Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

Impactul atacurilor cibernetice asupra administrației publice

- lucrare de licență, specializarea Administrație Publică -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolventă

Brăilescu Alessandra-Elisa

București
2025

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).

2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Brăilescu Alessandra-Elisa

Data și semnătura: 22.12.2024

Cuprins

Abstract

În procesul de dezvoltare a administrației publice moderne, se observă cu ușurință direcția digitală spre care aceasta se îndreaptă. Fenomenul digitalizării instituțiilor publice se află în plină desfășurare, iar, odată cu progresul semnificativ, apar și noi pericole care pun la încercare siguranța datelor pe care acestea le posedă. Astfel, amenințările atacurilor cibernetice se intensifică. Luând în considerare cele menționate, această lucrare urmărește să ilustreze maniera în care atacurile cibernetice pot afecta funcționarea sistemului administrativ, dar și cum acestea impactează cetățenii, care reprezintă o componentă deosebit de importantă a structurii administrative. Pentru ca lucrarea să ofere o imagine de ansamblu complexă subiectului abordat, vor fi incluse informații esențiale colectate din texte de specialitate redactate de autori străini, cursuri ale profesorilor universitari și cercetări efectuate de pasionați ai domeniului, reușind prin această modalitate să se îmbine diferite perspective. Interviul, ca metodă de cercetare, va constitui fundamentul obiectivelor propuse și va contura armonios conglomeratul informațional înscris în acest document. Totodată, studiul de caz ales va fortifica ideea concluzivă a acestor consemnări. Mai precis aceea că, adesea, instituțiile integrante ale administrației publice nu sunt pregătite pentru eventualele atacuri cibernetice, iar acestea atrag după sine dereglări profunde, începând de la simple defecțiuni în procesul de funcționare al serviciilor publice, până la punerea sub mare risc a siguranței naționale. Important de precizat este faptul că expunerea de conținut din această teză își propune să contribuie la înțelegerea deplină a impactului atacurilor cibernetice asupra instituțiilor publice și de a furniza soluții de ameliorare a pericolelor eminente. O asemenea problematică nu trebuie tratată cu superficialitate. Trăim într-o contemporaneitate incertă și este imperios necesar să ne apărăm de orice primejdie, altmiteri, consecințele pot fi catastrofale. Dacă am particulariza conform tematicii lucrării, repercusiunile pot face referire la colapsul sistemului, revolte ale cetățenilor sau chiar un război cibernetic.

Cuvinte cheie: digitalizare, servicii publice, instituții publice, război cibernetic.

Introducere

Era digitalizării[1] se află într-o continuă expansiune, iar tehnologia informației și a comunicațiilor joacă un rol fundamental în procesele guvernamentale și în administrația publică, sistemele informatice[2] ale insituțiilor administrative devenind din ce în ce mai vulnerabile la atacuri cibernetice[3]. [1] Impactul acestor atacuri asupra funcționării administrației publice nu mai constituie doar o preocupare de ordin tehnologic, ci o problemă de securitate națională, economică și socială, având consecințe semnificative asupra eficienței guvernării și încrederii cetățenilor în instituțiile statului. [2]

În contextul digitalizării serviciilor publice, instituțiile administrației publice sunt din ce în ce mai dependente de structuri bazate pe IT[4], care, în mod inevitabil, devin ținte sigure pentru atacurile cibernetice, dacă aceste structuri nu sunt securizate în conformitate cu pericolele unor astfel de atacuri. De la furtul de date la perturbarea activităților administrative esențiale, atacurile cibernetice pot afecta grav operațiunile zilnice ale instituțiilor, generând pierderi din multiple puncte de vedere sau în diverse domenii. [3]

În afara elementelor tehnice care trebuie protejate, sunt necesare măsuri de apărare pentru cetățeni împotriva atacurilor cibernetice. Cetățenii reprezintă una dintre cele mai importante componente ale administrației publice, căci aceasta nu ar exista fără ei. În eventualitatea unui atac cibernetic, în funcție de magnitudinea acestuia, cetățenii își pot pierde încrederea în capacitatea guvernării de a-i apăra. Tocmai de aceea, se poate crea o destabilizare a statului, iar de la mici nemulțumiri se poate ajunge la dorința populației de a-i înlătura pe cei aflați la conducere. Populația nu trebuie

[1] Aceasta se referă la procesul de schimbare a informațiilor de la forma analogică la cea digitală. De asemenea, implică echiparea obiectelor analogice cu tehnologie informatică și de comunicații.
[2] Acestea cuprind elemente precum calculatoare, programe, rețele de calculatoare, utilizatori etc.
[3] Încercări de compromitere a securității sistemelor informatice, rețelelor și datelor.
[4] Prescurtare din englezescul ”information technology”. Tehnologia informației este tehnologia necesară pentru prelucrarea informației, în particular prin folosirea computerelor electronice la convertirea, procesarea și transmiterea informației.

ignorată în ceea ce privește pericolul atacurilor cibernetice deoarece și aceasta poate fi afectată puternic de un asemenea incident. [4, 5]

De aceea, prin această lucrare de cercetare se dorește înțelegerea pe deplin a modului în care atacurile cibernetice afectează funcționarea instituțiilor administrației publice și ce măsuri sunt adecvate pentru prevenirea și gestionarea acestora. Scopul documentului este acela de a analiza impactul atacurilor cibernetice asupra sistemului administrativ, incluzând atât măsurile de securitate cibernetică aplicabile administrației publice, cât și politicile publice ce pot fi implementate, precum și direcțiile pentru dezvoltarea de soluții eficiente pentru protejarea sistemelor IT guvernamentale.

Având în vedere cele înscrise anterior, cercetarea va contribui la o deschidere informațională asupra modului în care administrațiile publice pot răspunde provocărilor din această arie a tehnologiei și cum pot împiedica eventualele dezastre iscate de atacurile cibernetice prin implementarea de măsuri protecționiste capabile să asigure funcționarea continuă și sigură a serviciilor publice, cât și a cetățenilor.

Ipotezele de cercetare

- Atacurile cibernetice reduc semnificativ eficiența instituțiilor publice prin îngreunarea cursului activităților acestora și prin pierderea de date importante;
- Instituțiile cu un grad scăzut privind educația digitală în rândul angajaților sunt mai predispuse atacurilor cibernetice;
- Lipsa unor politici publice referitoare la securitatea cibernetică duce la o creștere exponențială a atacurilor cibernetice asupra instituțiilor publice;
- Atacurile cibernetice determină scăderea încrederii cetățenilor în instituțiile administrației publice și a serviciilor operate de acestea;
- Folosirea unor sisteme informatice depășite în instituțiile administrației publice sporesc pericolul atacurilor cibernetice.

Obiective

- Identificarea principalelor tipologii de atacuri cibernetice care lezează sistemul administrației publice;
- Evaluarea accesibilității cetățenilor la serviciile publice în urma alterării acestora din cauza agresiunilor cibernetice;
- Determinarea impactului produs de atacurile cibernetice asupra sistemului administrativ;
- Analizarea consecințelor operative și economice provocate de atacurile cibernetice în administrația publică.

Metodologia de cercetare

Metodologia de cercetare reprezintă „abordarea teoretică și filozofică a cercetării, care include alegerea metodelor și justificarea lor”. Aceasta constituie o pârghie ce contribuie la conturarea unui cadru clar, sistematizarea și interpretarea datelor expuse în lucrarea de cercetare. Din aceste considerente, corelate cu tematica lucrării, metodologia aleasă este una calitativă pentru a putea fi posibilă o analiză detaliată a fenomenului atacurilor cibernetice asupra sistemului administrativ. [6]

Instrumentul principal utilizat în cercetare este studiul de caz, o metodă calitativă care oferă perspective detaliate și explorează diverse nuanțe. Metoda studiului de caz are ca scop analiza în profunzime a unui fenomen, a unei organizații sau a unui eveniment, relevante pentru cercetarea efectuată. Ilustrativ pentru această lucrare este cazul Ucrainei din 2022 deoarece această serie incidente înglobează un nou început pentru digitalizare, în special pentru siguranța cibernetică a administrației publice. Iar fără acest incident, cel mai probabil, securitatea cibernetică ar fi devenit un domeniu care se dezvolta lent și atenția asupra sa ar fi fost una mult mai scăzută, față de cum

este în momentul de față. Bineînțeles, acestea sunt doar presupuneri și trebuie să analizăm contextul spațiului cibernetic, factorii declanșatori și motivele utilizării atacurilor cibernetice prin prisma acestui studiu de caz.

Capitolul 1. Fundamente teoretice și evoluția administrației publice.

Progresele din domeniul tehnologiei au condus la noi moduri în care societățile se administrează, introducând treptat rețelele informatice pentru a fluidiza acest proces administrativ, devenind elemente de infrastructură critică atât în domeniul public, cât și în mediul privat. Creșterea volumului de date în format digital și dependenței de serviciile online[5] au atras după sine amenințări cibernetice din ce în ce mai complexe. [7] În momentul prezent, atacurile cibernetice nu mai reprezintă doar acțiuni izolate cu scopul de a exploata vulnerabilități tehnice, ci pot fi organizate, pregătite în detaliu, avansate și au capacitatea de a provoca consecințe substanțiale asupra stabilității instituționale. [8]

Odată cu ajutorul oferit de tehnologie, trebuie să aruncăm o privire asupra faptului că răspândirea Internetului[6] a determinat și accesibilitatea mai ușoară la instrumentele de hacking[7], fenomen ce a favorizat dezvoltarea de piețe negre în mediul online, în cadrul cărora sunt vândute diverse, de la datele furate până la malware[8]. [8] Totodată, numărul de atacatori se extinde, având diferite nivele de compentență, iar cei ce sunt responsabili de protejarea infrastructurilor sunt constrânși să facă față noilor provocări, să devină din ce în ce mai pregătiți și să încercere să contracareze amenințările. [9]

Tocmai din aceste motive este imperios necesar să știm cu ce tipologii de atacuri cibernetice ne putem confrunta, cum au evoluat și să fim conștienți de vulnerabilitățile pe care le dețin sistemele informatice, aspecte care vor fi parcurse în continuarea acestui capitol.

1.1. Aspecte introductive ale administrației publice.

Administrația publică este o componentă fundamentală a statului modern, reprezentând sistemul prin care se asigură aplicarea legii și satisfacerea interesului general al cetățenilor. Privită în sens material, aceasta desemnează activitatea de organizare a executării și de executare efectivă a legii, desfășurată în multiple domenii ale vieții sociale. În sens organic, administrația publică este constituită din ansamblul structurilor organizatorice și instituțiilor care realizează această activitate, aflate în serviciul puterii executive și în legătură cu celelalte puteri ale statului. [10]

În raport cu organizarea statală, administrația publică se constituie ca un subsistem funcțional și organizatoric al sistemului global al organizării sociale. Aceasta este strâns legată de stat, în calitatea sa de instituție care deține suveranitatea și autoritatea legitimă asupra teritoriului și populației. Administrația publică acționează în virtutea competenței conferite prin Constituție și lege, realizând coordonarea, aplicarea și controlul politicilor publice în cadrul unei guvernări legitime, caracteristice statului de drept. [11]

Structura administrației publice reflectă complexitatea și diversitatea funcțională a acesteia. Potrivit literaturii de specialitate, administrația publică poate fi împărțită în mai multe forme: administrație centrală și administrație teritorială; administrație de stat și administrație locală; administrație generală și administrație specializată. Administrația centrală include autoritățile puterii executive (Guvernul, ministerele), în timp ce administrația teritorială este formată din

[5] A fi conectat la o rețea de Internet.
[6] Rețea la nivel global.
[7] Intruziunea neautorizată într-un computer sau rețea.
[8] Orice tip de software conceput special pentru a ataca un computer/rețea.

instituțiile care funcționează în unitățile administrativ-teritoriale (prefecturi, servicii publice deconcentrate). [10]

Administrația publică locală se constituie la nivelul comunelor, orașelor și județelor, unde autoritățile, adică consiliile locale și primarii, sunt alese de către cetățeni. Acestea administrează în mod autonom interesele colectivităților locale, în baza principiului descentralizării. În contrast, instituțiile deconcentrate ale administrației publice centrale funcționează la nivel teritorial, dar sunt subordonate autorităților centrale, având o competență administrativă delegată. [12]

Din punct de vedere funcțional, administrația publică îndeplinește atât funcții politice, legate de implementarea programelor guvernamentale, cât și funcții tehnico-administrative, de tip prestator sau decizional. Aceasta implică, pe de o parte, organe cu rol de conducere politică (precum Guvernul sau miniștrii) și, pe de altă parte, aparatul administrativ format din funcționari publici care aplică în mod concret legile și reglementările. [10]

În ceea ce privește principiile de organizare, administrația publică funcționează în baza centralizării, deconcentrării și descentralizării. Centralizarea presupune luarea deciziilor la nivel central și transmiterea lor ierarhică în teritoriu, fără autonomie locală. Deconcentrarea implică existența unor structuri teritoriale ale administrației centrale cu o anumită autonomie decizională, însă subordonate ierarhic. Descentralizarea, în schimb, recunoaște colectivităților locale dreptul de a se administra autonom, prin autorități alese local, care nu sunt subordonate direct Guvernului. [12]

Astfel, administrația publică apare ca o formă organizatorică esențială a statului, prin care acesta exercită puterea executivă, asigurând funcționarea ordinii de drept și gestionarea treburilor publice. Evoluția acestui sistem a fost influențată nu doar de transformări politice și instituționale, ci și de avansul tehnologic, care a impus treptat integrarea soluțiilor digitale în procesele administrative, aspect tratat în detaliu în subcapitolul următor, dedicat evoluției digitale a administrației publice.

1.2. Evoluția digitală în administrația publică.

Administrarea publică reprezintă ansamblul instituțiilor și mecanismelor prin care statul, alături de autoritățile locale, furnizează servicii și reglementează diverse domenii de activitate în interesul cetățenilor. În esență, ea implică gestionarea eficientă și transparentă a resurselor publice, aplicarea politicilor și legilor, precum și menținerea echilibrului între interesul public și drepturile individuale ale cetățenilor. În ultimele decenii, acest spațiu administrativ s-a confruntat cu cerințe crescânde de adaptare, reformă și modernizare, dat fiind contextul socio-economic și avansul tehnologic accelerat. Pe fondul avansului tehnologic și al presiunilor socio-economice, instituțiile publice sunt nevoite să adopte tehnologia informației și comunicațiilor pentru a răspunde cerințelor intensive de reformă și adaptare. [13, 14]

Un prim pas în această evoluție a presupun digitalizarea unor procese existente, mutând documentele din format fizic în arhive electronice, pentru a reduce costurile și birocrația. Însă, e-guvernarea[9] a căpătat repede un rol strategic, vizând interoperabilitatea instituțiilor, platformele de consultare publică și soluții online care să ofere transparență și să stimuleze participarea civică [13]. Prin astfel de metode și practici, statul și autoritățile acestuia pot scurta timpii de răspuns la cereri, pot face disponibile prin platforme online o multitudine de servicii și pot reduce, printr-o

[9] Reprezintă guvernarea electronică, mai exact modalitatea de aplicare şi utilizare a tehnologiilor informaţionale şi de comunicaţii, în scopul asigurării accesului la informaţie şi prestării serviciilor publice în regim interactiv;

astfel de manieră, contactul direct la ghișeu. Astfel, relația dintre cetățeni și administrație devine una mai rapidă, mai puțin costisitoare și mai transparentă. [15]

Implementarea inițiativelor de tip e-guvernare s-a întâmplat treptat, de la digitalizarea unor procese interne de pildă gestiunea documentelor sau evidența personalului, la furnizarea unor servicii publice online (depunerea declarațiilor fiscale, eliberarea documentelor oficiale, accesul la registre electronice etc). Printre factorii care determină succesul acestor proiecte se numără voința politică, cadrul legislativ clar, alocarea resurselor necesare și competențele digitale ale personalului implicat. [16]

Inițiativele de modernizare administrativă au la bază ideea optimizării proceselor, ceea ce presupune reducerea redundanțelor și a costurilor de funcționare, împreună cu îmbunătățirea calității serviciilor. Totuși, tranziția de la simpla computerizare[10] a unor proceduri către o transformare digitală autentică implică regândirea structurii instituționale și a abordărilor manageriale. [14] În acest sens, digitalizarea devine un fenomen mai amplu decât mutarea arhivelor de hârtie în suport electronic, ci reorganizarea fluxurilor de lucru și crearea unor canale de comunicare mai deschise cu mediul privat și cu cetățenii. [15]

Un alt salt al digitalizării este fundamentat de dezvoltarea „smart city-urilor”[11], care presupun o colaborare extinsă între sectorul public, mediul privat și comunitate în vederea eficientizării gestionării serviciilor urbane, de la transport și utilități până la siguranță publică. Într-un oraș inteligent, instituțiile pot folosi rețele de senzori, aplicații mobile și platforme de big data[12] pentru a lua decizii în timp real și a interveni rapid în situații neprevăzute. De pildă, gestionarea inteligentă a traficului poate reduce congestiile și poluarea, iar sistemele de iluminat public pot fi optimizate pentru a economisi energie și a îmbunătăți confortul locuitorilor. Integrarea tehnologiilor se rezumă la servicii mai fluide și o capacitate de reacție sporită a administrației. [17]

Îmbunătățirea transparenței și a participării civice se numără printre avantajele cele mai vizibile. Administrațiile pot publica online date despre cheltuielile bugetare, licitații publice sau indicatori de performanță, ceea ce duce la o relație mai corectă și mai deschisă cu cetățenii. Digitalizarea facilitează creșterea transparenței deoarece datele și informațiile relevante devin accesibile într-un mod rapid și structurat, iar cetățenii pot verifica oricând evoluția unui proiect public, de exemplu. De asemenea, prin introducerea aplicațiilor electronice, instituțiile își pot reduce semnificativ timpul de procesare a documentelor și costurile administrative. Interacțiunea constantă și directă prin canale digitale (e-mail, platforme online, forumuri de consultare) asigură un grad mai înalt de participare cetățenească și poate impulsiona demersurile de tip e-democrație sau e-participare. Prin intermediul platformelor digitale, aceștia pot consulta proiecte de lege, pot participa la dezbateri și pot transmite sesizări într-un mod simplu și accesibil. Totodată, feedback-ul permanent din partea societății poate contribui la eficientizarea serviciilor publice și la crearea unui climat de încredere între instituții și beneficiari. [13, 17]

Totuși, aspectele pozitive vin la pachet și cu cele negative într-un proces evolutiv. În primul rând, problema securității cibernetice devine esențială. [18] Dat fiind faptul că tot mai multe procese administrative și fluxuri de date sensibile se mută în mediul online, este necesară adoptarea unor mecanisme și politici de protecție viguroase, care să poată preveni atacurile cibernetice, furtul de date, accesările neautorizate și multe altele. În acest sens, instituțiile trebuie să investească în sisteme de criptare, soluții de autentificare sigură și formarea personalului pentru a răspunde prompt amenințărilor. [16] O altă dificultate este legată de accesul uniform la tehnologie, mai ales

[10] A introduce folosirea computerului în diverse domenii de activitate;
[11] În română „oraș inteligent”, desemnează un mediu urban care folosește tehnologia și inovația pentru a crea un ecosistem sustenabil, conectat și centrat pe nevoile cetățenilor;
[12] Seturi de date extrem de mari și complexe care nu pot fi gestionate sau analizate cu ușurință cu instrumentele tradiționale de prelucrare a datelor;

în zonele rurale sau în rândul categoriilor vulnerabile. Digital divide-ul[13] poate accentua inegalitățile, dacă nu este gestionat prin politici adecvate de alfabetizare digitală și dezvoltare a infrastructurii de internet. [13] La acestea se adaugă și rezistența la schimbare din interiorul instituțiilor și lipsa unei culturi administrative deschise spre inovație. Este necesară, deci, instruirea personalului, elaborarea unui cadru legislativ clar și investiții în infrastructuri și competențe TIC[14], pentru a asigura o tranziție coerentă și un echilibru între inovare și protecția vieții private. [16]

Evoluția digitală a administrației publice conturează o schimbare majoră, care merge dincolo de simpla modernizare tehnologică. Ea include reforme legislative, parteneriate strategice și educație digitală, toate acestea pentru a atinge obiective precum eficiența, participarea și transparența. Beneficiile pe termen lung sunt considerabile, începând de la accesul facil la servicii și scăderea costurilor, până la întărirea relației dintre cetățeni și stat. Cu o abordare adecvată și investiții bune, administrația publică poate deveni un motor de dezvoltare socială și economică, păstrând și un grad înalt de protecție a datelor și de incluziune a tuturor categoriilor sociale. [17]

1.3. Structura și rolul infrastructurii IT în administrația publică.

Transformările profunde care au avut loc în societate odată cu dezvoltarea tehnologiilor informației și comunicațiilor au generat o nevoie tot mai accentuată de modernizare în administrația publică. Astăzi, instituțiile guvernamentale trebuie să gestioneze volume mari de date, să răspundă prompt solicitărilor cetățenilor și să ofere servicii transparente și eficiente. În acest context, o infrastructură IT solidă și bine structurată reprezintă pilonul esențial care susține digitalizarea și optimizarea proceselor de lucru.

