

EXPUNERE DE MOTIVE

Proiect de Lege pentru modificarea și completarea Ordonanței de Urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică aprobată prin Legea nr. 11/2022 publicată în Monitorul Oficial al României, Partea I nr. 25 din 7 ianuarie 2022

1 - Descrierea situației actuale

Prin Ordonanța de Urgență a Guvernului nr. 104/2021 a fost înființat Directoratul Național de Securitate Cibernetică (DNSC sau Directoratul). Ordonanța a fost aprobată prin Legea 11/07.01.2022, iar prin hotărârea CSAT nr.19 din 15 februarie 2022 au fost aprobate organigrama și statul de funcții ale Directoratului.

În vederea îndeplinirii obiectivelor instituționale referitoare la asigurarea unui nivel ridicat de securitate cibernetică a spațiului cibernetic național civil și stabilirea unui mecanism de cooperare eficace între statele membre ale UE așa cum este prevăzut în Directivele și Regulamentele UE, Directoratul, conform art. 13 al OUG 104/2021, are obligația să angajeze personal înalt calificat de securitate cibernetică, în funcții specifice de conducere și de execuție.

Directoratul are nevoie stringentă de personal înalt specializat în vederea îndeplinirii atribuțiilor și obligațiilor ce îi revin în calitate de autoritate competentă la nivel național. Ordonanța de Urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică prevede ca noile roluri, responsabilități și funcții ale Directoratului să fie îndeplinite de specialiști în domeniul securității cibernetice ce vor trebui încadrați urgent pe o serie de funcții specifice de conducere și de execuție absolut noi la nivelul României:

a. Funcții de conducere: Manager superior securitate cibernetică, Manager securitate cibernetică, Coordonator superior securitate cibernetică, Coordonator securitate cibernetică.

b. Funcții de execuție: Expert/Asistent securitate cibernetică, Expert/Asistent preluare, analiză primară și răspuns la incidente securitate cibernetică, Expert/Asistent investigații digitale și analiză malware, Expert/Asistent dezvoltare, implementare și administrare infrastructuri securitate cibernetică, Expert/Asistent analiză surse deschise, riscuri și amenințări securitate cibernetică, Expert/Asistent accesare fonduri, implementare și administrare proiecte securitate cibernetică, Expert/Asistent legal politici, standardizare de securitate cibernetică, Expert/Asistent evaluare și impact financiar securitate cibernetică, Expert/Asistent politici, strategii și cooperare securitate cibernetică, Expert/Asistent dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică.

Din motive legate de lipsa unui cadru legal adecvat, funcțiile specifice de conduce și de execuție ale Directoratului nu există în prezent în anexele la Legea-cadru 153/2017, prin urmare nu pot fi asimilate cu alte funcții din anexele acesteia.

Funcțiile specifice de conducere și de execuție din cadrul Directoratului pot fi ocupate doar de specialiști de securitate cibernetică cu o înțelegere detaliată a modului în care riscurile și amenințările cibernetice pot fi identificate, evaluate și contracarate, a modului în care sistemele IT

sau rețelele / infrastructura și lanțul de furnizori digitali al unei organizații funcționează, a modului în care tehnicile și protocoalele de răspuns la incidente cibernetice pot fi aplicate, acestea implicând un set complex și nou de cunoștințe și abilități.

Situația descrisă mai sus are ca efect imposibilitatea declanșării procedurilor de angajare și ocuparea posturilor Directoratului cu specialiști de securitate cibernetică, așa cum este prevăzut la art. 13 al OUG 104/2021 și așa cum a fost aprobat prin hotărârea CSAT nr.19 din 15 februarie 2022, ducând la un blocaj instituțional.

2 - Riscuri, amenințări și vulnerabilități de securitate cibernetică identificate, cu impact asupra bunei funcționări a democrației, societății și economiei românești

Transformarea digitală a societății generează noi provocări care necesită răspunsuri adaptate și inovatoare. Numărul atacurilor cibernetice este în continuă creștere, acestea fiind din ce în ce mai sofisticate și având ca sursă de inițiere resurse informatice din interiorul și din afara UE.

