ROMÂNIA
SERVICIUL ROMÂN DE INFORMAŢII
ACADEMIA NAŢIONALĂ DE INFORMAŢII
„MIHAI VITEAZUL"
Nr. 589973 din 16.11.2018

NESECRET
Ex. unic

COPIE XEROX
U.M. 0418 BUCUREŞTI
Nr. R.M. 0036/0649 ex. nr. 1

RAPORT DE ANALIZĂ
din data de 16.11.2018

Subsemnaţii,

din cadrul Academiei Naţionale de Informaţii „Mihai Viteazul", numiţi membri ai **Comisiei de analiză** prin Hotărârea de Senat nr. 589801/05.11.2018 şi Decizia Rectorului nr. 589804/05.11.2018, în vederea analizării tehnice a tezei de doctorat

Securitatea informatică - factor determinant în buna funcţionare a infrastructurilor critice, susţinută în data de **17.07.2013** la Academia Naţională de Informaţii „Mihai Viteazul" de către **MARIUS STICLARU**, sub coordonarea prof.univ.dr. **GHEORGHE TOMA**

- am analizat *Rapoartele de Similitudine* ale tezei menţionate, realizate la nivelul Academiei Naţionale de Informaţii "Mihai Viteazul" folosind programul www.sistemantiplagiat.ro validat prin Ordin nr. 3485 / 24.03.2016 privind lista programelor recunoscute de CNATDCU şi utilizate la nivelul instituţiilor de învăţământ superior organizatoare de studii universitare de doctorat şi al Academiei Române, în vederea stabilirii gradului de similitudine pentru lucrările ştiinţifice,

- totodată, am analizat, în întregime, din punctul de vedere al respectării normelor academice de redactare a unei lucrări ştiinţifice şi a eticii universitare teza de doctorat menţionată mai sus, şi am constatat următoarele:

NESECRET

CONFORM CU ORIGINALUL

1. Coeficientul de similitudine 1 (procent al documentelor analizate care au fost identificate în alte surse, excluzând fragmente găsite în Baza de Date cu Acte Legale) este de 38,8%;
2. Coeficientul de similitudine 2 (Numărul de procente al documentelor analizate găsite în alte surse, exceptând fragmentele găsite în Baza de date a Actelor Legale – numai fragmentele mai mari de 25 de cuvinte sunt luate în consideraţie) este de 15,7%.

În urma analizei tehnice realizate pornind de la rapoartele de similitudine generate de platforma www.sistemantiplagiat.ro (folosindu-se, pentru verificare, forma fizică a tezei de doctorat) am constatat faptul că unele surse conduceau către adrese web care nu pot fi accesate din Reţeaua Locală Internet (de ex. scribd.com/document). De asemenea, sursa http://ccpic.mai.gov.ro/ nu poate fi datată, sursa https://www.setthings.com/ro/conceptul-de-criminalitate-informatica/ este datată octombrie 2014, iar http://www.academiadepolitie.ro/root/studii/iosud/rezumate_teze/2016/toma/rezumat_toma.pdf este datată 2016.

Referitor la celelalte situaţii de similitudine, s-a constatat preluarea integrală sau parţială din textul sursă, fără citarea sursei şi menţionarea autorului nici în text și nici la bibliografie, a unui număr de 1.258 cuvinte (în Anexă cu Bold) (din totalul de 53.608 cuvinte al tezei) din sursele (*prezentarea detaliată a textelor identificate în Anexă*):

- https://andreivocila.wordpress.com/2010/10/01/consideratii-privind-securitatea-internationala-a-romaniei/
- https://www.bacau.net/strategie-in-domeniul-securitatii-cibernetice-la-nivel-european/
- http://riti-internews.ro/Capitolul%2005%20-%20Reglementarea%20criminalitatii%20informatice.pdf
- http://intelligence.sri.ro/atacuri-si-amenintari-la-adresa-securitatii-infrastructurilor-critice/

De asemenea s-au identificat, în teză, 6.335 cuvinte fără citare sursă, sursa fiind dată la bibliografie.

Comisia:

CONFORM CU ORIGINALUL

ANEXĂ

VERIFICAREA TEZEI DE DOCTORAT

Securitatea informatică -factor determinant în buna funcţionare a infrastructurilor critice

2013

Autor: MARIUS STICLARU

Conducător de doctorat prof. univ. dr. GHEORGHE TOMA

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
Coroiu Viorel, teza de doctorat *Criminalitatea informatică – factor de risc major pentru ordinea publică și siguranța națională*, Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf	2011	**Pagina 5.** Lumea de astăzi,presupune o modalitate de trai şi de a lucra într-o lume de conectivitate la nivel mondial. Putem face schimb de conversaţie sau putem realiza tranzacţii de milioane de dolari tranzacţii monetare cu oamenii de pe partea cealalta a planetei rapid şi ieftin. Proliferarea de calculatoare personale, acces facil la Internet, precum şi o piaţă în plină expansiune pentru noile dispozitive de comunicare ne-au schimbat modul în care ne petrecem timpul liber şi modul în care facem afaceri.	79	Fără citare sursă, sursa este dată la bibliografie.
Coroiu Viorel, teza de doctorat *Criminalitatea informatică – factor de*	2011	**Pagina 6.** Această evoluţie, rapidă şi radicală, ridică o serie de	69	Fără citare sursă, sursa

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
risc major pentru ordinea publică și siguranța națională, Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf		problem de ordin socioeconomic sau juridic, şi chiar în sectorul activităţii criminale - calculatorul deschizând posibilitatea unor acţiuni ilegale cu un caracter înalt sofisticat sau la săvârşirea unor infracţiuni clasice cum este furtul sau frauda. Toate aceste acţiuni ilegale au făcut să apară necesitatea ocrotirii valorilor sociale tradiţionale împotriva atacurilor ilicite prin intermediul calculatoarelor, susceptibile să producă pagube economice semnificative.		este dată la bibliografie.
Andrei Vocilă, *CONSIDERAŢII PRIVIND SECURITATEA INTERNAŢIONALĂ A ROMÂNIEI,* https://andreivocila.wordpress.com/2010/10/01/consideratii-privind-securitatea-internationala-a-romaniei/	**2010**	**Pagina 12. ....la începutul secolului XXI, caracteristica generală a mediului de securitate european constă în diminuarea riscurilor convenţionale şi, ca urmare, eliminarea premiselor apariţiei unui conflict armat de amploare continentală sau regională. Concomitent se constată un fenomen de amplificare a riscurilor şi ameninţărilor neconvenţionale.**	**42**	**Fără citare sursă**
Coroiu Viorel, teza de doctorat *Criminalitatea informatică – factor de risc major pentru ordinea publică și siguranța națională,* Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf	2011	**Pagini 13-14.** Deoarece dreptul tradiţional a devenit insuficient, neputând acoperi noile probleme, a devenit necesară modificarea normativului existent sau crearea unor noi categorii de infracţiuni, dacă alte măsuri se dovedesc nesatisfăcătoare. Modalităţile în care se comit infracţiuni sunt, de asemenea, în continuă schimbare. Accesibilitatea digitală universală deschide noi	**210**	Fără citare sursă, sursa este dată la bibliografie

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		oportunități pentru cei lipsiți de scrupule. Milioane de dolari sunt pierdute de către ambele părți, întreprinderi şi consumatori, din cauza activității criminale. Mai rău, computere şi rețele pot fi folosite pentru a hărțui victime sau pentru atacuri violente, inclusiv teroriste. Pentru a îmbunătăți lucrurile, legile vechi, care nu se potrivesc suficient de bine cu infracțiunile de acest gen, au fost abrogate sau modificate, fiind adoptate noi legi mai bine ancorate în realitate. In plus, dezbaterile asupra unor probleme de confidențialitate îngreunează capacitatea organelor de aplicare a legii de a aduna probele necesare pentru a urmări cazurile de infracționalitate cibernetică. Nu în ultimul rând, a existat şi o anumită cantitate de antipatie, sau cel puțin neîncredere, între cei doi dintre cei mai importanți jucători în orice luptă eficientă împotriva criminalității informatice: agențiile de aplicare a legii şi profesioniştii în IT. Cu toate acestea, o cooperare strânsă între aceştia este crucială pentru prevenirea şi combaterea criminalității informatice şi transformarea internetului într-un sistem sigur pentru utilizatorii săi.		
Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, Amenințări la adresa acestora. Sisteme de protecție,* Editura UNAp, Bucureşti, 2006,	2006	**Pagini 15-17.** Înmulțirea, fără precedent, în ultimele decenii, a riscurilor, pericolelor şi amenințărilor la adresa obiectivelor vitale ale statelor şi ale organismelor internaționale, concomitent cu creşterea numărului şi	**633**	Fără citare sursă, sursa este dată la bibliografie. Sunt copiate

