ABC
EDUCAȚIEI DE SECURITATE

UL

AWARENESS

CE ESTE PROGRAMUL DE AWARENESS?

Un **demers oficial al Serviciului Român de Informații** care reflectă preocuparea continuă a instituției **pentru îndeplinirea misiunii de prevenție** în raport cu evoluția societății și cu apariția unor noi provocări în planul securității naționale.

CUI SE ADRESEAZĂ PROGRAMUL DE AWARENESS?

Decidenților și angajaților din cadrul tuturor entităților care pot fi expuse unor amenințări cu impact în securitatea națională:

- **autorități și instituții publice** centrale și locale;
- **companii strategice** cu capital de stat și/sau privat;
- alte **persoane juridice de drept public sau privat**.

CARE SUNT BENEFICIILE PROGRAMULUI DE AWARENESS?

- **conștientizarea riscurilor și vulnerabilităților** la adresa instituțiilor statului și agenților economici, care pot fi exploatate de entități ostile - statale sau nestatale;
- **formarea și consolidarea culturii de securitate** prin dezvoltarea unor mecanisme personale de reacție și apărare în momentul conștientizării factorilor de risc;
- **dobândirea de bune practici** de către angajații beneficiarilor Programului.

CE FACEM ÎN CADRUL PROGRAMULUI DE AWARENESS?

Activitățile de awareness, derulate cu **titlu gratuit**, pot avea **formate variate**:

- conferințe;
- colocvii;
- *workshop*-uri;
- prelegeri;
- *training*-uri

și abordează **tematicile de securitate națională** din domeniile *prevenirea și combaterea terorismului, a extremismului ideologic, a amenințărilor transfrontaliere, cyberintelligence, contraspionaj, protecția informațiilor clasificate, securitate economică.*

Experți ai Serviciului Român de Informații pot susține prezentări interactive, adaptate necesităților și specificului beneficiarilor Programului, în cadrul cărora sunt utilizate materiale audio/video sugestive și se dezbat studii de caz relevante pe teme de securitate națională.

Într-un mediu extrem de dinamic, ne folosim experiența acumulată în domeniile de competență și ne concentrăm eforturile și resursele pentru a identifica, a înțelege și a răspunde adecvat noilor provocări de securitate.

CUM SE ACCESEAZĂ PROGRAMUL DE AWARENESS?

Puteți solicita Serviciului Român de Informații includerea în Programul de Awareness prin e-mail (**program.awareness@sri.ro**) sau în scris (la adresa B-dul Libertății nr. 14, sector 5, București).

În măsura în care aveți întrebări legate de Programul de Awareness, ne puteți contacta la numărul de telefon 0739.861.500.

Dezvoltarea culturii de securitate facilitează crearea unor mecanisme de reacție eficiente care pot anticipa și preveni potențiale situații de risc la adresa securității naționale.

ECHIPA AWARENESS

PREVENIREA ȘI COMBATEREA TERORISMULUI

ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII

SERVICIUL ROMÂN DE INFORMAȚII este autoritatea națională în domeniul prevenirii și combaterii terorismului.

Atacurile teroriste din ultimii ani au evidențiat un mod de operare simplu, nesofisticat, caracterizat de:

- alegerea unor ținte “soft” (civili, zone publice ușor accesibile și aglomerate);
- pregătire minimală a atacatorilor;
- documentare facilă în mediul online cu privire la realizarea unor dispozitive explozibile improvizate;
- mijloace ușor de procurat;
- cheltuieli reduse.

DACĂ OBSERVI:

- interesul nejustificat al unor persoane pentru studierea insistentă a unor locuri aglomerate (gări, stații de metrou, aeroporturi, mari centre comerciale, zone pietonale, obiective turistice, sportive, culturale etc.),

- prezența repetată sau prelungită a unor persoane neautorizate în zona unor obiective care ar putea constitui ținte ale unor atacuri teroriste (misiuni diplomatice străine, obiective militare NATO aflate pe teritoriul României, sedii ale unor instituții internaționale),