Securitatea cibernetică a devenit una dintre cele mai mari probleme cu care se confruntă lumea contemporană. Scurgeri de date și informații digitale și atacurile cibernetice de ultimă oră au determinat persoanele fizice, instituțiile publice și companiile să conștientizeze tot mai mult riscurile pe care le prezintă vulnerabilitățile din rețelele și sistemele informatice pentru societate.

Ca urmare a transformării digitale accelerate și a proliferării noilor tehnologii din perioada pandemiei COVID-19, s-a demonstrat într-un mod indubitabil că este nevoie stringentă de personal înalt specializat în vederea îndeplinirii atribuțiilor și obligațiilor legale din domeniul securității cibernetice și a celor asumate de România la nivelul UE, fapt ce nu poate fi ignorat și poate deveni un risc major și iminent, ducând inclusiv la crearea unui blocaj instituțional sever, cu impact negativ major la nivelul țării.

În același timp, deficitul de specialiști cu competențe în domeniul securității cibernetice reprezintă o problemă majoră atât pentru dezvoltarea economică, stabilitatea socială, cât și pentru securitatea națională. Acest deficit poate fi analizat prin două aspecte concurente: cantitativ și calitativ. Problema cantitativă este legată de oferta insuficientă de profesioniști în domeniul securității cibernetice pentru a satisface cerințele pieței muncii din România, iar cea calitativă este legată de lipsa recunoașterii (inclusiv prin lipsa unei asimilări cu grilele sau funcțiile existente în Legea-cadru nr.153/2017) ori de clasificarea inadecvată a ocupațiilor specifice domeniului securității cibernetice.

Odată cu adoptarea OUG nr.104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, s-a creat o instituție publică centrală care îndeplinește atribuțiile de autoritate competentă de securitate cibernetică la nivel național pentru spațiul cibernetic național civil.

Pentru a depăși actuala situație de blocaj instituțional a Directoratului, și a elimina dificultățile majore în operaționalizarea acestuia, datorate imposibilității de a angaja personal de specialitate, este urgentă și imperios necesară adaptarea cadrului legislativ actual privind încadrarea și salarizarea funcțiilor specifice de securitate cibernetică ale Directoratului, îndeosebi în contextul geopolitic actual.

Odată cu invazia Ucrainei de către Federația Rusă la 24 Februarie 2022, actori cibernetici afiliați intereselor Federației Ruse au inițiat atacuri cibernetice intense, repetate și de amploare asupra infrastructurilor cibernetice din țara noastră și a statelor aliate.

Astfel, începând cu finalul lunii februarie 2022, România a devenit ținta mai multor acțiuni cibernetice de recunoaștere în spațiul cibernetic civil, care au constituit prima fază a unei serii de atacuri cibernetice complexe ce au vizat obținerea accesului neautorizat cu drepturi de administrare

asupra infrastructurilor cibernetice și utilizarea acestora împotriva intereselor strategice ale României și aliaților săi.

La data de 6 martie 2022, Grupul KMG ROMPETROL a fost victima unui incident cibernetic major cu impact asupra infrastructurii, datelor, serviciilor informatice și operațiunilor grupului. Atacul a constat în criptarea serverelor de date virtuale, producând multiple efecte negative asupra activităților grupului, inclusiv în plan tehnic și economico-financiar.

La data de 25 martie 2022, țara noastră a fost ținta unei campanii cibernetice malițioase cu malware, vectorul de atac principal fiind platforma Gmail, care a vizat instituții de stat și private din România, cu scopul exfiltrării / extragerii de date și al blocării sistemelor informatice. Atacatorii au impersonat instituții publice sau companii private din România folosind liste de adrese de email existente în calculatoarele atacate pentru a transmite și propaga mesaje ce conțineau link-uri care redirectionau către pagini web infectate.

