FACTORI GENERATORI DE RISCURI LA ADRESA SECURITĂȚII UNIUNII EUROPENE

RISK FACTORS FOR THE SECURITY OF THE EUROPEAN UNION

Drd. Ioana NICA*

Rezumat: *Articolul realizează o cercetare teoretică și analitică asupra factorilor generatori de riscuri la adresa securității Uniunii Europene. Scopul acesteia este să analizeze atât factorii interni, cât și pe cei externi care contribuie la strategia de securitate a tuturor statelor membre. Având în vedere acest lucru, articolul pune în atenția cetățenilor factorii de risc care le pot pune în pericol siguranța și securitatea. Rolul Uniunii Europene este să le asigure acestora libertatea și să-i apere de orice factor care atentează la viața lor și îi face pe aceștia vulnerabili. Pentru a reuși acest lucru, U.E. a adoptat o strategie de apărare și securitate internă pentru a-i proteja pe cetățenii europeni.*

Cuvinte cheie: *securitate internațională, politica europeană de securitate și apărare, factori de risc, strategii de securitate, amenințare.*

Abstract: *This paper provides theoretical and analytical research on risk factors for European Union security. Its purpose is to analyze both internal and external factors that contribute to the security strategy of all member states. In view of this, the article draws the attention of citizens to the risk factors that may endanger their safety and security. The role of the European Union is to ensure their freedom and to protect them from any factor that threatens their lives and makes them vulnerable. To achieve this, the U.E. adopted an internal defense and security strategy to protect European citizens.*

Keywords: *international security, european security and defence policy, risk factors, security strategies, threat.*

Introducere

Instituțiile și statele europene au urmărit de-a lungul timpului să apere și să le garanteze cetățenilor respectarea drepturilor omului și statul de drept. Însă Uniunea Europeană (UE) se poate asigura, că politica de securitate este în continuare ancorată în valorile europene comune –

*Universitatea Națională de Apărare „Carol I”, Școala Doctorală, nica.ioana@myunap.net

respectarea și protejarea statului de drept, a egalității.[1] Ca europeni, avem libertatea de a munci, studia și trăi în orice țară din Europa dorim, fără ca viața să ne fie pusă în pericol. Securitatea internațională este un element foarte important în acest demers, iar pentru ca aceasta să fie pe deplin asigurată, UE trebuie să-și delimiteze clar obiectivele și să știe exact care sunt factorii generatori de riscuri care pot afecta siguranța cetățenilor. Membrii Consiliului European au creat astfel, o strategie de apărare pentru perioada 2020 - 2025, care își propune să dezvolte capacități pentru a asigura un mediu de securitate rezistent. Obiectivul principal al strategiei este acela de a oferi un dividend de securitate pentru a proteja toți cetățenii UE.

Securitatea internaţională este acea stare a sistemului de relaţii internaţionale în care toate statele lumii se află la adăpost de orice agresiune, act de forţă sau de ameninţare cu forţa în raporturile dintre ele, de orice atentat la adresa independenţei şi suveranităţii lor naţionale sau integrităţii teritoriale.[2]

Principalii factori generatori de riscuri cu care se confruntă, în acest moment, Europa sunt: terorismul, formele grave de criminalitate, criminalitatea organizată, traficul de droguri, criminalitatea informatică, atacurile cibernetice, traficul de fiinţe umane, exploatarea sexuală a minorilor și pornografia infantilă, infracţionalitatea economică și corupţia, traficul de armament și criminalitatea transfrontalieră. Totodată, însă, europenii se confruntă astăzi și cu un peisaj de securitate schimbător, afectat de amenințările în evoluție, precum și de alți factori, inclusiv schimbările climatice, tendințele demografice și instabilitatea politică dincolo de granițele UE.