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf		vulnerabilităţii acestora, a condus la sedimentarea şi statuarea unui nou concept, denumit generic: infrastructură critică. Dacă primele studii în domeniu au identificat obiectivele considerate „critice", încă din anii '80, sintagma „infrastructură critică" a fost folosită, în mod oficial, în iulie 1996, când preşedintele SUA a decretat „Ordinul Executiv pentru Protecţia Infrastructurilor Critice"1. În preambulul la acest act normative se explică noţiunea de infrastructura critică drept acea „parte din infrastructura naţională care este atât de vitală încât distrugerea sau punerea ei în incapacitate de funcţionare pot să diminueze grav apărarea sau economia SUA". Se considera că aceasta cuprindea: telecomunicaţiile, sistemul de aprovizionare cu electricitate şi apă, depozitele de gaze şi petrol, finanţele şi băncile, serviciile de urgenţă (medicală, poliţie şi pompieri), precum şi continuitatea guvernării. În toamna aceluiaşi an, a fost înfiinţată Comisia Prezidenţială pentru Protecţia Infrastructurilor Critice, care a apreciat că securitatea, economia, şi chiar supravieţuirea lumii industrializate depind de trei elemente interrelaţionate: energia electrică, comunicaţiile şi computerele2. 11 septembrie 2001 avea să demonstreze că o ţară, oricât de puternică ar fi, nu poate să-şi asigure, de		integral și notele de subsol din articolul original.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		una sigură, apărarea eficientă a tuturor centrilor săi vitali. După dezastrul rămas în urma loviturii teroriste, SUA au decis să unească în jurul lor statele lumii care doreau să lupte împotriva acestui flagel. Globalizarea, odată cu avantajele şi transformările pozitive ce le aduce la nivel naţional, dă posibilitatea propagării rapide, la scară planetară, a ameninţărilor directe la adresa securităţii tuturor. La incercările de globalizare a insecurităţii trebuia să se răspundă prin măsuri ferme de blocare şi eliminare a ameninţărilor prezente şi pericolelor viitoare şi instituirea unui sistem de globalizare a securităţii. În acest sens, un prim pas a fost făcut de Washington în direcţia eliminării vulnerabilităţii obiectivelor naţionale vitale, pe care le preciza ca fiind cele de natură umană, economică, informaţională, din cadrul serviciilor guvernamentale principale şi a securităţii naţionale a SUA. Pentru aceasta, în luna octombrie a aceluiaşi an, Casa Albă a elaborat: Ordinul Executiv pentru Protecţia Infrastructurilor Critice3. Prin acesta se urmărea asigurarea continuităţii conducerii vieţii politicoeconomice şi protejarea populaţiei de orice întrerupere a ei4. Tema a fost dezvoltată, în 2003, în cadrul Strategiei Naţionale de Securizare a Spaţiului Cibernetic. Documentul a definit, de data acesta, o		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		compunere a infrastucturii critice mult mai amplă şi mai precisă. Astfel, infrastucturile critice reprezentau: „instituţii publice şi private din sectoarele agriculturii, alimentaţiei, aprovizionării cu apă, sănătăţii publice, serviciilor de urgenţă, guvernării, industriei de apărare, informaţiilor şi telecomunicaţiilor, energiei, transporturilor, bancare şi financiare, chimice şi a materialelor periculoase, precum şi cele poştale şi de navigaţie"5. Nevoia de a defini şi proteja în mod organizat centrii vitali ai unei entităţi a fost resimţită şi de organizaţiile internaţionale. Astfel, în cadrul Alianţei Nord-Atlantice, prin infrastructură critică statele membre înţeleg: „facilităţi, servicii şi sisteme informatice care sunt atât de vitale pentru naţiuni, încât scoaterea lor din funcţiune sau distrugerea lor poate avea efecte de destabilizare a securităţii naţionale, economiei naţionale, stării de sănătate a populaţiei şi asupra funcţionării eficiente a guvernului"6. În ultimii ani, statele Uniunii Europene au întreprins acţiuni viguroase în direcţia stabilirii uni limbaj şi unui mod de acţiune comun în vederea protejării obiectivelor lor de valoare strategică. În general, statele comunitare au stabilit în categoria obiectivelor critice: telecomunicaţiile, sursele de apă şi de energie, reţelele de distribuţie, producţia şi distribuire a hranei, instituţiile		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		de sănătate, sistemele de transport, serviciile financiar-bancare, instituţiile de apărare şi ordine publică (armata, jandarmeria şi poliţia. Austria, Franţa, Marea Britanie, Spania au înfiinţat organisme specifice, au dezvoltat metodologii, şi au alocat fonduri substanţiale pentru protecţia infrastructurilor desemnate drept critice. Germania are un program de protecţie a acestora care este condus de Biroul Federal pentru Informaţii în Domeniul Securităţii.		
HG 718/13.07.2011 Strategia naţională privind protecţia infrastructurilor critice, http://www.legex.ro/Hotararea-718-2011-114287.aspx	2011	**Pagini 24-26.** Dezvoltarea economico-socială stimulată de progresul tehnologic accelerat şi manifestarea fenomenului globalizării au consolidat interdependenţa puternică şi interacţiunea sistemelor ce asigură securitatea şi bunăstarea societăţii umane. Necesitatea interconexării sistemelor pe fondul tendinţei de eliminare a barierelor administrative şi de acces pe noile pieţe emergente, concomitent cu integrarea reţelelor de infrastructuri, determină evoluţii în planul securităţii şi stabilităţii în plan global. Evoluţiile rapide și, uneori, cu un grad ridicat de imprevizibilitate, dublate de dimensiunea și complexitatea vulnerabilităților și riscurilor, generează o provocare majoră pentru sistemele de protecţie a infrastructurilor critice. Interconexiunile transnaţionale ale infrastructurilor și sfera de manifestare a riscurilor, ce au	**509**	Fără citare sursă, sursa este dată la bibliografie

