CZU 351.86:004
DOI https://doi.org/10.52388/1812-2566.2023.2(99).04

ROLUL INFRASTRUCTURILOR INFORMATICE CRITICE ÎN ASIGURAREA SECURITĂȚII NAȚIONALE

Maria PROCA
Doctor în științe politice, Institutul Național de Informații și Securitate „Bogdan Întemeietorul Moldovei", Chișinău, Republica Moldova
e-mail: *aprodan@mail.ru*
https://orcid.org/0000-0002-5104-7058

Nicolae PANFILII
Masterand, Universitatea de Stat din Moldova, Chișinău, Republica Moldova
e-mail: *n.panfilii22@gmail.com*
https://orcid.org/0009-0002-3640-6849

Prezentul articol abordează complexitatea și diversitatea riscurilor și amenințărilor, din ce în ce mai interconectate și caracterizate prin determinări multiple, care necesită o abordare integrativă, sistemică și cuprinzătoare a obiectivelor de securitate, cu accent pe protejarea acelor componente vitale pentru siguranță și buna desfășurare a vieții socio-economice. Activitatea de protejare a infrastructurilor critice nu mai ține cont de frontierele naționale și presupune eforturi comune. Ca atare, protecția infrastructurilor critice necesită amplificarea preocupărilor principalilor actori internaționali (state și organizații) pentru elaborarea și armonizarea unor strategii în domeniu. Acestea trebuie să permită identificarea și avertizarea timpurie a riscurilor, concomitent cu adoptarea și inițierea la timp a deciziilor/abordărilor de intervenție preventivă și contramăsuri. Infrastructurile critice au fost întotdeauna elementul cel mai sensibil și vulnerabil a oricărui sistem și proces. Indiferent cât de bine protejate, infrastructurile critice vor avea întotdeauna un grad ridicat de vulnerabilitate, deoarece, de obicei, sunt primele vizate atunci când se încearcă destabilizarea și chiar distrugerea unui sistem, proces sau când apare o situație de urgență.

Cuvinte-cheie: *infrastructură informațională critică, SCADA, securitate, riscuri, amenințări, securitate cibernetică, criminalitate cibernetică.*

THE ROLE OF CRITICAL IT-INFRASTRUCTURES IN ENSURING NATIONAL SECURITY

The complexity and diversity of risks and threats, increasingly interconnected and characterized by multiple determinations, call for an integrative, systemic and comprehensive approach to security objectives, with an emphasis on protecting those vital components for safety and the smooth running of socio-economic life.The activity of protecting critical infrastructures no longer takes into account national borders and involves joint efforts, in the sense of identifying and evaluating any of their vulnerable points. As such, the protection of critical infrastructures - a determining element for maintaining the state of stability and security - requires the amplification of the concerns of the main international actors (states and international organizations) to elaborate and harmonize some strategies in the field. They must allow the identification and early warning of risks, simultaneously with the adoption and timely initiation of decisions/approaches for

preventive intervention and countermeasures. Critical infrastructures have always been the most sensitive and vulnerable area of any system and process. Their sensitivity stems from their particular role within the structure. No matter how well protected, critical infrastructures will always have a high ratio of vulnerability, as they are usually the first to be targeted when seeking to destabilize and even destroy a system or process or even when an emergency situation occurs.

Keywords: *critical information infrastructure, SCADA, security, risks, threats, cybersecurity, cybercrime.*

LE RÔLE DES INFRASTRUCTURES INFORMATIQUES CRITIQUES POUR GARANTIR LA SÉCURITÉ NATIONALE

La complexité et la diversité des risques et des menaces, de plus en plus interconnectés et caractérisés par de multiples déterminations, nécessitent une approche intégrative, systémique et globale des objectifs de sécurité, en mettant l'accent sur la protection de ces composants vitaux pour la sécurité et le bon fonctionnement de la vie socio-économique. L'activité de protection des infrastructures critiques ne tient plus compte des frontières nationales et implique des efforts conjoints, dans le sens d'identifier et d'évaluer chacun de leurs points vulnérables. A ce titre, la protection des infrastructures critiques - composante déterminante du maintien de l'état de stabilité et de sécurité - nécessite l'amplification des préoccupations des principaux acteurs internationaux (Etats et organisations internationales) pour l'élaboration et l'harmonisation des stratégies sur le terrain. Ils doivent permettre l'identification et l'alerte précoce des risques, simultanément avec l'adoption et le lancement en temps opportun de décisions/approches d'intervention préventive et de contre-mesures. Les infrastructures critiques ont toujours été l'élément le plus sensible et le plus vulnérable de tout système et processus. Leur sensibilité vient de leur rôle particulier au sein de la structure. Aussi bien protégées soient-elles, les infrastructures critiques auront toujours un haut degré de vulnérabilité, car elles sont généralement les premières visées lorsque l'on tente de déstabiliser, voire de détruire un système, un processus ou lorsqu'une situation d'urgence se produit.

Mots-clés: *infrastructure d'information critique, SCADA, sécurité, risques, menaces, cybersécurité, cybercriminalité.*

РОЛЬ КРИТИЧЕСКИХ IT-ИНФРАСТРУКТУР В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Данная статья поднимает вопрос о многообразии рисков и угроз, взаимосвязанных между собой и характеризующихся многочисленными детерминантами, которые требуют комплексного и системного подхода к основным целям безопасности, с установлением акцента на защиту их основных элементов и устойчивого ритма социально-экономической жизни общества. В деятельности по защите критических инфраструктур не учитываются национальные границы, при этом прилагаются совместные усилия для выявления и оценки их уязвимых мест. Таким образом, защита критических инфраструктур, требующая внимания основных международных акторов (государств и организаций) для разработки и согласования определённых стратегий в этой сфере. Они должны выявлять и заблаговременно предупреждать о рисках, одновременно с принятием и своевременным инициированием решений/подходов к превентивному вмешательству и контрмерам. Критические инфраструктуры остаются наиболее чувствительной областью любой системы и процесса. Независимо от их степени защиты, они всегда будут иметь высокий коэффициент уязвимости, т.к. являются основными объектами воздействия при попытках дестабилизации или уничтожения системы/процесса, а также имеют риски при возникновении чрезвычайной ситуации.

Ключевые слова: *критическая информационная инфраструктура, SCADA, безопасность, риски, угрозы, кибербезопасность, киберпреступность.*

Introducere

Literatura de specialitate din domeniul studiilor de securitate, actualmente abordează o varietate imensă de riscuri și pericole la adresa securității naționale, datorită rapidității vitezei de transformare socială pe care omenirea nu a cunoscut-o anterior. Este evident că ne aflăm într-o perioadă de modificări profunde, în care paradigmele clasice cu privire la asigurarea securității necesită adaptări de conținut, pentru a oferi valoarea necesară realităților contemporane. Examinând doar secolul trecut, putem observa că lumea a traversat două războaie mondiale, pentru prima dată în istorie s-a confruntat cu un război rece, plus numeroase conflicte regionale. Doar că toate acestea nu au reușit să genereze atât de multe schimbări sociale, în măsura în care tehnologia a reușit[1].