Pandemia creată de Covid-19 în întreaga lume a dat o altă dimensiune securității, forțând UE și statele membre să se concentreze nu doar pe asigurarea siguranței fizice, ci și pe cea digitală. Astfel, a fost necesar ca acestea să se aprovizioneze cu echipamente și tehnologii performante, pentru a le oferi cetățenilor servicii și infrastructuri sigure. Se fac eforturi majore din partea U.E. și a țărilor terțe pentru a stopa

[1] O Uniune a egalității: Strategia privind egalitatea de gen 2020 - 2025, COM(2020) 152, disponibil la https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52020DC0152, accesat la 20.04.2021.

[2] Dicţionarul diplomatic, Editura Politică, Bucureşti, 1979, p. 789.

răspândirea virusului și pentru a proteja persoanele vulnerabile. Politica europeană de securitate și apărare se schimbă continuu, adaptându-se realității și încercând să surprindă principalii factori care sunt o amenințare pentru Europa.

Atacurile cibernetice și criminalitatea informatică continuă să crească, mai ales în aceste vremuri, când activitatea oamenilor s-a mutat în mediul online și Internetul este principala sursă de informare sau spațiu de lucru. În acest context, amenințările la adresa securității devin tot mai complexe și apăsătoare: se dezvoltă datorită capacității de a lucra transfrontalier și cu interconectivitatea; exploatează estomparea granițelor dintre lumea fizică și cea digitală; exploatează grupuri vulnerabile, divergențe sociale și economice. Atacurile pot apărea imediat și pot lăsa puține urme sau chiar deloc.

Trăim într-o eră în care schimbările apar de la o zi la alta. Programul de lucru s-a schimbat pentru majoritatea oamenilor, telemunca sau joburile remote (lucru de la domiciliu) fiind acum varianta optimă pentru a putea supraviețui într-o lume în care virusul a stopat mersul normal al lucrurilor. Suntem mereu conectați la diferite platforme de socializare și asta ne pune în fața unor riscuri de care mulți dintre noi nu suntem conștienți. În orice domeniu de activitate ai lucra, prezența online este esențială și contribuie la comunicarea cu oamenii. UE lucrează în permanență pentru a apăra cetățenii de atacuri cibernetice și furturi de date personale, și dorește să le asigure acestora un spațiu cibernetic securizat, unde să-și desfășoare activitățile în siguranță, fără temeri.

UE este un tot unitar, iar securitatea acesteia reprezintă și securitatea statelor membre. În ultima perioadă, amenințările asupra securității au tot apărut atât din exterior, cât și din interior, din diferite puncte de vedere: politic, militar, sanitar, economic, social, cultural etc.

1. Protejarea europenilor împotriva terorismului și a criminalității organizate

Terorismul rămâne o problemă nerezolvată în Europa și în întreaga lume și reprezintă o amenințare asupra modului de viață pe care-l au cetățenii. În 2019, s-a înregistrat o tendință de scădere a atacurilor teroriste în UE. Un număr de 13 state membre din UE au raportat 119 atacuri teroriste, iar 1004 persoane au fost arestate sub suspiciunea de infracțiuni legate de terorism în 19 state membre ale UE, Belgia, Franța, Italia, Spania

și Marea Britanie raportând cele mai mari cifre. Un număr de 10 persoane au murit din cauza atacurilor teroriste din UE și 27 de persoane au fost rănite. Cu toate acestea, se menține la un nivel ridicat amenințarea la adresa cetățenilor UE a unui atac jihadist comis de Da'esh și Al-Qaida și de grupările afiliate acestora sau inspirat de acestea.[3] În paralel, este în creștere și amenințarea violenței extremismului de dreapta.[4]

