**Test Nr.4**

**Subiectul nr.1. Acțiunile informative ale serviciilor de informații privind domeniile politice și strategice, potențialul militar şi economic, resursele umane și tehnologice cu relevanță strategică;**

Lumea are nevoie de o Europă capabilă să desfășoare misiuni militare pentru a contribui la stabilizarea situației în zonele de criză astfel trebuie să ne consolidăm politica externă și de securitate comună și avem nevoie de o abordare comună în chestiunile de apărare, deoarece impreună avem puterea și capacitatea de a transforma lumea intr-un loc mai echitabil, care este fondat pe reguli. Consiliul îşi reiterează apelul pentru menținerea și dezvoltarea în continuare a capacităților militare pentru susținerea și consolidarea PSAC. Acestea stau la baza capacității UE de a acționa ca garant al securității, în contextul unei abordări cuprinzătoare mai largi având în vedere necesitatea unei industrii europene a apărării puternice și mai puțin fragmentate pentru a susține și a consolida capacitățile militare ale Europei și capacitatea UE de a acționa autonom.Mediul strategic și geopolitic se află într-o evoluție rapidă și permanentă. Echilibrul mondial al puterilor se modifică odată cu emergența unor noi centre de gravitație și cu reorientarea interesului strategic al SUA către Asia. În această situație, Europa trebuie să își asume responsabilități mai mari pentru a-și asigura securitatea atât pe teritoriul european, cât și în străinătate. Pentru a putea acționa la întregul său potențial, UE trebuie să dezvolte o politică de securitate și apărare comună (PSAC) credibilă. Această evoluție trebuie să fie pe deplin compatibilă cu NATO și cu principiile sale. Provocările în materie de securitate cu care ne confruntăm astăzi sunt numeroase, complexe, interconectate și dificil de anticipat: este posibil să survină crize regionale care pot deveni violente, pot să apară noi tehnologii care implică noi vulnerabilități și amenințări, iar schimbările de mediu și penuria de resurse naturale pot provoca conflicte politice și militare. În același timp, multe amenințări și riscuri se propagă cu uşurință dincolo de frontierele naționale, estompând linia de demarcație tradițională dintre securitatea internă și cea externă. Provocărilor în materie de securitate menționate nu li se poate face față decât printr-o abordare cuprinzătoare care să combine diferite politici și instrumente, precum și măsuri pe termen scurt și pe termen lung. Această abordare trebuie să se bazeze pe o gamă largă de capabilități civile și militare. Este din ce în ce mai puțin probabil ca statele membre să poată suporta această sarcină pe cont propriu. Acest lucru este valabil în special pentru domeniul apărării, în care noile echipamente sunt adesea complexe din punct de vedere tehnologic și costisitoare. În prezent, statele membre întâmpină dificultăți în a-și echipa forțele armate în mod adecvat. Operațiunile recente din Libia au evidențiat faptul că Europa înregistrează deficiențe importante la nivelul capabilităților militare esențiale. Criza cheltuielilor publice conduce la reduceri în bugetele pentru apărare, fapt ce exacerbează problema, mai ales întrucât acestea nu sunt nici coordonate, nici puse în aplicare ținând cont de obiective strategice comune. Din 2001 până în 2010, cheltuielile UE din sectorul apărării au scăzut de la 251 de miliarde EUR la 194 de miliarde EUR. Aceste reduceri bugetare au, de asemenea, un impact considerabil asupra industriilor care dezvoltă echipamente pentru forțele noastre armate, antrenând reduceri ale programelor existente și planificate. Ele afectează în special investițiile în cercetarea și dezvoltarea din domeniul apărării, care sunt cruciale pentru dezvoltarea capabilităților viitoare. Între 2005 și 2010, bugetele europene pentru cercetare și dezvoltare (C&D) au cunoscut o scădere de 14 %, până la 9 miliarde EUR; numai SUA cheltuiește în prezent de şapte ori mai mult pentru cercetarea și dezvoltarea în domeniul apărării decât toate cele 27 de state membre ale UE .Acestea ar putea lua forma unei acțiuni pregătitoare cu privire la capabilitățile de apărare care sunt esențiale pentru operațiunile PSAC, vizând realizarea de sinergii cu programele de cercetare naționale. Comisia va defini conținutul și modalitățile, împreună cu statele membre, SEAE și AEA. În paralel, statele membre ar trebui să mențină un nivel adecvat de finanțare pentru cercetarea în domeniul apărării și să desfășoare o pondere mai mare a acestei cercetări într-un mod cooperativ.

