

Military Espionage – the Role of Drones and Autonomous Technologies

[Spionajul militar – rolul dronelor și tehnologiilor autonome]

Dan AMARINE¹

¹ Candidate Ph.D., Doctoral School of Legal and Economic Sciences, State University of Moldova, Romania, e-mail: dan_amarine@yahoo.com

Abstract

The emergence of unmanned aerial vehicles (UAVs), autonomous platforms, and artificial intelligence (AI) has transformed military espionage more profoundly than any technological innovation of the last century. From strategic surveillance conducted at high altitudes to miniature drones operating in urban combat environments, autonomous systems have redefined intelligence, surveillance, and reconnaissance (ISR) capabilities. Their ability to operate for long durations, penetrate hostile areas, and collect multispectral data has shifted the emphasis of military espionage from human-centered operations to machine-driven analysis and remote sensing.

This paper examines the evolution of espionage practices in contemporary warfare through the integration of autonomous technologies. It explores three fundamental dimensions:

(1) the strategic role of long-endurance UAVs capable of persistent monitoring and signals intelligence; (2) the tactical deployment of small, agile drones on the battlefield; (3) the progressive shift toward autonomous decision-making, including target recognition, pattern identification, and predictive analysis through AI. The study also evaluates hybrid systems such as loitering munitions-platforms that merge reconnaissance with precision strike capabilities.

Beyond technical aspects, the paper addresses ethical and legal challenges associated with the use of autonomous surveillance tools. The deployment of drones without pilot risk reduces political costs, potentially lowering the threshold for conducting cross-border espionage operations. AI-driven interpretation of data introduces concerns regarding algorithmic bias, accountability gaps, and the risk of misidentification. The proliferation of commercial drones has further democratized access to aerial surveillance, making it available not only to states but also to non-state actors and irregular groups.

Ultimately, the paper argues that drones and autonomous systems enhance the precision, speed, and scope of intelligence collection. However, their growing use calls for updated international regulations, transparent accountability mechanisms, and increased emphasis

on cyber-security and ethical restrictions. The future of military espionage will likely be determined by the balance between technological innovation, operational necessity, and the protection of fundamental human rights.

Keywords: military espionage; drones; autonomous systems; ISR; artificial intelligence; surveillance technologies.

How to cite: Amarine, D. (2026). Military Espionage – the Role of Drones and Autonomous Technologies. *Anuarul Universității "Petre Andrei" din Iași, Fascicula: Drept, Științe Economice, Științe Politice*, 36, 01-10.
<https://doi.org/10.63331/upalaw/36/01>

Introducere

Spionajul militar reprezintă una dintre componentele centrale ale artei războiului, fiind totodată și printre cele mai sofisticate forme de culegere a informațiilor. De-a lungul istoriei, informația a fost un multiplicator de putere: armatele care au reușit să colecteze, să interpreteze și să exploateze date despre adversar au obținut avantaje decisive.

În prezent, acesta a devenit o componentă fundamentală a securității naționale și a strategiilor geopolitice globale. Lucrarea de față analizează principalele direcții de evoluție ale spionajului militar contemporan, cu accent pe transformările tehnologice și implicațiile juridice.

Context istoric

Practica spionajului militar este atestată încă din Antichitate, fiind utilizată de marile imperii pentru a obține informații despre inamic. În Evul Mediu, spionajul a continuat să joace un rol semnificativ în războaiele de cucerire, iar în epoca modernă s-a profesionalizat. Războiul Rece a reprezentat o perioadă istorică marcată de tensiuni geopolitice, competiție tehnologică și rivalitate militară între Statele Unite ale Americii (SUA) și Uniunea Republicilor Sovietice Socialiste (URSS). Una dintre componentele cele mai importante ale acestui conflict ideologic a fost **obținerea informațiilor strategice**. Deși sateliții de spionaj aveau să devină principala sursă de date, începuturile recunoașterii aeriene moderne se leagă direct de primele **aparate de zbor fără pilot**, precursori ale dronelor militare contemporane. În acest context, „*Războiul Rece a fost o confruntare globală în care informațiile militare aveau un rol decisiv*”¹.

În continuare, vom analiza evoluția acestor aparate în timpul Războiului Rece, rolul lor în culegerea de informații, tehnologiile dezvoltate și impactul lor asupra strategiilor militare ulterioare.