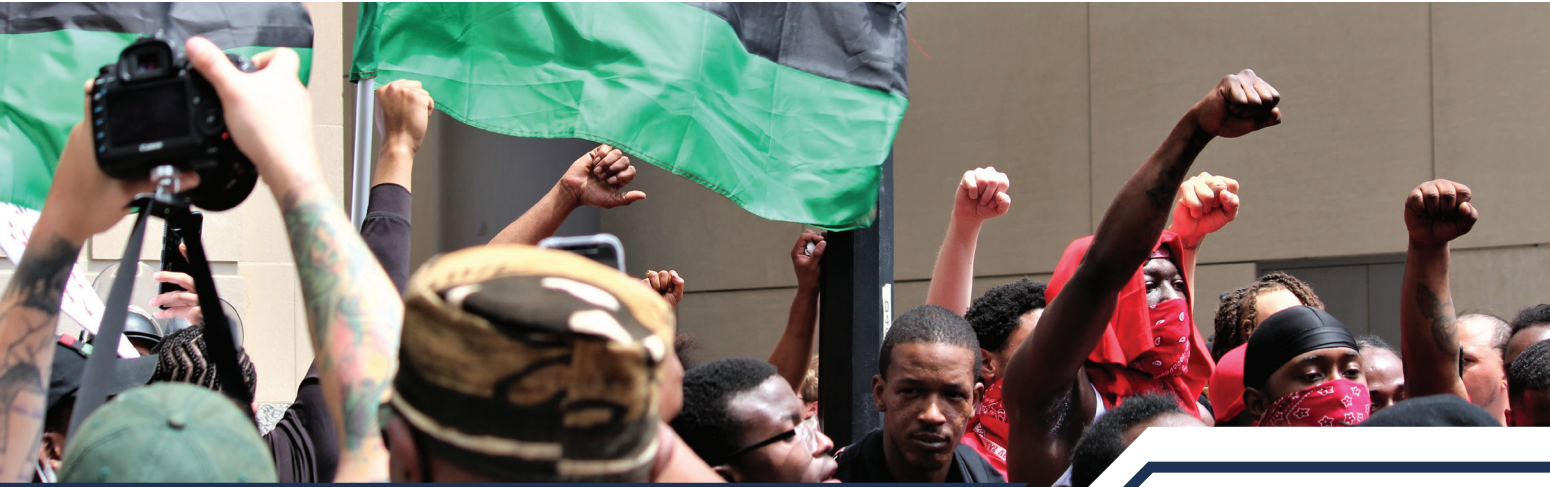
- tendința unor persoane de a fotografia/filma obiective care sunt supuse unor restricții în acest sens,

- interesul nejustificat al unor persoane pentru studierea insistentă a diferitelor căi de acces (feroviar, rutier, subteran, aerian),

- alte aspecte care ridică suspiciuni cu privire la manifestarea unui posibil risc terorist,

ai la dispoziție **linia permanentă și gratuită TEL VERDE 0800 800 100**.

APELUL TĂU AR PUTEA SALVA VIEȚI!



EXTREMISM

INDICATORI POSIBILI AI EXTREMISMULUI:

- persoanele care instigă la ură/violență față de minorități (pe criterii religioase, etnice, rasiale, sexuale) sau care promovează concepte neonaziste, neolegionare, fasciste, xenofobe, rasiste sau anarhiste pot fi identificate ca exponenți ai fenomenului extremist;

- promovarea cultului unor persoane vinovate de săvârșirea unor infracțiuni contra păcii și omenirii.

Aspectele menționate, corelate cu schimbările de comportament (dificultăți de adaptare socială, crize identitare), apariția unor indicatori ai procesului de (auto) radicalizare și/sau fascinația față de arme pot indica un comportament extremist.

Nu ignora persoanele care generează, incită, mențin sau dezvoltă, în mod repetat, stări conflictuale ce pot pune în pericol sub orice formă unitatea și integritatea teritorială a României și pot periclita ordinea statului de drept.

Pentru menținerea unui **climat optim de securitate** este recomandată **sesizarea oricăror acțiuni violente** sau a altor activități care au ca scop schimbarea ordinii constituționale, îngreunarea sau împiedicarea exercitării puterii de stat.

Imaginea instituției în care "extremistul" își desfășoară activitatea **poate fi afectată** de acțiunile acestuia, chiar dacă excedează atribuțiilor profesionale.

SERVICIUL ROMÂN DE INFORMAȚII acționează pentru cunoașterea, prevenirea și contracararea amenințărilor la adresa securității naționale în domeniul extremismului ideologic.

