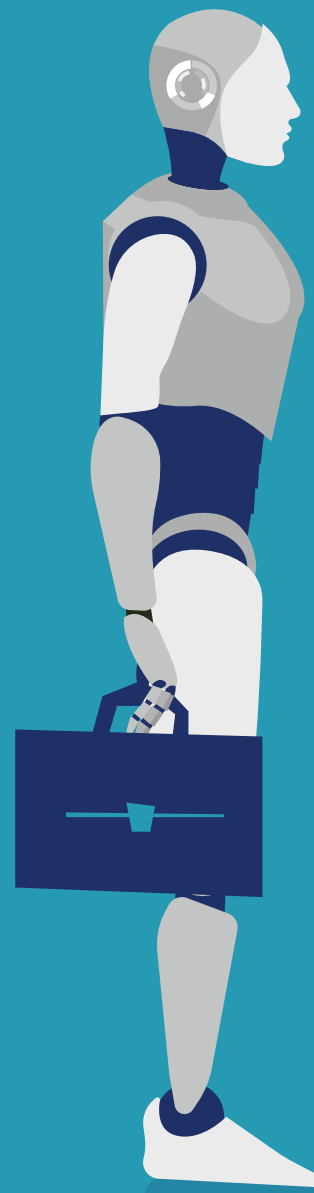
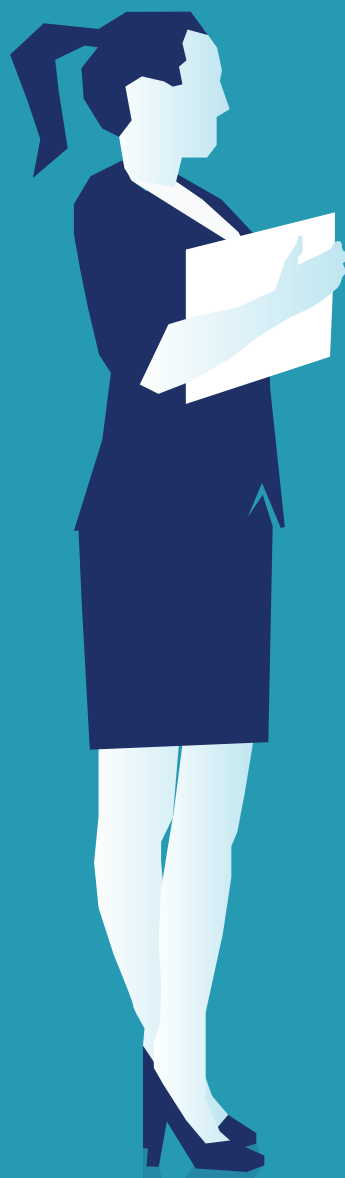
Although artificial intelligence allows for a much faster and objective analysis of data compared to human capabilities and, implicitly, the adoption of better-founded decisions, the responsibility for these is basically transferred to computer systems, whose *modus operandi* becomes similar to a black box.

The need for AI regulation arises when such systems are used in politically and human rights sensitive areas. In the context of the states' use of AI systems, human rights are an important starting point, as they draw attention to those applications in which the use of artificial intelligence is closely linked to state constraints. Countries such as the US or the UK have already introduced AI systems for the activity of police structures: predictive policing forecasts are made about where and when criminal acts are expected, as well as their perpetrators. Such systems are also used in the US to support court rulings, for example in order to pass a sentence. An emphasis on these developments is seen in China, where the government analyzes and sanctions citizens' behavior through a Social Credit System.

But it is largely unclear whether and, if necessary, how states' use of AI systems can be compatible with human rights laws. This issue arises in particular with regard to the right to a fair trial (Art. 14 of the International Covenant on Civil and Political Rights/ ICCPR) or the right to privacy (Art. 17 of the ICCPR).

The military use of AI systems comes as a priority within the scope of international humanitarian law. Many countries are already investing extensively in the development of autonomous weapon systems. Even a partial transfer of decisions concerning the use of force to AI systems would fundamentally question the protection mechanisms of international humanitarian law.

There is also a need for regulation concerning the use of AI systems by private companies. Guidance in this regard is again provided by the norms of international law: states are also responsible for protecting human rights from violations by third parties. As most companies operate in this field at trans-national level, national measures must be supplemented by appropriate forms of international regulation.



Firme private precum *Amazon*, *Google* sau *Baidu* folosesc sisteme IA pentru elaborarea unor profiluri ample de (potențiali) clienți. Aceste profiluri servesc personalizării inofensive a reclamelor sau furnizării de servicii digitale precum transmiterea unor mesaje personalizate.

Profilurile de persoane pot constitui însă și baza unor decizii importante: băncile, de exemplu, utilizează sisteme IA într-o măsură tot mai mare, pentru a evalua solvabilitatea propriilor clienți. Totodată, companii precum *LinkedIn* analizează cu ajutorul unor astfel de sisteme profilurile persoanelor aflate în căutarea unui loc de muncă. În cele din urmă, IA reprezintă un element esențial pentru dezvoltarea sistemelor de trafic autonome de către firme precum *Tesla*, *Google* sau *Baidu*.

Deși această formă de utilizare a IA de către companii nu este legată de constrângeri de ordin statal, ea are consecințe considerabile asupra vieții unui număr tot mai mare de oameni. Este responsabilitatea statelor să o reglementeze în concordanță cu norme precum interzicerea discriminării (Art. 26 din ICCPR) sau cu dreptul la protecția vieții private (Art. 17 din ICCPR).

Remarcabil este faptul că unele dintre cele mai importante companii solicită din proprie inițiativă o dezbatere publică pe tema reglementării sistemelor IA. Exemplară în acest sens este implicarea reprezentanților unor firme precum *Deepmind*, *Apple* și *IBM* în elaborarea *Asilomar AI Principles*. Principiile respective, concepute în 2017 în Asilomar (California/ SUA), formulează cerințe privind evoluția sistemelor IA și reliefează necesitatea creării unui cadru juridic adecvat pentru utilizarea acestora³⁰.

Private firms such as *Amazon*, *Google*, or *Baidu* use AI systems for drafting extensive profiles of (potential) clients. These profiles are used to harmlessly personalize marketing or for providing digital services such as the display of personalized messages.

Personal profiles can also form the basis for important decisions: banks, for example, are increasingly using AI systems to assess consumer solvency. At the same time, companies such as *LinkedIn* analyze the profiles of people looking for a job by using these systems. Finally, AI is an essential element for the development of autonomous traffic systems by companies such as *Tesla*, *Google*, or *Baidu*.

Although this form of corporate use of AI is not linked to state constraints, it entails substantial consequences for the lives of an increasing number of people. It is the responsibility of states to regulate this use in accordance with rules such as the prohibition of discrimination (Art. 26 of ICCPR) or the right to privacy (Art. 17 of ICCPR).

It is remarkable that some of the most important companies are calling for a public debate on the regulation of AI systems on their own initiative. Exemplary in this respect is the involvement of representatives of companies such as *Deepmind*, *Apple*, and *IBM* in developing the *Asilomar AI Principles*. These principles, conceived in Asilomar (California/ USA), in 2017, formulate requirements for the evolution of AI systems and emphasize the need to create an appropriate legal framework for their use³⁰.

COMPETIȚIA MARILOR PUTERI

China, Rusia și SUA au recunoscut oficial importanța critică a inteligenței artificiale pentru viitorul securității naționale, cele trei națiuni identificând în tehnologii IA precum drone autonome și *software*-uri de procesare date un instrument de creștere a capacității de apărare.

China demonstrează cea mai mare ambiție de a deveni o putere mondială în domeniul IA, Consiliul de Stat adoptând, încă din iulie 2017, o strategie detaliată în acest sens, cu obiectivul declarat de transformare a țării în „principal centru de inovație IA la nivel global”.

China urmărește să depășească Occidentul în domeniul IA până în anul 2025 și să devină lider global până în 2030, cu o industrie și dotări în valoare de 1,6 trilioane de dolari. Beijingul speră ca, prin programul strategic Made in China 2025³¹ și prin intermediul utilizării IA, să orienteze țara către o economie bazată pe inovație, parametri superiori de calitate și produse de înaltă tehnologie.

Pentru îndeplinirea acestui deziderat, în iulie 2017, Consiliul de Stat al Chinei a publicat Planul de dezvoltare a inteligenței artificiale de generație viitoare, iar în luna decembrie a aceluiași an, Ministerul Industriei și al Tehnologiei Informației (MIIT) a pus în aplicare Planul de Acțiune 2018 - 2020, destinat dezvoltării unei noi generații a industriei IA și centrat pe integrarea deplină a tehnologiei informației în vederea transformării Chinei într-o superputere în domeniul ciberneticii.

China este bine poziționată în ceea ce privește atingerea obiectivelor referitoare la IA, acest domeniu atrăgând, în perioada 2013 - 2018, 60% din finanțarea globală. În plus, companii chineze de top, precum *Alibaba*, *Tencent* și *Baidu*, folosesc deja inteligența artificială într-o gamă extinsă de servicii³².

Prin intermediul *Artificial Intelligence Industry Alliance/* AIIA, ca parte a strategiei sale de a obține *leadership*-ul global în domeniu, Guvernul chinez își propune să încurajeze colaborarea între guvernele locale, instituțiile academice și companii.

În unele cazuri, statul chinez folosește AIIA pentru a aloca subvenții companiilor favorizate din industria IA. În plus față de rolul său de a avansa politica industrială a Chinei, AIIA se remarcă printr-un eșantion diversificat de companii focusate pe IA (precum *Baidu*, *Alibaba*, *Tencent*, *Huawei* și *ByteDance*, cunoscute ca firme cu „joc pur”, care furnizează doar produse și/ sau servicii IA) sau cu activități prea puțin asociate IA (precum *Sinovation Ventures* și *Phicomm*).

