B.1. Propunerea de proiect (max. 10 pagini în limba română)

1. Titlul, cu indicarea domeniului științific din lista de la secțiunea VI

Cyber Diplomacy ca Instrument de Guvernanță in Societatea Digitala

25. Dezvoltarea digitală a societății

2. Cuvinte cheie: cyber diplomacy, digitalizare, reziliență, relații internaționale, guvernanță, non-proliferare

3. Obiective, cu indicarea importanței acestora.

Tehnologia și spațiul cibernetic au evoluat exponențial în ultimii ani, oferind o multitudine de beneficii precum accesul la informație sau instrumente pentru dezvoltarea domeniilor esențiale. Cibernetica a devenit o problemă transversală care afectează toate domeniile, atât în interiorul, cât și în afara granițelor fiecărei țări individuale și a jurisdicției autorităților sale legitime și competente. Din acest motiv, cooperarea devine esențială pentru a adresa noile provocări, precum amenințări accidentale și deliberate, riscuri sistemice și adoptarea sustenabilă a noilor tehnologii. Diplomația cibernetică este un domeniu emergent care caută să promoveze cooperarea și coordonarea între țări și alte entități pentru guvernanța spațiului cibernetic și a domeniilor interdependente.

Gheorghe et al (2018) au descris problematica infrastructurilor critice, a activelor cheie și resurselor cheie a căror producție de bunuri și servicii critice este vitală pentru buna funcționare a societăților noastre. Aceste infrastructuri critice, care includ sisteme variate, de la termocentrale, la piețe financiare și administrație publică, au inclusiv dimensiuni transnaționale și sunt din ce în ce mai interconectate cibernetic prin sisteme TIC (tehnologia informațiilor și comunicațiilor). Prin digitalizare și interconectare, spațiul cibernetic devine un suprastrat de comandă, control, coordonare și comunicare pentru aceste infrastructuri (Georgescu et al, 2020). Digitalizarea și interconectarea sunt două procese care decurg extrem de rapid, asistate de noi tehnologii și paradigme precum ubicuitatea Internetului, Internet-of-Things, rețele 5G, high-performance computing, Big Data etc.

Pe lângă noile capabilități și eficiențe generate de aceste două fenomene, avem și noi riscuri, vulnerabilități și amenințări care decurg din interdependențe cibernetice, care li se alătură celor fizice, geografice, logice și informaționale (subsumate de cele cibernetice) ca vectori de propagare a riscurilor și întreruperilor de funcționare (Pescaroli și Alexander, 2016). Fenomenul globalizării și digitalizării a internaționalizat aceste sisteme, generând nevoia de guvernanță globală.

Problema coordonării între actorii suverani este crucială și poate fi abordată doar prin diplomație, cu excepția reglementărilor supranaționale precum cea prevăzută de UE. Chiar și atunci, adoptarea și implementarea sunt obiectul unei interacțiuni continue, încurajare și stimulare. Problema TIC, așa cum au subliniat Bauer & van Eeten (2009), este că un sistem TIC descentralizat, indiferent dacă îl privim din punct de vedere jurisdicțional sau economic, va genera riscuri semnificative din cauza externalităților produse de deciziile de securitate din partea părților interesate. Problema "deciziilor de securitate care nu reflectă în mod corespunzător beneficiile și costurile sociale" poate fi rezolvată doar prin reglementare, fie a activității, fie a stimulentelor părților interesate. Deși au fost propuse alte modele, există încă un spectru de externalități care nu poate fi abordat doar prin acțiune privată. Dar, dată fiind globalizarea, această reglementare nu se poate opri la granițe, deoarece țările se plâng deja că standardele de securitate mai scăzute ale altor țări le afectează propria securitate. Diplomația este cea care poate ajuta la eliminarea acestei diviziuni.