În acest sens, Gilles de Kerchove, coordonatorul UE al luptei împotriva terorismului, a declarat că: *„Trebuie să fim vigilenţi, din moment ce ameninţarea reprezentată de aşa-numitul Stat Islamic (IS) şi revenirea luptătorilor străini ar putea să persiste în următorii ani. Aceşti oameni sunt instruiţi să folosească explozibili şi arme de foc şi au fost îndoctrinaţi cu ideologia jihadistă. Un răspuns eficient necesită o abordare cuprinzătoare şi un angajament pe termen lung. Desigur, responsabilitatea principală în lupta împotriva terorismului le revine statelor membre. Cu toate acestea, UE şi agenţiile sale, cum ar fi Europol, pot şi ar trebui să joace un rol de susţinere, ajutând la combaterea caracterului transfrontalier al ameninţării"*.[5]

De-a lungul timpului, UE a adoptat diferite strategii pentru combaterea terorismului, multe dintre ele având efecte pozitive. În urma atacurilor teroriste din Franța, Germania și Austria, din 2020, miniștrii afacerilor interne din UE au decis să pună și mai mult accent pe combaterea terorismului, fără a se abate de la valorile comune care fac referire la democrație, justiție și libertatea de exprimare. Fiind un subiect atât de delicat, căruia i se acordă o atenție deosebită, UE mai adoptă în martie 2021, un regulament prin care să prevină și să combată conținutul online cu caracter terorist. Actul normativ obligă furnizorii de servicii din mediul online *„să elimine conținutul cu caracter terorist sau să blocheze accesul la*

[3] Europol, European Union Terrorism Situation and Trend Report (TE-SAT) 2020, disponibil la https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020, accesat la 04.05.2021.

[4] În 2019, s-au înregistrat șase atacuri teroriste de dreapta (unul a fost dus la capăt, unul a eșuat, patru au fost dejucate: trei dintre acestea având ca țintă state membre UE), comparativ cu un singur atac în 2018, și mai multe decese survenite în cazuri care nu au fost clasificate drept acte de terorism (Europol, 2020).

[5] Islamic State Changing Terror Tactics to Maintain Threat in Europe, 02 December 2016, Press Release, disponibil la https://www.europol.europa.eu/newsroom/news/islamic-state-changing-terror-tactics-to-maintain-threat-ineurope, accesat la 06.05.2021.

acesta în toate statele membre. Platformele de internet trebuie apoi să elimine conținutul sau să blocheze accesul la acesta în termen de o oră."[6]. Normele legislative urmează să fie puse în aplicare începând cu anul 2022.

Combaterea acestui fenomen începe prin abordarea polarizării societății, discriminării și altor factori dăunători care creează conflicte între cetățeni și întărește vulnerabilitatea acestora. Uniunea Europeană urmărește să descopere cauzele profunde care provoacă atentatele de terorism și dorește să urmărească penal teroriștii, chiar și luptătorii teroriști străini. Pentru a îndeplini acest obiectiv, va trebui să se ia în considerare măsuri de consolidare a legislației privind securitatea frontierelor și o utilizare mai eficientă a bazelor de date existente. Comunicarea și colaborarea cu țările terțe, dar și cu organizațiile internaționale va fi foarte importantă pentru combaterea terorismului, deoarece în acest mod se vor elimina sursele de finanțare a acestuia.

Criminalitatea organizată produce costuri uriașe pentru victime, dar și pentru state, afectând foarte mult partea economică a acestuia. Din unele evaluări prezentate la recentele congrese de specialitate, desfăşurate la nivel mondial, a reieşit faptul că economia interlopă este a doua afacere la nivel mondial.[7]

Combaterea acestei amenințări poate fi efectuată printr-o comunicare directă cu interlopii care practică astfel de lucruri, determinându-i să renunțe și să își reamintească valorile statului din care fac parte.

2. Amenințări cibernetice

Atacurile cibernetice au început să crească în această perioadă, când majoritatea afacerilor își desfășoară activitatea în mediul online, fiind dependente de tot ce înseamnă Internet. Acestea provin dintr-o gamă largă de surse, atât din interiorul UE, cât și din exteriorul acesteia și au ca țintă zone foarte vulnerabile. Se preconizează că această tendință va continua să crească în viitor, date fiind previziunile conform cărora 22,3 miliarde de dispozitive la nivel mondial vor fi conectate la internetul obiectelor până în

[6] Răspunsul UE la amenințarea teroristă, Noi norme ale UE privind eliminarea conținutului cu caracter terorist de pe internet, disponibil la https://www.consilium.europa.-eu/ro/policies/fight-against-terrorism/, accesat la 06.05.2021.

