INTELLIGENCE ŞI CULTURA DE SECURITATE

CONFERINȚA ȘTIINȚIFICĂ STUDENȚEASCĂ

PROCEEDINGS

VOLUMUL 2
2023

Editura Academiei Naţionale de Informaţii „Mihai Viteazul”

ANALIZĂ DE CONȚINUT A ARIILOR STRATEGICE DE SECURITATE CIBERNETICĂ – STATELE UNITE ALE AMERICII, MAREA BRITANIE, SPANIA ȘI ROMÂNIA

(CONTENT ANALYSIS OF STRATEGIC CYBER SECURITY FOCUS AREAS – UNITED STATES OF AMERICA, UNITED KINGDOM, SPAIN AND ROMANIA)

Cristian CONDRUȚ[*]

Abstract:

Nowadays cybersecurity is a topic that is more extensively addressed at a strategic level, both form a technical as well as form a non-technical perspective. In this context, the most important international organizations address cybersecurity by organizing international discussions aimed at keeping an open, free and secure cyberspace. These endeavours are usually taking the form a policy paper, a recommendation guide or a common initiative signed by multiple states. This kind of practice requires a correspondent in national strategic policy papers, the most important one being the national cybersecurity strategy. Taking into consideration that cybersecurity is not only a technical matter, multiple strategic areas are needed to be addressed. Thus, in this paper we aim to identify the most important cybersecurity strategic areas at a national level and their corelations. To achieve this research objective, we apply a content analysis and a frequency analysis methodology, using MAXQDA 20222 software. Our findings show that cybersecurity governance strategic area and preparedness and resilience strategic area are the most important ones at a national level, having multiple corelations with other strategic areas retrieved from the Guide to Developing a National Cybersecurity Strategy published by International Telecommunications Union in 2021.

Keywords: *cybersecurity, strategy, ITU, USA, UK, Spain, Romania*

Introducere

Am pornit cercetarea, de la premisa că securitatea cibernetică este un domeniu care a dobândit o importanță strategică, din ce în ce mai

[*] Asistent universitar, doctorand în cadrul Școlii Doctorale „Informații și Securitate Națională”, Academia Națională de Informații „Mihai Viteazul”, condrut.cristian@animv.eu

ridicată în ultimii ani, având în vedere preocupările statelor pentru elaborarea strategiilor naţionale de securitate cibernetică. Conform *International Telecommunications Union* (ITU), în *Global Cybersecurity Index 2020* (GCI 2020), 127 de state din 194 aveau în vigoare, în 2020, o strategie naţională de securitate cibernetică (i.e. 65%) (ITU Development Sector, 2021, p. p. 9). La nivelul Uniunii Europene (UE) şi *European Free Trade Association* (EFTA) toate cele 31 de state, 27 membre UE şi 4 membre ETFA, au în vigoare o strategie naţională de securitate cibernetică (ENISA, s.a.). De asemenea, tematicile existente în cadrul strategiilor naţionale de securitate cibernetică sunt extrem de diversificate, Agenţia Europeană de Securitate Cibernetică (ENISA) identificând 21 de categorii de obiective strategice de securitate cibernetică în cadrul acestor documente (ENISA, s.a.), iar ITU, în *Guide to Developing a National Cybersecurity Strategy*, 7 arii strategice de securitate cibernetică: guvernanţă; management al riscului; pregătire şi reziliență; infrastructuri critice şi servicii esenţiale; capabilitate, capacitate şi consolidarea conştientizării; legislaţie şi reglementare şi cooperare internaţională (ITU, 2021, pg. pp. 2-3).

Aceste aspecte ne determină să investigăm aprofundat strategii naţionale de securitate cibernetică, în scopul identificării modului în care securitatea cibernetică este reflectată la nivel strategic, ghidaţi de întrebarea: *Cum este reflectată securitatea cibernetică la nivel strategic prin raportare la ariile strategice prezentate în Guide to Developing a National Cybersecurity Strategy, elaborat de ITU?* Alegerea acestei lucrări drept referenţial este justificată, pe de o parte, de nivelul ridicat de autoritate al emitentului său – ITU este organism internaţional specializat în domeniul comunicaţiilor electronice, parte a Organizaţiei Naţiunilor Unite –, iar pe de altă parte, prin structura şi conţinutul ei, explicând detaliat modul în care statele ar trebui să elaboreze strategiile naţionale de securitate cibernetică.

Obiectivul de cercetare, pe care ni-l propunem, este identificarea celor mai importante arii strategice de securitate cibernetică şi a conexiunilor dintre acestea, în cadrul strategiilor naţionale de securitate cibernetică selectate. Modul în care, vom selecta strategiile naţionale de securitate cibernetică incluse în demersul de cercetare este explicat în secţiunea *metodologie*. Pentru a satisface obiectivul de cercetare, vom aplica metodele analizei calitative de conţinut şi analizei de frecvenţă şi vom utiliza aplicaţia software MAXQDA 2022. În această lucrare vom prezenta rezultatele cercetării noastre, prin respectarea următoarei structuri: *metodologie*, *rezultate*, *interpretări* şi *concluzii*.

Metodologie

Vom aplica metoda analizei calitative de conţinut în maniera etapizată descrisă de Denscombe în *The Good Research Guide*: eşantionare, alegerea unei unităţi de analiză, dezvoltarea unor categorii relevante pentru analizarea datelor, codarea unităţilor în acord cu categoriile alese, analizarea frecvenţei unităţilor de analiză şi a conexiunilor dintre acestea (Denscombe, 2010, pg. pp. 281-282).

Eşantionarea o vom realiza, prin aplicarea următoarelor criterii de selecţie, pentru strategiile naţionale de securitate cibernetică: 1) să aparţină statelor se află pe primele poziţii în clasamentul GCI 2020 şi să aparţină României; 2) să aparţină statelor membre NATO, având în vedere apartenenţa României la NATO; 3) să fi fost adoptate cu maxim 5 ani în urmă, faţă de perioada de derulare a cercetării[1]; 4) să fie în vigoare la momentul derulării cercetării; 5) să fie publicate în limbile engleză sau română.

