Sesiune de comunicări științifice
Dimensiunile securității naționale a Republicii Moldova: politică, economică, socială, umană, ecologică

CZU: 32:004.056
DOI: 10.5281/zenodo.6832915

IMPORTANȚA ASIGURĂRII SECURITĂȚII CIBERNETICE ÎN CADRUL DOMENIULUI POLITIC. PROBLEME, RISCURI ȘI NOI OPORTUNITĂȚI

Tatiana BUSUNCIAN
Republica Moldova, Chișinău
Universitatea de Stat din Moldova
Facultatea Relații Internaționale, Științe Politice și Administrative
doctor în politologie, conferențiar universitar
e-mail: busuncian@gmail.com
ORCID ID: 0000-0003-0242-8863

Ion MOLDOVAN
Republica Moldova, Chișinău
Universitatea de Stat din Moldova / Institutul Național de Informații și Securitate „Bogdan, Întemeietorul Moldovei"
masterand
e-mail: ion.moldovan@gmail.com
ORCID ID: 0000-0001-7364-8738

In the 21st century, the age of new scientific technologies when humanity has reached a high level of computing technology development and interconnectivity, in addition to many multidimensional uses, we have come across a multitude of problems that were not preeminent until recently. Indeed, the requirement to maintain security in the cybernetic dimension has become equally vital for individuals, companies and organizations, both at the national and global levels. This paper aims, considering the aspect of ensuring high level of cybersecurity, to provide a multidimensional and equidistant analysis and identify central issues in the field: the problem of critical infrastructure, electronic voting, darknet and transnational hacking groups.

Keywords*: cybersecurity, politics, problems, risks, critical infrastructure, electronic voting, darknet, cybercrime, hackers, international hacker networks, cyberwarfare*

Aflându-ne în secolul XXI, în epoca noilor tehnologii științifice, în care umanitatea a ajuns la un nivel înalt de dezvoltare a tehnicii de calcul și a nivelului de inter conectivitate, pe lângă numeroase foloase aduse multidimensional, am ajuns să ne ciocnim cu o multitudine de probleme care până nu demult nu erau primare, astfel necesitatea menținerii securității în dimensiunea cibernetică a devenit una vitală atât pentru indivizi aparte, cât și a companiilor și organizațiilor, ajungând chiar și la nivel de țară și global. Astfel, pentru a ne putea asigura un nivel ridicat de securitate cibernetică, în lucrarea prezentă, ne propunem să depistăm și să analizăm multidimensional și echidistant principalele probleme din domeniul dat. Cu toate că la momentul actual există numeroase probleme de ordin cibernetic, în articolul prezent v-om numi și prezenta detaliat cele mai importante dintre acestea, care pot crea dificultăți și riscuri suplimentare sistemelor de securitate cibernetică naționale.

Printre cele mai importante probleme ale securității cibernetice mondiale în prezent putem considera: *problema infrastructurii critice; problema votului electronic; problema darknet-ului; problema grupărilor transnaționale de hackeri.*

Însăşi prin termenul de „*infrastructură critică*" se creează opinia despre un sistem de infrastructură care are o importanță foarte majoră pentru stat şi societate la general. În fiecare țară la momentul actual există sisteme naționale, dar şi corporative-private legate de controlul şi mentenanța sistemelor de infrastructură critică. Conform directivei 2008/114 /CE al Consiliului Uniunii Europene, infrastructura critică este definită ca „un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, şi a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții" [1].

Conform cercetătorilor români de la Centrul de Studii Strategice de Apărare şi Securitate, Grigore Alexandrescu și Gheorghe Văduvă, infrastructurile fac parte din structura de rezistență a unui sistem, sunt relaționale şi funcționale şi constituie in integrum suportul necesar pentru ca sistemul să se identifice, să se individualizeze, să intre în relații cu alte sisteme, să se stabilizeze şi, evident, să funcționeze. Infrastructurile se pot împărți, în funcţie de locul, rolul şi importanța lor pentru stabilitatea şi funcționalitatea sistemelor, precum şi pentru siguranța şi securitatea sistemelor şi procese în trei mari categorii: *infrastructuri obişnuite; infrastructuri speciale; infrastructuri critice* [2, p. 6].

