UNIVERSITATEA „BABEȘ-BOLYAI”
CLUJ-NAPOCA
FACULTATEA DE ISTORIE ȘI FILOSOFIE
ȘCOALA DOCTORALĂ RELAȚII INTERNAȚIONALE ȘI STUDII DE SECURITATE

TEZĂ DE DOCTORAT

- REZUMAT -

Conducător de doctorat:
Prof. Univ. Dr. Adrian Ivan

Student-doctorand:
Sorin Gurzău

Cluj-Napoca
2021

UNIVERSITATEA „BABEȘ-BOLYAI”
CLUJ-NAPOCA
FACULTATEA DE ISTORIE ȘI FILOSOFIE
ȘCOALA DOCTORALĂ RELAȚII INTERNAȚIONALE ȘI STUDII DE SECURITATE

Securitatea cibernetică în secolul XXI. Sustenabilitate în Business Intelligence

Conducător de doctorat:
Prof. Univ. Dr. Adrian Ivan

Student-doctorand:
Sorin Gurzău

2021

CUPRINS

CUVINTE CHEIE: Securitate cibernetică, Guvernanță, Relații internaționale, Diplomație cibernetică, Infrastructuri critice, Strategii de apărare cibernetică, Uniunea Europeană, Organizația Tratatului Atlanticului de Nord, Business Intelligence, Competitive Intelligence, Cyber Intelligence, Principiul precauție, Etica, Globalizarea sănătății publice, Sistemul de sănătate românesc, Modelul ”Swiss Cheese”, Troika erorilor, COVID-19

INTRODUCERE

ARGUMENT ȘI MOTIVAȚIE

Datorită digitalizării extensive, a conectării masive online a populației globale și a deținerii de dispozitive electronice fixe și mobile, tehnologiile dezvoltate aparținând celei de a patra și ulterior a celei de-a cincea revoluții industriale au generat pe lângă avantaje și o serie de consecințe negative printre care și în ceea ce privește securitatea cibernetică, atacurile informatice devenind un pericol real și pentru mediul de afaceri. De altfel, există informații din mediul de afaceri la nivel mondial, care așează atacurile informatice în primele zece cele mai probabile riscuri și cu cel mai mare impact. (WEF 2020 *c*. 60-63).

Referitor la importanța de necontestat a tehnologiei la nivel mondial, guvernarea cibernetică devine un deziderat imperativ, un parteneriat public-privat putând puncta semnificativ în domeniul securității informatice. Pe de altă parte, în contextul golului de guvernanță informatică, discrepanța dintre țintele securității cibernetice proprii și/sau ale partenerilor și dezvoltarea tehnologiei solicită mediul de afaceri la eforturi suplimentare și vitale pentru sustenabilitate în *Business Intelligence*. Din perspectiva securității cibernetice, implicarea majoră a tehnologiei informaționale în toate domeniile de activitate produce schimbarea continuă și rapidă a statusului securității naționale și internaționale, mai ales în cazul infrastructurilor critice (sisteme energetice, de transport, sănătate, aprovizionare cu apă), cu posibil impact asupra relațiilor interstatale (WEF 2020 *c*. 65). Identificarea punctelor critice și a vulnerabilităților în atingerea securității cibernetice, dar și a punctelor de control a acesteia sunt părți integrante ale *Business Intelligence* și pot fi asimilate principiului precauției, care își dovedește și aici utilitatea, nu numai în sănătatea publică unde a fost enunțat și aplicat.

În acest context, teza de față deschide o temă de studiu foarte actuală, securitatea cibernetică și particularizarea aspectelor de sustenabilitate în *Business Intelligence*.

Motivația alegerii temei se regăsește nu numai în evoluția actuală a fenomenului de insecuritate cibernetică relativ marcantă, ci și în cea deja clasică a securității în general. Pe plan mondial, starea de securitate de azi este caracterizată încă de suficiente vulnerabilități, de cauzalitate complexă și nu întotdeauna cunoscută, cu manifestări mai mult sau mai puțin violente în diferite sectoare. Această situație s-a produs ca urmare a presiunii cumulative, în timp, a unor factori multipli: politici, economici, financiari, sociali, culturali, biologici,

religioși, demografici, militari - care au influențat climatul de siguranță a statelor și cetățenilor.

Indiferent de forma de finanțare, publică sau privată, sistemul de sănătate este o afacere: vinde servicii, deține, analizează și transmite date la nivel național (orizontal și vertical/ierarhic) și internațional către organisme europene și mondiale și parteneri ai proiectelor de cercetare. Este evident că în acest context diplomația sănătății și principiile generale ale eticii și în particular ale eticii medicale dobândesc un rol și mai important, cu deosebire atunci când breșele de securitate cibernetică creează oportunități de ”fake news” cu scop definit de manipulare, în situații medicale extreme, cum ar fi epidemiile.

OBIECTIVE

Cercetarea de față își propune să contribuie la analiza aspectelor de securitate cibernetică cu deosebire la nivel organizațional/instituțional și să ofere în același timp deschiderea spre găsirea de soluții noi, moderne, care să asigure sustenabilitatea în *Business Intelligence*.

Obiectivul principal al cercetării este atât abordarea tematicii de securitate cibernetică dintr-o perspectivă multidisciplinară, cât și posibilitatea de a continua dezbaterea și relaționarea pe această temă, care este fundamentală atât pentru securitatea națională cât și pentru securitatea regională și internațională, cu atât mai mult cu cât nicio entitate nu poate singură să elimine sau să reducă insecuritatea cibernetică.

Pornim de la **ipoteza** că trei domenii/sectoare importante (denumite în continuare ținte), aparent independente, interferează în generarea insecurității cibernetice (vulnerabilități și amenințări) sau la generarea securității cibernetice (reziliența) la nivel organizațional, societal, și finalmente internațional. Aceste ținte sunt relațiile internaționale/diplomația, decidența politică/guvernanța și mediul de afaceri/*Business Intelligence*/infrastructuri critice.

Am ales ca studiu de caz al securității cibernetice în sustenabilitatea *Business Intelligence* o infrastructură critică, cea a serviciilor de sănătate, în particular sistemul serviciilor de sănătate din România. Digitalizarea sistemului medical (e-Health) ca cerință pentru stocarea, prelucrarea și transmiterea de date permite asumpția că dacă există securitate cibernetică există siguranța datelor, o analiză corectă în cadrul procesului de *Business*

Intelligence permițând măsuri și strategii ca parte integrantă a strategiei de securitate generală.

Pentru a răspunde la aceste întrebări și a atinge scopul cercetării ne-am propus următoarele **obiective**:

1. Plasarea securității cibernetice în contextul actual al securității generale
2. Evaluarea riscurilor/hazardelor/vulnerabilităților în securitatea cibernetică la nivel individual, organizațional, statal și global
3. Analiza poziționării *Business*, *Competitive*, *Market* și *Cyber Intelligence* în funcționalitatea infrastructurilor critice
4. Integrarea/asocierea domeniilor țintă în atingerea securității cibernetice și sustenabilității în *Business Intelligence*

METODOLOGIA ȘI STRATEGIA DE CERCETARE

Lucrarea de față este rezultatul unei cercetări de tip inductiv desfășurată în trei direcții centrate pe securitatea cibernetică. Două etape importante, dar întrepătrunse au stat la baza cercetării și anume documentarea prin parcurgerea/revizuirea/sistematizarea literaturii de specialitate și analize - studiu de caz.

