Academia Oamenilor de Ştiinţă din România

Academy of Romanian Scientists

STUDIU PRIVIND INTERCONECTAREA OPERAȚIONALĂ ȘI TEHNICĂ A SISTEMELOR DE TELECOMUNICAȚII ȘI IT ALE ARMATEI CU CELE ALE SERVICIULUI DE TELECOMUNICAȚII SPECIALE ȘI CU CELE ALE OPERATORILOR PRIVAȚI, ÎN SCOPUL CREȘTERII VIABILITĂȚII ȘI CONTINUITĂȚII ÎN FUNCȚIONARE ÎN CAZ DE CALAMITĂȚI NATURALE ȘI ÎN ALTE SITUAȚII PERICULOASE

- RAPORT DE CERCETARE ȘTIINȚIFICĂ -

Conducătorul echipei de cercetare: General-maior dr. Valentin BECHERU
Cercetător: Maior dr. Benedictos IORGA
Colaboratori: Maior Gheorghe Adrian STAN
Căpitan ing. Laurențiu CHIOSEAUA
Locotenent Valeria LINCĂ

București, 2020

Avizat coordonatori proiect:

General(r) prof.univ.dr.Teodor Frunzeti

General-locotenent(r) prof.asoc.dr.Constantin Mincu

Descrierea CIP a Bibliotecii Naţionale a României
Studiu privind interconectarea operaţională şi tehnică a sistemelor de telecomunicaţii şi IT ale armatei cu cele ale serviciului de telecomunicaţii speciale şi cu cele ale operatorilor privaţi, în scopul creşterii viabilităţii şi continutăţii în funcţionare în caz de calamităţi naturale şi în alte situaţii periculoase : raport de cercetare ştiinţifică /
conducătorul echipei de cercetare: general-maior dr. Valentin Becheru ;
cerect: maior dr. Benedictos Iorga ; colab.: maior Gheorghe Adrian Stan, căpitan ing. Laurenţiu Chioseaua, locotenent Valeria Lincă.
- Bucureşti : Editura Academiei Oamenilor de Ştiinţă din România, 2020
ISBN 978-606-8636-72-6

I. Becheru, Valentin
II. Iorga, Benedictos
III. Stan, Gheorghe Adrian
IV. Chioseaua, Laurenţiu
V. Lincă, Valeria

62

CUPRINS

INTRODUCERE

Cercetarea științifică prezentă, în eforturile de elaborare a unui studiu privind interconectarea operațională și tehnică a sistemelor de telecomunicații ale structurilor din sistemul național de apărare și securitate, cu cele ale operatorilor privați, în scopul creșterii viabilității și continuității funcționării serviciilor critice în caz de calamități naturale și situații de criză, atunci când salvarea vieților umane, funcționarea statului și menținerea climatului de securitatea națională, devin primordiale.

Studiul actual își propune determinarea riscurilor manifestate asupra infrastructurii naționale critice de comunicații, în scopul aplicării celor mai bune practici, tehnici și proceduri de limitare a acestora precum și de creștere a interconectării și rezilienței infrastructurii și serviciilor, indiferent de condițiile sociale și de mediu. Problematica identificării corecte a riscurilor emergente, este vitală, fiind etapa de bază care determină ulterior întreg procesul de cercetare pentru dezvoltarea rezilienței infrastructurii de comunicații naționale în situații de criză și calamități naturale, prin implementarea unor arhitecturi de rețea hibride interconectate, de tip guvernamental - private. În prezenta cercetare, pentru atingerea obiectivului, am urmărit efectuarea unei analize tehnice aplicate asupra modului în care, infrastructuri critice similare din state dezvoltate tehnologic precum SUA, Canada, dar și Uniunea Europeană au fost afectate și au răspuns la amenințări emergente exercitate asupra serviciilor de comunicații și rețelelor de date, în situații de criză și calamități naturale.

De asemenea, am urmărit limitarea efectelor riscurilor identificate și dezvoltarea rezilienței de sistem, prin tehnologie și prin implementarea tehnicilor avansate din domeniul IT&C disponibile la momentul actual în industria de profil, precum NGN (Next Generation of Networks), MPLS (Multiprotocol Label Switching), tehnologii de comunicații satelitare și sisteme cloud computing.

Subiectul creșterii rezilienței infrastructurilor de comunicații critice a statelor, prin managementul riscului de securitate și prin soluții arhitecturale de rețea dinamice, interconectate, virtuale, bazate pe tehnologia IP, este intens dezbătută atât în literatura de specialitate, cât și la nivelul politicilor guvernamentale regionale, europene și mondiale, fiind un domeniu vital pentru stabilitatea economică, socială și chiar globală în actualul context tehnologic și de insecuritate.

Politica europeană privind protecția infrastructurilor critice reliefată prin raportul Comisiei Europene *„Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”*

și prin politica comună *„European principles and guidelines for Internet resilience and stability - 2011”*, abordarea SUA din strategia *„National Strategy for Physical Protection of Critical Infrastructures and Key Assets”,* dar și literatura de specialitate, reprezentată de raportul de cercetare *„Best practices for Critical information infrastructure Protection (CIIP) – Experiences from Latin America and the Caribbean and selected countries”* al autorilor *Antoni Garcia Zaballos si Inkyung Jeun* și studiile de caz realizate de Argenti Paul - *Criza comunicațiilor.Lecții învățate din 11 septembrie - Harvard Business Review* și respectiv Ramgopal Rajan - *Reducing coordination risks around communication infrastructure protection during disasters:an Alberta floods case study,* pot constitui modele de bune practici și analiză în procesul de cercetare și identificare corectă a riscurilor, exercitate în actualul context, asupra infrastructurii naționale critice de comunicații, astfel încât, procesul de creștere al rezilienței să beneficieze de o experiență aplicată și fundamentată practic în domeniul managementului de risc.

INFLUENȚA CADRULUI ORGANIZAȚIONAL ȘI RISCURILOR EMERGENTE ASUPRA INFRASTRUCTURII DE COMUNICAȚII CRITICE

I. Cadrul organizatoric național și relațiile funcționale între principalii deținători de infrastructuri critice de comunicații în actualul context organizatoric, procedural și legislativ

„Dezvoltarea rapidă a domeniilor tehnologia informației și comunicații - condiție sine qua non a edificării societății informaționale - a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului și culturalului, dar și asupra vieții de zi cu zi a individului. Practic, în prezent, accesul facil la tehnologia informației și comunicațiilor reprezintă una dintre premisele bunei funcționări a societății moderne”[1].

„În actualul context, în țara noastră încă există dezbateri cu privire la categoriile de sisteme sau locațiile care pot fi încadrate în infrastructura critică, respectiv care sunt acele structuri vitale societății, care, prin discontinuitatea lor, conduc la imposibilitatea de exercitare a atribuțiilor. Inexistența unui limbaj unic între actorii din sfera public-privat, care să faciliteze și dialogul instituțional, determină incapacitatea de creare a unui cod unic de la care să fie inițiat dialogul cu privire la strategia de management al riscului necesară punerii în funcție a întregului flux acțional. O analiză a potențialului de risc al unei infrastructuri critice impune o abordare integrată a tuturor strategiilor, procedurilor și programelor privind prevenirea, pregătirea, răspunsul și procedurile de recuperare în caz de dezastre și situații de urgență”[2].