Infrastructurile obişnuite reprezintă o structură, un cadru, care asigură construcția şi funcționarea sistemului. Aceste infrastructuri nu prezintă calități deosebite, în afara celor care le justifică existența şi prezența în cadrul sistemelor şi proceselor. O ţară, spre exemplu, va avea totdeauna drumuri, căi ferate, localități, şcoli, biblioteci etc. Pe parcurs, unele dintre acestea pot deveni speciale sau chiar critice, în funcţie de noul rol pe care îl pot avea, de dinamica importanței şi de alte criterii. Spre exemplu, localitățile care au aerodromuri, puternice centre de comunicații, centrale nucleare, noduri de cale ferată etc. pot face parte din infrastructuri speciale şi, în anumite condiţii, chiar din infrastructurile critice [2, p. 6].

Infrastructurile speciale au un rol deosebit în funcționarea sistemelor şi proceselor, asigurându-le acestora o eficientă sporită, calitate, confort, performanță. De regulă, infrastructurile speciale sunt infrastructuri de performanță. Unele dintre acestea, mai ales cele care pot avea, prin extensie sau prin transformare (modernizare), un rol important în stabilitatea şi securitatea sistemelor, pot intra şi în categoria infrastructurilor critice [2, p. 6].

Infrastructurile critice sunt, de regulă, acele infrastructuri de care depind stabilitatea, siguranța şi securitatea sistemelor şi proceselor. Ele pot face parte din categoria infrastructurilor speciale. Nu este însă obligatoriu ca toate infrastructurile care sunt sau pot deveni, la un moment dat, critice să facă parte din această categorie de infrastructuri. Este foarte posibil ca, în funcţie de situație, chiar şi unele dintre infrastructurile obişnuite – cum ar fi, spre exemplu, drumurile de ţară sau canalele magistrale din sistemele de irigații etc. – să devină infrastructuri critice. De aceea, în definirea infrastructurilor critice, pot să intervină şi alte elemente, ceea ce conduce la concluzia că există un criteriu de flexibilitate şi un altul de imprevizibil în identificarea şi evaluarea unor astfel de structuri [2, p. 7].

Infrastructurile critice sunt acele infrastructuri cu rol important în asigurarea securităţii în funcționarea sistemelor şi în derularea proceselor economice, sociale, politice, informaționale şi militare. Infrastructurile sunt considerate critice datorită:

- condiției de unicat în cadrul infrastructurilor unui sistem sau proces;
- importanței vitale pe care o au, ca suport material sau virtual (de rețea), în funcționarea sistemelor şi în derularea proceselor economice, sociale, politice, informaționale, militare etc.;
- rolului important, de neînlocuit, pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranța, funcționalitatea şi, mai ales, în securitatea sistemelor;
- vulnerabilității sporite la amenințările directe, precum şi la cele care vizează sistemele din care fac parte;

- sensibilității deosebite la variația condițiilor și, mai ales, la schimbări bruște ale situației [2, p. 7].

Protecția infrastructurii critice se referă la măsuri pentru asigurarea securității sistemelor, rețelelor și activelor interdependente care stau la baza serviciilor vitale pentru funcționarea societății. Exemple de infrastructură fizică vitală includ drumuri, poduri, aeroporturi, comunicații și centrale electrice. Toate celelalte tipuri de infrastructură sunt imposibile fără infrastructura informațională, adică fără computere și rețele, reprezentate în principal de sisteme de monitorizare, control și achiziții de date (SCADA), a căror interconectare le permite să facă schimb de informații și să efectueze analize asupra tuturor funcțiilor critice. Aceste tipuri de infrastructură includ serviciile bancare, generarea și distribuția energiei electrice, serviciile medicale, serviciile guvernamentale de urgență și transportul [3].

Deoarece în majoritatea țărilor infrastructura informațională critică este în mare măsură deținută de sectorul privat, care o operează, este necesară nevoia de un set dinamic de soluții care să reflecte faptul că reglementarea nu ține pasul cu dezvoltarea atât a celor mai noi amenințări, cât și a tehnologiilor necesare pentru întreținere lor. Fluiditatea inerentă rapidă și constantă a internetului, împreună cu acoperirea sa globală, necesită soluții flexibile care se adaptează rapid la circumstanțe noi și în schimbare [3].