• *Revizuirea și sistematizarea literaturii de specialitate*

Literatura de specialitate din domeniile de interes (țintă) ale cercetării este bogată, interesul nostru fiind îndreptat cu deosebire spre publicațiile și alte tipuri de surse naționale și internaționale de după anul 2000 și până în prima jumătate a anului 2021. Prezentarea conceptelor generale și evoluția acestora a pornit însă de la lucrările (cărți și articole) autorilor consacrați, clasici ai fiecărui domeniu prezenți în special în capitolele 1 și 3 ale tezei elaborate. Lucrarea conține peste 300 de referințe bibliografice, dintre care un număr mai mic tratează subiectul securității cibernetice în sistemele serviciilor de sănătate și mult mai puține cel al *Business Intelligence*-ului în același sector, preocuparea sistematică pentru acestea fiind de dată recentă, iar literatura de specialitate mai săracă.

• *Analize și studiu de caz*

Am inclus în cuprinsul tezei câteva analize personale referitoare la patru subiecte care conectează securitatea cibernetică, *Business Intelligence*, organizațiile supranaționale și alianțele politico-militare, relațiile internaționale, sistemele de sănătate și sănătatea publică. Aceste analize s-au bazat pe culegerea de date din surse oficiale (rapoarte, note, declarații

de presă ale guvernelor/agențiilor guvernamentale/ministerelor și reprezentanților acestora, organisme internaționale și organizații profesionale). Parte din informații au fost preluate din surse online/mass media și aici ne referim la informații noi/puncte de vedere, încă nesistematizate.

Analiza problemelor de securitate cibernetică și rolul *Business Intelligence* în sistemul de sănătate din România s-a bazat pe adaptarea a două modele de analiză consacrate (”Swiss Cheese” și ”Troika erorilor”), utilizate în diverse domenii, dar nu și pentru problemele de securitate cibernetică din sectorul sănătății sau combinația securitate cibernetică – *Business Intelligence* în România.

Abordarea inductivă a fost aleasă și pentru studiul de caz, în care am optat pentru metoda calitativă. În acest sens s-a creat un chestionar care a fost autoadministrat de către persoanele care au acceptat să răspundă întrebărilor formulate. Rezultatele au fost interpretate descriptiv.

Teza de doctorat a fost structurată în cinci capitole, astfel:

Capitolul 1 - SECURITATEA GLOBALĂ ÎN SECOLUL XXI pornește de la prezentarea unor aspecte teoretice care vizează evoluția conceptului și mediului de securitate și care susțin încadrarea securității cibernetice și provocările la adresa acesteia ca priorități actuale.

În contextul trendului continuu ascendent al procesului de globalizare, migrarea atenției privind spectrul de insecuritate de la dimensiunea militară mai mult spre dimensiunile economică, politică, socială și de mediu au arătat că amenințările în creștere nu mai pot fi stăpânite strict în cadrul național. După Războiul Rece, conceptul de securitate a primit o abordare diferită, politicile internaționale si supranaționale având un rol mai bine conturat, intervenind și alte tipuri de actori pe lângă cei statali (Chifu 2009. 1-18), de departe, cel mai important rol în reformularea conceptului de securitate fiind deținut de Școala de la Copenhaga. Nevoia de cooperare și acțiune pentru conservarea securității colective în toate dimensiunile ei, strâns interconectate, a devenit și mai evidentă, iar intervenția instituţiilor şi organizaţiilor de securitate (UE, NATO, ONU) mai mult decât salutară (Burke *et al.* 2016. 64-79). Dinamica și multidimensionalitatea problemelor de securitate au sporit atenția asupra securității umane. Plasarea securității umane în centrul agendei internaționale de

securitate a fost oficial recunoscută la începutul anilor ‘90 în Raportul cu privire la dezvoltarea umană al Organizației Națiunilor Unite, care menționează că "securitatea a simbolizat protecția împotriva unor amenințări precum bolile, foametea, șomajul, criminalitatea, conflictul social, represiunea politică și riscurile pentru mediu" (United Nations Development Program 1994. 22), afectând în fapt toate nivelurile societății cu extindere consecutivă în relațiile internaționale. Schimbarea ierarhiei amenințărilor la adresa securității în secolul XXI a adus în prim plan amenințările la adresa funcționării sistemului economic, proliferarea armelor de distrugere în masă, schimbările climatice, terorismul internațional, migrarea populației, bolile cu evoluție epidemică/pandemică și nu în ultimul rând infracțiunile în spațiul cibernetic, care au devenit prin frecvența și magnitudinea lor cu adevărat de temut. În mediul de securitate contemporan liantul între terorism și situații de criză sau război este chiar spațiul cibernetic ca punte între stat, sectorul politic, sectorul de afaceri si structurile organizaționale teroriste.

Ciberizarea este considerată în prezent o consecință a informatizării și cibernetizării, (Ma 2016. 1-9), conducând la apariția puterii cibernetică și migrarea acesteia către actori non-statali, ca o nouă dimensiune a puterii în secolul XXI (Nye 2010. 1-19). Cu certitudine, apariția Internetului a oferit posibilități nelimitate de comunicare și cunoaștere și a deschis, chiar dacă inițial aparent neînsemnată, problema securității cibernetice și apoi a hipersecuritizării asociate a spațiului cibernetic (Hansen–Nissenbaum 2009. 1164). Provocările la adresa securității cibernetice, inclusiv războiul cibernetic sunt o realitate, iar acțiunile cât mai precise pentru combaterea lor sunt esențiale pentru toate sectoarele și domeniile de activitate. Principala problemă a vulnerabilității sistemelor informatice este însă legată de mediul de afaceri și de spionaj, în pofida impresiei generale date de spectrul unui incident cibernetic major la nivelul infrastructurilor critice. E-sănătatea este o punte care face conexiunea cu lumea digitală a unui sector de importanță critică, cel al serviciilor de sănătate și nu poate fi separată actualmente de Internetul lucrurilor, care a devenit un punct focal important pentru sănătatea publică ca și componentă definitorie a securității umane și implicit a securității generale. Problema securizării spațiului cibernetic a apărut pe agenda politică a UE și este percepută ca o amenințare crescândă pentru cetățeni, guverne și mediul de afaceri din statele sale membre. În acest sens, UE este un actor al securitizării în domeniul securității cibernetice, chiar dacă la nivelul Uniunii există sarcini diferențiate în consensul efortului colectiv de a aborda securitatea cibernetică (Christou 2018. 278-301).

Tocmai în contextul celor prezentate mai sus, UE împreună cu NATO au fost forțate să își regândească radical abordarea comună privind protecția rețelelor informatice.

Nu în ultimul rând, am constatat că guvernanța și diplomația cibernetică, ca ramuri noi ale domeniilor de bază au un rol covârșitor în obținerea soluțiilor optimale pentru acte de guvernanță generală sustenabilă. Ca urmare în mod particular a impactului multinațional al infracțiunilor cibernetice necesitatea unui consens la nivel internațional privind securitatea cibernetică este subînțeles, impunând o punere de acord a cadrului juridic, care trebuie în mod obligatoriu continuată cu implementare și consens operațional. Deși securitatea cibernetică abordează aspecte strâns legate de suveranitate, gestionarea securității cibernetice la nivel național sau internațional implică o multitudine de aspecte și presupune diferite tipuri de domenii de expertiză aliniate într-o relație de comunicare și cooperare.

SECURITATEA CIBERNETICĂ ȘI STRATEGII DE APĂRARE A ENTITĂȚILOR CHEIE sunt prezentate în **capitolul 2**.