[7] Iulian Cifu, „Lungul drum de la dialog la cooperare", *Ocasional Papers*, nr. 2/2003, Casa NATO, p. 34.

2024. În acest context, este extrem de important ca spitalele, centrele de cercetare, infrastructura companiilor și a tuturor cetățenilor să fie bine protejată.

Există mai multe metode prin care hackerii pot accesa date importante ale unei companii sau ale unei persoane. Una dintre acestea este folosirea unor programe malware, care reușesc să obțină accesul unui dispozitiv fără ca deținătorul să-și dea seama de acest lucru. Această modalitate este folosită deseori și în spionaj. Atacurile prin Internet se realizează și prin diferite tehnici de utilizare și redirecționare a browser-ului către site-uri rău intenționate.

O altă modalitate prin care se poate face furt de date personale este prin Phishing. Prin intermediul acesteia se încearcă obținerea datelor personale sau confidențiale cum ar fi numărul de telefon, adresa de e-mail, cardul de credit sau alte informații importante pe care le deține o persoană. În timpul epidemiei s-a observat o creștere alarmantă a furtului de date personale prin phishing, cu 67% a înșelătoriilor. Un alt mod prin care se realizează atacurile cibernetice este trimiterea de mesaje spam, prin care se distribuie conținutul care te direcționează spre site-uri dubioase. Un procent de 66% dintre amenințările cibernetice legate de pandemia de Covid-19 provin din e-mailurile de tip spam.

Tentativele frauduloase mai pot fi făcute și sub forma de „*darknet*" (partea întunecată/ilegală a Internetului), pentru a vinde bunuri ilicite și servicii de piratare. Astfel, securitatea informațională este extrem de importantă și trebuie să le asigure cetățenilor siguranță în preluarea datelor cu caracter personal. UE trebuie să le asigure acestora o infrastructură digitală care să nu le afecteze viața și activitățile zilnice.

În timpul pandemiei de Covid-19, noile tehnologii au menținut funcționarea multor întreprinderi și servicii publice, indiferent dacă ne-au menținut conectați prin munca la distanță sau prin menținerea logisticii lanțurilor de aprovizionare. Acest lucru a deschis, însă, ușa unei creșteri extraordinare a atacurilor cibernetice, încercând să valorifice perturbarea pandemiei și trecerea în mediul digital, care funcționează în scopuri criminale. Hackerii au profitat de pandemie și au produs pagube în bugetul multor companii, în special, celor din domeniu sănătății. Aceștia au profitat de situația din această perioadă și le-au trimis oamenilor știri false legate de Covid-19, au intrat în sistemul organizațiilor de sănătate, au făcut înșelătorii

online cu măști, tratamente și medicamente sau au efectuat atacuri cibernetice împotriva infrastructurii de telemuncă.

În martie 2020, Spitalul Universitar din Brno, Cehia a suferit un atac cibernetic în urma căruia spitalul a fost nevoit să redirecționeze pacienți și să amâne intervenții chirurgicale (Europol: Pandemic Profiteering. How criminals exploit the Covid-19 crisis). Inteligența artificială poate fi utilizată în mod abuziv pentru atacuri digitale, politice și fizice, precum și în scopul supravegherii. Colectarea datelor în cadrul internetului obiectelor poate fi utilizată pentru supravegherea persoanelor (ceasuri inteligente, asistenți virtuali etc.).[8]

Din cauza faptului că oamenii au lucrat mai mult de acasă, angajatorii au fost obligați să găsească soluții de securitate pentru ca aceștia să acceseze datele în siguranță, fără a exista teama de furt de date sau chiar intrări în sistem. Astfel, companiile au apelat la software VPN, programe pentru detectarea atacurilor cibernetice sau varianta autentificării în doi pași.

