I2DS2 Pro Decizii Strategice Inteligente

INTELLIGENCE STRATEGIC

Decembrie 2021

www.i2ds2.org

INTELLIGENCE STRATEGIC

Raport periodic

Decembrie 2021

Cristian EREMIA

- **Retrospectivă**

”Status quo-ul în intelligence-ul militar este inacceptabil în noua eră”.

În ultima perioadă de timp, o tendință certă la care s-au aliniat mai toate serviciile de intelligence (serviciile de informații civile și militare) din statele cu potențial ridicat de finanțare a sectorului de cercetare/dezvoltare în tehnologii avansate a fost aceea de a accelera eforturile de asimilare și implementare în operațiile și activitățile de intelligence a tehnologiilor duale, emergente sau chiar a celor disruptive/perturbatoare (1).

Domeniile care au fost modernizate și perfecționate - în paralel sau rând pe rând, cu tehnologii avansate sau critice de culegere/achiziție, procesare și stocare, respectiv diseminare a informațiilor externe au fost cele din zonele SIGINT, IMINT, GEOINT, MASINT, CYBINT sau DNINT (Cyber sau digital network intelligence), TECHINT, desigur OSINT și nu numai.

O altă caracteristică a dezvoltărilor a fost aceea de a se inova și implementa soluții integrate de intelligence prin utilizarea noilor tehnologii, chiar dacă aceasta presupune adevărate

provocări pentru serviciile de informații și securitate de pretutindeni, inclusiv pentru cele din state cu potențial mare de cercetare/proiectare și experimentare a tehnologiilor avansate din Occident, din Europa de Est sau din alte zone ale lumii.

La nivel doctrinar este acceptată ideea că în războaiele actuale și din viitor (hibride, neregulate, totale sau de nouă generație), transformarea digitală, analiza predictivă, învățarea automată, inteligența artificială, cibernetica și robotica vor modifica fundamental afacerile în informațiile militare și civile – rol de ”game changer”. Contează extrem de mult și viteza de asimilare a acestor tehnologii de către serviciile de informații și celelalte structuri de forță ale statelor.

Referindu-se la activitatea în ansamblu a serviciilor de informații, Generalul american Matthew Glavy (USMC) declara că ”Toate lucrurile pe care am contat în ultimii peste 20 de ani sunt pe cale de a nu mai fi cazul (n.n. - să contăm) în viitor...Status quo-ul în intelligence-ul militar este inacceptabil în noua eră.” Așadar, cuvântul de ordine pentru eforturile viitoare în intelligence–ul atât militar cât și civil, a devenit ”schimbarea”. Iar aceasta trebuie să se producă la timp pentru ca structurile de informații să mențină situația sub control, pentru a dobândi superioritate și a prevala în războaiele declarate sau nevăzute, în fața de amenințărilor tot mai mari și mai sofisticate din partea adversarilor.

Așa cum arată situația din ultimii ani, o caracteristică de bază a serviciilor de informații ruse este creșterea intensității și agresivității acțiunilor de humint strategic (de agentură potrivit terminologiei ruse) pentru a penetra sistemele politice și de securitate ale statelor vecine în primul rând, chiar a structurilor NATO și UE.

A bloca operațiile externe ale serviciilor de informații ale Moscovei este practic primul pas către o descurajare cu succes.

(1) Cele șapte tehnologii cheie emergente și disruptive/perturbatoare pe care NATO le-a identificat drept critice pentru viitor: inteligența artificială (IA), capabilități autonome, prelucrarea big-data, tehnologiile cuantice, biotehnologia, domeniul hipersonic și spațiul cosmic. Rusia este extrem de interesată și acționează pentru implementarea tehnologiilor avansate și emergente disruptive, liderul rus plasând priorități industriei sale de apărare.

- **Serviciile de informații asimilează tehnologii emergente disruptive**

Soluții integrate pe baza Inteligenței Artificiale (AI)

Una dintre tendințele pentru viitor deja abordate de marile puteri tehnologice este aceea de a crea platforme integrate tehnologice avansate pe baza Inteligenței Artificiale (AI), care să integreze și să centralizeze toate datele și informațiile despre forțele potențial inamice într-un singur sistem, ceea ce va permite achiziția, procesarea, analizarea, extragerea și diseminarea datelor și informațiilor necesare pentru operații militare sau de altă natură, desfășurate cu mare viteză. SUA și Israel sunt mai transparente în această direcție.