Protecția infrastructurilor critice împotriva atacurilor cibernetice s-a constituit în timp într-o problemă acută, proporțională cu probabilitatea unui atac cibernetic, Uniunea Europeană și SUA adoptând inițiative importante în domeniul securității cibernetice a infrastructurilor critice care în prezent, practic, sunt deja sau sunt pe cale să devină infrastructuri critice informaționale, toate fiind de importanță vitală. Investigațiile conduse la nivel european au evidențiat faptul că a patra amenințare în materie de criminalitate informatică a fost cea considerată în relație cu atacurile care distorsionează sau chiar subminează funcțiile interne ale uneia sau mai multor infrastructuri critice (EUROPOL 2019. 23). Atacurile cibernetice masive asupra infrastructurilor critice au deja un istoric bogat, cele mai cunoscute începând cu Estonia (2007) și extinsul WannaCry (2017-2019) declarat de Europol de un nivel fără precedent, cu atât mai mult cu cât doar câteva țări nu au fost afectate de atac (EUROPOL 2017. 30). Referitor la acțiunile de tip criminalitate cibernetică în România, în cursul anului 2019 au fost înregistrate atacuri cu un grad redus de complexitate adresate în cea mai mare parte sectorului de servicii de sănătate și care au evidențiat vulnerabilitatea și lipsa de preocupare pentru asigurarea unor măsuri minime de protecție cibernetică în sistemul medical. (SRI 2020*a*).

Amenințările la adresa securității cibernetice au impus dezvoltarea noii strategii de securitate în domeniu, astfel că la nivelul Uniunii Europene cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică a fost declanșat procesul de revizuire a Directivei

(UE) 2016/1148, cunoscută ca Directiva NIS, fiind lansată propunerea de Directiva NIS 2.0. Integrarea dimensiunilor europeană și globală a securității cibernetice revine diplomației cibernetice, care joacă un rol important în capacitatea de răspuns direct la amenințările actuale și la fundamentarea unei mai bune cooperări în acțiunile împotriva amenințărilor viitoare. În acest context, UE și-a construit strategia de securitate cibernetică a infrastructurilor sale pe baza apărării și a diplomației cibernetice în cadrul poziționării ca militant pentru pace (Cîrnu 2019. 35-40) care are ca fundament principiul precauției, cu un real potențial de dezamorsare al conflictelor din spațiul cibernetic.

Având ca punct de plecare prezentarea în evoluție a strategiei de securitate cibernetică a Uniunii Europene, am analizat pe baza unor criterii definite strategiile naționale de securitate cibernetică în vigoare la nivelul anilor 2015-2021 România, Germania, Franța, Belgia și Estonia. A rezultat că România și Germania se concentrează asupra stabilirii și promovării rolului parteneriatelor public-private și a utilizării în condiții de siguranță a tacticilor de comunicații și informatică de către cetățeni, organizații private și autorități în mediul cibernetic. Pe de altă parte, Franța vizează siguranța mediului de afaceri și a sustenabilității spațiului cibernetic. În mod specific, cooperarea internațională și consolidarea competențelor sunt menționate în strategiile României, Estoniei, Germaniei și Franței și nu în ultimul rând protejarea infrastructurilor critice (serviciilor esențiale) se regăsesc specificate clar în strategiile României, Franței, Germaniei și Belgiei.

Ultimul subcapitol referitor la impactul acțiunilor pentru menținerea securității internaționale a spațiului cibernetic este destinat discutării rolului puterilor și elitelor în era globalizării, în speță a NATO, pentru care am argumentat încadrarea ca elită. Potrivit lui Burke realitatea politică globală impune noi abordări în materie de securitate, bazate pe o viziune etică mai bună a ceea ce înseamnă cu adevărat securitatea (Burke *et al.* 2016. 64-79). În contextul amenințărilor contemporane globale ne-am propus să analizăm principiul (etic) potrivit căruia „toți actorii din domeniul securității au responsabilitatea de a crea securitate pentru toți" așa cum consideră SUA și NATO pentru realizarea securității globale. Este poziția de elită pusă în pericol de vulnerabilitatea securității cibernetice? Datele prezentate arată că atacurile cibernetice și securitatea cibernetică a NATO reprezintă un subiect sensibil evidențiat în rapoartele oficiale ale organizației și ale unor instituții guvernamentale începând din anul 1998, tipul și concepția unui atac informatic reprezintând o amenințare directă la adresa poziției lor, din cauza problemelor asimetrice generate. Printre

deciziile pe termen lung cu privire la securitatea cibernetică pe care statele membre NATO le-au luat la reuniunea la nivel înalt de la Varșovia din anul 2016 s-a numărat și recunoașterea spațiului cibernetic ca al cincilea domeniu de conflict armat în care NATO va fi operațional, pe lângă celelalte domenii: aerian, maritim, terestru sau spațial. De asemenea, în cadrul consolidării cooperării și provocărilor comune, în februarie 2016 NATO a semnat un acord tehnic cu UE privind cooperarea în domeniul apărării cibernetice.

Am ales să tratăm în **capitolul 3 - RELAȚIA BUSINESS INTELLIGENCE - SECURITATE CIBERNETICĂ** în care *Business Intelligence* este factor cheie în dezvoltarea performanței organizaționale, atât în entități de drept privat cât și de drept public.

Integrat în societate și în instituțiile acesteia, mediul de afaceri are pe lângă interesul financiar și perspective etice și politice, având o puternică influență în luarea deciziilor și determinând modul în care companiile decid să-și gestioneze activitățile (Freeman–Burton 2019. 1). Spre deosebire de *Business Intelligence, Business Analytics* presupune utilizarea procedurilor statistice în analiza datelor care stau și la baza modelelor predictive care fundamentează managementul deciziei, în acest fel fiind o completare a procesului de *Business Intelligence.* Mai multe studii consideră că patru elemente integrează domeniile *Business Intelligence, Business Analytics* și managementul performanței organizaționale: competența, documentarea, vizualizarea și cultura muncii, dar elementele care integrează *Business Intelligence* și *Business Analytics* sunt programele software și managementul datelor, elemente prezente inclusiv în sectorul public în scopul gestionării managementului performanței, guvernanța electronica fiind complementara (Yahaya *et al.* 2019. 292-298).

După anul 2000 au început să apară informații privind aspectele culegerii de date în *Business Intelligence*, care ridică problema operării etice. Spre deosebire de *Business Intelligence,* extragerea de date din mediul extern al organizației, care este cadrul specific al *Competitive Intelligence*, permite analiza predictivă, fapt care devine din ce în ce mai important în procesul de *Business Intelligence* și ca urmare, utilizarea *Competitive Intelligence* în mediul de afaceri apare ca o extensie necesară a *Business Intelligence,* ambele depinzând de calificarea factorului uman. În mod firesc se pune întrebarea când virează *Competitive Intelligence* spre spionaj industrial? Spionajul industrial poate fi încadrat ca o formă de extragere de date cu caracter comercial, iar limita dintre *Competitive Intelligence* și spionajul industrial poate fi uneori estompată, lăsând cu ușurință loc devierii spre spionaj într-o manieră voluntară sau nu, dar cu certitudine facilitată de accesul larg la o tehnologie

de informații și comunicații avansată. Nu este de neglijat faptul că există implicări cunoscute ale statelor în spionajul industrial, dar și implicări ale companiilor private în acțiuni de spionaj industrial ale guvernelor. (Crane 2005. 233-240). Un alt tip de *intelligence* legat de mediul de afaceri, de fapt o componentă a afacerii, este *market intelligence*, care se referă de asemenea la culegerea și analiza de informații din mediul extern al unei companii dar care, spre deosebire de *Competitive Intelligence* investighează mai extins, într-o abordare integrată, rezultatele obținute având implicații pe termen lung, cu o caracteristică evidentă de complementaritate cu *Competitive Intelligence* (Jamil 2013. 465-469). Am notat în demersul nostru că securitatea spațiului cibernetic și corectitudinea informațiilor culese sunt completate și corelate cu *cyber intelligence* care se referă la colectarea, analiza și interpretarea datelor digitale în și prin spațiul cibernetic, care reprezintă amenințări, transformate sau nu în riscuri și care devin informații strategice în mediul de afaceri. În acest fel, *cyber intelligence* devine parte importantă în crearea unui spațiu cibernetic sigur și în sustenabilitatea *Business Intelligence*. (Moore 2020. 1-14).