În acest fel putem clasifica infrastructura critică pe domenii de activitate:

- Energie (producția și extragerea de petrol și gaze naturale, producția, distribuția și stocarea combustibilului, inclusiv în rețelele de conducte, producția de energie electrică, transportul de energie electrică, gaze și petrol, distribuția);
- Sisteme de comunicații și informații (Sisteme informaționale și protecția rețelelor, Elemente tehnologice și de control ale sistemelor, Internetul, Elemente tehnologice ale rețelelor de comunicații electronice staționare, Elemente tehnologice ale rețelelor mobile de comunicații electronice, Elemente tehnologice ale rețelelor de radiodifuziune, televiziune și de navigație, Elemente tehnologice de comunicare prin satelit, radiodifuziune);
- Gestionarea apei (Protecția surselor de apă potabilă, controlul calității apei, tratarea apei și controlul cantității de producție);
- Alimente (producția de alimente, siguranța și protecția alimentelor);
- Asistență medicală (servicii medicale și spitalicești, medicamente, seruri, vaccinuri și medicamente, laboratoare biologice și agenți biologici);
- Piața financiară (Servicii de plată și structuri de plată, administrația financiară de stat);
- Asigurare socială, drept și securitate (asigurare socială, drept și securitate, administrație, justiție și locuri de detenție);
- Administrație publică (administrație publică, forțele armate, autonomia locală, servicii poștale și de livrare);
- Transport (Transport rutier, Transport feroviar, Transport aerian, Transport fluvial, Transport maritim și costier);
- Industria chimică și nucleară (Producția, depozitarea și prelucrarea substanțelor chimice și a materialelor nucleare, Produse ale substanțelor chimice periculoase)
- Spațiu cosmic și știință [4, p. 28-30].

Pentru a înțelege impactul neglijenței protecției securității cibernetice în domeniul infrastructurii critice propunem spre analiză un caz care a avut loc recent. În februarie 2021, în orașul Oldsmar, statul Florida, SUA, oamenii legii și autoritățile locale au comunicat că un hacker necunoscut a obținut acces la sistemele de tratare și curățire a apei a orașului și a modificat compoziția chimică a apei. Făptașul a utilizat aplicația populară de acces și control de la distanță, care permite întreținerea computerelor și a altor dispozitive „TeamViewer”, cu ajutorul acesteia el a accesat de două ori calculatorul principal al Stației de tratare a apei, după care a modificat indicatorii componenței chimice a apei tratate pentru un oraș de aproape 15.000 de locuitori. Ca urmare a acestor manipulări, atacatorul a crescut cu succes nivelul de hidroxid de sodiu (NaOH) la niveluri periculoase, apoi s-a deconectat [5].

„Hidroxidul de sodiu, cunoscut și sub numele de sodă caustică, este ingredientul principal în produsele de curățare a țevilor. De asemenea, este utilizat pentru a controla aciditatea apei și a elimina metalele din apa potabilă din stațiile de tratare a apei. Hackerul a schimbat conținutul de hidroxid de sodiu al apei de la aproximativ 100 părți per milion la 11.100 părți per milion. Evident, aceasta este o creștere semnificativă și potențial periculoasă” a declarat șeriful Bob Gualtieri în conferința de presă susținută [5]. Din fericire, apa periculoasă nu a fost furnizată localnicilor, deoarece atacul a fost observat la timp și, de îndată ce hackerul s-a deconectat, operatorul stației a readus imediat toate valorile substanțelor chimice la normal. Primarul orașului Oldsmar, Eric Seidel, a subliniat că sistemul de tratare a apei din oraș este configurat cu redundanță și oricum ar suna o alarmă dacă nivelurile chimice ar atinge niveluri periculoase fără ca oamenii să observe [5]. Cu toate acestea, există oricum un risc ca așa tipuri de infrastructuri critice să fie sparte, iar cifra victimelor la așa atacuri ar putea fi respectiv foarte mare.