Contextul geopolitic al Războiului Rece

După încheierea celui de-al Doilea Război Mondial, lumea a fost împărțită în două blocuri antagonice: cel occidental, condus de SUA, și cel estic, dominat de URSS. Rivalitatea dintre aceste puteri a generat o competiție continuă pentru supremație tehnologică și militară. Capacitatea de a obține informații despre inamic devenise crucială, cu atât mai mult cu cât ambele superputeri dezvoltau arsenal nuclear.

Până la apariția sateliților de spionaj la sfârșitul anilor 1950, principalele metode de recunoaștere erau misiunile aeriene pilotate. Acestea, însă, comportau riscuri enorme, atât pentru piloți, cât și pentru echilibrul politic internațional. Evenimentul doborârii avionului american U-2 în 1960 este un exemplu celebru, care a subliniat necesitatea unor alternative mai sigure în acțiunile de recunoaștere aeriană. Așadar, *Incidentul U-2 a determinat accelerarea programelor de recunoaștere fără pilot*².

Originile și evoluția aparatelor de zbor fără pilot

Primele concepte pentru aparate de zbor fără pilot au apărut în timpul Primului și celui de-al Doilea Război Mondial. Totuși, abia în contextul Războiului Rece aceste idei au fost

¹ Francis Gary Powers, *Operation Overflight*, Holt, 1970, p. 12.

² Kenneth Werrell, *The Evolution of UAV During the Cold War*, Air University Press, 1996, pp. 45-46.

dezvoltate sistematic, pentru a înlocui sau suplimenta misiunile riscante ale avioanelor pilotate.

Statele Unite au fost principalii inovatori, dezvoltând încă din anii '50 prototipuri de UAVs (Unmanned Aerial Vehicles) destinate recunoașterii. URSS, la rândul ei, a explorat aceste tehnologii, însă progresele au fost mai lente comparativ cu cele americane.

Motivele dezvoltării și recunoașterii importanței UAVs în timpul Războiului Rece au fost multiple. Printre acestea se numără: a) Reducerea riscurilor umane: folosirea dronelor elimina riscul capturării piloților, care putea genera situații politice sensibile. Criza U-2 a întărit argumentul utilizării aparatelor fără pilot; b) Capacitatea de operare în zone periculoase: UAV-urile puteau pătrunde în spații aeriene puternic apărate, unde șansele de supraviețuire ale avioanelor obișnuite erau reduse; c) Costuri reduse: comparativ cu un avion de recunoaștere precum U-2 sau SR-71, dronele experimentale erau mai ieftine de produs și de înlocuit; d) Progresul tehnologic: dezvoltarea miniaturizării, a camerelor de înaltă rezoluție și a controlului radio a făcut posibilă apariția unor UAV tot mai performante.

În acest context, au existat *proiecte și programe* de dezvoltare a UAVs în perioada Războiului Rece. Dintre **proiectele și programenle americane amintim**: 1. **Ryan Firebee**, unul dintre primele și cele mai de succes programe UAV americane, dezvoltat în anii 1950. Acest aparat era lansat de pe avioane de transport și recuperat ulterior cu parașuta. În timpul Războiului din Vietnam, Firebee a efectuat peste 3.000 de misiuni de recunoaștere. Astfel, „*Ryan Firebee a fost una dintre primele platforme UAV utilizate extensiv militar*”³, Firebee putea transporta camere foto, radar sau senzori infraroșu, devenind primul UAV utilizat sistematic în război; 2. **Programul „Lightning Bug”**, prin care a fost creat un nou model, o variantă dezvoltată special pentru recunoaștere și folosită pentru misiuni în sudul Chinei, Coreea de Nord și Vietnamul de Nord. Datorită utilizării sale, SUA au reușit să obțină date cruciale despre instalații militare greu accesibile; 3. **Experimente cu UAV de mare altitudine**: după criza U-2, au fost inițiate proiecte precum **Compass Arrow**, o dronă capabilă să opereze la altitudini mari pentru a evita radarele sovietice⁴.