În aceeași perioadă, martie 2022, la nivel național, au fost derulate ample campanii de atacuri cibernetice asupra utilizatorilor obișnuiți, îndeosebi prin tehnici de impersonare a unor servicii oferite de către bănci, firme de curierat, platforme de vânzări online, cu scopul livrării unor aplicații malițioase către populație, prin care atacatorii puteau obține accesul la datele bancare și cu caracter personal, precum și controlul total al dispozitivelor mobile pentru a fi folosite ulterior în alte activități ilegale.

Atacurile cibernetice derulate până în prezent au vizat inclusiv afectarea confidențialității, integrității și disponibilității datelor și informațiilor vehiculate prin rețelele guvernamentale ale statului român.

De asemenea, în perioada 30 aprilie – 3 mai 2022, grupări de criminalitate cibernetică – îndeosebi gruparea pro-rusă Killnet – au inițiat și derulat atacuri masive de tip DDoS (Distributed Denial of Service) asupra paginilor web ale instituțiilor fundamentale ale statului român, precum: Președinția României, Senatul României, Camera Deputaților, Guvernul României, Directoratul Național de Securitate Cibernetică, Ministerul Apărării Naționale, Ministerul de Interne, Poliția Română, Poliția de Frontieră, Jandarmeria Română, Ministerul Finanțelor, Ministerul Sănătății, Institutul Național de Statistică.

Majoritatea atacurilor derulate recent au fost de tip Distributed Denial of Service (DDoS) și au vizat blocarea accesului utilizatorilor la paginile web menționate, în scopul creării unei stări de panică și amenințare. Acestea au fost însoțite de amenințări concrete împotriva Guvernului României și instituțiilor statului român, precum și împotriva unor entități mass-media, transmise prin intermediul canalelor de comunicare ale platformei Telegram de către grupările de atacatori cibernetici.

În aceste tipuri de atac au fost utilizate până la aceasta dată un număr de 11.414 adrese IP unice, dintre care unele erau asociate cu infrastructuri de servicii internet din România, fapt ce atestă o intensificare deosebită și o diversificare a metodelor de acțiune folosite.

În cazul atacului de tip DDoS din 30 aprilie 2022, asupra site-ului de web al Camerei Deputaților, atacatorii Killnet au utilizat infrastructuri localizate în multiple locații geografice, astfel:

Nr.	Locație geografică aparentă	Număr adrese IP utilizate de atacatori
1.	Brazilia	2
2.	China	1
3.	Columbia	1
4.	Franța	5
5.	Germania	1

Nr.	Locație geografică aparentă	Număr adrese IP utilizate de atacatori
6.	Indonezia	1
7.	Irlanda	1
8.	Liban	1
9.	Marea Britanie	7
10.	Mexic	2
11.	Olanda	1
12.	Romania	8
13.	Rusia	517
14.	Singapore	2
15.	Spania	1
16.	Suedia	2
17.	Taiwan	1
18.	Statele Unite ale Americii	3
19.	Ungaria	1
20.	Vietnam	1
21.	Noduri TOR	2
	TOTAL	561

Din această perspectivă, este relevant și faptul că atacatorii cibernetici au vizat inclusiv Sistemul Național de Plată Electronic Online cu Cardul Bancar (SNEP), care poate fi accesat prin pagina web Ghișeul.ro.

Totodată, atacatorii cibernetici ai grupării pro-ruse Killnet au vizat resursele informatice ale unor instituții și firme private care oferă servicii esențiale populației din domeniul sănătății, al transporturilor, energie, bancar și educație, dintre care se evidențiază 13 aeroporturi, Tarom, CFR Călători, Petrom, Rompetrol, SMURD, Administrația Spitalelor și Serviciilor Medicale București.

În paralel, atacatorii cibernetici au vizat furnizorii de servicii internet (Orange, RCS & RDS) și, pentru a perturba canalele de informare a populației, au vizat și au reușit să afecteze temporar paginile de web ale unor diferite trusturi media (Digi24, Hotnews, Antena 3, Active News, Aleph News).