O altă problemă modernă cu care se ciocnește domeniul securității cibernetice la etapa actuală este problema votului electronic. Ideile privind implementarea unor sisteme electorale electronice (inclusiv în Republica Moldova) nu sunt noi, și speculațiile privind faptul că acestea nu sunt implementate din motive netemeinice, de exemplu că în așa mod fiecare cetățean ar putea avea acces mai rapid la procesul electoral, respectiv există posibilitatea ca acel masiv care nu participă la procesul electoral din motive diferite ar putea destabiliza procentajul clasei politice aflate la guvernare. Aceste declarații de fapt sunt complet eronate, există mai multe motive absolut temeinice datorită cărora la etapa actuală foarte puține state ale lumii nu implementează sistemele electronice de vot. Trebuie de menționat și faptul că procesul electoral presupune două părți indispensabile – anonimitatea (că decizia votată de tine este cunoscută doar pentru tine) și încrederea (că votul tău va fi considerat ca valid și corect, deci respectiv glasul tău va fi auzit), votul electronic nu poate garanta cu o probabilitate de 100% niciuna dintre acestea.

Printre cele mai observabile motive pentru care votul electronic nu trebuie utilizat putem considera:

1. Lipsa de resurse financiare pentru elaborarea și întreținere a sistemelor electronice electorale;
2. Lipsa de personal calificat pentru elaborarea și întreținere a sistemelor electronice electorale;
3. Lipsa de garantare a secretului electoral;
1. Problemele de ordin software și hardware;
2. Atacuri cibernetice (din intern și extern) asupra sistemelor;
3. Erorile de ordin tehnic și uman;
4. „Calibrarea internă” a rezultatelor;
5. Problema criptografiei nesigure;
6. Cumpărarea de voturi (ceea ce este imposibil de monitorizat în cadrul procesului electoral electronic).

Fiecare dintre factorii menționați mai sus pot crea o situație de incertitudine și neîncredere în sistemul electoral din partea societății civile, iar alegerile ar putea fi considerate, la necesitate, drept falsificate.

La etapa actuală există numeroase sisteme de votare electronică, acestea pot fi clasificate pe mai multe tipuri:

1. Sistemul electoral electronic pe hârtie (procesul electoral decurge în mod tradițional, doar că foaia cu ștampila/imprimarea candidatului ales este introdus într-un aparat care scanează locul unde a fost înscris candidatul ales, după care punctează candidatul în sistemul electronic ca votat);
2. Sistemul electoral electronic local (prin care un aparat de tip terminal care nu are conexiunea la Internet acceptă votarea în regim electronic, la finalul procesului electoral baza cu votanți stocată pe unitatea de stocare a datelor din terminal este deschisă iar rezultatele sunt

trimise organului electoral central, există și variante cu printarea rezultatelor fiecărui buletin de vot pe suport de hârtie);

3. Sistemul electoral electronic local care utilizează rețeaua Internet (se aseamănă cu sistemul electoral precedent, doar că datele privind votul efectuat sunt trimise imediat organului electoral central utilizând rețeaua Internet, la fel rezultatele pot fi printate pe suport de hârtie adăugător);

4. Sistemul electoral electronic prin Internet (procesul electoral are loc prin logarea pe un site specializat cu datele unui buletin electoral electronic, după care este ales candidatul votat, informația este trimisă imediat către serverele organului electoral central);

5. Sistemul electoral electronic interactiv (procesul electoral decurge prin utilizarea unei telecomenzi speciale care are conexiune cu stația centrală de recepție a votului, acest sistem este utilizat în grupuri restrânse, de exemplu în companii, universități, școli, instituții de stat unde există un număr mare de persoane cu drept de vot, de exemplu Parlament).

Până la momentul actual fiecare dintre aceste sisteme a demonstrat ineficiența și nesiguranța în rezultatele finale ale sistemelor electorale electronice, câteva exemple de probleme putem menționa mai jos.

1. Grigoriy Bakunov, expert în domeniul TIC care a analizat sistemul de vot utilizat în alegerile locale din regiunea Moscova (Federația Rusă) în 2019 și în referendumul privind modificarea Constituției Federației Ruse, a declarat că rezultatele votului produs prin intermediul sistemul electoral electronic pot fi modificat și deanonimizate cu ușurință de către cei care îl controlează [6].