În 2019, AIIA a cooperat cu *Transwarp Technology*³³, pentru a înființa o academie de formare IA în provincia Shaanxi. În același an, a semnat un acord cu *Meritdata*³⁴, pentru a oferi instruire personalului și a sponsoriza concursuri de IA.

GREAT POWER COMPETITION

China, Russia, and the US have officially recognized the critical importance of artificial intelligence for the future of national security, the three nations seeing AI-related technologies such as autonomous drones and intelligence processing software as tools for boosting defense capabilities.

China displays the highest ambition to become a global AI power, with the State Council adopting a detailed strategy in this regard as early as July 2017, officially stating the goal to turn the country into “the world’s leading AI innovation center”.

China aims to overtake the West in the field of AI by 2025 and become a global leader by 2030, with an industry and endowments worth 1.6 trillion dollars. Beijing hopes that, through the *Made in China 2025* strategic program³¹ and the use of AI, it will steer the country towards an innovation-based economy, with high quality parameters and high-tech products.

To fulfill this goal, in July 2017, the State Council of China published the Next Generation Artificial Intelligence Development Plan and, in December 201, the Ministry of Industry and Information Technology (MIIT) implemented the 2018-2020 Action Plan, aimed at developing a new generation of AI and focused on the full integration of information technology in order to turn China into a cyber superpower.

China is well-positioned to meet its AI targets, that sector attracting 60% of global funding between 2013 and 2018. In addition, leading Chinese companies such as *Alibaba*, *Tencent*, and *Baidu* are already using artificial intelligence for an extensive range of services³².

As part of its strategy to achieve global leadership in the field, the Chinese government aims to encourage cooperation among local governments, academic institutions, and companies through the *Artificial Intelligence Industry Alliance/* AIIA.

In some cases, China uses AIIA to allocate subsidies to favored companies in the AI industry. In addition to its role in advancing China’s industrial policy, AIIA stands out as a diverse sample of companies focused on AI activities (such as *Baidu*, *Alibaba*, *Tencent*, *Huawei*, and *ByteDance*, known as “pure play” companies, which provide only AI products and/ or services) or with very little AI activity (such as *Sinovation Ventures* and *Phicomm*).

In 2019, AIIA cooperated with *Transwarp Technology*³³ to establish an AI training academy in Shaanxi province. That same year, it signed an agreement with *Meritdata*³⁴ to provide staff training and sponsor AI competitions.

Alianța dispune de 10 grupuri de lucru – axate pe domenii precum standardizare și promovare, politici și reglementări, proprietate academică și intelectuală – care colectează contribuții de la parteneri publici și privați și elaborează cărți albe pe subiectele respective. Cartea albă a Alianței din decembrie 2020 privind proprietatea intelectuală, realizată în colaborare cu birouri guvernamentale chineze, universități de top și giganți tehnologici, prezintă tendințele brevetelor IA și oferă resurse companiilor pentru dezvoltarea proprietății intelectuale³⁵.

IA deține și va continua să dețină un rol important în domeniul apărării, Beijingul propunându-și să fabrice armament de înaltă tehnologie care să permită depășirea capacităților militare ale SUA prin integrarea tehnologiilor avansate la nivelul Armatei chineze (*People's Liberation Army/ PLA*). Totodată, se apreciază că întreaga gamă de tehnologii militare ale Chinei va fi dotată cu IA – de la vehicule de luptă aeriene fără pilot (UCAV), drone de tip *fire and forget* ori rachete – chiar și cele utilizate în atacuri cibernetice.

Strategia IA a Chinei conexează în mod direct evoluțiile inteligenței artificiale în plan comercial cu aplicații circumscrise domeniului apărării – o caracteristică puternic influențată de guvernarea centrală. *Baidu*, principala companie chineză furnizoare de servicii de Internet, administrează la nivel național un *Machine Learning Labor* în scopul creșterii competitivității. Universitatea Beihang, specializată în dezvoltarea dronelor militare, este, de asemenea, parte a proiectului chinez de *machine learning*.

Un aspect important îl constituie faptul că PLA își propune să utilizeze IA pentru susținerea operațiunilor de *intelligence* și a *system-of-systems warfare*. Potrivit cercetătorilor chinezi³⁶, supremația cunoașterii (adică abilitatea de a interfera cu sau de a distruge informațiile deținute de inamic) va substitui concepte anterioare de război, vizând obținerea superiorității militare în plan terestru, maritim și aerian și, mai recent, în domeniile cibernetic și spațial. Conform acestei abordări, odată deținută supremația în raport cu inamicii în spațiul informațional, controlul asupra altor domenii devine inutil. Utilizarea IA va fi, de asemenea, imperios necesară pentru sistemele de monitorizare și *early warning*³⁷.

În opinia expertului american Jon Harper³⁸, investiția PLA în capacități de IA militare este la fel de consistentă ca cea a Departamentului american al Apărării. Ca argument, expertul citează un raport al *Georgetown University Center for Security and Emerging Technology*³⁹, potrivit căruia, „pe fondul unei industrii a apărării înfloritoare, forțele armate chineze au făcut progrese extraordinare în ceea ce privește achiziția de sisteme IA pentru funcții de luptă și suport”. PLA este concentrată pe asigurarea de sisteme IA pentru analiză de *intelligence*, mentenanță, război informațional, precum și pentru navigație și recunoaștere pe vehicule autonome⁴⁰.

The Alliance has 10 working groups – focused on areas such as standardization and promotion, policies and regulations, academic and intellectual property – that collect contributions from public and private partners and produce white papers on the respective topics. The Alliance's December 2020 white paper on intellectual property, conducted in collaboration with Chinese government offices, top universities, and technology giants, covers trends in AI patents and provides resources for companies to develop intellectual property³⁵.

AI has and will continue to have an important role in the defense field, with Beijing aiming to manufacture high-tech weaponry that will enable China to overcome US military capabilities by integrating advanced technologies at People's Liberation Army/ PLA level. At the same time, China's entire range of military technologies will supposedly be equipped with AI – from unmanned aerial combat vehicles (UCAV), fire-and-forget drones, or missiles – even those used in cyberattacks.

China's AI strategy directly associates the commercial use of artificial intelligence with defense-related applications – an aspect which is strongly influenced by the central government. Baidu, China's leading Internet service provider, runs a nationwide Machine Learning Lab designed to increase competitiveness. Beihang University, which specializes in the development of military drones, is also part of the Chinese machine learning project.

An important aspect is that PLA plans to use AI to support intelligence operations and system-of-systems warfare. According to Chinese researchers³⁶, knowledge supremacy (i.e., the ability to interfere with or destroy information held by the enemy) will replace previous concepts of war, aiming to achieve military superiority on land, sea, and air and, more recently, in space and cyberspace. Based on this approach, once information supremacy over the enemies is established, it is useless to gain control over other domains. The use of AI will also be imperative for monitoring and early warning systems³⁷.

According to American expert Jon Harper³⁸, PLA's investment in military AI capabilities is as substantial as that of the US Department of Defense. In support of his opinion, the expert mentions a report drafted by the *Georgetown University Center for Security and Emerging Technology*³⁹, according to which “along with a thriving defense industry, the Chinese military has made tremendous progress in terms of acquiring AI systems for combat and support functions”. PLA is focused on procuring AI systems for intelligence analysis, maintenance, information warfare, as well as for navigation and reconnaissance on autonomous vehicles⁴⁰.



De asemenea, China dispune de atuul experienței utilizării IA în plan intern, în scopul monitorizării propriei populații, practică mai puțin exersată de democrațiile occidentale, având în vedere stilul diferit de guvernare⁴¹.

Potrivit unui raport⁴² elaborat de *Center for Naval Analyses/ CNA* din SUA, **Federația Rusă** își construiește, la rândul său, cadrul juridic structural și de guvernare necesar pentru a dezvolta și concura în IA, încercând să implementeze strategii la nivel național, în scopul promovării unui mediu care să susțină dezvoltarea digitală în Rusia. Punerea în aplicare a acestor eforturi este, în mare parte, condusă de Guvern prin intermediul întreprinderilor de stat, dar lipsa de accent pe inițiativele private ar putea afecta eforturile ruse în viitor.

O serie de firme de stat joacă un rol important în implementarea programului național „Economia digitală”. Guvernul a însărcinat *Rostec*⁴³ să creeze, împreună cu *Rostelecom*⁴⁴, foi de parcurs pentru *blockchain*, IoT și telecomunicații 5G. Și *Rosatom*⁴⁵ este profund implicată în economia digitală, având responsabilitatea principală pentru dezvoltarea calculului cuantic. De asemenea, *Rostec* și *Rosatom* au semnat (august 2020) un acord de intenție cu Guvernul rus pentru realizarea proiectului federal „Tehnologii digitale”, iar o serie de entități finanțate de stat, precum *Skolkovo*⁴⁶, au mai multe roluri minore în modernizarea digitală a Rusiei.

Inițiative de utilizare a inteligenței artificiale au și structuri guvernamentale ruse care nu sunt implicate în modernizarea digitală. În decembrie 2020, Ministerul Dezvoltării Digitale din Rusia a publicat o listă a proiectelor IA pe care și-a propus să le implementeze în patru ministere ruse și trei departamente guvernamentale până în anul 2024. Acestea presupun, printre altele, utilizarea inteligenței artificiale de către Ministerul Afacerilor Interne, analiza imaginilor cu ajutorul IA de către Ministerul Urgențelor pentru identificarea și gestionarea dezastrelor naturale și crearea unui *chatbot* bazat pe rețele neuronale pentru Ministerul Industriei și Comerțului.

Ecosistemul IA rus - constând, conform CNA, în clustere de activități interconectate în cadrul Guvernului, corporațiilor de stat, mediilor militar, academic și privat - are drept caracteristici-cheie conducerea companiilor de către stat și finanțarea amplă de care acestea beneficiază din partea Guvernului rus pentru dezvoltarea tehnologiilor compatibile IA.