Apărarea națională a unui stat este în prezent îngreunată de răspândirea gravă a provocărilor cauzate de războiul asimetric, care, deși a evoluat, este în continuă transformare și persistă să se folosească de inovațiile tehnice. Reușitele domeniului tehnologic se regăsesc și în modul de operaționalizare a unui război hibrid ori cognitiv. Aceste noi tipuri de amenințări au transformat paradigmele tradiționale de securitate, deoarece forțele militare puternice nu mai pot garanta pacea socială a statelor[2].

Mai mult ca atât, vechea abordare strategică a securității își pierde treptat relevanța, fiind perturbată de un șir de alți factori de insecuritate, precum: diverse intervenții economice, sancțiuni, indisponibilitatea continuă a apei potabile, alimentelor, vulnerabilitățile infrastructurilor critice etc.

Definirea conceptului de infrastructură informatică critică

Literatura de specialitate care abordează infrastructura critică (IC) explică termenul „critic" prin referirea la „*infrastructura care, dacă este perturbată sau distrusă, poate aduce la catastrofe și pagube majore*"[3]. Din noțiunea enunțată rezultă că obiectele de infrastructură critică pot fi de natură diferită, începând cu servicii publice și organizații, finalizând cu instalații materiale și instituții financiar-bancare. Criteriul central de desemnare a unui obiectiv drept infrastructură critică este determinat în raport cu riscurile potențiale, inclusiv pentru întreaga societate, ce pot fi cauzate de perturbarea sau distrugerea acestor obiective. Unele elemente de infrastructură pot fi tratate ca fiind „critice" pe parcursul existenței lor, așa cum altele îl pot primi sau pierde, la un moment dat, în funcție de reziliența acestora, dar și de dinamica economică si social-politică a societății.

Directiva Consiliului UE nr. 114/2008/CE privind *„Identificarea și desemnarea infrastructurilor critice europene și evaluarea necesităților de îmbunătățire a protecției acestora*" (adoptată la 8 decembrie 2008) definește infrastructura critică după cum urmează: „*un element, sistem sau o parte componentă a acestuia, aflată pe teritoriul statelor membre, care este esențială pentru menținerea funcțiilor sociale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții vitale*"[4], iar potrivit

[1] Adriana ALEXANDRU, Victor VEVERA, Ella Magdalena CIUPERCĂ, *National Security and Critical Infrastructure Protection*. În: *International Conference Knowledge-Based Organization*, vol. XXV, nr. 1/2019, DOI: 10.2478/kbo-2019-0001, pp. 8-13. Disponibil la: https://www.researchgate.net/publication/334677561_National_Security_and_Critical_Infrastructure_Protection.

[2] Miklos BOROCZ, *Politicile privind protecția infrastructurilor critice la nivel european*, În: Impact Strategic nr. 3/2021, NATO și UE: politici, strategii, acțiuni, DOI: 10.53477/1842-810X-21-13,p. 49

[3] Netherlands - Report on Critical Infrastructure protection; Ministry of the Interior September 2005.

[4] Directiva Consiliului UE nr. 114/2008/CE privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţilor de îmbunătăţire a protecţiei acestora, pu-

Cărții verzi privind programul european de protecție a infrastructurii critice (European Programme for Critical Infrastructure Protection - EPCIP), „*infrastructura critică este constituită atât din componente fizice, precum construcții hidrotehnice, cât și din componente virtuale, precum spațiul cibernetic*”[5].

Multitudinea infrastructurilor critice rămâne totdeauna deschisă și variabilă. În funcție de spațiul-suport, mai exact de spațiul sau spațiile în care sunt sau pot fi identificate, se clasifică în mai multe categorii, principalele fiind: *fizice, cosmice și virtuale*[6]. Aceste tipuri de infrastructuri, deși se află în spații diferite, au o legătură strânsă între ele, unele dintre acestea devenind chiar interdependente.

Una dintre principalele caracteristici ale infrastructurilor critice o reprezintă sistemele informatice datorită cărora toate sectoarele operează aproape complet, automatizat utilizând sisteme IT. Atât în literatura de specialitate, cât și în legislația națională a multor țări, inclusiv europene, conceptul de infrastructură informatică critică (IIC) este definit în cele mai diverse moduri.

Respectiv, unii autori[7] consideră că infrastructurile informatice critice reprezintă: „*bunuri materiale și digitale, rețele informatice, servicii electronice și instalații care, dacă ar fi perturbate sau distruse, ar avea un impact grav asupra sănătății, securității sau bunăstării economice a cetățenilor și asupra funcției eficiente a guvernului unei țări*”.

Într-o altă accepțiune, Recomandarea Consiliului OECD[8] pentru protecția infrastructurilor informatice critice [C(2008)35] definește infrastructurile informatice critice (Critical Information Infrastructure - CII) referindu-se la „*acele sisteme și rețele de informații interconectate, a căror întrerupere sau distrugere ar avea un impact grav asupra sănătății, siguranței, securității sau bunăstării economice a cetățenilor sau asupra funcționaării eficiente a guvernului sau a economiei*”[9].

Prin urmare, sistemele informatice prin care operează majoritatea infrastructurilor critice *reprezintă o țintă predilectă a atacurilor cibernetice, din ce în ce mai bine organizate și mai sofisticate.* Atacurile asupra sistemelor informatice aparținând unor instituții ale statului sau aflate în proprietate privată, asimilate infrastructurilor critice, devin tot mai periculoase și mai dificil de prevenit. Ele pot fi inițiate de grupări de criminalitate organizată care vizează, în cele mai multe cazuri, obținerea de resurse financiare, dar și de către state ostile, ca arme pentru atingerea unor scopuri politice[10].

Din aceste considerente, ar trebui luate toate măsurile de protecție necesare pentru a se asigura că IIC a niciunui sector vital nu este atacat pe teritoriul unui stat.

Protecția unei infrastructuri critice este constituită din totalitatea măsurilor stabilite pentru reducerea riscurilor de blocare a funcționării sau de distruge-

blicată în Jurnalul Oficial al Uniunii Europene nr. L345/75 la 23.12.2008. Disponibil la https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[5] Comunicarea Comisiei Europene nr. COM(2006) 786 final din 12.12.2006 privind Carta verde privind programul european de protecție a infrastructurii critice (EPCIP) Disponibil la: https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html

[6] Gr. ALEXANDRESCU, Gh. VĂDUVA, *Infrastructuri critice: pericole, amenințări la adresa acestora, sisteme de protecție,* București: Editura Universității Naționale de Apărare „Carol I”, 2006, 47 p. ISBN (10) 973-663-412-4; ISBN (13) 978-973-663-412-3, p. 21.