SECURITATE CIBERNETICĂ

Actorii cibernetici exploatează vulnerabilitățile de natură umană, tehnologică și procedurală, generând:

- atacuri cibernetice asupra infrastructurilor critice naționale/europene sau a infrastructurilor IT&C cu valențe critice pentru securitatea națională;
- modificări, ștergeri sau deteriorări neautorizate de date ori restricționări ilegale ale accesului la aceste date;
- acțiuni de spionaj cibernetic;
- prejudicii patrimoniale, acțiuni de hărțuire și șantaj împotriva persoanelor fizice și juridice, de drept public și privat.

CATEGORIILE DE ACTORI CARE GENEREAZĂ AMENINȚĂRI ÎN SPAȚIUL CIBERNETIC SUNT:

- **actori cu motivație strategică** care inițiază sau derulează operațiuni în scopul culegerii de informații din diverse domenii (guvernamental, militar, economic ș.a.);

- **persoane sau grupări de criminalitate cibernetică** ce exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;

- **persoane sau grupări motivate ideologic** (*hacktivism și cyber terorism*) care derulează atacuri cibernetice ce vizează promovarea unor idei și obținerea unui impact mediatic. Astfel de atacuri nu sunt persistente sau disimulate, fiind asumate și expuse mediatic.

CÂTEVA RECOMANDĂRI PENTRU SECURITATEA TA PERSONALĂ ȘI INSTITUȚIONALĂ:

- setează parole de acces complexe, prin alegerea unor combinații de litere (majuscule și minuscule), simboluri și cifre;
- schimbă parolele la intervale regulate de timp;
- protejează-ți datele gestionate prin criptare și back-up periodic;
- evită accesarea link-urilor primite prin intermediul e-mailurilor/rețelelor de socializare;
- utilizează ultima versiune de browser;
- utilizează un program anti-virus cu licență și actualizează-l permanent;
- actualizează aplicațiile și sistemele de operare utilizate;

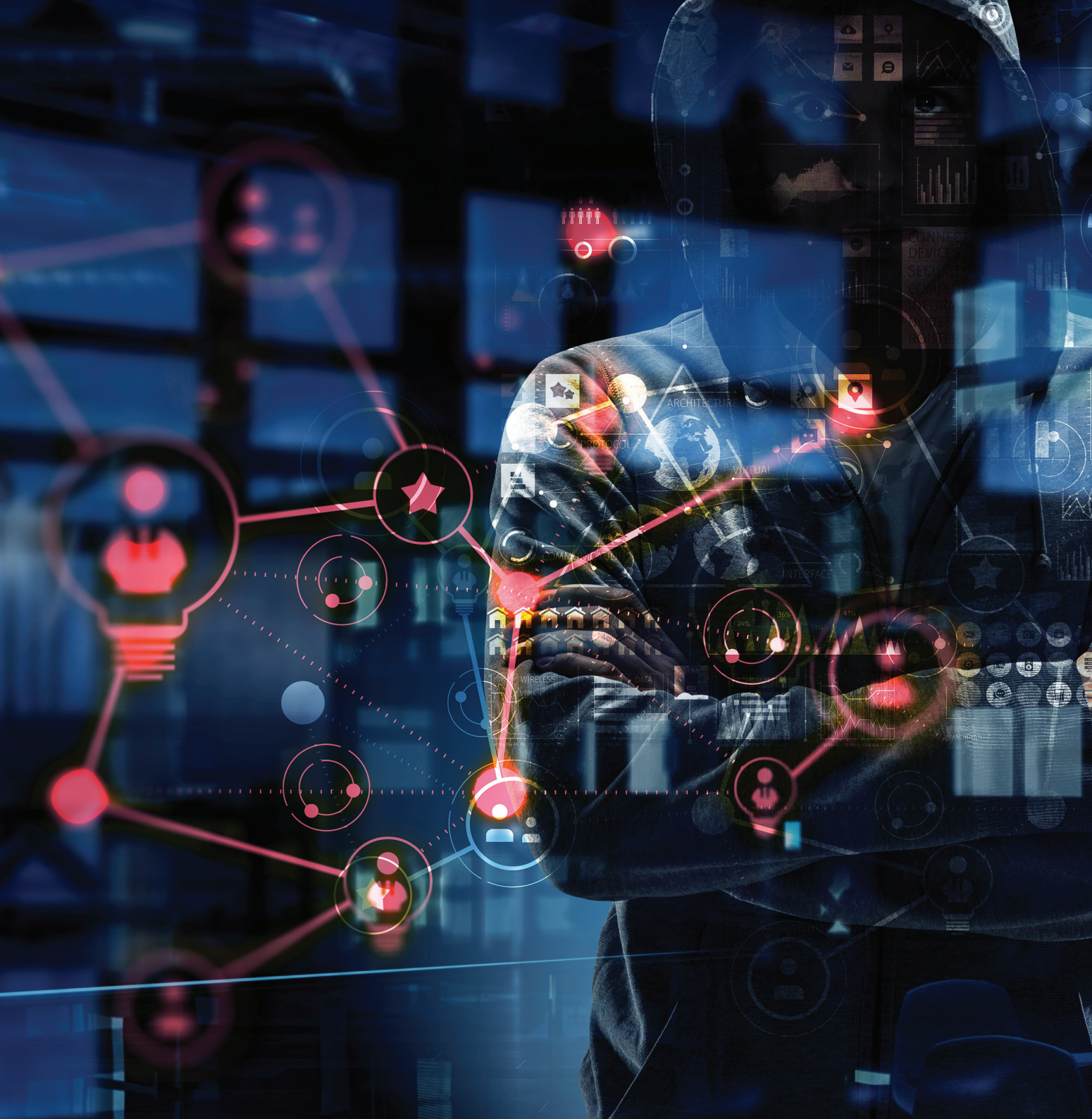
- evită utilizarea rețelelor Wi-Fi nerestricționate;
- evită rularea programelor software a căror origine nu poate fi verificată;
- fii prudent în accesarea documentelor provenite din surse neverificate;
- evită accesarea site-urilor care nu prezintă încredere;
- evită introducerea unor suporți de memorie neverificați în sistemele informatice;
- evită conectarea unor echipamente/accesorii IT&C proprii în cadrul organizației;
- în cazul unei suspiciuni legate de modul de funcționare a sistemului, utilizează funcția de scanare manuală a soluției anti-virus instalate;
- respectă principiile “need to know” și “need to share”;
- fii atent la gestionarea dispozitivelor mobile (telefon/laptop) de serviciu în spații exterioare locului de muncă.