Există „incubatoare” guvernamentale (*Skolkovo*), finanțatori (*Russian Direct Investment Fund*) și inițiative (*National Technology Initiative*) care vizează facilitarea dezvoltării tehnologiilor de acest tip. Deși sectorul privat este divers din punct de vedere al dimensiunii companiilor (de la firme precum Yandex la entități mult mai mici), numărul de *startup*-uri este redus în comparație cu cel din SUA și China⁴⁷.

At the same time, China has the advantage of having used AI internally to monitor its own population, a practice which is less commonly used by Western democracies, given their different form of governance⁴¹.

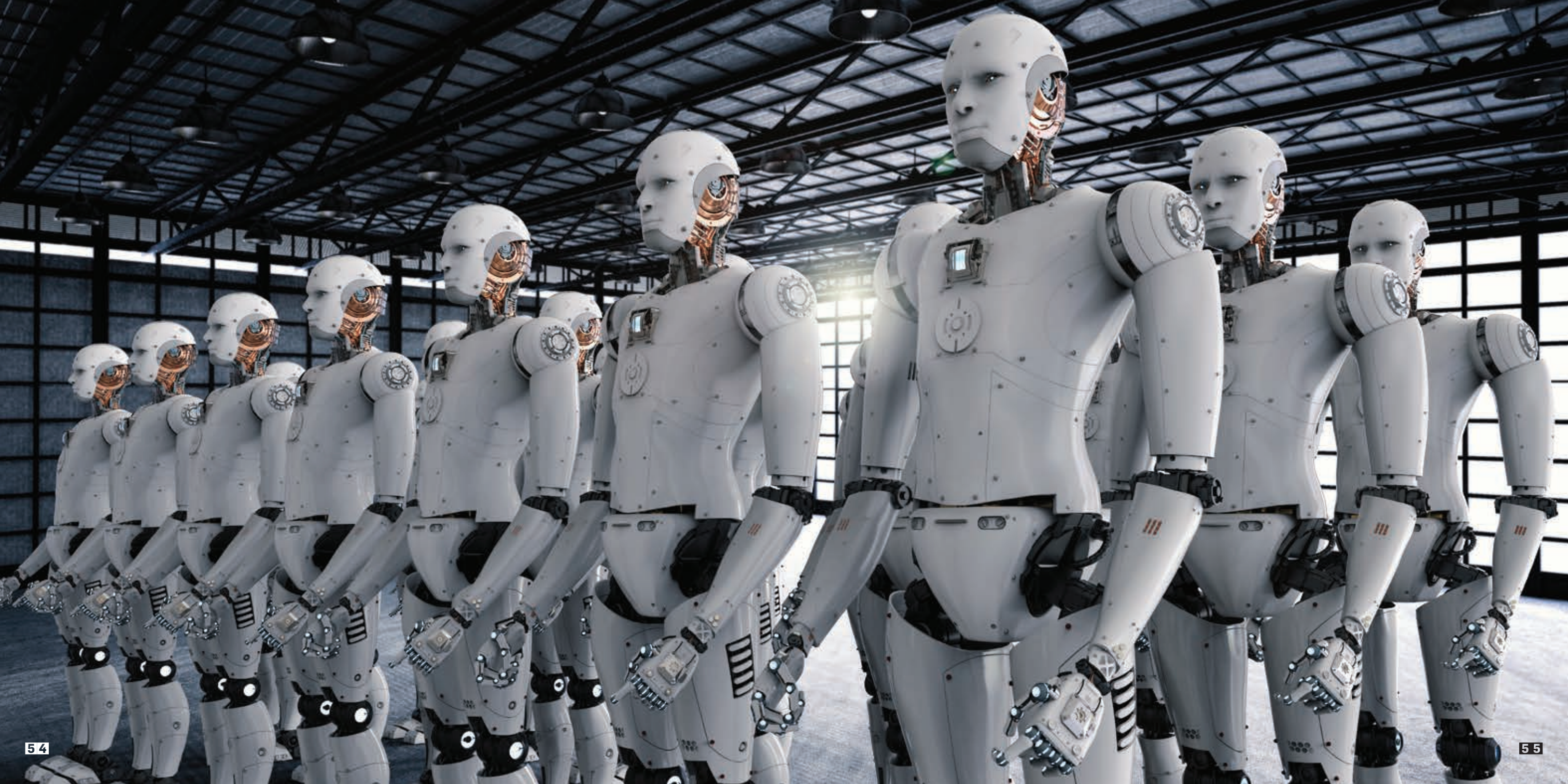
According to a report⁴² issued by the US *Center for Naval Analyses/ CNA*, the **Russian Federation** is currently building the structural and governing legal framework needed to develop and compete in the field of AI, seeking to implement nationwide strategies in order to promote an environment that supports Russia’s digital development. The implementation of these efforts is mainly led by the government through state-owned enterprises, but the lack of focus on private initiatives could affect Russian efforts in the future.

A number of state-owned enterprises play an important role in implementing the “Digital Economy” national program. The government has commissioned *Rostec*⁴³ to produce, in cooperation with *Rostelecom*⁴⁴, roadmaps for *blockchain*, IoT, and 5G telecommunications. *Rosatom*⁴⁵ is also deeply involved in the digital economy and has as main responsibility the development of quantum computing. *Rostec* and *Rosatom* also signed (August 2020) an agreement with the Russian Government to carry out the “Digital Technologies” federal project, while a number of state-funded entities such as *Skolkovo*⁴⁶ have several minor roles in Russia’s digital modernization.

Other initiatives to use artificial intelligence have also been launched by Russian government structures that are not involved in the digital modernization process. In December 2020, the Russian Ministry of Digital Development published a list of AI projects that it plans to implement in four Russian ministries and three government departments by 2024. These include, among others, the use of artificial intelligence by the Ministry of Internal Affairs, the use of AI image analysis by the Ministry of Emergency Situations for the identification and management of natural disasters, and the establishment of a neural network-based chatbot for the Ministry of Industry and Trade.

The key features of the Russian AI ecosystem – consisting, according to CNA, of clusters of activities that are interconnected within the government, state-owned corporations, the military, academia, and the private sector – are the leading role of the state in managing the companies and the extensive funding they receive from the Russian Government for the development of AI-compatible technologies.

There are government “incubators” (*Skolkovo*), financing entities (*Russian Direct Investment Fund*), and initiatives (*National Technology Initiative*) aimed at facilitating the development of such technologies. Although the private sector is diverse in terms of company size (from companies such as Yandex to much smaller entities), the number of start-ups is small compared to that in the US or China⁴⁷.



Compania de stat *Sberbank*, care a dezvoltat multe dintre inițiativele naționale în domeniu, beneficiază de conexiuni extinse în mediile private și statale de business și cercetare. În decembrie 2020, *Sberbank* a anunțat deschiderea unui *Artificial Intelligence Research Institute*, primul de acest gen în Rusia, cu misiunea promovării cercetării în IA. Totodată, în noiembrie 2019, a anunțat crearea unei *AI Alliance Russia*, sub patronajul Ministerului Dezvoltării Economice, în scopul consolidării cooperării în domeniul IA în sectorul privat. Din alianță fac parte *Russian Direct Investment Fund/ RDIF*, *Sberbank*, *Gazprom Neft*, *Yandex*, *Mail.ru* și *Mobile TeleSystem/ MTS*⁴⁸.

În domeniul militar, inovația este condusă de Ministerul Apărării de la Moscova, prin intermediul programelor de armament de stat, și facilitată de *Rostec* și alte întreprinderi de profil, cu finanțare de la „incubatoare” speciale. Este, însă, de așteptat ca și evoluțiile din mediul civil să se traducă în progrese militare.

Odată cu dezvoltarea sistemelor militare fără pilot, ministerul a început să investească resurse umane și materiale semnificative în dezvoltarea sistemelor de inteligență artificială în propriile departamente, academii, instituții și centre de cercetare și dezvoltare. Mai mult decât atât, în aprilie 2021, și-a anunțat intenția de înființare a unui departament specializat pentru dezvoltarea inteligenței artificiale, considerată esențială pentru consolidarea credibilității factorului de descurajare nucleară față de SUA, menținerea forței, îmbunătățirea capacității de avertizare timpurie și înfrângerea sistemelor de apărare antirachetă ale adversarului.

La rândul său, *National Defense Management Center/ NDMC* din Rusia, principalul nod militar C2⁴⁹ pe timp de criză sau de conflict, ar putea folosi tehnologii compatibile IA pentru facilitarea procesului decizional. Invocând „datele *open source* disponibile”, experții *Center for Naval Analyses* susțin că armata rusă va utiliza inteligența artificială în cadrul NDMC, dar nu va externaliza luarea deciziilor către sisteme IA. În schimb, tehnologiile de acest tip vor contribui la procesul decizional prin colectarea și transmiterea, în timp util, a tuturor informațiilor necesare operatorilor umani.

În majoritatea declarațiilor publice ale oficialilor ruși, inteligența artificială este discutată în termeni de C2 și ISR⁵⁰ pentru dezvoltarea și testarea vehiculelor autonome, care minimizează atât numărul de personal necesar, cât și pericolul asociat adesea cu misiunile de recunoaștere⁵¹.

Comisia rusă pentru industria armamentului și-a propus ca obiectiv ca, până în 2025, nivelul de producție a roboților de luptă să ajungă la 30% din totalul tehnologic militar.