Conform GCI 2020, primele 4 poziţii în clasamentul celor mai puternice state, din puncte de vedere al securităţii cibernetice, de la nivel global sunt ocupate de: Statele Unite ale Americii (prima poziţie); Marea Britanie şi Arabia Saudită (poziţia a doua); Estonia (poziţia a treia) şi Coreea de Sud, Singapore şi Spania (poziţia a patra). România ocupă poziţia 62 (ITU Development Sector, 2021, p. pp. 25). Am selectat câte o strategie naţională de securitate cibernetică, pentru fiecare dintre primele poziţii din clasamentul GCI 2020 (i.e. Statele Unite ale Americii, Marea Britanie şi Spania) şi le-am eliminat pe cele emise de state, care nu fac parte din NATO (i.e. Arabia Saudită, Coreea de Sud şi Singapore). Am eliminat şi strategia de securitate cibernetică a Estoniei, deoarece perioada de aplicare a acesteia a fost 2019 – 2022 (i.e. nu îndeplineşte criteriul 2) de selecţie) (MAEC Estonia, 2019, p. pp. 1). De asemenea, am inclus şi Strategia de Securitate Cibernetică a României pentru perioada 2022 – 2027, având în vedere că, pe parcursul cercetării ne-am propus inclusiv investigarea comparativă a aspectelor strategice de securitate cibernetică, de la nivel naţional, cu cele existente în Statele Unite ale Americii, Marea Britanie şi Spania. Am ales ca unitate de analiză paragraful din cadrul documentului de tip strategie naţională de securitate cibernetică, având în vedere că, o astfel de abordare ne-a

[1] Cercetarea a fost derulată în perioada februarie – mai 2023 şi face parte din programul individual de cercetare doctorală al autorului.

permis să identificăm conexiuni între ariile strategice de securitate cibernetică – aspecte prezentate în secțiunile *rezultate* și *interpretări*.

Am extras categoriile din literatura de specialitate, acestea fiind ariile strategice de securitate cibernetică, din cadrul *Guide to Developing a National Cybersecurity Strategy*, elaborat de ITU: guvernanță; management al riscului; pregătire și reziliență; infrastructuri critice și servicii esențiale; capabilitate, capacitate și consolidarea conștientizării; legislație și reglementare și cooperare internațională (2021, pg. pp. 2-3). Procesul de codare a fost realizat în acord cu cele 7 categorii alese și am utilizat funcțiile aplicației software MAXQDA 2022. Pentru analizarea frecvențelor categoriilor și a conexiunilor dintre acestea am utilizat funcția *Code Frequencies*[2], respectiv *Code Relations Browser*[3]. În ceea ce privește conexiunile, vom utiliza tipul de analiză de intersecție a codurilor (i.e. în cazul cercetării noastre – categoriilor) dintr-un segment (i.e. în cazul cercetării noastre – un paragraf). Acest tip de analiză este cel mai relevant pentru cercetarea noastră, având în vedere că, documentele strategice de securitate cibernetică tratează transversal arii strategice de la nivel național, conexându-le în cele mai multe situații în cadrul aceluiași paragraf.

Rezultate

În continuare vom prezenta rezultatele cercetării noastre după cum urmează: frecvența fiecăreia dintre cele 7 categorii în strategiile naționale de securitate cibernetică în *Figura 1* (vezi mai jos); frecvența tuturor corelațiilor dintre categorii în *Figura 2* (vezi mai jos); frecvența celor mai importante 10 corelații dintre categorii, în *Tabelul 1* (vezi mai jos).

[2]Mai multe informații referitoare la această funcție se regăsesc la https://www.maxqda.com/help-mx20/statistics-and-graphics-functions/code-frequencies, accesată la data de 12.05.2023.

[3] Mai multe informații referitoare la această funcție se regăsesc la https://www.maxqda.com/help-mx20/visual-tools/code-relations-browser-visualizing-overlapping-codes, accesată la data de 12.05.2023.

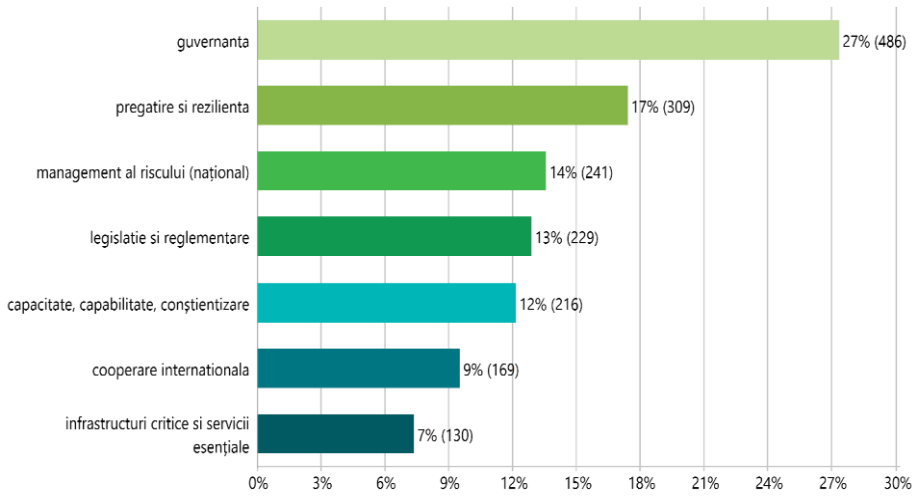

Figura 1: Frecvenţa categoriilor, exprimată procentual şi numeric. Figura a fost generată prin utilizarea funcţiei *code frequencies* a aplicaţiei software MAXQDA 2022.

Prin codarea celor patru strategii de securitate cibernetică alese (i.e. Statele Unite ale Americii, Marea Britanie, Spania şi România) şi analizarea frecvenţei de apariţie a categoriilor am obţinut o listă, ordonată descrescător, a ariilor strategice de securitate cibernetică, exprimată în valori procentuale şi numerice. Această clasificare furnizează o parte din răspunsul aşteptat pentru întrebarea de cercetare formulată, urmând ca, în secţiunea *Interpretări* să aprofundăm analiza rezultatului obţinut.