Situația de criză este definită ca fază în evoluția unei societăți marcată de mari dificultăți generate de apariția unui/unor incident(e)/eveniment(e) la nivel național/internațional sau de amenințări, riscuri și vulnerabilități la adresa valorilor, intereselor și necesităților actorilor

[1] Hotărârea nr. 271/2013 pentru aprobarea *Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*.

[2] Revista Intelligence, *Protecția infrastructurilor critice. Studiu de caz: sectorul energetic, https://intelligence.sri.ro/protectia-infrastructurilor-critice-studiu-de-caz-sectorul-energetic/*, 2010, accesat la 04.06.2019.

implicați, care impun soluții urgente și eficiente de înlăturare a cauzelor și revenirea imediată la starea de normalitate. Consecințele unei situații de criză se pot manifesta prin: întreruperea/afectarea activității politice, sociale, economice sau de altă natură; punerea în pericol a cetățenilor sau a factorilor materiali; expunerea la riscuri majore de securitate a populației sau a unei colectivități; propagarea din plan regional în cel național a efectelor crizei cu afectarea concretă a securității, obiectivelor și intereselor strategice ale statului.

„**Sistemul Național de Securitate** este definit ca ansamblul organelor legislative, executive și judecătorești, al instituțiilor, organismelor economice, organizațiilor neguvernamentale și cetățenilor care, potrivit legii ori liber consimțit, își asumă obligații sau manifestă preocupări și inițiative civice în legătură cu realizarea, protejarea ori afirmarea valorilor și intereselor de securitate. În concordanță cu îndeplinirea atribuțiilor acestora, instituțiile pot adopta o serie de măsuri proactive și/sau reactive, care pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor”[3].

„Prin infrastructuri critice putem înțelege dispozitivele, rețelele, serviciile, sistemele de bunuri materiale (energetice, de transport, de comunicații și de tehnologia informației, de furnizare a utilităților) de interes strategic și/sau de utilitate publică, a căror distrugere, aducere în stare de nefuncționare, degradare ori perturbare ar avea efecte negative majore, la nivel național sau regional, asupra stării de sănătate și siguranței cetățenilor, mediului, funcționării economiei și activității instituțiilor statului”[4].

În conformitate cu ***Strategia Națională de Apărare a Țării pentru perioada 2015 - 2019***[5], „două dintre obiectivele naționale de securitate le reprezintă asigurarea eficienței sistemelor naționale de prevenire și gestionare a situațiilor de criză, interne și externe, militare sau de natură civilă și consolidarea securității și protecției infrastructurilor critice - energetice, de transport și cibernetice” [...]. Fiecare dintre instituțiile cu atribuții în domeniul securității naționale, conform legii de funcționare, are implicații directe și/sau indirecte în prevenirea și gestionarea situațiilor de criză, indiferent de natura acestora, dezastre naturale, calamități, conflicte armate, etc. astfel:

1. „**Ministerul Apărării Naționale** este organul de specialitate al administrației publice centrale, care conduce și desfășoară, potrivit legii, activitățile în domeniul apărării țării [6], cu atribuții specifice: mobilizarea armatei, constituirea forțelor de rezervă, rechiziționarea de bunuri și chemarea persoanelor fizice la prestări de serviciu în interes public”[7].

2. „**Ministerul Afacerilor Interne** este organul de specialitate al administrației publice centrale, care își îndeplinește atribuțiile în domeniul protecției infrastructurilor critice prin intermediul *Centrului național de coordonare a protecției infrastructurilor critice*[8], ca punct național de contact în relația cu alte state membre ale Uniunii Europene, Comisia Europeană, Organizația Tratatului Atlanticului de Nord și alte organizații și organisme internaționale, precum și managementul rețelei de alertă privind infrastructurile critice - CIWIN la nivel național. Protecția infrastructurilor critice (PIC) este o activitate care are drept scop asigurarea funcționalității, a continuității și a integrității infrastructurilor critice naționale și europene (ICN

---

[3] *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, nr. DSN1/1682 din 07.12.2015.
[4] Idem.
[5] *https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf*, accesat la 04.06.2019.
[6] Legea nr. 346/2006 privind organizarea și funcționarea Ministerului Apărării.
[7] *https://www.mapn.ro/legislatie/atributii/, accesat la 04.06.2019*, accesat la 04.06.2019.
[8] *http://ccpic.mai.gov.ro/desprenoi.html, accesat la 04.06.2019*, accesat la 04.06.2019.

și ICE) pentru a descuraja, diminua și neutraliza o amenințare, un risc sau un punct vulnerabil. Într-o enumerare neexhaustivă, aceasta cuprinde activitățile desfășurate succesiv privind identificarea infrastructurilor critice naționale și europene, desemnarea acestora, evaluarea și analiza riscurilor, asigurarea protecției informațiilor clasificate din domeniul PIC, realizarea planurilor de securitate a operatorilor de infrastructură critică (PSO), stabilirea ofițerilor de legătură și a modului de realizare a comunicațiilor, precum și exerciții, rapoarte, reevaluări și actualizări ale documentelor elaborate pe linia protecției infrastructurilor critice"[9].

3. „**Autoritatea Națională pentru Administrare și Reglementare în Comunicații** (ANCOM) este o autoritate publică autonomă cu personalitate juridică, sub control parlamentar, având rol de punere în aplicare a politicii naționale în domeniul comunicațiilor electronice, comunicațiilor audiovizuale și al serviciilor poștale, administrează și gestionează resursele limitate din domeniul comunicațiilor electronice, incluzând, dar fără a se limita la acestea, spectrul de frecvențe radio, resursele de numerotație și alte resurse tehnice asociate, și monitorizează benzile de frecvențe radio cu utilizare neguvernamentală. ANCOM controlează îndeplinirea cerințelor esențiale privind compatibilitatea electromagnetică, a obligațiilor privind utilizarea eficientă a spectrului de frecvențe radio cu utilizare neguvernamentală, controlează îndeplinirea obligațiilor privind utilizarea resurselor de numerotație și a resurselor tehnice asociate, realizează controlul pieței echipamentelor radio și echipamentelor terminale de telecomunicații"[10].

4. „**Ministerul Comunicațiilor și Societății Informaționale** se organizează și funcționează ca organ de specialitate al administrației publice centrale, cu personalitate juridică, în subordinea Guvernului, având rolul de a realiza politica Guvernului în domeniul comunicațiilor electronice, serviciilor poștale, securității cibernetice, tehnologiei informației, societății informaționale și a cadrului național de interoperabilitate[11.] În context, în ultimii ani, România a înregistrat un parcurs pozitiv în sensul asigurării protecției infrastructurilor critice, reunind eforturi din diferite sectoare de activitate, dintre care se impune a fi menționate: înființarea, în anul 2009, a Centrului de Expertiză în Domeniul Securității Informatice (CERT RO) și adoptarea, în anul 2010, a cadrului legislativ aferent protecției infrastructurilor critice. Sub autoritatea Ministerului Comunicațiilor și Societății Informaționale, în cadrul Institutului Național de Cercetare -Dezvoltare în Informatică, s-a înființat Centrul de Expertiză în Domeniul Securității Informatice (CERT RO), un centru de excelență în domeniul securității informațiilor, echipamentelor, rețelelor și sistemelor informatice, care reunește experți din mai multe instituții, pentru asigurarea securității spațiului virtual din România. Prin crearea acestui centru, s-a urmărit crearea unei infrastructuri tehnice, a unui cadru informațional și operațional necesar pentru cooperarea în caz de incident survenit în rețelele IT&C, cu accent pe infrastructura critică, precum și eliminarea sincopelor din procesul educațional al societății, prin elaborarea unui set de informații accesibile și capabile să acopere breșele din educație, în special pe cele care privesc accesarea spațiului virtual"[12].

