ACADEMIA DE STUDII ECONOMICE DIN BUCUREŞTI
SENATUL UNIVERSITAR
Telefon/Fax 021-319.20.25, 021-319.19.00/int. 283, www.senat.ase.ro, e-mail: senat@ase.ro

Hotărârea nr. 10/09.02.2023

cu privire la aprobarea

Raportului privind implicațiile Planului de implementare a Strategiei de securitate cibernetică a României pentru perioada 2022-2027 asupra mediului academic

În temeiul Hotărârii Consiliului de Administrație nr. 07/25.01.2023 cu privire la înaintarea către Senatul ASE a propunerii de aprobare a Raportului privind implicațiile Planului de implementare a Strategiei de securitate cibernetică a României pentru perioada 2022-2027 asupra mediului academic;

În conformitate cu prevederile art. 213 alin. 2 lit. n) din Legea nr. 1/2011 a educației naționale, modificată și completată, ale art. 38 pct. 36 din Carta ASE, ale art. 3 pct. 36 din Regulamentul de organizare și funcționare a Senatului ASE, precum și ale Hotărârii Senatului nr. 8/22.01.2020;

Senatul Academiei de Studii Economice din București

Hotărăște

Art. 1. Aprobarea Raportului privind implicațiile Planului de implementare a Strategiei de securitate cibernetică a României pentru perioada 2022-2027 asupra mediului academic, conform anexei care face parte integrantă din prezenta hotărâre.

Art. 2. Consiliul de Administrație va duce la îndeplinire prevederile prezentei hotărâri.

Președinte Senat,

Prof. univ. dr. Dumitru MIRON

Cancelar Senat,

Prof. univ. dr. Paul POCATILU

Avizat pentru legalitate,

Director Direcția Juridică și Contencios Administrativ

Consilier Juridic Elena GĂMAN

MINISTERUL EDUCAȚIEI
ACADEMIA DE STUDII ECONOMICE DIN BUCUREŞTI
Direcţia Tehnologia Informaţiei şi Comunicaţii
Piaţa Romană nr. 6, sector 1, Bucureşti, cod 010374, România
Telefon 021.319.19.00, 021.319.19.01, fax +40 21.319.18.99
www.ase.ro, e-mail: depinfo@ase.ro

RAPORT
privind implicatiile Planului de implementare a
Strategiei de securitate cibernetică a României pentru perioada 2022-2027
asupra mediului academic

Prin H.G. nr. 1321/30.12.2021 au fost aprobate ***Strategia de securitate cibernetică a României, pentru perioada 2022-2027***, precum şi ***Planul de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027***.

Prin Decizia nr. 2300 din 04.05.2022, a fost aprobată componența Comisiei, care la nivelul Academiei de Studii Economice din Bucureşti, se va ocupa de armonizarea cu noile reglementări în materie de securitate cibernetică.

Componența comisiei stabilită conform Deciziei anterior menționată, este urmatoarea:

- Prof. univ. dr. Cristian CIUREA – Director – Departamentul de Informatică și Cibemetică Economică;
- Mihai NEGRILĂ – Director – Direcţia Tehnică Investiţii;
- Gabriel ŞUTAC – Director – Direcţia Tehnologia Informaţiei şi Comunicaţii;
- Florin BOACĂ – Analist,

In cele ce urmeaza se prezinta raportul elaborat de catre comisie.

I. Considerații generale asupra conținutului Strategiei de securitate cibernetică a României pentru perioada 2022 – 2027

I.1. Entitățile participante la implementarea Strategiei de securitate cibernetică

Actuala strategie de securitate cibernetică este elaborată pe baza rezultatelor și concluziilor desprinse de autoritățile române în urma aplicării strategiei anterioare, care a fost aprobată prin H.G. nr. 271/2013.

În cuprinsul actualei strategii se evidențiază că: „*[...] noul document are ca scop stabilirea principalelor linii directoare şi a abordărilor generale privind domeniul securităţii cibernetice. Noua Strategie va promova o viziune actualizată, care să vină în ajutorul întregii societăţi: autorităţi şi instituţii ale administraţiei publice şi entităţi private,* ***mediul academic****, cetăţeni.*
Implementarea şi aplicarea prevederilor Strategiei de către toţi actorii relevanţi va sprijini pe de o parte îndeplinirea obiectivelor naţionale de securitate şi angajamentelor asumate de România la nivel NATO şi UE, iar pe de altă parte ***va crea premisele necesare dezvoltării*** *mediului de afaceri, economiei naţionale şi* ***zonei educaţionale şi de cercetare***.”

Așadar, implementarea actualei strategii de securitate cibernetică, în perioada 2022 – 2027, se va face cu participarea și în folosul tuturor entităților relevante, în cadrul cărora se regăsesc **entitățile mediului academic**.

I.2. Contextul actual de aplicare a securității cibernetice

În cuprinsul actualei strategii se evidențiază că:

„*Atacurile cibernetice se află într-o evoluţie continuă, atât din punct de vedere al numărului, cât şi al complexităţii metodelor specifice utilizate. Acestea vizează un număr mare şi o varietate de reţele şi sisteme informatice, de la cele care deservesc persoane fizice, autorităţi şi instituţii ale administraţiei publice sau entităţi private, până la cele care deservesc entităţi a căror activitate se încadrează în ecuaţia securităţii naţionale* ."

„*Un spaţiu cibernetic sigur este atât responsabilitatea statului, prin autorităţile competente, cât şi a sectorului privat şi a societăţii civile. Consolidarea parteneriatelor între autorităţile şi instituţiile administraţiei publice şi societatea civilă, respectiv mediul privat, precum şi a celor între state şi organizaţii internaţionale este un punct esenţial de atins în obţinerea unui spaţiu cibernetic mondial, deschis şi sigur.*"

„*Atacurile cibernetice derulate de actori statali sunt de regulă de tip Advanced Persistent Threat (APT). Au un nivel tehnologic ridicat, atât în ceea ce priveşte modul de operare, cât şi din punct de vedere al aplicaţiilor malware folosite, actualizate permanent în vederea eludării mecanismelor de detecţie şi menţinerii persistenţei pentru o perioadă îndelungată de timp.*
lnstrumentarul cibernetic folosit de atacatori este divers, adaptat scopurilor operaţionale ale acestora."

„*Peisajul autohton a fost dominat în ultimii ani de atacuri cibernetice cu aplicaţii malware de tip ransomware, infostealer sau cryptojacking, care au vizat reţele şi sisteme informatice aparţinând unor autorităţi şi instituţii ale administraţiei publice sau entităţi private. De asemenea, se remarcă intensificarea atacurilor cibernetice din ce în ce mai complexe, inclusiv de tip APT, dedicate exploatării sistemelor informatice din domeniul financiar-bancar.*"

„*Exponenţii acestor categorii de atacatori derulează de regulă atacuri cibernetice de tip defacement, Distributed Denial of Service (DDoS) şi SQL Injection pentru a indisponibiliza sau afecta funcţionalitatea unor reţele şi sisteme informatice. Ţintele vizate sunt reprezentate îndeosebi de autorităţi şi instituţii ale administraţiei publice, dar şi de entităţi private sau* ***academice***."

Având în vedere că ASE din București a fost ea însăși ținta unui atac cibernetic în data de 02.10.2020 și că acest atac a debutat prin manifestări DDoS, continuate cu *ransomware*, constatăm că profilul ASE din București corespunde în foarte mare măsură contextului avut în vedere de către legiuitor și care conduce la **necesitatea de aplicare inclusiv în cadrul ASE din București a noii Strategii de securitate cibernetică în perioada 2022 – 2027**.

I.3. Viziunea strategiei naționale de securitate cibernetică pentru perioada 2022 – 2027

În cuprinsul Strategiei se regăsesc următoarele referiri:

„România are capacitatea de a detecta atacuri cibernetice la adresa reţelelor şi sistemelor informatice de pe teritoriul naţional şi de a diminua efectele acestora."

„[...] în faţa unei ameninţări cibernetice din ce în ce mai complexe, România să îşi dezvolte şi consolideze capabilităţile de prevenire, descurajare şi răspuns, precum şi reziliența, inclusiv printr-o abordare proactivă, adecvată cadrului internaţional de cooperare în domeniu."

„Acţiunile conjugate ale actorilor implicaţi trebuie să vizeze:

- prevenire şi descurajare – dezvoltarea permanentă a capabilităţilor de detecţie, investigare, combatere şi atribuire a atacurilor cibernetice;
- apărare şi contracarare – dezvoltarea şi implementarea unor capabilităţi eficiente de apărare şi a unor mecanisme proactive, de răspuns la atacuri cibernetice curente şi emergente;
- dezvoltare şi consolidare – creşterea nivelului de securitate cibernetică şi reziliență prin:

1. *prioritizarea investiţiilor în domeniul securităţii cibernetice;*
2. *dezvoltarea programelor educaţionale;*
3. *consolidarea culturii de securitate cibernetică;*
4. *dezvoltarea cercetării şi inovării în domeniu;*
5. *definirea şi promovarea unui model naţional de reziliență cibernetică ;*
6. *cooperarea la nivel naţional, european şi internaţional."*

Actuala viziune de aplicare a Strategiei naționale de securitate cibernetică pentru perioada 2022 – 2027 ia în considerare necesitatea creșterii nivelului de securitate cibernetică și de reziliență, stabilește căile de abordare în acest sens și **exemplifică în mod relevant pentru mediul academic** prin:

- prioritizarea investițiilor în domeniul securității cibernetice;
- dezvoltarea programelor educaționale;
- consolidarea culturii de securitate cibernetică;
- dezvoltarea cercetării şi inovării în domeniu;

I.4. Obiectivele Strategiei naţionale de securitate cibernetică pentru perioada 2022 – 2027

În cuprinsul Strategiei se regăsesc următoarele referiri:

„Cele 5 obiective de importanţă strategică pentru 2022 – 2027 în domeniul securităţii cibernetice sunt:
1. Rețele și sisteme informatice sigure si reziliente;
2. Cadru normativ și instituțional consolidat;
3. Parteneriat public-privat pragmatic;
4. Reziliență prin abordare proactivă și descurajare;
5. România – actor relevant în arhitectura internațională de cooperare."