Prin infrastructură IT, înțelegem ansamblul de resurse hardware, software și de rețea care asigură colectarea, prelucrarea și transmiterea informațiilor în cadrul instituțiilor publice. De la centre de date și servere, până la platforme de comunicare și aplicații de e-guvernare, toate aceste componente contribuie la buna desfășurare a activităților administrative. În esență, infrastructura IT oferă soluția prin care funcționarii publici și cetățenii pot interacționa în mod rapid și sigur, fără să mai depindă de procedurile tradiționale pe suport de hârtie. [13, 19, 20]

Un rol deosebit de important al infrastructurii IT constă în facilitarea accesului la informații și servicii. Cetățenii pot depune cereri, pot obține documente sau pot verifica stadiul unor solicitări prin intermediul portalurilor online, fără să se mai deplaseze la ghișeu. [21] Astfel, timpul de așteptare se reduce considerabil, iar resursele administrative sunt folosite mai eficient. În paralel, și instituțiile publice beneficiază de un flux de lucru mai clar, bazat pe evidențe digitale, ceea ce minimizează riscul erorilor umane și crește transparența. [22]

Mai mult decât atât, infrastructura IT sprijină procesele de analiză și luare a deciziilor la nivelul administrației. Datorită soluțiilor de tip big data sau instrumentelor de automatizare bazate pe inteligență artificială, pot fi colectate și interpretate volume semnificative de informații într-un timp scurt. [23]

Aceste date de volum imens, provenite din surse diverse (registre oficiale, platforme de feedback de la cetățeni, sisteme interne), permit celor ce iau decizii să identifice mai ușor problemele urgente și să adopte politici publice mai apropiate de realitate. De exemplu, într-o situație de criză

[13] În română „decalajul digital”, se referă la decalajul dintre cei care pot beneficia de internet și cei care nu au această posibilitate;

[14] Acronim pentru Tehnologia Informației și a Comunicațiilor. Acest concept constă în tehnologia necesară pentru prelucrarea (procurarea, procesarea, stocarea, convertirea și transmiterea) informației;

sanitară sau economică, administrația poate reacționa mai rapid dacă are acces la date actualizate în timp real despre incidența unor fenomene ori despre nevoile comunității. [24]

Odată cu digitalizarea acțiunilor, administrația publică gestionează informații sensibile despre cetățeni și mediul de afaceri. Pentru a preveni atacurile informatice și scurgerile de date, în cadrul infrastructurilor IT trebuie să fie integrate mecanisme solide de protecție, precum sisteme de criptare[15], firewall-uri[16] avansate și proceduri stricte de autentificare. În plus, instruirea continuă a personalului cu privire la bunele practici de securitate devine esențială pentru a menține un nivel ridicat de protecție împotriva amenințărilor. [13, 19]

În același timp, crearea și întreținerea unei infrastructuri IT performante presupun și greutăți. Pe de o parte, investițiile inițiale pot fi considerabile, mai ales în cazul modernizării unor structuri vechi care nu au fost proiectate pentru cerințele actuale. [25] Pe de altă parte, procesul de migrare de la un sistem tradițional la unul digital implică și o componentă de schimbare organizațională. Instituțiile trebuie să își adapteze modul de lucru, iar funcționarii publici au nevoie de formare profesională pentru a utiliza noile instrumente digitale. În absența unei strategii ferme de implementare și a unei voințe politice puternice, există riscul ca aceste inițiative să rămână la stadiul de proiect-pilot sau să fie fragmentate între diferitele departamente. [20]

Un alt element care merită evidențiat face referire la dimensiunea colaborării între diversele nivele guvernamentale (național, regional, local) și partenerii externi (sector privat, ONG-uri). O infrastructură IT nu funcționează izolat, ci necesită interoperabilitate și armonizare legislativă. De pildă, schimbul de date între ministere și agenții trebuie să respecte standarde comune, astfel încât cetățenii să nu fie nevoiți să introducă aceleași informații în sisteme diferite. Prin interoperabilitate, se reduc duplicările și se îmbunătățește calitatea serviciilor, deopotrivă pentru utilizatorii interni și externi. [22, 24]

Pe termen lung, beneficiile unei infrastructuri IT bine consolidate sunt semnificative: procese mai transparente, costuri administrative reduse, viteză sporită de răspuns și o relație mai apropiată cu cetățenii. Cu toate acestea, pentru ca impactul să fie cu adevărat remarcabil, investițiile în tehnologie trebuie dublate de o schimbare de mentalitate în rândul personalului administrativ. Adaptarea la un mod de lucru digital implică renunțarea treptată la proceduri învechite și o atenție mai mare acordată nevoilor populației. [13]

În general, o infrastructură IT este alcătuită din mai multe componente, toate intercontectate. Pentru comprehensivitate amintim astfel:

- Centre de date și echipamente hardware, de exemplu: servere, echipamente și sisteme de stocare a datelor; [24]
- Aplicații software și mecanisme de interoperabilitate, cum ar fi platformele de gestiune a documentelor, aplicații de e-servicii și cele de schimb de date dintre instituții; [20]
- Tehnologii de securitate cibernetică, de pildă firewall, criptarea; [13]
- Instrumente de analiză și automatizare, precum tehnologiile de tip big data sau inteligență artificială. [23]

Luând în considerare afirmațiile precedente, infrastructura IT nu se limitează la a fi un simplu set de echipamente și programe, ci devine un instrument strategic de modernizare a administrației

[15] Constă în acțiunea de conversie a informațiilor, din text scris în text cifrat, în așa fel încât entitățile neautorizate să nu le poată accesa. În eventualitatea în care datele criptate sunt pierdute sau furate, riscul ca acestea să fie dezvăluite este minim pentru că oricine ar dori să le vizualizeze nu deține cheia de decriptare a informațiilor;

[16] Sistem de securitate care monitorizează traficul de rețea care intră și iese și permite sau blochează pachetele de date pe baza unui set de reguli. Scopul său este de a stabili o barieră între rețeaua ta internă și traficul de intrare din surse externe;

publice. Prin implementarea și integrarea corespunzătoare a resurselor tehnologice, instituțiile pot evolua către un model de guvernare axat pe eficiență, transparență și inovare. Rămâne imperios necesar ca aceste eforturi să fie coordonate, finanțate adecvat și susținute de politici publice clare, care să sprijine colaborarea interinstituțională și dezvoltarea competențelor digitale ale angajaților. Numai așa se poate asigura un cadru în care serviciile publice să răspundă prompt cerințelor societății actuale, contribuind la creșterea încrederii în instituții și la bunul mers al comunităților. [21]

1.4. Vulnerabilitățile sistemelor informatice.

Transformarea digitală a diverselor sectoare, atât în mediul privat, cât și în administrația publică, a dus la creșterea exponențială a volumului de date procesate și partajate. Această evoluție generează, însă, un numar tot mai mare de puncte slabe, denumite vulnerabilități, ce pot fi exploatate de indivizi sau grupuri rău intenționate. Într-o lume în care infrastructurile critice și aplicațiile online devin tot mai dependente de componente software și hardware interconectate, înțelegerea modului în care apar și pot fi soluționate vulnerabilitățile devine esențială. [26]

O modalitate de producere a vulnerabilităților derivă din erori de proiectare și implementare a sistemelor informatice. Chiar și cele mai simple vulnerabilități, precum parolele slab configurate, pot fi exploatate rapid de instrumente automatizate. [27] Astfel, lipsa testării riguroase, documentarea incompleta și interfețele neprotejate oferă posibilitatea atacatorilor să acceseze, modifice ori să fure date sensibile. În mod similar, în sfera administrației publice, configurarea defectuasă a unor servicii digitale crește semnificativ riscul ca informațiile personale și instituționale să ajungă pe mâini nepotrivite. [7]

Un alt factor care contribuie la apariția vulnerabilităților este complexitatea tot mai ridicată a infrastructurilor de tip industrial sau a rețelelor ce aparțin marilor instituții, unde pot exista numeroase dispozitive conectate. În cadrul infrastructurilor critice, orice breșă de securitate poate avea consecințe majore asupra stabilității unor servicii de importanță națională. Tocmai de aceea, un dezavantaj, un segment de rețea neactualizat la timp, poate fi folosit într-o succesiune de atacuri avansate. [26] Prin tehnici sofisticate de infiltare, precum cele puse în evidență de evoluția tipologiilor de malware, atacatorii reușesc să se strecoare și să submineze rezistența sistemelor. [9]

Un rol substanțial îl ocupă și factorul uman. Chiar dacă există proceduri de securitate, multe atacuri reușesc să creeze efecte prin intermediul erorilor de utilizare, neatenției ori lipsei de educație digitală. În administrația publică, de exmplu, un simplu e-mail de tip phishing ori un fișier periculos poate oferi acces la date confidențiale și infrastructuri strategice, dacă angajații nu înțeleg riscurile. [7] Mai mult de atât, lacunele în formarea personalului și absența unor reguli clare pentru gestionarea datelor duc la amplificarea vulnerabilităților. [28]

În plus, ritmul rapid de inovare tehnologică face ca unele sisteme să fie puse în funcțiune înainte de a fi testate corespunzător. Cu fiecare nouă versiune software ori cu fiecare actualizare majoră, pot apărea deficiențe nesesizate de catre echipele de dezvoltare, ceea ce atacatorii pot exploata cu atacuri zero-day. În acest context, infrastructurile publice devin extrem de vulnerabile când nu există mecanisme de monitorizare, patch-uri rapide sau redundanțe[17] de siguranță. [27]

[17] Surplus de informație transmis față de strictul necesar și care asigură exactitatea transmiterii informației;

Capitolul 2. Impactul atacurilor cibernetice.

Progresele din domeniul tehnologiei au condus la noi moduri în care societățile se administrează, introducând treptat rețelele informatice pentru a fluidiza acest proces administrativ, devenind elemente de infrastructură critică atât în domeniul public, cât și în mediul privat. Creșterea volumului de date în format digital și dependenței de serviciile online[18] au atras după sine amenințări cibernetice din ce în ce mai complexe. [7] În momentul prezent, atacurile cibernetice nu mai reprezintă doar acțiuni izolate cu scopul de a exploata vulnerabilități tehnice, ci pot fi organizate, pregătite în detaliu, avansate și au capacitatea de a provoca consecințe substanțiale asupra stabilității instituționale. [8]

Odată cu ajutorul oferit de tehnologie, trebuie să aruncăm o privire asupra faptului că răspândirea Internetului[19] a determinat și accesibilitatea mai ușoară la instrumentele de hacking[20], fenomen ce a favorizat dezvoltarea de piețe negre în mediul online, în cadrul cărora sunt vândute diverse, de la datele furate până la malware[21]. [8] Totodată, numărul de atacatori se extinde, având diferite nivele de compentență, iar cei ce sunt responsabili de protejarea infrastructurilor sunt constrânși să facă față noilor provocări, să devină din ce în ce mai pregătiți și să încercere să contracareze amenințările. [9]

Tocmai din aceste motive este imperios necesar să știm cu ce tipologii de atacuri cibernetice ne putem confrunta, cum au evoluat și să fim conștienți de vulnerabilitățile pe care le dețin sistemele informatice, aspecte care vor fi parcurse în continuarea acestui capitol.

Guvernarea electronică (e-guvernarea) constituie una dintre cele mai semnificative schimbări din administrația publică modernă, având drept scop eficientizarea serviciilor publice prin intermediul tehnologiilor informației și comunicațiilor. Această transformare digitală aduce numeroase beneficii, printre care reducerea costurilor administrative, creșterea transparenței și facilitarea accesului cetățenilor la serviciile publice în mod continuu. Totuși, această digitalizare masivă aduce și vulnerabilități majore, făcând administrația publică predispusă la riscurile atacurilor cibernetice, care pot compromite atât securitatea informațiilor, cât și funcționarea propice a serviciilor publice furnizate cetățenilor. [13]

Întretăierea dintre e-guvernare și atacurile cibernetice este, din păcate, inevitabilă, deoarece adoptarea tehnologiilor informaționale crește expunerea instituțiilor publice la amenințări informatice. Din cauza intensificării utilizării platformelor digitale în administrația publică, atacurile cibernetice devin o preocupare majoră, fiind necesară implementarea unor politici și reglementări eficiente de securitate cibernetică. Managementul accesului la date, autentificarea și autorizarea utilizatorilor sunt elemente fundamentale în protejarea informațiilor guvernamentale și asigurarea continuității operaționale a serviciilor publice electronice. În lipsa unor strategii clare, concrete și a instruirii adecvate a funcționarilor publici în legătură cu securitatea cibernetică, riscul de breșe și atacuri asupra sistemelor informaționale devine iminent, generând consecințe grave asupra funcționării administrației și asupra încrederii cetățenilor în autorități. [29]

Provocările digitalizării sunt reprezentate și de dificultăți precum decalajul digital, rezistența organizațională la schimbare și limitările infrastructurii tehnologice existente. Tocmai de aceea, administrațiile publice sunt nevoite să dezvolte parteneriate strategice cu firme din domeniul IT

[18] A fi conectat la o rețea de Internet;
[19] Rețea la nivel global;
[20] Intruziunea neautorizată într-un computer sau rețea;
[21] Orice tip de software conceput special pentru a ataca un computer/rețea;

pentru implementarea unor soluții care să ajute infrastructura informațională și să contribuie la informarea online a cetățenilor.

Astfel, dezvoltarea unor politici eficiente și pregătirea adecvată a personalului administrativ devin imperative, pentru a limita riscurile și a asigura protecția informațiilor publice sensibile și funcționarea sigură a platformelor digitale guvernamentale. [13, 30]

În urma celor menționate anterior, capitolul 2 al lucrării urmărește oferirea unui context mai amplu în ceea ce privește digitalizarea în administrația publică, reglemenările actuale în materie la nivel european și internațional, precum și consecințele unor asemenea incidente.

2.1. Definiția și evoluția atacurilor cibernetice.

Regăsim mai multe definiții pentru „atac cibernetic", acestea variază, însă înglobează aceleași idei cum că reprezintă o acțiune neautorizată, ostilă sau intruzivă asupra unei rețele sau a unui sistem informatic, având ca scop de a obține acces la date, de a le perturba, distruge sau delapida informații importante sau clasificate. [31, 32] Pe măsură ce infrastructurile tehnologice au început să fie integrate în sitemele economice, militare și guvernamentale, atacurile cibernetice s-au amplificat. [8]

În sectorul public, de obicei, un atac cibernetic vizează incapacitarea site-urilor și serviciilor administrației publice, furtul sau alterarea datelor confidențiale și/sau compromiterea sistemelor critice naționale. Astfel, un atac cu succes asupra infrastructurii poate avea consecințe puternice asupra securității și stabilității unui stat. [7]

La început, atacurile cibernetice au constat în apariția virușilor și viermilor informatici. Aceste forme de malware au fost concepute, mai întâi, ca experimente sau demonstrații de „abilități" în domeniul IT. Gradual s-au tranformat în instrumente utilizate cu scopuri distructive. Atacatorii nu vizau instituții semnificative ale statului sau ale companiilor. [9]

Cu timpul, însă, în jurul anilor 2000, atacurile cibernetice au devenit din ce în ce mai divesificate. Răspândirea tehnologiei de tip broadband[22], introducerea tranzacțiilor online și digitalizarea informațiilor personale au creat oportunități de întreprindere a unor astfel de acțiuni. În această perioadă își fac apariția atacuri de tip phishing, troieni bancari și primele forme de hacking către furtul de date sensibile ale indivizilor și ale instituțiilor publice. [8, 33] În același interval temporal, au început să fie vizate și instrastructurile critice, instituțiile financiare și organizațiile guvernamentale care s-au expus în mediul online, iar evoluția tot mai intensă a dus la constituirea de rețele botnet[23], facilitând atacurile de tip DDoS (Distributed Denial-of-Service)[24].

Într-o următoare etapă de evoluție, atacurile au devenit mai sofisticate, îndreptându-se și spre aria politică și geopolitică. S-au manifestat atacuri împotriva unor state sau instituții guvernamentale. Un exemplu relevant este cel al Estoniei din anul 2007, unde au fost paralizate site-urile unor instituții cheie, cum ar fi cel al Parlamentului, bănci, ministere etc. Tot în această perioadă au apărut și cazuri de spionaj cibernetic și tentative de a compromite sisteme militare. Acest salt a pus bazele conceptului de „război cibernetic". [7, 9, 33]

În ultimul deceniu, odată cu maturizarea tehnologiilor și a rețelelor sociale, atacurile au devenit foarte greu de detectat deoarece au început să utilizeze tehnici complexe de camuflare, inginerie

[22] Tradus în română ca „bandă largă", termen care descrie accesul la Internet de mare viteză;
[23] Serie de dispozitive conectate la Internet, denumite și boți, acestea fiind infectate cu programe malware care permit atacatorului să le controleze de la distanță;
[24] Tip de atac cibernetic care încearcă să indisponibilizeze sau să blocheze resursele unui calculator;

socială[25] și ransomware[26]. De aceea, s-a constatat o creștere majoră a atacurilor țintite, cunoscute și sub denumirea de APT (Advanced Persistent Threats)[27], lansate de grupuri bine organizate care sunt susținute financiar și politic. [7, 8]

2.2. Tipuri de atacuri cibernetice.

Principalele categorii de atacuri care pot afecta instituțiile administrației publice sunt:

- Malware;
- Ransomware;
- Atacuri de tip phishing și alte tehnici de inginerie socială;
- Atacuri de tip DoS și DDoS;
- Atacuri asupra integrității datelor;
- Atacuri asupra Supply Chain;
- Atacuri de tip Zero-Day;
- Atacuri APT;
- Atacuri de tip Man-in-the-Middle.

Termenul de „malware" descrie orice tip de software[28] malițios, conceput pentru a se infiltra în sistemele informatice fără consimțământul utilizatorilor. Atacul de tip malware acționează prin viruși, viermi, troieni, programe spion, având rolul de a perturba activitatea sau de a extrage informații confidențiale. Într-o instituție publică, malware-ul poate bloca accesul la bazele de date, poate compromite integritatea documentelor oficiale și poate duce la scurgeri de date cu caracter personal sau strategic. [34] Virușii și viermii sunt capabili să se autocopieze în sistemul compromis, diferența dintre cele două categorii fiind faptul că virușii corup fișiere, iar viermii pot provoca daune întregii rețele. Iar, troineii imită programe legitime care sunt fabricate pentru a fura date sau a permite altor utilizatori acces la sistemul infectat. [35]

Cea de a doua tipologie de atac cibernetic, ransomware, este tot o formă de malware care criptează fișierele ori sistemele vizate și solicită o recompensă pentru redobândirea accesului la date. Mai exact, după infectare, fișierele instituției devin inaccesibile, iar atacatorii cer, de obicei, sume de bani pentru deblocare. Acesta întrerupe serviciile publice, blochează fluxul de documente și posibile pierderi financiare cauzate de downtime. [35, 36]

Phishing-ul este o încercare frauduloasă de a obține date private prin email-uri care imită surse oficiale sau de încredere. Incluse în acest tip de atac sunt vishing-ul (atac prin telefon) și smishing (mesaje text). Prin această metodă, atacatorii exploatează încrederea sau neatenția utilizatorilor reușind să păcălească în a accesa link-uri infectate sau să ofere chiar date confidențiale. În eventualitatea în care un astfel de fenomen are loc într-o instituție publică, angajații pot dezvălui neintenționat date importante, parole sau informații privind procedurile interne, fapt ce poate genera compromiterea securității instituției. [34, 27]

Atacurile DoS și DDoS vizează supraîncărcarea resurselor unor unui sistem, astfel încât acesta să devină indisponibil pentru utilizatorii reali. Atacatorii trimit un volum foarte mare de cereri sau date către serverele țintă, depășind capacitatea sistemului de procesare. Aceste întreruperi pot bloca platformele de e-guvernare, portalurile de depunere a documentelor sau alte servicii publice, provocând întârzieri și nemulțumiri în rândul cetățenilor. [36, 37]

[25] În contextul securității informațiilor, reprezintă manipularea persoanelor pentru a efectua unele acțiuni sau pentru a divulga informații confidențiale;
[26] Tip de software rău intenționat;
[27] O campanie de lungă durată, ilegală, în care un intrus sau o întreagă echipă de intruși își stabilesc prezența într-o rețea pentru a extrage date;
[28] Set de instrucțiuni sau programe care instruiesc un computer să facă sarcini specifice;

Atacurile asupra integrității datelor se concentrează pe modificarea neautorizată a acestora, cu scopul de a genera confuzie, de a influența deciziile administrative sau de a compromite veridicitatea informațiilor publice. [36]

Cel de al șaselea atac, acel asupra Supply Chain[29] sau lanțul de aprovizionare, constituie compromiterea unui furnizor sau partener terț pentru a ajunge ulterior la entitatea dorită. Se bazează pe exploatarea breșelor din sistemele unor colaboratori externi, cum ar fi o firmă de software, și transmit apoi spre instituția dorită a fi periclitată. [36]

Un atac zero-day are loc atunci când o vulnerabilitate software sau hardware[30] este utilizată în scopuri negative înainte să fie dispus un patch de securitate[31] pentru a ameliora problema. Un asemenea atac este extrem de periculos deoarece nu poate fi detectat de sisteme și profită de fisuri necunoscute nici de echipele tehnice. [34, 38]

APT-urile implică un grup de atacatori bine pregătiți, care resurse imense pentru a obține acces pe termen îndelungat la sistemele unui anumit organism public sau la rețele de interes strategic. Nu produc efecte vizibile în momentul infiltrării și extrag un paletar larg de date, reușind să submineze un întreg sistem de securitate. [27]

Atacurile de tipologie Man-in-the-Middle au loc în momentul în care un atacator intervine între două sau mai multe părți care comunică, reușind să intercepteze, să modifice informațiile transmise sau să fure identități fără ca interlocutorii să observe. Acestea sunt cu greu detectate și pot fi infiltrate cu ajutorul Wi-Fi-urilor sau paginilor Web nesecurizate (cele care utilizează protocolul HTTP). [39]

Pentru a clarifica, protocolul HTTP este diferit de cel HTTPS, cdiferența dintre cele două fiind faptul că cel de al doilea menționat are un strat de criptare în plus pentru a securiza comunicarea. [40]

Fig. 1. Tipuri de amenințări.
Sursa: https://www.europarl.europa.eu/topics/ro/article/20220120STO21428/securitate-cibernetica-principalele-amenintari

[29] Rețea de organizații;
[30] Reprezintă partea fizică a unui computer;
[31] Actualizarea unui software în vederea înlăturării unor defecţiuni/vulnerabilităţi anterioare ale acestuia;

2.3. Atacatorii implicați în atacurile cibernetice.

Sistemele informatice ale instituțiilor guvernamentale reprezintă o țintă frecventă pentru atacatori diverși, de la grupuri susținute de state până la persoane individuale, fiecare urmărind interesele proprii. În funcție de motivație, atacurile cibernetice pot avea o natură politică, cum este cazul războiului cibernetic, al spionajului sau al hacktivism-ului, ori una financiară sau personală, vizând obținerea de câștiguri ilegale, furtul de date sau chiar răzbunarea unor angajați nemulțumiți. Indiferent de scop, realitatea rămâne, din păcate, aceeași: nicio rețea nu este complet sigură, iar un atac poate se poate desfășura de oriunde, indiferent de moment, din partea oricui cu resurse suficiente și intenții. [7, 41].