5. „**Serviciul de Telecomunicații Speciale** coordonează activitățile în domeniul telecomunicațiilor speciale pentru autoritățile publice din România și alți utilizatori prevăzuți de lege[13]. Serviciul de Telecomunicații Speciale este autoritatea publică responsabilă pentru

---

[9] *http://ccpic.mai.gov.ro/index.html#, accesat la 04.06.2019,* accesat la 04.06.2019.

[10] *Ordonanța de urgență a Guvernului nr. 22/2009* privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare.

[11] *https://www.comunicatii.gov.ro/*, accesat la 04.06.2019.

[12] Revista Intelligence, *Protecția infrastructurilor critice în contextul parteneriatului public-privat,* https://intelligence.sri.ro/protectia-infrastructurilor-critice-contextul-parteneriatului-public-privat/, 2011, accesat la 04.06.2019.

[13] *https://www.sts.ro/ro/atributii*, accesat la 04.06.2019.

infrastructurile critice aflate în administrare, aferente sectoarelor „Tehnologia Informației și Comunicații" și „Securitate națională", conform legislației în vigoare. În categoria infrastructurilor critice operate de STS intră: infrastructura de comunicații și tehnologia informației, centre de date, sisteme și servicii informatice, serviciul 112, servicii oferite în rețele speciale și de cooperare"[14].

6. „**Serviciul Român de Informații**, în calitatea sa de autoritate națională în domeniul cyberintelligence, în urma desemnării de către CSAT, prin Centrul Național Cyberint, pledează și acționează pentru cunoașterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor la adresa securității cibernetice a României, inclusiv la adresa securității și protecției infrastructurilor critice. Principala misiune este corelarea sistemelor tehnice de apărare cu capacitățile informative pentru a identifica și furniza beneficiarilor legali informațiile necesare prevenirii, limitării și/sau stopării consecințelor unei agresiuni asupra sistemelor de tehnologia informației și comunicații (TIC) care reprezintă infrastructuri critice[15]. Din perspectiva atribuțiilor legale de identificare, analiză, prognoză și contracarare a amenințărilor vizând securitatea națională, Serviciul Român de Informații aduce un plus de cunoaștere, consolidându-și poziția de actor principal în prevenirea și combaterea terorismului, a amenințărilor cibernetice și coordonator al activităților de protecție a informațiilor clasificate din zona infrastructurilor critice. SRI fundamentează, în plan intern, dar și extern, prin intermediul parteneriatelor externe, deciziile autorităților responsabile pentru asigurarea protecției acestora, prin integrarea în analize multisursă a informațiilor secrete (HUMINT), a surselor deschise (OSINT) și tehnice (SIGINT), identificând potențialul de risc, vulnerabilități și amenințări din zona securității economice, cibernetice ș.a."[16].

„Situația actuală și cadrul normativ existent în România au fost impuse de evoluția amenințărilor la nivel global, corelată cu statutul politico-militar și economic actual al României în cadrul Alianței Nord-Atlantice și Uniunii Europene, determinând translatarea potențialilor factori de risc și asupra infrastructurilor naționale asimilabile celor critice, mai ales, în contextul rolului jucat de țara noastră în asigurarea climatului de stabilitate și securitate regională, cu accent în zona bazinului Mării Negre. Astfel, perspectiva manifestării unor potențiale amenințări a determinat abordări strategice, instituționale și funcționale într-un sistem integrat al problematicii protecției infrastructurilor critice naționale. Având în vedere dependența mare față de serviciile oferite de infrastructurile critice, societatea a devenit foarte vulnerabilă. Această vulnerabilitate a crescut nu doar ca urmare a riscurilor și amenințărilor externe, ci și din cauza **interdependențelor dintre diferitele infrastructuri din interiorul sistemelor relevante,** context în care perturbațiile/întreruperile pot determina pagube imense pentru economia națională. În materia protecției infrastructurilor critice, efortul statului și al societății trebuie direcționat, în principal, pe două mari categorii de amenințări: cea teroristă și cea generată de dezastre/calamități naturale, ce au un impact tot mai mare asupra infrastructurii considerate critică. Primele etape în vederea configurării unui cadru legal normativ coerent destinat reglementării protecției infrastructurii critice în România au fost parcurse odată cu adoptarea Ordonanței de urgență a Guvernului nr. 98/2010, aprobată cu modificări prin Legea nr. 18/2011, și a Hotărârii Guvernului nr. 1.110/2010. În baza acestora a fost creat Grupul de lucru interinstituțional pentru protecția infrastructurilor critice, organism ce asigură cadrul de cooperare interinstituțională necesar elaborării proiectelor naționale indispensabile dezvoltării

[14] *https://www.sts.ro/ro/infrastructuri-critice*, accesat la 04.06.2019.
[15] *https://www.sri.ro/cyberint*, accesat la 04.06.2019.
[16]Revista Intelligence, *Protecția infrastructurilor critice în contextul parteneriatului public-privat,* 2011, *https://intelligence.sri.ro/protectia-infrastructurilor-critice-contextul-parteneriatului-public-privat/*, accesat la 04.06.2019.

unei abordări integrate și fundamentate a protecției infrastructurilor critice"[17]. „Grupul de lucru interinstituțional pentru protecția infrastructurilor critice este format din experți/specialiști desemnați de autoritățile publice responsabile și anume: Ministerul Economiei, Comerțului și Mediului de Afaceri, Ministerul Comunicațiilor și Societății Informaționale, Ministerul Educației, Cercetării, Tineretului și Sportului, Ministerul Sănătății, Ministerul Mediului și Pădurilor, Serviciul de Telecomunicații Speciale, Serviciul de Informații Externe, Serviciul Român de Informații, Ministerul Agriculturii și Dezvoltării Rurale, Autoritatea Națională Sanitară Veterinară și pentru Siguranța Alimentelor, Ministerul Administrației și Internelor, Ministerul Apărării Naționale, Ministerul Transporturilor și Infrastructurii, Agenția Spațială Română, Ministerul Dezvoltării Regionale și Turismului"[18].

*II. Riscuri emergente curente și viitoare asupra infrastructurilor de comunicații critice**

Perioada actuală cunoaște o dinamică ascendentă de dezvoltare a sistemelor de comunicații datorată, pe de o parte, evoluției din sectorul tehnologiei informației (hardware și software), iar pe de altă parte, migrării societății umane de la era informațională către era inteligenței artificiale. Sistemele de comunicații au reprezentat și vor continua să reprezinte, suportul principal sau temelia de bază care asigură infrastructura necesară funcționării rețelelor de date și dezvoltării, la nivel global, a oricărui proces sau sistem informațional. **Subliniind, putem aprecia că, oriunde există informație, aflată în dinamică sau în procesare, vom depinde biunivoc de un sistem de comunicații sau de o infrastructură de rețea.**

Suplimentar, evoluția și dezvoltarea agresivă a societății umane a generat concomitent o globalizare a dependenței statelor de tehnologie și implicit, a creat o relație de tip determinist față de infrastructura de comunicații deținută de către fiecare stat. Începând cu anul 2001, odată cu atentatele teroriste din SUA, dar și ulterior în Europa, simultan cu agresiunea cibernetică asupra infrastructurii bancare și guvernamentale a Estoniei din anul 2007, s-a dovedit că, cu cât nivelul de dezvoltare și digitalizare al unui stat este mai ridicat, cu atât dependența față de sistemele de comunicații și față de infrastructurile de rețele naționale este mai mare.

