EXPUNERE DE MOTIVE

Proiect de Lege pentru modificarea şi completarea Ordonanţei de Urgenţă a Guvernului nr. 104/2021 privind înfiinţarea Directoratului Naţional 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 situaţiei actuale

Prin Ordonanţa de Urgenţă a Guvernului nr. 104/2021 a fost înfiinţat Directoratul Naţional de Securitate Cibernetică (DNSC sau Directoratul). Ordonanţa a fost aprobată prin Legea 11/07.01.2022, iar prin hotărârea CSAT nr.19 din 15 februarie 2022 au fost aprobate organigrama şi statul de funcţii ale Directoratului.

În vederea îndeplinirii obiectivelor instituţionale referitoare la asigurarea unui nivel ridicat de securitate cibernetică a spaţiului cibernetic naţional civil şi stabilirea unui mecanism de cooperare eficace între statele membre ale UE aşa cum este prevăzut in Directivele şi Regulamentele UE, Directoratul, conform art. 13 al OUG 104/2021, are obligaţia sa angajeze personal înalt calificat de securitate cibernetică, în funcţii specifice de conducere şi de execuţie.

Directoratul are nevoie stringentă de personal înalt specializat în vederea îndeplinirii atribuţiilor şi obligaţiilor ce îi revin în calitate de autoritate competentă la nivel naţional. Ordonanţa de Urgenţă nr. 104/2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică prevede ca noile roluri, responsabilităţi şi funcţii ale Directoratului să fie îndeplinite de specialişti în domeniul securităţii cibernetice ce vor trebui încadraţi urgent pe o serie de funcţii specifice de conducere şi de execuţie absolut noi la nivelul României:

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

b. Funcţii de execuţie: Expert/Asistent securitate cibernetică, Expert/Asistent preluare, analiză primară şi răspuns la incidente securitate cibernetică, Expert/Asistent investigaţii digitale şi analiză malware, Expert/Asistent dezvoltare, implementare şi administrare infrastructuri securitate cibernetică, Expert/Asistent analiză surse deschise, riscuri şi ameninţări securitate cibernetică, Expert/Asistent accesare fonduri, implementare şi administrare proiecte securitate cibernetică, Expert/Asistent legal politici, standardizare de securitate cibernetică, Expert/Asistent evaluare şi impact financiar securitate cibernetică, Expert/Asistent politici, strategii şi cooperare securitate cibernetică, Expert/Asistent dezvoltare competenţe, aptitudini şi cunoştinţe specifice de securitate cibernetică.

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

Funcţiile specifice de conducere şi de execuţie din cadrul Directoratului pot fi ocupate doar de specialişti de securitate cibernetică cu o înţelegere detaliată a modului în care riscurile şi ameninţările cibernetice pot fi identificate, evaluate şi 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 descrisa mai sus are ca efect imposibilitatea declanșării procedurilor de angajare si 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 Romania, iar cea calitativă este legată de lipsa recunoașterii (inclusiv prin lipsa unei asimilări cu grile sau funcții 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 cadrul 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 şi utilizarea acestora împotriva intereselor strategice ale României şi aliaţilor săi.

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

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

În aceeaşi perioadă, martie 2022, la nivel naţional, au fost derulate ample campanii de atacuri cibernetice asupra utilizatorilor obişnuiţi, îndeosebi prin tehnici de impersonare a unor servicii oferite de către bănci, firme de curierat, platforme de vânzări online, cu scopul livrării unor aplicaţii maliţioase către populaţie, prin care atacatorii puteau obţine accesul la datele bancare şi cu caracter personal, precum şi controlul total al dispozitivelor mobile pentru a fi folosite ulterior în alte activităţi ilegale.

Atacurile cibernetice derulate până în prezent au vizat inclusiv afectarea confidenţialităţii, integrităţii şi disponibilităţii datelor şi informaţiilor vehiculate prin reţelele guvernamentale ale statului român.

De asemenea, în perioada 30 aprilie – 3 mai 2022, grupări de criminalitate cibernetică – îndeosebi gruparea pro-rusă Killnet – au iniţiat şi derulat atacuri masive de tip DDoS (Distributed Denial of Service) asupra paginilor web ale instituţiilor fundamentale ale statului român, precum: Preşedinţia României, Senatul României, Camera Deputaţilor, Guvernul României, Directoratul Naţional de Securitate Cibernetică, Ministerul Apărării Naţionale, Ministerul de Interne, Poliţia Română, Poliţia de Frontieră, Jandarmeria Română, Ministerul Finanţelor, Ministerul Sănătăţii, Institutul Naţional de Statistică.