[7] Victor PHILIP, Elvin PRASAD, Aaron BOYD, *Introduction to critical information infrastructure protection*. 43 p. Disponibil la: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/Pacific%20Drill%202020/CII-Protection-ITU-Pacific-Drill-Dec-2020-Final.pdf p. 7

[8] OECD (Organization for Economic Cooperation and Development) – Organizația pentru Cooperare Economică și Dezvoltare.

[9] https://www.oecd.org/sti/40825404.pdf, p. 4

[10] Serviciul Român de Informații, Protecția Infrastructurilor Critice, 25 p. Disponibil la: https://www.sri.ro/upload/Brosura-ProtectiaInfrastructurilorCritice.pdf, p. 19

re a unei infrastructuri critice[11]. Așadar, securitatea națională, inclusiv cea internațională, sunt dependente, în foarte mare măsură, de infrastructurile critice ale societății și statului, dar acestea sunt tot mai vulnerabile în fața mijloacelor din ce în ce mai sofisticate de atac asupra lor.

Literatura de specialitate acordă spații ample pentru descrierea modalităților de protecție a infrastructurilor critice. Unii autori acceptă două axiome în analiza acestui domeniu:

- practic, este imposibil să se asigure protecția la nivelul de 100% a unei infrastructuri critice;
- nu există o soluție unică, universală pentru rezolvarea acestei probleme.

Aceiași autori consideră că specialiștii oferă trei modalități de abordare a protecției infrastructurilor critice:

- protecția infrastructurilor informatice critice care ia în considerare numai securitatea conexiunilor IT și soluțiile de protecție a acestora, competențele protecției fizice a celorlalte infrastructuri fiind disipată între diverse organisme de stat sau private;
- asigurarea funcționării neîntrerupte a rețelelor informatice și a elementelor fizice ale infrastructurilor critice. În acest caz, protecția fizică reprezintă o componentă a sistemului național de protecție civilă. În prezent, se încearcă o cooperare cât mai strânsă între sectorul public și cel privat pentru atingerea unui grad cât mai înalt de protecție a infrastructurilor critice. La nivel de planificare strategică însă, cooperarea este aproape inexistentă. Acest tip de tratare a fost denumit generic „*all hazards approach*" (abordarea tuturor riscurilor);
- realizarea unui sistem minim obligatoriu de protecție a sistemului de guvernare și a anumitor organisme statale, vitale.

Totodată, analiștii acordă o atenție sporită atacurilor cibernetice organizate, capabile să cauzeze destabilizarea infrastructurii naționale, a economiei sau chiar a tuturor componentelor securității naționale. Complexitatea tehnică solicitată pentru înfăptuirea unui astfel de atac este destul de ridicată și, parțial, explică de ce încă nu s-au înregistrat astfel de atacuri până acum[12].

Totuși, nu trebuie să fim prea încrezători, deoarece atacurile cibernetice asupra rețelelor informatice ale oricărei țări pot avea consecințe grave, cum ar fi întreruperea funcționării unor componente-cheie, provocarea pierderilor de venituri și proprietăți intelectuale, inclusiv pierderea vieților omenești.

Exemple de atacuri asupra infrastructurilor informatice critice cu impact asupra securității naționale

Unele state au investit importante resurse economice, tehnice și umane în dezvoltarea amenințărilor avansate persistente (APT – *Advanced Persistent Threat*), care atacă agresiv și aleg obiective foarte specifice în scopul de a menține o prezență constantă în cadrul rețelelor posibilelor victime. Atacurile grupărilor APT[13] sunt foarte dificil de detectat, din cauza faptului că utilizează tehnici și componente care sunt special proiectate pentru a se infiltra și a rămâne în rețea fără a fi detectate.

În mod corespunzător, problematica protecției infrastructurilor critice a devenit unul dintre subiectele importante inclusiv de pe agenda NATO, elaborându-se în acest sens o serie de analize și studii asupra

[11] Gr. ALEXANDRESCU, Gh. VĂDUVA, *Infrastructuri critice: pericole, amenințări la adresa acestora, sisteme de protecție,* București: Editura Universității Naționale de Apărare „Carol I", 2006, 47 p. ISBN (10) 973-663-412-4; ISBN (13) 978-973-663-412-3, p. 12

[12] Nicolae PANFILII, *Aspecte relevante privind protecția infrastructurilor informatice critice*. Teză de master. Universitatea Tehnică din Moldova, Chișinău, 2022, 100 p. URI: http://repository.utm.md/handle/5014/19140, p. 14

[13] O grupare APT este cel mai frecvent o organizație sponsorizată de un anumit stat, cu obiective definite pe termen lung, ale cărei acțiuni sunt de obicei folosite pentru a se infiltra în rețelele informatice de profil înalt, adesea guvernamentale, și pentru a extrage informații sensibile sau confidențiale.

gradului de pregătire a statelor membre în ceea ce privește identificarea și protejarea infrastructurilor critice. Aceste studii au fost inițiate de către comisiile de specialitate aflate în subordinea Comitetului de Planificare în Domeniul Urgențelor Civile (*Senior Civil Emergency Planning Committee* - SCPEC), principalul organism al NATO care reglementează intervenția protecției civile în situațiile de urgență.

Lumea reală și conflictele fizice s-au extins în lumea virtuală a spațiului cibernetic. În ultimii ani, au fost detectate atacuri cibernetice împotriva infrastructurilor critice ale diferitor țări și obiectivelor specifice. Câteva exemple cunoscute publicului larg sunt: atacul cibernetic din Estonia, în 2007, *care a dus la dezactivarea temporară în mare parte a infrastructurilor critice ale țărilor baltice*; atacul cibernetic lansat de Rusia împotriva Georgiei, în 2008, ca un preludiu la invazia terestră; cazul Stuxnet, cu atacuri cibernetice împotriva sistemelor SCADA[14]; cazul Duqu, cu atacuri cibernetice împotriva organizațiilor industriale; atacurile cibernetice suferite de rețelele clasificate ale Guvernului Statelor Unite, comise de către hackeri de pe teritoriul chinez etc.

Ulterior, astfel de atacuri au mai avut loc și în Ucraina, între iulie 2014 și iulie 2018, unde mai multe infrastructuri critice (aprovizionarea cu energie, sectorul de transport, alimentarea cu apă potabilă, sistemul bancar și piețele finaciare) au fost atacate de grupuri de hackeri din Rusia. Grupurile de hackeri ruși CyberBerkut și GreenDragon au accesat în mod neautorizat sistemul PrivatBank și au dezvăluit informații confidențiale (detalii despre conturi, numere de telefon etc.).