Putem identifica astfel, o primă relație de interdependență între nivelul de dezvoltare al statelor – complexitatea infrastructurilor critice deținute și dependența de sistemele de comunicații naționale aflate în exploatare. Sub perspectiva evoluției dependenței societății informaționale europene actuale de sistemele de comunicații, atât în zona statelor dezvoltate vestice, dar și a statelor aflate în curs de dezvoltare din zona estică, printre care și România, putem identifica două evoluții majore.

Prima dintre ele se referă la tendința de dispariție a sistemelor de comunicații "clasice" (așa cum sunt ele cunoscute astăzi) și migrarea acestora către rețele integrate în tehnologie IP, care oferă servicii unificate atât din sfera serviciilor de comunicații (transmisii de voce, date și multimedia), cât și din sfera specifică mediului IT. Explicația acestei tendințe se bazează pe faptul că dezvoltarea sistemelor de aplicații este una accelerată exponențial de automatizările din societate, dar și de sistemele de aplicații mobile, iar

[17] MONITORUL OFICIAL AL ROMÂNIEI, PARTEA I, Nr. 555/4.VIII.2011, *Strategia națională privind protecția infrastructurilor critice.*

[18] Hotărârea nr. 1.110 din 3 noiembrie 2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice.

* Cercetarea științifică din prezentul subcapitol a fost diseminată si prezentată, cu acceptul Academiei Oamenilor de știință din România, în cadrul Conferinței Nationale de toamnă a AOSR , 20-21 septembrie 2019, Brașov, fiind publicat in volumul II, comunicări integrale, pag,651-66, editura Expert , București, 2019.

comunicațiile privite ca serviciu, au devenit aplicații informatice hibride ce tranzitează rețele de date TCP/IP, prin intermediul tehnologiilor de tip VoIP sau EoIP.

Ce de-a doua tendință, manifestată în special în zona statelor puternic dezvoltate tehnologic, este aceea de virtualizare a rețelelor de comunicații, urmare a capabilităților și facilităților oferite de tehnologiile virtual computing și virtual networking, care permit prin intermediul instrumentelor și aplicațiilor software, generarea unor noi rețele de comunicații virtuale (tehnologii VPN sau VLAN), în interiorul aceleiași infrastructuri fizice.

Cele două tendințe existente, la nivelul sistemelor de comunicații și tehnologiei informației au un impact semnificativ asupra nivelul de asigurare al serviciilor tradus în fapt, prin creșterea complexității și diversificarea tipurilor de servicii de comunicații, dar și prin creșterea calității acestora (QoS Quality of Services) urmare a unor noi capabilități reziliente facilitate de tehnologia avansată. Cu toate aceste, pe lângă avantajele unui QoS ridicat și a unei diversități de servicii, asupra sistemelor de comunicații naționale migrează o serie de riscuri emergente, generate de complexitatea ascendentă și de interdependențele tehnologice inter-sisteme, care necesită un management permanent preventiv și o abordare holistică la nivelul statelor, regional, sau chiar global.

Dependența societății de infrastructurile critice exploatate, de tehnologia informației (aplicații, inteligență artificială, automatizări, software) și a tuturor acestora, de rețelele de comunicații operaționale utilizate ca suport, determină o propagare a riscurilor în lanț, în ambele sensuri ale ecuației.

Pentru a exemplifica, putem analiza succint situația apărută în SUA urmare a atentatelor teroriste din septembrie 2001. Atacurile teroriste din 11 septembrie 2001 asupra turnurilor gemene World Trade Center au creat pe lângă efectele directe și pierderile de vieți umane incomensurabile și o imagine edificatoare asupra vulnerabilităților tehnologice ale societății americane, care a cunoscut un nivel ridicat de maturitate digitală. Astfel, odată cu prăbușirea turnurilor gemene WTC1 și WTC 2, întreaga infrastructură critică de alimentare cu apă din zona Lower Manhattan, New York City a fost afectată semnificativ, producând inundarea centrelor și nodurilor de comunicații magistrale zonale, dispuse subteran.

De asemenea, prin efecte directe, prăbușirea turnurilor gemene a generat scoaterea din funcțiune a rețelelor de telefonie și a infrastructurii de cablare a zonei, considerată ca fiind unul dintre principalele noduri de comunicații regionale. ”Efectele produse au generat distrugerea a 300.000 de linii de acces pentru servicii de voce, 4.5 milioane de circuite de date și a zece turnuri pentru sisteme celulare active, afectând în mod direct 14.000 de companii și 20.000 de clienți rezidențiali. Din cauza acestor întreruperi, multe companii, inclusiv Bursa de Valori din New York, nu au avut asigurate servicii de comunicații pentru câteva zile înregistrând pierderi financiare uriașe ce nu au putut fi evaluate complet de societatea americană.[19]”

Putem aprecia, pe baza evoluției societății și al nivelului de extindere a infrastructurilor critice, coroborat cu cercetările din alte state, faptul că la nivel național patru infrastructuri sunt vitale la apariția unei situații de urgență, determinată de un dezastru natural, de o stare de calamitate extinsă local, regional sau național sau de o situație provocată de factorul uman.

Cele patru infrastructuri vitale funcționării societății pentru asigurarea vieții sunt: **infrastructura energetică critică, infrastructura de asigurare a apei, infrastructura de comunicații națională și infrastructura de transport**. Infrastructura energetică este critică pentru asigurarea în situații de urgență atât a apei, cât și a serviciilor esențiale vieții umane, dar și a capacităților de transport pentru intervenția autorităților statului. La nivel global, dar și

[19] Argenti, Paul A., *Criza comunicațiilor. Lecții învățate din 11 septembrie,* Harvard Business Review. Decembrie 2002, disponibil la *https://hbr.org/2002/12/crisis-communication-lessons-from-911*, accesat la 14.06.2019.

național, infrastructurile energetice critice, au beneficiat în ultima decadă de un amplu proces de automatizare[20] bazat pe sisteme software automate de control și pe rețele de comunicații operaționale (radio, mobile GSM și de bandă largă prin infrastructura de fibră optică), atât în zona de dispecerat, cât și în zona de producție și distribuției, **devenind dependente tehnic de sistemele de comunicații operaționale sau de infrastructura web-based, de acces la rețeaua internet.**

Astfel, putem observa că **infrastructura de comunicații reprezintă elementul cheie** de care depinde funcționarea societății în situații de criză, dar în același timp determină funcționarea celorlalte 3 (trei) infrastructuri vitale: energie, apă, transport. Indisponibilizarea acestei infrastructuri sau diminuarea nivelului de operativitate, va determina o reacție în lanț asupra funcționalității tuturor celorlalte. Așadar, relația de tip determinist, generată inițial de extinderea tehnologiei informației, în toate mediile sociale și subliniată în prima parte a cercetării noastre, este impusă și de nivelul existent de interconectare și automatizare al infrastructurilor critice.