De menționat că pentru îndeplinirea fiecărui **obiectiv** dintre cele menționate anterior sunt enumerate mai multe **măsuri**, iar pentru fiecare măsură în parte se evidențiază una sau mai multe **acțiuni principale**.

Măsurile concrete ce trebuie întreprinse pentru atingerea obiectivelor sunt cuprinse în ***Planul de Acţiune pentru implementarea Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027*** *şi reprezintă o responsabilitate comună a tuturor actorilor implicaţi.*

În **anexa** prezentului document se regăsește analiza implicațiilor pe care le are conținutul Planului de acțiune pentru entitățile mediului academic în general și pentru ASE din București în special.

Pentru fiecare **obiectiv** strategic se enumeră **măsurile** avute în vedere de către legiuitor.

Analiza se prezintă în format tabelar pentru fiecare dintre **acțiunile principale** care definesc cadrul și contextul în care se pune în aplicare fiecare dintre măsurile avute în vedere.

***

Pe baza analizei efectuate, în cele ce urmează, Comisia prezintă propunerile sale pentru **Planul de acțiuni de implementare în cadrul ASE din București a Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027**.

II. Propuneri pentru Planul de acțiuni de implementare în cadrul ASE din București a Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027

În elaborarea seturilor de propuneri care sunt evidențiate în continuare în prezentul document, Comisia a luat în considerare următoarele:

1) Importanța măsurilor organizatorice în materia protecției datelor cu caracter personal, avându-se în vedere aplicabilitatea prevederilor GDPR[1] în întregul Spațiu Economic European și obligativitatea de aplicare în România a acestui regulament european, sens în care, în cadrul universității, în anul 2018 a fost adoptată ***Politica A.S.E. pentru personalul didactic, didactic auxiliar și nedidactic care, în calitate de angajat al A.S.E., prelucrează date cu caracter personal***.
2) Incidența simultană a GDPR și a legislației naționale aferentă implementării și exploatării sistemelor de securitate (cum ar fi sistemele de supraveghere video), sens în care, prin **Decizia nr. 3260 din 29.07.2021** a Rectorului universității, în cadrul ASE din București a fost reglementat regimul de prelucrare a datelor cu caracter personal prin mijloace de supraveghere video.
3) Cadrul de asigurare a suportului instituțional de îndrumare a tuturor utilizatorilor de tehnologii digitale în cadrul universității, reglementat prin aplicarea **Politicii de securitate IT în Academia de Studii Economice din București**, aprobată prin Hotărârea Senatului Universitar nr. 127 din 30.07.2021.
4) Demersurile efectuate pentru adoptarea **Regulamentului privind utilizarea resurselor Cloud gestionate de către ASE din București**.
5) **Strategia de Digitalizare a Academiei de Studii Economice din Bucureşti pentru perioada 2022-2027**, adoptată prin **Hotărârea Senatului Universitar al ASE nr. 76 din 02.06.2022**, din care enumerăm orientările strategice ale ASE din București în privința asigurării securității sale cibernetice:
   a. alinierea la prevederile legislației în vigoare cu incidență în materia securității cibernetice;
   b. alinierea la prevederile standardelor europene și internaționale privind securitatea informației;
   c. creșterea performanțelor / capabilităților soluției de securitate cibernetică implementată pentru domeniul Intranet.ase;
   d. adoptarea în cadrul soluției de securitate cibernetică implementată pentru domeniul Intranet.ase în măsura în care acest lucru va fi posibil din punct de vedere tehnic și accesibil din punct de vedere financiar, a tehnologiilor digitale de tip **machine learning (ML)** și **artificial intelligence (AI)**, în mod special pentru automatizarea algoritmilor de identificare a tiparelor (pattern-urilor) manifestate în desfășurarea unor atacuri cibernetice care pot avea manifestări de debut cu o dinamică de mare amploare, cum ar fi cele din categoriile **brute force** și **distributed denial of services** (**DDoS**).
6) Conținutul proiectului **Universitatea sustenabilă prin digitalizare. Investiții în infrastructura de cercetare și educație (ASE 4.0)**, depus de către ASE în cadrul **Apelului de proiecte dedicat digitalizării universităților**, cu finanțare din fonduri europene din **Planul Național de Redresare și Reziliență**.

Având în vedere cele enumerate anterior, Comisia a elaborat propunerile evidențiate în continuare astfel încât acestea să asigure consistență și continuitate în abordarea ASE asupra securității sale cibernetice, astfel:

II.1. Propuneri de acțiuni prioritare cu implicații organizatorice, tehnice și logistice

[1] - **REGULAMENTUL nr. 679 din 27 aprilie 2016** privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) emis de PARLAMENTUL EUROPEAN şi CONSILIUL UNIUNII EUROPENE - **GDPR**

Pentru implementarea propunerilor de **acțiuni prioritare** evidențiate în prezentul paragraf, termenele nu depasesc finalul anului **2023**.

II.1.1. Adaptarea în cadrul ASE din București a *seturilor de recomandări emise / diseminate de către Directoratul Național pentru Securitate Cibernetică (DNSC) cu privire la politici şi măsuri de securitate cibernetică*
Compartiment funcțional responsabil: DTIC
Termen: 6 luni de la publicarea respectivelor seturi de recomandări, având în vedere că termenul de emitere a acestora este fixat pentru semestrul I / 2023.

II.1.2. Implementarea și transpunerea politicilor și măsurilor de securitate cibernetică adoptate în cadrul ASE din București
Compartiment funcțional responsabil: DTIC
Termen: finele semestrului al II-lea / 2023

În funcție de volumul efortului bugetar care va rezulta ca necesar pentru implementarea și transpunerea politicilor și măsurilor de securitate cibernetică adoptate, termenul asumat se poate prelungi cu o perioadă de 6 – 12 luni.

II.1.3. Aplicarea în cadrul ASE din București *a metodologiei de evaluare a nivelului de securitate cibernetică* şi întocmirea *planului de recuperare în caz de atac cibernetic.*
Compartiment funcțional responsabil: DTIC
Termen: 6 luni de la publicarea respectivei metodologii și a conținutului planurilor de recuperare în caz de atac cibernetic ce vor fi recomandate, având în vedere că termenul de emitere a acestora este fixat pentru semestrul I / 2023.

II.1.4. Implementarea în cadrul ASE din București a rezultatelor și concluziilor obținute din *evaluarea nivelului de securitate cibernetică*.
Compartiment funcțional responsabil: DTIC
Termen: finele semestrului al II-lea / 2023

În funcție de volumul efortului bugetar care va rezulta ca necesar pentru implementarea concluziilor/rezultatelor obținute din *evaluarea nivelului de securitate cibernetică*, termenul asumat se poate prelungi cu o perioadă de 6 – 12 luni.

II.1.5. Asigurarea includerii unei componente de securitate cibernetică în toate proiectele de investiții din domeniul TIC, care sunt supuse avizării Comitetului tehnico-economic instituit prin HG 941/2013.
Compartiment funcțional responsabil: DTIC
Termen de intrare în vigoare: cu începere din 01.07.2022

II.1.6. Preluarea de pe pagina de Internet a DNSC și postarea pe pagina de Internet alocată DTIC a informațiilor publicate de către DNSC cu privire la bune practici şi recomandări în detectarea, investigarea și contracararea atacurilor cibernetice.
Compartiment funcțional responsabil: DTIC
Termen de intrare în vigoare: 01.07.2022

II.1.7. Implementarea de tehnologii de ultimă generaţie pentru detectarea, investigarea și contracararea atacurilor cibernetice.
Compartiment funcțional responsabil: DTIC
Termen de intrare în vigoare: 01.07.2022

În funcție de volumul efortului bugetar care va rezulta ca necesar pentru implementarea de tehnologii de ultimă generaţie pentru detectarea, investigarea și contracararea atacurilor cibernetice, termenul de intrare în vigoare asumat se poate prelungi cu o perioadă de 6 – 12 luni.

II.1.8. Actualizarea organigramei DTIC și a fișelor de post aferente pentru transformarea denumirii unor posturi în concordanță cu finalizarea demersurilor de includere în nomenclatorul COR a ocupaţiilor specifice domeniului securităţii cibernetice.
Compartimente funcționale responsabile: DTIC, DRU
Termen: Acțiunea va putea fi pusă în practică după publicarea informațiilor relevante privind includerea în nomenclatorul COR a ocupațiilor specifice domeniului securității cibernetice.

II.1.9. Constituirea unei echipe de tip CERT (Echipă de răspuns la incidente de securitate cibernetică) la nivelul ASE din București.
Compartiment funcțional responsabil: DTIC
Termen: semestrul al II-lea / 2023

II.1.10. Analiza implicațiilor asupra mediului academic din partea conținutului viitoarei Legi privind Securitatea şi Apărarea Cibernetică; Ministerul Apărării Naționale (MApN) este inițiatorul proiectului de lege.
Compartimente funcționale responsabile: DTIC, DJCA
Termen: 30 zile după publicarea viitoarei legi.