Deși dispune de o industrie a tehnologiei mai slab reprezentată comparativ cu cea a Chinei sau a SUA, Moscova profită de tradiția sa academică în domeniul tehnico-științific. În opinia lui Gregory C. Allen, *fellow* în cadrul *think tank*-ului *Center for a New American Security* din Washington, Federația Rusă se pregătește să utilizeze IA ca parte a companiilor sale

State-owned company *Sberbank*, which has developed many of the national initiatives in this field, has extensive connections in the private and public business and research sectors. In December 2020, *Sberbank* announced the opening of an *Artificial Intelligence Research Institute*, the first of its kind in Russia, with the mission of promoting research in the field of AI. Furthermore, in November 2019, it announced the establishment of the *AI Alliance Russia*, under the patronage of the Ministry of Economic Development, aimed at strengthening cooperation in the field of AI in the private sector. The alliance includes *Russian Direct Investment Fund/ RDIF*, *Sberbank*, *Gazprom Neft*, *Yandex*, *Mail.ru* and *Mobile TeleSystem/ MTS*⁴⁸.

In the military field, innovation is led by the Russian Ministry of Defense, through state armament programs, and facilitated by *Rostec* and by other specialized companies, with funding from special “incubators”. However, civilian developments are also expected to translate into military progress.

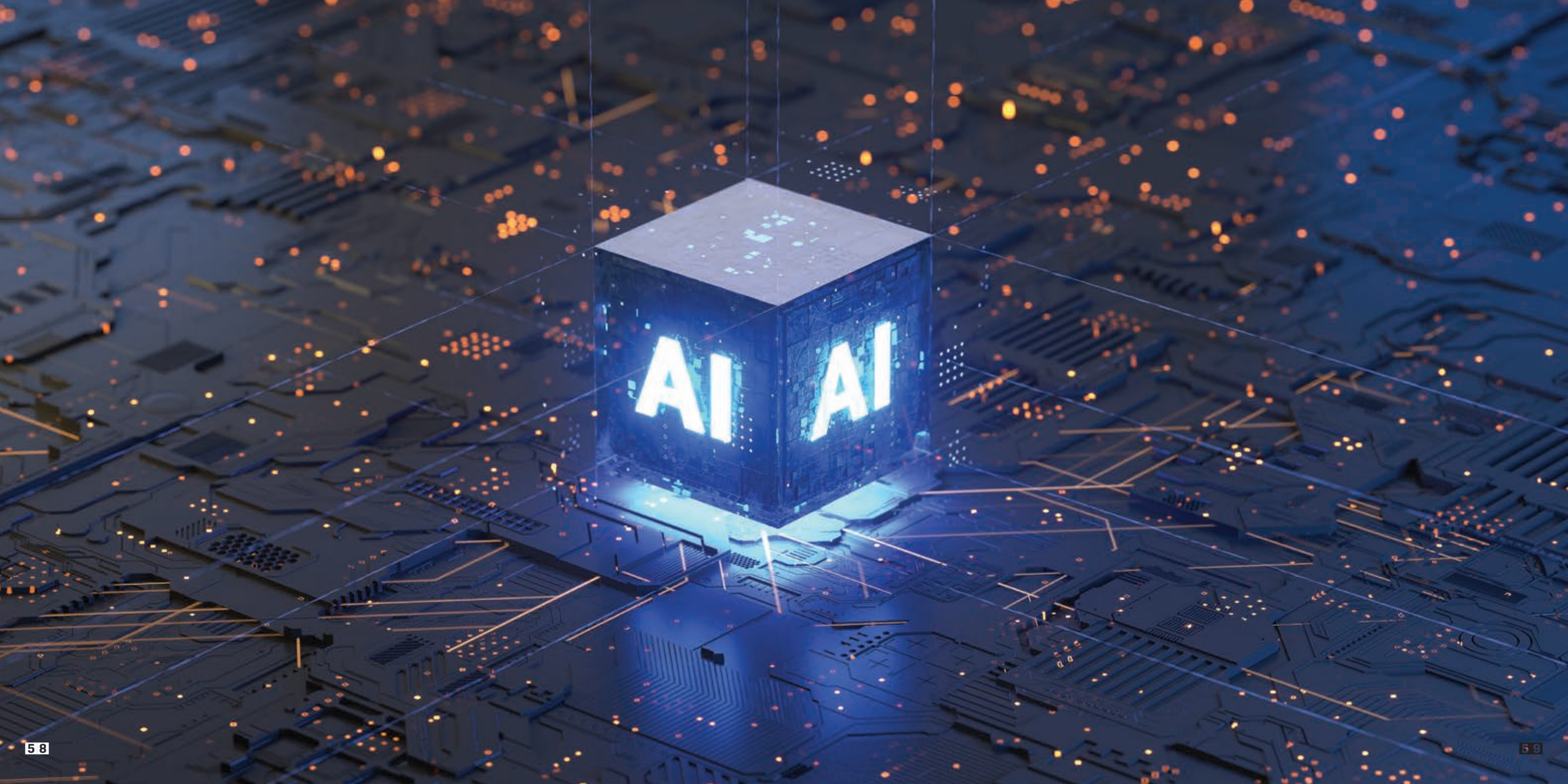
Concurrent with the development of unmanned military systems, the ministry has begun to invest significant human and material resources in the development of artificial intelligence systems across its departments, academies, institutions, and research and development centers. Moreover, in April 2021, it announced its intention to set up a specialized department for the development of artificial intelligence, which is considered essential for strengthening the credibility of its nuclear deterrence against the US, maintaining the force, improving its early warning capabilities, and defeating the opponent's missile defense systems.

The Russian National Defense Management Center/ NDMC, the main military C2 node⁴⁹ for crisis and conflict situations, could also use AI-compatible technologies to facilitate the decision-making process. Relying on “available open source data”, the experts from the Center for Naval Analyses believe that the Russian military will use artificial intelligence at NDMC, but it will not outsource decision-making to AI systems. Instead, such technologies will contribute to the decision-making process by collecting and sending, in a timely manner, all the information that human operators need.

In most public statements made by Russian officials, artificial intelligence is discussed in terms of C2 and ISR⁵⁰ for the development and testing of autonomous vehicles, which minimize both the number of personnel required and the danger often associated with reconnaissance missions⁵¹.

The Russian Military Industrial Commission has set the goal to bring combat robot production to 30% of all military technology by 2025.

Although it has a weaker technology industry as compared to that of China or the United States, Moscow takes advantage of its academic tradition in the technical and scientific field. According to Gregory C. Allen, a fellow at the Washington-based think tank *Center for a New American Security*, the Russian Federation is preparing to use AI as part of its impressive



impresionante de *hacking*, *social media* sau propagandistice. La fel ca Beijing, Guvernul rus dispune, grație caracterului său centralist, de mai multă putere de influențare a evoluției IA în plan național și se va axa, cel mai probabil, pe utilizarea inteligenței artificiale în domeniile militar și al serviciilor de informații⁵².

Principala țintă a eforturilor ruse de cooperare internațională în domeniul IA o constituie China, care a devenit, în ultimii cinci ani, partenerul-cheie al Moscovei în sfera *high-tech*, în general, și a IA, în special. Acest parteneriat s-a consolidat pe fondul alinierii tot mai pregnante a intereselor și preocupărilor de securitate, generată, în parte, de sentimentul comun că ambele țări sunt în competiție cu SUA și contestă rolul dominant al Washingtonului în sistemul internațional.

Politica americană față de aceste două state – inclusiv sancțiuni, controale la export și taxe vamale – au determinat Rusia și China să colaboreze mai strâns pentru a-și dezvolta industriile de înaltă tehnologie.

La nivelul anului 2019, Centrul Național de Cercetare a Inteligenței Artificiale din cadrul *Moscow Institute of Physics and Technology*/ MIPT a încheiat un parteneriat cu firma chineză *Huawei*. Într-o primă etapă a cooperării, *Huawei* a tradus în limba chineză primul număr (iunie 2019) al publicației bimestriale „*Artificial Intelligence*” a Centrului Național de Cercetare a Inteligenței Artificiale, fapt care a permis experților companiei chineze să se familiarizeze cu firmele de top din industria IA din Federația Rusă, respectiv să identifice entități cu care pot încheia noi parteneriate⁵³.

Strategia națională a Rusiei pentru dezvoltarea inteligenței artificiale până în 2030, adoptată prin decret prezidențial la 10 octombrie 2019, a inclus noutăți importante cu privire la abordarea acestui domeniu și evidențiază sectoarele-cheie în care Moscova întrevide oportunități și avantaje în planul competitivității. În pofida pretensei utilizări non-militare a IA, în strategie sunt menționate „domenii intermediare” în care ar putea fi folosite astfel de tehnologii (printre care *robotics & unmanned vehicle control* – deja testate de Moscova în Siria).

Strategia subliniază, totodată, importanța strategică a IA pentru ralierea Rusiei la grupul liderilor economici mondiali, precum și pentru independența și competitivitatea tehnologică a țării⁵⁴.

Încă din 2017, Vladimir Putin declara că IA este „viitorul, nu doar pentru Rusia, ci pentru întreaga omenire”, adăugând că „cine va deveni lider în acest domeniu, va deveni și liderul lumii”.

hacking, social media, or propaganda campaigns. Like Beijing, the Russian Government, thanks to its centralized nature, has more power to influence the evolution of AI at national level and will most likely focus on the use of artificial intelligence in the military and intelligence fields⁵².

The main target of Russia's international cooperation efforts in this field is China, which has become, for the past five years, Moscow's key high-tech partner in general and in the field of AI in particular. This partnership has been strengthened by a growing alignment of security interests and concerns, generated in part by the common belief that both countries are in competition with the United States and challenging Washington's dominant role on the international arena.

The US policy regarding these two states – including sanctions, export controls, and custom tariffs – has compelled Russia and China to work more closely together to develop their high-tech industries.

In 2019, the National Artificial Intelligence Research Center within the Moscow Institute of Physics and Technology/ MIPT established a partnership with the Chinese company *Huawei*. As a first step in their cooperation, *Huawei* translated into Chinese the first issue (June 2019) of *Artificial Intelligence*, the bimestrial magazine of the *National Artificial Intelligence Research Center*, which allowed the Chinese company's experts to become acquainted with the top companies in the Russian Federation's AI sector and to identify entities with which they could establish new partnerships⁵³.