Acțiuni: Comisia intenționează să sprijine un sistem de achiziții publice înainte de comercializare pentru achiziționarea de prototipuri. Primele domenii care ar putea beneficia de acest lucru ar fi următoarele: detectarea CBRNE, RPAS și echipamentele de comunicare bazate pe tehnologii de tip radio definit prin software. Comisia va lua în considerare posibilitatea de a sprijini cercetarea referitoare la PSAC, spre exemplu prin intermediul unei acțiuni pregătitoare. S-ar pune accentul pe acele domenii în care ar exista cea mai mare nevoie de capabilități de apărare ale UE, vizând, în măsura posibilului, realizarea de sinergii cu programele de cercetare naționale. 5. Dezvoltarea capabilităților Comisia lucrează deja la modalitățile de a răspunde nevoilor în materie de capabilități nemilitare care servesc sprijinirii politicilor de securitate deopotrivă internă și externă, cum ar fi protecția civilă,gestionarea crizelor, securitatea cibernetică, protecția frontierelor externe și supravegherea maritimă. Până în prezent, aceste activități au fost limitate la cofinanțarea și coordonarea capabilităților statelor membre. Comisia intenționează să facă încă un pas înainte pentru a se asigura că Europa dispune de întreaga gamă de capabilități de securitate de care are nevoie, că acestea sunt exploatate în modul cel mai eficient din punct nemilitare și cele militare este garantată în domeniile relevante. vedere al costurilor și că interoperabilitatea dintre capabilitățile Acțiuni: Comisia va continua să sporească interoperabilitatea partajării de servicii de informare dintre utilizatorii civili și cei din domeniul apărării, precum în inițiativa pilot „Mediul comun în vederea schimbului de informații pentru supravegherea maritimă"; Pe baza rețelelor existente ale UE, Comisia va explora, impreună cu statele membre, posibilitățile de creare a unui grup de cooperare civilo-militar în domeniile următoare: a) tehnologiile de detectare și b) metodele de protecție împotriva dispozitivelor explozive improvizate, a sistemelor portabile de apărare antiaeriană (MANPAD) și a altor amenințări pertinente, cum ar fi amenințările CBRNE; · Comisia va colabora cu SEAE în ceea ce privește o evaluare comună a nevoilor în materie de capabilități cu dublă utilizare care sunt necesare pentru politicile de securitate și apărare ale UE. Pe baza acestei evaluări, Comisia va prezenta o propunere identificând nevoile în materie de capabilități care, după caz, ar putea fi cel mai bine acoperite prin resurse achiziționate, deținute și exploatate în mod direct de către Uniune.

Spațiul și Apărarea Majoritatea tehnologiilor, infrastructurilor și serviciilor spațiale pot servi atât obiectivelor civile, cât și celor de apărare. Cu toate acestea, spre deosebire de situația din toate statele deținătoare de tehnologii spațiale, în UE nu există nicio legătură structurală între activitățile spațiale civile și cele militare. Această separare are un cost economic și politic pe care Europa nu și-l mai poate permite. Acest cost este exacerbat de dependența Europei de furnizori din țări terțe ai anumitor tehnologii critice, care fac adesea obiectul unor restricții la export. Deși unele capabilități spațiale trebuie să rămână sub un control național și/sau militar exclusiv, există mai multe domenii în care realizarea unor sinergii sporite între activitățile civile și cele de apărare va reduce costurile.Aceste infrastructuri sunt critice, intrucât formează baza pentru aplicații și servicii care sunt esențiale pentru economia noastră, precum și pentru bunăstarea și securitatea cetățenilor noștri. Aceste infrastructuri trebuie să fie protejate. Deşeurile spațiale au devenit cea mai gravă amenințare pentru sustenabilitatea activităților noastre spațiale. Pentru a reduce riscul de coliziune este necesar să se identifice și să se monitorizeze sateliții și deșeurile spațiale.