Diplomația cibernetică este un instrument cu potențialul de a facilita transformarea guvernanței globale pentru a asigura stabilitate, reziliență și previzibilitate, minimizând elemente perturbatoare, atât deliberate cât și accidentale. Necesitatea diplomației cibernetice reiese ca urmare a mai multor

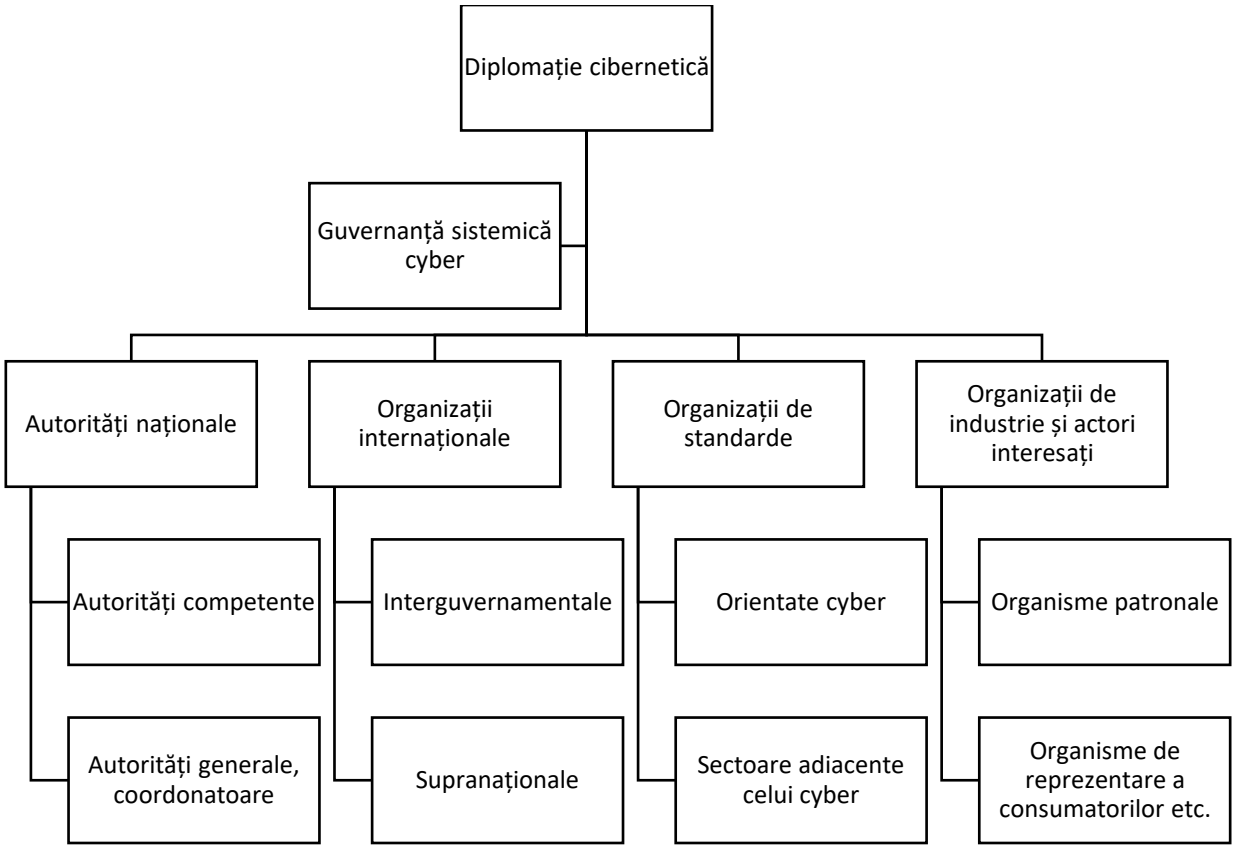
factori: administrarea problemelor transfrontaliere rezultate din digitalizare vieții sociale, economice și politice a societăților; paradigma războiului cibernetic și proliferarea armelor și atacatorilor cibernetici, mai ales pentru competiții inter-statale; amenințarea războiului hibrid și asimetric cibernetic, inclusiv la adresa infrastructurilor critice civile (energie, administrație publică); protecția împotriva criminalității transfrontaliere perturbatoare, administrarea rețelelor, tehnologiilor, infrastructurilor, standardelor, regulamentelor și conduitei globale în domeniul cibernetic; managementul problemelor colective noi sau încă nedescoperite, cum ar fi cele legate de implementarea noilor tehnologii digitale (blockchain, inteligență artificială, 5G).

Practic, diplomația cibernetică devine un contribuitor la guvernanța cibernetică globală și la guvernanța sistemică globală facilitată și amenințată de digitalizare.