II.2. Propuneri de acțiuni de perspectivă cu implicaţii organizatorice, tehnice și logistice

Pentru implementarea propunerilor de **acțiuni de perspectivă** evidențiate în prezentul paragraf, termenele sunt cuprinse în intervalul de timp **sem. al II-lea / 2022 – finele sem. al II-lea / 2027**.

II.2.1. Participarea la derularea programelor finanțate din fonduri europene (POCIDIF, POEO), PNRR, fonduri alocate din Programul Europa Digitală, hub-urilor de inovare digitală, pentru implementarea unor componente de securitate cibernetică.
Compartiment funcțional responsabil: DTIC
Termen: în funcție de calendarul de desfășurare a programelor de finanțare relevante

La nivel național, acțiunea se află în coordonarea / responsabilitatea Secretariatului General al Guvernului (SGG).

Este foarte important dacă Ministerul Educației va promova și va susține alocarea de fonduri bugetare pentru securitatea cibernetică a universităților aflate în coordonarea sa.

II.2.2. Elaborarea propunerilor de achiziții în cadrul ASE din București pentru produse și tehnologii de securitate cibernetică care au fost evaluate și certificate potrivit legii.
Compartiment funcțional responsabil: DTIC
Termen de intrare în vigoare: cu începere din semestrul al II-lea / 2023, în funcție de finalizarea acțiunilor de desemnare şi/sau autorizare a entităţilor de evaluare şi certificare a produselor și tehnologiilor de securitate cibernetică.

II.3. Acțiuni prioritare și de perspectivă la nivel național, cu potențial impact de imagine pentru ASE din București

Pentru implementarea la nivel național a **acțiunilor prioritare și de perspectivă** evidențiate în prezentul paragraf, termenele sunt cuprinse în intervalul de timp **sem. al II-lea / 2022 – finele sem. al II-lea / 2027**.

Nivelul de participare / implicare a ASE din București în derularea acestor acțiuni prioritare și de perspectivă va fi stabilit de către factorii de decizie ai universității.

II.3.1. Dezvoltarea unor formate de pregătire a palierului managerial din cadrul autorităţilor şi instituţiilor administraţiei publice și entităţilor private, în vederea alocării eficiente și complementare a resurselor necesare pentru asigurarea unui nivel corespunzător de securitate cibernetică.
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: sem. al II-lea/2023

a) ASE din București va raspunde afirrmativ unei posibile invitatii a Directoratului Național pentru Securitate Cibernetică (DNSC) privind contribuția la această acțiune.
b) Eventualul termen se va stabili de comun acord între DNSC și ASE din București.
c) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.3.2. Derularea unor campanii de conştientizare şi de informare prin programe media, broşuri, website-uri dedicate, ghiduri de bune practici.
Responsabili la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC) și Serviciul Român de Informații (SRI)
Termen: permanent

a) ASE din București va raspunde afirrmativ unei posibile invitatii a Directoratului Național pentru Securitate Cibernetică (DNSC) și / sau a Serviciul Român de Informații (SRI) privind contribuția la această acțiune.
b) Eventualul termen se va stabili de comun acord între DNSC și/sau SRI și respectiv ASE din București.
c) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.3.3. Derularea unor activităţi care să vizeze conştientizarea palierului managerial din cadrul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private cu privire la necesitatea asigurării securităţii cibernetice.
Responsabili la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC), Serviciul Român de Informații (SRI)
Termen: permanent

a) ASE din București va raspunde afirrmativ unei posibile invitatii a Directoratului Național pentru Securitate Cibernetică (DNSC) și / sau a Serviciul Român de Informații (SRI) privind contribuția la această acțiune.
b) Eventualul termen se va stabili de comun acord între DNSC și/sau SRI și respectiv ASE din București.
c) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.3.4. Organizarea de evenimente cu experţi în domeniul securităţii cibernetice.
Responsabil la nivel ASE: structurile organizatorice ASE
Termen: permanent

a) Asumarea acestei acțiuni este exclusiv de competența factorilor de decizie din cadrul ASE din București.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitatea organizatorică a ASE și respectiv a potențialilor invitați experți în domeniul securității cibernetice.

II.3.5. Realizarea unor demersuri privind introducerea unor noţiuni de igienă în spaţiul cibernetic (set de practici şi deprinderi în materie de securitate cibernetică, necesare pentru desfăşurarea în siguranţă a activităţilor zilnice întreprinse de utilizatori) la nivel preuniversitar.
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) In cazul in care în care Ministerul Educației (ME) va solicita universităților din coordonare să se implice în derularea acestei acțiuni, ASE va raspunde pozitiv solicitarii
b) În cazul in care ASE din București va fi invitată de către Directoratul Național pentru Securitate Cibernetică (DNSC) să participe / să își aducă contribuția la această acțiune, se va raspunde pozitiv, ținându-se seamă și de eventualul punct de vedere exprimat de către ministerul coordonator.
c) Eventualul termen se va stabili de comun acord între DNSC și ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității

II.4. Acțiuni prioritare și de perspectivă la nivel național, cu impact în activitatea didactică și de cercetare științifică desfășurate de către ASE din București

Pentru implementarea la nivel național a **acțiunilor prioritare și de perspectivă** evidențiate în prezentul paragraf, termenele sunt cuprinse în intervalul de timp **sem. al II-lea / 2022 – finele sem. al II-lea / 2027**.

Nivelul de participare / implicare a ASE din București în derularea acestor acțiuni prioritare și de perspectivă se va stabili de către factorii de decizie ai universității.

II.4.1. Dezvoltarea şi implementarea unor programe de studii de securitate cibernetică la nivel universitar şi postuniversitar
Termen: permanent

a) Asumarea acestei acțiuni este exclusiv de competența factorilor de decizie din cadrul ASE din București, cu privire la actualizarea programelor de studii.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a lărgi oferta sa educațională cu programe de studii de securitate cibernetică la nivel universitar şi postuniversitar.

II.4.2. Susţinerea integrării pe piaţa muncii a studenţilor şi absolvenţilor programelor de studii în domeniul securităţii cibernetice, inclusiv prin realizarea unor stagii de practică în cadrul unor autorităţi şi instituţii ale administraţiei publice sau entităţi private din domeniu.
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Asumarea acestei acțiuni este de competența factorilor de decizie din cadrul ASE din București și este oarecum în subsecvență la acțiunea precedentă, de lărgire a ofertei educaționale a universității cu programe de studii de securitate cibernetică la nivel universitar şi postuniversitar;
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a lărgi oferta sa educațională cu programe de studii de securitate cibernetică la nivel universitar şi postuniversitar, care vor necesita în mod evident organizarea unor stagii de practică pentru studenții înscriși la aceste programe educaționale.

II.4.3. Realizarea demersurilor de accesare a finanțării din fonduri externe (europene) a unor proiecte corelate cu derularea programelor de studii de securitate cibernetică la nivel universitar şi postuniversitar.
Responsabili la nivel național: Ministerul Educației (ME), Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Nu se poate exclude ipoteza în care Ministerul Educației (ME) să propună universităților din coordonare să se implice în derularea acestei acțiuni, prin participare la concursurile de proiecte de acest tip.
b) Este posibil ca ASE din București să fie invitată de către Directoratul Național pentru Securitate Cibernetică (DNSC) să participe la această acțiune.
c) Eventualele termene se vor stabili de comun acord între DNSC și ASE din București, cu înștiințarea în consecință a Ministerului Educației.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.4.4. Derularea unor activități pentru pregătirea și instruirea personalului didactic alocat programelor de studii de securitate cibernetică la nivel universitar şi postuniversitar.
Responsabili la nivel național: Ministerul Educației (ME), Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Nu se poate exclude ipoteza în care Ministerul Educației (ME) să solicite universităților din coordonare să se implice în derularea acestei acțiuni.
b) In cazul in care ASE din București va fi invitată de către Directoratul Național pentru Securitate Cibernetică (DNSC) să își aducă contribuția la această acțiune, se va raspunde pozitiv, ținându-se seamă și de eventualul punct de vedere exprimat de către ministerul coordonator, dar și de caracterul subsecvent al acestei acțiuni în raport cu una dintre acțiunile precedente, cea de lărgire a ofertei educaționale a universității cu programe de studii de securitate cibernetică la nivel universitar şi postuniversitar;
c) Eventualele termene se vor stabili de comun acord între DNSC și ASE din București, cu înștiințarea în consecință a Ministerului Educației.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.4.5. Organizarea de cursuri de specializare (postuniversitare) în domeniul securității cibernetice adresate diferitelor categorii profesionale.
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Asumarea acestei acțiuni este exclusiv de competența factorilor de decizie din cadrul ASE din București.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a lărgi oferta sa educațională cu cursuri de specializare (postuniversitare) în domeniul securității cibernetice adresate diferitelor categorii profesionale.

II.4.6. Dezvoltarea de centre de instruire pentru cei care desfăşoară activităţi în domeniul securităţii cibernetice
Termen: permanent

a) Asumarea participării la această acțiune, fie doar în nume propriu, fie în colaborare cu alte instituții, este exclusiv de competența factorilor de decizie din cadrul ASE din București.

b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a participa la această acțiune.

II.4.7. Dezvoltarea de parteneriate public-private în domeniul cercetării şi inovării cu aplicare în securitatea cibernetică.
Termen: permanent

a) Asumarea participării la această acțiune, fie în nume propriu, fie în colaborare cu alte instituții, este exclusiv de competența factorilor de decizie din cadrul ASE din București.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE, pentru fiecare caz in parte, de a participa la această acțiune.