Guvernanţa de securitate cibernetică se clasează pe prima poziţie în graficul din *Figura 1* (vezi mai sus), această categorie fiind utilizată pentru a coda 486 de segmente sau 27% din totalitatea segmentelor codate, în cele 4 strategii naţionale de securitate cibernetică analizate. Pe cea de-a doua poziţie se clasează *pregătirea şi reziliența* cu 309 segmente codate sau 17% din totalitatea segmentelor codate. Următoarele rezultate pot fi grupate, din punct de vedere numeric, în două intervale, diferenţa dintre cele două capete ale intervalelor fiind de exact 2%:

Intervalul α – (12%; 14%) – este compus din categoriile de *management al riscului* de securitate cibernetică, 241 de segmente codate sau 14%, *legislaţie şi reglementare*, 229 de segmente codate sau 13% şi *capacitate, capabilitate şi conştientizare*, 216 segmente codate sau 12% din totalul segmentelor codate.

Intervalul β – (7%; 9%) – este compus din categoriile de *cooperare internațională*, 169 de segmente codate sau 9% și infrastructuri critice și servicii esențiale, 130 de segmente codate cu 7%.

Code System	guvern...	manag...	infrastr...	pregat...	capaci...	legisla...	coope...
guvernanta		137	67	183	120	128	87
management al riscului (național)	137		43	101	39	58	29
infrastructuri critice si servicii esențiale	67	43		66	20	50	16
pregatire si rezilienta	183	101	66		75	98	64
capacitate, capabilitate, conștientizare	120	39	20	75		43	36
legislatie si reglementare	128	58	50	98	43		54
cooperare internationala	87	29	16	64	36	54	
Σ SUM	722	407	262	587	333	431	286

Figura 2: Matricea de corelație a categoriilor, exprimată numeric. Figura a fost generată prin utilizarea funcției *code frequencies* a aplicației software MAXQDA 2022.

Rezultatele prezentate în *Figura 2* (vezi mai sus) completează răspunsul la întrebarea de cercetare având în vedere că reflectă modul în care ariile strategice de securitate cibernetice sunt corelate între ele în cadrul strategiilor naționale de securitate cibernetică. În ceea ce privește matricea de ocurență, aceasta este de tip simetric (i.e. o valoare aleasă arbitrar de pe linia *i* și coloana *j* este egală cu o valoare aleasă arbitrar de pe linia *j* și coloana *i*), ceea ce presupune că indiferent de modul în care alegem să citim un anumit rezultat (ex. corelația dintre *pregătire și reziliență* cu *legislație și reglementare* sau corelația dintre *legislație și reglementare* și *pregătire și reziliență*) acesta va fi același prin raportare la diagonala matricei. Pentru a facilita interpretările cu privire la cele mai importante corelații dintre categorii (i.e. ariile strategice de securitate cibernetică), vom prezenta cele mai frecvente 10 rezultatele din *Figura 2* în *Tabelul 1* (vezi mai jos).

Tabelul 1: Cele mai frecvente 10 corelaţii ale ariilor strategice extrase din *Figura 1*.

Nr.crt.	Intersecţie	Valoare
1.	guvernanţă – pregătire şi reziliență	183
2.	guvernanţă – management al riscului (național)	137
3.	guvernanţă – legislaţie şi reglementare	128
4.	guvernanţă – capacitate, capabilitate şi conştientizare	120
5.	management al riscului (național) – pregătire şi reziliență	101
6.	pregătire şi reziliență – legislaţie şi reglementare	98
7.	guvernanţă – cooperare internaţională	87
8.	pregătire şi reziliență – capacitate, capabilitate şi conştientizare	75
9.	guvernanţă – infrastructuri critice şi servicii esenţiale	67
10.	pregătire şi reziliență – infrastructuri critice şi servicii esenţiale	66

Interpretări

În continuare ne propunem să discutăm rezultatele prezentate în *Figura 1* (vezi mai sus) şi în *Tabelul 1* (vezi mai sus). Datele prezentate în *Figura 1*, frecvenţele exprimate procentual şi numeric ale ariilor strategice de securitate cibernetică, ne ajută să atingem o parte din obiectivul de cercetare pe care ni l-am propus – identificarea celor mai importante arii strategice de securitate cibernetică. Datele prezentate în *Tabelul 1*, cele mai frecvente corelaţii ale ariilor strategice de securitate cibernetică, ne ajută să atingem şi al doilea aspect al obiectivului de cercetare – identificarea conexiunilor dintre ariile strategice de securitate cibernetică. În cele ce urmează, vom discuta cele 7 arii strategice cuprinse în Ghidul ITU, în ordinea scorurilor frecvenţelor obţinute în cadrul cercetării noastre (vezi *Figura 1*).

Guvernanţă

Guvernanţa de securitate cibernetică face referire la modul în care, statul consolidează rezilienţa cibernetică şi reduce riscurile asociate, prin definirea de obiective strategice şi desemnarea de autorităţi responsabile (ITU, 2021, p. pp. 34). De asemenea, aria

strategică a guvernanței de securitate cibernetică include următoarele dimensiuni strategice: asigurarea celui mai ridicat nivel de suport; stabilirea unei autorități competente de securitate cibernetică; asigurarea cooperării intra-guvernamentale; asigurarea cooperării inter-sectoriale; alocarea de buget și resurse; dezvoltarea unui plan de implementare (ITU, 2021, pg. pp. 2-3). Guvernanța de securitate cibernetică a obținut cel mai ridicat scor în analiza noastră – 27% ,din totalitatea segmentelor codate. Semnificația acestui rezultat este că, cele 4 state analizate prioritizează, din punct de vedere strategic, modul în care este planificat domeniul securității cibernetice la nivel național. În toate cele 4 strategii analizate am putut să observăm, că strategia desemnează o autoritate de securitate cibernetică responsabilă cu implementarea strategiei – *Office of National Cyber Director* (ONCD) în SUA, *National Cyber Security Centre* (NCSC) în Marea Britanie, *National Cybersecurity Council* (NCC) în Spania și Directoratul Național de Securitate Cibernetică în România (DNSC). De asemenea, toate cele 4 state încurajează dezvoltarea unui plan de implementare și alocarea de resurse, pentru domeniul securității cibernetice, ceea ce relevă că, cele 4 țări planifică la nivel strategic implementarea de proiecte strategice în domeniu. Cooperarea inter-guvernamentală și cooperarea intra-guvernamentală sunt dimensiuni strategice regăsite de asemenea în toate cele 4 strategii, ceea ce înseamnă, pe de o parte, că responsabilitățile în domeniu sunt alocate unor instituții publice diferite, care trebuie să coopereze pentru a duce la îndeplinire obiectivele strategice, iar pe de altă parte, că îndeplinirea obiectivelor strategice de securitate cibernetică este dependentă de implicarea unui număr cât mai mare de actori societali. Singura strategie de securitate cibernetică, în care nu există o secțiune dedicată sprijinului oferit de un înalt oficial al statului, este cea a României. Strategiile SUA, Marea Britanie și Spania debutează cu o astfel de secțiune.