Statele naționale au devenit actanți principali în spațiul cibernetic, dezvoltând competențe ofensive pentru a-și atinge diferitele țeluri, cum ar fi cele politice, militare sau economice. Guvernele din întreaga lume investesc în echipe și instrumente de atac cibernetic pentru a fura informații sensibile, a obține avantaje economice sau a pregăti terenul pentru posibilele conflicte de natură armată în spațiul digital. Având parte de finanțări și dotați cu aparatură sofisticată, atacatorii statali se pot infiltra în rețelele administrației și pot afecta infrastructuri deosebit de importante, amenințând atât sistemele IT guvernamentale, cât și serviciile esențiale care depind de acestea. Un exemplu în acest sens este virusul Stuxnet din anul 2010, care a fost adjudeat unor agenții guvernamentale, care a sabotat instalațiile nucleare ale Iranului prin infectarea sistemelor industriale, acest incident demonstrând că un atac cibernetic bine planificat și executat poate produce pagube considerabile. [7]

Organizațiile de tipologia celor teroriste pot utiliza atacurile cibernetie pentru a provoca haos și panică în societate, urmărind efecte similare terorismului clasic, dar prin mijloace digitale. Asemenea grupări vizează în special infrastructuri fundamentale (precum rețelele electrice, de transport sau de comunicații) sau sistemele financiare, cu scopul de a perturba sever funcționarea statului și a semăna spaimă în rândul populației. Deși, până în prezent atacurile cibernetice cu adevărat catastrofale din partea a astfel de grupări au fost rare, amenințarea este reală și în creștere, determinând autoritățile să acorde o atenție sporită acestui pericol cu posibilitate ridcată de realizare. [7, 41]

O multitudine de atacuri provin de la grupări infracționale care au drept motivație elementul financiar. Infracțiunile cibernetice întreprinse de grupările organizate constituie o industrie, la nivel global, profitabilă, prin intermediul cărora hackerii specializați, spărgătorii de sisteme de plată și alți complici colaborează pentru a fura bani sau date sensibile prin fraudă informatică, furt de identitate, spălare de bani ori șantaj (ransomware) vizând atât companii din aria privată, cât și instituții publice. Consecințele acestor atacuri includ întreruperea serviciilor care se aflau la dispoziția cetățenilor, pierderi financiare consistente și erodarea încrederii publice în capacitatea autorităților de a-și proteja sistemele și de a le menține în siguranță datele. [2, 7]

De asemenea, angajații sau foștii angajați ai unei instituții pot reprezenta, la rândul lor, o amenințare dacă acționează răuvoitor. O persoană din interior care este motivată de ranchiună, dorință de răzbunare sau interese personale propii și deține acces în mod direct la sistemele interne și cunoaște mecanismele de securitate, poate sustrage sau distruge date ori sabota funcționarea optimă a rețelei din interior. Totodată, erorile umane pot contribui la atacurile din exterior. Pentru a fi mai comprehensiv, luăm situația unui angajat neinstruit. Acesta poate oferi involuntar acces atacatorilor, printr-un e-mail de tip phishing care îi fură datele de autentificare. Consecințele unor acțiuni interne de rea-voință sau ce țin de neglijență pot fi la fel de grave ca ale unui atac extern rde succes deoarece există posubilitatea să se divulge datele confidențiale ale cetățenilor, să se compromită integritatea informațiilor sau să fie întrerupte serviciile administrative, toate acestea însoțite de pierderi financiare și diverse alte prejudicii. [7, 42]

Pe lângă cele menționate anterior, există și numeroși atacatori independenți care nu sunt interesați de bani sau interese politice, ci mai degrabă îi determină provocarea intelectuală, curiozitatea sau prestigiul în comunitatea hackerilor. Nivelul lor de cunoștințe diferă destul de mult pentru că se regăsesc atât hackerii experți, capabili să descopere vulnerabilități complexe și să se infiltreze în sisteme sigure, cât și persoanele novice („script kiddies") care folosesc programele fără a înțelege cu exactitate cum funcționează. Chiar dacă multe dintre aceste acțiuni sunt realizate din diferite motive, indiferent că sunt serioase sau frivole, ele pot cauza pagube semnificative. De exemplu, un hacker poate modifica neautorizat conținutul unor site-uri oficiale (defacement) sau poate provoca pierderea ori furtul unor date confidențiale deținute de stat. [2, 7]

O altă categorie, hacktiviștii care nu sunt interesați de bani, ci de ideile în care cred. Sunt persoane care folosesc mijloace tehnice pentru a protesta împotriva nedreptăților sociale, politice sau economice. Spre deosebire de infractorii cibernetici clasici, care urmăresc câștiguri materiale, hacktiviștii încearcă să atragă atenția asupra unor cauze sau probleme pe care le consideră importante. De multe ori, metodele pe care le folosesc stârnesc controverse. Pot, de exemplu, să modifice fără autorizație site-uri oficiale, să publice informații sensibile sau să blocheze temporar accesul la platforme guvernamentale ori comerciale prin atacuri de tip DDoS. Un exemplu cunoscut este cel al grupului Anonymous. În 2010, membrii acestuia au reacționat împotriva măsurilor luate împotriva platformei WikiLeaks atacând site-urile autorităților suedeze și ale companiilor Visa și MasterCard. În viziunea lor, a fost un gest de protest față de cenzură și de limitarea libertății de exprimare. Deși astfel de atacuri nu provoacă, în general, distrugeri majore sau pierderi financiare semnificative, ele pot afecta imaginea instituțiilor vizate. Dacă site-urile statului sunt atacate des și utilizatorii observă probleme frecvente de funcționare sau modificări suspecte, încrederea în serviciile online publice poate scădea. În timp, oamenii pot deveni reticenți și evita aceste platforme, considerându-le instabile sau nesigure. [7]

Din paragrafele anterioare înțelegem faptul că atacurile cibernetice pot proveni din partea unor actori foarte diferiți, de la state și grupări teroriste, până la hackeri individuali, rețele infracționale sau chiar angajați din interiorul instituțiilor. Această diversitate face ca apărarea sistemelor administrative să fie o provocare reală. Fiecare dintre acești atacatori are propriile motive și folosește metode specifice, ceea ce înseamnă că nu există o soluție universală. Tocmai de aceea, instituțiile publice trebuie să adopte măsuri de securitate care să fie atât adaptabile, cât și bine fundamentate. Apărarea nu ține doar de instrumente tehnice, ci este la fel de important să înțelegem comportamentele umane și contextul internațional în care aceste amenințări apar. [43, 44, 45]

2.4. Efectele potențiale ale atacurilor cibernetice.

Atacurile cibernetice constituie una dintre cele mai complexe și persistente amenințări la adresa securității globale, având potențialul să provoace consecințe semnificative asupra sferei economice, sociale, politice și chiar militare, după cum s-a mai menționat și în alte paragrafe ale lucrării. [46] Într-o eră în care serviciile, infrastructurile și aproape toate tipurile de interacțiuni umane depind din ce în ce mai mult de spațiul digital, un atac cibernetic poate cauza perturbări majore și de durată. [47]

Un prim nivel de analiză se referă la potențialele efecte asupra infrastructurilor critice. În numeroase conflicte, atacurile cibernetice pot viza rețele de electricitate, sisteme de transport, baze de date guvernamentale ori servicii de urgență, întrucât paralizarea acestora generează haos la scară largă. [48] Prin utilizarea de tehnici de tip malware, phishing avansat sau atacuri distribuite de tip Denial-of-Service (DDoS), agresorii pot întrerupe furnizarea de servicii indispensabile, punând în pericol și viețile cetățenilor. [49] Iar, odată compromise, aceste sisteme pot fi folosite pentru a obține acces suplimentar la alte componente ale infrastructurii unui stat, amplificând exponențial consecințele inițiale ale atacului. [50]

Din perspectivă economică, pierderile se pot dovedi uriașe. În general, costurile directe implică sistarea temporară a operațiunilor, recuperarea și restaurarea datelor, precum și eventualele răscumpărări plătite în cazul atacurilor de tip ransomware. Însă efectele indirecte sunt cel puțin la fel de importante precum reputația organizației atacate, care poate fi afectată iremediabil, ceea ce duce la pierderea încrederii din partea clienților și partenerilor, scăderea valorii acțiunilor la bursă ori diminuarea investițiilor. [51] În plus, un lanț de aprovizionare[32], puternic informatizat, poate fi blocat, iar firmele, care depindeau de produsele și serviciile atacate, să-și vadă propriile afaceri paralizate temporar. Astfel, chiar și atacurile de anvergură medie pot avea efecte în lanț, propagându-se prin multiple industrii și domenii conexe. [52]

La nivel social, atacurile cibernetice pot submina încrederea în instituții și pot crea panică în rândul populației. Infrastructura orașelor inteligente (Smart City) este deosebit de expusă, întrucât colectează și prelucrează volume mari de date ce vizează transportul, consumul de energie, serviciile medicale și multe altele. [37] Un scenariu în care semafoarele sunt manipulate digital pentru a genera ambuteiaje masive sau chiar accidente pentru un atac cibernetic, deși poate părea desprins dintr-un film, este perfect posibil. [46] De asemenea, prin breșe de securitate, pot fi accesate informații personale (numere de identitate, date bancare, dosare medicale), ducând la încălcarea severă a intimității cetățenilor. [53]

Din punct de vedere politic, atacurile cibernetice sunt adesea folosite fie pentru a submina guvernele, fie pentru a influența deciziile acestora. [47] Actorii statali pot recurge la astfel de atacuri pentru a sabota concurenții politici, fie prin operațiuni de spionaj, fie prin perturbarea proceselor electorale. Cazurile de spionaj electronic[33], în care date confidențiale despre strategii guvernamentale, militare sau economice sunt sustrase, au potențialul de a destabiliza relații diplomatice. [52] În același timp, grupări non-statale precum organizațiile teroriste pot folosi mijloace cibernetice pentru răspândirea propagandei și recrutare online, generând nesiguranță. [48] Reputația actorilor implicați este de asemenea supusă unor riscuri, întrucât divulgarea neautorizată a informațiilor compromițătoare poate afecta decisiv încrederea publică. [54]

La nivel individual, efectele se pot manifesta prin pierderi materiale (furt de identitate, golirea conturilor bancare), hărțuire online sau șantaj pe baza informațiilor obținute ilicit. [53] Factorul uman rămâne deseori veriga slabă în lanțul de securitate. Adesea, neglijența ori lipsa de pregătire în domeniul securității cibernetice reprezintă principala cauză a reușitei multor atacuri. [54] Pe lângă aceste amenințări vizibile, se adaugă și aspectele legate de supravegherea excesivă și colectarea masivă de date, care pot conduce la restrângerea libertăților civile și la instituirea unei forme de "Big Brother"[34] digital. [47]

Hacktivismul, definit drept acțiune de protest digitală, cu obiective politice ori sociale, poate avea efecte semnificative prin redirecționarea atenției opiniei publice asupra anumitor probleme. [47] Atacurile de tip DDoS sau modificarea neautorizată a conținutului unor site-uri guvernamentale servesc, în acest caz, ca formă de contestare a puterii. Deși rareori produc daune majore asupra infrastructurii, pot eroda imaginea instituțională și pot crea solidaritate virtuală între comunitățile care susțin o anumită cauză. [46]

Consecințele asupra stabilității și securității internaționale sunt și ele demne de atenție. Într-un context de conflict armat, atacurile cibernetice pot fi integrate în strategii hibride, combinate cu tactici militare convenționale. [52] Ele pot fi orchestrate pentru a afecta moralul populației inamice, a sabota sistemele de comandă și control militar sau a submina alianțele internaționale.

[32] Procesul generat din momentul în care clientul plasează o comandă până în momentul în care produsul sau serviciul a fost livrat și taxat;
[33] Acţiune care vizează obţinerea accesului neautorizat la informaţii cu caracter confidenţial sau clasificat, stocate în cadrul unui sistem IT&C, cu scopul de a fi utilizate de o entitate străină;
[34] Un program de monitorizare și o emisiune de televiziune de succes în care un grup de persoane trăiesc în aceeași casă, izolați de exterior și urmăriți permanent de camere video.

La rândul lor, statele țintă pot reacționa fie prin contraatacuri cibernetice, fie prin sancțiuni economice, iscându-se astfel tensiuni geopolitice greu de controlat. [49]

Astfel, atacurile cibernetice pot avea multiple efecte potențiale, ce variază de la pierderi financiare imediate și perturbări de servicii, până la schimbări majore în dinamica politico-socială ori militară. [51] Tehnologia digitală, deși un declanșator al progresului, se dovedește a fi și un spațiu al vulnerabilităților profunde, necesitând investiții constante în soluții de securitate și programe de educație menite să reducă factorul de risc uman. [50] Cooperarea internațională, schimbul de informații și dezvoltarea unor cadre juridice ferme reprezintă elementele esențiale pentru gestionarea adecvată a efectelor atacurilor cibernetice și pentru protejarea intereselor comune, atât la nivel național, cât și global. [48]

2.5. Politici și reglementări privind securitatea cibernetică.

Securitatea cibernetică reprezintă astăzi un element esențial pentru funcționarea adecvată a societății și pentru prosperitatea economică, într-o lume în care tehnologia digitală a devenit un motor al inovației și dezvoltării. Conexiunile crescute aduc avantaje semnificative, însă, în egală măsură, expune statele, organizațiile și indivizii la o serie de riscuri cibernetice, precum atacuri informatice, furt de date și perturbări operaționale. În acest context, politicile și reglementările în domeniul securității cibernetice au dobândit un rol central, contribuind la menținerea echilibrului între progresul tehnologic și protejarea drepturilor fundamentale. [55]

O serie de documente internaționale și europene subliniază că managementul riscurilor digitale trebuie să fie unul strategic, integrat și orientat spre protejarea intereselor economice și sociale. [56] Din punct de vedere economic, protejarea infrastructurilor și a datelor sensibile facilitează încrederea utilizatorilor în serviciile digitale și încurajează investițiile în inovație, comerț electronic și digitalizare. [57] Și adoptarea unor norme și standarde clare asigură reducerea vulnerabilităților prin stabilirea de mecanisme de colaborare între autorități și sectorul privat. [58]

Pe plan social, asigurarea securității cibernetice consolidează încrederea cetățenilor în guvern și în instituții, protejându-le totodată drepturile și libertățile, inclusiv viața privată și datele personale. [59] Conform unor principii fundamentale, cum ar fi cele din Convenția de la Budapesta, care reglementează criminalitatea informatică, buna funcționare a spațiului cibernetic se bazează pe cooperare internațională și instrumente legale adaptate la amenințările în continuă schimbare. [60]

Atât la nivel european, cât și internațional, s-au implementat o serie de măsuri pentru contracararea amenințărilor cibernetice. Printre acestea, se evidențiază adoptarea și actualizarea periodică a directivelor care să ofere un cadru mai închegat de coordonare între state și entitățile private.

Directiva NIS 2 reprezintă un text deosebit de relevant în uniformizarea standardelor de securitate în Europa, extinzând domeniul de aplicare al vechii Directive NIS și solicitând statelor membre să-și consolideze măsurile de prevenție, detectare și răspuns la incidente cibernetice. Această directivă încurajează, de asemenea, investițiile în infrastructuri și competențe, pentru a se asigura că entitățile critice, precum furnizorii de servicii de sănătate, transport ori energie, dispun de protecție cibernetică adecvată. NIS 2 pune accent și pe alertarea promptă a incidentelor și pe cooperarea dincolo de frontiere, recunoscând că atacurile cibernetice nu se opresc la granițe. [55]

La nivel internațional, Convenția de la Budapesta rămâne un document fundamental în materie de criminalitate cibernetică, punând bazele unei cooperări judiciare eficiente între state și oferind un instrument legal pentru incriminarea faptelor grave din spațiul cibernetic. Acest tratat facilitează schimbul de informații și probe între autorități, asigurând, totodată, respectarea drepturilor omului și a standardelor privind protecția datelor. [60]

OCDE încurajează statele să considere riscul digital ca pe un element de management general al riscului, recunoscând că majoritatea activităților economice se sprijină pe tehnologii informatice. În acest sens, politicile de securitate cibernetică trebuie integrate în planul strategic al organizațiilor și guvernelor, pentru a spori reziliența și a susține creșterea durabilă. [56]

Analizând documentele menționate anterior, se pot observa similitudini la nivelul textelor înscrise în cadrul acestora, mai exact ce strategii sunt scoase în evidență și direcțiile generale pentru menținerea securității cibernetice: managementul riscului, evaluarea permanentă, cooperarea instituțională și internațională, dezvoltarea competențelor, protejarea drepturilor fundamentale, crearea unor standarde înalte de protecție. Având în vedere enumerarea anterioară, primul punct comun al documentelor este reprezentat de evaluarea riscurilor, fiind recomandate adoptările de politici flexibile și adaptate realităților tehnice și amenințărilor în schimbare. De exemplu, documentul produs de OCDE accentuează importanța unui ciclu de îmbunătățire continuă: identificarea amenințărilor, implementarea măsurilor, monitorizarea și revizuirea periodică. [55, 56]

Pentru cooperarea instituțională și interinstituțională, pentru a combate atacurile cibernetice, se sugerează ca guvernele, companiile private și organizațiile internaționale să lucreze împreună, să facă schimb de informații și bune practici. În acest fel, se creează un răspuns colectiv mai puternic și se limitează impactul atacurilor. [58, 60]

Majoritatea documentelor evidențiază nevoia de a îmbunătăți competențele digitale ale populației și ale angajaților din instituții publice și private pentru combatere. Un factor esențial este conștientizarea pericolelor, de la phishing până la inginerie socială, și asumarea responsabilității personale în protejarea informațiilor. [59]

În plus, protejarea securității cibernetice nu trebuie să intre în conflict cu drepturile și libertățile indivizilor. Atât Convenția de la Budapesta, cât și directivele europene pun accent pe protecția datelor cu caracter personal și pe libertatea de exprimare, cerând măsuri proporționale și transparente. [55, 60]

Documentele oficiale recomandă implementarea de standarde recunoscute internațional, cum ar fi ISO/IEC 27001[35], precum și scheme de certificare care să asigure un nivel ridicat de încredere în serviciile digitale. [56]

Pe măsură ce tehnologii precum inteligența artificială și IoT[36] devin tot mai răspândite, regulamentele și politicile de securitate trebuie să țină pasul cu noile dificultăți. [61] Aplicarea unor algoritmi avansați în prevenirea și detectarea atacurilor ridică însă întrebări legate de etică și confidențialitate. Prin urmare, instituțiile publice și companiile private sunt încurajate să adopte politici clare privind colectarea și prelucrarea datelor, care să respecte drepturile fundamentale și să prevină discriminarea. [59]

Conștiente de riscurile eminente ale posibilelor intruziuni în plan cibernetic, țări precum Germania, România, Africa de Sud, Estonia, Singapore și multe altele, au integrat în sistemul lor legislativ sau și-au însușit norme care asigură protecție.

Germania și-a consolidat cadrul legislativ privind securitatea cibernetică prin Legea privind Oficiul Federal pentru Securitatea Tehnologiei Informației, intitulată BSI-Gesetz sau, mai pe scurt, BSI. Norma stabilește competențele acestei autorități naționale (BSI) în domeniu cibernetic

[35] Este un standard internațional de securitate a informației ce impune un sistem de management al securității informației;

[36] Sau „Internet of Things", ori în română „Internetul obiectelor", este un concept ce presupune folosirea Internetului pentru a conecta între ele diferite dispozitive, servicii și sisteme automate, formând astfel o rețea de obiecte;

și cere implementarea unor standarde ridicate de protecție. Nu numai atât, Germania a adoptat și IT-Sicherheitsgesetz, în anul 2015, care are drept scop principal întărirea măsurilor de protecție cibernetică pentru infrastructurile critice și pentru furnizorii de servicii esențiale. IT-Sicherheitsgesetz a cimentat rolul BSI și a stabilit o serie de obligații și responsabilități clare în ceea ce privește securitatea IT, atât pentru sectorul public, cât și pentru companiile private. Prevede amenzi, obligativitatea raportării incidentelor majore și implementarea de standarde înalte privind securitatea. [62, 63] Mai mult decât atât, Germania a implementat, în anul 2021, IT-Sicherheitsgesetz 2.0, lege care a extins puterea BSI, dorește uniformizarea tuturor reglementărilor din domeniul securității cibernetice, consolidează siguranța sistemelor IT și îmbunătățește protecția consumatorilor. [64, 65]

În România, principalul act normativ, în legătură directă cu securitatea cibernetică, este Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, care transpune directiva europeană NIS 2 în legislația națională și stabilește responsabilități pentru operatorii de servicii fundamentale (energie, sănătate, transporturi etc.) și furnizorii de servicii digitale. Această lege reglementează atât prevenția, cât și reacția la incidente cibernetice, cerând înștiințări rapide și colaborare cu autoritățile. De asemenea, această lege desemnează Directoratul Național de Securitate Cibernetică (DNSC) și Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) ca autorități responsabile pentru asigurarea și monitorizarea respectării măsurilor în vigoare atât în domeniul public, cât și în cel privat. În cazul abaterilor de la cerințele legale, se pot aplica sancțiuni contravenționale, menite să descurajeze practicile neglijente și să stimuleze conformarea. [66, 67] De asemenea, în cadrul legislativ al României, mai există norme care reglemntează aspecte privind securitatea cibernetică, oferundu-i o claritate mai sporită domeniului, respectiv Legea nr. 58/2013. [68] Mai mult decât atât, în cadrul conferinței intitulate ZF Cybersecurity Trends 2025, susținută în data de 14 mai 2025, directorul DNSC, domnul Dan Cîmpean, a oferit informații noi în spațiul public referitor la exercițiile de apărare cibernetică. Cel mai recent astfel de exercițiu a fost unul organizat la nivel internațional instituțional între România, Republica Moldova și Ucraina. Conform mențiunilor sale, este prima acțiune de acest tip care a avut loc la nivel european între diferite state. Această acțiune arată gradul de implicare al României privind domeniul securității, iar cu ajutorul măsurilor efectuate, specialiștii români își dezvoltă cunoștințele pentru a putea consolida legislația internă în legătură cu acest domeniu esențial. [69]

Cybercrimes Act din Africa de Sud aduce o schimbare în modul de abordare a infracțiunilor cibernetice, oferind un cadru legal consolidat pentru a combate diversitatea amenințărilor din mediul online. Prin această lege, activități precum accesul neautorizat la date, fraudarea sistemelor informatice, interceptarea ilegală a comunicărilor sau distribuirea de software rău intenționat sunt definite și sancționate. Actul obligă instituțiile statului și companiile private să colaboreze strâns, inclusiv prin partajarea rapidă a informațiilor despre atacuri cibernetice și respectarea cerințelor de păstrare și protejare a datelor. Totodată, Cybercrimes Act introduce proceduri mai stricte pentru investigarea și urmărirea penală a infractorilor cibernetici, punând accent pe protejarea drepturilor fundamentale și pe echilibrul dintre securitate și libertățile individuale. [70, 71]

Făcând un salt pe continentul asiatic, Cybersecurity Act 2018 din Singapore a fost conceput pentru a asigura o protecție cât mai eficientă a infrastructurilor critice și pentru a reduce vulnerabilitățile generate de digitalizarea extinsă din această țară. Prin intermediul acestei legi, furnizorii de servicii esențiale (transporturi, telecomunicații, energie etc.) au primit responsabilități precise în ceea ce privește menținerea unui standard ridicat de protecție cibernetică, fiind obligați să implementeze măsuri de prevenție și să raporteze imediat orice incident considerabil. Actul îi conferă, totodată, autorității de reglementare competențe sporite pentru a investiga și a opri potențialele atacuri cibernetice la scară largă, precum și puterea de a emite directive tehnice pe care organizațiile vizate trebuie să le respecte. Un aspect deosebit al legii este preocuparea pentru un echilibru între asigurarea securității infrastructurilor și respectarea vieții private a cetățenilor, consfințind principii de transparență și proporționalitate în colectarea și utilizarea datelor digitale. [72, 73]

În anul 2007, Estonia a fost victima unui atac cibernetic timp de 22 de zile, atac provocat de Rusia din cauza disputelor celor două privind relocarea unui monument istoric sovietic. [74] În urma acestui incident, Estonia a contribuit enorm la formarea unei infrastructuri digitale avansate, devenind una dintre cele mai bune țări în materrie de servicii publice digitale. [75] Astfel, și-a îmbunătățit și legislația în legătură cu securitatea cibernetică adoptând Cybersecurity Act în 2018, care completează legislația deja existentă. Legea extinde și detaliază obligațiile operatorilor de servicii și ale instituțiilor publice, cerându-le să implementeze măsuri solide de securitate și să raporteze incidentele care le-ar putea afecta funcționarea. În plus, reglementarea stabilește un cadru de colaborare între autoritățile naționale și sectorul privat, astfel încât amenințările cibernetice să poată fi identificate și gestionate rapid. [76]

Capitolul 3. Studiu de caz: Atacurile cibernetice asupra Ucrainei în contextul războiului ruso-ucrainean din 2022.

Studiul de caz ales, în speță atacurile cibernetice asupra Ucrainei din 2022, reprezintă un exemplu specific și concis care subliniază, în note evidente, impactul pe care un atac cibernetic îl are asupra unui stat și a instituțiilor ce îl coordonează și îi fac posibilă existența.