De asemenea, a fost vizată și componenta de decizie politică a statului, fiind afectate paginile web ale Partidului Social Democrat, Partidului Național Liberal și Partidului AUR, element relevant în contextul vizitei delegației oficiale de nivel înalt a României în Ucraina și al sprijinului pe care clasa politică românească îl arată public pentru Ucraina.

Pentru încetarea atacurilor și limitarea efectelor acestora, Directoratul Național de Securitate Cibernetică a fost principala instituție solicitată, fiind deosebit de activă atât pe partea de prevenire, conștientizare dar și de răspuns efectiv, rapid și coordonat – atât la nivel național, cât și în coordonare cu țările UE și cu alte state aliate României. .

În acest context, se evidențiază faptul că, în prezent, România, prin Directoratul Național de Securitate Cibernetică se află într-o situație extrem de critică în ceea ce privește capacitatea de reacție la varietatea și complexitatea atacurilor cibernetice care au ca țintă spațiul cibernetic național civil, parte a securității naționale, întrucât **nu dispune de suficiente resurse umane cu expertiză în domeniul securității cibernetice**. La acest moment Directoratul include doar 59 angajați, inclusiv Directorul, Adjuncții Directorului și consilierii acestuia. Nici una dintre funcțiile specifice de conducere sau de execuție ale Directoratului nu poate fi încă încadrată cu personal de specialitate, din cauza lipsei bazei legale privind salarizarea acestora.

Situația are ca principală cauză lipsa cadrului legal necesar declanșării procedurilor de angajare și stabilirii cuantumului salarial adecvat pentru atragerea, motivarea și menținerea specialiștilor care

să dispună de cunoștințele și expertiza necesare reacției rapide la incidente cibernetice, limitării pagubelor, efectuării de investigații complexe și restabilirii funcționării normale a infrastructurilor afectate.

Având în vedere caracterul de continuitate care se conturează în jurul conflictului dintre Federația Rusă și Ucraina, războiul în spațiul cibernetic se va intensifica, existând riscul major ca Directoratul să nu poată asigura securitatea spațiului cibernetic național civil conform prevederilor legale din cauza situației explicate mai sus. Acest aspect va determina o blocare a sistemelor informatice esențiale ale statului român, fapt ce va genera situații de criză economică și socială.

Dinamica schimbărilor în domeniul securității cibernetice, noile cerințe ale Uniunii Europene, inclusiv responsabilitățile primite prin intrarea în vigoare a Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice generează probleme de fond, ca urmare a depășirii capacităților funcționale și a resurselor alocate Directoratului pentru a face față noilor provocări, riscuri și amenințări de securitate cibernetică.

În baza Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, a Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, a OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, este necesar a avea în vedere două obiective principale: (1) asigurarea unui nivel ridicat de securitate cibernetică a spațiului cibernetic național civil; (2) stabilirea unui mecanism de cooperare eficace între statele membre ale UE pentru a promova acest obiectiv, dar resursele trebuie să fie, înainte de toate, dedicate realizării acestor două obiective importante.

Totodată s-a creat și cadrul adecvat de lucru și de exprimare pentru specialiști români cu pregătire înaltă în domeniul securității cibernetice, fapt ce va genera o dezvoltare sustenabilă a acestui domeniu la nivel național cu efecte benefice directe și imediate în economia națională. Astfel, prin această instituție se vor putea crea nuclee de excelență de specialiști care vor contribui la stoparea fenomenului negativ de brain-drain și la menținerea în țară a forței de muncă înalt calificată, care în prezent migrează peste hotare.