Victor Gânsac, CEO al Safetech Innovations, a declarat într-un interviu faptul că *„2020 a fost cu adevărat un an prielnic pentru atacatorii cibernetici. Multe nume sonore din piaţă au avut probleme de securitate şi pierderi de date care au avut un impact reputaţional major pe lângă pierderile evidente de bani. Ce am observat noi este faptul că efortul atacatorilor are o distribuţie mai targetată astfel că, odată ce reuşesc să treacă de sistemele de apărare ale companiilor, caută să exploateze vulnerabilităţile care le aduc cel mai mare câştig”*.[9]

În cadrul reuniunii extraordinare a Consiliului European din octombrie 2020, liderii UE au solicitat sporirea capacității UE de a se proteja împotriva amenințărilor cibernetice, de a oferi un mediu de comunicare securizat, în special prin intermediul criptării cuantice, și de a asigura accesul la date în scopuri judiciare și de asigurare a respectării

[8] Europol: Pandemic Profiteering. How criminals exploit the Covid-19 crisis, Report, disponibil lahttps://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis, accesat la 06.05.2021.

[9] Apud Alex Ciutacu, „Atacurile cibernetice ating noi culmi. Cum a ajutat pandemia hackerii şi unde s-a ajuns de la vremurile când funcţionau atacurile de tip „prinţul nigerian”, disponibil la https://www.businessmagazin.ro/business-hi-tech/atacurile-cibernetice-ating-noi-culmi-cum-a-ajutat-pandemia-hackerii-19779316, accesat la 07.05.2021.

legii.[10] Astfel, Uniunea Europeană a decis să combată atacurile informaționale prin diferite metode: să crească reziliența cibernetică, să combată criminalitatea cibernetică, să stimuleze diplomația cibernetică, să întărească apărarea cibernetică, să cerceteze și să inoveze noi tehnologii împotriva atacurilor cibernetice și să protejeze infrastructura critică, care este pusă în pericol.

3. Factori de risc psihosociali

Munca de la distanță a adus beneficii pentru majoritatea persoanelor, mai ales din punct de vedere economic. Însă, după un an în care ai stat ore în șir la biroul din cameră sau la masa din bucătărie, apar și efectele negative ale telemuncii. Stresul și epuizarea create de pandemie sunt în creștere și tot mai mulți oameni se plâng de faptul că nu mai rezistă să-și petreacă timpul doar în casă, făcând zi de zi aceleași lucruri. Lipsa de concentrare la job a scăzut față de începutul pandemiei și productivitatea nu mai este la fel de mare. Aceste lucruri dau naștere mai multor riscuri de securitate, din cauza faptului că nu mai acordăm o atenție deosebită protecției împotriva atacurilor cibernetice. Acum, după un an petrecut la biroul de acasă, ești tentat să cazi pradă involuntar hackerilor din cauza presiunii mentale. Oamenii pot comite greșeli fatale în aceste momente încărcate cu stări negative și pot deschide e-mailuri sau pot da click-uri pe site-uri de phishing, sau pot distribui site-uri rău făcătoare fără să-și dea seama.

4. Factori de risc privind dezastrele naturale și schimbările climatice

UE investește constant în măsurile de reducere a efectelor dezastrelor naturale sau a celor provocate de om. Incendiile, cutremurele sau inundațiile afectează întreaga populație și duc la pierderi semnificative. Dezastrele naturale accentuează polarizările și sărăcia, iar cel mai îngrijorător lucru din ultima perioadă este încălzirea globală. Natura pare că are alte planuri și după cum declară Jerome Haegeli, Group Chief Economist, Swiss Re *„schimbările climatice devin tot mai vizibile în creşterea frecvenţei cu care apar pericolele secundare, cum ar fi inundaţii fulgerătoare, secete şi incendii de vegetaţie.*

[10] Securitatea cibernetică: modul în care UE combate amenințările cibernetice, disponibil la https://www.consilium.europa.eu/ro/policies/cybersecurity/, accesat la 08.05.2021.