II.4.8. Participarea ASE din București la în programe de cercetare şi inovare în securitate cibernetică derulate la nivel regional, european şi internaţional.
Responsabil la nivel național: Ministerul Cercetării, Inovării și Digitalizării (MCID)
Termen: permanent
a) Este posibil ca ASE din București să fie invitată de către Ministerul Cercetării, Inovării și Digitalizării (MCID) să participe / să își aducă contribuția la această acțiune.
b) Adoptarea unui curs pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București;
c) Eventualele termene se vor stabili de comun acord între MCID și ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.4.9. Capitalizarea prezenței în România a *Centrului de competenţe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică.*
Termen: permanent

a) Asumarea participării la această acțiune, fie în nume propriu, fie în colaborare cu alte instituții, este exclusiv de competența factorilor de decizie din cadrul ASE din București.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a participa la această acțiune.

II.4.10. Crearea unor mecanisme instituţionale pentru consultanţă şi susţinere financiară a activităţilor de cercetare şi inovare din domeniul securităţii cibernetice.
Responsabil la nivel național: Ministerul Cercetării, Inovării și Digitalizării (MCID)
Termen: permanent
a) Este posibil ca ASE din București să fie invitată de către Ministerul Cercetării, Inovării și Digitalizării (MCID) să participe / să își aducă contribuția la această acțiune.
b) Adoptarea unui curs pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București;
c) Eventualele termene se vor stabili de comun acord între MCID și ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.4.11. Impulsionarea, prin oferirea de consultanţă şi susţinere financiară, iniţiativelor de dezvoltare a incubatoarelor de afaceri şi *start-up-urilor* în domeniul securității cibernetice.
Responsabili la nivel național: Ministerul Antreprenoriatului și Turismului (MAT), Ministerul Economiei (MEc)
Termen: permanent

a) Este posibil ca ASE din București să fie invitată de către Ministerul Antreprenoriatului și Turismului (MAT) și / sau Ministerul Economiei (MEc) să participe / să își aducă contribuția la această acțiune.
b) Adoptarea unui curs pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București;
c) Eventualele termene se vor stabili de comun acord între MAT și/sau MEc și respectiv ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.5. Acţiuni prioritare şi de perspectivă la nivel naţional, cu posibil impact în resursele TIC / de securitate cibernetică ale ASE din București

Pentru implementarea la nivel național a **acțiunilor prioritare și de perspectivă** evidențiate în prezentul paragraf, termenele sunt cuprinse în intervalul de timp **sem. al II-lea / 2022 – finele sem. al II-lea / 2027**.

Nivelul de participare / implicare a ASE din București în derularea acestor acțiuni prioritare și de perspectivă trebuie stabilit de către factorii de decizie ai universității.

II.5.1. Derularea unor campanii de conştientizare a factorilor de decizie de la nivelul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private cu privire la avantajele şi necesitatea constituirii unor echipe de tip CERT (Echipă de răspuns la incidente de securitate cibernetică) și SOC (Centru Operaţional de Securitate) sectoriale.
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Nu se poate exclude posibilitatea ca ASE din București să fie invitată de către Directoratul Național pentru Securitate Cibernetică (DNSC) să participe / să își aducă contribuția la această acțiune.
b) Un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualele termene se vor stabili de comun acord între DNSC și ASE din București.
d) Compartiment funcțional responsabil din partea ASE din București: DTIC.

II.5.2. Crearea unor formate și mecanisme de cooperare între structurile de tip CERT(Echipă de răspuns la incidente de securitate cibernetică) / SOC(Centru Operațional de Securitate) sectorial, inclusiv între cele din SNAOPSN (Sistemul Național de Apărare, Ordine Publică și Siguranță Națională).
Responsabil la nivel național: Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: Semestrul II / 2022, se continuă permanent

a) Nu se poate exclude posibilitatea ca ASE din București să fie invitată de către Directoratul Național pentru Securitate Cibernetică (DNSC) să participe / să își aducă contribuția la această acțiune.
b) Un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualele termene se vor stabili de comun acord între DNSC și ASE din București.
d) Compartiment funcțional responsabil din partea ASE din București: DTIC.

II.5.3. Cooperare la nivel naţional în vederea organizării şi participării la exerciţii cu aplicabilitate practică ridicată în domeniul securităţii cibernetice
Termen: permanent

a) Asumarea participării la această acțiune, fie doar în nume propriu, fie în colaborare cu alte instituții, este exclusiv de competența factorilor de decizie din cadrul ASE din București.
b) Eventualele responsabilități și termene se vor stabili funcție de disponibilitățile și resursele ASE de a participa la această acțiune.

II.5.4. Organizarea şi participarea la exerciţii naţionale cu aplicabilitate practică ridicată, în domeniul securităţii cibernetice
Responsabili la nivel național: Serviciul Român de Informații (SRI), Directoratul Național pentru Securitate Cibernetică (DNSC)
Termen: permanent

a) Este relevant să precizăm că resursele TIC ale ASE sunt destinate exploatării în cadrul activităților desfășurate de către facultățile și unitățile administrative ale ASE; alocarea unor resurse tehnice și umane pentru participarea la astfel de exerciții se va face in masura in care aceasta activitate se apreciaza a avea un impact semnificativ pentru activitatea ASE.
b) In ipoteza în care ASE din București va fi invitată de către Serviciul Român de Informații (SRI) și / sau de către Directoratul Național pentru Securitate Cibernetică (DNSC) să participe / să își aducă contribuția la această acțiune, un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualul termen se va stabili de comun acord între SRI și/sau DNSC și respectiv ASE din București.
d) Compartiment funcțional responsabil din partea ASE din București: DTIC

II.5.5. Organizarea de exerciţii civil-militare de pregătire şi integrare coerentă a procedurilor specifice de răspuns la incidentele de securitate cibernetică ce afectează infrastructuri esenţiale
Responsabil la nivel național: Ministerul Apărării Naționale (MApN)
Termen: permanent

a) Este relevant să precizăm că resursele TIC ale ASE sunt destinate exploatării în cadrul activităților desfășurate de către facultățile și unitățile administrative ale ASE; alocarea unor resurse tehnice și umane pentru participarea la astfel de exerciții se va face in masura in care aceasta activitate se apreciaza a avea un impact semnificativ pentru activitatea ASE.
b) In ipoteza în care ASE din București va fi invitată de către Ministerul Apărării Naționale (MApN) să participe / să își aducă contribuția la această acțiune, un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualul termen se va stabili de comun acord între MApN și respectiv ASE din București.
d) Compartiment funcțional responsabil din partea ASE din București: DTIC.

II.6. Acțiuni prioritare și de perspectivă la nivel național, cu anvergură internațională

Pentru implementarea la nivel național a **acțiunilor prioritare și de perspectivă** evidențiate în prezentul paragraf, termenele sunt cuprinse în intervalul de timp **sem. al II-lea / 2022 – finele sem. al II-lea / 2027**.

Nivelul de participare / implicare a ASE din București în derularea acestor acțiuni prioritare și de perspectivă trebuie stabilit de către factorii de decizie ai universității.

II.6.1. Participarea activă la consultări şi iniţiative internaţionale, guvernamentale, a actorilor relevanţi din mediul public, privat şi academic, precum şi din cadrul societăţii civile.
Responsabil la nivel național: Ministerul Afacerilor Externe (MAE)
Termen: permanent

a) Nu se poate exclude ipoteza în care ASE din București ar putea fi invitată de către Ministerul Afacerilor Externe (MAE) să participe / să își aducă contribuția la această acțiune.
b) Un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualul termen se va stabili de comun acord între MAE și respectiv ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

II.6.2. Dezvoltarea și organizarea unui eveniment, de anvergură internaţională, recunoscut ca punct de referinţă în domeniul securităţii cibernetice
Responsabil la nivel național: Secretariatul General al Guvernului (SGG)
Termen: Semestrul II / 2023, se continuă anual

a) Nu se poate exclude ipoteza în care ASE din București ar putea fi invitată de către Secretariatul General al Guvernului (SGG) să participe / să își aducă contribuția la această acțiune.
b) Un eventual raspuns pozitiv pentru respectiva invitație se decide la nivelul conducerii ASE din București.
c) Eventualul termen se va stabili de comun acord între SGG și respectiv ASE din București.
d) Compartimentele funcționale responsabile din partea ASE din București se vor stabili de către conducerea universității.

Comisia desemnată prin Decizia nr. 2399 din 04.05.2022

Prof. univ. dr. Cristian CIUREA – Director – Departamentul de Informatică și Cibemetică Economică;

Mihai NEGRILĂ – Director – Direcţia Tehnică Investiţii;

Gabriel ŞUTAC – Director – Direcţia Tehnologia Informaţiei şi Comunicaţii;

Florin BOACĂ – Analist

MINISTERUL EDUCAȚIEI
ACADEMIA DE STUDII ECONOMICE DIN BUCUREŞTI
Direcţia Tehnologia Informaţiei şi Comunicaţii
Piaţa Romană nr. 6, sector 1, Bucureşti, cod 010374, România
Telefon 021.319.19.00, 021.319.19.01, fax +40 21.319.18.99
www.ase.ro, e-mail: depinfo@ase.ro

IMPLICAȚIILE
asupra mediului academic generate de
Planul de Acţiune pentru implementarea Strategiei de Securitate Cibernetică a României, pentru perioada 2022-2027

Obiectivul 1 – Rețele și sisteme informatice sigure și reziliente
Măsuri
1.1. Implementarea de politici şi măsuri de securitate cibernetică

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
1.1.a.	Realizarea și diseminarea unor *seturi de recomandări cu privire la politici şi măsuri de securitate cibernetică*, în concordanţă cu nivelul ameninţării cibernetice şi cu trendul rapid de dezvoltare al tehnologiilor	SRI, STS, MApN, MAI, ORNISS, SIE, SPP, ANCOM, DNSC	DNSC	Semestrul I, 2023, se continuă permanent	După finalul semestrului I/2023, va trebui ca **entitățile mediului academic** să ia la cunoștință despre conținutul respectivelor *seturi de recomandări cu privire la politici şi măsuri de securitate cibernetică*, pentru: - a își alinia propriile politici de securitate cibernetică la conținutul acestor recomandări; - a aplica măsurile de securitate cibernetică recomandate, având în vedere nivelul de relevanță a acestora pentru mediul academic **Obs.** Deoarece acțiunea se continuă permanent, pe măsură ce respectivele seturi se vor actualiza, va trebui ca entitățile mediului academic să își actualizeze politicile de securitate cibernetică, să cunoască și să aplice măsurile de securitate cibernetică actualizate în funcție de nivelul de relevanță a acestora pentru mediul academic.