ORICINE POATE FI ȚINTA UNUI ATAC CIBERNETIC

În principal sunt vizate instituții ale statului (ministere, reprezentanțe diplomatice, structuri guvernamentale, servicii militare, servicii de informații), companii naționale sau private de interes strategic, trusturi media etc.

Asigurarea securității cibernetice trebuie să fie o prioritate pentru utilizatori - organizații și indivizi.

SERVICIUL ROMÂN DE INFORMAȚII, prin Centrul Național Cyberint, acționează pentru cunoașterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor la adresa securității cibernetice a României.


ARCHITECTURE
PROTOCOL
VIRTUAL
INTERFACE
WIRELESS
DATA

PROTECȚIA INFORMAȚIILOR CLASIFICATE

De la **transmiterea de secrete de stat unei entități statale/non-statale** la **neglijență în păstrarea acestora**, amenințările la adresa securității naționale îmbracă forme diverse în ceea ce privește informațiile clasificate.

Respectarea legii și **gestionarea informațiilor clasificate** într-un mod conștient și responsabil previne:

- incidentele de securitate;
- accesarea neautorizată de astfel de informații;
- compromiterea, alterarea sau modificarea conținutului acestora;
- prejudiciile la adresa securității naționale sau a intereselor entităților care le gestionează.

Accesul la informații clasificate implică **responsabilitatea** protejării acestora. Prin urmare, apreciem utile următoarele **recomandări**:

- adoptă întotdeauna o atitudine prudentă cu privire la activitatea profesională și informațiile la care ai acces (informațiile le purtăm cu noi oriunde, întotdeauna);
- evită expunerea aspectelor din viața profesională în mediul personal;
- nu lua "notițe" din documente clasificate/sensibile;
- fii conștient de impactul negativ generat de compromiterea informațiilor clasificate pe care le accesezi;
- nu permite accesul persoanelor neautorizate în spații și la documente cu caracter restricționat;
- oferă doar informațiile necesare în cadrul activităților de cooperare/colaborare;
- evită lăsarea nesupravegheată a materialelor sau a documentelor clasificate, sensibile sau de importanță strategică;
- respectă legislația privind protecția informațiilor clasificate.