Russia's National Strategy for the Development of Artificial Intelligence by 2030, adopted by presidential decree on October 10, 2019, includes important innovations regarding the approach to this field and highlights the key sectors where Moscow sees opportunities and advantages in terms of competitiveness. Despite the alleged non-military use of AI, the strategy mentions certain “intermediate fields” where such technologies could be used (including robotics & unmanned vehicle control – already tested by Moscow in Syria).

The strategy also emphasizes the strategic importance of AI for Russia's integration into the group of world economic leaders, as well as for the technological competitiveness and independence of the country⁵⁴.

As early as 2017, Vladimir Putin stated that AI is “the future not only for Russia, but for the entire humankind”, adding that “whoever becomes a leader in this field will also be the leader of the world”.



În contextul invadării Ucrainei, ambițiile președintelui rus în ceea ce privește inteligența artificială vor fi însă, probabil, afectate în mod semnificativ, sancțiunile economice impuse Kremlinului de Occident urmând a genera probleme financiare și, implicit, o încetinire a ritmului de implementare a IA în orice sector de activitate⁵⁵.

Deși **SUA** sunt recunoscute drept centru global al IA avansate, această evoluție a fost concentrată aproape în totalitate în sectorul privat, Administrația americană având mult de recuperat în ceea ce privește strategia și cercetarea în domeniu. Decidenții de la Washington nu pot impune sectorului tehnologic privat o cooperare similară celei existente în China, intensitatea acesteia variind în funcție de climatul politic⁵⁶.

Administrația SUA este depășită, în unele puncte, de cele două state în ceea ce privește utilizarea IA. Motivul: regimurile autoritare din aceste țări sunt dependente, pentru propria supraviețuire, de capacitatea de a identifica și contracara acțiunile subversive interne și pot face uz de tehnologie fără a respecta viața privată și drepturile cetățenești⁵⁷.

În acest context, *National Security Commission on Artificial Intelligence* (NSCAI) a solicitat, în ianuarie 2021, o creștere a finanțării R&D în domeniul inteligenței artificiale în următorii câțiva ani pentru a se asigura că America va fi capabilă să își mențină avantajul tactic asupra adversarilor și să asigure „pregătirea pentru IA militară” până în 2025⁵⁸.

De asemenea, un raport al NSCAI datat martie 2021 oferă o strategie integrată privind IA până în anul 2025. Documentul conține o serie de recomandări adresate Administrației de la Washington atât pentru dezvoltarea și utilizarea în mod responsabil a tehnologiilor care au la bază inteligența artificială, cât și pentru promovarea inovației în domeniu, în scopul îmbunătățirii competitivității naționale și protejării avantajelor critice ale SUA în concurența sa strategică cu națiuni precum China⁵⁹.

In the context of Ukraine's invasion, the Russian president's ambitions with regard to artificial intelligence will probably be significantly affected, as the economic sanctions imposed on the Kremlin by the West will generate financial difficulties and thus a slowdown in the implementation of AI in all sectors⁵⁵.

Although the **US** is recognized as a global center of advanced AI, this evolution focused almost entirely on the private sector, while the US Administration has much to recover in terms of strategy and research in this field. Washington's decision-makers cannot compel the private technology sector to cooperate on similar terms as in China, as the extent of cooperation varies depending on the political situation⁵⁶.

The US Administration is, in some points, outranked by the two countries in terms of AI use. The reason: authoritarian regimes in these countries depend for survival on the ability to identify and counter internal subversive actions and they can make use of technology with no respect for privacy and civil rights⁵⁷.

In this context, in January 2021, National Security Commission on Artificial Intelligence (NSCAI) called for an increase in R&D funding in artificial intelligence over the next few years to ensure that America would be able to maintain its tactical advantage over its adversaries and to achieve “military AI readiness” until 2025⁵⁸.

Also, a March 2021 NSCAI report provides an integrated strategy on AI by 2025. The document contains a number of recommendations addressed to the Washington Administration for responsibly developing and using artificial intelligence technologies, as well as for promoting innovation in the field, in order to improve national competitiveness and protect the critical advantages of the US in its strategic competition with nations such as China⁵⁹.

Experții NSCAI aduc în atenție **patru piloni** care necesită acțiuni imediate:

■ **leadership**: înființarea unui Consiliu pentru Competitivitate Tehnologică, în scopul elaborării, de către acesta, a unei strategii care să țină cont de provocările complexe de securitate, economice și științifice generate de IA și tehnologiile asociate;

■ **deficitul de talente**: crearea unei Academii de Servicii Digitale și a unei Rezerve Naționale Civile, care să ajute la dezvoltarea talentului tehnologic și la îmbunătățirea educației STEM și a sistemului de acceptare și păstrare a imigranților cu înaltă calificare;

■ **hardware**: revitalizarea producției interne de semiconductori și reevaluarea importanței rezilienței și securității lanțului de aprovizionare;

■ **investiții în inovare**: asocierea Administrației SUA cu companii americane în scopul dezvoltării de aplicații IA; dublarea investițiilor federale în vederea extinderii și democratizării cercetării și dezvoltării în domeniul inteligenței artificiale; construirea unei infrastructuri digitale sigure la nivel de țară, crearea de orașe inteligente și asigurarea unui acces partajat în cloud computing.

Referitor la competiția tehnologică sino-americană, raportul NSCAI avertizează asupra faptului că, deși SUA păstrează avantaje în domenii critice, **tendențele actuale sunt îngrijorătoare** și impun:

■ modernizarea controalelor la export și screening-ul investițiilor străine în scopul apărării tehnologiilor critice cu dublă utilizare;

■ protejarea centrelor de cercetare ca activ național prin acordarea de instrumente și resurse agențiilor guvernamentale, forțelor de ordine și instituțiilor academice pentru efectuarea de evaluări nuanțate ale riscurilor și pentru partajarea informațiilor privind amenințările;

■ construirea unei ordini tehnologice internaționale conforme normelor și valorilor democratice prin coordonarea, cu statele aliate și partenere, a politicilor și investițiilor destinate promovării și implementării infrastructurilor și tehnologiilor digitale și respectării standardelor globale în domeniu;

■ elaborarea unei liste unice și autorizate a tehnologiilor asociate IA (microelectronică, biotehnologie, calcul cuantic, 5G, robotică și sisteme autonome, tehnologii de stocare a energiei), care vor sprijini competitivitatea națională în secolul 21.

NSCAI experts draw attention to **four pillars** that require immediate action:

■ **leadership**: setting up a Council for Technological Competitiveness in order to develop a strategy that takes into account the complex security, economic, and scientific challenges generated by AI and associated technologies;

■ **talent shortage**: setting up a Digital Service Academy and a National Civil Reserve to help develop technological talent and improve STEM education and the system of accepting and retaining highly qualified immigrants;

■ **hardware**: revitalizing domestic semiconductor production and reassessing the importance of supply chain resilience and security;

■ **investments in innovation**: the association of the US Administration with American companies in order to develop AI applications; doubling federal investments to expand and democratize artificial intelligence research and development; building a secure digital infrastructure at country level, creating smart cities, and providing shared access to cloud computing.

Regarding the China-US technological competition, the NSCAI report warns that although the US still has advantages in critical areas, **current trends are worrisome** and require:

■ to modernize export controls and foreign investment screening in order to protect critical dual-use technologies;

■ to protect research centers as a national asset by providing tools and resources to government agencies, law enforcement agencies, and academic institutions for carrying out nuanced risk assessment and for sharing information on threats;

■ to establish an international technological order in accordance with democratic norms and values through coordination, with allied and partner states, of policies and investments aimed at promoting and implementing digital infrastructures and technologies and respecting global standards in the field;

■ to develop a unique and authorized list of AI-associated technologies (microelectronics, biotechnology, quantum computing, 5G, robotics and autonomous systems, energy storage technologies), which will support national competitiveness in the 21st century.

Spre deosebire de China și SUA, **UE** nu deține deocamdată o strategie coordonată pentru a promova dezvoltarea de tehnologii IA, dar se îndreaptă în această direcție. Un prim demers îl constituie proiectul de Regulament pentru stabilirea unor norme armonizate privind inteligența artificială, prezentat de Comisia Europeană în aprilie 2021. Cadrul legal propus se concentrază pe utilizarea specifică a sistemelor IA și pe riscurile asociate. Sunt stipulate o definiție neutră din punct de vedere tehnologic a sistemelor IA în legislația europeană și o clasificare a acestora, cu diferite cerințe și obligații adaptate unei „abordări bazate pe riscuri”.

Se urmărește interzicerea unor sisteme care prezintă riscuri „inacceptabile”, precum și autorizarea unei game ample de sisteme „cu risc ridicat”, dar supuse unui set de cerințe și obligații pentru obținerea accesului pe piața UE.

Sistemele „cu risc limitat” ar urma să fie supuse unor norme de transparență foarte laxe. Deși susțin, în general, propunerile Comisiei de la Bruxelles, părțile interesate și experții au solicitat o serie de amendamente, inclusiv revizuirea definiției sistemelor IA, extinderea listei de sisteme IA interzise, consolidarea mecanismelor de aplicare și asigurarea unui control democratic asupra configurării și implementării regulamentului privind IA⁶⁰.

Un pas către crearea unui *leadership* global al UE în domeniul IA îl constituie Planul Coordonat privind Inteligența Artificială, dedicat accelerării investițiilor în IA, elaborării de strategii și programe în domeniu și alinierii politicilor IA în vederea evitării fragmentării. Adoptat în 2018, acesta a fost revizuit în 2021 (*Coordinated Plan on Artificial Intelligence 2021 Review*), fiind aliniat cu prioritățile ecologice și digitale ale Comisiei Europene, precum și cu răspunsul blocului comunitar la pandemia de COVID-19. Documentul prevede investiții ale UE în IA în valoare de cel puțin un miliard de euro anual din programele *Horizon Europe* și *Digital Europe*.