2. Un alt expert în criptografie, Pierrick Gaudry, directorul Centrului Național de Cercetări Științifice (fr. Centre National de la Recherche Scientifique, CNRS), într-un raport pentru Universitatea Cornell (eng. Cornell University) a declarat că același sistem menționat mai sus poate fi spart în aproximativ 20 de minute [7].

3. În anul 2007 un grup de hackeri care au fost autorizați pentru a testa preventiv sistemul electoral electronic din statul California, SUA, au spart cu succes sistemul electoral electronic planificat să fie utilizat în procesul electoral [8].

4. Într-un audit post-electoral al Comisiei de Asistență Electorală din SUA (eng. US Election Assistance Commission) privind alegerile prezidențiale din SUA din 2016, în statul Maryland (unde este utilizat Sistemul electoral electronică pe hârtie) au fost depistate mai multe buletine de vot care după scanarea fișei electorale, în urma unor erori a aparatului de scanat au invalidat buletinele de vot, care în original erau valide [9].

Cu toate acestea, trebuie menționat faptul că criptografia cuantică ar putea garanta un nivel mai înalt de securitate procesului electoral, în așa mod, în protecția datelor utilizate în alegerile din statul Geneva, Confederația Elvețiană din anul 2007 criptografia cuantică a fost utilizată pentru prima dată pentru securizarea rezultatelor alegerilor [10]. Dar este necesar de subliniat faptul că așa tehnologii sunt extrem de costisitoare, iar necesitatea mentenanței acestora este extrem de importantă.

O altă problemă a securității cibernetice a statelor lumii la etapa actuală putem considera problema rețelei Darknet, denumit informal drept „Rețeaua ascunsă” sau „Rețeaua întunecată”, aceasta reprezintă o rețea conectată la Internetul clasic, dar datorită tehnologiei TOR (acronimul The Onion Router) care prevede că pentru a se conecta la rețeaua dată, este utilizată tehnica de rutare (marșrutizare) de tipul cepei (din engleză onion) care prevede că traficul de informații dintre clientul TOR (Punctul A) și serverul destinație (Punctul B) este criptat, după care trece prin trei servere intermediare independente selectate aleatoriu din rețeaua TOR după care serverul de ieșire (al treilea) se conectează la serverul destinatar, această tehnică nu poate fi controlată de către organele guvernamentale (cu excepția utilizării atacului de tip man-in-the-middle) [11]. respectiv informațiile publicate pe site-urile care se află în domeniul special ONION nu pot fi șterse atât de ușor cum de exemplu cele aflate în Internetul simplu, iar detactarea și deanonimizarea utilizatorilor acestor platforme este cu mult mai grea. TOR-ul a fost dezvoltat de către trei ingineri din Laboratorul Naval de Cercetări al Statelor Unite - Paul

Syverson, Michael G. Reed și David Goldschlag în anii 1990, după care finanțarea acestuia a trecut către Fundația EFF, iar dezvoltatorul acestui sistem este organizația non-profit Tor Project [12].

Cu toate că TOR-ul inițial fiind dezvoltat cu scopuri militare (exact ca și Internetul), după ce a trecut în utilizare publică acesta s-a axat în primul rând pe anonimitatea informațiilor transmise, fiind pe larg utilizat de către jurnaliști independenți până în prezent pentru a publica, transmite și primi informații sub caracter anonim, pentru ca regimurile nedemocratice sau persoane cointeresate să afle cine este expeditorul lor. TOR permite persoanelor care îl utilizează să navigheze pe web în mod anonim, acoperind identitatea reală a utilizatorului. Acesta poate proteja utilizatorul de la orice analiză a traficului și spionaj în rețea (cu condiția respectării unor reguli ale igienei anonime în rețea). Din acest motiv, de la apariția sa, Darknet-ul a început a fi utilizat masiv în scopuri ilegale pentru vânzări de droguri, arme, pornografie infantilă, bani și acte false, angajare de asasini și hackeri dar și alte activități ilegale [13].