Majoritatea atacurilor derulate recent au fost de tip Distributed Denial of Service (DDoS) şi au vizat blocarea accesului utilizatorilor la paginile web menţionate, în scopul creării unei stări de panică şi ameninţare. Acestea au fost însoţite de ameninţări concrete împotriva Guvernului României şi instituţiilor statului român, precum şi împotriva unor entităţi 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 şi o diversificare a metodelor de acţiune folosite.

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

Nr.	Locaţie geografică aparentă	Număr adrese IP utilizate de atacatori
1.	Brazilia	2
2.	China	1
3.	Columbia	1
4.	Franţa	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 şi faptul că atacatorii cibernetici au vizat inclusiv Sistemul Național de Plată Electronic Online cu Cardul Bancar (SNEP), care poate fi accesat prin pagina web Ghişeul.ro.

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

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

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

Pentru încetarea atacurilor şi limitarea efectelor acestora, Directoratul Național de Securitate Cibernetică a fost principala instituție solicitată, fiind deosebit de activă atât pe partea de prevenire, conştientizare dar şi de răspuns efectiv, rapid şi coordonat – atât la nivel național, cât şi in coordonare cu tarile UE şi 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 priveşte capacitatea de reacție la varietatea şi 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 şi 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 declanşării procedurilor de angajare şi stabilirii cuantumului salarial adecvat pentru atragerea, motivarea şi menținerea specialiştilor care

să dispună de cunoştinţele şi expertiza necesare reacţiei rapide la incidente cibernetice, limitării pagubelor, efectuării de investigaţii complexe şi restabilirii funcţionării normale a infrastructurilor afectate.

Având în vedere caracterul de continuitate care se conturează în jurul conflictului dintre Federaţia Rusă şi Ucraina, războiul în spaţiul cibernetic se va intensifica, existând riscul major ca Directoratul să nu poată asigura securitatea spaţiului cibernetic naţional civil conform prevederilor legale din cauza situaţiei explicate mai sus. Acest aspect va determina o blocare a sistemelor informatice esenţiale ale statului român, fapt ce va genera situaţii de criză economică şi socială.

Dinamica schimbărilor în domeniul securităţii cibernetice, noile cerinţe ale Uniunii Europene, inclusiv responsabilităţile primite prin intrarea în vigoare a Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice generează probleme de fond, ca urmare a depăşirii capacităţilor funcţionale şi a resurselor alocate Directoratului pentru a face faţă noilor provocări, riscuri şi ameninţări de securitate cibernetică.

În baza Directivei (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune, a Legii 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, a OUG 104/ 2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică, este necesar a avea în vedere două obiective principale: (1) asigurarea unui nivel ridicat de securitate cibernetică a spaţiului cibernetic naţional 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 şi cadrul adecvat de lucru şi de exprimare pentru specialişti români cu pregătire înaltă în domeniul securităţii cibernetice, fapt ce va genera o dezvoltare sustenabilă a acestui domeniu la nivel naţional cu efecte benefice directe şi imediate în economia naţională. Astfel, prin această instituţie se vor putea crea nuclee de excelenţă de specialişti care vor contribui la stoparea fenomenului negativ de brain-drain şi la menţinerea în ţară a forţei de muncă înalt calificate, care în prezent migrează peste hotare.

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

Piaţa forţei de muncă din domeniul securităţii cibernetice este una extrem de activă şi concurenţială şi oferă, atât în România cât şi la nivel UE, pachete salariale foarte atractive şi net superioare celor posibile prin grilele de salarizare prevăzute de Legea-cadru nr.153/2017.

O salarizare atractivă este esenţială pentru realizarea acestui obiectiv şi păstrarea specialiştilor guvernamentali în domeniul securităţii cibernetice.

Funcţiile specifice de conducere şi de execuţie din cadrul Directoratului pot fi ocupate doar de specialişti cu o stăpânire a fundamentelor securităţii cibernetice şi cu o înţelegere detaliată a modului în care sistemele IT sau reţelele / infrastructura şi lanţul de furnizori digitali al unei organizaţii funcţionează.

Există un set complex şi nou de cunoştinţe şi abilităţi care sunt esenţiale pentru aceasta, incluzând printre altele: o înţelegere a regulamentelor şi standardelor internaţionale aplicabile, a arhitecturii IT şi de securitate, a datelor, a criptografiei, a reţelelor de telecomunicaţii, a principiilor de