1.1.b.	Implementarea la nivelul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private a seturilor de recomandări cu privire la politici şi măsuri de securitate cibernetică	Autorităţile şi instituţiile administraţiei publice şi entităţile private care au în administrare şi operare reţele și sisteme informatice, **mediul academic**, societatea civilă	-	Semestrul II, 2023, se continuă permanent	Se deduce că, pentru entitățile din mediul academic, **finalul semestrului al II-lea / 2023 este <u>termenul</u> de implementare / transpunere** a respectivelor *seturi de recomandări cu privire la politici şi măsuri de securitate cibernetică*, elaborate în contextul prezentat anterior. **Obs.** 1. Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a se autoverifica pentru încadrarea în termenul fixat pentru îndeplinirea acesteia. 2. Faptul că această acțiune se continuă permanent obligă pe fiecare dintre entitățile vizate să procedeze la actualizarea periodică a politicilor și măsurilor de securitate cibernetică adoptate / implementate.
1.1.c.	Realizarea și diseminarea unor *metodologii de evaluare a nivelului de securitate cibernetică* şi a unor *planuri de recuperare în caz de atac cibernetic*	SRI, STS, MApN, MAI, ORNISS, SIE, SPP, ANCOM, DNSC	DNSC	Semestrul I, 2023, se continuă permanent	După finalul semestrului I/2023, va trebui ca fiecare dintre entitățile mediului academic să ia la cunoștință despre conținutul respectivelor *metodologii de evaluare a nivelului de securitate cibernetică* şi a respectivelor *planuri de recuperare în caz de atac cibernetic*, pentru: - a proceda la evaluarea propriului nivel de securitate cibernetică; - a adapta la caracteristicile proprii planurile de recuperare în caz de atac cibernetic recomandate la nivel național. **Obs.** Deoarece acțiunea <u>se continuă permanent</u>, pe măsură ce respectivele metodologii de evaluare și planuri de recuperare se vor actualiza, va trebui ca entitățile mediului academic să procedeze, după caz, la: - reevaluarea periodică a propriului nivel de securitate cibernetică; - actualizarea propriilor planuri de recuperare în caz de atac cibernetic.

1.1.d.	Implementarea la nivelul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private a metodologiilor de evaluare a nivelului de securitate cibernetică și a planurilor de recuperare în caz de atac cibernetic	Autorităţile şi instituţiile administraţiei publice şi entităţile private care au în administrare şi operare reţele și sisteme informatice, **mediul academic**	-	Semestrul II, 2023, se continuă permanent	Se deduce că, pentru toate entitățile din mediul academic, **finalul semestrului al II-lea / 2023 este <u>termenul</u> de implementare** a respectivelor *metodologii de evaluare a nivelului de securitate cibernetică* și a respectivelor *planuri de recuperare în caz de atac cibernetic*, elaborate în contextul prezentat anterior. **Obs.** 1. În mod evident, evaluarea și reevaluarea nivelului de securitate cibernetică vor deveni acțiuni periodice, pentru care <u>o abordare pragmatică poate fi efectuarea periodică a unor audituri de securitate cibernetică pe baze contractuale</u>. 2. Actualizarea planului de recuperare în caz de atac cibernetic poate fi una dintre cerințele de prestare de servicii din cadrul contractului ce poate fi încheiat pentru efectuarea periodică a auditurilor de securitate cibernetică. 3. Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a se autoverifica pentru încadrarea în primul termen fixat pentru îndeplinirea acesteia (finalul sem. al II-lea / 2023).
1.1.e.	Dezvoltarea de programe de instruire cu privire la implementarea politicilor şi măsurilor de securitate cibernetică	SRI, STS, MApN, MAI, ORNISS, SIE, SPP, ANCOM, DNSC, ADR	DNSC	Semestrul II, 2023, se continuă permanent	Pentru instituțiile care au fost desemnate responsabile pentru această acțiune <u>nu rezultă în niciun fel obligația / posibilitatea de colaborare cu **toate** entitățile din mediul academic</u>. Totuși, este posibil ca aceste instituții să aibă în vedere cooperarea cu instituțiile de învățământ superior din Sistemul Național de Apărare, Ordine Publică și Siguranță Națională. În mod evident, oricare universitate va putea analiza oportunitatea de a oferi programe educaționale de instruire cu privire la implementarea politicilor și măsurilor de securitate cibernetică
1.1.f.	Consolidarea mecanismului de verificare / validare a	Reprezentanţii instituţiilor	ADR	Semestrul II, 2022	Rezultă că, **începând cu 01.07.2022**, va trebui ca toate proiectele de investiții cu specific IT&C, care se supun avizului CTE, să aibă

	componentei de securitate cibernetică a proiectelor tehnologiei informaţiilor si comunicaţiilor depuse de autorităţile şi instituţiile administraţiei publice în Comitetul tehnico-economic instituit prin HG 941/2013	membre în CTE cu atribuţii în securitate cibernetică			o componentă de securitate cibernetică, pe care membrii CTE o vor audita distinct. Această cerință se va transpune obligatoriu în conținutul Caietelor de sarcini ce vor fi elaborate pentru organizarea achizițiilor publice aferente.

1.2. Dezvoltarea capabilităţilor naţionale de detectare, investigare şi contracarare a atacurilor cibernetice

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
1.2.a.	Schimb de informaţii, bune practici şi recomandări în detectarea, investigarea și contracararea atacurilor cibernetice, între autorităţi şi instituţii ale administraţiei publice, precum și între acestea şi entităţile private	SRI, STS, MApN, MAI, ORNISS, SIE, SPP, ANCOM, DNSC, **entităţi private**	DNSC	Permanent	Referirea la entitățile private poate include și entitățile din mediul academic; cel puțin universitățile particulare acreditate ar intra în această categorie. În ceea ce privește **investigarea** atacurilor cibernetice care s-au produs există un cadru legal și procedural, în care entitățile atacate se pot adresa cu plângeri penale *in rem* către Poliție (DCCO/BCCO din cadrul IGPR/DGPMB) și/sau către DIICOT. În funcție de natura și implicațiile unui atac cibernetic deja produs, cadrul legal în vigoare permite inclusiv comunicarea către SRI. În ceea ce privește **detectarea și contracararea** atacurilor cibernetice posibile în viitor, nu toate entitățile mediului privat pot fi în măsură să prezinte informații relevante sau să recomande bune practici. În legătură cu aceste două aspecte, entitățile mediului academic pot lua în considerare informațiile și bunele practici recomandate de către DNSC pe pagina de Internet a acestei instituții. Această abordare este sugerată din faptul că este stabilit un termen permanent pentru această acțiune.

1.2.b.	Dezvoltarea și implementarea de tehnologii de ultimă generaţie pentru detectarea, investigarea și contracararea atacurilor cibernetice	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat, **academic** şi de cercetare	-	Permanent	Este foarte posibil ca *seturile de recomandări cu privire la politici şi măsuri de securitate cibernetică* ce vor fi adoptate la nivel național să cuprindă cel puțin o referire la implementarea de tehnologii capabile măcar să detecteze atacuri cibernetice. Obs. 1. Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a se autoverifica pentru încadrarea în termenul fixat pentru îndeplinirea acesteia. 2. Caracterul permanent al termenului de îndeplinire a acestei acțiuni sugerează că fiecare entitate vizată va trebui să auditeze (direct sau prin terți) eficacitatea tehnologiilor implementate pentru detectarea atacurilor cibernetice și chiar să fie în măsură să își modernizeze / actualizeze tehnologia implementată.
1.2.c.	Consolidarea cooperării și colaborării instituţiilor din SNAOPSN cu autorităţi și instituţii ale administraţiei publice şi entităţi private în vederea asigurării coerenţei acţiunilor comune de descurajare a eventualelor atacuri cibernetice și conjugării eforturilor de realizare a securităţii și apărării cibernetice la nivel naţional	Instituţii din SNAOPSN, autorităţi şi instituţii ale administraţiei publice şi entităţi private	-	Permanent	Referirea la entitățile private poate include și entitățile din mediul academic; cel puțin universitățile particulare acreditate ar intra în această categorie. În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
1.2.d.	Dezvoltarea cadrului procedural necesar pentru atribuirea atacurilor cibernetice	MAE, SRI, SIE, STS, AP	MAE	Semestrul I, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”.

					Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

1.3 Alocarea eficientă a resurselor financiare, tehnologice şi umane

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
1.3.a.	Furnizarea de sprijin şi consultanţă pentru realizarea de investiţii în tehnologii necesare asigurării securităţii şi rezilienţei cibernetice	Instituţii reprezentate în COSC, DNSC, ADR	DNSC	Permanent	Pentru această acțiune legiuitorul a desemnat participanții, dar nu a precizat care sunt destinatarii (publicul-țintă) pentru „*furnizarea de sprijin și consultanță*”. Pe cale de consecință, oricare entitate interesată în asigurarea propriei securități și reziliențe cibernetice, va putea solicita sprijin și consultanță în acest scop, cel puțin de la nivelul DNSC.
1.3.b.	Finalizarea demersurilor de includere în nomenclatorul COR a ocupaţiilor specifice domeniului securităţii cibernetice	DNSC, MMSS, SRI, entităţi din mediul privat şi **academic**	DNSC, MMSS	Semestrul II, 2022	Este posibil ca includerea în nomenclatorul COR a ocupațiilor specifice domeniului securității cibernetice să fie precedată de o consultare în acest scop a mediului academic din partea instituțiilor participante la această acțiune. După finele sem. al II-lea / 2022, așteptându-ne la actualizarea adecvată a nomenclatorului COR cu ocupațiile specifice domeniului securității cibernetice, fiecare dintre entitățile vizate va putea să procedeze la: - actualizarea statelor de funcții, pentru evidențierea posturilor ce vor trebui ocupate cu persoane calificate pentru domeniul securității cibernetice; - actualizarea fișelor posturilor în cauză.
1.3.c.	Dezvoltarea profilurilor de competenţe comune de securitate și apărare	Instituţii reprezentate în COSC, DNSC	DNSC	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”.

	cibernetică bazate pe bune practici și certificate folosite la nivelul UE şi NATO				Cel mai probabil, în derularea acestei acțiuni va trebui, mai întâi, să se definească sintagma „**profiluri de competențe comune de securitate și apărare cibernetică**”, iar apoi să se definească / stabilească direcțiile / componentele de dezvoltare a acestor profiluri. Totuși, nu rezultă cum vor influența profilurile sus-menționate aplicarea / îndeplinirea celorlalte măsuri / acțiuni. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
1.3.d.	Dezvoltarea unor formate de pregătire a palierului managerial din cadrul autorităţilor și instituţiilor administraţiei publice și entităţilor private, în vederea alocării eficiente și complementare a resurselor necesare	Instituţiile reprezentate în COSC, DNSC, entităţi din mediul privat și **academic**	DNSC	Semestrul II, 2023	Această acțiune are în vedere conștientizarea managerilor entităților vizate în legătură cu importanța alocării resurselor necesare asigurării unui nivel adecvat de securitate cibernetică. Este posibil ca DNSC să consulte entitățile din mediul academic în legătură cu conținutul „***formatelor de pregătire a palierului managerial***”. <u>Recomandare</u>: În situația în care DNSC va solicita ASE din București să își aducă contribuția la conținutul formatelor de pregătire a palierului managerial pentru alocarea resurselor necesare asigurării unui nivel adecvat de securitate cibernetică, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
1.3.e.	Coordonarea și prioritizarea alocărilor bugetare pentru componenta de securitate cibernetică din fonduri europene (POCIDIF, POEO), PNRR, fonduri alocate din	SGG, ADR, MCID	SGG	Permanent	Această acțiune este foarte relevantă pentru toate instituțiile finanțate de la bugetul de stat. În măsura în care Ministerul Educației va aprecia că poate aloca fonduri bugetare pentru securitatea cibernetică a universităților aflate în coordonarea sa, această acțiune va deveni relevantă inclusiv pentru ASE din București.

	Programul Europa Digitală, hub-urilor de inovare digitală				

1.4 Consolidarea mecanismului de raportare a incidentelor de securitate cibernetică

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
1.4.a.	Realizarea unui sistem de management centralizat al incidentelor de securitate cibernetică înregistrate la nivel naţional	DNSC, autorităţi şi instituţii ale administraţiei publice şi entităţi private care au în administrare şi operare reţele şi sisteme informatice	DNSC	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Folosirea sintagmei „sistem de mangement centralizat” induce ideea de ținere a evidenței incidentelor de securitate cibernetică, în vedere constituirii unei baze de cunoștințe asupra acestor evenimente. Este posibil ca ASE din București să fie consultată de către DNSC asupra detaliilor relevante ale atacului cibernetic pe care l-a suferit în 02.10.2020.

1.5 Crearea unor mecanisme de certificare, conformitate și standardizare în domeniul securității cibernetice

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
1.5.a.	Crearea unui set clar de criterii tehnice şi non-tehnice de verificare, inclusiv prin raportare la aspecte ce ţin de securitate naţională	Instituţii reprezentate în COSC, DNSC	DNSC	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, în definirea și adoptarea respectivelor criterii tehnice și non-tehnice de verificare, inclusiv prin raportare la aspecte ce țin de securitatea națională, nu se întrevede necesitatea de implicare a entităților din mediul academic.

1.5.b.	Elaborarea și implementarea proiectelor legislative în domeniul tehnologiilor inovative cu impact în domeniul securității cibernetice	Instituţii reprezentate în COSC, ANCOM, DNSC	-	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, nu se întrevede modalitatea de implicare a entităților din mediul academic în stabilirea și promovarea inițiativelor legislative.
1.5.c.	Desemnarea şi/sau autorizarea entităţilor de evaluare și certificare a produselor și tehnologiilor de securitate cibernetică	DNSC, SRI	-	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Desemnarea și/sau autorizarea entităților de evaluare și certificare a produselor și tehnologiilor de securitate cibernetică este de natură să conducă la situația în care nu vor mai putea fi achiziționate decât produse / tehnologii certificate de către aceste entități.

1.6 Securizarea lanţului de aprovizionare

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
1.6.a.	Elaborarea şi promovarea cadrului de reglementare privind securizarea lanţului de aprovizionare în domeniul produselor și serviciilor de securitate cibernetică	Instituţii reprezentate în COSC, ANCOM, DNSC	SGG	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe de altă parte, în cuprinsul Strategiei, la paragraful 4.1.6., se regăsește sintagma: „*Este necesară definirea criteriilor de încredere pentru furnizorii de echipamente hardware, software şi servicii, în special pentru sistemele ce ţin de securitatea naţională.*” Astfel, se deduce că reglementarea privind securizarea lanțului de aprovizionare este necesară în principal pentru instituțiile din SNAOPSN.

					Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

Obiectivul 2 – Cadru normativ și instituțional consolidat
Măsuri

2.1 Consolidarea cadrului normativ

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
2.1.a.	Introducerea proiectului *Legii privind Securitatea şi Apărarea Cibernetică* în propunerile de iniţiativă legislativă ale Ministerului Apărării Naţionale	MApN	MApN	Semestrul II, 2022	Introducerea de către MApN în cursul sem. al II-lea / 2022 a acestui proiect de lege pe agenda de lucru a Parlamentului României nu este de natură să permită estimarea datei la care actul normativ va fi adoptat și promulgat. După publicarea în Monitorul Oficial al României a legii respective, entitățile din mediul academic vor putea stabili măsura în care prevederile acestei legi sunt aplicabile inclusiv în mediul academic.
2.1.b.	Evaluarea și actualizarea periodică a cadrului legislativ în domeniul securităţii şi apărării cibernetice, raportat la evoluţia ameninţării și la progresul tehnologic	Instituţii reprezentate în COSC, DNSC, ANCOM, ADR	COSC	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. De altfel, actualizarea cadrului legislativ este legal posibilă numai pentru instituțiile abilitate să promoveze inițiative legislative.

2.2 Consolidarea cadrului instituţional

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
2.2.a.	Consolidarea rolului şi responsabilităţilor COSC, în conformitate cu prevederile *Legii privind Securitatea şi Apărarea Cibernetică*	COSC	COSC	Semestrul II, 2022, se continuă permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Totodată, este relevant de menționat că, în cuprinsul Strategiei, la paragraful 4.2.2., se stipulează următoarele: „*Consiliul Operativ de Securitate Cibernetică (COSC) rămâne mecanismul de cooperare inter-instituţională, care coordonează unitar, la nivel operaţional, activităţile SNSC. Activităţile, componenţa şi responsabilităţile COSC trebuie stabilite în cadrul Legii privind Securitatea şi Apărarea Cibernetică.* *De la înfiinţarea sa, COSC a avut un rol esenţial în susţinerea unor demersuri în domeniul securităţii cibernetice cu impact atât la nivel naţional, cât şi internaţional. COSC trebuie să rămână formatul în care să fie actualizate constant priorităţile, în funcţie de rezultatele obţinute anterior, şi adoptate deciziile care să fie transpuse ulterior în măsuri concrete de nivel procedural, operaţional, tactic şi strategic.* *În urma analizei şi evaluării stării de securitate cibernetică la nivel naţional, COSC trebuie să adopte decizii, transpuse în propuneri înaintate Consiliului Suprem de Apărare a Ţării (CSAT), privind nivelurile de alertă cibernetică naţionale, planuri şi direcţii de acţiune, dezvoltare şi investiţii, precum şi linii de mandat referitoare la decizii şi documente de politică externă în domeniul securităţii cibernetice.* *În acest sens, pentru o coordonare optimă între deciziile adoptate şi măsurile identificate şi o impulsionarea implementării acestora, este necesar ca activitatea COSC să fie organizată după un calendar prestabilit.*” Notă: CNSC = Consiliul Național de Securitate Cibernetică