Incidentele narate în cadrul capitolului de față au schimbat percepția privind conflictele armate deoarece s-a manifestat o extindere a confruntării dincolo de câmpul de luptă fizic în spațiul digital. Deși nu este primul caz de război hibrid, evenimentele petrecute au fost reprezentate de complexitate în utilizarea coordonată a forței armate și a atacurilor cibernetice. Consolidarea conceptului de război hibrid a avut loc odată cu anexarea Crimeei de către Rusia în anul 2014. [77]

În primele luni ale invaziei, Ucraina a fost vizată de o gamă largă de operațiuni cibernetice. Acestea au perturbat funcționarea instituțiilor publice, afectând comunicarea între autorități, sistemele de management al documentelor și portalurile de servicii online destinate cetățenilor. Administrația publică a trebuit să răspundă într-un timp foarte scurt la un context de criză tehnologică și logistică, demonstrând reziliență, dar și descoperirea de vulnerabilități ale sistemelor. [78]

Consecințele acestor atacuri nu s-au limitat doar la daune tehnice. Ele au slăbit temporar capacitatea de coordonare guvernamentală, au afectat încrederea publică în infrastructura digitală a statului și au necesitat o reconfigurare accelerată a arhitecturii de securitate cibernetică. Răspunsul Ucrainei a arătat o mobilizare unică între sectorul public, privat și cetățeni în apărarea spațiului cibernetic național. [79]

3.1. E-guvernarea din spațiul ucrainean.

E-guvernarea a devenit o prioritate majoră în Ucraina zilelor noastre datorită parcursului pro-european al țării. Integrarea Ucrainei în spațiul digital european impune digitalizarea tuturor domeniilor din sfera publică, incluzând administrația. Acest lucru a transformat digitalizarea într-un factor esențial pentru dezvoltarea statului în unul modern, a societății digitale și a unei guvernanțe democratice în Ucraina. Guvernanța electronică este privită nu doar ca instrument de eficientizare administrativă, ci și ca un pas spre integrarea europeană, asigurând deschiderea și personalizarea serviciilor publice la toate nivelurile administrației pentru cetățeni și mediul de afaceri. În acest context, autoritățile ucrainene au demarat, încă din anii 2018-2019, reforme și politici dedicate transformării digitale a sectorului public recunoscând că astfel de măsuri au un rol critic pentru creșterea transparenței, eficienței și calității serviciilor pentru cetățeni. [80, 81, 82]

Transformarea administrației publice din Ucraina a constat în atingerea unor obiective digitale de mare anvergură. Cabinetul de Miniștri al Ucrainei a aprobat în 2018 Proiectul pentru Dezvoltarea Economiei și Societății Digitale 2018-2020, document ce definea digitalizarea ca mecanism de stimulare a dezvoltării unei societăți informaționale. De asemenea, Strategia de Reformă a Administrației Publice 2018-2021 a subliniat importanța e-guvernării pentru îmbunătățirea eficienței sistemului de administrație publică, a transparenței și confortului acestuia. În vederea implementării acestor strategii, în 2019 a fost înființat Ministerul Transformării Digitale[37]. Acest nou minister a lansat inițiativa guvernamentală „Statul în smartphone", menită să transfere în mediul online interacțiunile între stat și cetățeni. Astfel, după numai un an de la înființare, Ministerul a demarat proiecte de e-guvernare la scară națională punând bazele unei administrații publice digitale. [81, 82]

Cel mai emblematic rezultat al transformării digitale ucrainene este platforma de servicii publice Diia[38]. Lansată în 2020 sub denumirea „Statul într-un smartphone", Diia constă într-un singur portal online și o aplicație mobilă pentru accesul facil la documente și servicii administrative electronice. Acest concept înglobează un nou nivel de interacțiune între autorități și cetățeni. Obiectivul principal al Diia este digitalizarea completă a serviciilor publice astfel încât orice serviciu guvernamental să fie disponibil online într-o manieră ușoară și rapidă. Până la sfârșitul anului 2022, rezultatele proiectului erau remarcabile prin prisma faptului că aproximativ 18,5 milioane de ucraineni și-au actualizat aplicația mobilă Diia și peste 21,7 milioane de utilizatori accesau portalul unic al serviciilor publice și îl utilizau. Prin intermediul Diia erau oferite peste 70 de servicii guvernamentale online. Platforma permite stocarea și utilizarea a 14 documente digitale, cum ar fi cartea de identitate, pașaportul electronic, permisul auto, certificatele de naștere sau asigurări. Toate acestea sunt recunoscute cu valoare juridică egală cu cele originale în format fizic. Ucraina a devenit astfel prima țară în care un act de identitate digital este pe deplin valabil și a patra din Europa care a implementat un permis de conducere digital. Prin Diia cetățenii pot partaja copii electronice ale actelor și pot efectua plăți de amenzi sau impozite. [80, 81, 83]

Portalul Diia ilustrează pilonul metamorfozării digitale a administrației publice ucrainene. Numeroase procese birocratice au fost reproiectate pentru a funcționa digital, eliminând birocrația excesivă. Spre exemplu, înregistrarea unei afaceri a devenit un proces record în ceea ce privește rapiditatea oricine poate obține statutul de antreprenor individual în aproximativ 2 secunde și poate înregistra o societate cu răspundere limitată în doar 30 de minute, fiind cea mai rapidă asemenea procedură din lume. Acest serviciu a fost utilizat intens. La începutul anului 2021 erau deja peste 250.000 de antreprenori individuali și 2.500 de companii înregistrate online și, până în 2022, numărul firmelor noi, îbnregistrate digital, a ajuns la 14.000. Tot pe portalul Diia, cetățenii și firmele pot obține diverse autorizații și licențe dorind să ajungă treptat la înregistrarea unei afaceri să devină complet automată. [84]

În paralel, Ucraina s-a remarcat la nivel global și prin digitalizarea serviciilor legate de nașterea copiilor prin serviciul eMalyatko[39] unde părinții pot accesa online până la 9 servicii diferite legate de nou-născuți, de la certificatul de naștere la alocații, fiind nevoie doar de o singură cerere depusă și răspunsul se livrează în 15 de minute. Acest pachet digital pentru nou-născuți poziționează Ucraina printre liderii mondiali în servicii publice pentru părinți demonstrând preocuparea și empatia autorităților de a digitaliza inclusiv evenimentele din viața cetățenilor. [85]

Transformarea digitală a Ucrainei nu s-a limitat doar la servicii pentru populație, ci a vizat și crearea unui ecosistem favorabil economiei prin inovație. În februarie 2022, cu puțin timp înainte de declanșarea războiului , a fost lansat și proiectul Diia.City care reprezintă un cadru juridic și fiscal înfloritor, destinat companiilor IT și start-up-urilor tehnologice. Prin Diia.City, Ucraina și-

[37] Instituție dedicată politicilor de digitalizare a societății;
[38] Acronim din ucraineană pentru „Держава і Ya" sau „ Derzhava i Ya", adică „Statul și Eu";
[39] Tradus în limba română ca „eBebelușul";

a propus să devină cel mai mare hub[40] IT din Europa oferind firmelor din domeniu un regim fiscal ultra-competitiv[41], opțiuni flexibile de colaborare cu specialiști, mecanisme legalizate pentru investiții de capital de risc și alte facilități menite să atragă inovația. Din cauza izbucnirii războiului, Diia.City nu doar că a supraviețuit, ba chiar a crescut vertiginos. La un an de la debut, peste 400 de companii IT s-au alăturat la acest sistem, dintre care 330 s-au afiliat după începerea conflictului, însumând peste 33.000 de specialiști în acest domeniu. Această evoluție reflectă reziliența de necontestat a industriei IT ucrainene care, chiar și în condiții de război, a continuat să evolueze. În primele zece luni din 2022, exporturile de servicii informatice ale Ucrainei au crescut până aparoape de 10% și generând un profit de 6 miliarde de dolari, făcând din IT singura ramură economică în creștere în acea perioadă dificilă. Acest succes al sectorului digital, susținut de politici guvernamentale vizionare, a stimulat și inovația economică contribuind semnificativ la menținerea pe o linie de plutire a economiei în vremuri predispuse la o criză majoră. [86, 87]

Un alt element important al e-guvernării din Ucraina este simbolizat de accentul pus pe alfabetizarea digitală. Pentru ca transformarea digitală să fie benefică întregii societăți, guvernul a investit în programe de formare a competențelor digitale. Ministerul Transformării Digitale a dezvoltat Platforma Națională Online de Alfabetizare Digitală, intitulată Diia.Education. Aceasta are scopul de a instrui cel puțin 6 milioane de cetățeni în utilizarea tehnologiilor digitale de bază. Platforma este structurată sub forma unor serii de videoclipuri educaționale care înglobează diverse niveluri și categorii de competențe: noțiuni elementare de utilizare a calculatorului, securitate online pentru copii, cursuri specializate pentru profesori, antreprenori sau funcționari publici. Până în 2022, Diia.Education înregistrase deja 3,6 milioane de vizitatori, iar 1,2 milioane de ucraineni au parcurs cursurile online și au obținut certificate care atestă competențele lor digitale. La dezvoltarea programei, experții ucraineni au adoptat standarde europene, precum Cadrul European al Competențelor Digitale pentru Cetățeni[42], numit DigComp, asigurând astfel calitatea și relevanța instruirii. Această abordare în sfera educației digitale a extins cu mult baza de utilizatori capabili să acceseze serviciile e-guvernării și să beneficieze de oportunitățile economiei digitale. Totodată, autoritățile au creat și o platformă de învățare online dedicată funcționarilor publici, menită să sprijine dezvoltarea profesională a acestora și să îi familiarizeze cu noile instrumente administrative. [88, 89, 90]

În plus, conducerea Ucrainei au avut în vedere creșterea transparenței și reducerea corupției. Sistemele electronice precum platforma de achiziții publice ProZorro au deschis accesul la datele privind contractele publice permițând identificarea automată a indicatorilor de risc și implicarea societății civile în supravegherea licitațiilor. De exemplu, ProZorro a implementat peste 40 de indicatori inteligenți, având la bază inteligența artificială, care semnalează probabilitatea de corupție în procedurile de achiziții. Aceste instrumente digitale au economisit resurse și au diminuat interacțiunile lipsite de transparență, făcând administrația mai responsabilă. E-guvernarea s-a dovedit a fi un instrument de modernizare a administrației publice prin introducerea soluțiilor IT, a platformelor digitale, a inovațiilor manageriale, a crescut productivitatea și a îmbunătățit comunicarea între instituțiile statului, mediul de afaceri și cetățeni. Aceste evoluții reflectă un nou model de administrație, adică mai deschis, mai eficient și mai centrat pe nevoile cetățeanului. [81, 91]

Procesul de digitalizare din Ucraina nu a fost lipsit de provocări, însă chiar și impedimentele s-au transformat în combustibil pentru e-guvernare. Începând cu 2014, odată cu declanșarea tensiunilor din Crimeea și începerea conflictului hibrid cu Rusia, mediul virtual al Ucrainei a fost supus unui val continuu de atacuri cibernetice menite să perturbe infrastructurile critice și

[40] Spațiu în care ai posibilitatea să lucrezi la proiectele propri, unde ești alături de alte persoane și sunt puse la dispoziție condițiile necesare pentru a lucra eficient;
[41] Prin „ultra-competitiv" este vorba condiții foarte avantajoase din punct de vedere fiscal prin măsuri precum impozite scăzute sau zero, sistem fiscal simplificat, legi fiscale clare și rapide, stimuli fiscali etc.
[42] În limba engleză „Digital Competence Framework for Citizens";

serviciile statului. Cu toate acestea, introducerea digitalizării nu a fost oprită de agresiunea Rusiei. Dimpotrivă, a accelerat implementarea acliunilor progresive necesare furnizării de servicii electronice de calitate și accesibile cetățenilor. Războiul a impus autorităților ucrainene adaptarea rapidă a platformelor digitale pentru a răspunde nevoilor urgente ale populației și armatei. Ministerul Transformării Digitale a extins programul Diia cu opțiuni speciale pe timp de criză. De exemplu, a fost dezvoltat serviciul eDocument pentru eliberarea de documente de identitate digitale în cazul pierderii actelor fizice, au fost create mecanisme pentru acordarea de ajutoare financiare de urgență persoanelor afectate de război și pentru depunerea de cereri de despăgubire privind locuințele sau bunurile distruse, iar cetățenii care au fost obligați să își părăsească casele sau regiunea de reședință au putut beneficia de drepturile aferente tot prin Diia. Iar tot prin intermediul Diia, populația a putut sprijini direct apărarea statului prin donații către armată sau prin accesul la informații oficiale, asigurându-se astfel o mobilizare digitală fără precedent. Aceste măsuri evidențiază capacitatea de adaptare a e-guvernării ucrainene în condiții de criză care a devenit un instrument crucial pentru rezistența națională. [82, 92]

3.2. Contextul războiului ruso-ucrainean.

Ucraina a reprezentat cea de a doua cea mai populată republică a fostei Uniuni Sovietice, cea care și-a proclamat independența în 1991 reușind să grăbească procesul de prăbușire al URSS[43]. După destrămarea Uniunii Sovietice, Ucraina a moștenit un arsenal nuclear pe care a acceptat să îl cedeze în 1994 în schimbul unor garanții de securitate. Prin Memorandumul de la Budapesta[44], Rusia, SUA și Regatul Unit promiteau să respecte suveranitatea și frontierele Ucrainei și să se abțină de la orice agresiune împotriva sa. [93, 94]

După încetarea Războiului Rece[45], NATO s-a extins până în estul Europei, fiind incluse în această alianță militară țări din fosta zonă de influență sovietică[46] și ajungând până aproape de granițele Rusiei. Moscova[47] a perceput această expansiune ca pe o amenințare, acuzând Occidentul[48] că a încălcat garanțiile din anii 1990 privind încetarea expansiunii NATO în fostul spațiu sovietic. Un moment critic al relațiilor internaționale a fost summit-ul NATO de la București din 2008, când aliații luat în considerare aspirațiile euro-atlantice ale Ucrainei și Georgiei, declarând că aceste țări "vor deveni membre NATO". Vladimir Putin[49] a avertizat atunci că aderarea Ucrainei la NATO ar fi "un act ostil față de Rusia", urmat cu câteva luni mai târziu de intervenția militară a Rusiei în Georgia care a demonstrat disponibilitatea Kremlinului[50] de a recurge la forță pentru a-și apăra interesele. [93, 95]

Societatea ucraineană era între orientarea pro-occidentală și orientarea în opoziție, adică cea pro-rusă. Însă, din cauza alegerilor prezidențiale din 2004, care au adus la putere forțe politice pro-occidentale, frustrând planurile Kremlinului de a menține Ucraina în sfera sa de influență. Acest incident a fost denumit ca Revoluția Portocalie. Viktor Ianukovici, candidatul pro-rus învins în 2004, a câștigat alegerile prezidențiale din 2010 și a încercat să reducă apropierea Ucrainei față

[43] Acronim pentru Uniunea Republicilor Sovietice Socialiste, din care au făcut parte și state precum Ucraina, Belarus, Lituania, Letonia, Georgia, Estonia etc.
[44] Acord politic internațional semnat la data de 5 decembrie 1994 prin intermediul căruia Ucraina, Belarus și Kazahstan au renunțat la arsenalul nuclear către Rusia pentru oferirea de către aceasta a unor garanții de securitate;
[45] Perioadă de tensiuni ideologice, geopolitice, economice și militare între SUA și URSS care s-a desfășurat între anii 1947-1991;
[46] Din această zonă au făcut parte România, Polonia, Cehoslovacia, Republica Democrată Germană, Ungaria, Bulgaria, Albania și Iugoslavia;
[47] Capitala fostei URSS și a actualei Federații Ruse;
[48] Termen care face referire la țările din vestul Europei;
[49] Președintele Federației Ruse;
[50] Termen care desemnează guvernarea sau conducerea politică a Rusiei;

de Uniunea Europeană, fapt ce a declanșat o criză majoră. Din cauza presiunii provocate de oficialii de la Moscova, Ianukovici a renunțat în ultima clipă la semnarea Acordului de Asociere cu Uniunea Europeană[51], în timp ce Rusia promova integrarea Ucrainei în noua alianță numită Uniunea Economică Eurasiatică[52]. Decizia a fost percepută ca o trădare și a generat proteste în masă ale mișcării Euromaidan[53] care au dus la înlăturarea lui Ianukovici în februarie 2014. [93]

Conducerea rusă a considerat schimbarea de regim din Ucraina ca o amenințare la adresa intereselor sale. Putin a catalogat revolta drept o tentativă de preluare a puerii de stat orchestrată de Occident. În primăvara aceluiași an, Rusia a atacat militar statul ucrainean prin ocuparea și anexarea Crimeei, eveniment care a reprezentat prima anexare teritorială cu forța în Europa de după al Doilea Război Mondial. Concomitent, în provinciile Donețk și Lugansk[54] au izbucnit revolte separatiste sprijinite de Federația Rusă care a invocat conceptul istoric de „Noua Rusie”[55] pentru a-și justifica implicarea. Conflictul din Donbas s-a transformat într-un război de uzură[56], conflict care a durat 8 ani și a rămas nerezolvat până în 2022. [93]

Nereușind să readucă Ucraina de partea ei pe cale pașnică, Rusia a menținut presiuni constante chiar și după 2014. La rândul său, Ucraina a continuat accederea spre partea occidentală. În acest sens, a extins cooperarea militară cu NATO și a obținut în 2020 statutul de partener NATO cu Oportunități Sporite[57], reafirmându-și oficial obiectivul aderării depline la Alianță. În contrast, Vladimir Putin a invocat insistent legăturile istorice dintre cele două națiuni, afirmând că rușii și ucrainenii formează „un singur popor” și a considerat aspirațiile euro-atlantice ale Ucrainei drept o amenințare existențială la adresa securității Rusiei. Liderii de la Kremlin și-au exprimat deschis îngrijorarea față de securitate europeană de după Războiul Rece spunând că extinderea influenței occidentale în fostul spațiu sovietic că este un risc substanțial pentru Rusia. [93]

În decembrie 2021, Rusia a trimis trupe la frontiera Ucrainei și a oferit țărilor occidentale un ultimatum care s-a referit la încetarea extinderii NATO, retragerea prezenței militare din Europa de Est și garantarea neutralității Ucrainei. Puterile occidentale au refuzat aceste cereri reafirmând politica “ușilor deschise” a NATO. Și într-un final s-a întâmplat inevitabilul. Pe 24 februarie 2022, după eșuarea demersurilor diplomatice, Rusia a declanșat un atac asupra Ucrainei din trei direcții cu scopul declarat de a cuceri Kievul[58] și a înlătura guvernul pro-occidental. Putin a justificat acțiunea ca o “operațiune militară specială” menită să demilitarizeze și să elibereze de naziști Ucraina. Această justificare a reafirmat afirmațiile propagandei ruse despre presupusa amenințare reprezentată de NATO și a comparat conducerea de la Kiev cu regimul nazist. [93, 96]

[51] Tratat ce stabilea cadrul pentru asocierea politică și economică a Ucrainei cu Uniunea Europeană;
[52] Organizație economică regională înființată cu scopul de a integra cât mai multe state din fosta zonă de influență sovietică. A fost creată de Rusia și poate fi considerat un echivalent al Uniunii Europene;
[53] Mișcare formată din proteste și revolte în Ucraina;
[54] Teritorii ucrainiene care fac parte din regiunea Donbas, din estul Ucrainei;
[55] Sau „Novorossiya”, desemnează un concept istoric și geopolitic care făcea referire la teritoriile din sudul actualei Ucraine care au fost anexate de Imperiul Țarist după confruntările armate cu Imperiul Otoman și Hanatul Tătar din Crimeea;
[56] Tipologie de conflict militar care nu are neapărat scopul de a ajunge la o victorie imediată, ci, mai degrabă, încercarea de epuizare treptată a adversarului până când nu mai poate continua lupta;
[57] În limba engleză „Enhanced Opportunities”, noțiune folosită pentru un stat cu statut special care colaborează cu NATO;
[58] Capitala Ucrainei;

3.3. Desfășurarea atacurilor.

Primele semne ale declanșării unui război cibernetic și-au făcut simțită prezența înaintea invaziei propriu-zise a Ucrainei de către Rusia. În data de 13 ianuarie 2022, specialiștii de la Microsoft și autoritățile ucrainene au detectat un malware de tip wiper[59], denumit ulterior WhisperGate[60], integrat în rețelele unor instituții guvernamentale, ONG-uri și companii IT din Ucraina. Acest software era creat să șteargă datele de pe calculatoare sub acoperirea unui fals ransomware, fiind similar cu cel al cazului NotPetya[61]. O zi mai târziu, aproape 70 de site-uri guvernamentale ucrainene, precum cel al Cabinetului de Miniștri, Ministerului Apărării, Afacerilor Externe, Educației și Științei și multe altele, au fost ținte ale unui atac de defacement digitală. Hackerii au compromis paginile Web oficiale, înlocuind conținutul acestora cu un mesaj amenințător în limbile ucraineană, rusă și poloneză. Textul menționa că toate datele personale ale cetățenilor au fost făcute publice și că informațiile de pe computerele compromise au fost distruse fără posibilitate de recuperare. Mesajul reamintea și despre câteba fapte istorice într-o încercare evidentă de a semăna discordie interculturală și panică în rândul populației. Autoritățile din Ucraina au reacționat rapid prin închiderea site-urile infectate și dând curs la o investigație. Serviciul de Securitate al Ucrainei[62] a afirmat că atacatorii au profitat de o breșă de securitate a unei companii private care se ocupa de infrastructura Web a Guvernului și au reușit reușit să modifice conținutul a 10 site-uri. Chiar dacă la momentul respectiv nu a fost nimeni învinuit pentru eveniment, indiciile tehnice au sugerat implicarea unor grupuri de hackeri care colaborau cu serviciile secrete rusești. În plus, Ministerul Transformării Digitale din Ucraina a declarat public că Rusia este responsabilă pentru acest atac cibernetic, făcând astfel prima acuzație oficială din 2022 privind o operațiune cibernetică legată de Rusia. Incidentul din 14 ianuarie a ridicat brusc nivelul de alertă, din îngrijorarea cum că Federația Rusă va recurge la tot mai mult la sabotaj cibernetic împotriva instituțiilor statului ucrainean. [97, 98, 99, 100]

La scurt timp după această întâmplare, atacurile cibernetice au continuat să se intensifice în ceea ce părea a fi începutul unui război de proporții. În zilele de 15 și 16 februarie 2022, și mai multe site-uri guvernamentale, platforme ale unor ministere, pagini Web ale unor bănci de renume[63] în Ucraina și posturi de radio au fost atacate prin Distributed Denial-of-Service care le-a blocat funcționarea timp de câteva ore. Acest atac cibernetic a fost conceput să supraîncarce serverele cu trafic generat automat, a făcut ca serviciile publice online să fie neaccesat și a generat confuzie în rândul ucrainienilor. Guvernul de la Kiev a afirmat despre atac că este o încercare de a răspândi panică și destabilizare, iar imediat după multe state occidentale, cum ar fi SUA și Marea Britanie, au menționat în spațiul public că Serviciul de Informații al Armatei ruse[64] este principalul suspect în acest caz. Aceștia au declarat că Rusia este răspunzătoare de orchestrarea acestui DDoS. [101, 102, 103, 104]

Din nefericire, acesta a fost doar începutul. Chiar cu o zi înaintea invaziei tereritoriale asupra Ucrainei, pe 23 februarie 2022, aceleași site-uri guvernamentale, în special a instituțiilor cu rol deosebit de important în apărare, au fost din nou victimele unor atacuri DDoS și au semnalat o sincronizare clară cu pregătirile militare efective. Mai mult decât atât, tot în ziua de 23 februarie, experții în securitate cibernetică au descoperit declanșarea unui nou tip de malware dăunător în

[59] Program creat pentru a șterge definitiv date dintr-un sistem informatic, recuperarea lor fiind extrem de dificilă sau chiar imposibilă;
[60] Denumit astfel deoarece este greu de detectat și poate produce pagube semnificative și ireversibile;
[61] Este explicat în alt subcapitol intitulat „Alte evenimente internaționale similare";
[62] În limba ucraineană „Slujba Bezpeky Ukrayiny", recunoscut după acronimul SBU;
[63] PrivatBank și Oșadbank;
[64] În limba rusă „Glavnoe Razvedyvatelnoe Upravlenie", având acronimul GRU;

rețelele ucrainene. Era vorba de virusul de tip wiper denumit HermeticWiper[65] care a infectat aproximativ 100 de sisteme din sectorul financiar, IT și de transport aerian. Acest malware era proiectat să șteargă datele și să facă calculatoarele nefuncționale, pregătind un haos administrativ odată cu începerea războiului. [97, 98]