Importanța guvernanței de securitate cibernetică este reliefată și de rezultatele prezentate în *Tabelul 1,* având în vedere că, această arie strategică de securitate cibernetică se corelează puternic (i.e. 6 din primele 10 poziții ale corelațiilor), cu toate celelalte incluse în analiza noastră, pe pozițiile: 1 cu *pregătire și reziliență*; 2 cu *management al riscului;* 3 cu *legislație și reglementare;* 4 cu *capacitate, capabilitate și conștientizare*; 7 cu *cooperare internațională*; 9 cu *infrastructuri critice și servicii esențiale*.

Pregătire şi reziliență

Pregătirea şi reziliența de securitate cibernetică se referă la bune-practici necesar a fi implementate la nivel naţional, pentru stabilirea şi consolidarea unor capabilităţi eficiente de securitate cibernetică, necesare pentru pregătirea, prevenirea, detectarea, diminuarea efectelor şi răspunsul la incidente grave de securitate cibernetică (ITU, 2021, p. p. 39). Dimensiunile strategice asociate de ITU ariei pregătire şi reziliență sunt: stabilirea de capabilităţi de răspuns la incidente de securitate cibernetică, stabilirea de planuri de contingență şi management al crizelor, promovarea schimbului de informaţii, derularea de exerciţii de securitate cibernetică şi stabilirea impactului şi severităţii incidentelor de securitate cibernetică (ITU, 2021, pg. pp. 2-3). Singurul domeniu strategic, care nu îşi găseşte corespondent în toate cele 4 strategii analizate, este cel al exerciţiilor de securitate cibernetică, acesta fiind abordat de Marea Britanie, Spania şi România, ceea ce indică o omogenitate în abordarea statelor europene, din eşantionul nostru. Stabilirea capabilităţilor de răspuns la incidente de securitate cibernetică este tratată în toate cele 4 strategii analizate, având în vedere că, desemnează instituţii de tip *Computer Emergency Response Team* (CERT) responsabile de acest domeniu: SUA – *Cybersecurity & Infrastructure Security Agency* (CISA); Marea Britanie – *National Cyber Security Centre* (NCSC); România – Directoratul Naţional de Securitate Cibernetică (DNSC); Spania – Institutul Naţional de Securitate (INCIBE). Stabilirea de planuri de contingență şi management al crizelor îşi găseşte corespondent în toate cele 4 strategii, având în vedere necesitatea de reacţie post-incident de securitate cibernetică. Lipsa unei astfel de reacţii, poate conduce la amplificarea consecinţelor iniţiale ale unui incident de securitate cibernetică şi la diversificarea obiectelor de securitate afectate. Practica schimbului de informaţii este recunoscută ca fiind benefică, la nivelul tuturor celor 4 state, constatându-se ca fiind, în general, abordată prin referiri la operatori de infrastructuri critice şi servici esenţiale, la industria privată de securitate cibernetică şi la platforme naţionale, create special în acest scop. O altă practică inclusă în aria strategică *pregătire şi reziliență* este cea a stabilirii impactului şi severităţii incidentelor de securitate cibernetică, abordarea celor 4 state fiind asociată unor linii de acţiune clare, ce presupun reorganizarea unor autorităţi în domeniu sau realizarea unor metodologii de evaluare a incidentelor de securitate.

Corelaţiile cele mai frecvente ale ariei strategice *pregătire şi reziliență*, în conformitate cu *Tabelul 1*, sunt cu: *guvernanța*, pe poziţia 1;

management al riscului, pe poziția 5; *legislație și reglementare*, pe poziția 6; *capacitate, capabilitate și conștientizare*, pe poziția 8; *infrastructuri critice și servicii esențiale*, pe poziția 10. Astfel, 5 din primele 10 cele mai frecvente corelații între arii strategice de securitate cibernetică includ *pregătirea și reziliența*. Acest aspect relevă faptul că, cele 4 state sunt preocupate cu sprijinirea, din punct de vedere strategic, a demersurilor care vizează consolidarea rezilienței cibernetice naționale, fiind astfel, în acord cu o serie de documente elaborate la nivelul NATO, precum *Rezoluția 475/2022 privind dezvoltarea rezilienței cibernetice în societățile aliate*[4] sau cu *Cyber Defence Pledge*[5] adoptată la Summitul de la Varșovia în 2016. Reținem faptul că, cele 4 strategii corelează puternic *reziliența și pregătirea* cu *guvernanța* de securitate cibernetică, ceea ce înseamnă, că *pregătirea și reziliența* este tema prioritară pe agenda strategică a celor 4 state. De asemenea, *pregătirea și reziliența* este corelată puternic și cu *managementul riscului*, aspect care ne relevă, că măsurile de management al riscului cibernetic susțin capacitatea de reziliență cibernetică a statului și că, un management mai eficient al riscurilor de securitate cibernetică se realizează prin asumarea obiectivului de consolidare a rezilienței cibernetice de la nivel național.