Nu uita! Gestionarea cu precauție a informațiilor clasificate **contribuie la asigurarea securității naționale!**

SERVICIUL ROMÂN DE INFORMAȚII este autoritate desemnată de securitate în domeniul protecției informațiilor clasificate.

În această calitate, SRI asigură coordonarea generală și controlul măsurilor privitoare la protecția informațiilor secrete de stat și secrete de serviciu la nivelul entităților din sfera sa de responsabilitate.

CONTRASPIONAJ

Spionii vizează **obținerea de date și informații** politico-militare, tehnologice sau economice. Persoanele care desfășoară activități de spionaj tind să-și creeze **conexiuni în mediile de interes**, folosind în acest scop diverse acoperiri - diplomat, om de afaceri, jurnalist, membru al unei organizații neguvernamentale, cercetător, profesor, student, cetățean străin etc.

Țintele activităților de spionaj sunt acele persoane care, prin prisma activității profesionale, au sau pot avea acces la informații de interes (clasificate sau nedestinate publicității) ori pot influența procesele decizionale în defavoarea intereselor naționale.

ADOPTĂ UN **COMPORTAMENT PROACTIV** CARE PRESUPUNE:

- conștientizarea poziției deținute în organizație sau în statul român și, implicit, importanța ta pentru serviciile de informații străine;
- respectarea normelor de conduită și a procedurilor privind protecția datelor sensibile (personale și profesionale);

- semnalarea suspiciunilor către structura de securitate și notificarea aspectelor relevante către instituțiile abilitate pentru a beneficia de sprijin specializat.

FII ATENT LA PERSOANE SAU ORGANIZAȚII CARE:

- se arată interesate, în mod nejustificat, de obținerea unor informații clasificate/sensibile din domeniul tău de activitate;
- manifestă un interes nejustificat față de tine sau activitatea ta profesională, proveniența și cuantumul veniturilor, membrii familiei, prieteni etc..

ÎN CAZUL **DEPLASĂRILOR ÎN STRĂINĂTATE**, ÎN INTERES PROFESIONAL SAU PERSONAL, ESTE RECOMANDAT SĂ:

- te documentezi, din surse oficiale, în legătură cu relațiile bilaterale și starea de securitate din țara de destinație;
- respecți legislația din statul în care călătorești;
- reții datele de contact ale reprezentanței diplomatice a României din țara de destinație;
- eviți oferirea de date personale și din activitatea profesională;
- păstrezi documentele sensibile asupra propriei persoane;
- eviți utilizarea rețelelor de internet din spațiile publice;
- eviți deplasarea în zonele de conflict, participarea la manifestații publice care pot genera pericole la adresa securității personale și angrenarea în discuții pe teme sensibile (religioase, politice, ideologice etc.)
- semnalezi instituțiilor conaționale abilitate orice suspiciune referitoare la derularea asupra ta a unor activități informative.

SERVICIUL ROMÂN DE INFORMAȚII acționează în vederea cunoașterii, prevenirii și contracarării activităților de spionaj care pot fi derulate, pe teritoriul național, împotriva intereselor României și ale aliaților săi.

SECURITATE ECONOMICĂ

Accesul inegal la resurse, piețe și dezvoltare economică, globalizarea și digitalizarea sunt doar câteva dintre elementele care au condus, la nivel mondial, la creșterea competiției pentru accesul la resurse și valorificarea acestora, inclusiv prin utilizarea unor modalități ce excedează cadrului legal.

Evaluări de securitate pe componenta economică relevă acțiuni ale unor actori globali (statali și non-statali), dar și ale unor grupuri de interese care se angajează în noi forme de competiție, dând naștere unor provocări de securitate tot mai complexe pentru interesele strategice ale României.

Există multiple forme de manifestare, de la acțiuni subversive la acțiuni de influență, atât în zona decidenților guvernamentali, cât și în zona reglementărilor de ordin legislativ (legislație primară, secundară și uneori chiar terțiară), în care entitățile ostile încearcă să-și proiecteze propriul interes, în detrimentul statului român.