O oportunitate fără precedent de modernizare și accelerare a investițiilor în IA o constituie Mecanismul de Redresare și Reziliență. Până în prezent, 19 din cele 27 de state membre au adoptat strategii naționale privind IA, în celelalte 8 țări (printre care se numără și România), o astfel de strategie fiind în curs de elaborare⁶¹.

Unlike China and the US, the **EU** does not yet have a coordinated strategy to promote the development of AI technology, but it is moving in this direction. A first step is the draft Regulation establishing harmonized rules on artificial intelligence presented by the European Commission in April 2021. The proposed legal framework focuses on the specific use of AI systems and the associated risks. The document stipulates a technologically neutral definition of AI systems in European legislation and also their classification, with different requirements and obligations adapted to "a risk-based approach".

The aim is to ban systems that present "unacceptable" risks and to authorize a wide range of "high-risk" systems, which are subjected to a set of requirements and obligations for obtaining access to the EU market.

"Limited risk" systems would have to follow very lax transparency rules. While generally supporting the European Commission's proposals, the interested parties and experts have called for a number of amendments, including revising the definition of AI systems, extending the list of AI banned systems, strengthening enforcement mechanisms, and ensuring democratic control over the configuration and implementation of the AI Regulation⁶⁰.

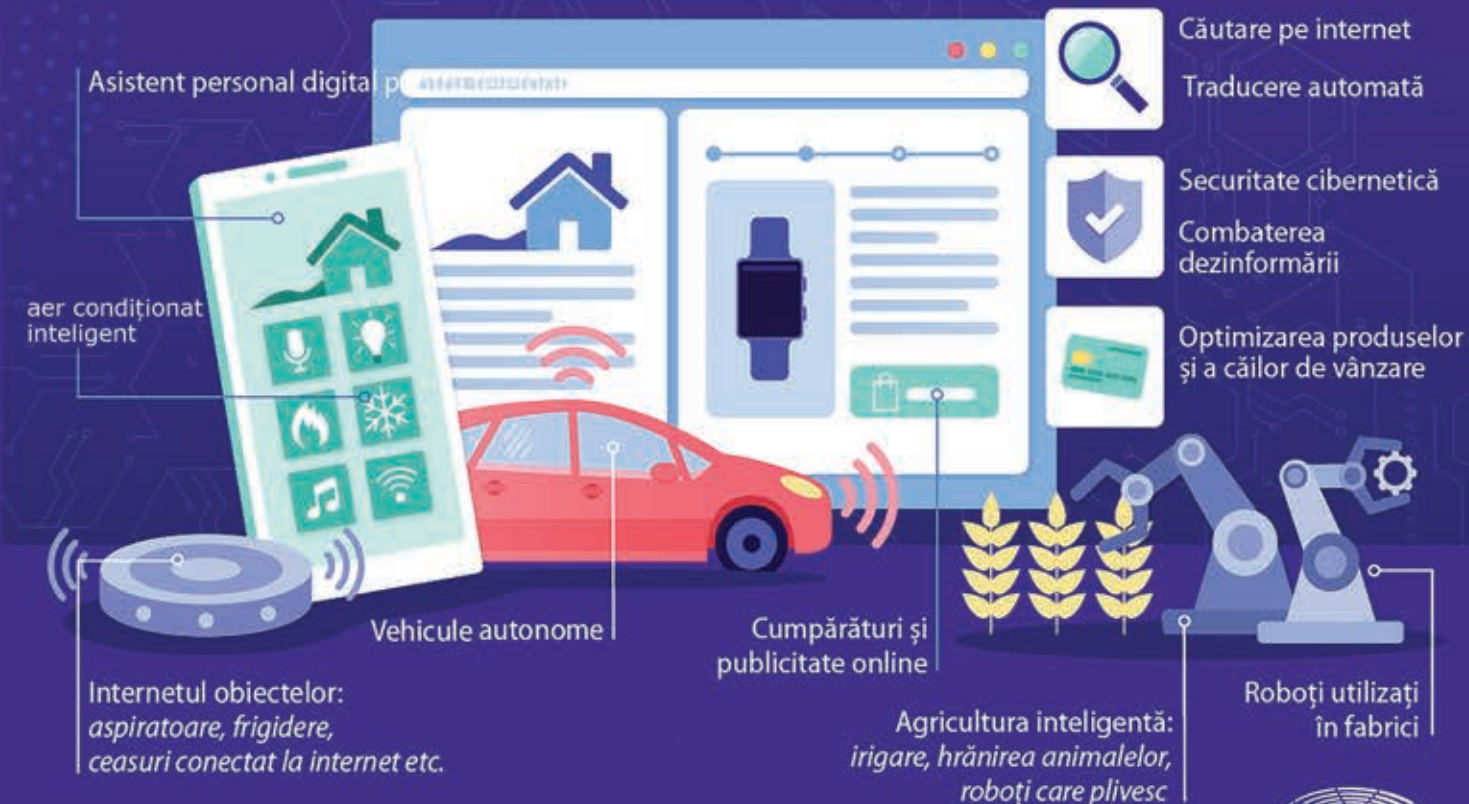
A step towards creating EU global leadership in AI is the Coordinated Plan on Artificial Intelligence, dedicated to accelerating AI investment, developing AI strategies and programs, and aligning AI policies to avoid fragmentation. Adopted in 2018, it was revised in 2021 (Coordinated Plan on Artificial Intelligence 2021 Review), being aligned with the European Commission's green and digital priorities, as well as with the EU's response to the COVID-19 pandemic. The document specifies EU investments in AI of at least 1 billion euros annually from the Horizon Europe and Digital Europe programs.

The Recovery and Resilience Facility represents an unprecedented opportunity to modernize and accelerate investment in AI. So far, 19 of the 27 Member States have adopted national AI strategies, while in the other 8 countries (including Romania) such strategies are in progress⁶¹.

INTELIGENȚA ARTIFICIALĂ

Utilizare zilnică și potențială

Câteva exemple despre cum folosim deja IA și despre posibilitățile pe care le oferă aceasta



ARTIFICIAL INTELLIGENCE

Everyday and potential use

A few examples of how we already use AI and the possibilities it offers



CONCLUZII

În domeniul *intelligence*, atât în ceea ce privește colectarea, cât și analiza datelor, IA oferă, în era *smart devices*, *Internet of Things* și *human internet activity*, posibilități de degrevare a resursei umane și de accelerare a proceselor analitice, inclusiv predictive.

Agențiile de informații trebuie să aibă însă o proiecție clară în ceea ce privește implementarea IA în activitatea specifică, din perspectiva modificărilor profunde pe care inteligența artificială le generează la nivel individual și statal, precum și a impactului asupra ordinii mondiale.

Intelligence-ului îi revine sarcina de a înțelege realitatea, respectiv de a contura scenarii viitoare, cu asumarea unui rol esențial în logica orientării opțiunilor politice pe linia apărării intereselor naționale, într-un *joint venture* IA – resursă umană.

Amplificarea dimensiunii spionajului cibernetic derulat de China, pe fondul avansului tehnologic al acesteia în domeniul IA, reclamă măsuri ferme din partea Uniunii Europene, respectiv a SUA, fie sub forma unor strategii coerente, fie a sancțiunilor concrete.

Oportunitățile tehnologice oferite de IA vor avea un impact major asupra viitorului. Dacă acesta va fi pozitiv sau negativ rămâne la latitudinea națiunilor, grupurilor și indivizilor, care își setează obiectivele pe care le vor atinse prin diversele utilizări ale unor astfel de tehnologii.

CONCLUSIONS

In the era of smart devices, Internet of Things, and human internet activity, AI offers, both in terms of data collection and data analysis, possibilities to reduce workload of employees and accelerate analytical processes, including predictive analytics, for the intelligence field.

Nevertheless, intelligence agencies should have a clear projection regarding the implementation of AI in their activity, considering the deep changes generated by artificial intelligence at individual and state level, as well as the impact on the world order.

Intelligence has the task of understanding the reality, namely to outline future scenarios, assuming an essential role in the logic of orienting political options towards defending national interests in an AI - human resource joint venture.

The increasing scale of China's cyberespionage efforts, due to its technological advance in AI, calls for strong measures from the European Union and the US, either in the form of coherent strategies or concrete sanctions.

The technological opportunities offered by AI will have a major impact on the future. Whether it will be positive or negative it is up to the nations, groups, and individuals to set the goals they want to achieve through the various uses of such technologies.