Riscurile de dezastre naturale sunt în creştere, iar schimbările climatice le vor exacerba în mod semnificativ. Acest lucru subliniază nevoia urgentă de a ne proteja mai bine comunităţile împotriva pierderilor provocate de catastrofe, reducând dramatic, în acelaşi timp, emisiile de carbon. Dacă nu se iau măsuri de atenuare, costul pentru societate va creşte în viitor"[11]. Astfel, dacă până acum ştiai clar când este iarnă şi când este vară, acum temperaturile s-au modificat şi apar schimbări bruşte de la o zi la alta. Pentru a preveni şi combate dezastrele naturale, statele membre trebuie să impună măsuri radicale de protejare a mediului înconjurător.

În 2015, UE a venit în sprijinul persoanelor afectate de dezastrele naturale şi ale celor provocate de om în Europa şi în alte părţi ale lumii. Astfel, au primit ajutor peste 134 de milioane de beneficiari afectaţi de dezastre naturale sau de conflicte în peste 80 de ţări[12]. Bugetul destinat ajutorului umanitar pentru 2015, – cel mai mare buget executat vreodată de Comisie – a constituit o reacţie la creşterea continuă a frecvenţei şi gravităţii dezastrelor naturale şi altor situaţii de criză umanitară.

În decembrie 2015, UE a anunţat o contribuţie de 125 de milioane euro pentru finanţarea unor acţiuni de urgenţă în ţările afectate de fenomene meteorologice extreme, cum ar fi fenomenul *El Niño* din Africa, Caraibe, America Centrală şi de Sud. În zonele extrem de vulnerabile la nivel local, sunt susţinute acţiuni specifice de reducere a riscului de dezastre şi dezvoltare a capacităţii locale.[13] Totodată, UE a contribuit şi la sprijinirea Portugaliei, în 2017, când a fost lovită de incendii, ajutând statul la reconstruirea regiunilor afectate de dezastre.

[11] Cristian Suca, „Catastrofele naturale din 2020 - pericolele secundare, in centrul atentiei", disponibil la https://www.1asig.ro/Swiss-Re-Catastrofele-naturale-din-2020-pericolele-secundare-in-centrul-atentiei-articol-3,117-65796.htm, accesat la 08.05.2021.

[12] Raport al Comisiei către Parlamentul European şi Consiliu, Raportul anual privind politicile Uniunii Europene în domeniul ajutorului umanitar şi al protecţiei civile şi privind punerea lor în aplicare în 2015, disponibil la https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A52016DC0751, accesat la 08.05.2021.

[13] Prevenirea dezastrelor naturale şi a celor provocate de om în Uniunea Europeană, disponibil la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM-:pr0005, accesat la 09.05.2021

Concluzii

Factorii generatori de riscuri se schimbă de la un an la altul, sau chiar de la o lună la alta, pericolul fiind imprevizibil pentru omenire. Există o mulțime de riscuri care pot afecta securitatea UE, însă potențialul și puterea pe care aceasta o deține nu poate destabiliza o forță atât de mare. Datorită pregătirii constante, investirii și dedicării, concentrarea spre nevoile cetățenilor, statele membre pot face față amenințărilor venite din diferite direcții prin politicile și strategiile bine implementate de securitate. Este necesar ca UE să facă îmbunătățiri în permanență asupra acestora și să caute cele mai bune soluții pentru cetățeni, pentru a-i proteja și a le respecta drepturile, securitatea fiind unul dintre acestea.