Platformele de integrare a informațiilor, de procesare și de elaborare a unor predicții pentru suport decizional, cursuri probabile de acțiune, sau elemente de intelligence proactiv sau

acționabil (transferat în acțiuni reale rapide pentru a lansa, de exemplu, o lovitură preventivă, sau pentru a pregăti o contra-acțiune rapidă) vor fi elemente cheie ale dezvoltării unor servicii de informații militare și civile performante.

Sursa: defense.gov

Un exemplu relevant în materie este cel dat de Agenția de Informații pentru Apărare (DIA) a SUA, care finalizează în această perioadă o altă etapă importantă în dezvoltarea sistemului său inovativ de intelligence MARS pentru gestionarea și analiza bazelor masive de date (meta baze de date) colectate de comunitatea de informații, lansând cu succes în acest an al doilea produs/modul al noului sistem de intelligence (informații militare externe) MARS – Machine-assisted Analytic Rapid-repository System.

Acest nou modul a fost denumit ”Order of Battle” și va asigura informații și evaluări de intelligence despre forțele armate străine, asigurând descrierea exactă a ”ierarhiei bazelor militare străine, cu prezentarea locației geografice a unităților militare și descrierea echipamentelor militare din dotarea acestora”. Sistemul MARS va fi un sistem de avangardă pentru comunitatea de intelligence, dezvoltat pe tehnologii de inteligență artificială și învățare automată (artificial intelligence and machine learning), și care se va baza totodată pe tehnologia ”cloud computing” pentru a opera cu meta date și a realiza automat analize extrem de complexe.

Abordările viitoare pentru forțele armate ca un întreg din perspectivă informativă și operațională va presupune integrarea tuturor informațiilor obținute de capabilitățile militare și civile de culegere de informații, de rețele unice, crearea unei mega-baze de date centralizate și a unei (unor) rețele tip internet dedicate pentru punerea acestora la dispoziția unităților combatante din toate categoriile și structurile de forțe ale unui stat. Activarea proceselor digitale ultra-rapide și a unui limbaj comun în spațiul de luptă digital va duce la reducerea timpilor pentru analiză, decizie și acțiune, pentru conștientizarea situației la nivelul comandanților, pentru stabilirea obiectivelor-țintă cu maximă viteză și cât se poate de mare precizie. Prin urmare, ceea ce dura zile întregi în trecutul nu îndepărtat, se va reduce la nivelul orelor sau mai puțin, pentru ca în final să se obțină efecte de surprindere strategică și de multiplicare a forțelor.

Operații de cyberintelligence/cybersurveillance

Confruntările actuale dintre serviciile de informații - inclusiv prin operații de tip război informațional, s-au extins mult dincolo de conflictele de mică sau mai mare intensitate și de cele din teatrele de operații. Adversarii democrațiilor autentice, precum China și Rusia, au căpătat expertiză în utilizarea spațiului cibernetic pentru a dezinforma și influența/manipula populații de pe tot globul asupra afacerilor geopolitice, comerțului, drepturilor omului, climei și multe altele. Cum deja am menționat, se folosesc vitezele net crescute datorate asimilării AI pentru a procesa informațiile necesare unor astfel de operații sofisticate.

Permanent au fost abordate tehnologii care să asigure superioritate și competitivitate în Spațiul Cibernetic, respectiv în operații complexe de CYBINT. Și iată că, la 26 octombrie 2021, oficiali guvernamentali și experți în securitate cibernetică din SUA, respectiv ai Microsoft, au lansat avertizări severe că serviciile de informații ale Rusiei au lansat o nouă și amplă campanie de operații sofisticate de spionaj - cyberintelligence sau cybersurveillance, care vizează să străpungă mii de rețele de computere guvernamentale, corporative sau chiar ale unor think-tank-uri americane de interes. Sunt vizate și alte state țintă din întreaga lume.