Management al riscului

Aria strategică a *managementului riscului de securitate cibernetică* cuprinde bunele-practici necesar a fi implementate, pentru eficientizarea proceselor de management al riscului: realizarea de evaluări de securitate cibernetică, definirea unei abordări de management al riscului, identificarea unei metodologii comune de management al riscului, dezvoltarea unor profiluri de risc cibernetic sau stabilirea de politici de securitate cibernetică (ITU, 2021, pg. pp. 37-38). Singura practică de management al riscului, care nu este abordată în toate cele 4 strategii, este identificarea unei metodologii comune de management al riscului de securitate cibernetică, în strategia Spaniei neexistând referiri la aceasta. Practica evaluărilor de securitate cibernetică este încurajată de toate cele 4, preponderent, prin raportare la amenințările curente de securitate cibernetică (ex. spionajul cibernetic, sabotajul cibernetic,

[4] Disponibilă în 15.05.2023 pe https://www.nato-pa.int/download-file?filename=/sites/default/files/2022-11/RESOLUTION%20475%20%20ENHANCING%20THE%20CYBER%20RESILIENCE%20OF%20ALLIED%20SOCIETIES.pdf

[5] Disponibilă în 15.05.2023 pe https://www.nato.int/cps/en/natohq/official_texts_133177.htm

criminalitatea cibernetică, hacktivismul sau dezinformarea şi propaganda prin mijloace cibernetice). Definirea unei abordări de management al riscului se reflectă în cele 4 strategii analizate prin elemente, precum dezvoltarea de tehnologii pentru detectarea ameninţărilor de securitate cibernetică, dezvoltarea capabilităţilor de colectare şi analizare a informaţiilor de securitate cibernetică sau dezvoltarea parteneriatelor, între mediul public şi cel privat. Stabilirea profilurilor de risc este abordată în cele 4 strategii de securitate cibernetică, prin încurajarea realizării unor evaluări de risc de securitate cibernetică, pentru sectoarele de activitate ce administrează şi operează infrastructuri cibernetice critice. Politicile de securitate cibernetică trebuie să fie definite la toate nivelurile domeniului securităţii cibernetice (i.e. strategic, operaţional şi tactic) (ITU, 2021, p. p. 38). Toate cele 4 state analizate definesc sau încurajează demersuri menite să consolideze aplicarea de politici de securitate cibernetică, câteva exemple în acest sens fiind: crearea, diseminarea şi aplicarea de standarde de securitate cibernetică; acordarea de stimulente financiare companiilor care implementează standarde de securitate cibernetică; reconsiderarea politicii de resurse umane.

Corelaţiile ariei strategice *management al riscului de securitate cibernetică*, în conformitate cu *Tabelul 1* (vezi mai sus), sunt cu: *guvernanţa*, pe poziţia 2; *pregătirea şi reziliența*, pe poziţia 5. Astfel, managementul riscului de securitate cibernetică reprezintă o arie strategică, necesar a fi coordonată de la nivelul autorităţilor publice cu responsabilităţi de ordin tehnic (ex. organismele de tip CERT) sau de la nivelul celor cu responsabilităţi non-tehnice (ex. instituţii din domeniul afacerilor externe, servicii de informaţii), fiecare dintre aceste autorităţi contribuind, conform competenţelor legale, la definirea unui cadru naţional în materie. Menţinem concluziile referitoare la corelaţia cu aria strategică *pregătire şi reziliență*, în ceea ce priveşte modul în care cele două arii strategice se influenţează reciproc.

Legislaţie şi reglementare

Legislaţia şi reglementarea de securitate cibernetică se referă la modul în care, statele trebuie să îşi construiască elemente de cadru legislativ, în ceea ce priveşte protejarea societăţii împotriva criminalităţii cibernetice şi promovarea unui spaţiu cibernetic sigur (ITU, 2021, p. pp. 47). Domeniile strategice incluse în aria *legislaţie şi reglementare* sunt: stabilirea unui cadrul legislativ naţional de securitate cibernetică; stabilirea unui cadru legal naţional pentru criminalitate cibernetică şi

pentru dovezi digitale; recunoașterea și protejarea drepturilor și libertăților omului; crearea unor mecanisme de control; stabilirea de procese inter-organizaționale; sprijinirea cooperării internaționale pentru combaterea amenințărilor și criminalității cibernetice (ITU, 2021, pg. pp. 47-50). Toate cele 4 state abordează, în proporții variabile, fiecare domeniu strategic inclus în aria *legilsație și reglemetare*. Stabilirea unui cadru legal de securitate cibernetică este relaționată în cele 4 documente analizate, cu existența sau necesitatea de adoptare a unui cadru normativ, care să reglementeze responsabilitățile instituționale în domeniul securității cibernetice. De asemenea, la nivelul statelor europene analizate, sunt realizate referiri cu privire implementarea Directivei NIS – *nr. 1148 din 2016 privind măsurile pentru un nivel ridicat de securitate a rețelelor și sistemelor informatice din Uniune*[6]. În ceea ce privește stabilirea unui cadru legal de criminalitate cibernetică și dovezi digitale, cele 4 state fac referiri la elemente, precum: tragerea la răspundere a criminalilor cibernetici, prin adoptarea sau actualizarea unor elemente legislative judiciare (ex. în Marea Britanie se propune amendarea *Computer Misuse Act* și *Proceeds of Crime Act 2002*) și implementarea de standarde legale de combatere a utilizării în scopuri ilicite a criptomonedelor. În ceea ce privește protejarea drepturilor omului, toate cele 4 state recunosc importanța acestui demers și încurajează comportamentul responsabil al statelor în spațiul cibernetic și respectarea legislației internaționale. Domeniul mecanismelor de control este reliefat în cele 4 strategii, prin: necesitatea de adoptare a unor standarde de natură tehnică și non-tehnică; definirea de criterii de încredere pentru entitățile care furnizează echipamente IT&C; criterii de securitate cibernetică specifice fiecărui sector critic de activitate. Practica stabilirii proceselor inter-organizaționale este reliefată în strategiile analizate, prin elemente precum: crearea de mecanisme de cooperare interinstituțională, pentru afirmarea de poziții naționale și pentru consultanță în domeniul securității cibernetice; dezvoltarea unor proceduri de atribuire a atacurilor cibernetice; crearea de mecanisme de raportare a incidentelor de securitate cibernetică. Cooperarea internațională pentru combaterea criminalității cibernetice este un domeniu exprimat în cele 4 strategii analizate, preponderent, prin raportare la eforturile internaționale de diminuare a amenințărilor de criminalitate cibernetică (ex. acțiuni realizate în cooperare, de

[6] Disponibilă la https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148, la data de 16 mai 2023.

organizaţiile de aplicare a legii; iniţiative internaţionale comune de combatere a unor fenomene, manifestate în spaţiul cibernetic).