Pe 23 decembrie 2015, după câteva luni de muncă, grupul APT 28[15] a lansat un atac la distanță, întrerupând serviciile de aprovizionare cu electricitate către clienți din Kiev, Prykarpattia și Cernăuți. Atacul a lăsat aproximativ 225 000 de consumatori fără energie electrică și încălzire, timp de șase ore. Acesta a fost primul atac cibernetic, documentat public, împotriva unui sistem de control al rețelei electrice. De asemenea, un *malware*[16] denumit BlackEnergy a fost detectat la timp în rețeaua aeroportului internațional Borispil de lângă Kiev, astfel încât hackerii nu au putut efectua atacul cibernetic.

În anul 2017, un virus[17] de tip *ransomware*[18], denumit NotPetya (care inițial viza Ucraina, dar a atins cercurile de afaceri din întreaga lume), a afectat mai multe sectoare, inclusiv sectoare deținătoare de infrastructuri critice. Atacurile cibernetice au vizat guvernul ucrainean, sectorul energetic (stația de monitorizare a radiațiilor de la Cernobîl), sectorul bancar (Banca Națională a Ucrainei și bancomatele la nivel național) și sectorul transporturilor (sistemul de plăți electronice pentru metrou, în Kiev), iar în iulie 2018, Serviciul de Securitate al Ucrainei a reușit să combată o operațiune de sabotaj ce viza aprovizionarea cu apă potabilă. Datorită rolului deosebit al infrastructurii, dacă atacul ar fi avut succes, ar fi cauzat grave probleme de alimentare cu apă la nivel național.

[14] SCADA este abrevierea din engleza pentru Monitorizare, Control și Achiziții de Date (Supervisory Control And Data Acquisition). Termenul se referă la un sistem amplu de măsură și control. Automatizările SCADA sunt folosite pentru monitorizarea sau controlul proceselor chimice, fizice sau de transport.

[15] APT28 este o grupare de hackeri care provine din Rusia. Activitatea lor datează încă de la mijlocul anilor 2000. Grupul APT28 este cunoscut sub numele Fancy Bear, dar este recunoscut și sub diferite alte pseudonime - Sofacy Group, STRONTIUM, Sednit, Pawn Storm și Tsar Team.

[16] Programele *malware* („malicious software") reprezintă un termen care grupează toate tipurile de programe rău-intenționate. Tipul cel mai cunoscut de program malware este un virus.

[17] Virusul este un program malware de dimensiuni mici care în general se instalează singur, fără voia utilizatorului, atașându-se altor programe, și poate provoca pagube atât în sistemul de operare, cât și în elementele hardware (fizice) ale computerului.

[18] *Ransomware* este un program *malware* care, după ce se instalează pe dispozitivul victimei, criptează datele victimei, ținându-le „ostatice", sau șantajează victima amenințând-o că îi va publica datele dacă aceasta nu plătește o „răscumpărare".

Cercetătorii[19] spun că atacurile anterioare s-au putut suprapune peste încercări mai mici efectuate între noiembrie și decembrie 2015, care vizează sistemele miniere și feroviare ucrainene (cu programe *malware*, precum KillDisk și BlackEnergy). Prin urmare, rezultă că contracararea unor astfel de atacuri este obligatorie și necesită realizarea unor componente riguroase încă destul de anevoios de proiectat cu mijloacele existente în prezent[20].

Din analiza atacurilor menționate mai sus deducem că pericolele și amenințările din spațiul virtual vizează, în general, rețelele, nodurile de rețea și centrele vitale, mai exact, echipamentele și sistemele fizice ale acestora (calculatoare, prestatori de servicii internet (ISP – Internet Service Provider), conexiuni și noduri de rețea etc.), precum și celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, rețele de energie electrică, cabluri, fibră optică și alte componente). În aceeași măsură, ele vizează și depozitele de date și de programe, sistemele de înmagazinare, de păstrare și de distribuție a informației, suportul material al bazelor de date și multe altele. Însă, înainte de toate, asemenea pericole și amenințări vizează sistemele IT (întreprinderi, linii de producție, sisteme de aprovizionare cu materiale strategice, infrastructuri de resurse și de piețe, institute de cercetări, sisteme de comunicații etc.).

Într-o altă opinie a specialiștilor, din categoria mereu în extensie a pericolelor și amenințărilor împotriva infrastructurilor critice ale ciberspațiului fac parte și următoarele [6, p. 35-36]:

- pericolele și amenințările rezultate din lupta dintre marile firme pentru supremația IT, resurse și piețe;
- pericolele și amenințările asimetrice;
- dezvoltarea rețelelor subversive și neconvenționale IT;
- activitatea tot mai intensă a hackerilor;
- cyberterorismul.

În consecință, se constată că obiectivul multor organizații publice/private și/sau internaționale este de a obține secrete de stat/industriale și economice de la alte state sau organizații competitoare, aceste tipuri de atacuri fiind de multe ori executate cu sprijin guvernamental[21].

Numărul tot mai mare și complexitatea crescută a atacurilor cibernetice evidențiază o nevoie imediată de schimbare a modului în care se examinează securitatea infrastructurilor critice. Dezvoltarea unor infrastructuri reziliente la amenințări și riscuri reprezintă o necesitate, prin adoptarea unor abordări de tipul „*secure by design*[22]” și „*security by default*[23]” în sectoarele declarate ca fiind de importanță deosebită[24].

[19] Miklos BOROCZ, *Politicile privind protecția infrastructurilor critice la nivel european,* În: Impact Strategic nr. 3/2021, NATO și UE: politici, strategii, acțiuni, DOI: 10.53477/1842-810X-21-13, pp. 48-64, p. 51

[20] Gr. ALEXANDRESCU, Gh. VĂDUVA, *Infrastructuri critice: pericole, amenințări la adresa acestora, sisteme de protecție,* București: Editura Universității Naționale de Apărare „Carol I”, 2006, 47 p. ISBN (10) 973-663-412-4; ISBN (13) 978-973-663-412-3, p. 14

[21] Vasile Florin POPESCU, *Securitatea cibernetică a infrastructurilor critice într-o lume din ce în ce mai conectată*. În: Buletinul Universității Naționale de Apărare „Carol I”, Septembrie 2019, pp. 83-87. Disponibil la: https://revista.unap.ro/index.php/revista/article/download/628/585/2725, p. 85

[22] Securizarea prin proiectare (*secure by design*) este un principiu potrivit căruia produsele și capabilitățile *software* urmează a fi concepute pentru a fi sigure la bază, chiar din momentul proiectării. Strategiile, tacticile și modelele alternative de securitate sunt luate în considerare la începutul unui proiect de *software*, iar cele mai bune sunt selectate și aplicate de arhitectură și sunt folosite ca principii directoare pentru dezvoltatori. Este, de asemenea, recomandabil să se utilizeze modele de design strategice care au efecte benefice asupra securității, chiar dacă aceste modele de design nu au fost concepute inițial, având în vedere securitatea.

[23] Securitatea implicită (*security by default*) semnifică că setările implicite de configurare ale unui sistem, program, etc. sunt cele mai sigure setări posibile, care nu sunt neapărat cele mai ușor de utilizat.