BIBLIOGRAFIE

¹ pe lângă Internetul lucrurilor, vehicule autonome, imprimare 3D, nanotehnologie, biotehnologie, stocarea energiei și calcul cuantic

² Klaus Schwab, „The Fourth Industrial Revolution: what it means, how to respond”, 14.01.2016, disponibil la <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>

³ <https://www.aist.org/resources/digital-applications-101/review-of-4-industrial-revolutions>

⁴ Alejandro Lapova, Michele Delera, „What is the Fourth Industrial Revolution?”, ianuarie 2021, disponibil la <https://iap.unido.org/articles/what-fourth-industrial-revolution>

⁵ Devon McGinnis, „What is the Fourth Industrial Revolution?”, 27.10.2020, disponibil la <https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir>

⁶ Klaus Schwab, „The Fourth Industrial Revolution: what it means, how to respond”, 14.01.2016, disponibil la <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>

⁷ George Lueddeke, „The Fourth Industrial Revolution and the Intelligence Era: What Next?”, 10.10.2021, <https://impakter.com/fourth-industrial-revolution-intelligence-era/>

⁸ <https://www.information-age.com/artificial-intelligence-fourth-industrial-revolution-123475170/>

⁹ Devon McGinnis, „What is the Fourth Industrial Revolution?”, 27.10.2020, disponibil la <https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir>

¹⁰ Yang Qiang, expert în inteligență artificială și data mining, profesor și șef al Computer Science and Engineering Department în cadrul Hong Kong University of Science and Technology, într-un interviu pentru „The UNESCO Courier”, 2018, disponibil la <https://en.unesco.org/courier/2018-3/fourth-revolution>

¹¹ ZDNet, „IT-Sicherheit: Schwachstellen mithilfe von Künstlicher Intelligenz suchen”/ Securitatea IT: Identificarea vulnerabilităților cu ajutorul inteligenței artificiale, 14.08.2017, disponibil pe [zdnet.de](https://www.zdnet.de)

¹² Center for a New American Security, „Artificial Intelligence and International Security”, iulie 2018, disponibil pe [cnas.org](https://www.cnas.org)

¹³ „Sécurité & Défense MAGAZINE”, „L'IA et la lutte contre le blanchement d'argent et le terrorisme”, 12.10.2017, disponibil pe [sd-magazine.com](https://www.sd-magazine.com); „Luxemburger Wort”, „L'intelligence artificielle contre le blanchiment d'argent”, 09.07.2021, disponibil pe [wort.lu](https://www.wort.lu)

¹⁴ Miles Brundage, Ben Garfinkel, Allan Dafoe, Carrick Flynn, Sebastian Farquhar, Clare Lyle, Owain Evans (Future of Humanity Institute/ University of Oxford); Shahar Avin, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield (Centre for the Study of Existential Risk/ University of Cambridge); Jack Clark, Michael Page, Dario Amodei (OpenAI); Helen Toner (Open Philanthropy Project); Peter Eckersley (Electronic Frontier Foundation); Paul Scharre, Gregory C. Allen (Center for a New American Security); Thomas Zeitzoff (American University); Bobby Filar, Hyrum Anderson (Endgame); Heather Roff (University of Oxford/ Arizona State University/ New America Foundation); Jacob Steinhardt (Stanford University); Rebecca Crootof (Information Society Project/ Yale University); Joanna Bryson (University of Bath); Roman Yampolskiy (University of Louisville)

¹⁵ „The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”, februarie 2018, disponibil pe [american.edu](https://www.american.edu)

¹⁶ Oliver Schonschek, Nico Litzel, „Künstliche Intelligenz als Angriffswerkzeug”, 08.05.2017, disponibil pe [bigdata-insider.de](https://www.bigdata-insider.de)

¹⁷ „The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”, februarie 2018, disponibil pe [american.edu](https://www.american.edu)

BIBLIOGRAPHY

¹ besides the Internet of Things, autonomous vehicles, 3D printing, nanotechnology, biotechnology, energy storage, and quantum computing

² Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond", January 14, 2016, available at <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>

³ <https://www.aist.org/resources/digital-applications-101/review-of-4-industrial-revolutions>

⁴ Alejandro Lapova, Michele Delera, "What is the Fourth Industrial Revolution?", January 2021, available at <https://iap.unido.org/articles/what-fourth-industrial-revolution>

⁵ Devon McGinnis, "What is the Fourth Industrial Revolution?" (October 27, 2020), available at <https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir>

⁶ Klaus Schwab, "The Fourth Industrial Revolution: what it means, how to respond", January 14, 2016, available at <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>

⁷ George Lueddeke, "The Fourth Industrial Revolution and the Intelligence Era: What Next?" (October 10, 2021), available at <https://impakter.com/fourth-industrial-revolution-intelligence-era/>

⁸ <https://www.information-age.com/artificial-intelligence-fourth-industrial-revolution-123475170/>

⁹ Devon McGinnis, "What is the Fourth Industrial Revolution?", October 27, 2020, available at <https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir>

¹⁰ Yang Qiang, expert on artificial intelligence and data mining, professor and head of Computer Science and Engineering Department at Hong Kong University of Science and Technology, in an interview with The UNESCO Courier, 2018, available at <https://en.unesco.org/courier/2018-3/fourth-revolution>

¹¹ ZDNet, "IT-Sicherheit: Schwachstellen mithilfe von Künstlicher Intelligenz suchen"/ IT Security: Identifying vulnerabilities with artificial intelligence, August 14, 2017, available on [zdnet.de](https://www.zdnet.de)

¹² Center for a New American Security, "Artificial Intelligence and International Security", July 2018, available on [cnas.org](https://www.cnas.org)

¹³ "Sécurité & Défense MAGAZINE", "L'IA et la lutte contre le blanchement d'argent et le terrorisme", October 12, 2017, available on [sd-magazine.com](https://www.sd-magazine.com); "Luxemburger Wort", "L'intelligence artificielle contre le blanchiment d'argent", July 9, 2021, available on [wort.lu](https://www.wort.lu)

¹⁴ Miles Brundage, Ben Garfinkel, Allan Dafoe, Carrick Flynn, Sebastian Farquhar, Clare Lyle, Owain Evans (Future of Humanity Institute/ University of Oxford); Shahar Avin, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield (Centre for the Study of Existential Risk/ University of Cambridge); Jack Clark, Michael Page, Dario Amodei (OpenAI); Helen Toner (Open Philanthropy Project); Peter Eckersley (Electronic Frontier Foundation); Paul Scharre, Gregory C. Allen (Center for a New American Security); Thomas Zeitzoff (American University); Bobby Filar, Hyrum Anderson (Endgame); Heather Roff (University of Oxford/ Arizona State University/ New America Foundation); Jacob Steinhardt (Stanford University); Rebecca Crootof (Information Society Project/ Yale University); Joanna Bryson (University of Bath); Roman Yampolskiy (University of Louisville)

¹⁵ "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", February 2018, available on [american.edu](https://www.american.edu)

¹⁶ Oliver Schonschek, Nico Litzel, "Künstliche Intelligenz als Angriffswerkzeug", May 8, 2017, available on [bigdata-insider.de](https://www.bigdata-insider.de)

¹⁷ "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", February 2018, available on [american.edu](https://www.american.edu)

¹⁸ Center for a New American Security, „Artificial Intelligence and International Security”, iulie 2018, disponibil pe cnas.org

¹⁹ Tristan Green, „CIA plans to replace spies with AI”, 23.04.2018, disponibil pe thenextweb.com

²⁰ National Security Commission on Artificial Intelligence, „Interim Report and Third Quarter Recommendations”, octombrie 2020, disponibil pe nscai.gov; Amy J. Nelson, Alexander H. Montgomery, „Is the U.S. military's futurism obsession hurting national security?”, 18.01.2022, disponibil pe brookings.edu

²¹ Institut israelian de cercetare, afiliat Universității Tel Aviv, abordează o tematică subsumată domeniului securității naționale, precum afaceri militare și strategice, terorism și conflicte de intensitate redusă, război cibernetic.

²² Shmuel Even, David Siman-Tov, „Research in the Intelligence Community in the Age of Artificial Intelligence”, octombrie 2020, disponibil pe strategiassessment.inss.org.il

²³ Marcel Dickow, Daniel Voelsen, „The Global Debate on the Future of Artificial Intelligence”, 16.04.2018, disponibil pe swp-berlin.org

²⁴ Jo Cavan, Paul Killworth, „GCHQ embraces AI, but not as a black box”, 08.10.2019, disponibil pe aboutintel.eu

²⁵ conceptualizare alternativă a inteligenței artificiale, focusată pe rolul de asistență al inteligenței artificiale, tehnologia cognitivă fiind considerată drept factor de augmentare a inteligenței umane, și nu de înlocuire a acesteia

²⁶ Paula Kift, „Augmentation as artifice: a Palantir look at AI”, 30.10.2019, disponibil pe aboutintel.eu

²⁷ Oskar J. Gstrein, „Predictive policing: positivism is not enough to rule our complex world”, 13.11.2019, disponibil pe aboutintel.eu

²⁸ Kwasi Mitchell, Joe Mariani, Adam Routh, „A task-level view of the impact of artificial intelligence on intel analysis”, 11.12.2019, disponibil pe www2.deloitte.com

²⁹ Brian Katz, „The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection”, 13.07.2020, disponibil pe csis.org

³⁰ Marcel Dickow, Daniel Voelsen, „The Global Debate on the Future of Artificial Intelligence”, 16.04.2018, disponibil pe swp-berlin.org

³¹ Elaborat (mai 2015) de Cabinetul premierului Li Keqiang, acesta vizează îmbunătățirea capabilităților în domeniile precum tehnologia informației, robotică, energie durabilă și aviație.

³² Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, 18.12.2018, disponibil pe iiss.org

³³ companie de Big Data și IA cu sediul în Shanghai

³⁴ firmă chineză de analiză a datelor

³⁵ Ngor Luong, Zachary Arnold, „China's Artificial Intelligence Industry Alliance”, mai 2021, disponibil pe cset.georgetown.edu

³⁶ Shen Shoulin, cercetător în cadrul Nanjing Army Command College, și Zhang Guoning, cercetător la Wuhan University/ China

³⁷ Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, 18.12.2018, disponibil pe iiss.org

³⁸ fost Managing Editor al revistei „National Defense”, în prezent Managing Editor al „DefenseScoop”

³⁹ Ryan Fedasiuk, Jennifer Melot, Ben Murphy, „Harnessed Lightning. How the Chinese Military is Adopting Artificial Intelligence”, octombrie 2021, disponibil pe cset.georgetown.edu

⁴⁰ Jon Harper, „China Matching Pentagon Spending on AI”, 06.01.2022, disponibil pe nationaldefensemagazine.org

⁴¹ Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, 18.12.2018, disponibil pe iiss.org

¹⁸ Center for a New American Security, „Artificial Intelligence and International Security”, July 2018, available on cnas.org

¹⁹ Tristan Green, „CIA plans to replace spies with AI”, April 23, 2018, available on thenextweb.com

²⁰ National Security Commission on Artificial Intelligence, „Interim Report and Third Quarter Recommendations”, October 2020, available on nscai.gov; Amy J. Nelson, Alexander H. Montgomery, „Is the U.S. military's futurism obsession hurting national security?”, January 18, 2022, available on brookings.edu

²¹ Israeli research institute affiliated to Tel Aviv University, approaches topics pertaining to the field of national security, such as military and strategic business, terrorism and low intensity conflicts, cyber war.