Propunerea de față vizează studierea diplomației cibernetice care este, în acest moment, o practică emergentă, pentru a dezvolta un cadru comprehensiv al domeniului care să asiste atât la cercetări viitoare cât și la dezvoltarea instrumentelor sale. Prin intermediul unui studiu al literaturii de specialitate în domeniu, vor fi dezvoltate o serie de aporturi originale la diplomația cibernetică, printr-o analiză pe bază de chestionar a opiniilor practicanților de diplomație cibernetică și prin elaborarea unor documente de referință – profilul diplomatului cibernetic, analiza a două subdomenii a diplomației cibernetice.

Cadrul diplomației cibernetice se referă la principii, practici, perspective și abordări. Diferența față de alte domenii ale diplomației este dată de natura inter-disciplinară și multi-disciplinară a domeniului, ținând cont de necesitate cunoștințelor specifice din domeniul TIC și din domenii conexe, dar și de varietatea actorilor implicați. Parafrazând pe Slaughter (2004), care vorbea despre reglementatori în general, diplomații trebuie să capete expertiză cibernetică, iar experții cibernetici trebuie să se diplomatizeze pentru a acționa într-un cadru contextual și organizațional foarte larg, implicând nu doar ambasade și sedii ale organizațiilor transnaționale de tip UE și ONU, a alianțelor (NATO), dar și organizații de standardizare (International Standards Organization, organizațiile europene ESO, CEN, CENELEC, ETSI), organizații de luptă împotriva criminalității, organizații de guvernanță generală (Uniunea Internațională a Telecomunicațiilor, Internet Engineering Task Force) și multe altele. Conform Slaughter (2004), "reglementatorii sunt, într-adevăr, noii diplomați – în prima linie a problemelor care erau, odinioară, domeniul exclusiv al politicilor interne, dar care acum nu mai pot fi rezolvate doar de autoritățile naționale acționând individual. Noii reglementatori trebuie adesea să lucreze îndeaproape cu 'vechii diplomați', membrii bine pregătiți ai corpului diplomatic care trebuie să abordeze probleme delicate. Dar lumea în care ambasadorii își prezentau unii altora punctele de vedere pe o selecție limitată de probleme economice și de Securitate a dispărut" (Slaughter, 2004, p. 64).

Figura de mai jos reunește principalele elemente ale cadrului de diplomație cibernetică, care poate rezulta în acorduri de cooperare, standarde, proceduri, norme, cutume, regulamente, atât voluntare, cât și obligatorii



Guvernanța sistemică este o obligație inevitabilă din partea guvernelor și a altor părți interesate în era globalizării și digitalizării. Au fost create sisteme digitale performante pe care societatea se bazează pentru securitate, creștere economică și procese socio-politice. Sfera de aplicare a guvernării sistemice depășește jurisdicțiile naționale și, prin urmare, trebuie să implice nenumărate forme de cooperare între statele suverane. Diplomația cibernetică este o parte importantă a procesului, întrucât cibernetica este domeniul/sectorul transversal care leagă majoritatea statelor, atât din punct de vedere funcțional, cât și din punct de vedere al apariției și transmiterii riscurilor, vulnerabilităților și amenințărilor. În cele din urmă, guvernanța sistemică este imposibilă fără cibernetică, dar cibernetica durabilă va fi imposibilă fără guvernanța sistemică în domeniul său, fie că are loc prin sprijinul organizației de stabilire a standardelor cooperative sau competitive, negocieri directe între guverne sau cooperare supranațională.

Diplomația cibernetică nu este doar o realitate la nivelul Uniunii Europene, prin Cyber Toolbox și numeroase exemple de cooperare și consultare cu terți în domeniul digital, dar și la nivel României, care a acordat asistență de specialitate Ucrainei pentru îmbunătățirea securității sale cibernetice și care trebuie, mai ales, să formuleze și să implementeze o agendă de cooperare digitală cu partenerii săi care să servească intereselor naționale. Găzduirea de către România a Centrului European pentru Competențe Cibernetice este rezultatul diplomației cibernetice românești, la fel ca și prezența României în eforturile de asigurare a securității cibernetice colective la nivelul NATO și în rândul rețelelor de schimb de informații, inclusiv cibernetic, stabilite la nivel european și transatlantic.

Lista obiectivelor proiectului evidențiază subliniază contribuțiile clare care pot fi aduse la cercetarea diplomației cibernetice:

O1. Realizarea unui studiu al literaturii de specialitate, rezultând o metodologie de cercetare pentru eforturi viitoare în domeniu.