Obiectivul 3 – Parteneriat public-privat pragmatic
Măsuri

3.1 Derularea unor programe de conştientizare publică şi de creştere a nivelului de cultură de securitate cibernetică

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
3.1.a.	Derularea unor campanii de conştientizare şi de informare prin programe media, broşuri, website-uri dedicate, ghiduri de bune practici	Instituţii reprezentate în COSC, DNSC și entităţi din mediul privat şi **academic**	DNSC, SRI	Permanent	Recomandare: În situația în care DNSC și/sau SRI vor solicita ASE din București să își aducă contribuția la derularea acestor campanii de conștientizare și de informare prin programe media, broşuri, website-uri dedicate, ghiduri de bune practici, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
3.1.b.	Derularea unor activităţi care să vizeze conştientizarea palierului managerial din cadrul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private cu privire la necesitatea asigurării securităţii cibernetice	Instituţii reprezentate în COSC, DNSC și entităţi din mediul privat şi **academic**	DNSC, SRI	Permanent	Această acțiune are în vedere conștientizarea managerilor entităților vizate în legătură cu importanța alocării resurselor necesare asigurării unui nivel adecvat de securitate cibernetică. **Obs.** Acțiunea este asemănătoare cu cea detaliată la punctul 1.3.d. Recomandare: În situația în care DNSC și/sau SRI vor solicita ASE din București să își aducă contribuția la derularea unor activități care să vizeze conştientizarea palierului managerial din cadrul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private cu privire la necesitatea asigurării securităţii cibernetice, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
3.1.c.	Organizare de evenimente cu experţi în domeniul securităţii cibernetice	Autorități și instituții ale administrației publice,	-	Permanent	Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a lua în considerare necesitatea și

		entități din mediul privat și **academic**			oportunitatea organizării de evenimente cu experți în domeniul securității cibernetice.
3.1.d.	Realizarea unor demersuri privind introducerea unor noţiuni de igienă în spaţiul cibernetic la nivel preuniversitar.	ME, DNSC, SRI, entităţi din mediul privat și **academic**	DNSC	Permanent	Conform Strategiei, se definește sintagma: ***Igienă în spaţiul cibernetic*** – aplicarea unui set de practici şi deprinderi în materie de securitate cibernetică, necesare pentru desfăşurarea în siguranţă a activităţilor zilnice întreprinse de utilizatori; Recomandare: În situația în care Ministerul Educației (ME) va solicita ASE din București să își aducă contribuția la conținutul acestor demersuri, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.

3.2 Dezvoltarea de programe educaţionale în domeniul securităţii cibernetice

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
3.2.a.	Dezvoltarea şi implementarea programelor de studii de securitate cibernetică la nivel preuniversitar, universitar şi postuniversitar	ME, DNSC, SRI, MApN, entităţi din mediul privat și **academic**	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității includerii unor programe de studii de securitate cibernetică în cadrul programelor educaționale acreditate pe care deja le derulează.
3.2.b.	Susţinerea integrării pe piaţa muncii a studenţilor şi absolvenţilor programelor de studii în domeniul securităţii cibernetice, inclusiv prin realizarea unor stagii de practică în cadrul unor autorităţi şi instituţii ale	MMSS, ME, instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	DNSC	Permanent	În situația în care ASE din București va opta pentru lărgirea ofertei sale educaționale prin includerea de programe de studii de securitate cibernetică, în mod evident, se va implica în organizarea stagiilor de practică obligatorii pentru studenții săi.

	administraţiei publice sau entităţi private din domeniu				
3.2.c.	Realizarea demersurilor necesare susţinerii financiare şi materiale a programelor educaţionale în domeniul securităţii cibernetice, inclusiv prin accesarea de finanţare externă şi maximizarea cooperării cu mediul privat	ME, MIPE, MApN, SRI, SPP, DNSC, entităţi din mediul privat şi **academic**	ME, DNSC	Permanent	În situația în care ASE din București va opta pentru lărgirea ofertei sale educaționale prin includerea de programe de studii de securitate cibernetică, în mod evident, se va implica în demersuri de accesare a finanțării din fonduri externe (europene) a unor proiecte corelate cu derularea respectivelor programe de studii.
3.2.d.	Derularea unor activităţi de pregătire şi instruire a cadrelor didactice, inclusiv prin maximizarea cooperării cu mediul privat	ME, MApN, SRI, DNSC, entităţi din mediul privat şi **academic**	ME, DNSC	Permanent	În situația în care ASE din București va opta pentru lărgirea ofertei sale educaționale prin includerea de programe de studii de securitate cibernetică, în mod evident, se va implica în activități pentru pregătirea personalului didactic alocat acestor programe.

3.3 Derularea unor programe de formare profesională pentru cei care desfăşoară activităţi în domeniul securităţii cibernetice

Nr. crt.	**Principalele acțiuni**	**Participanți**	**Respon-sabil**	**Termen**	**Implicațiile asupra mediului academic**
0	**1**	**2**	**3**	**4**	**5**
3.3.a.	Organizarea de cursuri de specializare în domeniul securităţii cibernetice adresate diferitelor categorii profesionale	Instituţii reprezentate în COSC, DNSC, MMSS, entităţi din mediul privat şi **academic**	DNSC	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității includerii unor cursuri de specializare (postuniversitare) în domeniul securității cibernetice în cadrul programelor educaționale acreditate pe care deja le derulează.
3.3.b.	Dezvoltarea de centre de instruire pentru cei care desfăşoară activităţi în	Instituţii reprezentate în	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a se implica (în colaborare sau nu cu alte instituții) pentru dezvoltarea de centre de

	domeniul securităţii cibernetice	COSC, DNSC, entităţi din mediul privat şi **academic**			instruire pentru cei care desfăşoară activităţi în domeniul securităţii cibernetice.

3.4 Dezvoltarea şi consolidarea cercetării şi inovării în domeniul securităţii cibernetice

Nr. crt.	**Principalele acțiuni**	**Participanți**	**Respon-sabil**	**Termen**	**Implicațiile asupra mediului academic**
0	**1**	**2**	**3**	**4**	**5**
3.4.a.	Dezvoltarea de parteneriate public-private în domeniul cercetării şi inovării	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a se implica în dezvoltarea de parteneriate public-private în domeniul cercetării şi inovării în domeniul securităţii cibernetice.
3.4.b.	Dezvoltarea unui program naţional privind implicarea actorilor eligibili la nivel naţional în programe de cercetare şi inovare de la nivel regional, european şi internaţional	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	MCID	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a participa în cadrul unui program naţional privind implicarea actorilor eligibili la nivel naţional în programe de cercetare şi inovare în domeniul securităţii cibernetice, derulate la nivel regional, european şi internaţional.
3.4.c	Capitalizarea prezenţei în România a *Centrului de competențe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică*	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a coopera cu *Centrul de competențe european industrial, tehnologic şi de cercetare în materie de securitate cibernetică*.
3.4.d.	Crearea unor mecanisme instituţionale pentru consultanţă şi susţinere	Instituţii reprezentate în COSC, MIPE,	MCID	Semestrul II, 2023	Recomandare: În situația în care Ministerul Cercetării, Inovării și Digitalizării (MCID) va solicita ASE din București să își aducă contribuția la

	financiară a activităţilor de cercetare şi inovare din domeniul securităţii cibernetice	MF, DNSC, ADR, entităţi din mediul privat şi **academic**			demersurile pentru crearea unor mecanisme instituţionale pentru consultanţă şi susţinere financiară a activităţilor de cercetare şi inovare din domeniul securităţii cibernetice, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.

3.5 Dezvoltarea industriei naţionale de securitate cibernetică

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
3.5.a.	Impulsionarea, prin oferirea de consultanţă şi susţinere financiară, iniţiativelor de dezvoltare a incubatoarelor de afaceri şi *start-up-urilor* în domeniul securității cibernetice	Instituţii reprezentate în COSC, MAT, MEc, MF, MIPE, DNSC, ADR, entităţi din mediul privat şi **academic**	MAT, MEc	Permanent	Recomandare: În situația în care Ministerul Antreprenoriatului și Turismului (MAT) și / sau Ministerul Economiei (MEc) vor solicita ASE din București să își aducă contribuția la demersurile pentru Impulsionarea, prin oferirea de consultanţă şi susţinere financiară, iniţiativelor de dezvoltare a incubatoarelor de afaceri şi *start-up-urilor* în domeniul securității cibernetice, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
3.5.b.	Implementarea unor mecanisme pentru motivarea, retenţia şi atragerea în ţară a experţilor în domeniul securităţii cibernetice	Instituţii reprezentate în COSC, MAT, MEc, MF, DNSC	MAT, MEc, DNSC	Semestrul II, 2023, se continuă permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „entități din mediul academic”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
3.5.c.	Implementarea unor mecanisme de atragere în România a unor companii private din domeniul securităţii cibernetice	Instituţii reprezentate în COSC, MAT, MEc, MF, DNSC	DNSC	Semestrul II, 2023, se continuă permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „entități din mediul academic”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

Obiectivul 4 - Reziliență prin abordare proactivă şi descurajare

Măsuri

4.1 Dezvoltarea de CERT-uri şi SOC-uri sectoriale

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
4.1.a.	Identificarea sectoarelor de activitate în care este necesară constituirea structurilor de tip CERT sau SOC	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	DNSC	Semestrul II, 2022, se continuă permanent	Conform Strategiei, se definește sintagmele: CERT = Echipă de răspuns la incidente de securitate cibernetică SOC = Centru Operaţional de Securitate Este posibil ca ASE din București să fie consultată de către DNSC asupra oportunității de constituire a structurilor de tip CERT sau SOC la nivelul entităților din mediul academic. Considerăm că la nivelul fiecărei universități se justifică înființarea unei echipe de răspuns la incidente de securitate cibernetică (CERT). Apreciem că înființarea de Centre Operaționale de Securitate (SOC) se justifică la nivelul instituțiilor administrației publice centrale, precum și la nivelul entităților publice sau private care gestionează infrastructuri critice.
4.1.b.	Derularea unor campanii de conştientizare a factorilor de decizie de la nivelul autorităţilor şi instituţiilor administraţiei publice şi entităţilor private cu privire la avantajele şi necesitatea constituirii unor echipe de tip CERT şi SOC sectoriale	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	DNSC	Permanent	Această acțiune are în vedere conștientizarea factorilor de decizie din instituțiile publice și din mediul privat asupra avantajelor şi necesității de constituire a unor echipe de tip CERT şi SOC sectoriale. <u>Recomandare</u>: În situația în care DNSC va solicita ASE din București să își aducă contribuția la derularea unor astfel de campanii de conștientizare, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.