CONFORM CU ORIGINALUL

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		împrumutat elementele de reprezentare și evoluție configurate de procesul de globalizare, prefigurează premise de perpetuare, prin "rezonanță", a riscurilor la adresa infrastructurilor critice și permit extinderea "în sistem cascadă", pe spațiul altor state, a efectelor agresiunii asupra unor sisteme sau procese. Fenomenul globalizării, odată cu avantajele și transformările pozitive ce le aduce la nivel internațional, dă posibilitatea propagării rapide, la scară planetară, a amenințărilor directe la adresa securității tuturor. La tendințele de globalizare a insecurității trebuie să se răspundă prin măsuri ferme de blocare și eliminare a amenințărilor prezente și pericolelor viitoare, precum și instituirea unui sistem de globalizare a securității. Riscurile și amenințările la adresa obiectivelor vitale pentru funcționarea societății și securitatea cetățenilor au căpătat noi valențe, cu dinamică ridicată și grad de intensitate crescut, fapt ce a condus la necesitatea unei abordări integrate a conceptului de "infrastructură critică". Pornind de la caracteristicile de bază ale infrastructurilor critice, elementul de criticitate al stabilității acestora, inclusiv în context transfrontalier, a căpătat noi conotații în planul strategiilor naționale/transnaționale. Complexitatea protecției infrastructurilor critice și importanța acestora pentru stabilitatea socială, respectiv		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		securitatea cetățeanului și a statului, a generat corelarea concretă a strategiilor inițiate la nivelul statelor și organizațiilor. Conexiunile dintre funcționalitatea și viabilitatea infrastructurilor critice și elementele fundamentale ale vieții economico-sociale, politice și militare ale unui stat, alianțe etc. consolidează semnificativ liantul dintre elementul de securitate și rolul sistemelor de infrastructuri în exprimarea necesităților și promovarea intereselor naționale, indiferent de configurația contextuală. În ultimii ani, producerea actelor teroriste, întreruperea deliberată a furnizării de materii energetice la nivelul unor state, producerea unor accidente tehnologice ca urmare a unor greșeli umane sau a unor dezastre/calamități naturale au scos în evidență vulnerabilitatea unor infrastructuri critice naționale, iar statele membre ale Uniunii Europene au întreprins acțiuni ferme în direcția stabilirii unui mod de acțiune comun în vederea protejării obiectivelor lor de valoare strategică. Mediul de securitate actual este caracterizat de mutații semnificative atât în privința relevanței actorilor regionali și globali și a caracteristicilor mediului de derulare a înfruntărilor, cât și a obiectivelor de gestionare optimă a problematicii. Astfel, motivațiile tradiționale, cum ar fi		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		câștigarea de teritorii sau de resurse vitale, își schimbă sensul și sunt completate cu altele noi, cum ar fi cucerirea de pieţe de desfacere sau protecția mediului. În acest context, au avut loc mutații și în strategiile de promovare a intereselor, care fixează ca obiective neutralizarea unor elemente ale infrastructurii critice ale competitorilor în locul disipării efortului pentru neutralizarea în ansamblu a competitorului.		
HG 718/13.07.2011 Pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice, http://www.legex.ro/Hotararea-718-2011-114287.aspx	2011	**Pagina 27.** Infrastructura critică poate fi expusă diverselor tipuri de riscuri și amenințări, în funcție de modul de manifestare a acestora. Spectrul general al riscurilor și amenințărilor include evenimente naturale, erori tehnice, tehnologice și umane, acțiuni sau atacuri săvârșite cu intenție, precum și alte forme de manifestare care prin natura ori amploarea lor pot afecta infrastructurile critice. Aceste evenimente și incidente au diverse cauze și pot provoca pagube semnificative sau pot distruge elementele de infrastructură care sunt vitale societății și populației în general. Datorită nivelului mare de dependență față de serviciile de infrastructură, societatea a devenit foarte vulnerabilă atât din cauza dezastrelor și riscurilor, cât și în contextul unor importante interdependențe între diferite zone ale infrastructurii în cadrul sistemelor relevante.	**118**	Fără citare sursă, sursa este dată la bibliografie

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, Amenințări la adresa acestora. Sisteme de protecție*, Editura UNAp, București, 2006, https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf	2006	**Pagini 27-32.** Perspectiva din ce în ce mai amenințătoare a acțiunilor teroriste, înmulțirea și diversificarea dezastrelor naturale și posibilitățile de producere a unor accidente tehnologice cu consecințe majore au impus în ultimii ani concentrarea atenției asupra protecției infrastructurilor critice (PIC). Aceasta este cu atât mai profundă cu cât interdependențele de natură națională, dar mai ales internațională a infrastructurilor industriale, cibernetice, de comunicații, transport, energetice, bancare etc. au devenit greu de substituit. În ciuda faptului că modalitățile de abordare a protecției structurilor critice diferă de la o țară la alta, de la o organizație la alta, se pot identifica elemente structurale comune, măsuri concertate desfășurate cu succes, funcții și responsabilități compatibile. Organizația de Cooperare și Dezvoltare Economică (OCDE) tratează problema PIC din punctul de vedere al incidentelor economice și catastrofelor. Măsurile se referă în special la restabilirea comunicațiilor în cazul cutremurelor de pământ, asigurarea fluenței traficului în caz de catastrophe naturale, securitatea în domeniul maritim, înlăturarea efectelor accidentelor chimice etc. În cadrul Uniunii Europene, Consiliul Europei a	**1500**	Fără citare sursă, sursa este dată la bibliografie