Sursa: http://aicd.companydirectors.com.au

Și asta la doar câteva luni după ce președintele Biden a impus sancțiuni corporațiilor tehnologice și financiare din Rusia (este adevărat nu dintre cele mai severe, pentru că se dorea spațiu diplomatic pentru un dialog politic cu Putin) ca răspuns la o serie de operațiuni

rafinate de spionaj desfășurase în întreaga lume la începutul anului. De exemplu, Casa Albă a dat vina atunci pe **Serviciul de Informații Externe al Rusiei (SVR)** pentru așa-numitul ”hacking SolarWinds”, operații extrem de rafinate de a schimba software-ul utilizat de cercuri de afaceri și de cele mai mari corporații ale SUA, oferind rușilor acces larg la 18.000 de clienți. **SVR** - care este etichetat ca ”operator ascuns de intelligence în spațiul cibernetic”, este și de această dată suspectat în primul rând (este de notorietate că implicarea clandestină a SVR a fost identificată în 2016 pe timpul alegerilor prezidențiale din SUA). Din alte surse deschise reiese că și celelalte servicii de informații ale Rusiei au un mare potențial de a executa operații ofensive de informații/război cibernetic și informațional**.**

Ofițeri guvernamentali din SUA au confirmat că unele operații erau extrem de bine acoperite, altele bine legendate care aparent vizau achiziția/cumpărarea de informații salvate în ”cloud”. Aceste operații de cyberintelligence au fost încadrate la categoria formelor de spionaj reciproc ale principalelor puteri, de regulă în opoziție una cu cealaltă. Acest lucru nu înseamnă că statele mai mici nu sunt expuse la astfel de operații.

Gradul ridicat de pericol al operațiilor de CYBINT menționate se datorează pe ansamblu, faptului că statele/entitățile țintă au dificultăți serioase în a stabili cu exactitate:

- **Identitatea certă a agresorului** (excepție fac cazurile în care agresorul nu folosește tehnologii rafinate, sau chiar dorește ca identitatea să fie cunoscută),
- **Gradul în care într-o operație sunt combinate acțiuni la vedere (fie că sunt acestea la limita legii) cu cele acoperite și ilegale**, și de aici și estimarea dificilă a gradului de complexitate a atacurilor, a numărului de atacuri profitabile și țintele finale,
- **Gravitatea penetrărilor și cantitatea informațiilor preluate/furate** (ultimele dăți, Microsoft a insistat parțial nejustificat că ponderea atacurilor profitabile ar fi mică, dar nu a precizat public gravitatea atacurilor/intruziunilor cibernetice, sau detalii privind gradul de compromitere a organizațiilor atacate în peste 20 de mii de atacuri).

Dar nu numai SUA sunt ținte ale spionajului cibernetic al Moscovei. Rusia este responsabilă pentru un operații cibernetice asupra UE și Germaniei, care au vizat mai mulți „membri ai parlamentelor, oficiali guvernamentali etc. din UE prin accesarea sistemelor informatice și conturi personale și furtul de informații”. Serviciul de informații al Germaniei a avertizat în iulie 2021 că au avut loc „atacuri intense” din partea grupului legendare din februarie, suspectând că s-ar putea pregăti pentru operațiuni de „hac and leal” în care informațiile sunt furate pentru a fi utilizate ulterior, inclusiv prin publicare.

Polonia a atribuit în iunie 2021, o serie de operații cibernetice serviciilor secrete rusești, care au atacat peste 100 de conturi de e-mail și rețele sociale ale unora dintre cei mai importanți oficiali ai guvernului polonez, din diferite partide politice. Întreaga campanie ar fi vizat peste 4350 de conturi ale diferitelor persoane publice sau simpli cetățeni polonezi, în care au fost extrase/modificate e-mailuri și documente. **Oficialii polonezi au declarat că obiectivul operațiilor a fost acela de ”a lovi societatea poloneză și a destabiliza (non- țara)”. Mai concret, operațiile au fost atribuite unui UNC1151 rusesc - conectat unei campanii legendare, concepute special pentru a destabiliza politic Europa Centrală.**