Întrucât tehnologia a devenit în prezent parte integrantă a sectorului sănătății, este esențial ca organizațiile din domeniul asistenței medicale să integreze în operațiunile lor sisteme adecvate de *Business Intelligence* (Ashrafi *et al.* 2014. 117-130). Am identificat instrumente ale *Business Intelligence* și *Business Analytics* comune în cadrul organizațiilor și a celor regăsite în activitățile de cercetare și am observat că instrumentele specifice ale *Business Intelligence* sunt integral comune ca etape în cercetare. Spre deosebire de *Business Intelligence, Business Analytics* este mult mai potrivit pentru desfășurarea în sine a cercetării (prognoza, modelarea predictivă) decât pentru evaluarea performanței proiectului.

Aprofundarea aplicării legilor internaționale din punct de vedere al eticii în sistemele de sănătate este cu atât mai importantă cu cât la intersecția dintre securitatea cibernetică și cercetarea medicală se află subiectul uman. Existența atâtor elemente comune de *Business Intelligence* și *Business Analytics* între organizații și cercetare aduce, cu atât mai mult în atenție aspectele de etică profesională, confidențialitate, precauție și responsabilitate socială. Securitatea cibernetică nu este opțională în cazul în care se au în vedere aspectele eticii în sănătate și cercetare, ci este o condiție obligatorie pentru aplicarea principiilor eticii medicale, în primul rând al confidențialității și este astfel preambulul respectării legislației referitoare la protecția datelor. Securitatea cibernetică funcționează astfel pe principiul precauției, aplicat în domeniul sănătății publice.

În **capitolul 4** ne-am propus să conturăm **CONJUNCTURA INTERNAȚIONALĂ ÎN PERIOADA PANDEMIEI DE COVID-19 (1 IANUARIE 2020 – 31 MARTIE 2021)**

La 31 decembrie 2019, autoritățile sanitare din China au raportat Organizației Mondiale a Sănătății un număr de cazuri de pneumonie virală de origine necunoscută în Wuhan, Hubei. Datorită răspândirii rapide a bolii, OMS a declarat fenomenul ca fiind o pandemie la 11 martie 2020 (European Centre for Disease Prevention and Control - ECDC 2020. 1-10). La un an diferență, OMS a făcut public raportul echipei internaționale de specialiști care nu a putut preciza exact sursa epidemiei din Wuhan, respectiv a pandemiei. Evoluția imprevizibilă a crizei sanitare produsă de pandemia de COVID-19 a pus încă din faza inițială semne de întrebare privind guvernanța globală relaționată acesteia, deoarece măsurile care au fost implementate de numeroase guverne au încălcat practic principiile diplomației sănătății prin decizii unilaterale. Pandemia arată că problemele de sănătate publică nu mai pot fi menținute strict la nivel național, răspândirea rapidă a bolii încadrându-se în contextul globalizării, cu implicații nedorite pentru dimensiunea economică, socială și chiar politică a securității (Jora 2020. 119).

Analiza personală privind principiul multilateralismului în acțiunile statelor și a OMS, ONU și NATO în timpul pandemiei de COVID-19 a evidențiat că translatarea multilateralismului în situația de criză sanitară produsă a fost acceptată de statele membre ale OMS în luna mai 2020 prin adoptarea rezoluției referitoare la răspunsul colectiv la COVID-19, și sublinierea rolului de lider al OMS în managementul crizei. Un alt aspect comun al ONU și OMS se referă la problema securității globale cu accent direct asupra domeniului sănătății, expertiza tehnică și nu în ultimul rând resursele financiare influențând eforturile de reconstruire a sistemelor de servicii de sănătate performante. Al treilea aspect comun remarcat în declarațiile celor două organizații este legat de problemele acestora de finanțare în contextul pandemiei de COVID-19 și acțiunilor de solidaritate. Acțiunile OMS si Chinei au inițiat diferende diplomatice, pierderi economice, tensiuni de tip comercial, în ansamblu la nivel mondial un climat de neîncredere reciprocă. OMS a pierdut din credibilitate, iar finanțarea multinațională a OMS a fost subiectul unei dezbateri intense la mijlocul lunii aprilie 2020, când administrația americană a anunțat oprirea temporară a finanțării pentru OMS (ulterior reluata). Acuzele împotriva OMS, ca părtinitoare a modelului chinez de abordare a epidemiei de COVID-19 ar putea fi încadrată ca o continuare a procesului de securizare de tip *hard* a Chinei, demarat de SUA în timpul Administrației

Trump (LARICS 2020). Tot în baza multilateralismului, NATO s-a confruntat cu necesitatea de a reinterpreta Articolul 5 al tratatului, posibil neaplicabil din cauza vulnerabilității egale generală a civililor și militarilor, însă a NATO a acționat permanent pentru ca ”această criză sanitară nu devine o criză de securitate” (NATO 2021 *a*) (NATO 2021 *b*).

Dezvoltarea vaccinurilor anti COVID-19 a însemnat o luptă acerbă între Rusia, SUA, Regatul Unit al Marii Britanii și China (deși dezvoltat după vaccinul rusesc Sputnik, vaccinul chinezesc CoronaVac a fost primul din lume utilizat la nivel național) nu numai pentru obținerea vaccinurilor și cu privire la eficiența acestora, ci și de modul (chiar prioritatea) în care statele lumii vor avea acces la dozele necesare, generând, cel puțin în prima fază naționalismul vaccinării. Chiar dacă și Uniunea Europeană s-a raliat parțial acestui curent, campania de vaccinare anti COVID-19 a început în toate țările UE simultan în data de 27 decembrie 2020, în spiritul solidarității europene (Consiliul Uniunii Europene 2021). Opusa naționalismului vaccinării, inițiativa multilaterală COVAX, condusă în parteneriat public-privat a mizat pe accesul echitabil la vaccin a țărilor cu venituri mici și mijlocii, însă a adus în discuție problema utilizării lor ca instrument strategic de politică externă și dobândirea de influență internațională (Ameyaw-Brobbey, 2021) prin consolidarea relațiilor și dominație geopolitică, exemple in acest sens fiind China și Rusia. In ceea ce privește politica României în relație cu pandemia de COVID-19, aceasta a urmat îndeaproape modelul Uniunii Europene, fiind în plus primul stat membru care gestionează rezerva strategică de echipamente medicale a UE. De asemenea, România a fost primul stat membru NATO care a folosit Capacitatea de Transport Strategic a Alianței, aducând în țară mijloace în lupta pentru combaterea pandemiei.