CONFORM CU ORIGINALUL

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		realizat „acordul parţial deschis privind riscurile majore" care are ca scop cooperarea în domeniul gestionării riscurilor. Se preocupă, de asemenea, de formarea unui culturi a riscului prin organizarea de cursuri universitare şi masterate. În octombrie 2004, Comisia Europeană a adoptat un document referitor la protecţia infrastructurilor critice20, care propune măsuri suplimentare de întărire a instrumentelor existente, în special, punerea în aplicare a unui program european de protecţie (EPCIP). În cadrul acestuia a fost constituit un forum permanent pentru realizarea unui echilibru, pe de o parte, între constrângerile impuse de concurenţă, responsabilitate în gestionarea informaţiilor şi, pe de altă parte, de avantajele ce decurg din realizarea unui sistem de protecţie eficient pentru infrastructurile critice. Din această perspectivă, Comisia Europeană şi-a propus să realizeze şi un sistem de avertizare pentru infrastructurile critice (CIWIN – Critical Infrastructure Warning Information Network). La începutul anului 2005, Comisia Europeană şi Agenţia Spaţială Europeană (ESA) au organizat un forum international de mare amploare, unde au fost invitate cele mai importante agenţii spaţiale. Tema reuniunii a fost întărirea cooperării în vederea prevenirii unor dezastre naturale sau accidente tehnologice majore şi a facilitării operaţiilor de salvare printr-o		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		supraveghere cât mai extinsă a planetei prin intermediul sateliţilor. De altfel, încă din 2001, Comisia Europeană a lansat iniţiativa GMES - supraveghere globală pentru mediu şi securitate – care are ca obiectiv realizarea, până în 2008, a unor capabilităţi operaţionale autonome de monitorizare a mediului. Organizaţia Internaţională pentru Protecţia Civilă (OIPC) este o federaţie de structuri naţionale de protecţie civilă. Aceasta se doreşte o platformă de comunicare, de schimburi de experienţe şi de cooperare în domeniu. Una din atribuţiile sale majore o reprezintă standardizarea procedurilor de urgenţă. Comisia Economică pentru Europa din cadrul ONU a stabilit o serie de norme şi standarde în domeniul infrastructurilor, al transporturilor de materiale periculoase şi al accidentelor transfrontaliere. G8 dezvoltă politici de protecţie a infrastructurilor critice. La summit-ul din 2003 a adoptat un text care cuprinde 11 principii directoare ce asigură statelor membre, dar şi altor ţări, un cadru de dezvoltare a strategiilor de protecţie a infrastructurilor critice, în special în domeniul informatic. Organizaţia pentru Securitate şi Cooperare în Europa (OSCE), ca şi celelalte organizaţii internaţionale, se află în plin proces de definire a unor noi atribuţii şi		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		structuri care să corespundă fenomenului de globalizare şi noilor tipuri de riscuri şi ameninţări. La Conferinţa Anuală de Revizuire a Securităţii din 2004 s-a pus problema intensificării schimbului de informaţii privind riscurile şi reacţia coordonată în domeniul PIC. Astfel, o prima măsură stabilită este organizarea de reuniuni ale experţilor, având ca finalitate imediată redactarea unui set de recomandări ale OSCE, pe baza cărora să se poată realiza o adevărată „securitate teritorială OSCE". Centrul pentru Politici de Securitate de la Geneva a organizat, la sfârşitul anului 2003, un forum dedicat coordonării în domeniul PIC. A fost primul forum de acest gen, la care au participat peste 180 de experţi din 28 de ţări. Concluziile au fost extrem de interesante, ele referindu-se la tendinţele generale ale PIC, soluţiile greşite la care s-a apelat până în prezent şi modalităţile de „a gândi diferit", de „a gândi imposibilul" şi de „a schimba mentalităţile". La 5 noiembrie 2005 a fost adoptat Programul de la Haye21, în care se prevedea, între altele, consolidarea măsurilor pentru gestionarea crizelor transfrontaliere, protecţia infrastructurilor vitale şi a problemelor ce ţin de tensiunile şi conflictualitatea specific ordinii publice şi securităţii. În acest sens, Consiliul European a încredinţat Comisiei Europene şi, respectiv, structurilor din cadrul Consiliului, sarcina		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		realizării unui dispozitiv integrat al UE, care să devină operaţional cel mai târziu în iulie 2006. Dispozitivul, potrivit programului adoptat, trebuie să evalueze capacităţile statelor member ale UE, să asigure pregătirea şi desfăşurarea unor exerciţii comune şi să întocmească un plan operaţional comun pentru o gestionare civilă a crizelor. El trebuie să realizeze, între altele: protecţia cetăţenilor şi infrastructurilor împotriva pericolelor şi ameninţărilor teroriste CRBN, în spaţiile publice, dar şi împotriva catastrofelor naturale (seisme, inundaţii, incendii de păduri) şi catastrofelor tehnologice, maritime, de transport, sanitare etc., în cadrul unei strategii europene integrate, printr-un dispozitiv de reacţie bine structurat şi interoperaţional; promovarea unor norme de securitate comune, la nivel UE, stabilirea unor scenarii şi exerciţii de pregătire şi de punere în aplicare a unor mecanisme de gestionare a crizelor, de alertă rapidă şi de protecţie civilă; realizarea unui sistem de reacţie rapidă şi eficientă împotriva atacurilor teroriste asupra infrastructurilor şi pentru lichidarea urmărilor acestora, care să garanteze revenirea în scurt timp la normalitate; întrucât infrastructurile europene sunt din ce în		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		ce mai mult interconectate şi interdependente, este nevoie de o politică şi o strategie unitare, care să folosească toate pârghiile statelor şi UE pentru protecţia acestora. Consiliul a făcut următoarele recomandări: a) punerea deplină în operă a recomandărilor Consiliului European privind stabilirea unui „mecanism integrat de gestionare a crizelor în UE", esenţial pentru întărirea legăturilor între cetăţenii şi instituţiile europene şi strângerea legăturilor de interdependenţă şi de solidaritate între statele membre; b) centrarea strategiei europene integrate pe contracararea ameninţărilor asupra infrastructurilor vitale a căror distrugere ar putea avea efecte grave asupra sănătăţii, securităţii, siguranţei şi bunăstării economice a cetăţenilor, punerea în aplicare şi armonizarea la nivel european a unei metode armonioase prin care să se identifice infrastructurilor vitale, să se analizeze vulnerabilităţile, să se evalueze ameninţările şi să se propună soluţii viabile pentru protecţia acestora; c) instituirea unui Program european de protecţie a infrastructurilor vitale (EPCIP); d) considerarea programului european ca fiind complementar programelor naţionale;		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		e) admiterea situaţiei potrivit căreia: - un sistem european de analiză a riscurilor trebuie să fie conceput şi pus în aplicare; - realizarea unor legături strânse între toate autorităţile care deţin informaţii şi care au competenţe în acest domeniu; - gestionarea corectă şi fiabilă a informaţiilor pertinente (informaţii militare şi civile, cooperare poliţienească), control parlamentar; - crearea, în sânul Comisiei, a unui sistem de alertă rapidă în caz de criză, la nivel european, naţional şi internaţional partajat printr-o reţea centrală (ARGUS); - asocierea Comitetului European de Normalizare; f) a veghea ca Programul European de Protecţie a Infrastructurilor Critice (EPCIP) să respecte următoarele condiţii: - să fie plasat sub controlul parlamentului european şi parlamentelor naţionale; - să constituie un element esenţial al viitorului dispozitiv continental şi mondial de protecţie a infrastructurilor critice; g) ameliorarea Fondului European de Solidaritate		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		(pentru intervenţii în interiorul UE) şi ECHO (pentru intervenţii în afara UE); h) crearea unei Forţe Europene de Protecţie Civilă; i) consolidarea parteneriatului cu societatea civilă pentru realizarea unei strategii privind protecţia împotriva ameninţărilor CBRN; j) asigurarea condiţiilor pentru ca toate aceste sisteme de alertă în caz de urgenţe civile şi militare şi de protecţie să nu afecteze viaţa cetăţenilor şi siguranţa lor, să nu îngrijoreze şi să panicheze în mod inutil populaţia; k) garantarea respectului vieţii private, protecţia informaţiei şi prevenirea difuzării ei neautorizate; l) elaborarea unui dispozitiv-cadru european de protecţie şi nedivulgare a datelor, astfel încât drepturile fundamentale ale omului să fie protejate; m) asigurarea condiţiilor ca protecţia populaţiei şi a infrastructurilor vitale să se bazeze pe scenarii realiste şi pe experienţe verificate (spre exemplu, experienţa dobândită în timpul Jocurilor Olimpice de la Atena din 2004). Aceste reglementări şi experienţe se regăsesc, într-o formă sau alta, în strategiile naţionale de protecţie a populaţiei şi infrastructurile vitale ale tuturor ţărilor europene. În Germania, spre exemplu, există aşa-numitul concept de protecţie de bază22. Punctul de		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		plecare îl reprezintă un proces de analiză şi de planificare multietajată, care cuprinde o evaluare a pericolelor, ameninţărilor şi riscurilor asociate, urmată de un control şi de o adaptare a măsurilor de protecţie. Acest concept german presupune23: I. identificarea diferitelor categorii de riscuri din diferite domenii: catastrofe naturale, accidente, terorism şi criminalitate; II. fixarea nivelului de protecţie bazat pe aceste categorii; III. conceperea de scenarii ale sinistrelor şi ameninţărilor; IV. analiza punctelor slabe; V. formularea obiectivelor de protecţie şi fixarea măsurilor de protecţie şi contra-protecţie care decurg de aici; VI. formularea urgenţelor (coordonarea între măsurile publice şi private); VII. punerea în aplicare, după nevoi, a acţiunii formulate; VIII. controlul sistematic al acestui proces de analiză şi planificare în cadrul gestionării calităţii		
Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, Ameninţări la adresa*	2006	**Pagini 32-34.** În realizarea şi implementarea unui program european de protecţie a infrastructurilor critice s-a pornit de la o realitate complexă şi de la o concluzie pe	**404**	Fără citare sursă, sursa este dată la bibliografie

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
acestora. Sisteme de protecţie, Editura UNAp, Bucureşti, 2006, https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf		măsură: este imposibil ca Uniunea Europeană să poată realiza, de facto, protecţia tuturor infrastructurilor critice. De aceea, programul are în vedere numai infrastructurile critice transnaţionale, protecţia celor naţionale rămânând în responsabilitatea statelor member ale UE, dar, evident, într-un cadru comun. În acest sens, există deja numeroase directive şi reglementări, care impun mijloace şi proceduri pentru sesizarea accidentelor, elaborarea unor planuri de intervenţie, în colaborare cu protecţia civilă, cu administraţia, cu serviciile de urgenţă etc. Există, spre exemplu, o mulţime de programe de acţiune şi de reacţie în urgenţe civile şi militare, cum ar fi accidentele nucleare, industriale, chimice, petroliere, ecologice, catastrofele naturale etc. Comisia Europeană ţine o evidenţă strictă a acestora, informează şi raportează în fiecare an situaţia în ceea ce priveşte evaluarea riscurilor, dezvoltarea tehnicilor de protecţie adică armonizarea, coordonarea şi colaborarea pe orizontală. Această comunicare a Comisiei Europene, în care se înglobează toate analizele şi măsurile sectoriale, constituie baza unui program european de protecţie a infrastructurilor critice (EPCIP). Programul trebuie să identifice infrastructurile critice, să le analizeze vulnerabilităţile, dependenţele şi interdependenţele şi să găsească soluţii pentru		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		securizarea acestora. Obiectivele programului sunt următoarele: - Identificarea şi inventarierea, prin guvernele statelor membre, a infrastructurilor critice situate pe teritoriile fiecărui stat, în funcţie de priorităţile stabilite prin EPCIP; - Colaborarea întreprinderilor, în cadrul sectoarelor respective şi cu guvernele pentru diseminarea informaţiei şi reducerea riscului unor incidente susceptibile de a produce perturbaţii extinse sau durabile infrastructurilor critice; - Abordarea comună a problemei securităţii infrastructurilor critice, graţie colaborării tuturor actorilor publici şi privaţi. Programul european are în vedere, între altele, reunirea, într-o reţea, a tuturor specialiştilor în protecţia infrastructurilor critice din statele membre ale UE. Aceasta ar putea contribui la realizarea unei reţele de alertă în ceea ce priveşte structurile critice (Critical Infrastructure Warning Information Network – CIWIN). Reţeaua a fost pusă deja în funcţiune în 2005. Funcţia principală a acestei reţele este aceea de a contribui la încurajarea schimbului de informaţii privind ameninţările şi vulnerabilităţile comune, la realizarea unui schimb de măsuri şi de strategii adecvate, care să permită		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		limitarea riscurilor şi protejarea infrastructurilor critice. Programul EPCIP ajută statele, proprietarii şi utilizatorii infrastructurilor critice. În acest sens, Comitetul European de Normalizare (CEN) şi alte organisme de normalizare sprijină reţeaua (CIWIN), propunând norme de securitate sectorială uniforme şi adaptate pentru toate sectoarele vizate.		
HG 718/13.07.2011 Pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice, http://legislatie.just.ro/Public/DetaliiDocument/130566	2011	**Pagina 34.** Evoluţia ameninţărilor la nivel global, corelată cu statutul politico-militar şi economic actual al României în cadrul Alianţei Nord-Atlantice şi Uniunii Europene, a determinat translatarea potenţialilor factori de risc şi asupra infrastructurilor naţionale asimilabile celor critice, mai ales, în contextul rolului jucat de ţara noastră în asigurarea climatului de stabilitate şi securitate regională, cu accent în zona bazinului Mării Negre. Astfel, perspectiva manifestării unor potenţiale ameninţări a determinat abordări strategice, instituţionale şi funcţionale într-un sistem integrat al problematicii protecţiei infrastructurilor critice naţionale. Având în vedere dependenţa mare faţă de serviciile oferite de infrastructurile critice, societatea a devenit foarte vulnerabilă. Această vulnerabilitate a crescut nu doar ca urmare a riscurilor şi ameninţărilor externe, ci şi din cauza interdependenţelor dintre diferitele infrastructuri din interiorul sistemelor relevante,	**173**	Fără citare sursă, sursa este dată la bibliografie