Și nu numai SVR este vizat și acuzat. În iulie 2021, agențiile SUA NSA, FBI și CISA au lansat o evaluare de securitate cibernetică prin care arătau că, cel puțin de la jumătatea anului 2019 și până în 2021, serviciul militar de informații al Rusiei, GRU (alias APT28 sau Fanny Baer) **a desfășurat operații "atacuri cibernetice în forță și pe scară largă", anonimizate, încercări de penetrare informativă a sute de ținte guvernamentale și din sectorul privat din SUA și întreaga lume.** Aceste capacități de forță permit rușilor să acceseze informații cel puțin confidențiale, sau să obțină acreditări de conturi care pot fi folosite în multe scopuri, cum ar fi obținerea accesului persistent, escaladarea privilegiilor și depășirea barierelor de protecție pentru diferite baze de date.

Concluzii ale experților americani arată că, în pofida faptului că serviciile ruse de informații sunt lipsite de avantajele tehnologiilor avansate emergente ale americanilor și aliaților lor occidentali, aceste servicii ruse s-au dovedit a fi din cele mai pricepute și eficace – și potențial cele mai periculoase prin amenințările generate în spațiul cibernetic: operațiile cibernetice rusești sunt o amenințare reală și actuală.

Concluziile mai arată că SVR nu încetinește ritmul operațiilor (dincolo de faptul că mereu "Spionii sunt gata să spioneze"), iar subminarea și intruziunile rețelelor occidentale continuă să se producă cu ritmul accelerat al unei curse a înarmărilor. Ultima tendință a fost observată inclusiv pe durata pandemiei Covid19, când serviciile de informații ruse au căutat informații secrete despre tehnologiile de fabricare a vaccinului. A mai rezultat că rușii caută de fapt tactici de "penetrare și acces sistemic la conturi sau baze cu informații".

De subliniat faptul că mai multe agenții de informații occidentale consideră că astfel se operații de CYBINT au devenit *"spionaj de rutină".* Aceste agenții acreditează din ce în ce mai vocal ideea că "marea vină" pentru neasigurarea unei securități adecvate la acțiunile Rusiei (și nu numai) aparține de fapt unor corporații occidentale ca Microsoft și furnizorii comparabili ai companiilor de cloud - deci din sectorul privat, care poartă de fapt responsabilitatea pentru că nu au implementat practici simple de securitate cibernetică pentru a încuia "ușile lor digitale".

Mai mult, un oficial înalt al Administrației americane susține că cele mai recente operații ruse sunt "operațiuni nesofisticate, uzuale, care ar fi putut fi prevenite dacă furnizorii de servicii cloud ar fi implementat bune-practici de bază de securitate cibernetică". Structurile guvernamentale au făcut eforturi pentru a plasa informații confidențiale suplimentare în "cloud", deoarece ar fi mult mai simplu să fie astfel păstrate informațiile (Amazon conduce

contractul de cloud al CIA; pe timpul administrației Trump, Microsoft a deținut contractul enorm de cloud al Pentagonului, deși acest contract a fost abandonat recent de administrația Biden pentru o procedură controversată de atribuire).

Totuși, cele mai recente operații ale serviciilor ruse de informații au generat o reevaluare a trecerii la cloud ca și soluție tehnologică. Mai ales datorită inexistenței unor soluții integrate de securitate care să anihileze strategiile Rusiei – și mai nou și pe cele ale Chinei, de a obține acces la nivel înalt la informațiile de care aveau nevoie, indiferent dacă este vorba de e-mailuri ale autorităților, de rezultate ale științelor aplicate sau la informații ale structurilor de forță.

- **Operații clasice de HUMINT strategic / spionaj cu agenturi**

Operații de spionaj ale serviciilor ruse

În ultima perioadă de timp au fost remarcate unele tendințe în operațiile clasice de intelligence cu HUMINT strategic sau spionajul cu agenturi ale Rusiei. UE și NATO acuză în ultima perioadă de timp spionajul rus pentru agresivitate crescândă. Guvernele europene acuză în mod public agenții ruși că au comis tentative de asasinat, de sabotaj, subversiune, diversiune sau de penetrare a instituțiilor politice, organizațiilor militare sau civile. Se poate face o legătură cu faptul că și diplomația rusă a devenit mult mai agresivă.