CONSTATĂM CĂ:

- dispar atât granițele dintre formele de agresiune, cât și cele dintre tipurile de agresori;
- interesele ostile se manifestă fie direct, prin reprezentanți ai cercurilor de putere, fie indirect, prin intermediul unor entități cu spectru larg de activitate;
- marile companii au structuri puternice de intelligence competitiv, ce concurează activitatea serviciilor de informații;
- grupurile de interese ostile pot lua forma unor "asasini economici" bine camuflați și vizează preluarea controlului asupra unor sectoare/resurse critice ale economiei.

CE URMĂRESC AGRESORII:

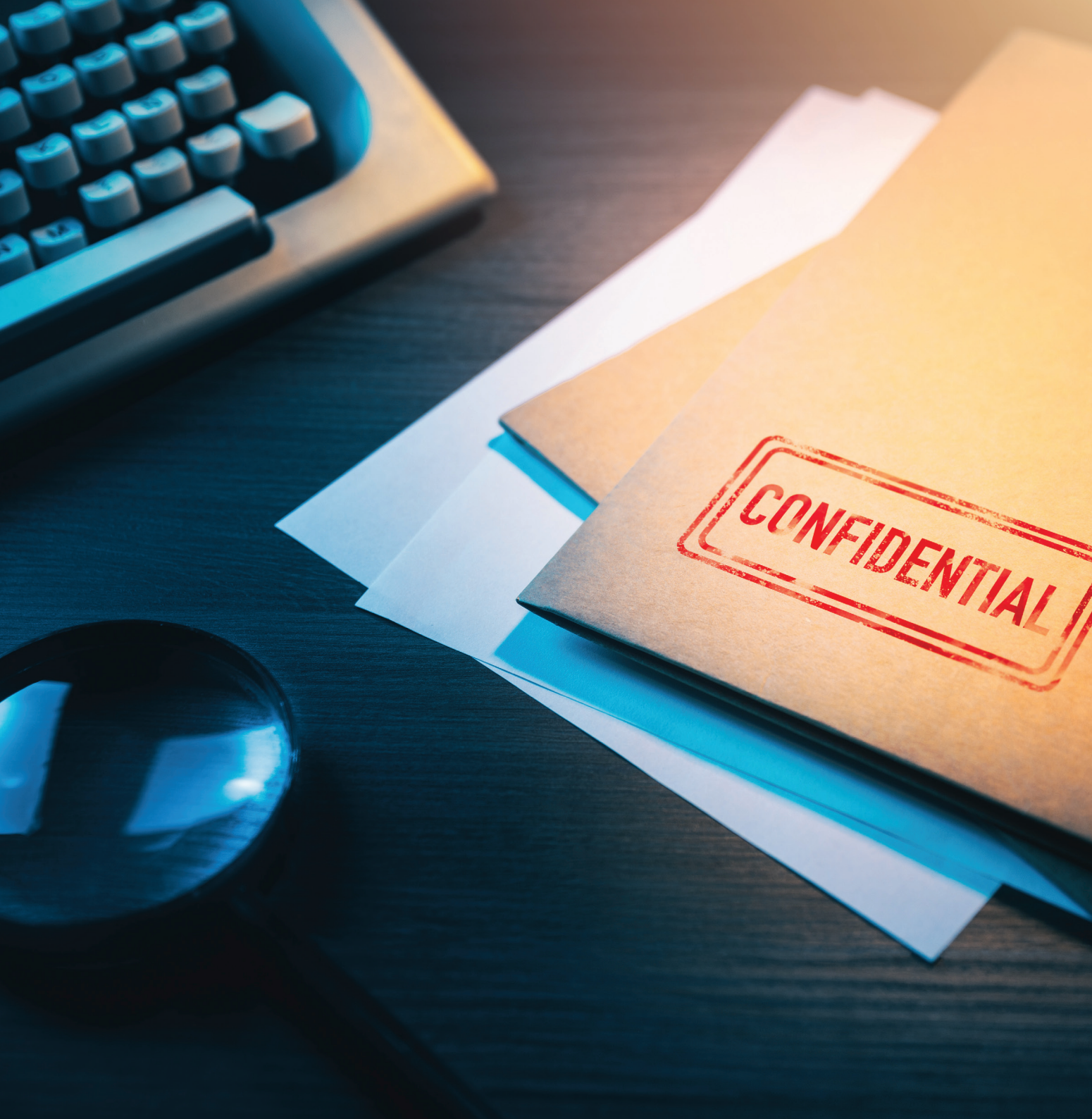
- obținerea de cunoaștere, pârghii și putere de influențare a deciziei strategice;
- obținerea de informații sensibile, confidențiale, care pot oferi avantaj competitiv în negocieri (ex. strategii, evaluări, studii, cercetări, hărți, planuri etc.);
- influențarea proiectelor legislative în domenii esențiale ale economiei;
- acces la diferite baze de date pentru a obține informații despre concurență, resurse importante sau domenii cu valențe strategice;
- derularea de acțiuni care vizează excluderea României din proiecte economice majore;
- penetrarea mediilor instituționale sensibile cu obiectivul de a condiționa deciziile economice ale statului.