Valul de atacuri din a doua jumătate a lunii februarie 2022 a arătat că toate acestea au fost o strategie de război hibrid care au fost utilizate de Rusia ca arme complementare pentru a slăbi rezistența instituțională a Ucrainei. Pe 24 februarie 2022 confruntarea militaraă dintre Ucraina și Federația Rusă a început. Rusia a extins frontul de luptă și mai mult în spațiul cibernetic printr-o serie de atacuri coordonate menite să paralizeze comunicațiile și infrastructura informatică a administrației ucrainene. Cu doar o oră înainte ca primele trupe rusești să treacă granița, un atac cibernetic a vizat rețeaua KA-SAT[66], satelit ce asigura servicii de comunicații esențiale în Ucraina. Hackerii ruși au distribuit un malware care a scos din funcțiune un număr extraordinar de mare de terminale de satelit[67] utilizate atât de agențiile guvernamentale ucrainene, cât și de clienții privați din mai multe țări europene. Imediat după, comunicațiile civile și oficiale au avut de-a face cu perturbări și blocaje, iar unii utilizatori au pierdut accesul la internet. Efectele s-au resimțit chiar și în afara Ucrainei deoarece atacul a afectat mii de terminale satelit din state membre UE, precum Franța, Germania, Italia, Polonia, care utilizau KA-SAT. Acest sabotaj cibernetic a reprezentat o strategie concepută să dezorganizeze apărarea Ucrainei și să blocheze fluxul de informații între autorități, forțele armate și cetățeni. Oficialii din diverse state europene au condamnat categoric atacul asupra Viasat ca fiind un act inacceptabil ce exemplifică comportamentul iresponsabil al Rusiei în spațiul cibernetic și în modul de desfășurare al invaziei sale. În lunile următoare, anchete internaționale au confirmat implicarea directă a guvernului rus, iar la 10 mai 2022 Uniunea Europeană, împreună cu Canada și Statele Unite ale Americii, au învinuit Rusia pentru acest atac. [97, 105]

Concomitent cu sabotarea comunicațiilor prin sateliți, în prima zi a invaziei, Ucraina s-a confruntat și cu altfel de atacuri cibernetice. Diversi operatori de infrastructură IT din partea Guvernului și câteva companii private au raportat infestarea rețelelor cu malware, precum noi variante de wipere ca IsaacWiper[68] și CaddyWiper[69]. Acestea au condus la ștergerea unor date și întreruperi locale în funcționarea sistemelor administrative și financiare. Totuși, datorită pregătirilor prealabile și a cooperării strânse cu experți occidentali, impactul acestor lovituri cibernetice a fost neutralizat, dar n complet. Multe instituții ucrainene își păstraseră copii de siguranță ale datelor, iar echipele de intervenție cibernetică, alături de specialiști americani trimiși în Ucraina pentru a oferi ajutor, au lucrat rapid pentru a identifica și elimina malware-ul introdus. Per total, primele 24 de ore ale războiului au demonstrat că strategia Moscovei a fost de a sincroniza atacurile cibernetice cu operațiunile militare pentru a dezorganiza administrața și societatea ucraineană prin combinarea componentei de război militar clasic și război cibernetic. [101]

Încă un incident relevant este cel din data de 1 martie 2022. În această zi armata rusă a bombardat turnul de televiziune din Kiev, iar mai multe companii de media și comunicații din capitala Ucrainei au avut de suferit din cauza unor atacuri cibernetice. Sistemele IT ale unor rețele de televiziune locale au fost compromise, fișierele au fost șterse și au fost raportate furturi de date sensibile. În următoarea zi, serviciile de securitate cibernetică au detectat prezența unor hackeri în rețeaua informatică a companiei nucleare de stat[70] unde, un grup rusofil, încerca să se infiltreze

[65] Denumirea provine de la faptul că s-a utilizat o semnătură digitală falsă pentru a valida fișierul compromițător, emis de o companie fictivă numită Hermetica Digital Ltd.;
[66] Satelit european de comunicații, deținut de compania Viasat;
[67] Echipament care permite trasmiterea și receptarea semnalelor între un utilizator și un satelit;
[68] Denumirea provine de la unul din fișierele care alcătuiau malware-ul deoarece conținea cuvântul „Isaac”, iar cercetătorii l-au folosit pentr a-i pune o etichetă;
[69] Explicație similară în nota de subsol nr. 65;
[70] Intitulată oficial „Energoatom”;

cu scopul de a pregăti un act de sabotaj la adresa celei mai mari centrale nucleare ale Ucrainei. În paralel, grupări de hackeri aliate cu Belarusul au lansat atacuri de tip phishing asupra instituțiilor ucrainene. CERT-UA[71] a avertizat că pe 25 februarie a fost descoperită o încercare a hackerilor din Belarus de a sparge conturile de email ale unor ofițeri din armata ucraineană, folosind mesaje capcană pe care le-au trimis, în numele acestora, prin intermediul altor email-uri către alte contacte. De asemenea, același grup ar fi preluat și din comunicațiile militare ucrainiene pentru a le folosi într-o campanie de phishing împotriva unor oficiali guvernamentali din țări membre UE care sprijineau Ucraina. [106, 107, 108, 101]

Oprirea unui alt incident cibernetic, cu impact deosebit de grav dacă avea loc, s-a întâmplat în prima parte a lunii aprilie 2022. Hackerii grupării Sandworm[72] au încercat să provoace un black-out în Ucraina. Ei au atacat rețeaua ce distribuia energia electrică prin introducerea unei variante noi de malware industrial, denumit Industroyer2. Acesta viza sistemele de control ale unor stații de conversie electrică. Atacatorii reușiseră să pătrundă, în primă fază, în rețeaua de birouri IT a companiei energetice și apoi să treacă la rețelele sale industriale SCADA[73] și ICS[74], unde au încercat să manipuleze echipamentele pentru a cauza o pană generală de curent. Din fericire, echipa de răspuns a CERT-UA, ajutată de experții firmei slovace ESET[75], a depistat la timp malware-ul și a blocat executarea lui înainte să producă daune propriu-zise, protejând astfel rețeaua electrică de o potențială întrerupere. Acest incident a demonstrat atât capabilitățile avansate ale hackerilor ruși de a ținti infrastructura critică, cât și gradul sporit de pregătire și vigilență atins de apărarea cibernetică ucraineană. În paralel, în ziua de 8 aprilie a anului 2022, concomitent cu bombardarea gării din Kramatorsk[76] de către armata rusă, hackerii Sandworm au lansat atacul cibernetic împotriva rețelei electrice ucrainene menționat anterior. [97, 109, 110, 111]

Câteva zile mai târziu, pe 22 aprilie, site-urile și sistemele informatice ale Poștei Naționale Ucrainene[77] au fost ținta unui atac DDoS care a întrerupt pentru o perioadă serviciile de livrare și platformele de monitorizare a coletelor poștale . Atacul a venit chiar în momentul unui transport masiv de colete și ajutoare umanitare, dar serviciile au revenit online după ce specialiștii au combătutacșiunea declanșată. În general, luna aprilie a evidențiat o schimbare a focalizării atacurilor ruse deoarece, inițial, s-au efectuat lovituri haotice, iar mai apoi s-au concentrat pe puncte de atac cu adevărat valoroase, de pildă rețeaua energetică, telecomunicațiile și transporturile. [112]

Alt atac pe frontul virtual s-a petrecut pe 7 mai 2022 când hackerii au vizat serverele Consiliului Local din Odesa exact în perioada în care orașul suferea un bombardament cu rachete asupra cartierelor rezidențiale. Practic, în vreme ce rachetele loveau infrastructura fizică, atacul cibernetic a încercat să paralizeze infrastructura administrativă locală prin blocarea site-urilor guvernamentale și a rețelelor interne ale primăriei, îngreunând comunicarea de urgență cu cetățenii. Două zile mai târziu, pe 9 mai, hackerii pro-ruși au inițiat un alt atac de tip DdoS. De data aceasta, împotriva unor operatori de telecomunicații ucraineni cu scopul de a bloca și redirecționa traficul de internet din anumite zone ocupate. Atacul urmărea crearea unei cenzuri în regiunile aflate sub control rusesc, izolându-le de restul Ucrainei și proiectând propagandă pro-rusă. Aceste acțiuni din luna mai au indicat încă o dată că pentru Rusia, frontul cibernetic, este un instrument important de război. Datele colectate de NATO până la 16 mai indicau că atacurile

[71] Computer Emergency Response Team of Ukraine, echipa națională de răspuns incidente cibernetice a Ucrainei;
[72] Grupare de hackeri care aparțin GRU (Serviciul de Informații al Armatei din Rusia);
[73] Acronim pentru Supervisory Control and Data Acquistion, sistem specializat în monitorizare și control la distanță;
[74] Acronim pentru Industrial Control System, se referă la toate sistemele industriale de control;
[75] Companie specializată în securitate cibernetică cu sediul în Bratislava, Slovacia;
[76] Oraș industrial din Ucraina, situat în regiunea Donețk;
[77] În ucraineană „Ukrposhta”;

cibernetice ruse făceau parte din invazia militară, dar nu au cauzat efecte catastrofale în afara granițelor Ucrainei, deși exista mereu riscul extinderii acestora în spațiul european. Comunitatea internațională a rămas în alertă, conștientă că astfel de atacuri asupra infrastructurilor critice pot produce efecte cu propagare neintenționate în țări vecine, punând în pericol securitatea cetățenilor europeni. [98, 105]

Războiul cibernetic din Ucraina nu s-a desfășurat doar dintr-o singură direcție. Pe lângă eforturile defensive, Ucraina și susținătorii ei au trecut la atac în spațiul cibernetic, mobilizând o comunitate globală de hackeri de partea sa. Guvernul de la Kiev a încurajat formarea unei „Armate IT", adică o rețea de voluntari alcătuită atât din experți, cât și amatori în domeniu care să ajute la protejarea rețelelor naționale și, uneori, să pătrundă în sistemul online rusesc. Conform autorităților, o multitudine de voluntari s-au alăturat acestei cauze colective în spre apărarea cibernetică a statului ucrainean. Totodată, gruparea de hackeri Anonymous[78] a declarat război digital împotriva Federației Ruse lansând numeroase acauri spre infrastructura IT a acesteia. Sub conducerea grupului Anonymous, hackeri din lumea întreagă s-au mobilizat pentru a demara atacuri care au indisponibilizat site-uri guvernamentale rusești, au desecretizat arhive confidențiale aparținând instituțiilor de la Moscova și chiar au întrerupt pentru scurt timp transmisia unor televiziuni de stat pentru a difuza imagini reale din război. [97, 101]

Aceste contraatacuri cibernetice coordonate de Ucraina și susținătorii lor au avut mai multe efecte. Mai întâi, au produs pagube și neajunsuri inamicului prin întreruperea serviciilor financiare (plăți online, tranzacții bancare), expunerea publică a unor informații confidențiale despre instituții, oficiali și despre operațiunile militare ale Rusiei. De exemplu, hackeri pro-ucraineni au sustras și publicat arhive de emailuri aparținând Ministerului Apărării din Rusia, date despre producția de energie și despre campaniile de propagandă ale Moscovei, ba chiar și liste cu ofițeri ai Serviciului Federal de Securitate[79]. Această divulgare de informații a fost menită să pedepsească Rusia pentru agresiune și să furnizeze material pentru contracararea dezinformării. În plus, valul de atacuri asupra infrastructurii digitale rusești a avut un efect psihologic și strategic pentru că a spulberat concepția greșită cum că securitatea cibernetică a Rusiei este de neatins. Dacă înainte de conflict experții considerau Federația Rusă o super-putere cibernetică, aproape intangibilă, succesele hacktiviștilor de a perturba sau penetra sisteme guvernamentale ruse au demonstrat contrariul. [98]

La nivel internațional, NATO și UE și-au intensificat cooperarea cu Ucraina în domeniul securității digitale. NATO a inclus Ucraina în Centrul de Excelență Cibernetică de la Tallinn, iar Uniunea Europeană a inițiat activitatea unei echipe de reacție cibernetică rapidă și să trimită în Ucraina specialiști pentru a ajuta instituțiile de la Kiev să facă față atacurilor digitale. Acest ajutor, alături de furnizarea de echipamente și cunoștințe practice occidentale, a dezvoltat capacitatea Ucrainei de a răspunde eficient la incidente. Pe lângă sprijinul tehnic, UE a recurs și la sancțiuni pentru a pedepsi comportamentul agresiv în spațiul cibernetic. Din 2019, Consiliul UE a instituit un regim de sancțiuni cibernetice folosit pentru a sancționa și trage la răspundere infractorii cibernetici. După începerea războiului efectiv, Parlamentul European a dorit utilizarea acestui set de sancțiuni împotriva celor responsabili de atacurile asupra Ucrainei și îmboșățirea de mijloace de aajutor pentru a împământeni rezistența la atacurile cibernetice desfășurate asupra Ucrainei. Într-o rezoluție din iunie 2022, Parlamentul a subliniat că apărarea cibernetică a Ucrainei este strâns legată de securitatea europeană și a îndemnat statele membre să își acorde sprijinul în acest domeniu. [113, 114]

[78] Grupare globală, independentă de hackeri care acționează în numele libertății de exprimare, al transparenței și împotriva abuzurilor;
[79] Cunoscut și sub acronimul FSB, în limba rusă „Federalnaia slujba bezopasnosti", echivalentul SRI din România;

Desfășurarea atacurilor cibernetice în conflictul din Ucraina evidențiază rolul critic al dimensiunii cibernetice în războaiele moderne și importanța rezilienței digitale. Campania condusă de Rusia a avut în compunerea sa unele dintre cele mai agresive și diversificate forme de incursiuni cibernetice văzute până în acel moment. Cu toate acestea, este de remarcat și apreciat rezistența Ucrainei, chiar dacă astfel de evenimente nu i-au fost străine din cauza atacurilor petrecute anterior războiului, acumulând o experiență în ceea ce privește modalitățile de operare și de împiedicare a acestor forme de atac. Încă un lucru ce poate fi de admirat este sprijinul substanțial oferit de statele partene, care au întins „o mână de ajutor" Ucrainei. În pofida eforturilor, susținute de oponentul rus, duse de grupările de hackeri bine pregătite, Ucraina a reușit să se mențină funcțională în majoritatea infrastructurilor critice și să se recupereze după incidente, adaptându-se încontinuu în funcție de tacticile abordate de adversar. Totodată, conflictul a scos în față capacitatea de mobilizare a actorilor neinstituționali (cu referire la indivizi) în spațiul cibernetic din ambele tabere ale conflictului. Pe măsură ce războiul a continuat, amenințarea cibernetică a rămas, totuși, prezentă și de temut. Însă, exemplul Ucrainei arată că prin pregătire, solidaritate care transcede frontierele și o reacție rapidă, efectele celor mai grave atacuri pot fi atenuate. [115]

Pe perioada 1 ianuarie 2022 până la data de 31 decembrie 2022, numărul înregistrat de atacuri cibernetice asupra Ucrainei, în funcție de sectorul de activitate, a fost următorul:

- Administrație Publică: 71;
- Tehnologia Informației și Comunicațiilor: 23;
- Energie: 14;
- Finanțe: 23;
- Asupra cetățenilor: 17;
- Media: 30;
- Transport: 16.

Cifrele consemnate anterior reprezintă doar o parte din suma totală de atacuri cibernetice suferite de Ucraina. Totalul de incidente înregistrate este de 231, atacuri de mai multe tipologii și din diverse domenii(precum cele menționate mai sus). [116]

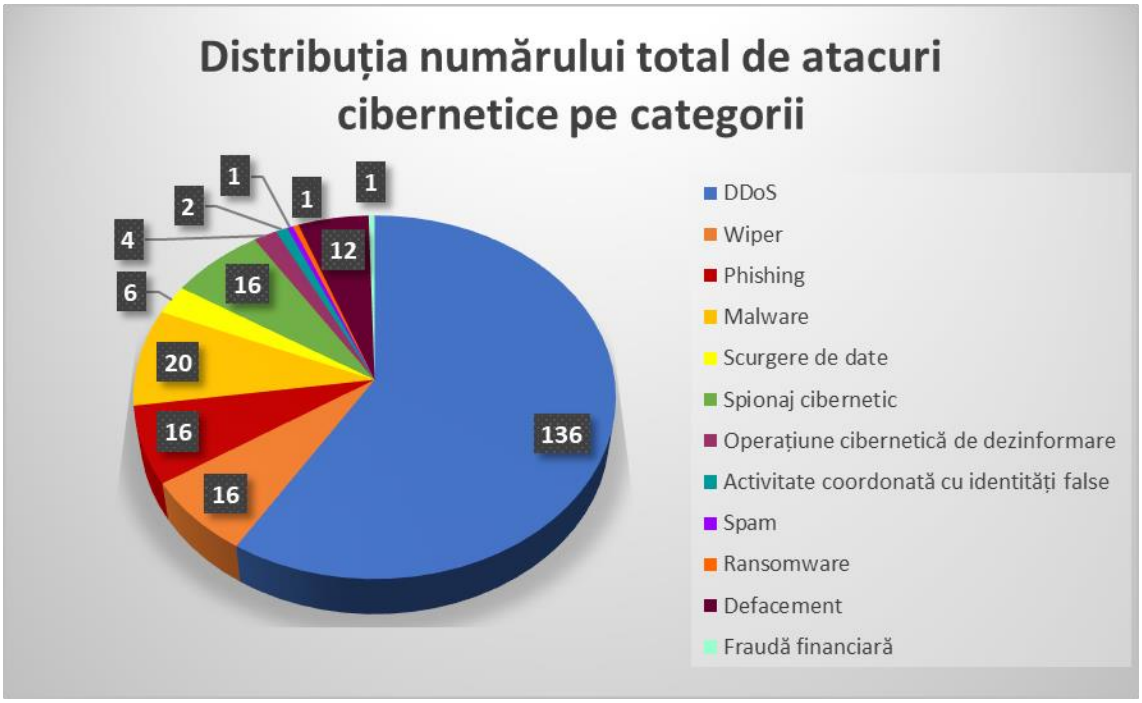

Fig. 2. Distribuția numărului total de atacuri cibernetice pe categorii.
Sursa: https://cyberconflicts.cyberpeaceinstitute.org/impact/geography

3.4. Alte evenimente internaționale similare.

Administrațiile publice din întreaga lume au fost ținta unor incidente cibernetice grave pe parcusul anilor. Aceste atacuri au dezvăluit vulnerabilități importante ale infrastructurilor digitale ale administrațiilor și au oferit lecții semnificative despre rezistența cibernetică. În continuare, vom încerca să analizăm mai multe asemenea evenimente remarcabile, de la atacuri cibernetice planificate de state până la atacuri de ransomware care au blocat servicii publice vitale. Se vor evidenția contextul, participanții, consecințele și lecțiile învățate din fiecare caz. [117, 118]

Un prim exemplu notabil îl constituie atacul Stuxnet din anul 2010 asupra Iranului, care a fost considerat prima armă cibernetică cunoscută. Malware-ul a distrus în mod fizic o parte semnificativă a centrifugelor utilizate în instalația Natanz[80] pentru exploatarea uraniului, având ca efect distrugerea fizică a unei părți dintre acestea. Deși nicio țară nu și-a asumat oficial responsabilitatea, investigațiile au indicat că Stuxnet a fost rezultatul unei operațiuni comune americano-israeliene, având ca scop întârzierea programului nuclear iranian. Impactul a fost major deoarece aproximativ o cincime din centrifugele Iranului au fost scoase din funcțiune, demonstrând în premieră că un atac cibernetic poate produce pagube fizice considerabile. Acest incident a marcat o schimbare de concepție în domeniul securității cibernetice, evidențiind potențialul armelor de nivel digital și stimulând Iranul să-și consolideze capacitățile ofensive și defensive în spațiul cibernetic. Totodată, Stuxnet a ridicat probleme etice și strategice la nivel global, arătând că instituțiile publice, cu precădere infrastructurile critice de stat, pot fi ținte ale unui atac cibernetic, ceea ce necesită mai multă prudență și cooperare globală. [118, 119]

În perioada 2014-2015, o serie de probleme majore de securitate au scos la iveală vulnerabilitățile semnificative ale administrației occidentale. Un exemplu relevant în acest sens este reprezentat de compromiterea Office of Personnel Management[81] din Statele Unite în anul 2015. OPM, agenția responsabilă de gestionarea datelor personalului guvernamental american, a suferit un atac cibernetic care a inclus furtul de date, considerat ca fiind acțiunea unor hackeri plătiți și susținuți de China. Pe parcursul acestui atac persistent, care s-a derulat probabil pe parcursul a doi ani înainte de descoperire, atacatorii au reușit să sustragă informații extrem de sensibile aparținând unui număr enorm de indivizi. Printre datele compromise s-au numărat aproximativ 4,2 milioane de fișe ale angajaților federali și dosarele de anchetă privind autorizațiile de securitate ale peste 21 de milioane de persoane, care conțineau detalii personale, inclusiv coduri numerice personale[82], adrese de domiciliu, rapoarte financiare și medicale, dar și amprentele digitale a aproximativ 5,6 milioane de persoane. Magnitudinea atacului a fost, fără doar și poate, una extrem de gravă, reprezentând un risc major la adresa securității naționale a SUA. Datele furate puteau fi folosite pentru spionaj, șantaj sau periclitarea identității oficialilor. Atacul a avut consecințe imediate asupra conducerii OPM și a generat o investigație congresională de amploare, concluziile fiind că atacul ar fi putut fi prevenit prin măsuri de securitate mai stricte. Lecțiile învățate au subliniat necesitatea modernizării sistemelor IT guvernamentale, adoptării principiilor de tip „zero trust”[83] și adoptarea unei politici ferme de securitate cibernetică în agențiile federale pentru a reuși să protejeze mai bine bazele de date ce conțin informații personale ale funcționarilor publici. [120, 121]

[80] Oraș aflat în statul Iran, în apropierea căruia se află centrul pentr exploatarea uraniului, centru care a preluat aceiași denumire

[81] Prescurtat OPM, în română Oficiul pentru Managementul Resurselor Umane, reprezintă o instituție a Guvernului federal al SUA;

[82] În Statele Unite ale Americii sunt cunoscute sub denumirea de Social Security Numbers (SSN);

[83] model de securitate care presupune că nicio entitate nu este de încredere, iar accesul la resurse este acordat doar după verificări amănunțite;

Tot în anul 2015, o țintă a fost și Parlamentul German[84], într-un atac care a ilustrat capacitatea campaniilor de spionaj cibernetic duse împotriva instituțiilor democratice din Europa. În luna mai, un grup de hackeri aparținând grupării APT28 , asociată serviciului militar de informații al Rusiei, au pătruns în rețeaua informatică a Parlamentului German. Atacatorii au reușit să instaleze malware care le dădea acces continuu în sistemele informatice parlamentare, reușind să exporte aproximativ 16 GB de date confidențiale, inclusiv e-mailuri aparținând deputaților și a altor angajați. Incidentul a alarmat autoritățile germane, fiind nevoie de o refacere riguroasă a infrastructurii IT cu ajutorul Agenției Naționale de Securitate Cibernetică[85]. Serviciul Intern de Informații al Germaniei[86] a menționat public că atacul provine din partea Rusiei, subliniind că scopul principal a fost furtul de informații, doar că astfel de incidente fac posibil sabotajul pe termen îndelungat. Ca urmare, Germania și-a consolidat politicile de securitate cibernetică la nivelul instituțiilor, inclusiv prin formarea unui comandament cibernetic în cadrul armatei. Totodată, a avertizat probabilitatea de intensificare a războiului hibrid[87] în spațiul european, unde atacurile cibernetice sponsorizate de diverse state pot încearca să destabilizeze procesele ce țin de democrație și infrastructurile critice. [122, 123]