Problema securității cibernetice, a scos în evidență încă de la începutul pandemiei o serie de aspecte de ordin etic, juridic și chiar tehnic în ceea ce privește volumul imens de date colectate și securitatea/ confidențialitatea acestora, precum și spionajul cibernetic. Am formulat în capitolele anterioare ipoteza că principiul precauției din sănătatea publică se suprapune cu securitatea cibernetică din punct de vedere al măsurilor și acțiunilor de identificare și prevenție a vulnerabilităților cauzatoare de insecuritate. Încă de la debut, pandemia de COVID-19 a fost acompaniată de un exod de informații adevărate și false (infodemie), cu implicarea unor actori statali, în mare măsură susținută de rețelele sociale care au generat rapid pentru fenomenul ”fake news” (China si Rusia au fost acuzate direct) măsuri de combatere și prevenire. Pandemia de COVID-19 a produs intensificarea temerilor

induse de avalanșa de informații online (cibercondria), cunoscută ca având impact asupra sănătății publice (Starcevič *et al.* 2020. 53-61). În ceea ce privește intensificarea spionajului cibernetic de tip statal, acesta a vizat nu numai cercetările concurențiale pentru tratament, dar și pentru crearea vaccinului (Fidler 2020 *b*), fapt ilustrat la începutul lunii decembrie 2020 când Agenția Europeană a Medicamentului a fost victima unui atac cibernetic care a vizat vaccinul Pfizer, producția și distribuția ulterioară a acestuia nefiind afectată (CERT-RO 2020*a*).

Evoluția pandemiei de COVID-19 a dovedit fără niciun dubiu că sistemele informaționale/informațiile dețin un rol central în reacția guvernelor naționale și organizațiilor internaționale, politica și deciziile acestora bazându-se pe analiza datelor și prognoze. Relația dintre Business Intelligence și pandemia de COVID-19 a fost analizată de Paul Grill care a constatat că problema bazelor de date mari din *Business Intelligence* este de fapt lipsa acestora și care, împreună cu un cuantum de date corecte culese conduc la date complet greșite în ceea ce privește parametrii utilizați pentru urmărirea pandemiei (cazuri confirmate, total decese, total vindecați), analiza datelor incomplete sau greșite conducând în mod evident la creșterea probabilității ca măsurile să fie de asemenea greșite. Implementarea *Business Intelligence* în managementul crizei pandemice trebuie să se bazeze pe date fiabile, doar în acest fel *Business Intelligence* ar avea o contribuție semnificativă în susținerea organismelor implicate în criza sanitară, nu numai din perspectivă medicală ci și din perspectiva mediului de afaceri (Grill 2020).

Capitolul 5 - CONTRIBUȚII PERSONALE. SECURITATEA CIBERNETICĂ ȘI BUSINESS INTELLIGENCE ÎN SERVICIILE DE ASISTENȚĂ MEDICALĂ ȘI GLOBALIZAREA SĂNĂTĂȚII aduce în atenție globalizarea sănătății publice și guvernanța internațională în materie de sănătate, precum și diplomația în domeniul sănătății, ca preambul al analizelor privind rolul securității cibernetice în funcționalitatea sistemelor serviciilor de sănătate ca unități de bază ai sănătății publice globale. Cuprinderea în politicile externe ale statelor a temei sănătății publice (Katz *et al.* 2011. 517-520) și a guvernanței acesteia este susținută de o multitudine de evenimente derulate și înregistrate cu precădere în ultimii o sută de ani care au evidențiat faptul că în contextul globalizării și dezvoltării guvernanței globale este inerent ca statele independente să încheie parteneriate în cadrul cărora să coopereze nu numai între ele, ci și cu actori non-statali (Kickbush–Buss 2011. 601-610). Raportat la numeroasele riscuri pentru sănătatea publică globală, asociate cu bolile

infecțioase, comerțul internațional cu opiu și alcool, riscurile profesionale și poluarea transfrontalieră (Fidler 2001. 844-845), Sophie Harman afirma faptul că ”guvernanța internațională în domeniul sănătății este un domeniu emergent care combină sănătatea publică, sociologia medicală, economia în domeniul sănătății, dreptul internațional, antropologia, știința politică și relațiile internaționale” (Harman 2017. 1-2). Astfel, amenințările pentru sănătatea globală au creat un trend care aduce în atenție implicarea curentă și efectivă a diplomației sănătății, un domeniu de pionierat și o ramură nouă în teoria și practica relațiilor internaționale (Jora 2020. 113) alături de managementul sistemelor de sănătate naționale pentru menținerea securității generale. Importanța în creștere a legăturii sănătate-securitate (amenințare de tip hibrid) reflectă de fapt responsabilitatea politică și implicațiile celor două legături dintre sănătate și securitate – securitizarea sănătății și medicalizarea securității (Nunes 2012. 151-152). România este parte activă a acordurilor internaționale, rețelelor și organizațiilor specifice fiind implicată în eforturile diplomatice de protejare a sănătății globale. Studiind istoricul sistemului serviciilor de sănătate din România am constatat că schimbarea și modernizarea semnificativă a acestuia s-a produs după anul 1990 datorită apariției în legislația sanitară a dreptului de funcționare a furnizorilor privați de asistență medicală. Pe de altă parte, sistemul de sănătate din România s-a confruntat cu disfuncționalități ale cardului de sănătate și dosarului electronic de sănătate precum și cu episoade de atacuri cibernetice, anunțate oficial începând din anul 2012 (WannaCry sau altele soldate inclusiv cu plăți pentru recuperarea parțială sau totală a bazelor de date). Securitatea datelor de sănătate este strict reglementată de Directiva UE 95/46/EC, iar în conformitate cu competențele SRI în domeniul securității naționale, Centrul Național Cyberint are ca misiune protecția infrastructurilor critice în care este inclus și sistemul de sănătate. Studiul nostru de caz privind problemele de securitate cibernetică si rolul *Business Intelligence* în sistemul de sănătate din România a pornit de la ipoteza conform căreia ca și consecință a erorilor active și de sistem securitatea cibernetică este afectată și conduce la evenimente cu impact negativ în asistența medicală. Utilizarea in analiză a modelului ”Swiss Cheese” (Reason 2000. 768-770) a evidențiat vulnerabilități în ceea ce privește securitatea cibernetică. Analiza vulnerabilităților, riscurilor și evenimentelor de insecuritate cibernetică fac parte din managementul riscurilor generale în organizație și constituie o parte integrantă a *Business Intelligence,* iar managementul erorilor este amplu fundamentat de ”Troyka erorilor” (Helmreich *et al.* 1999. 19–32). Scurta incursiune în interiorul sistemului de

sănătate românesc constituie partea calitativă a cercetării noastre și prezintă opiniile privind securitatea cibernetică și *Business Intelligence* în obținerea performanței și sustenabilității ale unui număr de persoane cu responsabilități de conducere în sectorul serviciilor de sănătate din România. Rezultatele au arătat nu numai o cunoaștere și conștientizare parțială a problematicii puse în discuție, dar și o implementare lacunară cu deosebire în sistemul public de sănătate a *Business Intelligence* și a măsurilor specifice securității cibernetice.