La fel trebuie menționat și faptul că darknet-ul a mai fost utilizat pe post de rețea de comunicare în cadrul mișcărilor de proteste din Africa de Nord și în Orientul mijlociu din anii 2010-2012 denumit drept „Primăvara arabă" [14]. În acest fel darknet-ul poate fi considerat pe drept ca un pericol al securității cibernetice moderne, iar controlul acestuia, cu toate că este greu, este necesar pentru protecția securității naționale ale statelor lumii.

Poate fi considerat interesant faptul că în ultimii ani rețeaua Darknet a început a fi utilizată activ și de serviciile secrete străine cu scopul de a primi informații prin intermediul acesteia, astfel din anul 2019 Agenția Centrală de Informații din SUA – CIA (eng. Central Intelligence Agency) și-a creat propria pagină WEB în rețeaua TOR asemănătoare paginii oficiale din Internetul obișnuit, astfel ca fiecare să poate accesa și transmite informații Agenției, dar și să acceseze știrile și informațiile cum aceștia pot aplica pentru un post de muncă în cadrul acesteia. [25] La fel și Serviciul de Informații Externe a Federației Ruse și-a creat o pagină în rețeaua TOR, unde oricine ar putea transmite careva informații privind amenințări la adresa securității Federației Ruse [26, 27].

O altă problemă a securității cibernetice moderne sunt grupările transnaționale de hackeri. Cu toate că detalii multe nu pot fi accesate datorită activității lor foarte atente, aceștia pot fi clasificați pe mai multe categorii, dar cea mai importantă clasificare, în cazul dat ar fi în raport cu țintele lor de atac.

În raport de ținte acestea le putem clasifica în:

- grupări guvernamentale, respectiv sunt controlate de către instituțiile statelor în care sunt bazați sau activează în folosul acestora, țintele lor principale sunt sistemele informaționale în special infrastructurile critice ale statelor neprietenoase sau dușmane, dar și pentru a culege informații pentru serviciile de informații externe (inclusiv cele militare) ale statului angajator.
- grupări neguvernamentale, care nu par a avea relații cu statele gazdă, marea parte din ele sunt compuse din hackeri de tip black hat (în marea parte a cazurilor din diferite țări) care s-au organizat pentru a ataca sisteme informatice ale companiilor, dar și în unele cazuri ale instituțiilor statelor pentru a estorca dividende financiare, inclusiv prin amenințări că vor publica informațiile sensibile colectate.
- grupări apartenente la organizații teroriste (inclusiv la proto-state precum ISIS, Al Qaeda, IRA), acestea au fost deosebit de active în perioada activității ISIS, combină trăsăturile celor două grupări de mai sus, dar cu toate acestea deține câteva diferențe majore – activează împotriva valorilor culturale umane, promovează terorismul internațional dar și dețin un caracter destructiv.

Una dintre cele mai discutate grupări de hackeri transnațional în spațiul media este gruparea „Anonymous". Această grupare este distinctă de alte grupări de hackeri datorită în primul rînd țintelor acestora, iar scopul lor fiind de a „restabili adevărul", fiind considerați drept „pălării gri" (din eng. grey hat hackers), ceea ce înseamnă că cu toate că încalcă legile (atacând sisteme informaționale guvernamentale și corporatiste) acestea sunt făcute cu scopuri nobile. Conform informațiilor din spațiul public, Anonymous este un grup transnațional hacktivist cu

membri în Olanda, SUA, Marea Britanie, Australia, Spania și Turcia. Aceștia au devenit renumiți pentru atacurile lor motivate politic, obiectivele grupului din trecut au inclus ISIS-ul, Biserica Scientologică, Bursa de Valori din New York și Departamentul Apărării al SUA, și recent după invazia Federației Ruse în Ucraina, a sistemelor informaționale de stat a Federației Ruse, dar și a mai multor resurse de mass-media afiliate acesteia. În Operațiunea „Payback" a grupării din 2012, aceștia au atacat companiile din domeniul financiar-bancar MasterCard, Visa și PayPal care la acel moment refuzau să proceseze donațiile și plățile pentru renumita organizație WikiLeaks [15].

În rândul grupărilor guvernamentale de hackeri printre cei mai activi pot fi considerate grupările afiliate Federației Ruse, Republicii Populare Chineze, Republicii Islamice Iran dar și Republica Populară Democrată Coreeană.