Fosta instituție CERT-RO nu a reușit încadrarea personalului de specialitate absolut necesar (având încadrate în 2020 doar 35 salariați pentru cele 149 posturi ale CERT-RO), ceea ce a condus la imposibilitatea îndeplinirii unor atribuții instituționale cheie, spre exemplu cele legate de implementare a Directivei NIS și a Legii 362/2018. Aceasta a condus la intrarea României în infringement prin cauza 2019/2214. Cauza fundamentală a acestei situații s-a datorat lipsei totale de atractivitate a salariilor oferite, în comparație cu pachete salariale foarte competitive oferite pe piața muncii, dar și ca urmare a proceselor rapide și flexibile de evaluare și selecție utilizate de firmele private pentru specialitatea securitate cibernetică.

Piața forței de muncă din domeniul securității cibernetice este una extrem de activă și concurențială și oferă, atât în România cât și la nivel UE, pachete salariale foarte atractive și net superioare celor posibile prin grilele de salarizare prevăzute de Legea-cadru nr.153/2017.

O salarizare atractivă este esențială pentru realizarea acestui obiectiv și păstrarea specialiștilor guvernamentali în domeniul securității cibernetice.

Funcțiile specifice de conducere și de execuție din cadrul Directoratului pot fi ocupate doar de specialiști cu o stăpânire a fundamentelor securității cibernetice și cu o înțelegere detaliată a modului în care sistemele IT sau rețelele / infrastructura și lanțul de furnizori digitali al unei organizații funcționează.

Există un set complex și nou de cunoștințe și abilități care sunt esențiale pentru aceasta, incluzând printre altele: o înțelegere a regulamentelor și standardelor internaționale aplicabile, a arhitecturii IT și de securitate, a datelor, a criptografiei, a rețelelor de telecomunicații, a principiilor de

codificare securizată și a sistemelor de operare, precum și competențe în utilizarea de noi tehnologii digitale, cunoașterea la un nivel ridicat a limbajelor de programare și familiarizarea cu metodele comune de exploatare a vulnerabilităților și tehnicile de atenuare/limitare a riscurilor cibernetice cunoștințe privind reglementările, politicile și normele de securitate cibernetică; cunoștințe juridice și economice privind impactul riscurilor, incidentelor, crizelor și atacurilor cibernetice.

A fost efectuată o analiză a caracteristicilor noilor funcții specifice de conducere și de execuție din cadrul DNSC, acestea având următoarele elemente determinate:

- a. Relevanța și importanța atribuțiilor și responsabilităților, la nivel național;
- b. Importanța rolului din punct de vedere al impactului acestuia legat de siguranța națională, economie, societate, reziliență;
- c. Tehnici, tehnologii și instrumente de lucru utilizate și complexitatea acestora;
- d. Program de lucru și impredictibilitatea acestuia (incidentele, atacurile și crizele cibernetice nefiind predictibile);
- e. Mediu de desfășurare a activității complex, solicitant, caracterizat printr-un nivel de stres ridicat, de impredictibilitate și de cerințe privind concentrarea și analiza;
- f. Situațiile de risc și de criză întâlnite și cerințele pentru adaptarea la acestea;
- g. Nivelul de instruire solicitat, natura și tipul calificărilor necesare exercitării funcției;
- h. Cunoștințele tehnice și non-tehnice, aptitudini și atitudini necesare exercitării funcției.

Personalul ce va fi încadrat pe funcțiile specifice de conducere și de execuție din cadrul Directoratului utilizează o gamă largă de tehnologii, procese și practici pentru a-și exercita atribuțiile, a răspunde la incidente de securitate cibernetică și a sprijini operatorii de servicii esențiale, cetățenii, IMM-urile, școlile în a-și proteja rețelele și infrastructurile informatice, datele, precum și a limita daunele și accesul ilegal.

În acest sens, este imperios necesară implementarea unor măsuri salariale la nivelul Directoratului care să asigure capacitatea minimă necesară pentru a adresa fără întârziere nivelul crescut de amenințare cibernetică ce pune în pericol însăși buna funcționare a sistemelor și rețelelor informatice esențiale ale statului român, ale operatorilor economici, precum și pentru a corespunde cerințelor europene și internaționale în domeniul securității cibernetice.