O2. Realizarea unui chestionar de specialitate adresat diplomaților și experților și factorilor de decizie în securitate cibernetică prin care să fie evaluat statutul actual al diplomației cibernetice și trendurile de dezvoltare
O3. Realizarea unui profil al diplomatului cibernetic, cuprinzând recomandări legate de pregătirea sa, poziționarea în cadrul organizației și organizarea eforturilor de diplomație cibernetică.
O4. Realizarea a două analize de subdomenii pentru diplomația cibernetică, în domeniul energiei și cel al protecției infrastructurilor critice.

4. Metodologie, cu indicarea gradului de originalitate
WP 1 – activități de management

- Activitatea 1.1 – coordonarea și managementul proiectului – activitățile legate de managementul proiectului așa cum sunt asumate în propunerea de proiect: gestionarea și controlul resurselor, termenelor și activităților proiectului

Managementul de proiect va fi foarte important pentru succesul în atingerea obiectivelor, pentru că directorul de proiect nu trebuie doar să coordoneze o muncă inter- și multidisciplinară în explorarea unui domeniu nou, ci va trebui să și interacționeze cu diplomați, experți și instituții pentru a asigura colectarea de informații pertinente și pentru a realiza cu succes activitățile planificate în cadrul proiectului.
WP 2 – studiu teoretic
Acest pachet de lucru vizează partea de analiză teoretică a domeniului și dezvoltarea unei metodologii de cercetare care să asiste eforturile de cercetare viitoare, ținând cont de varietatea surselor de informare și analiză.

- Activitatea 2.1 – studiu de literatură în ceea ce privește conceptul de Cyber Diplomacy, cu indicarea instrumentelor de profil și a evoluțiilor semnificative din acest domeniu

Membrii echipei de proiect vor studia literatura de specialitate emergentă în domeniul diplomației cibernetice prin surse *open access*, dar vor studia și documentele primare (ex: rezoluții ale Consiliului de Securitate ONU) și rapoarte de specialitate ale organizațiilor de profil, din care putem extrage concluzii cu privire la dezvoltarea diplomației cibernetice ca fenomen în curs de derulare. Studiul va urmări formularea de principii ale diplomației cibernetice, trasarea evoluției sale în timp, definirea tehnicilor și instrumentelor de diplomație cibernetică și crearea unei taxonomii a domeniilor de aplicabilitate a sa. Cunoștințele dobândite prin această activitate vor fi suplimentate de interviuri cu diplomați de carieră și cu experți în domeniul cyber care activează în rol cvasi-diplomatic sau de guvernanță sistemică, întreprinse în cursul Activității 3.1.

- Activitatea 2.2 – investigarea Cyber Diplomacy cu aplicabilitate la Uniunea Europeană și relația cu partenerii săi principali

Diplomația cibernetică poate fi indicată drept un pilon al politicii de securitate, dezvoltare și cooperare cibernetică a Uniunii Europene. Cooperarea internațională (și între membrii UE) în domeniul cibernetic este o prezență constantă în documentele programatice și în declarațiile Uniunii Europene. Diplomația cibernetică cu SUA, cu alte mari puteri, cu țările din vecinătatea UE și cu organizații internaționale și interguvernamentale avansează pe zi ce trece și afectează o suită de domenii conexe, cum ar fi 5G, noile tehnologii digitale și alte domenii cu componentă cyber (lanțurile globale de aprovizionare, finanțe, educație, investiții etc.). Putem enumera numeroase elemente de cooperare internațională în domeniul securității cibernetice. Spre exemplu, în relația transatlantică observăm: crearea recentă a unui Consiliu UE-SUA pentru Comerț și