Corelaţiile ariei strategice *legislaţie şi reglementare*, în conformitate cu *Tabelul 1* (vezi mai sus), sunt cu *guvernanţa*, la poziţia 3 şi cu *pregătirea şi reziliența,* la poziţia 6. Corelaţia puternică a ariei strategice *legislaţie şi reglementare* cu *guvernanţa* este explicată prin faptul că, statul este emitentul cadrului legislativ naţional pe orice subiect, nu doar pe cel de securitate cibernetică. De asemenea, având în vedere, că activităţile de criminalitate cibernetică intră sub incidenţa legislaţiei penale, în forme şi proporţii variate de definire, şi că pentru a combate aceste activităţi este necesară o bună cooperare intra-guvernamentală şi inter-sectorială (i.e. domenii strategice de guvernanţă), corelaţia puternică, dintre *guvernanţă* şi *legislaţie şi reglementare* este un rezultat normal. Intensitatea celei de-a doua corelaţii (i.e. *legislaţie şi reglementare* & *pregătire şi reziliență*) ne reliefează faptul că, pentru dezvoltarea rezilienţei cibernetice la nivel naţional, este nevoie de adoptarea unui cadru legislativ, care să ofere statului mecanisme rapide de acţiune, prin definirea de responsabilităţi instituţionale, stabilirea unor facilităţi fiscale şi sancţionarea, pe căi civile şi penale, a entităţilor care nu se supun legislaţiei în vigoare.

Capacitate, capabilitate şi conştientizare

Capacitatea, capabilitatea şi conştientizarea este o arie de securitate cibernetică ce tratează atât provocările asociate consolidării capacităţii şi capabilităţii tehnologice şi umane, cât şi provocările conexate creşterii nivelului de conştientizare a domeniului securităţii cibernetice în rândul entităţilor cheie, precum instituţii publice, cetăţeni şi organizaţii private (ITU, 2021, p. p. 44). Domeniile de interes din această arie strategică sunt: planificarea strategică; dezvoltarea *curriculei* de securitate cibernetică; stimularea dezvoltării capacităţii şi a formării profesionale; implementarea de programe coordonate de consolidare a conştientizării; consolidarea cercetării, inovării şi dezvoltării de securitate cibernetică; implementarea de programe pentru sectoarele şi grupurile vulnerabile (ITU, 2021, pg. pp. 44-48). Planificarea strategică nu a fost abordată în toate cele 4 strategii analizate, având în vedere, că Spania nu desemnează entităţi responsabile pentru această arie strategică. De asemenea, implementarea de programe pentru sectoarele şi categoriile vulnerabile este abordată doar în strategiile SUA, Marii Britanii şi Spaniei, fiind prezentate o serie de iniţiative deja existente în acest domeniu (ex.

dezvoltarea de competențe de securitate cibernetică pentru tineri; diversificarea incluziunii forței de muncă de securitate cibernetică pentru categorii, precum cea a imigranților și a persoanelor cu handicap) și necesitatea de implementare a unora noi. Domeniul dezvoltării unor cadre curriculare de securitate cibernetică este abordat în toate cele 4 strategii, fiind corelat cu măsuri, precum: acordarea de burse educaționale de securitate cibernetică; includerea în programele școlare și universitare a unor subiecte sau discipline de securitate cibernetică; organizarea de evenimente educaționale de securitate cibernetică (ex. tabere de pregătire). Stimularea capacității și formării profesionale de securitate cibernetică este reliefată prin măsuri, precum: organizarea de cursuri de specializare pentru profesioniștii în securitate cibernetică, inclusiv în parteneriat public-privat; dezvoltarea de centre de instruire naționale de securitate cibernetică; aplicarea unor cadre de competență de securitate cibernetică deja existente la nivel național. Domeniul conștientizării amenințării de securitate cibernetică este transpus în cele 4 strategii, prin necesitatea de informare a societății civile, derularea de programe educaționale, în scopul consolidării igienei de securitate cibernetică sau prin derularea de campanii specializate, pentru sectoarele critice de activitate. Consolidarea cercetării, inovării și dezvoltării de securitate cibernetică este percepută în cele 4 strategii, în raport cu reziliența cibernetică. Astfel, programele de cercetare în domeniul securității cibernetice trebuie să contribuie, pe de o parte la dezvoltarea tehnologiilor defensive de securitate cibernetică, iar pe de altă parte, să mențină avantajul competitiv al statului. De asemenea, cercetarea de securitate cibernetică este dependentă de o bună cooperare între mediul public, privat și academic, acest aspect fiind surprins în toate cele 4 strategii.

Corelațiile ariei strategice *capacitate, capabilitate și conștientizare*, în conformitate cu *Tabelul 1,* sunt cu: *guvernanță*, pe poziția 4 și *pregătire și reziliență*, pe poziția 8. Prima corelație (i.e. *guvernanță* & *capacitate, capabilitate și conștientizare*) se explică, prin implicarea autorităților publice în demersuri, care vizează dezvoltarea acestei arii strategice. Un domeniu extrem de important în acest context este cel al cooperării inter-sectoriale (i.e. inclus în aria strategică a *guvernanței*) având în vedere că, efectele consolidării capacității, capabilității și conștientizării de securitate cibernetică se resimt la nivelul întregii societăți. Spre exemplu, în ceea ce privește *dezvoltarea curriculei de securitate cibernetică*, este necesară implicarea autorităților publice, cu responsabilități în domeniul educațional și de securitate

cibernetică, pentru a asigura cadrul necesar formării viitorilor şi actualilor specialişti de securitate cibernetică. Efectele existenţei unui cadru coerent de educaţie de securitate cibernetică sunt resimţite la nivelul întregii societăţi, având în vedere că, specialiştii care au parcurs procese formative instituţionalizate, constituie masa critică de specialişti în domeniu, care îşi desfăşoară activitatea în diverse sectoare de activitate, indiferent dacă luăm în considerare mediul public, privat sau academic. Corelaţia dintre *capacitate, capabilitate şi conştientizare* & *pregătire şi rezilienţă* are un rol extrem de important în dezvoltarea domeniului securităţii cibernetice, pe termen mediu şi lung. Având în vedere că, ITU defineşte reziliența inclusiv prin raportare la pregătire (ITU, 2021, p. pp. 39), consolidarea capacităţii resursei umane, ce îşi desfăşoară activitatea în domeniul securităţii cibernetice, devine o misiune extrem de importantă pentru state. Cu toate acestea, putem identifica şi alte sinergii între cele două arii strategice, una dintre ele fiind cea a consolidării capacităţii de reacţie la incidente de securitate cibernetică (i.e. domeniu inclus în aria strategică *pregătire şi rezilienţă*) şi consolidarea cercetării, dezvoltării şi inovării (i.e. domeniu inclus în aria strategică interpretată în acest paragraf). Lipsa dezvoltării de tehnologii actuale de securitate cibernetică şi inacţiunea statului, pentru a valorifica aceste tehnologii, poate diminua capacitatea de răspuns la incidente, având în vedere creşterea complexităţii atacurilor cibernetice şi varietatea, din ce în ce mai ridicată, a instrumentelor utilizate de atacatori.