URSS a investit la rândul său în tehnologia aparatelor de zbor fără pilot. Deși mai puțin mediatizate decât cele americane, **proiectele sovietice** au inclus „*vehicule precum Tupolev Tu-123 și Tu-141 pentru misiuni strategice*”⁴: 1. **Tupolev Tu-123 „Yastreb”** - lansat în 1964, Tu-123 era un UAV masiv, cu motor rachetă, proiectat pentru recunoaștere strategică la altitudini mari. Transporta echipamente foto avansate, dar era consumabil, nefiind recuperabil; 2. **Tupolev Tu-141 „Strizh”** - dezvoltat în anii 1970, Tu-141 avea o rază mare de acțiune și putea fi reutilizat. A fost utilizat până în anii 1980 pentru supravegherea frontierelor URSS. Recent, unele unități Tu-141 au fost reutilizate în conflicte moderne, demonstrând durabilitatea proiectului.

Dacă ne raportăm la tehnologiile utilizate în UAV-urile de recunoaștere, acestea includ: 1. **Sisteme foto și video**: primele drone foloseau camere fotografice analogice cu peliculă, declanșarea fiind controlată prin radio; filmul era recuperat la finalul misiunii; 2. **Senzori radar și infraroșu**; deși primitive comparativ cu tehnologia modernă, aceste sisteme permiteau detectarea instalațiilor militare și a activității terestre pe timp de noapte; 3. **Sisteme de control de la distanță**: controlul radio avea limitări mari, precum interferențe, distanță redusă și vulnerabilitate la bruiaj; ulterior au fost dezvoltate sisteme semi-autonome programate înainte de zbor; 4. **Materiale și design aerodinamic**: dronele erau proiectate

³ Robert F. Futrell, *The United States Air Force in Southeast Asia*, Air Force History, 1981, p. 88.

⁴ Yefim Gordon, *Soviet Strategic Reconnaissance Vehicles*, Midland Publishing, 2003, pp. 102–103.

pentru a zbura la altitudini mari și cu viteză ridicată, pentru a evita radarele și rachetele antiaeriene.

Avantajele UAV-urilor în misiunile de recunoaștere sunt multiple: eliminarea riscului politic major în cazul pierderii; costuri operaționale reduse, permițând misiuni repetate; capacitate de penetrare a apărării inamice; flexibilitate în adaptarea senzorilor; posibilitatea utilizării în zone inaccesibile pentru aviația pilotată.

Deși, așa cum am văzut, avantajele sunt multiple, nu pot fi eludate limitările și provocările din epocă: precizia redusă a sistemelor de navigație – înainte de GPS, UAV-urile depindeau de pilot automat și radio; calitatea senzorilor era limitată de tehnologia analogică; raza de acțiune era adesea mică; exista vulnerabilitate la bruij electronic; recuperarea era dificilă, multe modele fiind de unică folosință.

Totuși, utilizarea UAV-urilor în Războiul Rece a avut efecte importante: a facilitat schimbarea de paradigmă: informația devenea mai importantă decât forța brută; a pregătit terenul pentru dezvoltarea sateliților de recunoaștere, care au preluat rolul principal după 1965; a impulsionat cercetarea în domeniile autonomiei, miniaturizării și telecomunicațiilor; a redus riscul escaladării conflictelor prin evitarea incidentelor diplomatice precum cel din 1960.

În acest context al discursului, nu putem să nu amintim și tranziția către era sateliților de spionaj. Începând cu programul american CORONA (1959), sateliții au devenit principala sursă de informații strategice. Totuși, UAV-urile nu și-au pierdut relevanța, fiind utilizate complementar pentru: misiuni la altitudine joasă, supravegherea zonelor mobile, colectarea de date care nu puteau fi obținute din spațiu. Astfel, dronele au reprezentat puntea tehnologică dintre recunoașterea aeriană pilotată și cea spațială.

Așadar, multe dintre dronele moderne, precum MQ-1 Predator sau Global Hawk, își au originea conceptuală în proiectele anilor '50-'80: zbor autonom, transmitere în timp real a imaginilor, integrarea senzorilor multipli, capabilități stealth. Prin urmare, Războiul Rece a creat condițiile pentru apariția industriei UAV actuale, care a devenit esențială în conflictele moderne și în operațiunile de supraveghere globală.