Tehnologie, care vizează inclusiv securitatea cibernetică și tehnologii digitale; crearea unui Cyber Defence Management Board la nivelul NATO cu rol de coordonare, cooperarea dintre NCIRC (*NATO Computer Incident Response Capability*) și CERT-EU (*Computer Emergency Response Team*), iar agenda NATO-UE menționează cyber printre șapte domenii de cooperare (și cu o pondere importantă printre cele 42 de recomandări și 32 de acțiuni concrete ale agendei NATO-UE). NATO și UE participă împreună la exerciții de securitate cu componentă cibernetică (CYBERSEC 2019, Cyber Coalition, Cyber Europe, Trident Juncture 18, Trident Jaguar 18, Coalition Warrior Interoperability Exercise 2018, Cyber Europe, Locked Shields, 2018 EU crisis management military exercise), iar cele două cooperează direct sub egida Centrului European de Excelență în Combaterea Amenințărilor Hibride (Mușetescu et al, 2022). Există un grup de lucru UE-SUA pe securitate cibernetică și crime cibernetice (EU-US 'Working Group on Cybersecurity and Cybercrime'– EU-US WG, înființat în 2010) și un dialog UE-SUA pe domeniul cyber (EU-US 'Cyber Dialogue', creat în 2014), precum și cooperare între FBI și EC3 (European Cyber Crime Center din cadrul Europol). În ceea ce privește 5G, UE a creat un 5G Cybersecurity Toolbox (ianuarie 2020), iar SUA a creat Clean Network (august 2020), care promovează criterii și standarde de risc americane pentru rețele de telecomunicații, cum ar fi 5G sau cloud. În octombrie 2020, SUA și UE au legat cele două inițiative și au discutat despre sinergiile dintre ele și despre angajamentul fiecăruia către principiile comune în domeniul securității 5G (Anagnostakis, 2020). De asemenea, marile inițiative americane și europene de securitate cibernetică (cel mai recent, *Cyber Diplomacy Act* în SUA și formarea *Cyber Diplomacy Toolbox* în Uniunea Europeană) prioritizează cooperarea cu parteneri și aliați și accentul asupra unui sistem de guvernanță adecvat ca precondiție pentru ameliorarea amenințărilor cibernetice.
Toate acestea sunt exemple de diplomație cibernetică ca fenomen emergent, complex și aflat în rapidă schimbare, odată cu mediul a cărui guvernanță o adresează.

WP 3 – studiu practic
Aceste pachet de lucru vizează implementarea activităților practice în cadrul proiectului, pornind de la livrabilele teoretice de la WP 2. În principal, este urmărită elaborarea unui chestionar de specialitate utilizând instrumente online gratuite și diseminarea acestuia în cadrul rețelei pre-existente de diplomați și experți cyber a colectivului de proiect. Prin analiza datelor obținute de la respondenți, vor fi dezvoltate produse de cercetare care vor fi publicate în jurnale de prestigiu. Trebuie evidențiată originalitatea acestui demers în domeniul diplomației cibernetice și relevanța sa pentru succesul academic al acestui proiect.

- Activitatea 3.1 – dezvoltarea unui chestionar de specialitate adresat actorilor relevanți

Pentru a minimiza costurile, chestionarul de specialitate va fi dezvoltat cu instrumente gratuite disponibile online. Grupul-țintă este constituit din diplomați, experți cyber cu activitate internațională și factori de decizie din cadrul organizațiilor de profil și autorităților competente. În acest scop, echipa de proiect va apela la rețeaua sa internațională coagulată ca parte a activității în domeniul securității și guvernanței cibernetice, profitând și de infrastructura pre-existentă a Centrului pentru Diplomație Cibernetică al Institutului Național pentru Cercetare-Dezvoltare în domeniul Informaticii ICI București. Chestionarul va fi compus din minim 4 capitole – date personale, ale organizației și activității lor, conștientizarea problemelor cibernetice, conștientizarea diplomației cibernetice, preferințe în abordarea viitoare a diplomației cibernetice și evaluări ale statutului actual al diplomației cibernetice în țara și regiunea lor. Datele vor fi colectate anonim. În cursul identificării potențialilor respondenți, vor fi efectuate și interviuri de specialitate care să suplimenteze cunoștințele acumulate în cursul activităților WP 2.

- Activitatea 3.2 – analiza datelor obținute în urma sondajului

Datele vor fi colectate automat la sfârșitul perioadei de diseminare ca urmare a aplicației online folosite. Ele vor fi analizate utilizând tehnici statistice și de analiză a datelor pentru a extrage concluzii pertinente cu privire la statutul actual al domeniului diplomației cibernetice. Concluziile vor fi reprezentate în mod grafic și prin selecție de răspunsuri individuale pertinente, pentru a oferi o contribuție originală la analiza eforturilor de guvernanță sistemică a domeniului cyber la nivel internațional. Este anticipată prelucrarea rezultatelor cercetării pentru publicarea într-un jurnal de prestigiu.