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		context în care perturbările/întreruperile pot determina pagube imense pentru economia naţională. În materia protecţiei infrastructurilor critice, efortul statului şi al societăţii trebuie direcţionat, în principal, pe două mari categorii de ameninţări: cea teroristă şi cea generată de dezastre/calamităţi naturale, ce au un impact tot mai mare asupra infrastructurii considerate critică.		
Grigore Alexandrescu, Gheorghe Văduva, *Infrastructuri critice. Pericole, Ameninţări la adresa acestora. Sisteme de protecţie,* Editura UNAp, Bucureşti, 2006, https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf	2006	**Pagini 36-37.** Protecţia infrastructurilor vitale (critice) naţionale româneşti se înscrie, într- o formă sau alta, în programul european de protecţie a infrastructurilor critice prin cel puţin trei modalităţi: adaptarea sistemului de legislaţie, de acţiune şi de reacţie în situaţii de urgenţă la cerinţele europene, în procesul pregătirii integrării şi integrării propriu-zise; dependenţele şi interdependenţele infrastructurilor vitale româneşti de cele europene; participarea la elaborarea şi punerea în aplicare a politicilor şi strategiilor de combatere a terorismului, traficului ilegal, crimei organizate şi ameninţărilor asimetrice. Infrastructurile vitale româneşti sunt, aproape în totalitate, infrastructuri critice din cel puţin câteva motive esenţiale:provin din infrastructurile unei economii-gigant, inflexibile şi greu adaptabile economiei de piaţă, ale cărei urme nu au fost încă nici lichidate, nici ameliorate; economia şi societatea românească, în ansamblul ei, se află într-o stare de haos, specifică perioadelor îndelungi şi repetate de tranziţie, în care totul sau aproape totul	**275**	Fără citare sursă, sursa este dată la bibliografie.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		este vital, critic şi vulnerabil; acțiunile fără discernământ asupra mediului, tăierea masivă a pădurilor, cultivarea haotică a terenurilor, dezastrul din agricultură, lipsa unei politici agrare, ecologice şi de protecție a mediului coerente şi eficiente creează şi proliferează pericole extrem de grave la adresa tuturor infrastructurilor şi îndeosebi asupra celor critice; se aşteaptă ca participarea României la coaliția antiteroristă şi la alte misiuni de gestionare a crizelor şi conflictelor şi de menținere a păcii să genereze un nou tip de amenințări asupra cetățenilor şi infrastructurilor vitale ale economiei, societății, informației şi condițiilor de trai. Desigur, pericolele şi amenințările sunt mult mai numeroase. Ele fac obiectul unor inițiative legislative, sunt cuprinse în strategia națională de securitate şi în alte documente importante, dar sunt departe de a fi pe deplin monitorizate, gestionate, controlate şi înlăturate.		
Coroiu Viorel, teza de doctorat Criminalitatea informatică – factor de risc major pentru ordinea publică și siguranța națională, Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf	2011	**Pagini 43-44.** În ultimii ani, activitatea infracțională de pe palierul criminalității informatice s-a amplificat. Spre deosebire totuși de anii precedenți, se constată o creștere a atacurilor provenite din statele în curs de dezvoltare. Ultimul raport al Symantec (aprilie 2010) aduce pentru prima dată în atenție un stat care, ca nivel de agresivitate pe linia cybercrime, se situează în top trei, și nu este vorba despre SUA, Germania ori China, ci, paradoxal, despre Brazilia. Nivelul de creștere al	**266**	Fără citare sursă, sursa este dată la bibliografie. Copiază inclusiv notele de subsol din sursa originală.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		amenințărilor informatice din acest stat este atât de alarmant, încât a determinat factorii politici să prioritizeze adoptarea unei noi legislații în acest domeniu1. Deși China ocupă detașat primul loc în topul statelor cu cel mai înalt nivel de amenințare în domeniu, studiile efectuate de firma Zscaler au indicat faptul că America de Sud2, prin Brazilia dar și alte state, constituie un puct fierbinte pe harta lumii în materia surselor de risc de nivel informatic. Dealtfel, continentul american este gazda a nu mai puțin de șapte dintre cele mai periculoase state care găzduiesc servere furnizoare de malware. (...) În ultimii ani, amenințările informatice s-au transformat din fenomene individuale, dobândind caracter organizat. Infractorii cibernetici pot lucre singuri, dar mai ales ca membri ai unui grup extins. Unii acționează ca și mercenari, alții în numele unor interese proprii (altele decât cele financiare, ca de exemplu angajații unor instituții care au acces la informații de nivel înalt). Un aspect de evoluție al fenomenului infracțional în constituie faptul că, raportat la situația din urmă cu câțiva ani, sindicate și carteluri de crimă organizată se implică din ce în ce mai mult în explozia fenomenului criminal informatic.		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, https://vdocuments.mx/documents/93361241097364infractiuniindomeniulinformatic.html	2006	**Pagina 52.** La executarea unei simulări a Web-ului, hackerul poate observa sau modifica toate datele trimise de la victimă la serverele Web. De asemenea, hackerul are controlul întregului trafic returnat de serverele Web către victimă, în consecință, hackerul dispunând de multiple posibilități de exploatare. Cele mai cunoscute metode de pătrundere într-o rețea sunt interceptarea şi simularea. Interceptarea (sniffmgul) este o activitate de tip supraveghere, deoarece hackerul urmăreşte traficul de rețea în mod pasiv. Simularea este o activitate de intercepție, deoarece hackerul convinge un host că este un alt host credibil, care poate primi informații. La simularea Web-ului, hackerul înregistrează conținutul paginilor vizitate de către victimă. Când victima completează un formular pe o pagină HTML, browser-ul său trimite datele introduse către serverul Web. Deoarece este interpus între client şi server, hackerul poate înregistra toate datele introduse de către client. De asemenea, hackerul poate înregistra şi conținutul răspunsului trimis de server către client. Deoarece majoritatea activităților comerciale online folosesc formulare, hackerul poate citi numere de cont, parole sau alte informații confidențiale introduse cu bună-ştiință de victimă în formularele simulate. Pot fi efectuate chiar şi activități de supraveghere, deşi victima dispune de o conexiune presupus sigură. Indiferent dacă această conexiune chiar dacă browser-ul victimei indică pictograma de	**217**	Fără citare sursă, sursa este dată la bibliografie.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		conexiune sigură (imaginea unui lacăt sau a unei chei), victima transmite folosind o conexiune desecurizată.		
Coroiu Viorel, teza de doctorat *Criminalitatea informatică – factor de risc major pentru ordinea publică și siguranța națională*, Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf	2011	**Pagina 75.** Securitatea informatică, într-un sens larg, incluzând cadrul legal, este esențială pentru atragerea actorilor economici pentru dezvoltarea unui mediu de afaceri favorabil. Societatea informațională globală şi economia bazată pe cunoaştere sunt limitate de dezvoltarea şi acceptanţa generală a unui cadru internaţional cibernetic. Valabilitatea unui astfel de cadru sau model necesită o abordare multidimensională pentru provocare cibernetică - de la indivizi la organizaţii şi state.	**63**	Fără citare sursă, sursa este dată la bibliografie.
https://www.bacau.net/strategie-in-domeniul-securitatii-cibernetice-la-nivel-european/	**8 februarie 2013**	**Pagini 99-101.** **Comisia Europeană a publicat o strategie în domeniul securităţii cibernetice, precum şi o propunere de directivă a Comisiei privind securitatea reţelelor şi a informaţiei (NIS). Strategia în domeniul securităţii cibernetice, „Un spaţiu cibernetic deschis, sigur şi securizat", reprezintă viziunea globală a UE asupra celor mai bune modalităţi de a preveni şi de a gestiona perturbările şi atacurile cibernetice. Scopul său este acela de a promova valorile europene de libertate şi democraţie şi de a garanta o creştere a economiei digitale în condiţii de siguranţă. Sunt prevăzute o serie de acţiuni specifice care au ca obiectiv**	**540**	**Fără citare sursă**