Urmare a elementelor analizate anterior, dar și a relației de dependență funcțională identificată între **infrastructura de comunicații critică și celelalte infrastructurilor critice naționale,** apare în mod firesc întrebarea, ***"Care sunt riscurile la nivelul sistemelor și infrastructurii de comunicații critice naționale?".***

Nivelul de extindere al infrastructurii de comunicații naționale de bandă largă în România este unul dintre cele mai ridicate din Europa la nivelul interconectărilor și extinderii conexiunilor în zona guvernamentală și al populației, aspect certificat prin raportul de țară al Comisiei Europene privind indicele DISA[21] în anul 2019. ***"În Romania 45% din locuințele casnice sunt abonate la servicii de bandă largă de foarte mare viteză, România clasându-se astfel pe locul al treilea în UE"[22].*** Cu toate acestea, dimensiunea gradului de extindere al conectivității naționale la servicii de bandă largă utilizând rețele fixe, situează România pe poziția 22 în UE, urmare a decalajului de dezvoltare a rețelelor de comunicații fixe dintre zonele urbane și zonele rurale, iar indicele general de digitalizare a societății plasează statul român pe poziția 27 din 28 de state. Putem astfel sublinia, o dependență crescută a societății la nivel național de rețelele și sistemele de comunicații mobile (tehnologie 3G si 4G) și de serviciile internet asigurate prin infrastructura GSM, concomitent cu o subdezvoltare a infrastructurii de comunicații fixe de bandă largă, mult mai stabile, în special în mediul rural.

[20] corporația ENEL, prezentă și pe piața din Romania și-a propus realizare unei investiții în digitalizarea infrastructurii de producție și transport de energie de aproximativ 5,4 miliarde de euro, pentru perioada 2019-2021, la nivelul global, pentru întreaga infrastructură a grupului, conform planului strategic, 2019-2021., disponibil la adresa, *https://www.enel.com/content/dam/enel-com/investors/presentations/enel-capital-markets-day-2018.pdf* , accesat la 14.06.2019.

[21] *http://ec.europa.eu/information_society/newsroom/image/document/2018-20/ro-desi_2018-country-profile_ eng_199 394CB-B93B-4B85-C789C5D6A54B83FC_52230.pdf* , accesat la 14.06.2019.

[22] Indicele Economiei și societății digitale (DESI) România, Raport de Țară 2019, p.3.

	România				UE
	DESI 2017	DESI 2018	DESI 2019		DESI 2019
	valoare	valoare	valoare	loc	valoare
1a1 Acoperirea serviciilor fixe de bandă largă % gospodării	**89%** 2016	**88%** 2017	**87%** 2018	***26***	**97%** 2018
1a2 Utilizarea serviciilor fixe de bandă largă % gospodării	**63%** 2016	**67%** 2017	**66%** 2018	***22***	**77%** 2018
1b1 Acoperire 4G² % gospodării (media operatorilor)	**45%** 2016	**72%** 2017	**77%** 2018	***28***	**94%** 2018
1b2 Utilizarea serviciilor mobile de bandă largă Abonamente la 100 de persoane	**71** 2016	**82** 2017	**85** 2018	***20***	**96** 2018
1b3 Gradul de pregătire pentru utilizarea rețelelor 5G Spectrul atribuit exprimat în % din totalul spectrului 5G armonizat	**NA**	**NA**	**0%** 2018	***13***	**14%** 2018
1c1 Acoperirea serviciilor fixe de bandă largă de mare viteză (NGA) % gospodării	**72%** 2016	**74%** 2017	**76%** 2018	***21***	**83%** 2018
1c2 Utilizarea serviciilor de bandă largă de mare viteză % gospodării	**44%** 2016	**53%** 2017	**55%** 2018	***9***	**41%** 2018
1d1 Acoperirea serviciilor de bandă largă de foarte mare viteză % gospodării	**NA**	**73%** 2017	**75%** 2018	***14***	**60%** 2018
1d2 Utilizarea serviciilor de bandă largă de foarte mare viteză % gospodării	**32%** 2016	**44%** 2017	**45%** 2018	***3***	**20%** 2017

Figura nr. 1– Statistica Comisiei Europene privind serviciile de comunicații in Romania, raport de țară 2019

Analizând gradul de extindere al infrastructurii de comunicații naționale, interdependențele existente, tendințele de digitalizare a societății și de automatizare a infrastructurilor critice derivate din Strategia Națională privind Agenda Digitală pentru România – 2020[23], evaluăm că principalele riscuri identificate asupra infrastructurii critice de comunicații naționale ce pot determina afectarea funcționării societății sunt:

1. Riscul de indisponibilizare fizică a infrastructuri critice de comunicații, sistemelor și serviciilor, urmarea a efectelor dezastrelor și calamităților naturale sau provocate de om, locale, regionale sau la nivel național.

Deși sub aspectul incidenței manifestării acestui risc, în ultimii 20 de ani, în România nu au fost identificate indisponibilizări pe scară regională sau națională ale sistemelor de comunicații la nivelul principalilor operatori publici de telefonie fixă și GSM (Orange România SA, Telekom Romania Mobile Communications, Vodafone România, Romanian Cable Sistem - RCS&RDS) sau asupra sistemelor guvernamentale, putem aprecia că probabilitatea apariției unui astfel de risc, nu este una ridicată. Cu toate acestea, în situația manifestării riscului, funcție de tipul de calamitate și gradul de extindere geografică, impactul unui astfel de risc asupra funcționării sistemului și rețelelor naționale de comunicații ar putea fi major, influențând semnificativ funcționarea normală a societății.

Sub raport tehnic, indisponibilizarea, într-o anumită zonă geografică, dens populată, a unui număr suficient de mare de celule GMS (stații de bază, aparținând mai multor operatori de telefonie publică), ar determina pe cale de consecință, pe lângă scăderea nivelului de acoperire cu servicii de comunicații de voce și date în zona afectată și **o congestie a traficului**, către celulele perimetrale zonei afectate, fapt ce va genera o reacție în lanț asupra disponibilității serviciilor de rețea.

Dacă efectele directe ale unui dezastru/calamități naturale sau provocate sunt de natură să determine scoaterea din funcțiune a unor stații de bază GSM sau turnuri nodale de comunicații, sunt situații precum cea din provincia Alberta, Canada în anul 2013, în care efectele indirecte au determinat riscuri semnificativ mai mari.

[23] *http://gov.ro/ro/guvernul/sedinte-guvern/strategia-nationala-privind-agenda-digitala-pentru-romania-2020*, accesat la 14.06.2019.

În data de 19 iunie 2013, întreaga infrastructură critică de comunicații a orașului canadian Calgary deținută și exploatată de companiile NMAX și TELUS **a fost scoasă din funcțiune de afectarea gravă a capacităților de alimentare cu energie electrică și de pierderea capacităților de alimentare redundantă.** Efectele pentru aproximativ 1,5 milioane de locuitori au fost majore, orașul Calgary și regiunea Alberta fiind lipsite de posibilitatea asigurării serviciilor de comunicații critice pentru autorități, dar și pentru sistemul medical de urgență. Pierderile financiare, ulterioare pentru ”refacerea infrastructurii si capabilităților de comunicații, au fost enorme fiind estimate la aproximativ 7 milioane de dolari pentru compania Telus”[24].