Există evaluări nuanțate, dar a devenit mai clar că serviciilor de informații (SI) ale Rusiei au devenit mult mai ostentative, suspectându-se că probabil ar avea mână liberă de a simula anumite neglijențe și a-și expune acțiunile în unele cazuri. Alte evaluări arată că agenții ruși au fost întotdeauna foarte activi, acum fiind mai "reperabili", parțial datorită "urmelor digitale" pe care le lasă, respectiv faptului că și cele mai bine organizate operații HUMINT sunt expuse la a fi detectabile și compromise cu tehnologii moderne.

După turbulenții ani 90, cele trei agenții ruse SVR, GRU și FSB (Serviciul Federal de Securitate) au acționat relativ "liber" în Europa, construind în timp **agenturi și hub-uri cu activități de intelligence intense în Viena, Budapesta și Praga.** State membre ale UE și NATO au avut în acest an adevărate conflicte diplomatice ca urmare a agresivității serviciilor de informații ruse:

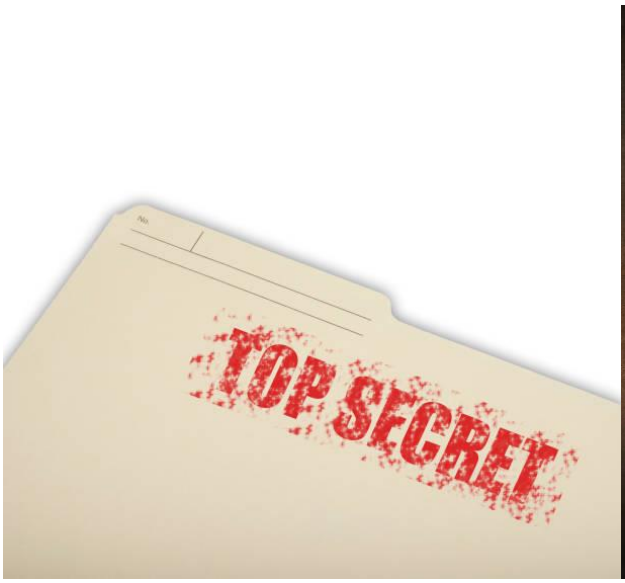
Finlanda constată că activitățile SI ruse sunt practic tot timpul la nivel ridicat,

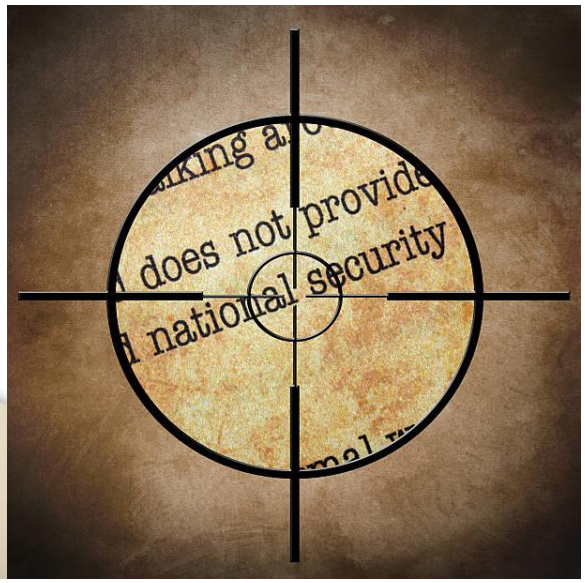
Cehia acțiunile ostile ruse din 2014 au declanșat în acest an o furtună politico-diplomatică între Praga și Moscova, soldată cu expulzări reciproce masive de diplomați, aproape cu închiderea ambasadei cehe, Cehia fiind desemnată "stat neprietenos" (ca și SUA) de către Rusia,

Bulgaria acuză Moscova pe spețe conexe cu cele din Cehia și suplimentare în perioada 2011-2021, dar cu o atitudine politică public mai blândă față de spionajul Rusiei,

Finlanda susține că agenturile moderne ruse au două sarcini, culegerea de informații clasificate și influențarea națiunilor europene,

Germania acuză activități ale SI ruse la nivelul Războiului Rece, semnalând tendința că cei mai mulți agenți ruși încearcă să contacteze/racoleze factori de decizie.