Cooperare internaţională

Aria strategică a cooperării internaţionale este caracterizată, prin angajamentele externe ale unui stat în domeniul securităţii cibernetice, atât la nivel regional, cât şi la nivel internaţional (ITU, 2021, p. pp. 50). Domeniile incluse în această arie strategică sunt: recunoaşterea securităţii cibernetice, ca o componentă a politicii externe; angajarea în discuţii internaţionale şi angajamentul pentru implementare; promovarea cooperării formale şi informale de securitate cibernetică; promovarea consolidării capacităţii de cooperare internaţională (ITU, 2021, pg. pp. 50-53). Securitatea cibernetică, percepută ca o componentă a politicii externe a statului, este o temă abordată în toate cele 4 strategii de securitate cibernetică, în relaţie cu rolul pe care fiecare dintre state doreşte să şi-l asume la nivel internaţional, în următorii ani: Marea Britanie – lider în domeniu şi putere cibernetică globală (HM Government , 2022, p. pp. 11); SUA – putere diplomatică activă, în

domeniul securității cibernetice (The White House, 2023, p. pp. 32); Spania – model de securitate cibernetică (DSN, 2019, p. pp.14); România – lider regional în domeniul securității cibernetice (Guvernul României, 2022, p. pp. 27). Angajarea în discuții internaționale este reliefată, în cele 4 strategii de securitate cibernetică, prin referiri la apartenența fiecăruia dintre state la diferite organizații (ex. ONU, NATO, UE, OSCE) și inițiative internaționale (ex. *Counter-Ransomware Initiative*) în domeniul securității cibernetice. Promovarea cooperării formale și informale, în domeniul securității cibernetice, este identificată în cele 4 strategii, prin referiri la: dezvoltarea de mecanisme de cooperare în cadrul organizațiilor internaționale; valorificarea prezenței globale a unor companii relevante de securitate cibernetică la nivel național; valorificarea prezenței unor organisme regionale și internaționale de securitate cibernetică la nivel național (ex. Centru European de Competențe de Securitate Cibernetică[7] are sediul în București); influențarea discuțiilor referitoare la standarde, asociate unor tehnologii cheie, din domeniul securității cibernetice (ex. 5G). Promovarea consolidării capacității de cooperare internațională este abordată, în relație cu dezvoltarea competențelor cibernetice de politică externă ale celor 4 state.

Singura corelație a ariei strategice *cooperare internațională*, conform *Tabelului 1*, este cu aria strategică a *guvernanței*, corelație aflată pe poziția a 7-a. Având în vedere, că aria strategică a *cooperării internaționale* de securitate cibernetică determină responsabilități doar pentru câteva tipuri de instituții publice (i.e. cele din domeniul afacerilor externe), nu este surprinzător faptul că, aceasta o obținut doar o singură corelație, în clasamentul primelor 10 (vezi *Tabelul 1*).

Infrastructuri critice și servicii esențiale

Aria strategică a *infrastructurilor critice și serviciilor esențiale* se referă la bunele-practici, asociate protejării acestor infrastructuri și a consolidării rezilienței acestora (ITU, 2021, p. pp. 41). Domeniile incluse în această arie strategică sunt: stabilirea unei abordări de management al riscului; adoptarea unui model de guvernanță; definirea unor standarde minime de securitate cibernetică; utilizarea pârghiilor de piață; stabilirea de parteneriate public private (ITU, 2021, pg. pp. 41-44). Domeniul stabilirii unei abordări de management al riscului este regăsit

[7] Disponibil la https://cybersecurity-centre.europa.eu/news/eccc-opens-its-doors-bucharest-2023-05-09_en, la data de 16.05.2023.

în toate cele 4 strategii analizate, fiind reliefat prin elemente, precum: elaborarea de proceduri de audit de securitate cibernetică, în conformitate cu cadrul legislativ în domeniu (i.e. pentru statele europene, legislaţia de transpunere a Directivei NIS, iar pentru SUA, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* şi *Executive Order on Improving the Nation's Cybersecurity* (The White House, 2023, p. pp. 6)), consolidarea rezilienţei infrastructurilor critice printr-o abordare de tip *zero trust*[8] sau implementarea obligativităţii de raportare a incidentelor de securitate cibernetică. Domeniul adoptării unui model de guvernanţă pentru securitatea cibernetică a infrastructurilor critice şi serviciilor esenţiale se regăseşte în strategiile SUA, Marii Britanii şi Spaniei, prin elemente, precum: desemnarea de autorităţi publice naţionale în materie; stabilirea de mecanisme de cooperare intra-guvernamentală şi inter-sectorială, pentru rezolvarea incidentelor de securitate cibernetică. Definirea de standarde minimale de securitate cibernetică se regăseşte în toate cele 4 strategii analizate şi este reliefată prin elemente, precum: transpunerea în legislaţia naţională a Directivei NIS (i.e. pentru statele europene); adaptarea criteriilor în funcţie de sectorul de activitate; furnizarea de sprijin pentru administratorii infrastructurilor critice în implementarea standardelor, inclusiv prin elaborarea de proceduri şi ghiduri de bune-practici în domeniu. Domeniul utilizării pârghiilor de piaţă a fost abordat doar în strategiile Marii Britanii şi Spaniei, într-o manieră extrem de sumară, principalele referiri fiind la modalitatea în care, statul trebuie să valorifice relaţionarea cu principalii actori economici din piaţa de securitate cibernetică, pentru asigurarea securităţii cibernetice. Practica parteneriatelor public-private, pentru asigurarea securităţii cibernetice a infrastructurilor critice este încurajată doar în strategiile SUA şi Marii Britanii.