Un alt incident similar a avut loc pe continentul asiatic, cu precădere atacul asupra Ministerului Apărării din Japonia din 2016. La sfârșitul anului 2016, presa japoneză a adus la cunoștință despre o breșă în rețeaua IT a forțelor de apărare. La momentul respectiv, a fost considerată ca fiind una dintre cele mai severe atacuri cibernetice întâmpinate de Japonia. Investigațiile ulterioare întâmplării au evidențiat că hackerii au obținut acces, în primă instanță, de la calculatoarele a două instituții interconectate, mai exact ale Academiei Naționale de Apărare și ale Colegiului Medical al Forțelor de Apărare. Le-au folosit drept pârghii pentru a pătrunde în profunzimea rețelei interne a Ministerului Apărării și a Forțelor de Autoapărare Terestre. Atacatorii au demonstrat un nivel deosebit de avansat de pregătire, afirmând prin fapte suspiciunile că ar fi vorba de o operațiune sponsorizată de un stat deoarece presa începuse să speculeze implicarea unor grupuri APT din China. În urma descoperirii intruziunii, Ministerul a deconectat de urgență sistemele de la internet și a recurs la ample verificări de securitate, refuzând să expună public gravitatea pagubelor sau despre eventualul furt al datelor cu caracter secret. Incidentul a reprezentat un semnal de alarmă pentru Japonia, evidențiind vulnerabilitățile infrastructurii sale cibernetice militare și necesitatea adoptării unei strategii mai ferme de apărare cibernetică. De altfel, în următorii ani, Japonia și-a intensificat cu mult soluțiile de protecție cibernetică, conștientizând că până și rețelele guvernamentale clasificate pot fi penetrate de actori statali bine echipați în cazul în care nu există o supraveghere și pregătire adecvată. [124, 125]

Un alt inicident care a periclitat securitatea cibernetică și a atras atenția globală a fost campania de atac NotPetya care portretizează încă un exemplu dramatic de război cibernetic care a pornit de la un conflict regional și s-a transformat într-o amenințare mondială. NotPetya a debutat în iunie 2017 cu o lovitură ce a vizat infrastructurile guvernamentale și companiile din Ucraina în contextul tensiunilor cu Rusia[88]. Malware-ul de tip ransomware, deghizat ca atare, dar cu scop totalmente distructiv, s-a răspândit rapid printr-o actualizare a unui software fiscal ucrainean utilizat pe scară largă, infectând calculatoarele din ministere, bănci, rețeaua electrică, companii de transport și alte servicii publice esențiale din Ucraina. Odată intrat în rețele, NotPetya a criptat datele sistemelor vizate, însă, spre deosebire de ransomware-ul clasic, nu oferea o cale reală de recuperare, semn că intenția a fost de a provoca daune și nu de a obține recompense financiare. Atacul s-a extins cu rapiditate dincolo de granițele Ucrainei, propagându-se în mod necontrolat

[84] Denumit în limba germană Bundestag;
[85] În limba germană Bundesamt für Sicherheit in der Informationstechnik, prescurtat BSI;
[86] Bundesamt für Verfassungsschutz în germană, având acronimul BfV, fiind un echivalent al SRI;
[87] reprezintă o combinație de tactici convenționale și neconvenționale, cum ar fi dezinformarea, atacurile cibernetice și presiunile economice, folosite pentru a submina stabilitatea unui stat fără a recurge la conflicte armate directe
[88] Aceste tensiuni nu erau recente, ci din anul 2014 când Federația Rusă a anexat Crimeea;

prin intermediul legăturilor comerciale. Numeroase organizații occidentale au fost afectate, cum ar fi companii multinaționale precum Maersk[89], FedEx[90], Merck[91] și alte firme au suferit întreruperi majore ale operațiunilor și pierderi financiare imense. Casa Albă[92] a afirmat mai apoi despre NotPetya că reprezintă „cel mai devastator și costisitor atac cibernetic din istorie", estimând pagubele globale la o medie de 10 miliarde de dolari. Statele Unite, Regatul Unit și aliații lor au atribuit oficial atacul serviciului militar rus[93], considerându-l o acțiune intenționată împotriva Ucrainei, dar cu efecte și la nivel mondial. Pe termen scurt, NotPetya a expus incapacitatea multor organizații de a-și diviza rețelele și de a-și actualiza sistemele la timp. Pe termen lung, a determinat revizuirea polițelor de asigurare cibernetică din cauza pierderilor masive neanticipate și a impulsionat eforturile internaționale de a stabili norme de conduită responsabilă în spațiul cibernetic. Lecția principală a fost că un conflict regional poate avea repercusiuni cibernetice și la nivel globale, evidențiind necesitatea cooperării internaționale în detectarea timpurie a atacurilor și consolidarea apărării cibernetice colective. [126, 127, 128, 129]

Revenind pe continentul american, în 2018 și 2019, amenințarea ransomware-ului îndreptat împotriva administrațiilor locale a devenit o realitate prin intermediul a două cazuri reprezentative, respectiv în orașele Atlanta și Baltimore. Pe 22 martie 2018, sistemele informatice ale orașului Atlanta au fost impactate de un atac ransomware de tip SamSam[94]. Malware-ul a criptat fișierele a aproape 3.800 de echipamente și servere municipale în câteva ore. Acest lucru a blocat multe servicii locale, inclusiv mandatele de arest și sistemele de plată online ale utilităților. Atacatorii au cerut o răscumpărare de aproximativ 50.000 de dolari în Bitcoin[95] pentru deblocarea tuturor sistemelor. În ciuda refuzului autorităților din Atlanta de a plăti, această decizie a avut o consecință considerabilă, mai exact restaurarea și securizarea sistemelor compromise au fost extrem de costisitoare. Orașul a cheltuit peste 2,6 milioane de dolari în săptămânile următoare pentru contracte de urgență pentru răspuns la incident, asistență tehnică și consultanță, iar costurile totale de recuperare au depășit în cele din urmă 10 milioane de dolari. Departamentul de Justiție al Statelor Uniteale Americii a acuzat două persoane de naționalitate iraniană de orchestrarea atacului, în absența acestora. Cazul din Atlanta a demonstrat cât de vulnerabile erau infrastructurile IT ale autorităților locale și a transpus importanța sunt practicilor de „igienă cibernetică", cum ar fi implementarea de actualizări regulate ale sistemelor și parole puternice, precum și salvarea unor copii de siguranță, astfel încât oamenii să poată reface datele fără a plăti pentru răscumpărare. În plus, a arătat o intensificare a eforturilor de cooperare între agențiile de aplicare a legii federale, cu precădere FBI[96] și Secret Service[97], și agențiile locale pentru investigarea și urmărirea penală a persoanelor care lucrează de după frontiere. [130, 131]

Cazul orașului Baltimore din mai 2019 a confirmat că amenințarea ransomware la adresa administrațiilor publice locale nu a fost doar o întâmplare. Un atac masiv cu ransomware

---

[89] Companie multinațională daneză cu sediul în Copenhaga, specializată în transport maritim și logistică. Este unul dintre cei mai mari operatori de transport containerizat din lume;
[90] Companie americană de curierat;
[91] Companie de farmaceutice de origine germană;
[92] Reședința oficială și principalul loc de muncă al președintelui Statelor Unite ale Americii, situată în Washington, D.C.
[93] GRU, acronimul pentru Glavnoe Razvedyvatelnoe Upravlenie, adică Direcția Principală de Informații a Statului Major General al Forțelor Armate ale Federației Ruse
[94] Atac cibernetic țintit și manual, realizat cu ajutorul unei variante de ransomware creată special pentru a cripta date sensibile ale organizațiilor și a cere o răscumpărare în schimbul decriptării acestora;
[95] Este un sistem de plată electronică descentralizat și o monedă digitală;
[96]Biroul Federal de Investigații, agenție federală de investigații a crimelor, aparținând Departamentului de Justiție al Statelor Unite;
[97] Agenție federală de aplicare a legii însărcinată cu desfășurarea de investigații penale și cu asigurarea protecției liderilor politici americani, a familiilor acestora și a șefilor de stat sau de guvern aflați în vizită

(cunoscut sub numele de RobinHood) a avut loc în Baltimore pe 7 mai 2019, ceea ce a dus la deconectarea majorității serverelor municipale, precum și la blocarea accesului la alte sisteme vitale, inclusiv email-ul oficial al orașului. Atacatorii au cerut aproximativ 80.000 de dolari în Bitcoin pentru a reda accesul la informații. Autoritățile locale, exact ca în situația din Atlanta, au refuzat plata, determinând hackerii să blocheze complet sistemele, ceea ce a afectat în mod sever funcționarea orașului. Pentru aproape o lună, localnicii nu au putut plăti online pentru apă, taxe și amenzi, tranzacții imobiliare, servicii de telefonie și e-mail ale primăriei. Recuperarea a fost extrem de costisitoare și foarte lentă deoarece sistemele au revenit în funcțiune abia în iunie. Bugetul orașului a raportat pierderi și cheltuieli de cel puțin 18 milioane de dolari. Aceste pierderi includ atât costurile directe pentru remediere, cum ar fi angajarea experților IT, îmbunătățirea infrastructurii și angajarea personalului suplimentar, cât și veniturile din partea localnicilor din cauza întreruperii serviciilor (cum ar fi întârzierea înregistrării impozitelor și facturilor). Investigatorii independenți au descoperit că atacul din Baltimore nu a implicat neapărat dispozitive de ultimă generație, doar a profitat de deficiențele administrației, cum ar fi sistemele slabe, lipsa de securitate cibernetică a copiilor și sistemele învechite. Evenimentul a provocat critici privind pregătirea cibernetică a orașelor și a dus la inițiative federale pentru a ajuta comunitățile locale să se protejeze de atacurile ransomware și să evolueze din acest punct de vedere. Deci, reziliența organizațională și planificarea continuității operațiunilor (inclusiv proceduri clare de răspuns la incidente și back-up offline al datelor critice) sunt esențiale pentru orice administrație publică în era digitală, indiferent de dimensiunea acesteia. [117, 132]

Pe lângă atacurile țintite direct asupra unor instituții sau orașe, o altă categorie important de menționat se referă la atacurile asupra lanțurilor de aprovizionare software folosite de administrații. La sfârșitul anului 2020, s-a descoperit faptul că un atacator din interiorul statului, printr-o modalitate sofisticată, a compromis actualizările unui software de management de rețea foarte răspândit numit SolarWinds Orion[98], inserând un cod dăunător în versiunile distribuite către mii de clienți, inclusiv agenții guvernamentale din SUA. Atacul, care a avut loc cu o discreție excepțional, a permis hackerilor să obțină acces de tip „backdoor”[99] în rețelele destinatarilor doriți care au și instalat actualizările corupte. Ulterior, a fost confirmat că Serviciul Rus de Informații Externe a fost responsabil pentru operațiune, ceea ce indică o campanie globală de spionaj cibernetic. Impactul a fost enorm, cu peste 18.000 de organizații care au descărcat pachetul compromis, iar câteva sute dintre aceste organizații au fost alese pentru a fi exploatate constant de către atacatori. În Statele Unite, multe agenții federale (inclusiv Departamentele Trezoreriei, Comerțului, Energiei și Justiției), precum și agenții precum DHS[100] și chiar părți din rețelele Pentagonului[101], precum și numeroase companii private importante, cum ar fi Microsoft[102], Cisco[103] și Intel[104], au fost afectate. Atacatorii au sustras cantități mari de date sensibile și au avut acces neautorizat timp de luni întregi, până când problema a fost descoperită în decembrie 2020 de către FireEye[105], victima colaterală a atacului. SolarWinds a arătat că dependența de furnizori terți de software este extrem de periculoasă de asemenea. Chiar și organizațiile care au practici solide de securitate pot fi compromise dacă folosesc software de administrare corupt la sursă.

[98] Platformă de monitorizare și gestionare a rețelelor IT**,** dezvoltată de compania americană SolarWinds. Este folosită pe scară largă de organizații guvernamentale, companii private și instituții din întreaga lume pentru a supraveghea performanța infrastructurii IT;

[99] Metodă de acces ascunsă și neautorizată la un sistem informatic, o aplicație sau o rețea, care ocoleste mecanismele normale de autentificare și securitate;

[100] Acronimul pentru Department of Homeland Security, în limba română Departamentul pentru Securitate Internă;

[101] Sediul central al Departamentului Apărării al Statelor Unite ale Americii

[102] Cea mai mare și influentă companie din domeniul tehnologiei din lume care pune la dispoziție o multitudine de servicii, precum sisteme de operare,

[103] Firmă privată din USA care produce o gamă completă de echipamente de rețea si tehnologiile aferente acestora, fiind lider mondial pe piață;

[104] Companie americană, cea mai mare companie de semiconductoare din lume;

[105] Firmă de securitate cibernetică;

Guvernul american a luat măsuri drastice în răspuns. A fost înființat un grup de coordonare cibernetică la nivel național, au fost emise directive de urgență pentru securizarea rețelelor federale și, în aprilie 2021, SUA au sancționat Rusia ca reacție pentru acest atac la adresa securității. Mai mult decât atât, reformele în politicile de securitate cibernetică ale lanțurilor de aprovizionare au fost accelerate ca urmare a evenimentului. Cerințe mai stricte de transparență și verificare a codului au fost impuse colaboratorilor guvernamentali și a fost promovată ideea de „zero trust" în proiectarea rețelelor federale. SolarWinds a dus la schimbare, demonstrând că atacurile indirecte de la terți de încredere pot ocoli uneori și cele mai bine fortificate sisteme, dacă nu se iau măsuri preventive. [133, 134]

Încă un moment care conchide ideea de bază a subcapitolului se referă la incidente cibernetice îndreptate împotriva administrației publice care au afectat și regiuni din afara spațiului euro-atlantic sau SUA. Un exemplu ilustrativ s-a întâmplat în Costa Rica în 2022, subliniind cât de vulnerabile sunt națiunile din America Latină față de grupurile de criminalitate cibernetică. În aprilie 2022, gruparea Conti[106] a lansat un atac ransomware care a paralizat mai multe ministere și agenții guvernamentale costaricane, inclusiv Ministerul Finanțelor. Utilizând date de logare furate, hackerii au infectat sistemele ministerului cu un malware care a criptat serverele fiscale și cele ale vămilor. Acest lucru a împiedicat guvernul să colecteze taxe, să proceseze plăți și să supravegheze procesele vamale. Prin această mișcare, Conti a sustras o cantitate enormă de date, mai precis sute de mii de Gb[107] de informații despre cetățeni și funcționari, și a amenințat că le va posta pe Internet.Această grupare a mai cerut și o răscumpărare de 10 milioane de dolari care a fost după dublată la 20 de milioane de dolari pentru că guvernul a refuzat să plătească suma inițial propusă. O criză națională fără precedent a apărut ca urmare a atacului cibernetic. Rețelele guvernamentale au fost închise pentru a opri răspândirea infecției, iar președintele din Costa Rica a declarat starea de urgență, făcându-dând Costa Rica prima țară din lume care a luat această măsură în urma unui atac cibernetic. Serviciile publice au fost grav afectate timp de mai multe săptămâni. Într-o încercare de a crește presiunea, hackerii au amenințat chiar cu răsturnarea guvernului și au extins atacurile către companii de stat importante. În iunie 2022, un alt grup de infractori cibernetici a atacat sistemul informatic al Casei de Asigurări de Sănătate din Costa Rica, ceea ce a făcut ca o multitudine de proceduri medicale să fie amânate. În cele din urmă, Costa Rica nu a acceptat șantajul și nu a plătit nicio sumă de bani cerută de grupul infracțional. Mai mult, câteva luni mai târziu, gruparea Conti a dispărut din cauza, sau mai degrabă zis datorită, conflictului dintre Rusia și Ucraina. În urma acestui moment de colaps cibernetic, statele din America Latină au trebuit să-și îmbunătățească strategiile de securitate cibernetică, fiind cele cu un număr extreordinar de redus în rândul specialiștilor pe securitate cibernetică. Costa Rica a reușit să se îndrepte din acest punct de vedere prin sprijinul oferit de Statele Unite care a oferit asistență de urgență guvernului costarican, inclusiv expertiză FBI. Acest lucru a scos în evidență, din nou, importanța colaborării internaționale. Cazul Costa Rica oferă o lecție generală, care poate fi aplicată și altor țări în proces de dezvoltare: digitalizarea accelerată trebuie să fie însoțită de investiții substanțiale în protejarea infrastructurii esențiale și de conștientizarea la nivel înalt a riscurilor, deoarece hackerii, fie că sunt finanțați de state ostile, fie că sunt motivați financiar, vor încerca să exploateze rapid orice breșă a sistemului digital. [135]

Pentru un portret mai bine conturat al situației globale, aceasta este harta lumii (Fig. 1) colorată în funcție de cât de sigure sunt statele din punct de vedere al securității cibernetice. Culoarea maro indică un nivel scăzut de securitate, iar culoarea verde simbolizează un nivel ridicat de securitate.

[106] Una dintre cele mai periculoase și bine organizate grupări de ransomware din lume, activă în special între 2020 și 2022
[107] Gigabiți;

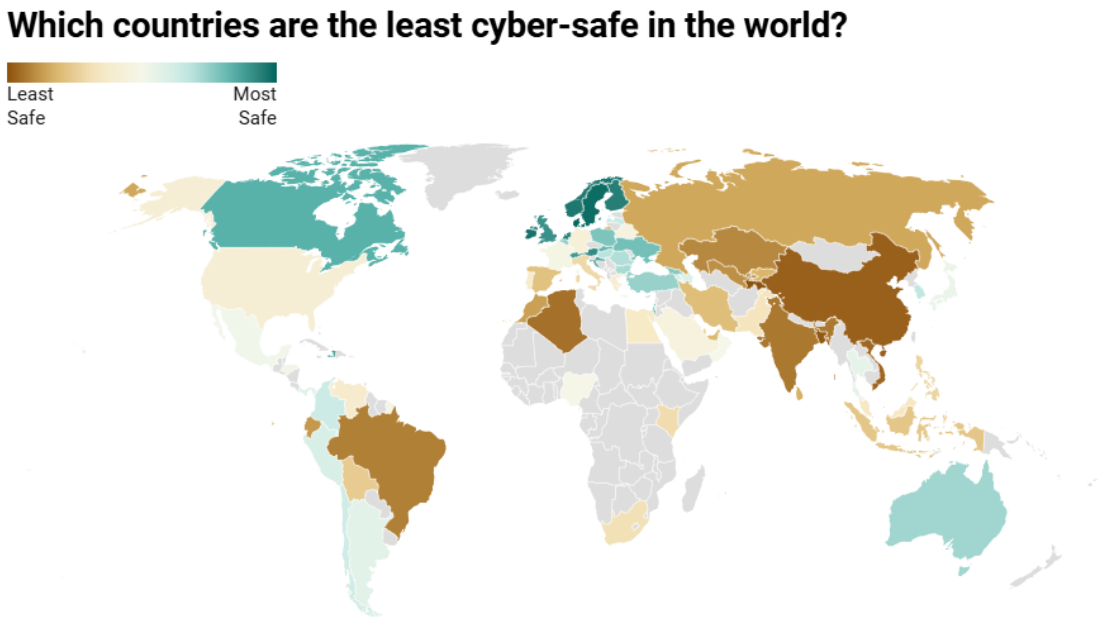

Fig. 3. Harta statelor în funcție de securitate.
Sursa: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Conform studiului efectuat, Tadjikistan ocupă ultimul loc în acest clasament, mai exact este cea mai nesigură țară referitor la securitatea cibernetică, fiind urmată de Bangladesh și China. Fruntașele hărții, cele mai protejate state împotriva atacurilor cibernetice, sunt Danemarca, Irlanda, Suedia, Norvegia și Finlanda. În cadrul acestui studiu s-au luat în considerare procentaje din mai multe categorii: utilizatorii de telefoane și a calculatoarelor infectate cu un tip de malware, utilizatorii atacați de troinei bancari prin intermediul dispozitivelor mobile sau non-mobile, utilizatorii afectați de un ransomware pe dispozitivele mobile sau non-mobile, consumatorii atacați prin surse Web, atacurile Telnet și SSH după țara de origine, atacurile realizate de programe cryptominer, totalul de e-mailuri spam în concordanță cu țara de proveniență, țările vizate de e-mailuri compromițătoare, calculatorele atacate prin phishing, statele cele mai bine pregătite pentru eventuale atacuri cibernetice. [136]

Privind în ansamblu conglomeratul înscris anterior de evenimente internaționale, devine evident că atacurile cibernetice împotriva administrației publice au căpătat o deschidere și complexitate tot mai înaintată, reușind cu succes să traverseze toate regiunile lumii și să facă parte dintr-un paletar larg în ceea ce privește motivele pentru care au loc. Spre exemplu, spionaj, răzbunare geopolitică, sabotaj și acțiuni rău-voitoare din perspectivă financiară. Fiecare incident analizat a scos la suprafață diverse carențe precum: lipsa actualizărilor de securitate, absența copiilor de rezervă, mijloace de protecție inadecvate, neglijarea securității lanțului de aprovizionare. Printre soluțiile care pot fi abordate pentru itensificarea securității se enumără necesitatea unei preocupări constante în securitatea cibernetică guvernamentală, implementarea principiilor de rezistență, întărirea cooperării internaționale în investigarea atacurilor, ajutorul reciproc global și descurajarea atacatorilor prin diferite metode.

Mai presus de toate, aceste cazuri au demonstrat că securitatea cibernetică a administrației publice nu este doar o problemă tehnologică, ci o prioritate strategică ce afectează siguranța națională, încrederea cetățenilor în instituții și buna funcționare a societății moderne.

Recomandări

Recomandările de mai jos derivă direct din constatările cercetării și vizează atenuarea vulnerabilităților identificate:

- Elaborarea și implementarea unei strategii naționale cuprinzătoare de securitate cibernetică deaorece este esențial ca persoanele cu funcții decizionale să stabilească un cadru legal unitar pentru protecția cibernetică a administrației publice. O astfel de strategie ar trebui să definească clar responsabilitățile instituțiilor, să impună standarde minime de securitate pentru toate entitățile guvernamentale și să prevadă mecanisme de cooperare inter-instituțională. Adoptarea unei strategii naționale actualizate, aliniate la bunele practici și directivele internaționale, va reduce fragmentarea și va oferi o direcție clară de acțiune în fața amenințărilor cibernetice tot mai complexe.

- Modernizarea infrastructurilor IT și eliminarea sistemelor depășite constituie încă o soluție potrivită pentru a descuraja și bloca atacurile cibernetice. Pentru a reduce zonele de atac ar trebui ca administrația publică să investească în actualizarea și înlocuirea sistemelor informatice vechite. Menținerea la zi a software-ului și hardware-ului, instalarea rapidă a actualizărilor de securitate și renunțarea la resurse depășite reprezintă condiții principale pentru îmbunătățirea securității. O parte din bugetele statelor ar trebui să fie direcționate către securitatea cibernetică ca domeniu de importanță majoră, permițând achiziția de tehnologii moderne de protecție. Prin înnoirea infrastructurii, vulnerabilitățile asociate sistemelor învechite vor fi eradicate, limitând posibilitățile de infiltrare ale atacatorilor. Totodată, sistemele noi sunt, de obicei, corelate cu mecanisme avansate de securitate, sporind și mai mult nivelul de protecție.