[24] Ioan-Cosmin MIHAI (coordonator), Costel CIUCHI,

Protecția infrastructurilor informatice critice în Republica Moldova

Identificarea infrastructurilor necesare susținerii actului de guvernare și a serviciilor administrației publice necesită automatizarea unor procese privind monitorizarea și implementarea de controale regulate prin dezvoltarea de centre specializate de monitorizare NOC/SOC (*Network Operations Center/ Security Operations Center*)[25].

În acest sens, în cadrul departamentelor de specialitate (publice/private) care operează infrastructuri critice este necesară implementarea unei componente specializate, cu capacități și cunoștințe speciale în dezvoltare și aplicare de politici privind modelarea, simularea și analiza riscurilor (*backup, disaster recovery* etc.), monitorizare și gestionare a sistemelor de protecție (*firewall-uri, antivirus-uri,* sistemelor de prevenire a intruziunilor etc.), precum și evaluarea și raportarea partajată a amenințărilor. Modelarea fluxurilor de cooperare în cazul incidentelor cibernetice reprezintă o componentă vitală în procesele de management al rețelelor și sistemelor informatice. Dezvoltarea unui ansamblu coerent de măsuri privind cooperarea sectorială în domeniu, detecția, răspunsul, recuperarea automată și asigurarea de capacități de protecție va reprezenta fundamentul pentru trecerea la un model național specific privind infrastructurile critice.

Protecția infrastructurilor critice, la modul general, în Republica Moldova se realizează de un șir de organe și subdiviziuni speciale ale acestora. Este vorba despre: Inspectoratul General pentru Situații de Urgență (IGSU) al Ministerului Afacerilor Interne, Centrul Antiterorist al Serviciului de Informații și Securitate (CAT), Ministerul Apărării etc.

Sistemul de reacție asupra situațiilor de urgență reprezintă un complex de instituții specializate ale statului, ce intră în componența Ministerului Afacerilor Interne, care execută, în condițiile legii, sarcini în domeniul protecției populației, teritoriului, mediului înconjurător și proprietății în caz de pericol sau declanșare a situațiilor excepționale.

În vederea perfecționării continue a pregătirii profesionale, angajații IGSU participă permanent la exerciții și aplicații tactice în cadrul poligoanelor speciale atât pe teritoriul statului nostru, cât și peste hotarele lui. Astfel, spre exemplu, în cadrul cooperării Republicii Moldova cu Statul Carolina de Nord, Statele Unite ale Americii, IGSU își are segmentul său de cooperare. Pe parcursul anilor de colaborare, IGSU a participat la un șir de evenimente, petrecute atât în țară, cât și peste hotarele ei: seminare, vizite de studii, exerciții de teren și de câmp. În colaborare cu experții Gărzii Naționale a Statului Carolina de Nord a fost organizat Exercițiul de teren „Codrii 2009", de asemenea experții menționați au participat și la Exercițiul internațional de teren „Codrii 2011", organizat cu suportul EADRCC/ NATO[26].

O altă subunitate specializată este Centrul Antiterorist al Serviciului de Informații și Securitate (CAT). Centrul respectiv a fost creat în anul 2006 în calitate de organ responsabil de coordonarea tehnică a măsurilor de prevenire și combatere a terorismului

---

Gabriel-Marius PETRICĂ, *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu*. Institutul European din România, București, 2018, 88 p. ISBN online: 978-606-8202-60-0. Disponibil la: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf, p. 36-37

[25] NOC menține și monitorizează infrastructura IT a unei companii, inclusiv infrastructura de rețea, punctele finale și configurațiile Cloud, pentru a se asigura că funcționează fără probleme și eficient în orice moment. SOC monitorizează punctele finale, rețeaua și serverele unei organizații pentru a o proteja de amenințările cibernetice.

[26] Terentie CARP, *Consideraţiuni privind managementul infrastructurilor critice în Republica Moldova.* În: Analele ştiinţifice ale Academiei „Ştefan cel Mare" a MAI al Republicii Moldova, ştiinţe socioumane, ediţia a XII-a, nr. 2, p. 168-169, p. 3.

desfășurate de către autoritățile publice competente. În conformitate cu pct. 6 din Hotărârea Guvernului nr. 1295 din 13.11.2006 privind Centrul Antiterorist al Serviciului de Informații și Securitate[27], acestuia îi revin mai multe sarcini de bază, unele dintre acestea fiind:

- culegerea, analiza și valorificarea informațiilor despre potențialele riscuri și amenințări de natură extremist-teroristă obținute în urma activităților desfășurate;
- aprecierea factorilor de risc și amenințărilor teroriste la securitatea națională a Republicii Moldova, acumularea și analiza informațiilor despre starea, dinamica și tendințele extinderii fenomenului terorismului și a altor manifestări de extremism;
- analiza informațiilor din diferite surse cu privire la procesele și evenimentele ce se referă la terorism și informarea autorităților publice competente privind situația operativă în domeniul prevenirii și combaterii terorismului;
- verificarea stării de protecție antiteroristă la obiectele de importanță strategică și înaintarea propunerilor privind sporirea nivelului securității acestora ș.a.

De asemenea, la lichidarea consecințelor situațiilor excepționale, nu în ultimul rând sunt implicate și forțele și efectivele Ministerului Apărării al Republicii Moldova, precum și alte organe și subdiviziuni specializate.

Dacă e să ne referim nemijlocit la protecția mediului/spațiului virtual al Republicii Moldova, în calitate de organ specializat în domeniul asigurării securității naționale (organ al securității statului), Serviciului de Informații și Securitate îi revine una dintre misiunile primordiale, și anume prevenirea și combaterea agresiunilor din mediul virtual, intern sau extern, îndreptate spre sistemele informatice și de comunicații electronice de importanță statală. Această misiune este realizată, în conformitate cu legislația în vigoare, de către Serviciu prin intermediul următoarelor procese operaționale[28]:

- elaborarea propunerilor privind asigurarea securității informatice, elaborarea și promovarea politicii de stat și exercitarea controlului în domeniul asigurării protecției informației atribuite la secretul de stat în spațiul cibernetic;
- crearea, asigurarea funcționării și securității sistemelor guvernamentale de comunicații electronice, elaborarea strategiei și realizarea politicii naționale în domeniul creării, administrării și asigurării funcționării și securității sistemelor speciale de comunicații electronice;
- asigurarea conducerii țării, a ministerelor, departamentelor și a altor autorități publice, inclusiv în străinătate, conform Nomenclatorului întocmit de Guvern, cu legătură guvernamentală, cifrată, secretă și cu alte tipuri de telecomunicații, organizarea și asigurarea siguranței exploatării lor;
- depistarea emiterilor radio ale mijloacelor radio electronice emițătoare a căror activitate periclitează securitatea de stat.