Apariția unei calamitați extinse, aptă să afecteze fizic infrastructura publică de comunicații dintr-o anumită regiune (stații de bază, stații de management regional, infrastructură de cablare pentru servicii și management) va determina cel mai probabil și afectarea infrastructurii și rețelei de distribuție energetică națională din acea regiune.

Marea majoritate a stațiilor de bază de telefonie publică care asigură majoritar comunicațiile de voce și date, dar și serviciile de urgență civilă (112[25], Ro-Alert[26]) precum și centrele regionale de management aparținând furnizorilor publici de servicii de comunicații sunt dependente direct și major, de infrastructura energetică națională, iar nivelul de redundanță al alimentării electrice este unul de natură să mențină capacitatea operațională în mod limitat pentru perioade de aproximativ câteva ore.

Concluzionând, riscurile indirecte generate de lipsa capacității energetice necesare va determina scoaterea din funcțiune sau diminuarea nivelului de acoperire cu servicii de comunicații a regiunii/zonelor afectate, concomitent cu apariția unor perioade mari necesare pentru restaurarea serviciilor în zonele compromise.

Amplificarea efectelor acestui tip de risc este cauzată și de dependența la nivel național a instituțiilor guvernamentale dar și civile, de serviciile de comunicații publice, oferite de operatorii naționali, începând cu entitățile și structurile locale: primării, centre de prim ajutor, centre ISU, spitale, structuri de ordine publică, etc.

2. Riscuri cibernetice generate de amenințări directe sau indirecte asupra infrastructurii critice de comunicații - atacul cibernetic definit ca ***„acea acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică”***[27], constituie principalul element de risc la adresa infrastructurii critice de comunicații la nivel național. Dacă acum aproximativ 15 ani, amenințările cibernetice asupra infrastructurii și sistemelor de comunicații erau considerate ca fiind ”avangardiste”, fiind conștientizate cel mult la nivelul aplicațiilor și serviciilor web, la momentul actual, principala amenințare asupra funcționării și stabilității infrastructurii critice de comunicații și rețelelor de comunicații magistrale o reprezintă acțiunile cibernetice directe și indirecte. Executarea unui atac cibernetic pentru exfiltrarea de date și informații a devenit astăzi mult mai ineficientă comparativ cu

[24] Ramgopal Rajan, *Reducing coordination risks around communication infrastructure protection during disasters:an alberta floods case study,* Universitatea Cambridge, 2015, p. 7.

[25] Sistemul 112 este un sistem operativ de telecomunicații, proiectat să notifice, recepționeze, proceseze și să transmită apelurile de urgență către serviciile responsabile, într-un mod centralizat și unitar, cu ajutorul funcțiilor integrate, disponibil la *https://www.sts.ro/ro/112-serviciul-de-urgenta*, accesat la data de 14.06.2016;

[26] ”Sistemul RO-ALERT permite difuzarea de mesaje de tip Cell Broadcast pentru avertizarea și alarmarea populației în situații de urgență, conform prevederilor legale. Tehnologia Cell Broadcast, pe care se bazează Sistemul RO-ALERT, permite ca antenele de comunicații mobile din zona selectată să difuzeze mesajul de avertizare tuturor telefoanelor mobile care funcționează în aria de acoperire a acestora”, disponibil la *https://roalert.ro/despre-ro-alert/*, accesat la data de 14.06.2019.

[27] Strategia de securitate cibernetică a României, 2013.p 7.

indisponibilizarea serviciilor oferite prin intermediul unei infrastructuri critice naționale care va determina efecte în cascadă asupra stabilității societății.

De asemenea, instrumentele cibernetice necesare indisponibilizării prin atacuri directe a unei întregi infrastructuri de comunicații au fost perfecționate și au devenit mai puțin costisitoare odată cu dezvoltarea, experimentarea și testarea cu succes, a atacurilor cibernetice de tip „***Denial-of-Service*” (DOS) și „*Distributed Denial-of-Service*” (DDOS)**, în conflictele militare și disputele interstatale din ultima decadă.

a. Atacurile de tip DOS și DOSS constituie principalul vector de risc cibernetic la adresa infrastructurii critice de comunicații. Evoluțiile din istoria contemporană, au demonstrat utilitatea și gradul de penetrabilitatea pe care îl induc vectorii de atac de tip DOS si DDOS, astfel:

- în perioada aprilie-mai 2007, Estonia s-a confruntat cu primele atacuri cibernetice de tip DoS „*Denial-of-Service*” și DDoS „*Distributed Denial-of-Service*” asupra propriei infrastructuri critice de comunicații. ”*Atacul cibernetic, primul de acest gen îndreptat împotriva unei infrastructuri critice de comunicații a unui stat, a fost declanșat de către entități și structuri informatice* ***de pe teritoriul a 178 de state****, coordonate de către Federația Rusă, ca urmare a reprimării manifestațiilor stradale pro-ruse din capitala Tallinn. Existența, la nivelul societății, a unei infrastructuri informatice dezvoltate și dependența întregului sistem bancar și de comunicații al statului de mediul de rețea, a făcut ca Estonia să fie extrem de vulnerabilă la acest tip de atac, iar concretizarea vulnerabilității s-a tradus prin scoaterea din funcțiune a siteurilor guvernamentale, a autorităților publice, a infrastructurii informatice bancare și a sistemului public de urgență*”[28];

- în luna august 2008, pe baza tensiunilor ruso-georgiene referitoare la regiunea Osetia de sud, Federația Rusă ”*a lansat o serie de atacuri cibernetice concertate, neasumate de o identitatea reală, asupra mediului de rețea național georgian, care au avut rolul de a destabiliza spațiul cibernetic și a de a întrerupe sistemul național de comunicații, diminuând astfel capacitatea operațională a forțelor georgiene și resursele de administrare și răspuns la criză ale statului. Atacurile cibernetice au fost realizate pe modelul aplicat cu succes în Estonia, numai că, de această dată, au fost alese ruterele de graniță și serverele aparținând sistemului bancar georgian, companiilor de telefonie precum și site-ul președinției, guvernului, Ministerului Afacerilor Externe și Ministerului Apărării”*[29].

- **în anul 2013 odată cu escaladarea divergențelor din Ucraina,** acțiunile cibernetice și-au făcut simțită prezența în infrastructura critică de comunicații ucraineană. ”*În luna februarie 2014, concomitent cu invazia aeroporturilor Sevastopol și Simferopol din Peninsula CRIMEEA de către grupurile paramilitare pro-ruse, a fost declanșată o amplă operațiune de atacuri cibernetice combinate asupra serverelor companiei de telefonie Ukrtelecom care oferea servicii telefonice și de date la nivel național cu o arie ridicată de acoperire și care au avut drept rezultat, blocarea activității acestei și scoaterea din funcțiune a serviciilor. În perioada imediat următoare, legăturile guvernamentale și cele necesare de funcționare a sistemului social, asigurate între Peninsula Crimeea și restul teritoriului Ucrainean au fost blocate, concomitent cu atacarea site-urilor guvernamentale prin atacuri masive care au combinat tehnica DDoS cu soluții de malware și produse software de tip virus modificate”*[30]. În conformitate cu analizele de securitate publice realizate de **experții BAE Systems,**

[28] Iorga Benedictos, *Dimensiunea cibernetică a conflictelor militare contemporane*, Buletinul UNAp Carol I, volumul 2 2015, p.86.
[29] Idem 87.
[30] Idem 88.