- Încă o măsură preventivă sunt programele de formare și conștientizare pentru angajați. Factorul uman rămâne o verigă slabă în domeniul securității. Din acest motiv, implementarea unor programe de training în domeniul securității cibernetice pentru toți angajații din administrația publică ar constitui o acțiune benefică. Aceste programe ar trebui să includă module de conștientizare privind amenințările informatice, să educe salariații referitor la tipologiile de intruși digitali cu care se pot confrunta (cum ar fi phishing sau alte modalități legate de ingineria socială) și să le menționeze bune practici de gestionare a parolelor și de protecție a datelor. Scopul unei astfel de măsuri este crearea unei culturi organizaționale a securității, în care fiecare angajat să înțeleagă rolul său în protejarea resurselor și datelor. De asemenea, se pot introduce simulări periodice de atac și evaluări ale cunoștințelor constante. Prin intermediul acestor demersuri instituțiile pot identifica punctele slabe și pot îmbunătăți încontinuu nivelul de pregătire al personalului. Rezultatul dorit este reducerea drastică a numărului de incidente cauzate de erori umane, fapt ce va crește reziliența generală a administrației la atacuri.

- O altă recomandare este reprezentată de adoptarea unor standarde și reglementări clare care să ghideze securitatea informațiilor în toate instituțiile publice. De exemplu, implementarea unor cadre de referință recunoscute internațional, precum standardul ISO/IEC 27001, ar oferi o bază comună de cerințe de securitate. Politicile stricte privind controlul accesului la baze de date, managementul autentificării trebuie impuse pentru a reduce riscul pătrunderii neautorizate în rețelele guvernamentale. De asemenea, este necesară instituirea unor protocoale de protecție a datelor (atât a datelor cu caracter personal ale cetățenilor, cât și a datelor administrativeimportante), alături de proceduri de back-up periodic și criptare a informațiilor stocate, astfel încât în eventualitatea unui atac pierderea datelor să fie minimă. Aceste măsuri tehnice și organizatorice ar trebui să devină obligatorii în tot aparatul public, asigurând un nivel de protecție preventiv și ridicat pretutindeni.

- Dat fiind faptul că riscul cibernetic nu poate fi eliminat complet, instituțiile publice trebuie să fie pregătite să reacționeze eficient atunci când un atac are loc. Este recomandată verificărilor periodice de vulnerabilități, dezvoltarea de planuri detaliate de răspuns la incidente și testarea lor prin exerciții simulate. Practici precum formularea de scenarii de atac cibernetic desfășurate cu factorii de decizie. Specialiștii recomandă, de asemenea, implicarea unor experți externi pentru a audita securitatea, a realiza teste de penetrare și a ghida prioritizarea investițiilor în funcție de riscurile identificate. Prin dezvoltarea și exersarea unor planuri puse la punct de răspuns, administrația publică își va spori considerabil rezistența, abilitatea de a absorbi șocul unui atac, de a continua funcționarea serviciilor critice în regim de criză și de a reveni rapid la normal cu un impact minim asupra cetățenilor.

- Amenințările cibernetice depășesc granițele organizaționale și naționale, motiv pentru care colaborarea este un element cheie în fortificarea securității publice. De aceea, este de preferat constituirea unor canale formale de schimb de informații și alerte între instituțiile publice și între state. La nivel național, ministerele și agențiile cu responsabilități în domeniu cibernetic/digital ar trebui să colaboreze îndeaproape pentru un răspuns concomitent și organizat la atacuri. Totodată, parteneriatele internaționale trebuie extinse, în primul rând, pentru o acoperire mai largă și, în al doilea rând, pentru participarea activă la inițiativele deoarece oferă acces la informații actualizate despre amenințări și posibilitatea unor expertize avansate. După cum subliniază analiștii, este din ce în ce mai evidentă nevoia unei intervenții coordonate la nivel statal și internațional pentru a sprijini eforturile de apărare cibernetică. Prin uniunea eforturilor și a resurselor, instituțiile publice pot ține pasul mai eficient cu atacatorii cibernetici care acționează, de obicei, în grupuri bine organizate și la scară globală.

- O recomandare utilă vizează modul în care instituțiile comunică și acționează după producerea unui eveniment cu impact negativ în securitate. Pentru a preveni deterioarea pe termen lung a încrederii cetățenilor, autoritățile ar trebui să adopte politici de transparență care să includă informarea publicului afectat cu privire la natura breșei, la datele compromise și la măsurile luate pentru remediere. Această comunicare de criză trebuie însoțită de acțiuni concrete pentru cetățeni și de asigurări credibile în așa fel încât să se întreprindă pași pentru a împiedica incidente similare în viitor. Recastigarea încrederii se realizează nu doar prin cuvinte, ci și prin fapte, adică instituțiile ar trebui să efectueze anchete amănunțite, să publice rapoarte clare despre cauzele incidentului și să ajusteze politicile interne pentru a corecta deficiențele. O atitudine deschisă și orientată spre asumare și învățare din greșeli poate ajuta la reconstruirea relației cu cetățenii, demonstrând că administrația tratează cu maximă seriozitate securitatea datelor și a serviciilor pe care aceștia le folosesc.

- Iar ca ultimă treaptă de parcurs pentru a consolida securitatea cibernetică în administrația publică se rezumă la sectorul privat și cetățeni. Pentru a nu periclita siguranța digitală națională, fiecare companie și individ, ca entitate singulară, trebuie să își asume răspunderea, pentru documentele sau datele personale care pot fi ținte ale unor atacuri, prin implementarea unor măsuri simple, dar de impact, în vederea prevenirii și combaterii unor evenimente neplăcute. Printre acțiunile ce pot fi întreprinse se enumeră: accesarea de conexiuni de tip HTTPS (nu HTTP), modificarea regulată a parolelor (evitând reutilizarea acestora), utilizarea factorilor de autentificare multiplă, evitarea conectării la rețele de Wi-Fi nesecurizate, efectuarea de back-up în mod constant, instalarea unui program antivirus, refuzarea deschiderii unor link-uri sau e-mail-uri de la adrese suspecte.

Concluzii

În urma cercetării efectuate, se confirmă impactul intens și negativ al atacurilor cibernetice asupra administrației publice, așa cum au anticipat ipotezele inițiale. Incidentele cibernetice au devenit tot mai frecvente și agresive, atacurile asupra instituțiilor publice crescând la nivel global cu aproximativ 40% doar în anul 2023. Consecințele acestor atacuri se reflectă pe multiple planuri, începând de la eficiența operațională a instituțiilor, până la încrederea publicului și necesitatea unor politici adecvate de securitate cibernetică. [137]

Cercetarea, per ansamblu, confirmă cea dintâi ipoteză, conform căreia atacurile cibernetice reduc eficiența instituțiilor publice, perturbând activitățile curente și provocând pierderi de date importante. În lipsa accesului la sistemele informatice sau la datele compromise, funcționarea serviciilor publice este grav afectată, adesea până la paralizare temporară. Astfel de incidente pot bloca baze de date, întrerupe comunicațiile interne și externe și pot genera costuri substanțiale de remediere și pauze operaționale. Un exemplu elocvent este atacul ransomware WannaCry din 2017, care a lovit sistemul public din peste 150 de țări și a forțat Serviciul Național de Sănătate din Marea Britanie să își suspende operațiile medicale. Acest incident a dus la anularea a mii de proceduri și programări și a cauzat pierderi de milioane de lire sterline, evidențiind în mod evident cum un atac cibernetic poate îngreuna cursul activităților unei instituții și compromite date esențiale. Dovezile empirice și studiile de caz analizate arată că atacurile cibernetice au un efect destabilizator major asupra eficienței operaționale a administrației publice, îngreunând prestarea serviciilor și generând pagube materiale și informaționale consistente. [138]

Cea de-a doua ipoteză specifică faptul că instituțiile în care angajații au un grad scăzut de educație digitală sunt mai predispuse atacurilor, iar aceasta este susținută de constatările studiului. Factorul uman s-a dovedit a fi adesea veriga slabă în lanțul securității cibernetice. Lipsa de pregătire și conștientizare a personalului face loc erorilor umane care pot facilita accesul atacatorilor. Erorile sau neglijența angajaților constituie principala cauză în marea majoritate a breșelor de securitate. Până la 95% dintre incidentele de securitate cibernetică implică o componentă de eroare umană. De exemplu, mulți funcționari publici pot fi ținta atacurilor de tip phishing din cauza neatenției sau a lipsei de instruire. Spre exemplu, 86% dintre angajați sunt încrezători că pot recunoaște un e-mail de tip phishing, aproape jumătate dintre aceștia au recunoscut că au căzut în capcana unor astfel de mesaje înșelătoare. Aceste date confirmă că instituțiile cu un nivel redus de cultură de securitate digitală devin ținte mai ușoare pentru atacatori, gradul scăzut de educație digitală amplificând exponențial riscul de succes al atacurilor cibernetice. Prin urmare, investițiile în formarea personalului și crearea unei culturi organizaționale orientate spre securitate devin esențiale pentru diminuarea vulnerabilităților interne. [139]

Ipoteza potrivit căreia lipsa unor politici publice coerente privind securitatea cibernetică duce la o creștere a atacurilor asupra instituțiilor publice este confirmată de cazul Ucrainei. Deși statul a realizat pași importanți în digitalizare, inclusiv prin platforma Diia, absența unui cadru strategic robust a lăsat administrația vulnerabilă. Atacuri masive precum cele cu malware cu potențial imens de distrugere a datelor (HermeticWiper, WhisperGate) și defacement au vizat rețele guvernamentale, afectând funcționarea serviciilor publice și capacitatea de reacție. Fără politici unitare și mecanisme clare de coordonare interinstituțională, răspunsul inițial a fost haotic, necesitând sprijin extern pentru stabilizare. Situația contrastează cu modelul estonian, unde securitatea digitală este tratată ca prioritate națională, integrată în toate politicile publice. Evenimentele relatate în studiul de caz s-au întâmplat în anul 2022, iar abia în acest an, 2025, s-au implementat legi care să vizeze securitatea cibernetică în legătură cu infrastructura critică, informațiile de stat și rețelele Web de stat (Legea nr. 4336-IX). Înainte de implementarea acestei legislații, exista, într-adevăr, o strategie la nivel național, a cărei impunere era planificată în intervalul 2021-2025 de către NCCC[108], care urmărea consolidarea rezilienței cibernetice și

[108] Acronim pentru National Coordation Center for Cybersecurity;

alinierea la standardele europene. Așadar, cazul ucrainean demonstrează că lipsa unei strategii clare expune instituțiile publice unui risc crescut în fața amenințărilor cibernetice. [140, 141, 142]

Ipoteza a patra, conform căreia atacurile cibernetice diminuează încrederea cetățenilor în administrația publică și serviciile acesteia, este de asemenea susținută de concluziile cercetării. Un incident cibernetic major nu are doar consecințe tehnice și operaționale, ci și un impact psihosocial asupra percepției publice. Atunci când datele personale ale cetățenilor sunt compromise sau serviciile publice devin indisponibile din cauza unui atac, cetățenii își pierd încrederea în capacitatea instituțiilor de a-i proteja și deservi. Studiile recente confirmă acest fenomen: expunerea directă la un atac cibernetic produce o scădere abruptă a încrederii publicului în guvern și instituții. De exemplu, în urma unui atac ransomware care a afectat un mare spital din Germania, populația din segmentul expus direct incidentului a manifestat o diminuare semnificativă a încrederii în autorități, mulți percepându-le drept incapabile să îi apere de amenințări viitoare. Aceste emoții de anxietate și indignare cauzate de atac au contracarat orice potențial efect unificator (precum cel întâlnit uneori în situații de criză tradiționale), alimentând în schimb sentimentul că statul nu deține controlul asupra situației. Consecința este o subminare a capitalului de încredere pe care se sprijină relația dintre cetățeni și administrație. Cu fiecare breșă de securitate mediatizată, credibilitatea instituțiilor suferă, ceea ce poate induce reticență în utilizarea serviciilor publice digitale și poate genera presiuni asupra decidenților de a întări măsurile de securitate. [143]

Cea de-a cincea ipoteză, conform căreia folosirea unor sisteme informatice depășite în administrația publică sporește pericolul atacurilor cibernetice, este validată de datele și exemplele înscrise. Infrastructurile IT vechi, neactualizate, prezintă vulnerabilități cunoscute pe care atacatorii le pot exploata cu ușurință. Multe instituții publice operează încă pe sisteme legacy[109] din cauza constrângerilor bugetare sau a inerției administrative. Această situație crește semnificativ probabilitățile de atac cibernetic: lipsa ultimelor actualizări de securitate și a patch-urilor face ca sistemele neîntreținute să fie ținte foarte bune. Infractorii cibernetici profită tocmai de existența tehnologiilor învechite și a resurselor de securitate insuficiente din sectorul public, considerând aceste instituții drept sigure comparativ cu organizațiile private. În practică, s-a observat că multe breșe de securitate de succes exploatează vulnerabilități pentru care existau deja remedii, dar care nu au fost aplicate la timp în sistemele guvernamentale învechite. De asemenea, sistemele mai vechi pot să nu fie compatibile cu soluțiile moderne de apărare, lăsând astfel porțițe deschise pentru intruziuni. Așadar, prezența tehnologiei depășite în infrastructura IT a administrației publice sporește considerabil riscul și potențialul de succes al atacurilor cibernetice, confirmând ipoteza propusă. Una dintre concluziile cheie ale lucrării este necesitatea stringentă de a moderniza infrastructurile informatice guvernamentale ca măsură preventivă de securitate. [144]

Având în vedere cele consemnate anterior, rezultă că toate cele cinci ipoteze de cercetare au fost validate, conturând o imagine de ansamblu în care atacurile cibernetice reprezintă o provocare reală și de speriat pentru administrația publică. Aceste atacuri nu numai că perturbă grav funcționarea instituțiilor și compromit date de mare importanță, dar evidențiază și lacunele în educația digitală a personalului, în strategiile și politicile publice de securitate, în relația de încredere cu cetățenii, precum și în gradul de înnoire tehnologică al aparatului administrativ. În acest context, se impune adoptarea unor măsuri cu caracter strategic la nivel de politici publice pentru a consolida securitatea cibernetică în administrația publică.

Drept concluzie finală a acestei lucrări de licență, impactul atacurilor cibernetice asupra administrației publice este unul complex și profund, resimțit atât în plan operațional, cât și în plan social. Eficiența instituțională poate fi serios compromisă de un singur atac major, încrederea publicului poate fi zdruncinată, iar fără reacții adecvate la nivel legislativ, astfel de incidente tind

[109] Platforme hardware/software ieșite din suportul producătorului.

să se reproliferereze. Cu toate acestea, concluziile lucrării evidențiază și laturile pozitive precum ideea că există soluții și direcții de acțiune clare care pot reduce semnificativ riscurile. Prin adoptarea unor politici publice adecvate și prin alocarea resurselor necesare pentru modernizarea și securizarea infrastructurilor IT, administrația publică poate trece de la vulnerabilitate la reziliență. Numai tratând securitatea cibernetică drept o prioritate de prim rang și integrând-o în cultura și structurile administrației, instituțiile publice își vor putea îndeplini misiunea în mod eficient și sigur în era digitală, protejând atât datele cetățenilor, cât și încrederea acestora în guvernare.

References

[1] K. Andreasson, Cybersecurity. Public Sector Threats and Responses, CRC Press, 2011, p. XIII.

[2] T. J. Holt, A. M. Bossler și K. C. Seigfried-Spellar, „Summary," în *Cybercrime and Digital Forensics. An Introduction*, New York, Routledge, 2018, p. 645.

[3] K. Andreasson, în *Cybersecurity. Public Sector Threats and Responses*, CRC Press, 2011, pp. 1-6.

[4] A. F. Rahmat, C. Vrabie și G. B. Soesilo, „Exploring the Cybercrime Prevention Campaign on Twitter: Evidence from the Indonesian Government," *Smart Cities and Regional Development (SCRD) Journal,* vol. 7, nr. 2, pp. 9-11, 2023.

[5] S. Iftikhar, „Cyberterrorism as a global threat: a review on repercussions and countermasures," *PeerJ Computer Science,* vol. 10, pp. 8-9, 2024.

[6] A. Cărăușu, „Metodologia Cercetării în Științele Administrative, Suport de Curs," 2023.

[7] K. Andreasson, Cybersecurity. Public Sector Threats and Responses, CRC Press, 2011.

[8] T. J. Holt, A. M. Bossler și K. C. Seigfried-Spellar, Cybercrime and Digital Forensics, New York: Routledge, 2018.

[9] M. N. Alenezi, H. Alabdulrazzaq, A. A. Alshaher și M. M. Alkharang, „Evolution of Malware Threats and Techniques: A Review," *International Journal of Communication Networks and Information Security,* vol. 12, 2020.

[10] G. Vaida, „Organizarea administrației publice. Suport de curs," București, 2022.

[11] G. Vaida, „Curs Statul și dreptul," București, 2022.

[12] C. Rădulescu , „Curs 14 BCAP," București, 2024.

[13] C. Vrabie , Elemente de e-guvernare, București: Pro Universitatea, 2024.

[14] D. H. Rosenbloom, R. S. Kravchuk și R. M. Clerkin, „Public Administration: Undestanding Management, Politics and Law in the Public Sector," 2022. [Interactiv]. Available: https://nibmehub.com/opac-service/pdf/read/Public%20Administration%20Understanding%20Management-%20Politics-%20and%20Law%20in%20the%20Public%20Sector%20by%20David%20H.%20Rosenbloom.pdf. [Accesat 23 Februarie 2025].

[15] T. d. M. Cartaxo, J. M. Castilla, M. Dymet și K. Hossain, „Digitalization and smartening susteinable city development: an investigation from the high north European cities," *SCRD,* vol. 5, pp. 88-101, 2021.

[16] European Parliament, „Security of eGovernment Systems Final Report Science and Technology Options Assasment," STOA, 2023. [Interactiv]. Available: https://www.academia.edu/23470217/Security_of_eGovernment_Systems_Final_Report_Science_and_Technology_Options_Assessment?hb-sb-sw=34303517. [Accesat 17 Februarie 2025].

[17] L. S. Beh, M. J. Lee, N. H. Abd Rahman și S. L. Lai, „Smart Cities and Digitalisation: A Research Agenda of Public Administration," *SCRD,* vol. 6, nr. 3, pp. 41-58, Iunie 2022.

[18] S. Sarbu, „About security culture," *SCIC,* vol. 9, pp. 63-69, Aprilie 2023.

[19] A. M. Romanenkov, „Digital public administration infrastructure and its effectiveness," *Personality & Society,* vol. 2, nr. 3, pp. 4-10, 7 Iunie 2021.

[20] I. Lindgren, C. O. Madsen, S. Hofmann și U. Melin, „Close encounters of the digital kind: A research agenda for the digitalization of public services," *Government Information Quarterly,* vol. 36, nr. 3, pp. 427-436, Iulie 2019.

[21] B. Dimeski, „Twenty years of transparency development in the public sector: What has been achieved?," *SCRD,* vol. 2, nr. 2, pp. 9-17, Iunie 2018.

[22] International Organization of Supreme Audit Institutions, „INTOSAI," [Interactiv]. Available: https://www.intosai.org. [Accesat 24 Martie 2025].

[23] C. Schachtner, „Smart government in local adoption - Authorities in strategic change through AI," *SCRD,* vol. 5, nr. 3, pp. 53-62, Iulie 2021.

[24] S. Bretschneider și I. Mergel , „Technology and public management information systems: Where have we been and where are we going," în *The State of Public Administration: Issues, Challenges and Opportunities*, M. E. Sharpe, 2011, pp. 187-203.

[25] J. Olusegun Fayomi și Z. Abdulqadir Sani, „Strategies for transforming the traditional workplace into a virtual workplace in smart cities," *SCRD,* vol. 6, nr. 1, pp. 35-54, 8 Martie 2022.

[26] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke și S. Rallis, „Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures," *ICST Transactions on Security and Safety*, 17 Octombrie 2018.

[27] National Cyber Security Centre, „NCSC," Ianuarie 2016. [Interactiv]. Available: https://www.ncsc.gov.uk/files/common_cyber_attacks_ncsc.pdf. [Accesat 1 Martie 2025].

[28] A. N. Diaconescu, „Transmiterea și protejarea informațiilor în mediul public digital," *SPR,* vol. 1, nr. 1, 1 Iulie 2023.

[29] L. A. Razuleu, „E-Governance and its Associated Cybersecurity: The Challemges and Best Practices of Authentication and Authorization among a Rapidly Growing E-Government," August 2018. [Interactiv]. Available: https://scholarworks.calstate.edu/downloads/mc87pt75n. [Accesat 1 Aprilie 2025].

[30] C. V. Anghel-Drugărin, „e-Guvernarea. Impactul guvernării electronice în administrația publică. Provocări și vulnerabilități ale guvernării digitale," Prouniversitatea, 2022. [Interactiv]. Available: https://www.prouniversitaria.ro/wp-content/uploads/2022/09/ARTICOL-9-Anghel-Dragusin-Cornelia-p.-197-220.pdf.

[31] S.R.I., „Glosar de termeni pentru domeniul securității cibernetice," 12 Septembrie 2019. [Interactiv]. Available: https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf. [Accesat 24 Martie 2025].

[32] Comisia Nationala pentru Controlul Activitatilor Nucleare, „Lege5," 22 Decembrie 2021. [Interactiv]. Available: https://lege5.ro/Gratuit/geydinjvgqyta/normele-privind-protectia-instalatiilor-nucleare-impotriva-amenintarilor-cibernetice-din-07122021?pid=442028885#p-442028885. [Accesat 1 Martie 2025].

[33] M. D. Băjan, „Securitatea Cibernetică în Instituțiile Publice," *SPR,* vol. 2, nr. 1, 8 Iulie 2024.

[34] A. Bendovschi, „Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance,* vol. 28, pp. 24-31, 2015.

[35] Bitdefender, „DNSC," [Interactiv]. Available: https://dnsc.ro/vezi/document/ghid-virusi-troieni-viermi. [Accesat 1 Martie 2025].

[36] ENISA, „ENISA Threat Landscape," 2024. [Interactiv]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. [Accesat 13 Martie 2025].

[37] A. Bogoni și B. F. Fabregue, „Privacy and Security Concerns in the Smart City," *Smart Cities,* vol. 6, nr. 1, 10 Februarie 2023.

[38] „Bitdefender," Bitdefender Business Solutions Group , [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-zero-day-vulnerability. [Accesat 1 Martie 2025].

[39] Bitdefender, „Ce este un atac Man-in-the-Middle?," Bitdefender, [Interactiv]. Available: https://www.bitdefender.ro/consumer/support/answer/79586/. [Accesat 11 Mai 2025].

[40] Cloudflare, „Why is HTTP not secure? | HTTP vs. HTTPS," Cloudfalre, [Interactiv]. Available: https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/. [Accesat 11 Mai 2025].

[41] I. Luknar și F. Jovanovic, „Various types of cyber threats," *Srpska politička misao,* vol. 83, nr. 1, pp. 161-177, Ianuarie 2024.

[42] O. A. Sarcea (Manea), „AI & Cybersecurity - connection, impacts, way ahead," *TRUST,* vol. 1, p. Iulie, 16 Iulie 2024.