Nu în ultimul rând, câteva aspecte legate de *Dreptul Internațional Public* trebuie menționate. Operațiunile de recunoaștere desfășurate cu UAV-uri în timpul Războiului Rece ridică probleme privind principiul suveranității statelor, deoarece fiecare stat deține control exclusiv asupra spațiului său aerian⁵. Trimiterea unui UAV în spațiul aerian al unui alt stat, fără consimțământ, poate constitui o încălcare a interdicției folosirii forței prevăzută de Carta ONU⁶. Spionajul, inclusiv cel realizat prin mijloace aeriene fără pilot, nu este reglementat explicit în dreptul internațional, dar statele pot reacționa în temeiul suveranității și protejării securității naționale⁷.

Problemele moderne legate de responsabilitatea statelor pentru utilizarea sistemelor autonome își au originea în dezbaterile similare din perioada Războiului Rece privind controlul și imputabilitatea acțiunilor UAV-urilor⁸.

Recunoașterea aeriană prin aparate de zbor fără pilot a constituit un element crucial în dinamica Războiului Rece. Deși sateliții aveau să domine ulterior domeniul informațiilor strategice, primele UAV-uri au demonstrat valoarea militară a tehnologiei fără pilot. Ele au

⁵ UN Charter, Article 2(4), United Nations, 1945.

⁶ Chicago Convention on International Civil Aviation, ICAO, 1944, Article 1.

⁷ Nico Schrijver, *Sovereignty over Natural Resources*, Cambridge University Press, 1997, p. 55.

⁸ Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO CCDCOE, 2013, p. 22.

oferit un mijloc eficient, relativ sigur și antrenează evoluții tehnologice majore, care astăzi sunt indispensabile în operațiunile militare contemporane. Datorită lor, recunoașterea aeriană a devenit mai precisă, mai flexibilă și mai puțin dependentă de factorul uman. Războiul Rece a fost astfel nu doar o confruntare geopolitică, ci și un catalizator al progresului tehnologic ce continuă să influențeze lumea actuală.

Spionajul militar contemporan

După cum afirmă Goodman, spionajul militar contemporan „este marcat de utilizarea dronelor și a tehnologiilor autonome care permit colectarea informațiilor fără expunere directă a personalului militar”⁹. De-a lungul timpului, el a evoluat de la metode tradiționale la tehnici sofisticate care implică tehnologia spațială.

Un exemplu în acest sens ar fi *spionajul satelitar și recunoașterea orbitală*. Sateliții de recunoaștere permit monitorizarea mișcărilor trupelor, instalarea de radar, urmărirea transporturilor și supravegherea infrastructurilor critice.

Spionajul satelitar are câteva caracteristici: *detalii tehnice* – rezoluție mare, capacitate de analiză multispectrală și radar; *transparență aparentă* – lansarea de sateliți este publică, dar operațiunile și analiza datelor sunt secrete; *aspect juridic* – conform Tratatului privind spațiul cosmic (1967), spațiul cosmic este liber pentru explorare, dar colectarea de informații de către sateliți nu este interzisă, creând o zonă gri între spionaj și recunoaștere legală.

Exemple practice în acest sens sunt sateliții Keyhole (SUA), Kosmos (Rusia), sateliți europeni precum Sentinel și SAR.

Astfel, spionajul satelitar permite obținerea rapidă de informații strategice fără violarea directă a teritoriului statului vizat.

În același context, amintim *spionajul cibernetic militar*. O dimensiune esențială a spionajului contemporan este cibernetica, care permite accesul la informații sensibile fără prezență fizică. Printre posibilele *tipuri de atacuri cibernetice* se numără: *interceptarea comunicațiilor militare* – hacking de servere sau rețele militare; *sabotajul digital* – manipularea datelor sau sisteme critice, de exemplu SCADA, drone autonome „*Dronele moderne execută misiuni de recunoaștere, supraveghere persistentă și colectare SIGINT/ELINT*”¹⁰; *atacuri asupra infrastructurii dual-use* – infrastructuri civile cu impact militar, supravegherea transnațională – prin cloud, satelit și internet.

Referitor la *jurisprudența și normele spionajului militar*, Tallinn Manual 2.0 (2017) stabilește că atacurile cibernetice care cauzează daune comparabile cu atacurile armate pot fi considerate acte de război. De asemenea, statul care permite sau tolerează atacurile poate fi tras la răspundere internațională. Totuși, spionajul cibernetic ridică probleme complexe de atribuție, dificultatea identificării actorului și lipsa unor sancțiuni uniforme internaționale.