CONCLUZII

Plasarea particulară a securității cibernetice în contextul actual al securității generale din secolul XXI este determinată de trendul ascendent al ciberizării, când practic adicția tot mai pronunțată față de spațiul cibernetic transcende în toate domeniile de activitate și-a modificat iremediabil mediul clasic al securității. În practică, dimensiunile militară, politică, economică, societală și de mediu nu mai pot fi separate de securitatea cibernetică, care actualmente devine echivalentul unui numitor comun al acestora. Indiferent dacă ne raportăm la relațiile dintre state, structuri non-statale sau organizații supranaționale (posibil afectate de transformarea spațiului cibernetic într-un spațiu al puterii prin deținere de informații, capacitate de descurajare, apărare sau atac, reziliență), guvernanță și aparent paradoxal la mediul de afaceri, aceste domenii „țintă" sunt contributoare atât la periclitarea cât și la generarea securității. Nu considerăm exagerat să afirmăm faptul că diplomația cibernetică devine o problemă esențială a politicii externe a secolului XXI, care vizează cumulat drepturile omului, securitatea și politica economică. „Vocea" și acțiunea comune constituie în esență o necesitate evidentă pentru securitatea spațiului cibernetic, în pofida reticenței încă existente din perspectiva suveranității și implicit a strategiilor naționale.

Multitudinea de amenințări concretizate cu atacuri cibernetice a unor structuri de stat, **infrastructuri critice**, sau chiar organizații private operaționale a unor infrastructuri critice și consecințele lor au fost definitorii în securitizarea spațiului cibernetic și au condus la formularea strategiilor de apărare cibernetică naționale sau comune (de ex. Uniunea Europeană) și care ulterior, după implementare au fost supuse unor up-datări conform noilor amenințări și nevoii de vigilență sporită. Din nou se impune menționarea rolului diplomației în găsirea măsurilor comune de acțiune, a evitării diferendelor și atingerii scopului de menținere a securității cibernetice fără a șterge însă diferențele impuse de principiul suveranității naționale (aspect rezultat din analiza noastră vizând strategiilor naționale de

securitate cibernetică a cinci state membre ale Uniunii Europene. Nu poate fi exclus faptul că dacă infrastructurile critice și infrastructurile critice informaționale au suferit de pe urma diverselor amenințări cibernetice (de ex. sistemele energetice, de transport, telecomunicații, militare), domenii mai puțin vizate în trecut au devenit noi ținte, și anume sistemele de servicii de sănătate (vezi atacul WannaCry) sau sistemele de aprovizionare centrală cu apă (triada cantitate-calitate-securitate cibernetică) în care informatizarea proceselor a evoluat extrem de rapid.

Evaluarea riscurilor/hazardelor/vulnerabilităților în securitatea cibernetică la nivel individual, organizațional, statal și global arată că nici puterile sau elitele nu au fost ocolite de problematica sensibilă a securității cibernetice. Chiar și **NATO**, despre care am argumentat în cuprinsul tezei opinia că este o elită, s-a situat între structurile atacate cibernetic încă de la sfârșitul anilor '90 în circumstanțele în care SUA deveneau un actor important în combaterea terorismului internațional. Analiza noastră a evidențiat existența vulnerabilităților și expunerea la amenințări directe generatoare de asimetrii în cazul puterilor/elitelor. Parafrazând articolul 16, alineatul 2 din Constituția României „nimeni nu este mai presus de lege" putem afirma în contextul analizei noastre că „nimeni nu este mai presus de vulnerabilitățile și amenințările cibernetice".

Integrarea sistemelor de tip *Business Intelligence* în managementul sistemic susținut în primul rând de cultura riscurilor ca parte a culturii organizaționale **(una din multiplele situații generatoare de vulnerabilități)** poate conduce la un proces eficient de bună guvernare. În domeniul sănătății, soluțiile de tip *Business Intelligence* se bazează pe un volum important de date („big data" colectate, stocate, analizate, raportate si transferate) față de care nu există dubii că au și vor avea potențialul impactului pozitiv asupra rolului de unități de bază pentru sănătatea publică națională și globală. **Sistemul de sănătate din România**, ca și cele din țările membre ale Uniunii Europene și nu numai, operează cu instrumente vulnerabile cibernetic și aici ne referim la cardul de sănătate și dosarul electronic de sănătate cu rol în eficientizarea serviciului, dar cu frecvente disfuncționalități și probleme legate de confidențialitatea datelor sensibile.

În ansamblu, analiza **poziționării *Business Intelligence* în funcționalitatea** infrastructurilor critice (inclusiv sistemele de sănătate) de drept public arată mai degrabă o implementare modestă și fracturată spre deosebire de sectorul privat unde sunt asociate și operaționale competitiv, *Market* și *Cyber Intelligence*. Între potențialele beneficii aduse de

Business Intelligence, ca și de celelalte tipuri de *intelligence* menționate în sectorul sănătății, consolidarea și protecția datelor (de exemplu, date cu caracter personal, date economice) par să fie pe primul loc. Altfel spus, *Business Intelligence* ca metodă integrativă, *Competitive Intelligence* ca metodă cu potențial constructiv, *cyber intelligence* ca metodă asiguratorie coexistă și funcționează în relație sinergică. În mod evident, complementaritatea între securitatea informatică și procesul de *Business Intelligence* în sustenabilitatea organizațională, poate defini rolul organizațiilor publice si private în strategiile naționale de securitate cibernetică. Pe de altă parte însă, atribuțiile organizațiilor private sectorului în protecția infrastructurilor critice și a infrastructurilor critice de informații nu poate fi exclus din procesul de securitizare colectivă.

În ce situații organizațiile/companiile din orice domeniu sunt mai vulnerabile? Conjunctura internațională în perioada pandemiei de COVID-19 (1 ianuarie 2020 – 31 martie 2021) pe care am analizat-o în teza noastră a readus în atenție, la o magnitudine exponențială, un fenomen prezent anterior și anume infodemia, de data aceasta cu consecințe incomparabil mai severe, fiind vorba de sănătatea publică globală (România nu a făcut excepție de la acutizarea infodemiei). În paralel cu infodemia, pandemia de COVID-19 a generat recrudescența cibercondriei, asociată cu augmentarea stării de nesiguranță și teama față de boală, fenomen care poate fi considerat similar terorismului. Din punct de vedere al securității cibernetice, pandemia de COVID-19 a arătat încă o dată disfuncționalitățile cunoscute și vulnerabilitățile sistemelor de asistență medicală, dar și o serie de aspecte de ordin etic, juridic și chiar tehnic în ceea ce privește mega-datele rezultate și securitatea/confidențialitatea acestora. Ca un tot unitar, securitatea cibernetică și *Business Intelligence*-ul ar asigura un cadru eficient de înțelegere a fenomenului și ar oferi modalități mai pertinente de ieșire din pandemie.

Tendința de izolare a țărilor membre UE, lipsa de cooperare, în prima fază motivată de suveranitate, iar la nivel mondial, acțiunile și măsurile cel puțin suspecte ale OMS în ceea ce a privit China la debutul pandemiei au perturbat climatul internațional prin contestarea vehementă de către SUA și alte țări. În contextul sănătății și securității globale, un alt aspect al pandemiei, și anume campania de vaccinare, a bulversat din nou situația internațională prin așa numita geopolitică a vaccinării, ca urmare a inițiativei COVAX, deși per total, OMS a avut o contribuție semnificativă din punct de vedere al diplomației sănătății prin promovarea principiului multilateralismului.