**Subiectul nr. 2. Securitatea informațională ca factor de organizare a societății contemporane.**

În ziua de azi este evident că sfera informațională, ca factor de organizare a societății contemporane, are o influență activă în situația politică, economică, de apărare și alte componente ale securității statului. În mare parte, integritatea lumii contemporane, ca societate globală, este asigurată de schimbul informațional. Globalizarea, este un fenomen amplu dezbătut, nu putea să nu influențeze aspectele legate de securitatea națională, de amenințările privind siguranța oamenilor și informațiilor, a instituțiilor naționale și internaționale. Extinderea la scară globală a utilizării diferitelor mecanisme de prelucrare și comunicare a informațiilor, de control al activităților a condus și la apariția nevoii de a lua în considerare noile aspecte ce influențează securitatea spațiului cibernetic global. Implementarea activă și multilaterală a tehnologiilor informaționale a determinat transformarea structurii societății mondiale, conducind treptat spre dispariția frontierelor naționale. In toate domeniile de activitate au apărut noi structuri funcționale, la baza cărora se află Rețeaua. Acestea sint și corporațiile transnaționale, și economia electronică , și asocierea colectivelor ştiințifice, care lucrează asupra unor probleme comune, dar se află în diferite regiuni ale planetei. Dar aceste schimbări au atins și partea negativă a vieții umane. Structurile de rețea au devenit baza criminalității mondiale. Rețelele de calculatoare sunt structuri deschise, la care se pot conecta mare și uneori necontrolat de calculatoare. Complexitatea arhitecturală și distribuția topologică a rețelelor conduc la o mărire necontrolată a mulțimii utilizatorilor cu acces numar nemijlocit la resursele rețelei- fișiere, baze de date, rutere etc. de aceea putem vorbi de o vulnerabilitate a rețelelor ce se manifestă în diferite moduri. Din această cauză un aspect crucial al rețelelor de calculatoare, în mod special al comunicaților pe Internet, il constituie securitatea informațiilor. Utilizatorii situați la mari distanțe trebuiesc bine identificați-in mod tipic prin parole. Cu părere de rău și sistemele de parole au devenit vulnerabile, atåt datorită hacker-ilor care și-au perfecționat metodele cât și datorită alegerii incorecte a parolelor de către utilizatori. Necesitatea de securitate și de autenticitate, apare la toate nivelele arhitecturale ale rețelelor. În lume s-a creat spațiul informațional global unic, in care s-a manifestat o confruntare geostrategică informațională între marile puteri, pentru atingerea superiorității in spațiul informațional mondial, în special in megapolisuri, centre-cheie ale societății informaționale globale. Aceasta însă provoacă frecvent situații critice, deoarece omul de astăzi este practic permanent supus stresului. În condițiile intersectării cu noile provocări și amenințări ale naturii, la care omul încă nu a reușit să se adapteze și să elaboreze contramăsuri, o actualitate deosebită capătă activitatea de asigurare a securității activității sale vitale securitatea în sensul larg cuprinzind toate domeniile activităților umane. Securitatea națională și economia sint total dependente de tehnologiile informaționale și de infrastructura informațională. Nucleul infrastructurii informaționale, de care depinde omenirea, se află Internetul. Utilizarea de către infractori a tehnologiilor informaționale și telecomunicaționale, în primul rind a rețelei Internet, prezintă un pericol serios în procesul de securității societăți la nivel global. Cea mai importantă problemă de care sunt promovare preocupați utilizatorii Internetului este problema securității informationale. Utilizării tehnicii de calcul în majoritatea domeniilor vieții, precum și conectarea calculatoarelor în rețele internaționale a dus la faptul că infracțiunea comisă cu ajutorul sau prin intermediul calculatorului să fie mai diversă, mai periculoasă și mai prezentă la nivel internațional. La studierea factorilor generatori de acțiuni criminale s-a demonstrat că rețelele de comunicare și calculatorul modern prezintă caracteristici specifice care sint de mare utilitate pentru criminali și implică serioase dificultăți pentru potențialele victime pentru aplicarea legii (probleme complexe de securizare a sistemelor, diversitatea sistemelor hard și soft, lipsa de experiență a multor utilizatori, anonimatul comunicării, criptarea și mobilitatea internațională). Grupurile care activează în domeniul crimei organizate, profesioniști în spionajul economic și serviciile secrete din intreaga lume exploatează deja aceste noi caracteristici ale acțiunilor criminale cibernetice. Ca rezultat al globalizării factorilor economici, politici și militari, al expansiunii rețelelor și sistemelor informaționale globale, guvernele lumii, organizațiile internaționale sint nevoite să-și concentreze și mai mult eforturile asupra asigurării securității globale, pentru că acum riscurile sint mai mari ca oricind, din cauza efectului de propagare în lanț. Dacă pină la apariția rețelei globale asigurarea securității sistemelor informaționale era o problemă de politică națională, în momentul de față la stabilirea strategiilor și politicilor de securizare a spațiului cibernetic trebuie luate în considerare și aspectele de compatibilizare și standardizare la nivel global. Securitatea informațională este un domeniu mult prea vast și cu prea multe domenii conexe pentru a fi detaliat complet undeva. Lumea este in continuă mișcare, cerințele de securitate și confidențialitate cresc pe zi ce trece, amenințările țin pasul,deaceea accentuez că noile condiții ce implică dezvoltarea societății informaționale pe baza utilizării rețelelor informaționale globale, dezvoltarea schimbului informațional transfrontalier, globalizarea sistemului economiei mondiale și creșterea nivelului informatizări necesită scoaterea în evidență a factorilor care anterior nu reprezentau amenințări considerabile. Acești ori fac ca securitatea intereselor naționale în informație element important al securității naționale a statului.