În ceea ce privește categoriile de *actori implicați* în spionajul militar contemporan, acestea sunt multiple: *statele suverane* – tradiționalele servicii de informații militare (CIA, GRU, DGSE, MI6); *agenții private și firme de intelligence* – subcontractate de guverne sau entități private, cum ar fi NSO Group; *actori non-statali* – organizații criminale sau hackeri independenți, folosiți pentru operațiuni hibride; *organizații internaționale* – NATO și UE folosesc spionaj strategic pentru protecția infrastructurilor critice. Însă problemele juridice relaționate cu unele dintre aceste categorii nu lipsesc: actorii privați și non-statali complică atribuția răspunderii; controlul statului asupra activităților private trebuie dovedit pentru

⁹ Michael Goodman, *The Official History of the Joint Intelligence Committee*, Routledge, 2014, p. 22.

¹⁰ Peter Bergen, *Drone Wars*, Cambridge University Press, 2021, p. 103.

răspundere internațională; normele europene privind protecția datelor și securitatea cibernetică impun limite și standarde.

Un alt aspect al colectării de informații secrete îl constituie *spionajul hibrid și războiul informațional*. Spionajul contemporan combină cibernetica, satelitul, infiltrările și propaganda digitală. Astfel, *dezinformarea strategică* – afectarea deciziilor politice și militare ale unui stat prin știri false, manipularea rețelelor sociale și campanii de influență; *atacurile hibride* – combinarea spionajului clasic cu acțiuni ciberneticе și sabotaj industrial; *vulnerabilitatea populației și a infrastructurilor civile* – spionajul modern vizează inclusiv date civile pentru a obține avantaje strategice, sunt doar câteva dintre posibilele elemente ale sferei menționate. Exemple recente în acest sens sunt conflictele din Ucraina (2022-2025) și utilizarea intensă a dronelor și a atacurilor ciberneticе pentru colectarea de informații militare, precum și operațiunile de hacking asupra comunicațiilor NATO și ale statelor membre UE.

O altă componentă importantă este *spionajul economic cu implicații militare*. Acesta presupune: colectarea de informații despre cercetare și dezvoltare în domeniul tehnologic și armament; transferurile de tehnologie și know-how către state străine prin infiltrarea companiilor și instituțiilor; utilizarea firmelor private de intelligence pentru achiziția de date sensibile. Acest tip de spionaj evidențiază legătura între securitatea națională și economia strategică, necesitând răspunsuri juridice și instituționale eficiente.

Raportându-ne la războiul din Ucraina (2022-2025), *utilizarea dronelor* pentru supraveghere și recunoaștere rapidă a devenit o constantă, chiar dacă conform Convenției de la Chicago „utilizarea dronelor peste teritoriul unui stat fără consimțământ ridică probleme de suveranitate aeriană conform”¹¹. De asemenea, nu au lipsit nici *spionajul cibernetic* asupra comunicațiilor militare și civile ori propaganda și dezinformarea pentru influențarea deciziilor politice interne și externe. Totodată, softuri precum *Pegasus* au operat în scop militar și de securitate.

Pe **cale de consecință**, se poate conchide că: spionajul militar contemporan este multidimensional, combinând tehnologia, infiltrarea și manipularea informațională; sateliții, dronele și atacurile ciberneticе au extins domeniul de acțiune al spionajului, creând provocări juridice noi, însă „operatorii rămân responsabili pentru utilizarea sistemelor autonome, conform principiului controlului uman semnificativ”¹²; deși actorii implicați pot fi atât statali, cât și privați sau non-statali, ceea ce complică atribuția responsabilității, totuși, „în situații de conflict, dreptul internațional umanitar impune respectarea principiilor distincției și proporționalității”¹³; spionajul economic și hibrid subliniază necesitatea unui cadru legal modern și cooperare europeană și internațională; studii de caz recente demonstrează aplicabilitatea practică și complexitatea problemei în secolul XXI.