WP 4 – elaborare documente de referință

În cadrul acestui pachet de lucru, vor fi elaborate o serie de documente de referință care vor reprezenta încă un aport original al echipei de proiect la domeniul diplomației cibernetice. Aceste documente pot sta la baza unor articole în jurnale de prestigiu, dar și la baza unor documente programatice naționale sau europene în domeniu.

- Activitatea 4.1 – elaborarea profilului diplomatului cibernetic;

Profilul diplomatului cibernetic este un studiu care va oferi recomandări cu privire la organizarea activității de diplomație cibernetică în cadrul ministerelor de resort sau a altor organizații implicate în diplomație cibernetică. Studiul va viza selecția și pregătirea diplomatului cibernetic, atât inițială, cât și continuă, dezvoltarea metodelor sale de lucru, localizarea sa în cadrul organizației și a mijloacelor prin care își întreprinde activitatea în colaborare cu alți membri ai organizației. Acest document va folosi rezultatele etapelor precedente, mai ales pe cele ale chestionarului pe diplomație cibernetică și a interviurilor care vor avea loc în paralel. Considerăm că acest livrabil reprezintă un aport original la literatura în domeniu, nu doar din perspectivă științifică, dar și a politicilor publice naționale și europene. Un efort similar ca principiu, la care au participat membri ai colectivului de proiect, a fost proiectul "SLO - Security Liaison Officer" (2012-2013) – condus de Universitatea Campus Bio-Medico din Rome, împreună cu Asociația Română pentru Promovarea Protecției Infrastructurilor şi Serviciilor Critice, Italian Association of Critical Infrastructure Experts – AIIC; The Italian Association of Continuity Managers; Italian ASIS Division (Chapter 211) of ASIS International – număr înregistrare HOME/2012/CIPS/AG/4000003747 – programul de "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks" al Comisiei Europene. Acest proiect a avut ca rezultat un profil al ofițerului de legătură în domeniul cooperării pentru protecția infrastructurilor critice. Rezultatele studiului au fost integrate în documente europene în domeniul protecției infrastructurilor critice. Profilul diplomatului cibernetic are aceeași utilitate din perspectiva practicii guvernanței sistemice cyber, dar într-un domeniu nou, aflat într-o continuă dezvoltare.

- Activitatea 4.2 – elaborarea unor analize subsidiare a două domenii identificate în cadrul diplomației cibernetice – energie și protecția infrastructurilor critice

Domeniul cibernetic este unul vast pentru că spațiul cibernetic reprezintă mediul de comandă, control, coordonare și comunicare pentru toate sistemele de infrastructuri, inclusiv cele critice (Georgescu et al, 2019). Diplomația cibernetică, ca activitate de dezvoltare a guvernanței sistemice cibernetice în interesul securității, dezvoltării și prosperității, va avea o amplitudine similară, acoperind nu doar guvernanța sistemelor TIC, dar și a altor sisteme (Georgescu et al, 2020). În acest sens, pot fi dezvoltate subdomenii ale diplomației cibernetice, care vor avea propriile

caracteristici rezultate din problemele specifice adresate. În cadrul acestei activități, vor fi elaborate analize pentru două subdomenii ale diplomației cibernetice – diplomația cibernetică în domeniul energiei și în domeniul protecției infrastructurilor critice. Selecția celor două domenii a fost realizată în baza experienței internaționale a echipei de proiect, observând interesul unor entități precum International Energy Forum, International Association for Critical Infrastructure Protection Professional, Consultation Forum on Sustainable Energy in Defence and Security Sectors (al Agenției Europene de Apărare) pentru aceste domenii. Analizele respective vor constitui o altă contribuție originală.

- Activitatea 4.3 – promovarea conceptului de diplomație cibernetică și a capabilităților naționale în domeniu, ca o componentă a interesului național

În plus față de activitatea lor științifică în cadrul conferințelor și jurnalelor de profil, membri ai echipei de proiect au oportunitatea de a promova rezultatele proiectului și prin alte mijloace – participarea la reuniuni internaționale ne-academice și publicarea în reviste non-academice dar de prestigiu. Dezvoltarea domeniului diplomației cibernetice ca subiect de cercetare va depinde și de astfel de contribuții.