Pe de altă parte, în vederea asigurării unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și liberei circulații a informațiilor, a fost adoptată Strategia de securitate informațională pentru anii 2019-2024[29]. Strategia prezintă o evaluare a situației actuale în domeniul securității informaționale, enumeră performanțele înregistrate și punctează noi tendințe de dezvoltare a societății informaționale, iar obiectivele con-

[27] Hotărârea Guvernului nr. 1295 din 13.11.2006 privind Centrul Antiterorist al Serviciului de Informații și Securitate. Publicată 17.11.2006 în Monitorul Oficial nr. 178-180, art. 1385.

[28] Pagina oficială a Serviciului de Informații și Securitate, rubrica Asigurarea securității informaționale. Disponibil la: https://sis.md/ro/content/asigurarea-securit%C4%83%C8%9Bii-informa%C8%9Bionale.

[29] Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024, aprobată prin Hotărârea Parlamentului nr. 257 din 22.11.2018. Anexa nr. 1. Publicată la 18.01.2019 în Monitorul Oficial nr. 13-21, art. 80.

stituie o preocupare majoră a Serviciului Tehnologia Informației și Securitate Cibernetică (STISC), instituție publică din subordinea Guvernului, și monitorizată de către Cancelaria de Stat.

Rolul Serviciului Tehnologia Informației și Securitate Cibernetică, în acest sens, este de a asigura o protecție tehnică în spațiul informațional prin realizarea acțiunilor de consolidare a capacităților de apărare cibernetică și de combatere a criminalității informatice sub aspect tehnic. Printre acțiunile de bază ale STISC-ului prevăzute în Planul de acțiuni privind implementarea Strategiei securitate informațională pentru anii 2019-2024[30] se enumeră următoarele:

- sistematizarea, analiza și evaluarea datelor statistice la capitolul securității cibernetice;
- determinarea politicii privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale;
- dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în domeniul tehnologiilor informaționale și comunicațiilor;
- desfășurarea acțiunilor de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile securității cibernetice;
- desfășurarea exercițiilor și antrenamentelor de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate;
- organizarea și efectuarea atelierelor de lucru în domeniul securității cibernetice.

Totodată, în vederea executării prevederilor Hotărârii Guvernului nr. 746 din 18.08.2010 cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului Republica Moldova – NATO actualizat (document abrogat la 30.07.2014) în cadrul Serviciul Tehnologia Informației și Securitate Cibernetică a fost creat Centrul pentru Securitatea Cibernetică - CERT-GOV-MD. Misiunea Centrului este de a susține societatea moldovenească în protejarea împotriva incidentelor cibernetice și este punctul central de raportare și coordonare privind incidentele de securitate în sistemele de comunicații și informatice aflate în administrarea Serviciului Tehnologia Informației și Securitate Cibernetică.

Cu atât mai mult, pentru a spori capacitățile de apărare cibernetică din Armata Națională, în cadrul Programului Știință pentru Pace și Securitate, realizat în sprijinul Pachetului de consolidare a capacităților de apărare (DCBI) pentru Republica Moldova, un Centru de Reacție la Incidente Cibernetice (CRIC) al Armatei Naționale a fost inaugurat la 21 ianuarie 2021, la Chișinău, având misiunea de a proteja infrastructura tehnologiilor informaționale, să prevină, să detecteze și să reacționeze operativ la atacurile cibernetice, precum și să consolideze securitatea cibernetică, obiectiv stabilit conform noului Plan Individual de Acțiuni al Parteneriatului Republica Moldova – NATO pentru anii 2022-2023, aprobat prin Hotărârea Guvernului nr. 26 din 19.01.2022.

Răspunderea juridică pentru fapte ce atentează la securitatea infrastructurilor critice în Republica Moldova

Sub aspectul protecției juridice a infrastructurilor critice, răspunderea penală pentru comiterea unor fapte care pot, inclusiv tangențial, atenta la protecția infrastructurilor critice este prevăzută de Codul penal al Republicii Moldova[31], care incriminează un șir de fapte de acest gen, în special: art. 278 - actul terorist; art. 278[1] - livrarea, plasarea, punerea în funcțiune

[30] Planul de acțiuni în vederea implementării Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024, aprobată prin Hotărârea Parlamentului nr. 257 din 22.11.2018. Anexa nr. 2. Publicată la 18.01.2019 în Monitorul Oficial nr. 13-21 art. 80.

[31] Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. Capitolul XIII, Infracțiuni contra securității publice şi a ordinii publice. Publicat la 14.04.2009 în Monitorul Oficial nr. 72-74 art. 195.

sau detonarea unui dispozitiv exploziv ori a altui dispozitiv cu efect letal; art. 279 - finanțarea terorismului; art. 289[1] - infracțiuni contra securității aeronautice și contra securității aeroporturilor; art. 289[2] - infracțiuni contra securității transportului naval; art. 289[3] - infracțiuni contra securității platformelor fixe; art. 293 încălcarea regulilor de evidență, păstrare, transportare și folosire a substanțelor ușor inflamabile sau corozive; art. 295 - sustragerea materialelor sau a dispozitivelor radioactive ori a instalațiilor nucleare, amenințarea de a sustrage sau cererea de a transmite aceste materiale, dispozitive sau instalații; art. 295[1] - deținerea, confecționarea sau utilizarea materialelor sau a dispozitivelor radioactive ori a instalațiilor nucleare; art. 295[2] - atacul asupra unei instalații nucleare; art. 296 - încălcarea regulilor de protecție contra incendiilor; art. 297 - neîndeplinirea dispozițiilor organelor de stat de supraveghere în domeniul protecției civile; art. 298 – încălcarea regulilor de exploatare a obiectivelor energetice; art. 300 - încălcarea regulilor privind efectuarea exploatărilor miniere sau a lucrărilor de construcție miniere; art. 301 - încălcarea regulilor de securitate în întreprinderile sau secțiile supuse pericolului exploziei etc.

În aceeași ordine de idei, un capitol din Codul penal este dedicat infracțiunilor informatice și infracțiunilor în domeniul telecomunicațiilor prevăzute la art. 259-261[1] din Codul penal[32], și anume: art. 259 - accesul ilegal la informația computerizată; art. 260 - producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloace tehnice sau produselor program; art. 260[1] - interceptarea ilegală a unei transmisii de date informatice; art. 260[2] - alterarea integrității datelor informatice ținute într-un sistem informatic; art. 260[3] - perturbarea funcționării sistemului informatic; art. 260[4] - producerea, importul, comercializarea sau punerea ilegală la dispoziție a parolelor, codurilor de acces sau a datelor similare; art. 260[5] - falsul informatic; art. 260[6] - frauda informatică; art. 261 - încălcarea regulilor de securitate a sistemului informatic; art. 261[1] - accesul neautorizat la rețelele și serviciile de telecomunicații, a căror investigare, potrivit Codului de procedură penală, se află în competența nemijlocită a procurorului.