Protecția juridică europeană împotriva spionajului militar

Uniunea Europeană și statele membre au dezvoltat un *cadru juridic* complex pentru protecția împotriva spionajului militar, care se concentrează pe securitatea cibernetică, protecția infrastructurilor critice și reglementarea informațiilor clasificate. Principalele acte normative în acest sens sunt:

¹¹ Chicago Convention on International Civil Aviation, ICAO, 1944, Article 1.

¹² Michael Schmitt, *Drone Operations and LOAC*, Naval War College Review, 2013, p. 38.

¹³ Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge UP, 2005, pp. 74–75.

1. Directiva (UE) 2022/2555 privind securitatea rețelelor și sistemelor informatice (NIS2) (aceasta: introduce cerințe stricte pentru infrastructurile critice, inclusiv cele cu aplicații militare; impune evaluarea riscurilor și raportarea incidentelor de securitate; obligă statele membre să coopereze și să partajeze informații cu organismele europene);

2. Regulamentul (UE) 2019/881 – Cybersecurity Act (acesta: creează un cadru european de certificare a securității cibernetice; stabilește standarde minime pentru echipamentele și software-ul utilizat în scop militar; sprijină dezvoltarea capacităților UE în protecția digitală);

3. Regulamentul (UE) 2019/2121 privind protecția informațiilor clasificate (acesta: introduce norme uniforme pentru clasificarea, stocarea și transferul informațiilor sensibile între statele membre; facilitează cooperarea între instituțiile civile și militare și reduce riscul scurgerilor de informații).

Aceste acte normative au rolul de a completa dreptul internațional clasic, oferind măsuri concrete de protecție împotriva spionajului modern.

Totodată, *Curtea Europeană a Drepturilor Omului* (CEDO) a abordat protecția drepturilor fundamentale în contextul activităților de spionaj și supraveghere: 1. Weber & Saravia v. Germany (2006) – condamnarea supravegherii excesive a comunicațiilor interne, chiar în context de securitate națională; 2. Liberty v. United Kingdom (2008) – protecția vieții private și a comunicațiilor față de interceptarea secretă; 3. Big Brother Watch și alții v. United Kingdom (2021) – limitele statului în colectarea și stocarea masivă de date, inclusiv informații militare și cibernetice.

Concluziile jurisprudențiale subliniază echilibrul necesar între securitatea națională și drepturile fundamentale. În context european, spionajul militar trebuie să fie reglementat astfel încât să nu compromită libertățile civile și protecția datelor.

De asemenea, au fost avute în vedere *protecția infrastructurilor critice și securitatea cibernetică*. Referitor la *infrastructurile critice*, în categoria acestora intră structurile și sistemele esențiale pentru funcționarea statului, inclusiv energia, transportul, telecomunicațiile și comunicațiile militare. Cât privește *protecția*, aceasta presupune implementarea standardelor de securitate, auditul intern și planurile de continuitate. Pentru aceasta, cooperarea transfrontalieră este foarte importantă, UE și NATO dezvoltând proceduri comune pentru prevenirea atacurilor și gestionarea incidentelor.

Cât privește *securitatea cibernetică*, aceasta presupune: utilizarea certificării UE pentru echipamente și software militare; identificarea vulnerabilităților în rețelele militare și dual-use; exerciții comune și schimb de informații pentru contracararea atacurilor hibride. Aceste măsuri permit detectarea și prevenirea spionajului cibernetic, reducând vulnerabilitatea statelor membre.

Nu în ultimul rând, protecția împotriva spionajului necesită o *coordonare complexă între instituțiile statale*, fie ele *servicii militare* (care au responsabilitatea principală pentru informațiile strategice și tactice), *servicii civile de intelligence* (care monitorizează comunicațiile și previn infiltrările), *autorități naționale de securitate cibernetică* (ce implementează standardele NIS2 și Cybersecurity Act) ori *de cooperare europeană* (schimb de bune practici, alerte rapide și proiecte comune de securitate, prin ENISA și EDA). Această cooperare este esențială pentru gestionarea eficientă a riscurilor și prevenirea vulnerabilităților.