Prin propunerea de act normativ se urmărește operaționalizarea Directoratului Național de Securitate Cibernetică, care să asigure performanța și capacitățile necesare în domeniul securității cibernetice. În plus, noua instituție va fi adaptată adecvat, putând face față provocărilor pe care dinamica de dezvoltare tehnologică le vor ridica în spațiul cibernetic.

Proiectul de act normativ va facilita implementarea unor mecanisme simple, eficiente și rapide care să asigure capacitatea necesară de personal al Directoratului.

3 – Soluția propusă

În aceasta situație, soluția identificată este aceea de modificare și completare a art.14 din OUG 104/2021 pentru precizarea modului de salarizare a funcțiilor de demnitate publică numite și a funcțiilor specifice de conducere și de execuție din cadrul Directoratului.

Astfel, funcțiile de demnitate publică numite și funcțiile specifice de conducere și de execuție din cadrul Directoratului, care nu sunt prevăzute în anexele Legii-cadru 153/2017, pot beneficia de o salarizare adecvată cu competențele necesare acestor funcții.

Față de cele prezentate, a fost elaborat proiectul privind modificarea și completarea Ordonanței de Urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică aprobată prin Legea nr. 11/2022 publicată în Monitorul Oficial Partea I, nr. 25 din 7 ianuarie 2022.

Inițiatori

Deputat Pavel POPESCU

Deputat Alfred-Robert SIMONIS

Deputat George-Cristian TUȚĂ

⤵

LISTĂ SEMNĂTURI INIȚIATORI

LEGE

pentru modificarea și completarea Ordonanței de Urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică aprobată prin Legea nr. 11/2022 publicată în Monitorul Oficial al României, Partea I nr. 25 din 7 ianuarie 2022

NR.CRT.	PARLAMENTAR	SEMNATURA	PARTID
1.	SORIN DAN MOLDOVAN		PNL
2.	GROSARU ANDR-GABRIEL		MIN
3.	Fifor Mihail		PSD
4.	Mang Ioan		PSD
5.	STANCU IONEL		MINO
6.	ZISOPOL DRAGOS		MINO
7.	STOICA BOGDAN - ALEX		MINO
8.	PIRCEAK IULIUS MARIAN		MINO
9.	CRISTIAN OSEAN		MINO.
10.	NACOV GHEORGHE		MIN.
11.	PETRECH/ NICOLAE		MIN
12.	FEDOR SILVIU		MIN
13.	LONGHER GHERVALEN		MIN
14.	GHERA GUREC-SLODAN		MIN
15.	GEORGE TUTA		PNL
16.	SEBASTIAN BURDA		PNL
17.	FAGARASIAN VALENTIN		PNL
18.	SIGHIARTAU ROBERT		PNL
19.	Balan Ioan		PNL
20.	Bogdan Gheorghe		PNL

22.	Ștefănescu	USMR
23.	CSEF EVA ANDREA	USMR
24.	STEA IOAN MARIN	PNL
25.	Fechet Mircea	PNL
26.	PIRBA MARILEA	PNL
27.	MOISĂ RAJU-NARIN	PNL
28.	GUDU MICHAEL	PNL
29.	ALEXE FLORIN	PNL
30.	Uroșu Diana	PNL
31.	ROSCA MIRCEA	PNL
32.	WEBER MIHAIL	PSD
33.	BALAC VIOREL	PSD
34.	Rujan DUKITRU	PNL
35.	LEOREANU LAURENȚIU IAN	PNL
36.	COZMA ADRIAN	PNL
37.	MĂRGĂRIT MARIUS	PSD
38.	CRĂȘTEȘU RANU	PSD
39.	PECINGINĂ GHEORGHE	PNL
40.	MARA CALISTA	PNL
41.	POLAȘ TUDOR	PNL
42.		
43.		
44.		
45.		
46.		
47.		
48.		