Numai în prima parte a acestui an, țările baltice, **Germania, Italia, Polonia și Bulgaria** au pus sub acuzare persoane documentate că au transmis informații clasificate/secrete Moscovei. Evident, **de notat expulzările diplomaților ruși de la Cartierul general NATO, care au provocat o reacție abruptă fără nicio reticență politică a Moscovei, care a rupt practic relațiile diplomatice cu NATO și activitățile Biroului Alianței de la Moscova.**

Schimbările și tendințele de creștere a agresivității operațiilor serviciilor ruse (care practică spionaj total) sunt în cea mai mare parte datorate faptului că Moscova a decis, în esență, să poarte un nou tip de război cu Occidentul, un război nedeclarat de natură hibridă, care se manifestă vizibil într-o primă fază în plan politic și economic.

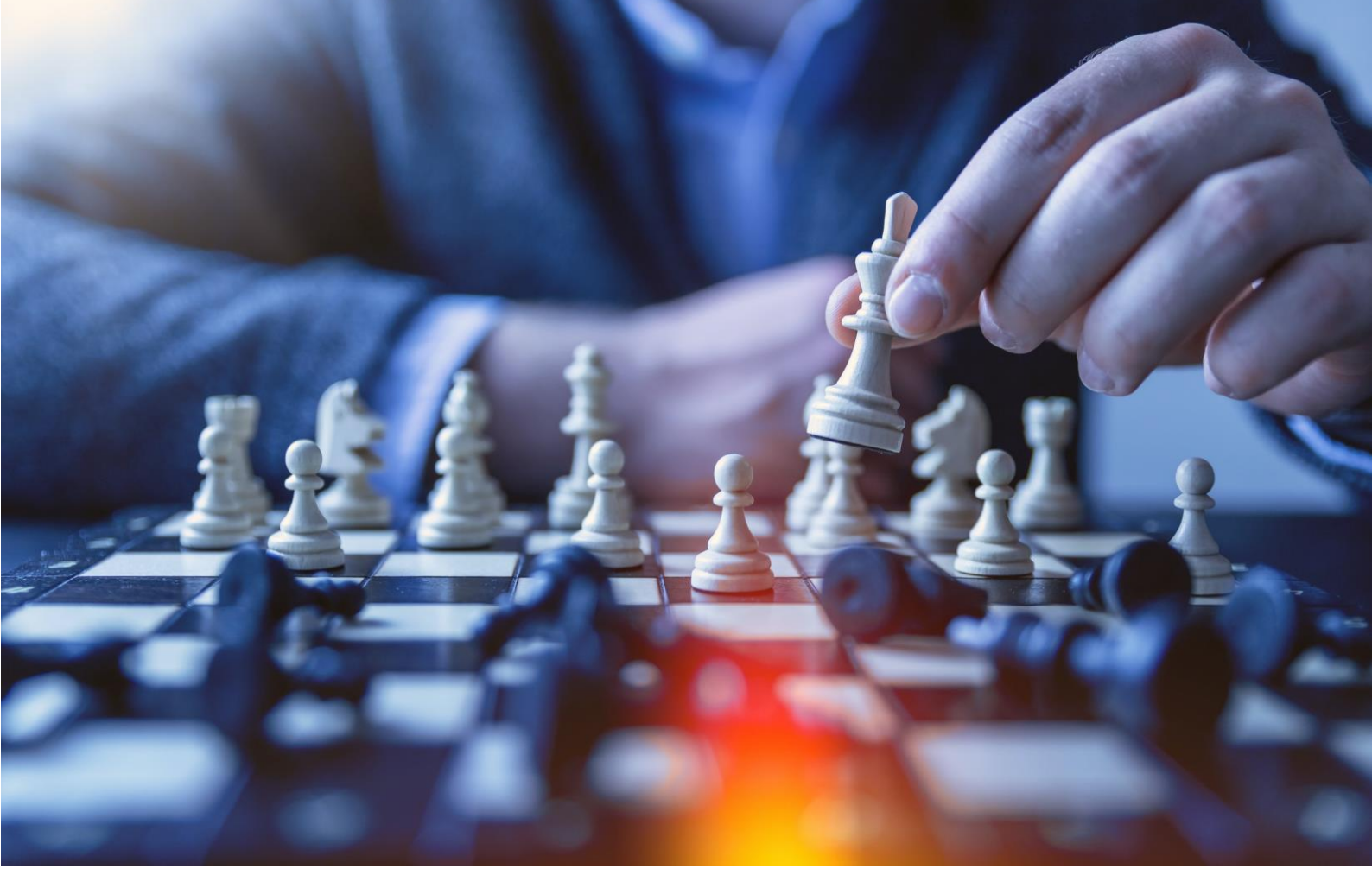
Cu sau fără Doctrina Primakov sau Gherasimov, s-a clarificat faptul că Kremlinul a decis (se poate constata și pe site-ul ministerului apărării al Rusiei) tipologia viitorului **"Război rus de Nouă Generație**" (RNG), care integrează coordonat la nivel central forțele armate cu toate celelalte instrumente și structuri de forță ale puterii naționale, folosind atât forțe convenționale, cât și forțe neconvenționale, toate dotate cu tehnologii de vârf, operând simetric sau asimetric, conform unor planuri operative dedicate pentru fiecare tip de operație/confruntare angajată. **Ipoteza strategică de bază rusă este aceea că, în secolul XXI, la nivel mondial, există o stare permanentă de conflict, cu estomparea demarcațiilor clare dintre stările de război și pace, războaiele moderne nu sunt declarate și nu se termină niciodată, iar după declanșare, evoluțiile devin impredictibile.**