”varianta modificată a codului malițios SNAKE a permis lansarea masivă a peste 22 de atacuri și a avut drept rezultat obținerea accesului distant, sustragerea de date și penetrarea infrastructurii cibernetice critice de comunicații a statului ucrainean.”[31]

Atacurile de tip DDOS, pot fi realizate la orice nivel din stiva ISO/OSI, dar pentru afectarea sistemelor de comunicații și rețelelor de date, sunt preferate atacurile de tip protocol si volumetrice desfășurate la nivelul 4 - transport și la nivel 3 - rețea. Acestea presupun utilizarea în totalitate a lărgimii de bandă din mediul de rețea IP, prin generarea artificială de volum mare de trafic, ilegitim, blocând astfel traficul legitim/util.

Un atac de tip DDoS executat asupra unei rețele de transmisii de date sau a unui sistem de comunicații este o acțiune cibernetică distructivă ce urmărește perturbarea traficului normal al unui server de control al infrastructurii de comunicații (server de management al serviciilor, de autentificare al utilizatorilor, de management al traficului, a unui router sau sistem de rutare etc.), prin copleșirea țintei sau a infrastructurii sale înconjurătoare, cu un trafic ilegitim, generat fie de către cererile unor calculatoare penetrate anterior (devenite boți) fie prin intermediul unei infrastructuri de rețea compromisă. Un atac DDoS, va genera blocarea traficului legitim de date la nivelul sistemului sau rețelei de comunicații automat și va dezafecta major serviciile de comunicații la nivelul utilizatorilor, indisponibilizând tehnic întreaga infrastructură critică/ funcție de viteza de atac, de numărul de vectori și de vulnerabilitățile rețelei de comunicații.

b. Atacuri combinate utilizând tehnologii malware avansate si capabilități avansate și persistente (APT) personalizate pentru sistemele de comunicații - Echipa de Cercetare și Analiză a companiei Kaspersky Lab a documentat și identificat în cadrul unui amplu proces de analiză cibernetică, prima platformă de hacking, dedicată exclusiv executării de atacuri cibernetice asupra rețelelor și infrastructurii de comunicații GSM, denumită REGIN[32], care facilitează prin instrumentele puse la dispoziție, penetrarea, monitorizarea și manipularea rețelelor GSM, concomitent cu executarea, în subsidiar, a activităților de spionaj cibernetic. Principalele ținte ale platformei REGIN au fost: operatori de telecomunicații, instituții guvernamentale și financiare din domeniul telecom și instituții de cercetare din domeniul telecomunicațiilor și sistemelor criptografice. Platforma REGIN a permis penetrarea infrastructurilor critice de comunicații din state precum Algeria, Afghanistan, Belgia, Brazilia, Fiji, Germania, Iran, India, Indonezia, Kiribati, Malaysia, Pakistan, Siria si Rusia. Sub raport tehnic, platforma de tip modular, a utilizat cu succes o metoda de comunicare complexă între rețelele GSM infectate și serverele de comandă și control, permițând controlul la distanță și transmiterea datelor obținute către o terță parte.

”Un modul REGIN putea monitoriza sistemele de control ale celulelor GSM, colectând date despre celulele GSM si infrastructura rețelei, iar ulterior putea penetra orice celulă GSM supusă documentării. Conform informațiilor logate pe sistemul de control al celulelor GSM obținute de experții Kaspersky în timpul investigației, atacatorii puteau accesa date care le permiteau să controleze celulele GSM din interiorul rețelei acelui operator de telecomunicații penetrat. Atacatorii au avut acces la datele despre apelurile procesate de o anumita celulă și au putut facilita redirecționarea apelurilor către alte celule, sau activarea unor celule vecine”[33]. Directorul Global Research and Analysis Team la Kaspersky Lab a afirmat, urmare a finalizării investigațiilor, faptul că ”*capacitatea de a accesa și monitoriza rețelele GSM este cel mai neobișnuit aspect al noilor operațiuni cibernetice. Rețelele de telefonie mobilă utilizează protocoale de comunicare învechite, care nu oferă securitate adecvată utilizatorului*

[31] The Snake Campaign, BAE Systems, 2014, *www.baesystems.com/ai/snakemalware*, accesat la 12.06.2019.
[32] *https://securelist.com/regin-nation-state-ownage-of-gsm-networks/67741/* , accesat la 14.06.2019.
[33] Analiza Kaspersky Lab, *https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03 /08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf* , accesat la 14.06.2019.

final. Deși rețelele GSM au mecanisme integrate care permit entităților precum organizațiile de aplicare a legii sa identifice suspecții, infractorii cibernetici se pot folosi de aceste mecanisme pentru a lansa diferite atacuri asupra utilizatorilor mobili."

c. Atacuri de tip ransomware asupra centrele de management și bazelor de date aparținând operatorilor și furnizorilor Telecom - Amenințările de tip ransomware (coduri de tip malware care realizează criptarea ilegală a datelor), deși au fost dezvoltate pentru obținerea de resurse financiare ilicite utilizând ca principală metodă șantajul, urmare a criptării ilegale a informației unei companii, folosind produse de criptare ilegitime, cu cheie unică, au fost reconvertite în ultimi doi ani, către utilizări de tip distructiv, asupra infrastructurilor critice, în special în zona bazelor de date și companiilor din domeniul energetic și telecom. În luna mai 2017, cea mai mare companie de telefonie mobilă din Federația Rusă, Megafone[34], a fost ținta unui atac de tip ransomware, prin folosirea malware-ul de tip Wanacry 2.0, fapt ce generat afectarea rețelei interne a companiei și stoparea activităților echipelor help-desk și suport tehnic din companie, urmare a afectării computerelor utilizate, în zona de management rețea.

În mod similar, în anul 2017 au fost afectate și companiile telecom și infrastructurile deținute, astfel: Telefonica, Spania, Portugal Telecom și Telenor Ungaria.[35]

Riscurile derivate din utilizare vectorilor de atac de tip ransomware asupra infrastructurii critice de comunicații sunt:

- indisponibilizarea accesului utilizatorilor la serviciile de comunicații, prin criptarea datelor de autentificare ale acestora;
- indisponibilizarea infrastructurii, pentru anumite perioade de timp, prin criptarea sistemelor de management de rețea;
- limitarea accesului parțial sau total, local sau regional la servicii de comunicații de voce și transmisii de date prin alterarea capabilităților de autentificare și identificare ale utilizatorilor;
- utilizarea infrastructurii penetrate pentru extinderea atacurilor sau lansarea unor atacuri noi către rețelele altor operatori și deținători de infrastructură de comunicații, la nivelul unui stat sau cel puțin la nivel regional;
- afectarea resurselor tehnice și financiare prin utilizarea ineficientă a resursei umane și prin producerea de prejudicii financiare și de imagine la nivelul providerilor de servicii de comunicații;
- afectare disponibilității serviciilor la nivelul instituțiilor guvernamentale din domeniul telecom, dar și la nivelul furnizorilor de serviciu de comunicații, prin penetrarea rețelelor interne de management și scoaterea acestora, fie și temporar din funcțiune.