În mod particular, **analiza sistemului de sănătate din România** a evidențiat faptul că modelul actual de management, structura învechită și încă vitalizată și remaniată insuficient determină ca problemele evidente, existente, serioase și periculoase, pentru care există un precedent să fie la originea cauzalității breșelor de securitate. Aplicabilitatea *Business* și *Competitive Intelligence* practic inexistentă în sectorul de stat, care atât cât este bugetat arată că în mare parte sistemul nu este suficient de motivat spre analiză și performanță. Aparent subfinanțat, utilizarea fondurilor disponibile este dirijată spre actul medical și departamentele semnificativ importante (bazele de date ale pacienților, echipamente electronice, dispozitive, aparatură de înaltă performanță sau unități medicale în ansamblu fiind susceptibile la atacuri cibernetice, care s-au și întâmplat și care așa cum s-a arătat pot determina disrupții severe sau consecințe iremediabile pentru a căror funcționalitate securitatea cibernetică ar fi cheia și în sustenabilitatea *Business Intelligence*-ului.

Este sistemul serviciilor de sănătate din România pregătit să confrunte realitatea insecurității informatice? Analiza problemelor de securitate cibernetică și marcarea rolului *Business Intelligence* în sistemul de sănătate din România s-a făcut cu ajutorul modelului ”Swiss Cheese” în care am cuprins 6 bariere defensive specifice. Modelul ne-a demonstrat că pentru sistemul public de sănătate există vulnerabilități în ceea ce privește securitatea cibernetică, care prin “alinierea” erorilor active s-au soldat și se pot solda în continuare cu evenimente adverse. Multe organizații din domeniul sănătății nu aplică însă practici durabile privind managementul erorilor, susținute prin analiza de *business* și care, ca și alte componente de *intelligence* în sectorul serviciilor de sănătate sunt condiționate de securitatea cibernetică. **Investigația efectuată privind securitatea și *Business Intelligence* în opinia și practica unor persoane cu putere decizională administrativă în sistemul românesc de sănătate** a evidențiat că deși importantă, securitatea cibernetică nu este considerată o prioritate și că *Business Intelligence* pare să fie încă un domeniu străin respondenților. Fiind vorba de un mediu concurențial, s-a conturat însă în sistemul privat de sănătate trend-ul ascendent de implementare a sistemelor performante de management al riscurilor, inclusiv cibernetice, și ca urmare securitatea cibernetică este considerată o problemă de *business*, care are nevoie și de o soluție de *business*.

Din analiza noastră se poate observa **că țintele (domeniile) sunt vulnerabile și decisiv afectate de insecuritatea informatică. Integrarea/asocierea relațiilor internaționale, guvernanței mediului de afaceri/infrastructurilor critice în atingerea securității**

cibernetice și sustenabilității în *Business Intelligence* este reală și prezentă. Nici una dintre aceste ținte nu ar putea fi nominalizată în contextul de securitate al secolului XXI ca dominantă sau subordonată, fluiditatea și dinamica lor interschimbabilă fiind continuă, dar securitatea cibernetică este elementul cheie și de joncțiune în relaționarea celor trei ținte. Desigur, putem identifica lianți între aceste ținte și securitatea cibernetică, aceștia fiind în opinia noastră principiile eticii (conduc la transparență și deschidere) și principiul precauției. Preluat de sănătatea publică din domeniul protecției mediului, principiul precauției (privit uneori cu reticență de o parte a comunității științifice) implementat în limite care să mențină progresul este superpozabil atât relațiilor internaționale, cât și guvernanței, mediului de afaceri și *Business Intelligence*-ului.

Reducerea unghiului de insecuritate cibernetică în secolul XXI nu poate fi bazată decât pe managementul erorilor și colaborare. Relația dintre prevenire, identificare/anihilare și atenuare/eliminare a riscurilor și amenințărilor presupune transferul „lecției învățate" în sensul în care oricare etapă superioară conduce la prevenția de bază, iar distribuirea experienței este primul pas al colaborării externe. În acest sens, unul dintre obiective este dezvoltarea capacităților de descurajare a criminalității cibernetice în toate țările și menținerea cooperării pentru reducerea riscurilor.

În ce direcție va evolua relația securitate cibernetică - *Business Intelligence*? În mod cert în contextul acceptării spațiului cibernetic ca spațiu al puterii, paradigma securității cibernetice „apărare-atac-reziliență" va avea o succesiune a evenimentelor greu predictibilă. Dezvoltarea societății și nevoia de performanță va include *Business Intelligence*-ul în practica curentă, secondat de *Competitive, Market* și *Cyber Intelligence*. Conexiunea securității cibernetice cu *Business Intelligence* nu este unilaterală, această relație este concret reciprocă, iar securitatea cibernetică datorită caracterului transnațional nu mai este opțională în niciun domeniu. Analiza vulnerabilităților, riscurilor și evenimentelor de insecuritate cibernetică fac parte din managementul riscurilor generale în orice domeniu și constituie o parte integrantă a *Business Intelligence.*

Elementele de noutate ale cercetării prezentate în capitolul introductiv al tezei s-au concretizat, așa cum rezultă din concluziile de față formulate, în contribuții personale la o temă de studiu foarte actuală, în speță securitatea cibernetică și particularizarea aspectelor de sustenabilitate în *Business Intelligence*, ce va deschide direcții de cercetare cu caracter inovativ în domeniul cooperării dintre mediul academic, mediul de afaceri privat și cel al

sectorului public. Totodată, posibilitatea de a continua dezvoltarea acestei teme, care este fundamentală atât pentru securitatea națională cât și pentru securitatea regională și internațională este cu atât mai importantă cu cât, așa cum am precizat în cuprinsul tezei, nicio entitate nu poate singură să elimine sau să reducă insecuritatea cibernetică.

BIBLIOGRAFIE (selectivă)

AMEYAW-BROBBEY, Thomas (2021): COVID-19 Vaccination: A Real Test of Sovereign Equality and Friendship. Global Policy Journal. https://www.globalpolicyjournal.com/blog/03/02/2021/covid-19-vaccination-real-test-sovereign-equality-and-friendship.

ASHRAFI, Noushin et al. (2014): The Impact of Business Intelligence on Healthcare Delivery in the USA. Interdisciplinary Journal of Information, Knowledge, and Management. Vol. 9. pp. 117-130. https://doi.org/10.28945/1993.

BURKE, Anthony *et al.* (2016): An Ethics of Global Security. Journal of Global Security Studies. Vol. 1. Issue 1. pp. 64-79. https://doi.org/10.1093/jogss/ogv004.

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO (2020 a): Știrile săptămânii din cybersecurity (10.12.2020). Disponibil la: https://cert.ro/citeste/stirile-saptamanii-10-12-2020. Accesat la 4 martie 2021.

CHIFU, Iulian (2009): Societal Security. An agenda for the Eastern Europe. Corpus ID: 199402475. pp. 1-18. Disponibil la: http://www.cpc-ew.ro/pdfs/societal_security.pdf. Accesat 5 mai 2020.

CHRISTOU, George (2018): The Collective Securitisation of Cyberspace in the European Union. West European Politics. Vol. 42. Issue 2: The European Union, Security Governance and Collective Securitisation. pp. 278-301. https://doi.org/10.1080/01402382.2018.1510195.

CÎRNU, Elena Carmen (2019): Cyber Diplomacy, Strategic Instrument in Foreign Affairs Policy. Romanian Cyber Security Journal. ROCYS. Spring 2019. Vol. 1. Issue 1. pp. 35-40. https://rocys.ici.ro/documents/spring2019/article_5.pdf.

CONSILIUL UNIUNII EUROPENE (2020): Combaterea dezinformării. Disponibil la: https://www.consilium.europa.eu/ro/policies/coronavirus/fighting-disinformation/. Accesat la 7 mai 2021.

CRANE, Andrew (2005): In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage. Business Horizons. Vol. 48. pp. 233-240. https://doi.org/10.1016/j.bushor.2004.11.005.