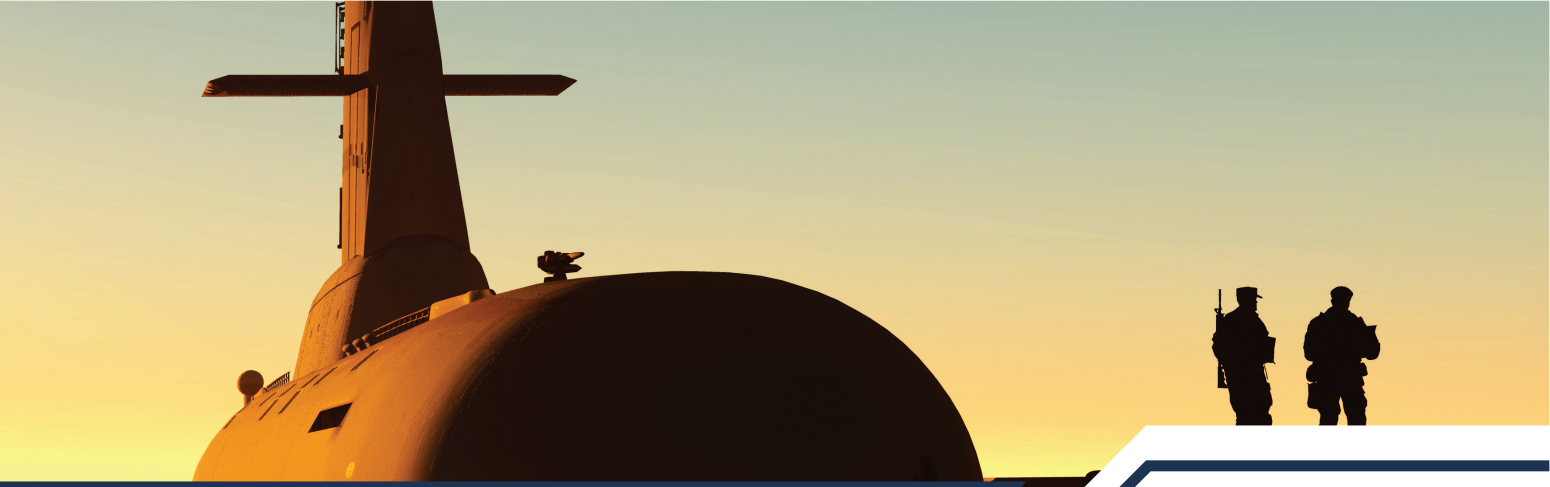
Țintele cele mai frecvente ale entităților ostile sunt reprezentate de instituțiile, organizațiile sau companiile care gestionează **informații clasificate** cu valențe economice sau elaborează strategii, studii și prognoze privind evoluția statului în diverse domenii. În egală măsură, aceeași preocupare se poate manifesta și față de **informațiile sensibile** deținute de corporații, în special în situația în care acestea operează contracte majore și complexe cu statul.

În **demersul de apărare** împotriva entităților ostile, respectiv de prevenire și contracarare a acțiunilor acestora, antidotul este unul instituțional, atât prin **conceperea și implementarea de strategii și politici** coerente, consecvente și eficiente, menite să consolideze domeniul economic, cât și prin luarea de **măsuri de protejare** adecvate împotriva influențelor negative și a efectelor acestora.