Întru asigurarea efectuării acțiunilor procesual-penale, și anume a activității de urmărire penală pe cazurile de criminalitate informatică, nu în ultimă instanță, este de specificat rolul deosebit de important al Secției combatere crime cibernetice a Procuraturii Generale, a Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale și a Direcției Investigare a Infracțiunilor Informatice din cadrul Inspectoratului Național de Investigații al Inspectoratului General al Poliției al Ministerului Afacerilor Interne, dar și a subdiviziunii specializate a Serviciului de Informații și Securitate, precum și a Centrului Tehnico-Criminalistic și de Expertize Judiciare al Inspectoratului General al Poliției al Ministerului Afacerilor Interne, autorități ce au atribuții nemijlocite privind prevenirea, investigarea și combaterea criminalității informatice.

Un rol nu mai puțin important rol îl au și prestatorii de servicii de comunicații electronice (providerii), care pot să sporească și să îmbunătățească calitatea investigării acestor tipuri de infracțiuni prin colaborare cu organele de drept și acordarea suportului necesar prin diverse mecanisme, de exemplu prin conservarea datelor informatice.

Concluzii

În contextul abordat, menționăm că infrastructura critică, inclusiv cea informatică critică, prezintă un interes major pentru securitatea națională, a cărei protejare căreia ar trebui să constituie inclusiv o prioritate politică, iar problemele existente în sectorul infrastructurilor critice afectează direct securitatea

[32] Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. Capitolul XI, Infracțiuni informatice și infracțiuni în domeniul telecomunicațiilor. Publicat la 14.04.2009 în Monitorul Oficial nr. 72-74 art. 195.

națională a Republicii Moldova. Securitatea drmult nu mai este o teorie, ci o realitate din ce în ce mai vulnerabilă, iar autoritățile Republicii Moldova trebuie să conștientizeze și să accepte noile abordări și evoluția firească a noului concept - protecția infrastructurii critice, într-un cadru mai larg, a sistemului de securitate și apărare națională. Factorul declanșator al noii dezbateri publice privind definirea locului și rolului pe care îl joacă actualmente conceptul de infrastructură critică în societate l-a constituit, de fapt, conștientizarea existenței unor elemente de infrastructură care, în funcție de starea în care se găsesc la un moment dat, pot avea un efect critic asupra funcționării întregii infrastructuri și cel mai important pas va consta în generarea unei noi voințe politice care să impulsioneze implementarea reformelor în sectorul infrastructurii critice din Republica Moldova.

Din păcate, deși dispunem de un cadru minim de reglementare a protecției infrastructurii critice din perspectivă antiteroristă[33] în Republica Moldova, la nivel instituțional, dificultatea principală constă în rolul-cheie atribuit Centrului Antiterorist în gestiunea acestor obiective. Astfel, protecția infrastructurii critice este efectuată doar din perspectiva antiteroristă, în principal, prin dotarea cu pașaport antiterorist, aprobarea planurilor de pază și desfășurarea testelor antiteroriste. Totuși, majoritatea țărilor dezvoltate economic au creat o singură instituție publică specializată în toate aspectele de gestiune a infrastructurii critice, precum Centrul Național de Coordonare a Protecției Infrastructurilor Critice (CNCPIC) din România.

Republica Moldova, în această etapă, dispune de o protecție limitată și fragmentată a infrastructurii critice. Stabilirea noilor reglementări privind infrastructura critică și securizarea acesteia trebuie să devină una dintre prioritățile cheie naționale și necesită a fi abordată sistemic prin adoptarea și implementarea unei legi-cadru cu privire la gestionarea și protecția infrastructurii critice naționale a Republicii Moldova și ar putea analiza în ce măsură crearea unei autorități naționale specializate de securitate cibernetică ar putea îmbunătăți cadrul instituțional de gestionare și protejare a obiectivelor de infrastructură critică, inclusiv din punct de vedere informatic. Un proiect de lege[34] privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice deja se află în Parlamentul Republicii Moldova, fiind adoptat la sfârșitul lunii aprilie 2021 în prima lectură.

Un alt aspect, care necesită atenție și urmează a fi soluționat, ține de protocoalele de protecție a infrastructurii critice nu doar de autoritățile publice, dar și de operatorii privați. Actele normative în vigoare nu stabilesc clar mecanismul de atribuire instituțiilor de resort a unor proceduri specifice de protecție a infrastructurilor critice. Având în vedere că infrastructurile critice protejate de diferite instituții pot deveni obiectul unor atacuri complexe, lipsa unor proceduri comune de protecție ar putea fi un obstacol major în gestiunea potențialelor incidente. Unele întreprinderi care furnizează servicii esențiale în calitate de operator privat de infrastructură critică, cum este, spre exemplu, S.A. „Moldovagaz", utilizează servicii de protecție prestate de întreprinderi private. Lipsa protocoalelor de protecție coordonate între întreprinderile private și instituțiile publice ar putea fi un impediment atât în prevenirea, cât și în soluționarea unor eventuale incidente sau atacuri.

De asemenea, este necesar un mecanism operațional de comunicare și avertizare timpurie cu privire la gestionarea și protejarea infrastructurii critice. Chiar dacă procedurile existente permit efec-

[33] Regulamentul privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701 din 11.07.2018. Publicat la 27.07.2018 în Monitorul Oficial nr. 277-284, art. 773.

[34] Proiect de lege privind infrastructura esențială. Disponibil la https://www.parlament.md/LegislationDocument.aspx?Id=3469b48c-dc0c-4e24-8fbc-fcce50db6870.

tuarea acțiunilor de prevenție, acestea rămân deficiente în asigurarea unei comunicări coordonate între organele specializate naționale și internaționale. În acest context, cooperarea și eventual participarea în cadrul Rețelei Europene de alertă privind infrastructurile critice (Critical Infrastructure Warning Information Network - CIWIN) ar putea oferi Republicii Moldova o valoare adăugată și la nivel național în termen lung.

Nu în ultimul rând, este necesară uniformizarea terminologică a noțiunii de „infrastructură critică". Cadrul normativ actual nu precizează dacă obiectivele infrastructurii critice se află într-un anumit raport față de alte tipuri de obiective, precum cele de importanță strategică. De asemenea, este necesară revizuirea metodologiei de identificare și desemnare a obiectivelor. Astfel, responsabilitatea de identificare ar trebui să fie atribuită doar instituțiilor publice. Operatorii privați ar urma să creeze un organ intern specializat doar în cazul gestionării a mai mult decât un obiectiv de infrastructură critică desemnată și să fie supuși verificărilor extinse de securitate din partea instituțiilor publice de resort[35].

În noua geografie a riscurilor generate de existența infrastructurilor critice în cadrul societății informatice este necesar să învățăm să gândim diferit asupra operabilității conceptelor de vulnerabilitate, siguranță, securitate și risc.