WP 5 - diseminarea științifică a rezultatelor

- Activitate 5.1 – crearea paginii web a proiectului
- Activitate 5.2 – diseminarea rezultatelor prin participarea la conferințe de specialitate, redactarea de articole științifice pentru jurnale de prestigiu și actualizarea informațiilor de pe site-ul proiectului

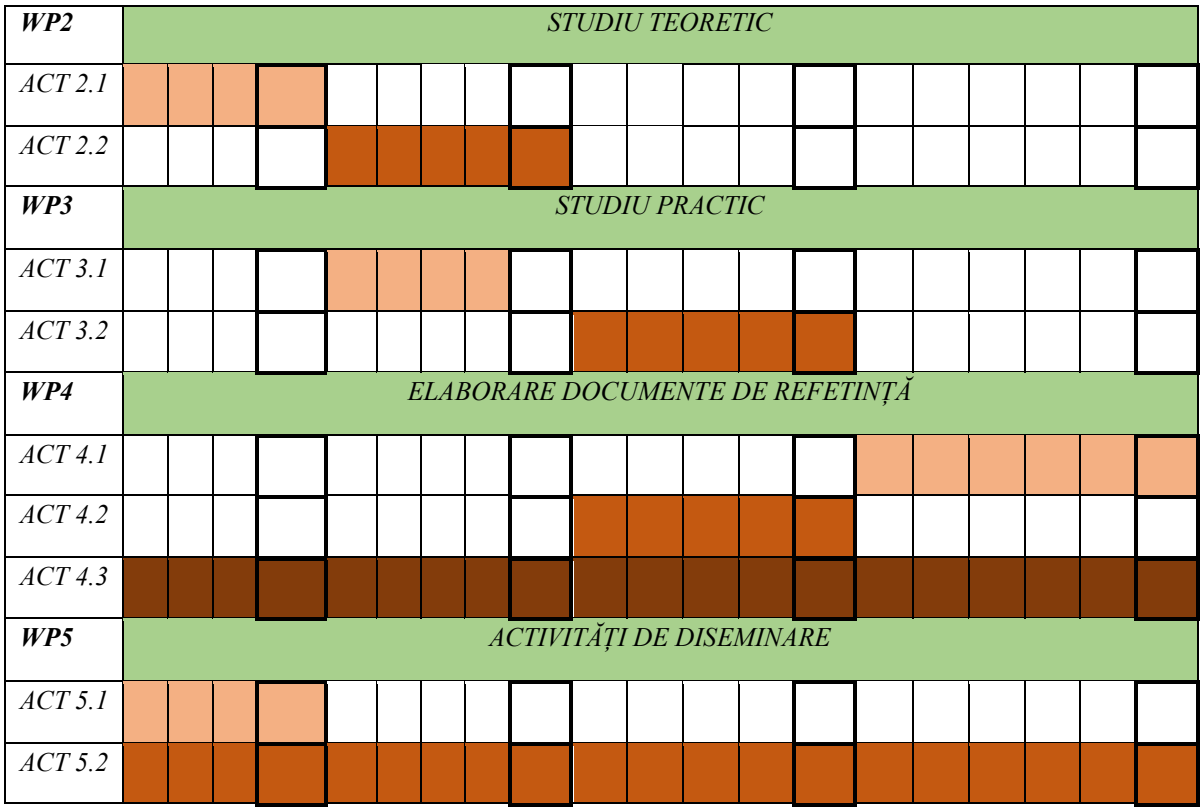
5. Rezultate estimate intermediare/finale cu indicarea calendarului de activități

La finalul fiecărei activități din WP 2-WP 5 vor exista livrabile care să dovedească parcurgerea și finalizarea activităților propuse: Detaliem următoarele livrabile:

- Activitatea 2.1 – studiu de literatură cu privire la diplomația cibernetică (termen: M4)
- Activitatea 2.2 – studiul cu privire la dimensiunile europene ale diplomației cibernetice (termen: M9)
- Activitate 3.1 – document chestionar de specialitate, listă de distribuție și listă de întâlniri de specialitate (termen: M8)
- Activitate 3.2 – pachet date brute pentru chestionar și document analiză statistică (termen: M14).
- Activitate 4.1 – studiu profil diplomat cibernetic (termen: M20).
- Activitate 4.2 – studiu subdomenii diplomație cibernetică (termen: M14).
- Activitate 4.3 – raport diseminare (termen: M20).
- Activitate 5.1 – site informare (termen: M4).
- Activitate 5.2 – raport diseminare științifică (termen: M20).