În aceste circumstanțe, noua gândire strategică rusă pune accent pe identificarea și stabilirea manierei de exploatare a vulnerabilitățile adversarilor, pe operațiile asimetrice - inclusiv clandestine sau acoperite pentru a fi eliminate avantaje esențiale de superioritate militară ale adversarului. Se mai pune accent pe folosirea unor capabilități specifice - serviciile de informații împreună cu forțe pentru operații speciale, ale căror acțiuni integrate și coordonate trebuie să fie combinate cu cele de război informațional, război cibernetic, război economic,

cu presiuni politice, diplomatice și cu orice alte instrumente care au impact asupra atingerii obiectivului strategic rusesc.

În această logică, rușii fac apel la tradițiile lor de ducere a unui **război total, conceptualizând RNG prin actualizarea, dezvoltarea, rafinarea și modernizarea cu tehnologii de vârf a unor concepte mai vechi, de sorginte sovietică**. Gândirea strategică rusă consideră că pentru câștigarea unui conflict inter-statal contemporan, este esențială **cooperarea integrată a cel puțin patru categorii de instrumente ale puterii naționale - cele militare, diplomatice, de intelligence (informații) și economice.**

Totodată, se consideră că tehnologiile avansate emergente și disruptive permit modernizări profunde, spațiul informațional deschizând posibilități de utilizare pe scară largă a instrumentelor asimetrice pentru reducerea potențialului de luptă al inamicului, în special prin utilizarea operațiilor de influență la nivel strategic.



Asociația „Soluții Integrate de Securitate, Apărare și Intelligence – I2DS2" este un *think tank* românesc a cărui principală misiune este promovarea, susținerea, dezvoltarea și diseminarea de orientări, analize, politici și strategii în domeniile securitate, apărare și intelligence.

În îndeplinirea misiunii sale, I2DS2 elaborează studii și analize, formulează recomandări de politică publică, organizează programe de instruire, mese rotunde, seminarii și conferințe, participă în diverse formate de parteneriate naționale și internaționale cu entități publice și private, elaborează și implementează proiecte cu obiective specifice domeniilor securitate, apărare și intelligence.

I2DS2 este „o comunitate deschisă pentru securitatea națională" și se raportează la deviza „împreună pentru o lume mai sigură".

Fotografia de pe coperta 4 este preluată de pe site-ul www. unsplash.com,

Asociația „Servicii Integrate de Securitate, Apărare și Intelligence"
București, Bd. CAROL I nr. 54, et.2, ap. 2, cam. 4, Sector 2
Nr. Reg. Special **48/21.05.2019**, CIF: **41374789**
www.i2ds2.org, office@i2ds2.org