d. Amenințări de tip web-based asupra sistemelor de management a serviciilor si asupra instrumentelor financiare aparținând provederilor de comunicații - Atacurile de tip web–based, sunt o succesiune de atacuri cibernetice, folosind diverse tehnologii, ce facilitează obținerea de acces neautorizat la resurse informatice din mediul online (internet) al unei companii, fără a avea astfel de drepturi. Aceste atacuri, aflate pe un trend ascendent, urmăresc exploatarea unor vulnerabilități ale sistemului de operare sau ale aplicațiilor aparținând serverelor web ale companiilor de comunicații și furnizorilor de servicii de internet și transmisii de date, prin intrarea în posesie a unor parole și nume de utilizator, prin compromiterea contului de administrare pe un server de e-mail, compromiterea unui server de Web, utilizând injecții Javascript, SQL sau tehnici de atac de tipul și "Man-In-The-Middle". Migrarea

[34] *https://www.rt.com/news/388153-thousands-ransomeware-attacks-worldwide/,* accesat la 14.06.2019.

[35] *https://www.tdworld.com/grid-security/utility-companies-among-those-impacted-ransomware-attack,* accesat la 14.06.2019.

serviciilor de comunicații către mediul smart IP și dezvoltarea nivelului de interactivitate a providerilor de servicii de comunicații și a deținătorilor de infrastructuri de comunicații cu utilizatorii finali, a determinat și creșterea nivelului de expunere în zona web folosind infrastructura internet.

Astfel, interesul pe zona de hacking a crescut la adresa serverelor web deținute de companiile telecom la nivel național, motivații fiind atât de faimă, cât și de posibilitatea penetrării ulterioare și a altor elemente de infrastructură critică. Nivelul de risc generat de aceste amenințări, nu este însă unul ridicat, în acest moment sub natura impactului la serviciile critice. Creșterea vitezei de acces la internet, migrarea către IoT și smart-mobile în viitorul imediat apropiat prin tehnologia 5G, va genera o extrapolare a riscului de atacuri de tip Web-based asupra bazelor de date deținute în spațiul web de către mari furnizori de servicii de comunicații, în special în sectorul public.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Figura nr. 2 – Analiză asupra amenințărilor cibernetice 2017 – 2018

Agenția europeană pentru securitatea rețelelor informatice **(ENISA)**[36], a evidențiat faptul că, în perioada 2017-2018 amenințările cibernetice la adresa infrastructurilor critice, în special la nivelul sistemelor de comunicații și rețelelor de transmisii de date de tip WAN, au cunoscut o dinamică ascendentă, iar amenințările de tip "DOD/DDOS", atacuri "web-based" și instrumentele cibernetice de tip "boot net" s-au intensificat, constituindu-se în principal vectorii de atac în mediul online european.

Implementarea tehnologiei 5G la nivel național, dar și european, prin facilitarea transmisiilor de date de bandă largă cu viteze de trafic cuprinse între de 10 Gbps si 50 Gbps (valoare de potențial), în benzile de frecvență de **28 GHz, 37 GHz și 39 GHz**, respectiv, acces partajat în banda de **37-37.6 GHz**, va genera creșterea ratei de succes pentru atacurile cibernetice care vor utiliza vectori de atac de tip DDOS concomitent cu extrapolarea riscurilor

[36] *http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape /enisathreat-landscape-2014*, accesat la 06.02.2019

cibernetice actuale, aspecte evaluate insuficient de către operatorii și furnizorii de servicii de comunicații la nivel național.

3. Riscul de incompatibilitate tehnică a sistemelor de comunicații naționale (publice și guvernamentale), generate de diferențele tehnologice de dezvoltare.

Obligația impusă prin efectul legii, de către Autoritatea Națională pentru Administrare și Reglementare în Comunicații către principalii furnizori de servicii de comunicații și deținători de infrastructură ”telecom”, de a acoperi cu servicii de voce zone locuite de cel puțin **98%** din populația României, prin intermediul rețelelor proprii de acces radio, până la data de 5 aprilie 2017, a determinat o extindere rapidă a infrastructurii operatorilor, de cele mai multe ori, utilizând **echipamente și tehnologii din generații diferite, cu un nivel de interoperabilitate insuficient testat.**

Chiar dacă nivelul de interoperabilitate este unul asumat de către operatori, dezvoltarea accelerată a pieței, concurența în asigurarea serviciilor și progresului tehnologic au impus utilizarea unor sisteme și echipamente fie de generație diferită, fie produse de mai mulți producători de tehnologie **(SUA, China, Europa).** La nivelul sistemelor de rutare, dar și a echipamentelor de tip switch și transport, utilizarea, la nivelul unei întregi infrastructuri de rețea a echipamentelor de aceeași generație aparținând aceluiași furnizor, este astăzi aproape imposibilă.

Principalele riscuri determinate fie de incompatibilitățile tehnice în sistemele de rețea (router, HUB, switch, concentratoare VPN, centrale VoIP, sisteme de comutație etc.) urmare a generațiilor tehnologice diferite, fie de personalizarea standardelor de comunicații de către diverși producători (CISCO, HUWEI, ZTE, ERICSSON etc.) sunt:

- afectarea scalabilității rețelelor, pe segmente de rețea sau la nivel global;
- discontinuitatea serviciilor pe segmente de rețea acolo unde sunt oferite servicii diferite precum telefonie PSTN, SDH sau/și telefonie, VOIP, GSM, în situația tranzitării mai multor infrastructuri de rețea și segmente de transport;
- pierderea continuității legăturilor și transportului de date între diverse segmente de rețea, sau între noduri de rețea de tip magistral;
- diminuarea QoS la nivelul utilizatorilor finali, aparținând diverșilor operatori, care au implementate tehnologii de diferite generații;
- probabilitatea apariției unor riscuri secundare de natură cibernetică, cu impact semnificativ, prin exploatarea agresivă și ilegală a vulnerabilităților echipamentelor de rețea, (comutare, rutare, și switch-ing), care au dovedit a avea breșe de securitate constructive sau erori software de tip ”zero days”;
- întreruperea periodică și repetată a serviciilor de voce și transmisiilor de date, la nivel regional sau la nivel de rețea/rețele, fără a exista o cauză precis determinantă sau cuantificabilă[37].

Migrarea, în viitorul apropiat, a infrastructurii de comunicații naționale la tehnologia 5G, va determina intensificarea și amplificarea riscurilor de compatibilitate tehnică la nivelul infrastructurii de comunicații critice naționale actuale, în mod semnificativ, prin menținerea în funcțiune și a sistemelor și infrastructurii de generația a II, precum sistemele de comutație analogică, ISDN, ATM, echipamentelor PABX/ PBX sau a sistemelor 2G/3G, aflate încă în exploatare.

[37] întreruperea serviciilor companiei Telekom in data de 5 martie 2018**,** conform comunicatului Telekom Romania, disponibil *la https://economie.hotnews.ro/stiri-telecom-22324224-probleme-tehnice-luni-reteaua-mobila-telekomromania-parte-dintre-clienti-pot-intampina-dificultati-accesarea-serviciilor-voce-date-mobile.htm*, accesat la data de 05.06.2019.