**Subiectul nr.3. Definirea conflictelor militare interne.**

Noțiunea de conflict armat intern, conformArt.3 comun Convențiilor la de la Geneva, prin excludere de la conflictul armat internațional, drept „.conflict armat neprezentând un caracter internațional și ivit pe teritoriul uneia dintre Înaltele Părți Contractante asimilând acestuia războaiele civile, religioase, de eliberare națională împotriva dominației coloniale, de schimbare a regimurilor politice şi de secesiune. Protocolul adițional II restrânge definiția conflictului armat intern, astfel cum aceasta este stipulată în Art. 3 comun Convențiilor de la Geneva şi stabileşte necesitatea îndeplinirii anumitor condiții speciale care îi determină aplicabilitatea.Astfel, Art. 1 definește conflictele armate interne drept „.toate conflictele care nu cad sub incidența la Protocolului adițional I și care se desfășoară pe inter- teritoriul unei Înalte Părți Contractante, între forțele intr-o sale armate și forțe armate dizidente sau grupuri înarmate organizate care, sub conducerea unui comandament responsabil, exercită un asemenea control asupra unei părți a teritoriului său, încât să le permită să desfășoare operații militare susținute și coordonate și să aplice prezentul Protocol". Alin.(2) al aceluiași articol prevede excepțiile de la calificarea unei situații ca și conflict armat intern, statuând că Protocolul adițional II nu se va aplica situațiilor de tensiune internă și tulburărilor interne cum sunt actele de dezordine publică, actele sporadice și izolate de violență şi alte acte analoge, care nu sunt conflicte armate", considerându-se că acestea exced sferei de aplicare a Dreptului Internațional Umanitar. armat internca fiind de două tipuri, respectiv cel tipic, căruia i se aplică Art. 3 comun Convențiilor de la Geneva" și cel de mare intensitate, căruia i se aplică în totalitate dispozițiile Protocolului adițional II. Deseori, fenomene precum tensiunile și tulburările interne armat intern. Cu toate acestea, din analizarea dispozițiilor conținute de Protocolul adițional II, nu pot fi identificate criterii exacte pentru delimitarea fenomenelor de tensiuni și pot fi confundate cu un conflict hemterna tulburări interne de conflictele armate interne. Astfel de criterii sunt stabilite, însă, pe cale jurisprudențială, Tribunalul Penal Internațional pentru Fosta Iugoslavie instituind două criterii de delimitare a situațiilor, respectiv intensitatea conflictului materializată prin .seriozitatea atacurilor, dacă a fost o creștere a confruntărilor armate, o răspândire a violenței asupra teritoriului pentru o perioadă de timp, o creștere a numărului de forțe guvernamentale și mobilizarea ca și distribuția de arme între ambele părți la conflict, precum și dacă a atras atenția Consiliului de Securitate și dacă au fost adoptate rezoluții cu privire la acest conflict" și organizarea părților prin luarea în considerare a anumitor factori arme precum existența sediilor, zone desemnate de violență și abilitatea de a procura, transporta și distribui arme". Conflictele armate interne de mare intensitate și fiind caracterizate prin opoziția autorităților statale și a comandamentelor militare centrale, exprimată față de forțele insurgente organizate, care controlează o porțiune din teritoriu și dispun de armate proprii, conflictele armate destructuratede identitate se manifestă pe fondul disoluției parțiale sau totale a autorității statale, autoritate care nu poate controla propriul teritoriu, nu poate combate violările legilor sale și a celor internaționale și nici nu poate identifica sau trage la răspundere autorii acestor violări. prin comiterea de acte contrare ordinii de drept, îndeosebi atrocități de o gravitate inimaginabilă, precum crimele de genocid, epurările etnice, Prezentând diferențe clare față de conflictele Acest tip de conflicte armate se caracterizează asasinatele în masă etc., individului aflat pe teritoriul respectivului stat neputându-i-se asigura și garanta respectarea demnității, securitatea, integritatea corporală și chiar viața.