Referitor la definirea direcțiilor de construcție și coordonare a eforturilor societale pentru protecția infrastructurilor informatice critice, o serie de aspecte se vor evidenția în continuare:

- Se impune imperativ schimbul reciproc de informații, date și cunoștințe referitoare la vulnerabilitatea diferitor sisteme de infrastructuri critice, între Guvern și sectoarele implicate, transversal între sectoare distincte în cadrul conceptului de infrastructuri critice;
- Este necesar să se construiască un sistem de responsabilități care să garanteze cooperarea între diferitele grupuri active în funcționarea infrastructurilor critice.
- Protecția infrastructurilor impune construirea de capabilități integrate în cadrul diverselor instituții în structura generală a societății din Republica Moldova.
- Este necesară realizarea unei culturi de securitate (security/safety culture) corespunzătoare;
- Sistemul de legi ale societății informatice trebuie să ia în considerare potențialul de impact al pericolelor cibernetice și reglementate în mod corespunzător.
- Se impune inițierea și coordonarea adecvată a unor activități de cercetare științifică care să adreseze problematica vulnerabilității și securității infrastructurilor critice (inclusiv a celor informatice critice).

[35] Protecția infrastructurii critice: O nouă prioritate a Republicii Moldova. Comentariu de Valeriu Țurcanu și Iulian Rusu. Disponibil la: https://ipre.md/2021/07/02/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/ (Accessat – 21.10.2023)

Referințe bibliografice

1. ALEXANDRU, Adriana, VEVERA, Victor, CIUPERCĂ, Ella Magdalena. *National Security and Critical Infrastructure Protection*. În: *International Conference Knowledge-Based Organization*, vol. XXV, nr. 1/2019, DOI: 10.2478/kbo-2019-0001, pp. 8-13. Disponibil la: https://www.researchgate.net/publication/334677561_National_Security_and_Critical_Infrastructure_Protection. (Accessat – 21.11.2023)

2. Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. Capitolul XIII, Infracţiuni contra securităţii publice şi a ordinii publice. Publicat la 14.04.2009 în Monitorul Oficial nr. 72-74 art. 195.

3. Codul penal al Republicii Moldova nr. 985-XV din 18.04.2002. Capitolul XI, Infracţiuni informatice și infracțiuni în domeniul telecomunicațiilor. Publicat la 14.04.2009 în Monitorul Oficial nr. 72-74 art. 195.

4. Comunicarea Comisiei Europene nr. COM(2006) 786 final din 12.12.2006 privind Carta verde privind

programul european de protecție a infrastructurii critice (EPCIP) Disponibil la: https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html (Accessat – 21.09.2023)

5. Directiva Consiliului UE nr. 114/2008/CE privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţilor de îmbunătăţire a protecţiei acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L345/75 la 23.12.2008. Disponibil la https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (Accessat – 21.11.2023)

6. ALEXANDRESCU, Gr., VĂDUVA, Gh. *Infrastructuri critice: pericole, ameninţări la adresa acestora, sisteme de protecţie*, București: Editura Universităţii Naţionale de Apărare „Carol I", 2006, 47 p. ISBN (10) 973-663-412-4; ISBN (13) 978-973-663-412-3.

7. Hotărârea Guvernului nr. 1295 din 13.11.2006 privind Centrul Antiterorist al Serviciului de Informaţii şi Securitate. Publicată 17.11.2006 în Monitorul Oficial nr. 178-180, art. 1385.

8. MIHAI, Ioan-Cosmin, (coordonator), CIUCHI, Costel, PETRICĂ, Gabriel-Marius. *Provocări actuale în domeniul securităţii cibernetice – impact şi contribuţia României în domeniu*. Institutul European din România, București, 2018, 88 p. ISBN online: 978-606-8202-60-0. Disponibil la: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf (Accessat – 29.11.2023)

9. BOROCZ, Miklos. *Politicile privind protecția infrastructurilor critice la nivel european*, În: *Impact Strategic,* nr. 3/2021, NATO și UE: politici, strategii, acțiuni, DOI: 10.53477/1842-810X-21-13, pp. 48-64.

10. Netherlands - Report on Critical Infrastructure protection; Ministry of the Interior September 2005.

11. PANFILII, Nicolae. *Aspecte relevante privind protecția infrastructurilor informatice critice*. Teză de master. Universitatea Tehnică din Moldova, Chișinău, 2022, 100 p. URI: http://repository.utm.md/handle/5014/19140

12. Pagina oficială a Serviciului de Informații și Securitate, rubrica Asigurarea securității informaționale. Disponibil la: https://sis.md/ro/content/asigurarea-securit%C4%83%C8%9Bii-informa%C8%9Bionale. (Accessat – 21.09.2023)

13. Planul de acțiuni în vederea implementării Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024, aprobată prin Hotărârea Parlamentului nr. 257 din 22.11.2018. Anexa nr. 2. Publicată la 18.01.2019 în Monitorul Oficial nr. 13-21 art. 80.

14. Proiect de lege privind infrastructura esențială. Disponibil la https://www.parlament.md/LegislationDocument.aspx?Id=3469b48c-dc0c-4e24-8fbc-fcce50db6870.

15. Protecția infrastructurii critice: O nouă prioritate a Republicii Moldova. Comentariu de Valeriu Țurcanu și Iulian Rusu. Disponibil la: https://ipre.md/2021/07/02/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/ (Accessat – 12.10.2023)

16. Regulamentul privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701 din 11.07.2018. Publicat la 27.07.2018 în Monitorul Oficial nr. 277-284, art. 773.

17. Serviciul Român de Informații, Protecția Infrastructurilor Critice, 25 p. Disponibil la: https://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf (Accessat – 12.10.2023)

18. Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024, aprobată prin Hotărârea Parlamentului nr. 257 din 22.11.2018. Anexa nr. 1. Publicată la 18.01.2019 în Monitorul Oficial nr. 13-21, art. 80.

19. CARP, Terentie. *Consideraţiuni privind managementul infrastructurilor critice în Republica Moldova.* În: *Analele ştiinţifice ale Academiei „Ştefan cel Mare"* a MAI al Republicii Moldova, ştiinţe socioumane, ediţia a XII-a, nr. 2, p. 168-169.

20. POPESCU, Vasile Florin. *Securitatea cibernetică a infrastructurilor critice într-o lume din ce în ce mai conectată*. În: *Buletinul Universităţii Naţionale de Apărare „Carol I"*, Septembrie 2019, pp. 83-87. Disponibil la: https://revista.unap.ro/index.php/revista/article/download/628/585/2725. (Accessat – 21.10.2023)

21. PHILIP, Victor, PRASAD, Elvin, BOYD, Aaron. *Introduction to critical information infrastructure protection.* 43 p. Disponibil la: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/Pacific%20Drill%202020/CII-Protection-ITU-Pacific-Drill-Dec-2020-Final.pdf (Accessat – 20.11.2023)

22. https://www.oecd.org/sti/40825404.pdf (Accessat – 21.10.2023)