ENISA (2020b): Prevention is the Cyberdefence for Hospitals. https://www.enisa.europa.eu/news/enisa-news/prevention-is-the-cyberdefence-for-hospitals. Accesat la 10 mar. 2020.

ENISA (2020c): Sectoral / Thematic Threat Analysis. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-cybersecurity-research. Accesat la 5 decembrie 2020.

EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL - ECDC (2020): Cluster of Pneumonia Cases Caused by a Novel Coronavirus, Wuhan, China. pp. 1-10.Disponibil la: https://www.ecdc.europa.eu/sites/default/files/documents/Risk%20assessment%20-%20pneumonia%20Wuhan%20China%2017%20Jan%202020.pdf.

EUROPOL (2017): Internet Organized Crime Threat Assessment (IOCTA) 2017. Disponibil la: https://www.europol.europa.eu/activities-services/main-reports/internet-organised -crime-threat-assessment-iocta-2017. Accesat la 14 aug.2018.

EUROPOL (2019): Internet Organized Crime Threat Assessment (IOCTA) 2019. Disponibil la: https://www.europol.europa.eu/activities-services/main-reports/internet-organised -crime-threat-assessment-iocta-2019 . Accesat la 12 febr.2020.

FAZAL, Tanisha M. (2020): Health Diplomacy in Pandemical Times. Cambridge University Press. International Organization. Vol. 74. Issue S1. pp. E78 - E97. https://doi.org/10.1017 /S0020818320000326. Accesat la 13 aprilie 2021.

FIDLER, David (2001): The Globalization of Public Health: The First 100 Years of International Health Diplomacy. Bulletin of the World Health Organization. Vol. 79. Issue 9. Geneva. pp. 842-849. Print version ISSN 0042-9686. https://www.who.int/bulletin/archives/79(9)842.pdf

FIDLER, David (2020 b): Cybersecurity in the Time of COVID-19. Digital and Cyberspace Policy Program. Council on Foreign Relations. https://www.cfr.org/blog /cybersecurity-time-covid-19. Accesat la 5 decembrie 2020.

FREEMAN, Edward–Burton, Joseph (2019): Should Businesses Fight for Democracy? MIT Sloan Management Review. Disponibil la: https://sloanreview.mit.edu/article/business-in-society/.

GRILL, Paul (2020): Business Intelligence and the COVID-19 Pandemic. InfoSol Blog. Disponibil la: https://infosolblog.com/business-intelligence-and-the-covid-19-pandemic/. Accesat la 30 martie 2021.

HANSEN, Lene–Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly. Vol. 53. Issue 4. pp. 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

HARMAN, Sophie (2017): International Health Governance. Oxford Bibliographies. Disponibil la: https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0140.xml. Accesat la 2 mai 2019.

HELMREICH, Robert L. et al. (1999): The Evolution of Crew Resource Management Training in Commercial Aviation. The International Journal of Aviation Psychology. Vol. 9. pp. 19–32. http://dx.doi.org/10.1207/s15327108ijap0901_2.

JAMIL, George. (2013): Approaching Market Intelligence Concept through a Case Analysis: Continuous Knowledge for Marketing Strategic Management and its Complementarity to Competitive Intelligence. Procedia Technology 9. pp. 463-472, http://dx.doi.org/10.1016/j.protcy.2013.12.051.

JORA, Lucian (2020): Considerations Regarding the Global Need for a "Health Diplomacy". Romanian Review of Political Sciences and International Relations. Vol. XVII. Issue 2. pp. 114–121. https://acad.ro/bdar/rapInt2021/12fil/2InstStPolRelIntern_Raport.pdf. Accesat la 17 martie 2021.

KATZ, Rebecca et al. (2011): Defining Health Diplomacy: Changing Demands in the Era of Globalization. Milbank Q. Vol. 89. Issue 3. pp. 503-523. https://doi.org/10.1111/j.1468-0009.2011.00637.x.

KICKBUSCH, Ilona–Buss, Paulo (2011): Global Health Diplomacy and Peace. Infectious Disease Clinics of North America. Vol. 25. Issue 3. pp. 601-610. https://doi.org/10.1016/j.idc.2011.05.006.

LARICS.RO (2020): Donald Trump, Organizația Mondială a Sănătății și securizarea hard a Chinei. Începutul unui nou Război Rece. Disponibil la: https://larics.ro/donald-trump-organizatia-mondiala-a-sanatatii-si-securizarea-hard-a-chinei-inceputul-unui-nou-razboi-rece/. Accesat la 9 noiembrie 2020.

MA, Jianhua et al. (2016): Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure

Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand. pp. 1-9, https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.17.

MOORE, Richard (2020): Cyber Intelligence-Driven Risk: How to Build and Use Cyber Intelligence for Business Risk Decisions. ©2021 John Wiley & Sons, Inc. (P)2021 Gildan Media. ISBN: 978-1-119-67684-3. pp. 1-192. https://www.wiley.com/en-us/Cyber+Intelligence+Driven+Risk%3A+How+to+Build+and+Use+Cyber+Intelligence+for+Business+Risk+Decisions-p-9781119676843.

NATO (2021 a): Joint Press Point by NATO Secretary General Jens Stoltenberg, US Secretary of State Antony Blinken and US Secretary of Defense Lloyd J. Austin III. Disponibil la: https://www.nato.int/cps/en/natohq/opinions_183061.htm. Accesat la 15 mai 2021.

NATO (2021 b): NATO's Response to Hybrid Threats. Disponibil la: https://www.nato.int/cps/en/natohq/topics_156338.htm. Accesat la 7 aprilie 2021.

NUNES, João (2012): Health, Politics and Security. e-cadernos CES (online). pp. 142-164. Disponibil la: http://dx.doi.org/10.4000/eces.989.

NYE, Joseph (2010): Cyber Power. Belfer Center for Science and International Affairs, Harvard Kennedy School. pp. 1-19. Disponibil la: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. Accesat la 6 septembrie 2020.

REASON, James (2000): Education and Debate. Human Error: Models and Management. British Medical Journal. Vol. 320. pp. 768-770. REASON, James (2000): Education and Debate. Human Error: Models and Management. *British Medical Journal*. Vol. 320. pp. 768-770. https://dx.doi.org/10.1136%2Fbmj.320.7237.768.

SERVICIUL ROMÂN DE INFORMAȚII – SRI (2020 a): Amenințarea cibernetică în 2019. Evaluare și perspective de evoluție. Buletin Cyberint semestrul I 2020. https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2020.pdf. Accesat la 5 august 2020.

STARCEVIČ, Vladan et al. (2020): Cyberchondria in the Time of the COVID-19 Pandemic. Human Behaviour & Emerging Technologies 2020. pp. 53–61. https://doi.org/10.1002/hbe2.233.

UNITED NATIONS DEVELOPMENT PROGRAM (1994): Human Development Report 1994: New Dimensions of Human Security. pp. 1-137. Disponibil la: https://doi.org/10.18356/87e94501-en.

WEF - WORLD ECONOMIC FORUM (2020 c): The Global Risk Report 2020. Disponibil la: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Accesat la 5 septembrie 2020.

YAHAYA, Jamaiah et al. (2019): The Implementation of Business Intelligence and Analytics Integration for Organizational Performance Management: A Case Study in Public Sector. International Journal of Advanced Computer Science and Applications. Vol. 10. Issue 11. pp. 292-298. http://dx.doi.org/10.14569/IJACSA.2019.0101140.