Corelaţiile ariei strategice *infrastructuri critice şi servicii esenţiale*, în conformitate cu *Tabelul 1* (vezi mai sus), se realizează cu: *guvernanţa*, la poziţia 9 şi cu *pregătirea şi reziliența* la poziţia 10. Niciuna, dintre cele două corelaţii, nu ocupă una dintre primele poziţii din *Tabelul 1.* Din punct de vedere cantitativ, acest aspect se poate explica, prin frecvenţa scăzută a segmentelor incluse în aria strategică *infrastructuri critice şi*

[8] Cadru de securitate cibernetică în care toţi utilizatorii unei reţele, indiferent de faptul că îşi desfăşoară activitatea în interiorul sau în afara ei, trebuie să fie validaţi din prin proceduri de autentificare, autorizare şi auditare de securitate. Mai multe informaţii despre *zero trust* se regăsesc la https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/, disponibil la data de 17.05.2023.

servicii esențiale (vezi *Figura 1*). Din punct de vedere calitativ, aria infrastructurilor critice și serviciilor esențiale desemnează doar o parte dintre infrastructurile cibernetice, existente la nivelul unui stat, existând totodată reglementări, metodologii și proceduri diferite pentru aceste tipuri de infrastructuri cibernetice. Aceste aspecte izolează aria strategică a *infrastructurilor critice și serviciilor esențiale*, de celelalte arii existente și determină, în consecință, un număr mai scăzut de corelații ale acesteia.

Concluzii

Pornind de la întrebarea de cercetare – *Cum este reflectată securitatea cibernetică la nivel strategic prin raportare la ariile strategice prezentate în Guide to Developing a National Cybersecurity Strategy, elaborat de ITU?* – considerăm că, am reușit să atingem obiectivul de cercetare pe care ni l-am propus: *identificarea celor mai importante arii strategice de securitate cibernetică și a conexiunilor dintre acestea, în cadrul strategiilor naționale de securitate cibernetică selectate*, respectiv, cele mai importante arii strategice de securitate cibernetică identificate de noi sunt *guvernanța*, cu 27% din totalitatea segmentelor codate și *pregătirea și reziliența*, cu 17% din totalitatea segmentelor codate. Acest aspect ne indică faptul că, statele acordă o importanță deosebită aspectelor ce țin de guvernanța de securitate cibernetică, statul fiind principalul actor relevant în domeniu, cu toate că, se constată la nivel strategic, necesitatea adoptării unei viziuni de tip *whole-of-society*. Cu toate acestea, pentru atingerea obiectivelor strategice de securitate cibernetică este necesară implicarea unei varietăți cât mai ridicate de actori de la nivelul societății, având în vedere că, guvernanța de securitate cibernetică include și domeniul cooperării inter-sectoriale. Un alt aspect important, de reținut, este dat de interpretarea rezultatului obținut de aria strategică *pregătire și reziliență*: statele conștientizează importanța adoptării de măsuri strategice, menită să consolideze reziliența cibernetică națională. În ceea ce privește corelațiile, constatăm că, *guvernanța* de securitate cibernetică realizează cele mai multe astfel de legături cu celelalte arii strategice, aspect care, completează concluziile ce rezultă din interpretarea rezultatelor, pe care fiecare arie de securitate cibernetică le-a obținut.

În ceea ce privește limitările, considerăm că, cercetarea prezentă ar fi putut obține o relevanță mult mai accentuată, în situația în care, am fi selectat un număr mai ridicat de strategii de securitate cibernetică, pentru a avea o reprezentativitate cât mai bună a documentelor de acest

fel. Astfel, considerăm că, o viitoare direcție de cercetare necesar a fi aprofundată este cea a realizării unui studiu, asupra unui număr reprezentativ de strategii de securitate cibernetică, prin aplicarea metodei analizei de conținut.

Bibliografie:

1. Denscombe, M. (2010). The Good Research Guide. Berkshire: Open University Press.

2. DSN. (2019). National Cybersecurity Strategy 2019. Preluat pe Aprilie 24, 2023, de pe DSN: https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr

3. ENISA. (fără an). National Cyber Security Strategies - Interactive Map. Preluat pe Mai 12, 2023, de pe https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

4. Guvernul României. (2022, Ianuarie 3). E-monitor. Preluat pe Aprilie 18, 2023, de pe Monitorul Oficial: https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html

5. HM Government. (2022). National Cyber Strategy 2022. Preluat pe Martie 16, 2023, de pe https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

6. ITU. (2021). Guide to Devepoling a National Cybersecurity Strategy. Preluat pe martie 16, 2023, de pe United Nations: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

7. ITU Development Sector. (2021). Global Cybersecurity Index 2020. Preluat pe Aprilie 6, 2023, de pe ITUPublications: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

8. MAEC Estonia. (2019). Cybersecurity Strategy. Republic of Estonia. Preluat pe Martie 16, 2023, de pe https://www.mkm.ee/media/703/download

9. The White House. (2023, Martie 2). FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. Preluat pe Aprilie 24, 2023, de pe The White House: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Aceasta este a doua ediție a volumului publicat de Academia Națională de Informații „Mihai Viteazul” (ANIMV), care cuprinde lucrările prezentate în cadrul Conferinței Științifice Intelligence și Cultura de Securitate 2023 (ICS2023). Inițiativa ICS2023 continuă să ofere studenților o platformă pentru dialog academic și pentru a împărtăși realizările lor științifice.

Ediția actuală își extinde participarea la un spectru mai larg de contributori, incluzând atât doctoranzi, cât și studenți din programele de master, cu un interes crescut pentru domenii precum intelligence, securitate națională, istorie și relații internaționale.

Organizarea conferinței a fost posibilă datorită eforturilor continue ale doctoranzilor și ale conducătorilor de doctorat din cadrul Școlii Doctorale Informații și Securitate Națională a ANIMV.

Anticipăm cu entuziasm noi discuții și schimburi de idei în viitoarea ediție a conferinței.

EDITURA ANIMV

ISSN 2972-1350
ISSN-L 2971-8139