Mai mult, *echilibrul între securitate și drepturile fundamentale* este atent monitorizat. Spionajul militar european se desfășoară într-un cadru juridic strict, care urmărește protecția cetățenilor prin felul în care are loc *colectarea de informații* (aceasta trebuie să respecte

proportionalitatea și să fie justificată strategic, prin asigurarea *transparenței și realizarea auditului intern* (care limitează abuzurile și infiltrațiile ilegale). Totodată, în timp ce statele membre trebuie să respecte *Dreptul european al protecției datelor* (GDPR) în operațiunile dual-use, Curtea Europeană și organismele europene monitorizează respectarea standardelor și aplicarea sancțiunilor.

Astfel, UE creează un cadru legal armonizat, care protejează atât securitatea statelor, cât și drepturile fundamentale ale cetățenilor.

Cu alte cuvinte, cadrul european completează dreptul internațional clasic, introducând reguli concrete pentru protecția infrastructurilor critice și informațiilor clasificate. Totodată, normele NIS2, Cybersecurity Act și regulamentele privind informațiile clasificate permit standardizare și cooperare transfrontalieră. Pe de altă parte, în timp ce jurisprudența CEDO asigură echilibrul între securitate și libertăți fundamentale, prevenind abuzurile, protecția europeană include măsuri tehnice, legislative și instituționale, adaptate provocărilor spionajului modern, inclusiv cibernetic și satelitar. Prin urmare, se poate afirma că, în ansamblu, UE furnizează un model de securitate juridică integrată, care poate fi aplicat și în situații hibride sau emergente.

Concluzii

Dronelor le revine un rol central în evoluția spionajului militar modern, datorită capacității lor de a colecta rapid informații detaliate, cu risc minim pentru personalul uman. Ele permit supravegherea persistentă a unor zone greu accesibile și oferă date în timp real, esențiale pentru decizii operative.

Totodată, tehnologiile autonome transformă caracterul operațiunilor de intelligence, trecând de la misiuni reactive la unele anticipative. Algoritmii de inteligență artificială pot analiza cantități masive de date, identificând tipare și amenințări care ar scăpa analizei umane.

Așadar, integrarea dronelor cu sisteme AI crește eficiența și precizia spionajului, făcând posibilă selecția automată a țintelor, cartografierea zonelor de interes și identificarea obiectivelor strategice, reducând în același timp intervalul dintre colectarea informației și utilizarea ei.

Autonomia sistemelor ridică însă probleme etice și juridice, în special în ceea ce privește supravegherea populațiilor, protecția vieții private, responsabilitatea în cazul erorilor și riscul escaladării conflictelor prin acțiuni automatizate.

Competiția globală pentru dominația tehnologică face din drone și AI instrumente de putere strategică, statele investind masiv pentru a nu rămâne în urmă. Această cursă crește atât capacitatea de apărare, cât și vulnerabilitățile legate de atacuri cibernetică sau preluare neautorizată a controlului.

În viitor, rolul dronelor și al tehnologiilor autonome va crește exponențial, direcția fiind reprezentată de sisteme complet integrate – supraveghere, analiză, decizie – capabile să acționeze coordonat în teatrele de operații.

În ansamblu, spionajul militar se află într-o transformare profundă: tehnologia reduce riscurile și crește eficiența, dar vine și cu provocări complexe. Succesul strategic va depinde nu doar de adoptarea acestor sisteme, ci și de modul responsabil în care sunt reglementate și utilizate.

References

- Chicago Convention on International Civil Aviation*, ICAO, 1944.
Francis Gary Powers, *Operation Overflight*, Holt, 1970.
ICAO, *Chicago Convention on International Civil Aviation*, 1944.
J.-M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, CUP, 2005.
James Bamford, *The Shadow Factory*, Doubleday, 2008.
Kenneth Werrell, *The Evolution of UAV During the Cold War*, Air University Press, 1996.
Michael Goodman, *The Official History of the Joint Intelligence Committee*, Routledge, 2014.
Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO CCDCOE, 2013.
NATO CCDCOE, *Tallinn Manual 2.0 on Cyber Operations*, 2017.
Nico Schrijver, *Sovereignty over Natural Resources*, Cambridge University Press, 1997.
Peter Bergen, *Drone Wars*, Cambridge University Press, 2021.
Robert F. Futrell, *The United States Air Force in Southeast Asia*, Air Force History, 1981.
Yefim Gordon, *Soviet Strategic Reconnaissance Vehicles*, Midland Publishing, 2003.