Astfel, se poate observa că noțiunea de securitate, în această perioadă, face referire mai mult la sistemul sanitar și cibernetic, la cum putem stopa răspândirea virusului și cum putem reveni la viața dinaintea pandemiei. Atacurile cibernetice și furturile de date personale sunt o reală problemă socială cu care ne confruntăm în această perioadă. Totuși, acțiunile de terorism și crimă organizată nu trebuie neglijate, ele reprezentând în continuare o amenințare pentru statele membre.

Noua strategie adoptată de UE, care are ca scop punerea bazelor unui ecosistem în materie de securitate, pornește de la premisa că securitatea este responsabilitatea tuturor statelor membre. Aceasta afectează în aceeași măsură pe toată lumea și principalul obiectiv al UE este siguranța individului, a cetățeanului și a drepturilor acestuia. Cu toții putem contribui la siguranța noastră prin îndeplinirea responsabilităților față de țară. Strategia recunoaște, de asemenea, faptul că amenințările la adresa securității nu se limitează la frontierele geografice, precum și interdependența tot mai mare dintre securitatea internă și cea externă.[14] Atacurile și amenințările pot apărea în orice moment, însă UE poate avea un răspuns imediat, bazat pe sistemul general de coordonare a situațiilor de criză și poate acționa ca atare, atât în interior, cât și în exteriorul frontierelor. Astfel, principalul obiectiv al strategiei adoptate de UE este să obțină o securitate aproape garantată pentru toți cetățenii europeni.

[14] EU Global Strategy, disponibil la https://eeas.europa.eu/topics/eu-global-strategy_en, accesat la 10.05.2021

BIBLIOGRAFIE

CIFU I., *Lungul drum de la dialog la cooperare*, Ocasional Papers, nr. 2/2003, Casa NATO;

CIUTACU A., „Atacurile cibernetice ating noi culmi. Cum a ajutat pandemia hackerii şi unde s-a ajuns de la vremurile când funcţionau atacurile de tip „prinţul nigerian", disponibil la https://www.businessmagazin.ro/business-hi-tech/atacurile-cibernetice-ating-noi-culmi-cum-a-ajutat-pandemia-hackerii-19779316, accesat la 07.05.2021;

SUCA C., „ Catastrofele naturale din 2020 - pericolele secundare, in centrul atentiei", disponibil la https://www.1asig.ro/Swiss-Re-Catastrofele-naturale-din-2020-pericolele-secundare-in-centrul-atentiei-articol-3,117-65796.htm, accesat la 08.05.2021;

Dicționarul diplomatic, Editura Politică, București, 1979;

O Uniune a egalității: Strategia privind egalitatea de gen 2020-2025, COM(2020) 152, disponibil la https://eur-lex.europa.eu-/legalcontent/RO/TXT/?uri=CELEX:52020DC0152, accesat la 28.04.2021;

Răspunsul UE la amenințarea teroristă, Noi norme ale UE privind eliminarea conținutului cu caracter terorist de pe internet, disponibil la https://www.consilium.europa-.eu/ro/policies/-fight-against-terrorism/, accesat la 06.05.2021:

Securitatea cibernetică: modul în care UE combate amenințările cibernetice, disponibil la https//www consilium.europa.eu/-ro/policies/cybersecurity/, accesat la 08.05.2021;

Prevenirea dezastrelor naturale și a celor provocate de om în Uniunea Europeană, disponibil la https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:pr0005, accesat la 09.05.2021;

EU Global Strategy, disponibilă la https://eeas.europa.eu/topics/eu-global-strategy_en, accesat la 10.05.2021;

Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis, Report, disponibil la https:/www.europol.europa.eu-

/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis, accesat la 06.05.2021;

European Union Terrorism Situation and Trend Report (TE-SAT) 2020, disponibil la https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020, accesat la 04.05.2021;

Islamic State Changing Terror Tactics to Maintain Threat in Europe, 02 December 2016, Press Release, disponibil la https://www.-europol.europa.eu/newsroom/news/islamic-state-changing-terror-tactics-to-maintain-threat-ineurope, accesat la 06.05.2021.