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

A fost efectuată o analiză a caracteristicilor noilor funcţii specifice de conducere şi de execuţie din cadrul DNSC, acestea având următoarele elemente determinante:

a. Relevanţa şi importanţa atribuţiilor şi responsabilităţilor, la nivel naţional;

b. Importanţa rolului din punct de vedere al impactului acestuia legat de siguranţa naţională, economie, societate, rezilienţă;

c. Tehnici, tehnologii şi instrumente de lucru utilizate şi complexitatea acestora;

d. Program de lucru şi impredictibilitatea acestuia (incidentele, atacurile şi crizele cibernetice nefiind predictibile);

e. Mediu de desfăşurare a activităţii complex, solicitant, caracterizat printr-un nivel de stres ridicat, de impredictibilitate şi de cerinţe privind concentrarea şi analiza;

f. Situaţiile de risc şi de criză întâlnite şi cerinţele pentru adaptarea la acestea;

g. Nivelul de instruire solicitat, natura şi tipul calificărilor necesare exercitării funcţiei;

h. Cunoştinţele tehnice şi non-tehnice, aptitudini şi atitudini necesare exercitării funcţiei.

Personalul ce va fi încadrat pe funcţiile specifice de conducere şi de execuţie din cadrul Directoratului utilizează o gamă largă de tehnologii, procese şi practici pentru a-şi exercita atribuţiile, a răspunde la incidente de securitate cibernetică şi a sprijini operatorii de servicii esenţiale, cetăţenii, IMM-urile, şcolile în a-şi proteja reţelele şi infrastructurile informatice, datele, precum şi a limita daunele şi 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 ameninţare cibernetică ce pune în pericol însăşi buna funcţionare a sistemelor şi reţelelor informatice esenţiale ale statului român, ale operatorilor economici, precum şi pentru a corespunde cerinţelor europene şi internaţionale în domeniul securităţii cibernetice.

Prin propunerea de act normativ se urmăreşte operaţionalizarea Directoratului Naţional de Securitate Cibernetică, care să asigure performanţa şi capabilităţile necesare în domeniul securităţii cibernetice. În plus, noua instituţie va fi adaptată adecvat, putând face faţă provocărilor pe care dinamicile de dezvoltare tehnologică le vor ridica în spaţiul cibernetic.

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

3 – Soluţia propusă

In aceasta situaţie, soluţia identificată este aceea de modificare şi completare a art.14 din OUG 104/2021 pentru precizarea modului de salarizare a funcţiilor de demnitate publică numite şi a funcţiilor specifice de conducere şi de execuţie din cadrul Directoratului.

Astfel, funcţiile de demnitate publică numite şi funcţiile specifice de conducere şi de execuţie din cadrul Directoratului, care nu sunt prevăzute în anexele Legii-cadru 153/2017, pot beneficia de o salarizare adecvată cu competenţele necesare acestor funcţii.

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 INIŢIATORI

LEGE

pentru modificarea şi completarea Ordonanţei de Urgenţă a Guvernului nr. 104/2021 privind înfiinţarea Directoratului Naţional 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 ANA-GABRIEL		MIN
3.	Fifor Mihai		PSD
4.	Mang Ioan		PSD
5.	STANCU IONEL		MINO
6.	ZISOPOL DRAGOS		MINO
7.	STOICA BOGDAN - ALIN		MINO
8.	PIRCZAK IULIUS MARIAN		MINO
9.	CRISTIAN OSMEAU		MINO.
10.	NACOV GHEORGHE		MIN.
11.	POTRECHI MICOLAO		MIN
12.	FEODOR SILVIU		MIN
13.	LONGHER GHERVAZEN		MIN
14.	GHERA GIURECI-SLOBODAN		MIN
15.	GEORGE TUTA		PNL
16.	SEBASTIAN BURDUJA		PNL
17.	FAGARASIAN VALENTIN		PNL
18.	SIGHIARTĂU ROBERT		PNL
19.	Bolaj Ioan		PNL
20.	Bogdan Liviu		PNL

22.	Szabó Ödön	UDMR	
23.	CSEP ÉVA ANDREA	UDMR	
24.	STOICA IONUȚ MARIN	PNL	
25.	Fechet Mircea	PNL	
26.	PÎRȚEA MARIUȚA	PNL	
27.	MOIȘIN RAȘU-MARIN	PNL	
28.	GUȘU MICHAEL	PNL	
29.	ALEXE FLORIN	PNL	
30.	Moraru Diana	PNL	
31.	ROȘCA MIRCEA	PNL	
32.	WEBER MIHAI	PSD	
33.	BALAȘ VIOREL	PSD	
34.	RUJAN DUMITRU	PNL	
35.	LEOREANU LAURENȚIU IOAN	PNL	
36.	COZMA ADRIAN	PNL	
37.	MĂRGĂRIT MARIUS	PSD	
38.	CRĂCIUNESCU RADU	PSD	
39.	PECINGINĂ GHEORGHE	PNL	
40.	MARIA CALOTA	PNL	
41.	POLAK TUDOR	PNL	
42.			
43.			
44.			
45.			
46.			
47.			
48.			