Mai jos, poate fi văzut calendarul activităților în cadrul proiectului.

LUNA	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
				R1					**R2**					**R3**						**R4**
WP1	*ACTIVITĂȚI DE MANAGEMENT*																			
ACT 1.1																				



Livrabile aferente fiecărei activități care vor fi introduse în rapoartele de progres, respectiv în raportul final menționate în "Pachetul de informații": rapoartele intermediare de la datele de 30 iulie, 5 decembrie 2022, 30 iunie 2023 și raportul final pe 4 decembrie 2023. De asemenea, rezultatele cercetării se vor regăsi și în diseminările din cadrul articolelor publicate.

6. Articole estimate a fi elaborate cu indicarea factorului de impact minim al revistei unde vor fi publicate.

Se estimează publicarea a minim 3 articole in reviste Q1 sau Q2. Se are in vederea trimiterea rezultatelor cercetării la reviste de prestigiu, ca de exemplu : "International Interactions", IF = 1,372 (2020), Q2; "Contemporary Security Policy", IF= 2,640 (2020), Q2; „Foreign Policy Analysis", IF = 1,776, Q2; „Security Dialogue" , IF = 3,459, Q1

7. Bibliografie

- Bauer, J. M., van Eeten, M. (2009) Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy 33(10-11):706-719, https://www.researchgate.net/publication/227426674_Cybersecurity_Stakeholder_incentives_externalities_and_policy_options
- Anagnostakis, D. (2021), The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. Journal of Cyber Policy, DOI: 10.1080/23738871.2021.1916975.
- Mușetescu R.C., (coordonator), Volintiru, C.A., Georgescu, A., Frantescu D. P. (2022). Consolidarea relației UE-SUA în noul context geopolitic, inclusiv din perspectiva

gestionării tehnologiilor emergente. Oportunități pentru România. în cadrul seriei Studii de Strategie și Politici SPOS 2021, Institutul European din România (în curs de apariție)
- Georgescu, A., Gheorghe, A., Piso, M.-I., Katina, P.F. (2019), "Critical Space Infrastructures: Risk, Resilience and Complexity", Topics in Safety, Risk, Reliability and Quality, Seria 36, eBook ISBN 978-3-030-12604-9, DOI 10.1007/978-3-030-12604-9, Hardcover ISBN 978-3-030-12603-2, Series ISSN 1566-0443, Springer International Publishing
- Georgescu, A., Vevera, V., Cirnu, C.E. (2020). The Diplomacy of Systemic Governance in Cyberspace. International Journal of Cyber Diplomacy, Volumul 1, Nr. 1, pag. 79-88
- Gheorghe, A., Vamanu, D.V., Katina, P., Pulfer, R., 2018. Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality. Springer International Publishing. https://doi.org/10.1007/978-3-319-69224-1
- Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82, 175–192. https://doi.org/10.1007/s11069-016-2186-3
- Slaughter, A. M. (2004) A New World Order. Princeton; Oxford: Princeton University Press. doi:10.2307/j.ctt7rqxg

8. Suma solicitată: 60.000 lei

Pentru a diminua costurile proiectului, se vor folosi platforme open source, cum ar fi Google Forms sau Qualtrics. Bugetul are in vedere si achitarea taxelor de publicare în regim *open access*. În acest mod, vom asigura o vizibilitate mai mare a cercetării și, prin urmare, un impact mai mare.

B.2. Titlu și rezumat în limba engleză (max. 10 rânduri)

Cyber Diplomacy as an Instrument of Governance for the Digital Society

Cyber Diplomacy is an emerging field concerned with the use of diplomatic means and instruments to address issues related to cyber governance. The rapid development of digitalization and interconnectivity has generated significant systemic cross-border challenges which individual states, organizations and other stakeholders are ill equipped to handle by themselves. These issues range from governance issues and risks stemming from greater complexity of networked critical infrastructures to the threat of asymmetric and hybrid warfare. Cyber diplomacy is a developing field that addresses these issues, by allowing states and other stakeholders to develop global cyber governance through laws, norms, regulations, and various other forms of cooperation and collective action. The project proposal envisions a literature review with a resulting research methodology, a specialty survey distributed within the cyber and diplomatic network of the team members and a series of studies, the most important of which is a profile of the cyber diplomat.