CONFORM CU ORIGINALUL

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		creşterea nivelului de rezilienţă a infrastructurilor cibernetice, reducerea criminalităţii informatice şi consolidarea politicii internaţionale a UE în materie de securitate cibernetică şi de apărare împotriva atacurilor cibernetice. **Strategia defineşte viziunea UE în materie de securitate cibernetică prin intermediul a cinci priorităţi: obţinerea unei rezilienţe a infrastructurilor cibernetice, reducerea drastică a criminalităţii informatice, dezvoltarea unei politici de apărare împotriva atacurilor cibernetice şi a capacităţilor necesare în contextul politicii de securitate şi apărare comună (PSAC), dezvoltarea resurselor industriale şi tehnologice necesare pentru securitatea cibernetică, stabilirea unei politici internaţionale coerente a Uniunii Europene privind spaţiul cibernetic şi promovarea valorilor fundamentale ale UE** **Politica internaţională a UE privind spaţiul cibernetic promovează respectarea valorilor fundamentale ale UE, stabileşte norme aplicabile comportamentului responsabil, sprijină aplicarea în spaţiul cibernetic a legislaţiei internaţionale existente, acordând, în acelaşi timp, asistenţă ţărilor din afara UE în ceea ce priveşte consolidarea capacităţilor în materie de securitate cibernetică şi**		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		promovând cooperarea internaţională în acest domeniu. **UE a făcut progrese importante în materie de protejare a cetăţenilor împotriva infracţiunilor online, inclusiv prin instituirea unui Centru european de combatere a criminalităţii informatice, prin propuneri legislative privind atacurile împotriva sistemelor informatice şi prin lansarea unei alianţe mondiale împotriva abuzurilor sexuale asupra copiilor comise prin intermediul internetului. De asemenea, strategia urmăreşte dezvoltarea şi finanţarea unei reţele de centre naţionale de excelenţă pentru combaterea criminalităţii informatice, care să faciliteze formarea profesională şi consolidarea capacităţilor.** **Directiva propusă în materie de securitate a reţelelor şi a informaţiei reprezintă componenta-cheie a strategiei globale şi ar impune tuturor statelor membre, principalilor operatori de servicii internet, operatorilor de infrastructură critică (de exemplu, platformele de comerţ electronic şi reţelele sociale) şi operatorilor de servicii în domeniile energiei, transporturilor, asistenţei medicale, precum şi în domeniul bancar obligaţia de a asigura un mediu digital securizat şi fiabil în întreaga UE. Printre măsurile prevăzute în directiva propusă se numără**		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		următoarele: Statele membre trebuie să adopte o strategie în materie de securitate a reţelelor şi a informaţiei şi să desemneze o autoritate competentă naţională în acest domeniu care să dispună de resursele financiare şi umane adecvate pentru a preveni, gestiona şi soluţiona riscurile şi incidentele NIS; Crearea unui mecanism de cooperare între statele membre şi Comisie pentru emiterea din timp a unor avertismente referitoare la riscuri şi incidente printr-o infrastructură securizată, pentru a coopera şi pentru a organiza evaluări periodice inter pares; Operatorii de infrastructuri critice din anumite sectoare (servicii financiare, transporturi, energie, sănătate), operatorii de servicii ale societăţii informaţionale (şi anume: magazine de aplicaţii, platforme de comerţ electronic, plăţi pe internet, cloud computing, motoare de căutare, reţele sociale) şi administraţiile publice trebuie să adopte practici de management al riscurilor şi să raporteze incidentele majore de securitate privind serviciile lor de bază.		
Strategia de Securitate cibernetică a României. HG 271/2013 de adoptare, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-	2011/ 2013	**Pagini 103-107.** **Întreg subcapitolul 4.3.** La sfârşitul lunii mai 2011, MCSI a lansat în dezbatere publică proiectul „ Strategiei de securitate cibernetică a României", aceasta fiind aprobată de CSAT în luna februarie 2013. Documentul strategic are	**1182**	Citare incorectă: se precizează titlul documentului, dar nu se