4.1.c.	Furnizarea de sprijin şi consultanţă în vederea constituirii unor echipe de tip CERT şi SOC sectoriale	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	DNSC	Permanent	Pentru această acțiune legiuitorul a desemnat participanții, dar nu a precizat care sunt destinatarii (publicul-țintă) pentru „*furnizarea de sprijin și consultanță*”. Pe cale de consecință, oricare entitate interesată în stabilirea oportunității privind constituirea la nivelul său a unei echipe sectoriale de tip CERT și/sau SOC, va putea solicita sprijin și consultanță în acest scop, cel puțin de la nivelul DNSC.
4.1.d.	Crearea unor formate și mecanisme de cooperare între structurile de tip CERT/SOC sectorial, inclusiv între cele din SNAOPSN	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	DNSC	Semestrul II, 2022, se continuă permanent	Recomandare: În situația în care DNSC va solicita ASE din București să își aducă contribuția la acțiunea de creare a unor formate și mecanisme de cooperare între structurile de tip CERT/SOC sectoriale, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.

4.2 Derularea de exerciţii cu aplicabilitate practică ridicată

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
4.2.a.	Cooperare la nivel naţional în vederea organizării şi participării la exerciţii cu aplicabilitate practică ridicată în domeniul securităţii cibernetice	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a coopera cu alte instituții pentru organizarea și participarea la exerciții cu aplicabilitate practică în domeniul securității cibernetice. Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a decide unilateral asupra cooperării cu alte instituții pentru organizarea și participarea la exerciții cu aplicabilitate practică în domeniul securității cibernetice.
4.2.b.	Organizarea şi participarea la exerciţii naţionale cu	Instituţii reprezentate în	SRI, DNSC	Permanent	Recomandare:

	aplicabilitate practică ridicată, în domeniul securităţii cibernetice	COSC, DNSC, entităţi din mediul privat şi **academic**			În situația în care SRI și/sau DNSC vor solicita ASE din București să co-organizeze și să participe la exerciţii naţionale cu aplicabilitate practică ridicată în domeniul securităţii cibernetice, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
4.2.c.	Participarea la exerciţii internaţionale cu aplicabilitate practică ridicată, în domeniul securităţii cibernetice	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	-	Permanent	Fiind o entitate din mediul academic, ASE din București va trebui să analizeze și să decidă asupra oportunității de a participa la exerciții internaționale cu aplicabilitate practică ridicată în domeniul securității cibernetice. Faptul că la nivel național nu este desemnată nicio instituție ca având responsabilitatea unică fie și numai pentru verificarea îndeplinirii acestei acțiuni conduce la concluzia că fiecare dintre entitățile vizate are obligația de a decide unilateral asupra implicării sale în participarea la exerciții internaționale cu aplicabilitate practică ridicată în domeniul securității cibernetice.
4.2.d.	Organizarea de exerciţii civil-militare de pregătire şi integrare coerentă a procedurilor specifice de răspuns la incidentele de securitate cibernetică ce afectează infrastructuri esenţiale	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**	MApN	Permanent	Recomandare: În situația în care MApN va solicita ASE din București să își aducă contribuția la acțiunea de organizare de exerciţii civil-militare de pregătire şi integrare coerentă a procedurilor specifice de răspuns la incidentele de securitate cibernetică ce afectează infrastructuri esenţiale, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.

Obiectivul 5 – România – actor relevant în arhitectura internațională de cooperare
Măsuri

5.1 Consolidarea rolului României la nivel global

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
5.1.a.	Promovarea la nivel global a modului de implementare la nivel naţional a cadrului ONU de comportament responsabil statal în spaţiul cibernetic (normele de comportament, aplicarea dreptului internaţional în spaţiul cibernetic, măsurile de creştere a încrederii între state şi a capacităţii acestora)	Instituţii reprezentate în COSC, AP, DNSC, SGG, ADR, ANCOM, entități din mediul privat	DNSC, MAE	Permanent	Referirea la entitățile private poate include și entitățile din mediul academic; cel puțin universitățile particulare acreditate ar intra în această categorie. În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.1.b.	Participarea activă la consultări şi iniţiative internaţionale, guvernamentale, a actorilor relevanţi din mediul public, privat şi **academic**, precum şi din cadrul societăţii civile	Instituţii reprezentate în COSC, DNSC, entităţi din mediul privat şi **academic**, societatea civilă	MAE	Permanent	Recomandare: În situația în care MAE va solicita ASE din București să își aducă contribuția la acțiuni de consultări şi iniţiative internaţionale, guvernamentale, a actorilor relevanţi din mediul public, privat şi academic, precum şi din cadrul societăţii civile, universitatea va fi în măsură să stabilească oportunitatea implicării sale în aceste acțiuni.
5.1.c.	Crearea unor mecanisme interinstituţionale care să permită definirea unor poziţii şi strategii naţionale privind subiectele de actualitate în	Instituţii reprezentate în COSC, AP, DNSC, ANCOM, ADR	-	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

	domeniul securităţii cibernetice				
5.1.d.	Dezvoltarea și organizarea unui eveniment, de anvergură internaţională, recunoscut ca punct de referinţă în domeniul securităţii cibernetice	Instituţii reprezentate în COSC, AP, SGG, DNSC, ANCOM, ADR, entităţi din mediul privat și **academic**	SGG	Semestrul II, 2023, se continuă anual	Recomandare: În situația în care SGG va solicita ASE din București să își aducă contribuția la dezvoltarea și organizarea unui eveniment anual, de anvergură internaţională, recunoscut ca punct de referinţă în domeniul securităţii cibernetice, universitatea va fi în măsură să stabilească oportunitatea implicării sale în această acțiune.
5.1.e.	Dezvoltarea unei abordări naţionale privind promovarea candidaturilor şi obţinerea de poziţii relevante în cadrul organismelor internaţionale cu relevanţă în domeniul securităţii cibernetice	Instituţii reprezentate în COSC, AP, SGG, DNSC, ANCOM, ADR	-	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

5.2 Consolidarea rolului României la nivel regional și pe plan bilateral

Nr. crt.	**Principalele acțiuni**	**Participanți**	**Respon-sabil**	**Termen**	**Implicațiile asupra mediului academic**
0	**1**	**2**	**3**	**4**	**5**
5.2.a.	Participarea activă a României în formate de cooperare și în cadrul organizaţiilor regionale	Instituţii reprezentate în COSC, DNSC, ADR, ANCOM	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.2.b.	Consolidarea relaţiilor de cooperare cu state aliate,	Instituţii reprezentate	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”.

	partenere, "like-minded" în vederea asigurării securităţii cibernetice	în COSC, DNSC, ADR, ANCOM, ADR			Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.2.c.	Implementarea măsurilor prevăzute în *EU Cyber Diplomacy Toolbox*	Instituţii reprezentate în COSC, DNSC	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.2.d.	Implicarea activă a României în operaţionalizarea măsurilor de creştere a încrederii între state ("Confidence Building Measures"/ CBMs) la nivel OSCE	Instituţii reprezentate în COSC, DNSC	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.2.e.	Dezvoltarea în continuare a politicii de apărare cibernetică a NATO, inclusiv consolidarea rezilienţei NATO în întregime şi a aliaţilor, a capabilităţilor cibernetice de descurajare şi apărare	SRI, MApN şi MAE	MApN, MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.2.f.	Ralierea la iniţiative de tip condamnare publică ("blame and shame") conform cadrului procedural naţional în caz de atribuire a unui atac cibernetic	Instituţii reprezentate în COSC, AP, DNSC	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

5.3 Consolidarea rolului diplomaţiei cibernetice

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	1	2	3	4	5
5.3.a.	Crearea unei poziţii de reprezentare diplomatică de nivel înalt – Ambasador / Reprezentant cu însărcinări speciale	MAE	MAE	Semestrul II, 2023	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.3.b.	Asigurarea sprijinului pentru o reprezentare adecvată a României la nivel internaţional şi pentru un mesaj coerent în consolidarea unei diplomaţii cibernetice eficiente	Instituţii reprezentate în COSC, AP, ANCOM, ADR, DNSC	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.
5.3.c.	Consolidarea capacităţii de acţiune în domeniul politicilor de securitate cibernetică la nivelul centralei MAE, al misiunilor diplomatice ale României în capitalele statelor partenere și al reprezentanţelor permanente la nivelul UE, NATO şi ONU.	MAE, MApN, SRI, SIE, DNSC	MAE	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.

5.4 Consolidarea capacităţii de transfer de expertiză la nivel regional

Nr. crt.	Principalele acțiuni	Participanți	Respon-sabil	Termen	Implicațiile asupra mediului academic
0	**1**	**2**	**3**	**4**	**5**
5.4.a.	Demararea unor proiecte cu impact regional pentru asigurarea transferului de cunoştinţe şi expertiză către statele din regiune	Instituţii reprezentate în COSC, DNSC	-	Permanent	În referire la participanții la această acțiune, legiuitorul nu a inclus sintagma „**entități din mediul academic**”. Pe cale de consecință, pentru această acțiune nu este obligatoriu să considerăm că ASE din București ar trebui să se implice, cel puțin nu într-o primă instanță.