²² Shmuel Even, David Siman-Tov, „Research in the Intelligence Community in the Age of Artificial Intelligence”, October 2020, available on strategiassessment.inss.org.il

²³ Marcel Dickow, Daniel Voelsen, „The Global Debate on the Future of Artificial Intelligence”, April 16, 2018, available on swp-berlin.org

²⁴ Jo Cavan, Paul Killworth, „GCHQ embraces AI, but not as a black box”, October 8, 2019, available on aboutintel.eu

²⁵ alternative conceptualization of artificial intelligence, focused on the assisting role of AI, the cognitive technology being considered an augmenting factor for the human intelligence, not a replacement

²⁶ Paula Kift, „Augmentation as artifice: a Palantir look at AI”, October 30, 2019, available on aboutintel.eu

²⁷ Oskar J. Gstrein, „Predictive policing: positivism is not enough to rule our complex world”, November 13, 2019, available on aboutintel.eu

²⁸ Kwasi Mitchell, Joe Mariani, Adam Routh, „A task-level view of the impact of artificial intelligence on intel analysis”, December 11, 2019, available on www2.deloitte.com

²⁹ Brian Katz, „The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection”, July 13, 2020, available on [pe csis.org](https://csis.org)

³⁰ Marcel Dickow, Daniel Voelsen, „The Global Debate on the Future of Artificial Intelligence”, April 16, 2018, available on swp-berlin.org

³¹ Drafted (May, 2015) by Prime Minister Li Keqiang's Cabinet, it aims to improve capabilities in key areas such as information technology, robotics, sustainable energy, and aviation.

³² Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, December 18, 2018, available on iiss.org

³³ Big Data and AI company based in Shanghai

³⁴ Chinese data analysis company

³⁵ Ngor Luong, Zachary Arnold, „China's Artificial Intelligence Industry Alliance”, May 2021, available on cset.georgetown.edu

³⁶ Shen Shoulin, a researcher at the Nanjing Army Command College, and Zhang Guoning, a researcher at Wuhan University/ China

³⁷ Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, December 18, 2018, available on iiss.org

³⁸ former managing editor of the “National Defense” magazine, currently managing editor of “DefenseScoop”

³⁹ Ryan Fedasiuk, Jennifer Melot, Ben Murphy, „Harnessed Lightning. How the Chinese Military is Adopting Artificial Intelligence”, October 2021, available on cset.georgetown.edu

⁴⁰ Jon Harper, „China Matching Pentagon Spending on AI”, January 6, 2022, available on nationaldefensemagazine.org

⁴¹ Meia Nouwens, Helena Legarda, „China's pursuit of advanced dual-use technologies”, December 18, 2018, available on iiss.org

⁴² „Artificial Intelligence and Autonomy in Russia” (mai 2021), semnat de Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chesnut, Dmitry Gorenburg, Michael Kofman, Kasey Stricklin și Julian Waller, disponibil pe [cna.org](#)

⁴³ conglomerat cu sediul la Moscova, specializat în investiții în companii relevante strategic, active, în principal, în industriile high-tech și de apărare

⁴⁴ cel mai mare furnizor de servicii digitale din Rusia

⁴⁵ corporație activă în domeniul energiei atomice

⁴⁶ centru de inovație care are ca sarcini dezvoltarea și comercializarea noilor tehnologii

⁴⁷ Center for Naval Analyses, „Artificial Intelligence and Autonomy in Russia”, mai 2021, disponibil pe [cna.org](#)

⁴⁸ Geohistory, „Artificial Intelligence in Russia”, 20.02.2022, disponibil pe [geohistory.today](#)

⁴⁹ Command and Control

⁵⁰ Intelligence, Surveillance and Reconnaissance

⁵¹ Center for Naval Analyses, „Artificial Intelligence and Autonomy in Russia”, mai 2021, disponibil pe [cna.org](#)

⁵² Sammy Zimmermanns, „China, Russland und die USA befinden sich in einem Wettrüsten um Waffen mit künstlicher Intelligenz”, 13.09.2017, disponibil pe [cybersam.de](#)

⁵³ EurekAlert, „MIPT and HUAWEI started cooperation in the field of artificial intelligence”, 19.08.2019, disponibil pe [eurekalert.org](#); Das Deutsche Wissenschafts- und Innovationshaus in Moskau (DWIH Moskau/Casa Germană de Inovație și Știință din Moscova), „Das Kompetenzzentrum 'Nationale Technologische Initiative' am Moskauer Institut für Physik und Technologie (MIPT) hat die erste Ausgabe des 'Almanach der Künstlichen Intelligenz (KI)' veröffentlicht"/Centrul de competență Inițiativa Tehnologică Națională din cadrul Institutului de Fizică și Tehnologie din Moscova a publicat prima ediție a Almanahului Inteligenței Artificiale, 27.06.2019, disponibil pe [dwh-moskau.org](#)

⁵⁴ Sergey Sukhankin, „Russia Adopts National Strategy for Development of Artificial Intelligence”, 19.11.2019, disponibil pe [jamestown.org](#)

⁵⁵ Jonathan Vanian, „Invading Ukraine has upended Russia's A.I. ambitions - and not even China may be able to help”, 25.03.2022, disponibil pe [fortune.com](#)

⁵⁶ Sammy Zimmermanns, „China, Russland und die USA befinden sich in einem Wettrüsten um Waffen mit künstlicher Intelligenz”, 13.09.2017, disponibil pe [cybersam.de](#)

⁵⁷ Paul D. Shinkman, „Artificial Intelligence: Putting Machines to Work for the Spies”, 10.08.2017, disponibil pe [usnews.com](#)

⁵⁸ Gary Grossman, „The AI arms race has us on the road to Armageddon”, 19.04.2021, disponibil pe [venturebeat.com](#)

⁵⁹ Sara Hsu, „China and Artificial Intelligence”, 19.04.2021, disponibil pe [thediplomat.com](#)

⁶⁰ Parlamentul European, „Artificial intelligence act”, 14.01.2022, disponibil pe [europarl.europa.eu/thinktank/en](#)

⁶¹ Comisia Europeană, „Coordinated Plan on Artificial Intelligence 2021 Review”, disponibil pe [digital-strategy.ec.europa.eu](#)

⁴² „Artificial Intelligence and Autonomy in Russia” (May 2021), signed by Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chesnut, Dmitry Gorenburg, Michael Kofman, Kasey Stricklin, and Julian Waller, available on [cna.org](#)

⁴³ Moscow-based conglomerate specializing in investments in strategically relevant companies, active mainly in the high-tech and defense industries

⁴⁴ the largest digital service provider in Russia

⁴⁵ a corporation operating in the field of atomic energy

⁴⁶ an innovation center responsible for the development and marketing of new technologies

⁴⁷ Center for Naval Analyses, „Artificial Intelligence and Autonomy in Russia”, May 2021, available on [cna.org](#)

⁴⁸ Geohistory, „Artificial Intelligence in Russia”, February 20, 2022, available on [geohistory.today](#)

⁴⁹ Command and Control

⁵⁰ Intelligence, Surveillance and Reconnaissance

⁵¹ Center for Naval Analyses, „Artificial Intelligence and Autonomy in Russia”, May 2021, available on [cna.org](#)

⁵² Sammy Zimmermanns, „China, Russland und die USA befinden sich in einem Wettrüsten um Waffen mit künstlicher Intelligenz”, September 13, 2017, available on [cybersam.de](#)

⁵³ EurekAlert, „MIPT and HUAWEI started cooperation in the field of artificial intelligence”, August 19, 2019, available on [eurekalert.org](#); Das Deutsche Wissenschafts- und Innovationshaus in Moskau (DWIH Moskau/ the German House for Research and Innovation in Moscow), „Das Kompetenzzentrum 'Nationale Technologische Initiative' am Moskauer Institut für Physik und Technologie (MIPT) hat die erste Ausgabe des 'Almanach der Künstlichen Intelligenz (KI)' veröffentlicht"/ Competence Center of the National Technological Initiative hosted by the Moscow Institute of Physics and Technology published the first edition of the Artificial Intelligence Almanac, June 27, 2019, available on [dwh-moskau.org](#)

⁵⁴ Sergey Sukhankin, „Russia Adopts National Strategy for Development of Artificial Intelligence”, November 19, 2019, available on [jamestown.org](#)

⁵⁵ Jonathan Vanian, „Invading Ukraine has upended Russia's A.I. ambitions - and not even China may be able to help”, March 25, 2022, available on [fortune.com](#)

⁵⁶ Sammy Zimmermanns, „China, Russland und die USA befinden sich in einem Wettrüsten um Waffen mit künstlicher Intelligenz”, September 13, 2017, available on [cybersam.de](#)

⁵⁷ Paul D. Shinkman, „Artificial Intelligence: Putting Machines to Work for the Spies”, August, 10 2017, available on [usnews.com](#)

⁵⁸ Gary Grossman, „The AI arms race has us on the road to Armageddon”, April 19, 2021, available on [venturebeat.com](#)

⁵⁹ Sara Hsu, „China and Artificial Intelligence”, April 19, 2021, available on [thediplomat.com](#)

⁶⁰ European Parliament, „Artificial intelligence act”, January 14, 2022, available at [europarl.europa.eu/thinktank/en](#)

⁶¹ European Commission, „Coordinated Plan on Artificial Intelligence 2021 Review”, available at [digital-strategy.ec.europa.eu](#)



ÎNDRĂZNEȘTE. ÎNVAȚĂ. INOVEAZĂ.
WWW.ANIMV.RO