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
cyber-security-strategies-ncsss/roncss.pdf/at_download/file sau HG 271/2013 de adoptare a Strategiei de Securitate cibernetică a României, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Romania_2013_Orig_Ro_StrategiaDeSecuritateCiberneticaARomaniei.pdf		scopul declarat de a implementa măsuri de securitate care să conducă la creşterea nivelului de protecţie a infrastructurilor cibernetice în concordanţă cu noile concepte şi politici din domeniul apărării cibernetice elaborate şi adoptate la nivelul NATO şi al Uniunii Europene. In preambulul documentului menţionat se specifică faptul că „cu cât o societate este mai informatizată, cu atât este mai vulnerabilă, iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu ". Necesitatea adoptării Strategiei menţionate este justificată prin faptul că România se confruntă în prezent cu ameninţări provenite din spaţiu cibernetic la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri precum cele din sectoarele financiar-bancar, transport, energie şi apărare naţională. Strategia de securitate cibernetică a României stabileşte următoarele obiective pe care Guvernul trebuie să le aducă la îndeplinire, alături de toate celelalte instituţii cu responsabilităţi în domeniu: • adaptarea cadrului normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic; • stabilirea şi aplicarea unor profile şi cerinţe minime de securitate pentru infrastructurile cibernetice naţionale, relevante din punct de vedere al funcţionării		specifică adresa la care poate fi accesat sau paginile din care se citează.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		corecte a infrastructurilor critice; • asigurarea rezilienţei infrastructurilor cibernetice; • asigurarea stării de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice a României; • valorificarea oportunităţilor spaţiului cibernetic pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic; • promovarea şi dezvoltarea parteneriatului public-privat, precum şi a cooperării în plan naţional şi internaţional în domeniul securităţii cibernetice; • creşterea culturii de securitate a populaţiei prin conştientizarea faţă de vulnerabilităţile, riscurile şi ameninţările provenite din spaţiul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii; • participarea activă la iniţiativele organizaţiilor internaţionale din care România face parte în domeniul definirii şi stabilirii unui set de măsuri destinate creşterii încrederii la nivel internaţional privind utilizarea spaţiului cibernetic. Pentru atingerea acestor obiective, în cadrul Strategiei de securitate cibernetică a României sunt identificate următoarele direcţii de acţiune la nivel naţional: A. Stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice. Principalele acţiuni prevăzute în cadrul		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		Strategiei pe această direcţie sunt: ■ Constituirea şi operaţionalizarea unui Sistem Naţional de Securitate Cibernetică; ■ Completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale. B. Dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui Program naţional. Acţiunile prevăzute în cadrul Strategiei pe această direcţie sunt: ■ Consolidarea, la nivelul autorităţilor competente potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a ameninţărilor şi minimizare a riscurilor asociate utilizării spaţiului cibernetic; ■ Asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public şi cel privat în domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, respectiv de reacţie la incidentele cibernetice; ■ Stimularea capabilităţilor naţionale de cercetare-dezvoltare şi inovare în domeniul securităţii cibernetice; ■ Creşterea nivelului de reziliență a infrastructurilor cibernetice; ■ Dezvoltarea entităţilor de tip CERT atât în cadrul instituţiilor publice, cât şi în sectorul privat. C. Promovarea şi consolidarea culturii de		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		securitate în domeniul cibernetic.Principalele acţiuni prevăzute în cadrul Strategiei pe această direcţie sunt: ■ Derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului privat cu privire la ameninţările, vulnerabilităţile şi riscurile specifice utilizării spaţiului cibernetic; ■ Formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificărilor profesionale în domeniu; ■ Includerea unor elemente referitoare la securitatea cibernetică în programele de formare şi perfecţionare profesională a managerilor din domeniul public şi privat. D. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice, prin: ■ încheierea de acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore; ■ Participarea la programe internaţionale care vizează domeniul securităţii cibernetice; ■ Promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care România este parte. Dintre formele de materializare a ameninţărilor din spaţiul cibernetic prin exploatarea vulnerabilităţilor de natura umană, tehnică şi procedurală enumerate în proiectul de strategie se numără: ■ atacurile cibernetice împotriva		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		infrastructurilor care susţin funcţii de utilitate publică ori servicii ale societăţii informaţionale a căror întrerupere/ afectare ar putea constitui un pericol la adresa securităţii naţionale; ■ accesarea neautorizată a infrastructurilor cibernetice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice ori restricţionarea ilegala a accesului la aceste date; ■ spionajul cibernetic; ■ cauzarea unui prejudiciu patrimonial, hărţuirea şi şantajul persoanelor fizice şi juridice, de drept public şi privat. Documentul strategic defineşte concepte precum cele de război cibernetic, terorism cibernetic şi criminalitate informatică şi propune constituirea unui Sistem National de Securitate Cibernetică menit să asigure cunoaşterea, prevenirea şi contracararea unui atac împotriva componentei naţionale a spaţiului cibernetic. Asigurarea securităţii reţelelor informaţionale proprii revine fiecărei persoane juridice de drept public sau privat în parte. în vederea coordonării acţiunilor în acest domeniu la nivel naţional, în cadrul Strategiei de securitate cibernetică a României a fost prevăzută constituirea Sistemului Naţional de Securitate Cibernetică ce reprezintă cadrul de cooperare inter-instituţională destinat asigurării securităţii cibernetice. In calitatea sa de autoritate naţională în domeniul cyberintelligence, Serviciului Român de Informaţii i-a fost încredinţată coordonarea tehnică a Sistemului		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		Naţional de Securitate Cibernetică. Adaptarea Serviciului Român de Informaţii la provocările erei informaţionale şi imperativul utilizării noilor instrumente cibernetice pentru consolidarea performantei operaţionale şi analitice constituie şi obiectivul Viziunii Strategice 2011-2015, intitulată „SRIîn era informaţională". în mesajul din preambulul Strategiei, directorul George Cristian-Maior evidenţiază: „ expansiunea lumii virtuale a condus la emergenţa unei noi dimensiuni a puterii statale", aşa-numita „putere digitală", ale cărei forme de evoluţie „vor reprezenta, în egala măsură, oportunităţi de dezvoltare, dar şi vulnerabilităţi şi provocări la adresa securităţii". Din perspectiva Viziunii Strategice 2011-2015, tehnologia informaţiei constituie o resursa fundamentală ce asigură, în egală măsură, un avantaj competitiv în intelligence şi un facilitator al cooperării în absenţa căreia gestionarea riscurilor şi ameninţărilor la adresa intereselor de securitate este, astăzi, imposibil de imaginat. Ca rezultat al unui proces continuu de racordare la politicile europene în domeniu, materializat prin participarea reprezentanţilor naţionali la demersul creionării documentului strategic european, Strategia de securitate cibernetică a României şi Strategia Europeană de Securitate Cibernetică prezintă numeroase puncte comune în ceea ce priveşte obiectivele şi direcţiile de acţiune identificate, dintre care se pot enumera: ■ asigurarea rezilienţei infrastructurilor critice		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		prin dezvoltarea unor parteneriate public-private şi creşterea culturii de securitate; ■ asigurarea stării de securitate prin dezvoltarea cadrului legislativ; ■ crearea unei politici internaţionale comune în spaţiul cibernetic prin creşterea încrederii privind utilizarea spaţiului cibernetic în mod liber şi deschis. Principiile de bază privind legislaţia specifică rezolvării criminalităţiiinformatice sunt legate de legislaţia penală în vigoare, chiar dacă, în unele cazuri, a suferit modificări ca urmare a aderării la Convenţie. în plus apare tot mai mult necesitatea formulării de consultări în materie nu numai cu specialişti ai dreptului, dar şi cu cei ai tehnologiei la zi.		
GHID INTRODUCTIV PENTRU APLICAREA DISPOZIŢIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ, http://riti-internews.ro/Capitolul%2005%20-%20Reglementarea%20criminalitatii%20informatice.pdf	**2004**	**Pagini 111-112.** **Legiferarea în domeniul criminalităţii informatice a urmat, începând din anii'70, mai multe "valuri". Primul a fost determinat de necesitatea protejării dreptului la** **viaţa privată. Legi privind protecţia persoanei fizice faţă de prelucrarea datelor cu caracter personal au fost adoptate în Suedia (1973), SUA (1974), Germania (1977), Austria, Danemarca, Franţa şi Norvegia (1978), sau mai recent în Belgia, Spania, Elveţia (1992),** **Italia şi Grecia (1997). Al doilea "val" este legat de represiunea infracţiunilor cu caracter economic, producând modificări legislative în SUA şi Italia**	**343**	**Fără citare sursă**

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		(1978), Australia (1979), Marea Britanie (1981), sau Elveţia (1994) şi Spania (1995). A treia serie de reglementări este legată de intervenţia legislativă în vederea protecţiei proprietăţii intelectuale în domeniul tehnologiei informatice, în ţări ca SUA (1980), Ungaria (1983), Germania, Franţa, Japonia, Marea Britanie (1985), sau Austria (1993), România (1996), Luxemburg (1997). Al patrulea "val" de reforme priveşte reglementarea distribuirii de informaţii ilegale sau prejudiciabile, **şi a fost puternic impulsionat la sfârşitul anilor '80 de amploarea luată de reţeaua Internet.** **Al cincilea "val" este legat de modificările intervenite în materia dreptului procesual, cu privire la aspectele de procedură penală ridicate de incidenţa tehnologiei informaţiei, în timp ce al şaselea "val" priveşte impunerea unor obligaţii şi limite în materia securităţii informatice.** **În acest sens, la nivel internaţional, Consiliul Europei a iniţiat o serie de reglementări cu privire la criminalitatea informatică. Astfel, dacă în 1995 a fost adoptată Recomandarea nr. R (95) 13 cu privire la problemele de procedură penală legate de tehnologiile informaţionale, în 23 noiembrie 2001 a fost semnată la Budapesta Convenţia privind criminalitatea informatică. Convenţia îşi propune să**		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		prevină actele îndreptate împotriva confidenţialităţii, integrităţii şi disponibilităţii sistemelor informatice, a reţelelor şi a datelor, precum şi a utilizării frauduloase a unor asemenea sisteme, reţele şi date, prin asigurarea incriminării unor asemenea conduite şi prin încurajarea adoptării unor măsuri de natură a permite combaterea eficace a acestor tipuri de infracţiuni, menite să faciliteze descoperirea, investigarea şi urmărirea penală a acestora atât la nivel naţional, cât şi internaţional, precum şi prin prevederea unor dispoziţii materiale necesare asigurării unei cooperări internaţionale rapide şi sigure.		
Dan Fifoiu, *Atacuri și amenințări la adresa securității infrastructurilor critice,* în Revista INTELLIGENCE, http://intelligence.sri.ro/atacuri-si-amenintari-la-adresa-securitatii-infrastructurilor-critice/	**2010**	**Pagini 151-152.** **Unul dintre studiile relativ recente care au semnalat potenţialul distructiv al atacurilor cibernetice a fost publicat, sub egida *„Centrului pentru Studii Internaţionale şi Strategice"* din SUA, la sfârşitul lunii ianuarie 2010, de actuali şi foşti oficiali din cadrul Departamentului pentru Securitate Internă american, membri marcanţi ai Congresului şi directori ai departamentelor de securitate cibernetică ai unor companii care gestionează infrastructura critică.** **Studiul se bazează pe un sondaj de opinie realizat în rândul a şase sute de directori IT şi de securitate ai unor companii care deţin şi/sau operează infrastructuri critice în şapte domenii**	**333**	**Fără citare sursă**