O economie funcțională este premisa de bază pentru stabilitatea statului și societății. În exercițiul său, statul trebuie să asigure, prin mecanismele și instrumentele instituționale de care dispune, atât protejarea intereselor naționale în activitatea economică și financiară, cât și crearea condițiilor necesare pentru creșterea calității vieții.

Serviciul Român de Informații acționează pentru cunoașterea, prevenirea și contracararea amenințărilor la adresa securității naționale în domenii vitale ale economiei, precum și pentru promovarea intereselor strategice de natură economică.


CONFIDENTIAL



CONTRAPROLIFERARE

România contribuie activ la eforturile comunității internaționale de contracarare a proliferării armelor de distrugere în masă - ADM și este parte semnatară în cadrul tratatelor și angajamentelor multilaterale care reglementează domeniul.

Statele și actorii non-statali cu grad ridicat de risc pot fi statele supuse unor embargouri internaționale, cele cu risc de deturnare, statele caracterizate de conflicte militare, firmele "paravan" ce acționează în beneficiul acestora, care:

- vizează procurarea clandestină de expertiză și produse/echipamente/ tehnologii utile pentru susținerea dezvoltării unor programe militare sensibile (de dezvoltare de ADM și armament convențional);

- manifestă preocupări pentru diversificarea constantă a metodelor de acțiune.

Rolul SRI în combaterea fenomenului proliferării se materializează pe linia cunoașterii, prevenirii și contracarării operațiunilor ilegale de transfer de tehnologie intangibilă și produse cu destinație specială, derulate cu încălcarea prevederilor legislației în domeniul controlului exporturilor și/sau în beneficiul unor state/actori non-statali cu grad ridicat de risc.

Pentru a veni în sprijinul autorităților naționale pentru identificarea timpurie și contracararea tentativelor de implicare a unor operatori economici autohtoni în tranzacții comerciale ilicite, este important să cunoști că:

Modus operandi utilizat de actorii care deservesc interesele statelor proliferante se bazează pe înființarea și coordonarea unor entități de acoperire (*persoane, companii și, în unele cazuri, chiar alte state cu rol de "plăci turnante"*), care să asigure disimularea operațiunilor de achiziție/ transfer.

Țintele prioritare vizate de actorii proliferanți sunt entitățile autohtone ce dețin:

- expertiză/cunoștințe în domenii sensibile, cum ar fi: inginerie nucleară; chimie aplicată, biologie; inginerie aerospațială; robotică; telecomunicații; IT ș.a. (*se vizează: specialiști; profesori; cercetători etc.*);

- capabilități de cercetare-dezvoltare și/sau producție de echipamente cu destinație specială, cum ar fi: produse cu dublă utilizare; produse înalt tehnologizate; tehnologii de ultimă oră; produse militare ș.a. (*se vizează: institute; fabrici; companii private; companii de stat producătoare de echipamente militare etc.*).

Pentru a evita implicarea în relaționări/transferuri ce pot avea ca efect susținerea unor activități de proliferare, **se recomandă**:

- cunoașterea legislației ce guvernează domeniul comerțului cu produse cu dublă utilizare, militare, chimice și biologice, precum și a celei prin care se implementează sancțiunile internaționale (*instituite la nivel internațional/ european/unilateral de anumite state*);

- o atitudine proactivă, dar precaută, în inițierea/angajarea în relaționări academice sau de afaceri cu parteneri ce provin din spații cu grad ridicat de risc;

- semnalarea cu promptitudine către autoritățile abilitate a oricăror suspiciuni referitoare la derularea unor activități subsumate proliferării ADM și a armamentului convențional, prin accesarea formularului de contact de pe site-ul **www.protector-romania.ro** (sesizarea unor comportamente care ies din tiparul logicii comerciale uzuale: solicitări atipice din partea partenerului de afaceri în ceea ce privește întocmirea documentației, modalitatea de plată, ruta de transport etc.; ezitări în furnizarea de date cu privire la destinația/utilizatorul final al tranzacției etc.).

DE REȚINUT:

Conștientizarea riscurilor asociate proliferării ADM și a armamentului convențional asigură atât protejarea intereselor de afaceri, cât și a imaginii României, prin neasocierea cu state/entități implicate în susținerea unor activități subsumate acestui fenomen.

AWARENESS

AWARENESS

Un material elaborat în cadrul
PROGRAMULUI DE AWARENESS
AL SERVICIULUI ROMÂN DE INFORMAȚII