Printre cele mai remarcabile grupări afiliate Federației Ruse pot fi remarcate:

1. Gruparea „Cozy Bear" (în traducere din engleză ca „Ursul Confortabil"), cunoscută și ca „The Dukes" identificată în studiile de securitate cibernetică ca APT29 sau Amenințarea Persistentă Avansată nr.29 (din eng. Advanced Persistent Threat no.29) aceasta a fost legat de mai multe atacuri cibernetice împotriva agențiilor guvernamentale, a organizațiilor politice și a companiilor din Asia, America de Nord și Europa, inclusiv Germania, Norvegia, Coreea de Sud, Uzbekistan și SUA. Cozy Bear a lansat un atac de tip spear-phishing împotriva unui sistem de e-mail neclasificat al Departamentului Apărării al SUA în august 2015. Grupul, de asemenea este vizat în atacurile împotriva Comitetul Național Democrat în anii 2015-2016, a Ministerului Apărării și cel al Afacerilor Externe al Norvegiei în ianuarie 2017 dar și asupra mai multor ministere ale guvernului olandez în anii 2016-2017. La fel gruparea aceasta este învinuită la compromiterea sistemelor informatice ale companiilor Microsoft, Solarwinds și Vmware, care erau utilizate de majoritatea instituțiilor și departamentelor strategice din Statele Unite. Compania de securitate cibernetică CrowdStrike a presupus că Cozy Bear pară să aibă legături cu Serviciul de Informații Externe al Federației Ruse (SVR), sau cu Serviciul Federal de Securitate al Federației Ruse (FSB) [15].
2. Gruparea „Fancy Bear" (din eng. Ursul Elegant) cunoscută și ca „Pawn Storm" identificată în studiile de securitate cibernetică ca APT28 sau Amenințarea Persistentă Avansată nr.28 (din eng. Advanced Persistent Threat no.28) aceasta este considerat de către firmele de securitate cibernetică și organizații guvernamentale că pare să fie sponsorizată de Direcția principală de informații (GRU) din Federația Rusă. Guvernul SUA a identificat Fancy Bear cu două unități GRU cunoscute sub numele de Unitatea 26165 și Unitatea 74455. Grupul a vizat agenții guvernamentale, instituții financiare, grupuri de reflecție, organizații politice și organizații internaționale situate în mai multe țări europene și nord-americane, inclusiv Canada, Franța, Germania, Țările de Jos, Suedia, Ucraina și SUA. Grupul, care este activ cel puțin din 2004, a folosit exploatări de tip Zero Day, atacuri de tip phishing și programe malware împotriva țintelor sale. Grupul a fost de asemenea acuzat că a intervenit în alegerile din Franța, Germania și SUA în 2016 și 2017 [15].
3. Gruparea „Energetic Bear" (din eng. Ursul Energetic) cunoscută și ca „DragonFly", „Koala", dar și „Iron Liberty". Obiectivele principale ale grupului Energetic Bear includ de la producători de gaze pînă la firme care transportă gaze lichide și petrol pînă la consumatorii finali. Grupul a folosit viruși de tip trojan și e-mailuri de phishing pentru a avea acces la sistemele de rețea electrică, facilități de producție și alte ținte [16].

Printre cele mai remarcabile grupări afiliate Republicii Populare Chineze pot fi remarcate:

1. Gruparea „Comment Crew" (din eng. „Echipajul comentator") cunoscută și ca „Comment Panda" sau denumirea militară – Unitatea nr. 61398. Aceasta este identificată în studiile de securitate cibernetică ca APT1 sau Amenințarea Persistentă Avansată nr.1 (din eng. Advanced Persistent Threat no.1). Gruparea este învinuită pentru atacuri și infiltrări în numeroase companii și organizații, printre cei mai mari victime sunt compania Coca-Cola și Lockheed Martin, cel mai important contractant de armament și tehnică militară al Forțelor Armate ale SUA [17].

2. Gruparea „Deep Panda” (din eng. „Panda adîncă”) cunoscută și ca „Shell_Crew”. Aceasta este identificată în studiile de securitate cibernetică ca APT19 sau Amenințarea Persistentă Avansată nr.1 (din eng. Advanced Persistent Threat no.19). Printre primele apariții activ cel puțin din 2011. Se crede că grupul este responsabil pentru atacul cibernetic din 2015 asupra Oficiului de Management al Personalului din Statele Unite în anul 2015 [18].