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		diferite, din 14 state. Potrivit acestora, atacurile cibernetice au o frecvenţă ridicată şi sunt întreprinse, în numeroase cazuri, de adversari de nivel înalt (state, organizaţii teroriste sau de criminalitate organizată), consecinţele fiind de multe ori grave iar costurile de remediere ridicate. China şi Statele Unite sunt considerate agresorii cibernetici cu cel mai ridicat potenţial. Aproximativ o treime din cei chestionaţi au opinat că sectorul lor nu este pregătit să facă faţă unor atacuri majore concertate de adversari de nivel înalt. **Potrivit companiei McAfee, India este ţara cu cea mai mare încredere în capacitatea propriului guvern de a preveni şi a opri atacurile informatice, în timp ce Rusia şi România reprezintă terenul cel mai propice pentru hackerii care coordonează reţele de tip botnet.** **La 18 februarie 2010, Comandamentul Forţelor Unite ale SUA a lansat un studiu în cuprinsul căruia a acreditat ideea că, prin intermediul spaţiului cibernetic, agresorii vor viza industria, guvernele, mediile academice şi infrastructura militară aeriană, terestră, maritimă şi spaţială, fapt confirmat de două dintre principalele cazuri de agresiuni care au afectat securitatea informatică la nivel global: Conficker şi GhostNet. Autorii documentului au atras atenţia asupra faptului că spaţiul virtual a fracturat barierele fizice care protejează un stat împotriva atacurilor asupra infrastructuri comerciale şi de telecomunicaţii şi au**		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare și nemenționate în bibliografie	Nr. cuvinte	Observații
		apreciat că adversarii au profitat de avantajele dezvoltării rețelelor informatice nu doar pentru a planifica și comite atacuri, ci și pentru a influența direct percepția autorităților și populației în acest sens.		
Coroiu Viorel, teza de doctorat *Criminalitatea informatică – factor de risc major pentru ordinea publică și siguranța națională*, Academia de Poliție „Alexandru Ioan Cuza", Rezumat disponibil la http://www.euroavocatura.ro/legi/teza_Crim_info.pdf	2011	**Pagini 175-177.** Securitatea informatică, deși a apărut mai târziu, face parte integrantă din securitatea națională și internațională.(...)Fără dubii, securitatea informatică a avut o accesiune deosebită în ultima perioadă, neținând cont de nici un criteriu de spațiu, timp, orânduirea socială, naţiune sau opţiune politică. • Toate acestea sunt determinate de: progresul științific accelerat, inovația tehnologică, vulnerabilitatea în creștere a sistemelor vitale și riscurile pe scară largă; Această stare de lucruri, a stat printre altele la baza formulării sistemelor de asistență judiciară a securității informatice în cadrul U.E. Cu toate că la nivel de detaliu, se pot constata progrese importante, UE nu a ajuns în general la o abordare comună în acest domeniu: cadrul actual nu a putut asigura nici rezultate optime, nici o protecție perfectă a individului în fața acțiunilor informatice ilicite; în plan normativ, au apărut o serie de convenții, complicate ca și conținut, dar numărul notificărilor la nivel global este redus; nu s-a reușit destructurarea acelor rețele internaționale care au atins prin activitatea lor ilicită până și cele mai pregătite state sau cele mai importante Organisme. Pe plan intern, formarea, nu a avut rezultate marcante, deși au fost multe cazuri, fie cu autori singuratici sau ca autori	**637**	Fără citare sursă, sursa este dată la bibliografie.

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		organizaţi în reţele bine structurate. • Ţara noastră, datorită fazei incipiente de pregătire a resursei umane, precum şi a dotării tehnice precare, a fost obligată să accepte ajutorul informaţional şi de investigare a altor state. Acest lucru nu este condamnabil, dar de regulă ajutorul a venit în cazurile când activitatea infracţională a atins interesele acestor state. Acest fapt a permis considerarea intensităţii şi densităţii infracţionalităţii ca factor care determină parţial conţinutul şi manifestările specific pilonilor securităţii informatice (identificare, detecţie, prevenire, avertizare şi dezvoltare), din poziţia acestora ca atribute manageriale. Urmând exemplul statelor UE şi a altor state, România a luat o serie de măsuri pentru realizarea securităţii informatice, condiţie existenţială pentru asigurarea continuului funcţionării infrastructurilor critice: • Legea 161/2003, cuprinde o serie de încriminări ale unor fapte considerate ca infracţiuni, dar eforturile legislative concentrate până în prezent de statul nostru nu au avut rezultatele scontate şi anume acelea de a eradica total fenomenul criminogen; • Privind managementul riscurilor în domeniul securităţii informatice, acesta se află în faza encipientă. Dacă în ceea ce priveşte activitatea de evaluare a riscurilor, au fost efectuate o serie de acţiuni la nivel naţional, atât separat pe domeniu sau în cadrul riscurilor de securitate naţionale, în ceea ce priveşte procedurile de înlăturare a acestor riscuri, acţiunile sunt aproape		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		insesizabile; • S-au elaborat la nivelul insitutiilor care folosesc domeniul I.T., precum şi la nivelul instituţiilor abilitate cu prevenirea criminalităţii informatice, o serie de standarde de evaluare, toate fiind aliniate la standardele internaţionale în vigoare. Astfel, Romana a luat în considerare ameninţări majore ca terorismul, spionajul industrial, spionajul economic, convingerile religioase etc. O concluzie pertinentă nu poate exista fără a sesiza un aspect de mare fineţe: analizele experţilor în domeniu conduc la idea că ameninţările informatice devin din ce în ce mai sofisticate, atât datorită posibilităţilor tehnice oferite de către producători, cât şi situaţiei sociale care determină o serie de conflicte sociale. Aceleaşi analize conduc la concluzia că nivelul de competenţă şi cunoştinţe necesare pentru a exercita o ameninţare informatică scade masiv. La o privire simplistă concluzia ar putea fi considerate anormală, dar nu este aşa. Un fenomen foarte complex cum este securitatea informatică, poate genera asemenea realităţi. Existenţa grupărilor organizate, formate din structuri specializate pe vânzarea de instrumente hardware sau software, ori pe schimbul de instrucţiuni sau programe, transformă chiar şi un novice în domeniul IT, dar dornic de ilicit, într-un potenţial făptuitor, într-o ameninţare. Nu este un secret, faptul că se oferă spre vânzare, la vedere, baze de date complete. Cercetările au stabilit şi o altă realitate. Remarca specialiştilor constă în creşterea riscului de infectare cu		

Titlu operă	Anul publicării sau postării	Paragrafele preluate fără citare şi nemenţionate în bibliografie	Nr. cuvinte	Observaţii
		viruşi a sistemelor informatice în scopul blocării acestora şi obţinerea de date de la alţi utilizatori.		