[43] D. de Sola, „U.S. agencies warn unauthorized employees not to look at WikiLeaks," CNN, 4 Decembrie 2010. [Interactiv]. Available: https://edition.cnn.com/2010/US/12/03/wikileaks.access.warning/index.html. [Accesat 11 Aprilie 2025].

[44] A. Smith , „The internet gives citizens new paths to government services and information," Pew Research Center, 27 Aprilie 2010. [Interactiv]. Available: https://www.pewresearch.org/internet/2010/04/27/government-online/. [Accesat 11 Aprilie 2025].

[45] I. Traynor , „Russia accused of unleashing cyberwar to disable Estonia," The Guardian, 17 Mai 2007. [Interactiv]. Available: https://www.theguardian.com/world/2007/may/17/topstories3.russia. [Accesat 11 Aprilie 2025].

[46] P. W. SINGER și A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.

[47] S. Baldi, E. Gelbstein și J. Kurbalija, „Hacktivism, Cyber-terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace," 2003.

[48] S. Iftikhar, „Cyberterrorism as a global threat: a review on repercussions and countermeasures," *PeerJ Computer Science,* 15 Ianuarie 2024.

[49] M. Baezner și P. Robin, „Publicații: Rapoarte de risc și rezistență," Octombrie 2017. [Interactiv]. Available: https://css.ethz.ch/. [Accesat 24 Martie 2025].

[50] T. Vaisanen, A. Farar, N. Pissanidis, C. Braccini, B. Blumbergs și E. Diez, „CCDCOE," 2015. [Interactiv]. Available: https://ccdcoe.org. [Accesat 23 Martie 2025].

[51] E. V. Cobos și S. Cakir, „A review of the Economic Costs of Cyber Incidents," 24 Septembrie 2024. [Interactiv]. Available: https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf. [Accesat 18 Aprilie 2025].

[52] O. Tsaruk și M. Korniiets, „Hybrid nature of modern threats for cybersecurity and information security," *SCRD,* vol. 4, nr. 1, pp. 57-78, 21 Martie 2020.

[53] B. Wittes și G. Blum, The Future of Violence: Robots and Germs, Hackers and Drones, Basic Books, 2015.

[54] D. C. Preda și M. M. Frangulea, „The Symbiotic Threat of Human Error, Intended Action and Cybernetic Security System," *SCIC,* vol. 10, pp. 407-416, 2023.

[55] ENISA, „NIS Investments," Noiembrie 2024. [Interactiv]. Available: https://www.enisa.europa.eu/. [Accesat 25 Martie 2025].

[56] OECD, „Publications>Digital Security Risk. Management for Economic and Social Prosperity," 1 Octombrie 2015. [Interactiv]. Available: https://www.oecd.org/. [Accesat 24 Martie 2025].

[57] R. Y. Maulana, „Overview of smart governance: A new approach to Jambi city policy innovation," *SCIC,* vol. 8, pp. 321-329, 1 Aprilie 2023.

[58] D. M. Popa , „A technological and legal investigation into how smart states deploy collective intelligence for security and surveillance purposes," *SCIC,* vol. 9, nr. 2, pp. 77-86, 17 Martie 2025.

[59] M. Stănciulescu, „Smart citizens, smart administration - between rights and responsibilities," *SCIC,* vol. 9, pp. 113-123, 2 Aprilie 2023.

[60] Consiliul Europei, „Convenția Consiliului Europei: privind criminalitatea informatică," 23 Noiembrie 2001. [Interactiv]. Available: https://rm.coe.int/16802fa41f. [Accesat 2 Aprilie 2025].

[61] A. Babin, S. Tutunaru și I. Covalenco, „The role of the Interreg Programmes in strengthening cyber security within regions of the Republic of Moldova," *TRUST,* vol. 1, pp. 45-58, 16 Iulie 2024.

[62] Bundesministerium der Justiz, „Legea privind Oficiul Federal pentru Securitatea Informației," 2009. [Interactiv]. Available: https://www.gesetze-im-internet.de/bsig_2009/. [Accesat 1 Aprilie 2025].

[63] Federal Office for Information Security, „German Security Act 1.0," Iulie 2015. [Interactiv]. Available: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/1-0/it_sig-1-0_node.html. [Accesat 1 Aprilie 2025].

[64] Federal Office for Information Security, „The German IT Security Act 2.0," Aprilie 2021. [Interactiv]. Available: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig-2-0_node.html. [Accesat 1 Aprilie 2025].

[65] K. Chin, „Cybersecurity Laws and Regulations in Germany," UpGuard, 18 Noiembrie 2024. [Interactiv]. Available: https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany. [Accesat 1 Aprilie 2025].

[66] Parlamentul României, „Lege nr. 362/2018," 28 Decembrie 2018. [Interactiv]. Available: https://legislatie.just.ro/public/detaliidocument/209670. [Accesat 1 Aprilie 2025].

[67] Guvernul României, „Ordonanță de Urgență nr.155," 31 Decembrie 2024. [Interactiv]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121. [Accesat 1 Aprilie 2025].

[68] Parlamentul României, „LEGE nr. 58," 14 Martie 2013. [Interactiv]. Available: https://legislatie.just.ro/public/DetaliiDocument/265677. [Accesat 30 Aprilie 2025].

[69] D. Cîmpean, „Cum construim reziliența în fața atacurilor?," în *ZF Cybersecurity Trends*, București, 2025.

[70] South African Parliament, „Cybercrimes Act," 1 Decembrie 2021. [Interactiv]. Available: https://cybercrimesact.co.za/. [Accesat 1 Aprilie 2025].

[71] Michalsons, „Cybercrimes Act in South Africa | Overview and Read," [Interactiv]. Available: https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-south-africa. [Accesat 1 Aprilie 2025].

[72] CSA Singapore, „Cybersecurity Act," 2 Aprilie 2025. [Interactiv]. Available: https://www.csa.gov.sg/legislation/cybersecurity-act. [Accesat 4 Aprilie 2025].

[73] Singapore Statutes Online, „Cybersecurity Act," 12 Martie 2018. [Interactiv]. Available: https://sso.agc.gov.sg/Acts-Supp/9-2018/?ProvIds=P11-#pr3-. [Accesat 1 Aprilie 2025].

[74] CCDCOE, „Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," 2018. [Interactiv]. Available: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. [Accesat 4 Aprilie 2025].

[75] e-Estonia, „Estonia among the best countries to provide digital public services according to the OECD," 31 Ianuarie 2024. [Interactiv]. Available: https://e-estonia.com/estonia-among-the-best-countries-to-provide-digital-public-services-according-to-the-oecd/. [Accesat 4 Aprilie 2025].

[76] „Cybersecurity Act," 9 Mai 2018. [Interactiv]. Available: https://www.riigiteataja.ee/en/eli/523052018003/consolide. [Accesat 4 Aprilie 2025].

[77] C. A. Prie și M. V. Crăsnean , „Hybrid Warfare. The Russian Intervention in Crimea in 2014 And The Lessons We Learned For the Current Military Context," Septembrie 2022. [Interactiv]. Available: https://www.armyacademy.ro/reviste/rev3_2022/Art_Prie_Crasnean_Raft_3_2022.pdf. [Accesat 25 Mai 2025].

[78] CyberPeace Institute, „Public Administration," [Interactiv]. Available: https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/public-administration. [Accesat 25 Mai 2025].

[79] G. B. Mueller, B. Jensen , B. Valeriano, R. C. Maness și J. M. Macias , „Cyber Operations during the Russo-Ukrainian War," Center of Strategic & International Studies, 23 Iulie 2023. [Interactiv]. Available: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. [Accesat 25 Mai 2025].

[80] Ministry of Digital Transformation, „Digital country," Ukraine.ua, [Interactiv]. Available: https://ukraine.ua/invest-trade/digitalization/. [Accesat 22 Mai 2025].

[81] European Comission, „Digital Public Administration factsheet 2022," 2 August 2022. [Interactiv]. Available: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Ukraine_vFinal_0.pdf. [Accesat 22 Mai 2025].

[82] O. Yevtushenko, „Digitalizattion: a tool for modernization of public administration in Ukraine," *Public Administration and Regional Development,* nr. 26, pp. 1158-1176, 2024.

[83] Visit Ukraine, „E-passport, E-support, Diia-Signature: how Ukraine became the first digital state in the world," 12 Mai 2023. [Interactiv]. Available: https://visitukraine.today/blog/1833/e-passport-e-support-diia-signature-how-ukraine-became-the-first-digital-state-in-the-world?/. [Accesat 22 Mai 2025].

[84] OECD, „Digitalisation for recovery in Ukraine," 1 Iulie 2022. [Interactiv]. Available: https://www.oecd.org/en/publications/2022/07/digitalisation-for-recovery-in-ukraine_40746fbe.html. [Accesat 22 Mai 2025].

[85] Kyifornia, „e-Malyatko,” Kyifornia, [Interactiv]. Available: https://diia.gov.ua/services/yemalyatko. [Accesat 22 Mai 2025].

[86] Diia City, „Freedom and Opportunities for IT business in Ukraine,” Diia.City, [Interactiv]. Available: https://city.diia.gov.ua/en. [Accesat 22 Mai 2025].

[87] Digital State UA, „information about the project Diia.City,” GOVTECH, [Interactiv]. Available: https://digitalstate.gov.ua/projects/govtech/diia-city. [Accesat 22 Mai 2025].

[88] Diia.Education, „About the project,” [Interactiv]. Available: https://osvita.diia.gov.ua/en/about. [Accesat 22 Mai 2025].

[89] United Nations Development Programme, „Diia.Education launches updated digital map with Digital Education Hub,” Februarie 2025. [Interactiv]. Available: https://www.undp.org/ukraine/press-releases/diiaeducation-launches-updated-digital-map-digital-education-hubs. [Accesat 22 Mai 2025].

[90] European Comission, „Digital Competence Framework for Citizens (DigComp),” 2018. [Interactiv]. Available: https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en. [Accesat 22 Mai 2025].

[91] I. Belova, O. Yaroshchuk și A. Homotiuk, „Development of digitalization processes in the European Union: prospective experience for Ukraine,” *Ekonomichnyy analiz,* vol. 33, nr. 1, pp. 180-191, Martie 2023.

[92] Visit Ukraine.today, „What do you need to know about the Crimean resistance to russian occupation?,” 26 Februarie 2024. [Interactiv]. Available: https://visitukraine.today/blog/3424/what-do-you-need-to-know-about-the-crimean-resistance-to-russian-occupation?srsltid=AfmBOoruF75z5AGbDv5DL_U-FiEDdZ5M631mJnl6YJolDpa1oDfqYiOK. [Accesat 22 Mai 2025].

[93] J. Masters, „Ukraine: Conflict at the Crossroads of Europe and Russia,” Council on Foreign Relations, 24 Februarie 2023. [Interactiv]. Available: https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia. [Accesat 23 Mai 2025].

[94] S. Pifer, „Why care about Ukraine and the Budapest Memorandum,” Brookings, 5 Decembrie 2019. [Interactiv]. Available: https://www.brookings.edu/articles/why-care-about-ukraine-and-the-budapest-memorandum/. [Accesat 23 Mai 2025].

[95] Heads of State and Government , „Bucharest Summit Declaration,” North Atlantic Treaty Organization, 2 Aprilie 2008. [Interactiv]. Available: https://www.nato.int/cps/en/natolive/official_texts_8443.htm. [Accesat 23 Mai 2025].

[96] R. Martin și C. Mayness, „Putin justifies Ukraine invasion as a `spacial military operation`,” npr, 24 Februarie 2022. [Interactiv]. Available: https://www.npr.org/2022/02/24/1082736110/putin-justifies-ukraine-invasion-as-a-special-military-operation. [Accesat 23 Mai 2025].

[97] Canandian Center for Cyber Security, „Cyber Threat Bulletin,” 22 Iunie 2022. [Interactiv]. Available: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf. [Accesat 26 Mai 2025].

[98] European Parliament, „Russia`s war on Ukraine: Timeline of cyber-attacks,” 8 Iunie 2022. [Interactiv]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. [Accesat 25 Mai 2025].

[99] infolivedaily, „US, EU cyber investment in Ukraine pay off amid war,” 14 Martie 2022. [Interactiv]. Available: https://infolivedaily.wordpress.com/2022/03/14/us-eu-cyber-investments-in-ukraine-pay-off-amid-war/. [Accesat 25 Mai 2025].

[100] C. Cîmpanu, „Hackers deface Ukrainian government websites,” The Record, 14 Ianuarie 2022. [Interactiv]. Available: https://therecord.media/hackers-deface-ukrainian-government-websites. [Accesat 26 Mai 2025].

[101] G. Sen, „Tracking the Cyberspace during Russo-Ukraine Crisis,” Cescube, 20 August 2022. [Interactiv]. Available: https://www.cescube.com/vp-tracking-the-cyberspace-during-russo-ukraine-crisis. [Accesat 25 Mai 2025].

[102] D. Antoniuk, „DDos attacks hit Ukrainian government websites,” The Record, 15 Februarie 2022. [Interactiv]. Available: https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces. [Accesat 25 Mai 2025].

[103] M. Baezner, „Cyber and information warfare in the Ukrainian conflict," Octombrie 2018. [Interactiv]. Available: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf. [Accesat 25 Mai 2025].

[104] C. Pozzi, „The EU Deploys Cyber Defence Team to Support Ukraine," Aprilie 2022. [Interactiv]. Available: https://finabel.org/wp-content/uploads/2022/04/IF-30.03.pdf. [Accesat 25 Mai 2025].

[105] Council of the EU, „Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union," European Council, 10 Mai 2022. [Interactiv]. Available: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/. [Accesat 26 Mai 2025].

[106] Reuters, „Russian air strike took out TV tower in Ukraine`s Kharkiv, Zelenskiy says," Reuters, 23 Aprilie 2024. [Interactiv]. Available: https://www.reuters.com/world/europe/tv-tower-collapses-ukraines-kharkiv-after-russian-missile-attack-2024-04-22/. [Accesat 26 Mai 2025].

[107] D. Antoniuk, „Ukraine`s state-owned nuclear power operator said Russian hackers attacked website," The Record, 17 August 2022. [Interactiv]. Available: https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website. [Accesat 26 Mai 2025].

[108] M. Santora, „The operator of Ukraine`s nuclear plants says it faced ambitious cyberattack," The New York Times, 16 August 2022. [Interactiv]. Available: https://www.nytimes.com/2022/08/16/world/europe/the-operator-of-ukraines-nuclear-plants-says-it-faced-an-ambitious-cyberattack.html. [Accesat 26 Mai 2025].

[109] R. Wright, „Industroyer2: How Ukraine avoided another black-out," TechTarget, 10 August 2022. [Interactiv]. Available: https://www.techtarget.com/searchsecurity/news/252523694/Industroyer2-How-Ukraine-avoided-another-blackout-attack. [Accesat 26 Mai 2025].

[110] Human Right Watch, „Death at the Station: Russian Cluster Munition Attack in Kramatorsk," 23 Februarie 2023. [Interactiv]. Available: https://www.hrw.org/video-photos/interactive/2023/02/21/death-at-the-station/russian-cluster-munition-attack-in-kramatorsk. [Accesat 26 Mai 2025].

[111] Kackers Arise, „SCADA Hacking: Anatomy of a SCADA Malware, BlackEnergy 3 Attack on the Ukraine Grid," 27 Decembrie 2022. [Interactiv]. Available: https://hackers-arise.com/scada-hacking-anatomy-of-a-scada-malware-blackenergy-3-attack-on-the-ukraine-grid/. [Accesat 26 Mai 2025].

[112] Reuters, „Ukraine`s postal service hit by cyberattack after sales of warship stamp go online," 22 Aprilie 2022. [Interactiv]. Available: https://www.reuters.com/world/europe/ukraines-postal-service-hit-by-cyberattack-after-sales-warship-stamp-go-online-2022-04-22/. [Accesat 26 Mai 2025].

[113] K. E. Eichensehr, „Ukraine, Cyberattacks, and the Lessons for International Law," 23 Mai 2022. [Interactiv]. Available: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/69B36016B06998BCE1EC67C757CDF34D/S2398772322000204a.pdf/ukraine-cyberattacks-and-the-lessons-for-international-law.pdf. [Accesat 26 Mai 2025].

[114] Botek Adam, „European Union establishes a sanction regime for cyber-attacks," CCDCOE, [Interactiv]. Available: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/. [Accesat 26 Mai 2025].

[115] S. Duguin și P. Pavlova, „The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict," 4 Septembrie 2023. [Interactiv]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf. [Accesat 26 Mai 2025].

[116] CyberPeace Institute, „Geopolitical Map," [Interactiv]. Available: https://cyberconflicts.cyberpeaceinstitute.org/impact/geography. [Accesat 27 Mai 2025].

[117] W. Fabritius, „The Ransomware Attack in Baltimore: A Failure of Organizational Resilience," Route Fifty, 10 Iulie 2019. [Interactiv]. Available: https://www.route-fifty.com/digital-government/2019/07/ransomware-baltimore-organizational-resilience/158314/. [Accesat 30 Aprilie 2025].

[118] A. Shalal-Esa, „Iran strengthened cyber capabilities after Stuxnet: U.S. general," Reuters, 18 Ianuarie 2013. [Interactiv]. Available: https://www.reuters.com/article/technology/iran-

strengthened-cyber-capabilities-after-stuxnet-us-general-idUSBRE90G1C4/. [Accesat 29 Aprilie 2025].

[119] Kaspersky, „Stuxnet explained: What it is, who created it and how it works," [Interactiv]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet. [Accesat 29 Aprilie 2025].

[120] J. Fruhlinger, „The OPM hack explained: Bad security practices meet China's Captain America," CSO, 12 Februarie 2020. [Interactiv]. Available: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html. [Accesat 30 Aprilie 2025].

[121] Congress of the United States, „The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation," Committee of Oversight , 2016.

[122] BBC News, „Russia 'was behind German parliament hack'," BBC, 13 Mai 2016. [Interactiv]. Available: https://www.bbc.com/news/technology-36284447. [Accesat 29 Aprilie 2025].

[123] Reuters, „German parliament foiled cyber attacks by hackers via Israeli website," Reuters, 29 Martie 2017. [Interactiv]. Available: https://www.reuters.com/article/world/german-parliament-foiled-cyber-attack-by-hackers-via-israeli-website-idUSKBN1701VV/. [Accesat 29 Aprilie 2025].

[124] L. Pascu, „Japanese Defences Ministry flip flops on allegations of hack by foreign state," Bitdefender, 28 Noiembrie 2016. [Interactiv]. Available: https://www.bitdefender.com/en-us/blog/hotforsecurity/japanese-defense-ministry-flip-flops-on-allegations-of-hack-by-foreign-state. [Accesat 29 Aprilie 2025].

[125] C. Cimpanu, „Japan Defence Ministry Targeted by Cyber-Attacks," BLEEPINGCOMPUTER, 28 Noiembrie 2016. [Interactiv]. Available: https://www.bleepingcomputer.com/news/security/japan-defense-ministry-targeted-by-cyber-attack/. [Accesat 29 Aprilie 2025].

[126] BBC, „UK and US blame Russia for 'malicious' NotPetya cyber-attacks," 16 Februarie 2018. [Interactiv]. Available: https://www.bbc.com/news/uk-politics-43062113. [Accesat 30 Aprilie 2025].

[127] A. Greenberg , „The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 22 August 2018. [Interactiv]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. [Accesat 30 Aprilie 2025].

[128] D. Jones, „Conflict over Ukraine raises cyber risk for US enterprises," Cybersecurity Dive, 1 Februarie 2022. [Interactiv]. Available: https://www.cybersecuritydive.com/news/ukraine-russia-cyber-threat/618084/. [Accesat 30 Aprilie 2025].

[129] The Claroty Team, „NotPetya: Looking Back Six Years Later," Claroty, 6 Iunie 2023. [Interactiv]. Available: https://claroty.com/blog/notpetya-looking-back-six-years-later/. [Accesat 30 Aprilie 2025].

[130] L. H. Newman , „Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare," Wired, 23 Aprilie 2018. [Interactiv]. Available: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/. [Accesat 30 Aprilie 2025].

[131] United States Attorney's Office, Northern District of Georgia, „Atlanta U.S. Attorney Charges Iranian nationals for City of Atlanta ransomware attack," 5 Decembrie 2028. [Interactiv]. Available: https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack/. [Accesat 2025 Aprilie 2025].

[132] Cyware, „A Timeline of the Baltimore City Ransomware Attack," 22 Mai 2019. [Interactiv]. Available: https://www.cyware.com/blog/a-timeline-of-the-baltimore-city-ransomware-attack-d006. [Accesat 30 Aprilie 2025].

[133] D. Temple-Raston, „A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," NPR, 16 Aprilie 2021. [Interactiv]. Available: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack/. [Accesat 30 Aprilie 2025].

[134] U.S. Government Accountability Office, „SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," GAO, 22 Aprilie 2021. [Interactiv]. Available: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic/. [Accesat 30 Aprilie 2025].

[135] C. Tornaghi, „The Dramatic Cyberattack That Put Latin America on Alert," Americas Quarterly, 25 Iulie 2023. [Interactiv]. Available: https://www.americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/. [Accesat 30 Aprilie 2025].

[136] P. Bischoff, „Cyberscurity rankings by country: Which countries have the worst (and best) cybersecurity?," Comparitech, 10 Ianuarie 2024. [Interactiv]. Available: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/. [Accesat 5 Mai 2025].

[137] CBIZ, „Cybersecurity Outlook for Public Sector," 22 Aprilie 2024. [Interactiv]. Available: https://www.cbiz.com/insights/article/cybersecurity-outlook-risks-and-trends-for-the-public-sector#:~:text=Share. [Accesat 2 Mai 2025].

[138] Institute for Defense & Business, „Top 5 Cyber Threats Facing the Public Sector," [Interactiv]. Available: https://www.idb.org/top-5-cyberthreats-facing-the-public-sector/. [Accesat 2 Mai 2025].

[139] L. French , „95% of data breaches involve human error, report reveals," SC Media, 11 Martie 2025. [Interactiv]. Available: https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals. [Accesat 2 Mai 2025].

[140] B. Smith, „Defending Ukraine: Early Lessons from the Cyber War," Microsoft, 22 Iunie 2022. [Interactiv]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. [Accesat 27 Mai 2025].

[141] M. Bagwe, „Zelenskyy Signs Law Advancing Cybersecurity of Ukraine`s State Networks and Critical Infrastructure," The Cyber Express, 21 Aprilie 2025. [Interactiv]. Available: https://thecyberexpress.com/zelenskyy-signs-advanced-cybersecurity-bill/. [Accesat 27 Mai 2025].

[142] National Security and Defance Council of Ukraine, „The working group at the NCCC at the NSDC of Ukraine approved the draft Cybersecurity Startegy of Ukraine," 4 Martie 2021. [Interactiv]. Available: https://www.rnbo.gov.ua/en/Diialnist/4838.html. [Accesat 27 Mai 2025].

[143] R. Shandler și M. A. Gomez , „The hidden threat of cyber-attacks - undermining public confidence in government," *Journal of Information Technology & Politics,* vol. 20, nr. 4, pp. 359-374, 2023.

[144] SentinelOne, „Public Sector Cybersecurity | Why State & Local Governments Are at Risk," 28 August 2023. [Interactiv]. Available: https://www.sentinelone.com/blog/why-the-public-sector-under-attack-understanding-the-cyber-risks-of-state-local-governments/. [Accesat 2 Mai 2025].