Cea mai remarcabilă grupare afiliată Republicii Populare Democrate Coreene este gruparea „Lazarus Group”. În dependență de sursă aceasta este catalogată ca asemănătoare cu activitatea grupărilor APT37 și APT38, unele surse le consideră ca fiind una și aceeași grupare. [19] Aceasta este învinuită că au furat circa 1.2 miliarde de dolari SUA din mai multe bănci din Africa, Bangladesh, Malta, Mexico și Vietnam datorită spargerii sistemelor informatice ale acestor bănci, dar și a transmiteri mai multor mesaje fraudulente prin intermediul sistemului internațional SWIFT [20], spargerea serverelor companiei cinematice Sony Pictures Entertainment ca răspuns la darea în cinema a filmului de tip comedie politică „The Interview” prin care se critica regimul dictatorial din Coreea de Nord [20]. Pe lângă acestea, gruparea mai este învinuită pentru crearea și răspândirea virusului de tip ransomware „WannaCry” în mai 2017 [20], cifrele oficiale arată că circa 300.000 de calculatoare au fost infectate cu acest virus [21] iar printre cele mai mari victime ale acestuia au intrat numeroase companii și organizații guvernamentale precum gigantul american producător de avioane și aparate de zbor Boeing [22], gigantul taiwanez producător de microcipuri și procesoare TSMC [23], dar și cea mai mare companie de transport feroviar din Europa și Germania – Deutsche Bahn [24].

În concluzie, putem constata că la etapa actuală când tehnologiile informaționale au împânzit viața de zi cu zi atât a oamenilor cât și a proceselor multidimensionale care au loc în lume, domeniul securității cibernetice necesită a fi luat în calcul în procesul decizional al actorilor politici. Evident că fiecare stat are nevoie de politici riguroase și programe de securitate și este nevoit să intensifice investițiile în protejarea securității cibernetice a sistemelor informaționale ale acestuia. Dependența de informații este tot mai mare, chiar periculoasă. Ignorarea amenințărilor a devenit imposibilă, informațiile au devenit un beneficiu absolut și vital. Confruntarea în spațiul cibernetic duce la pagube economice și fizice considerabile. Respectiv, este necesar de analizat și luat în calcul atât perspectivele, cât și riscurile pe care le poate aduce implementarea și utilizarea sistemelor informaționale.

BIBLIOGRAFIE

1. EUR-Lex. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32008L0114
2. ALEXANDRESCU, GR., VĂDUVA, GH. *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție.* București: Editura Universității Naționale de Apărare “Carol I”, 2006. p.6-8. https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf
3. McAfee. *Protecting Critical Infrastructure*. https://www.mcafee.com/enterprise/en-us/about/public-policy/critical-infrastructure.html
4. СМЕТАНА, М. *Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры*. 2014/15. 28-30 с. URL: https://fbiweb.vsb.cz/moldavia/files/_KI_Smetana.pdf
5. CBS News. *Feds tracking down hacker who tried to poison Florida town's water supply*. URL: https://www.cbsnews.com/news/florida-water-hack-oldsmar-treatment-plant/
6. ХАБР *Григорий Бакунов об электронном голосовании*. https://habr.com/ru/post/509692/
7. РБК. *Эксперт нашел уязвимость в онлайн-системе голосования на выборах в Москве.* https://www.rbc.ru/technology_and_media/15/08/2019/5d55640b9a7947b11c444371

8. SFGATE. *News. Politics. State Vote Machines Lose Test To Hackers.* https://www.sfgate.com/politics/article/STATE-VOTE-MACHINES-LOSE-TEST-TO-HACKERS-2550858.php
9. US. *Election Assistance Commision. Post Election Audits in Maryland*. https://www.eac.gov/sites/default/files/event_document/files/day1-2017-02-13-09_15-03-natasha-Post-Election-Audits-final.pdf
10. IDQ. IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation. URL: https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/
11. InfoSec Institute. Hacking Tor and Online Anonymity. Infosec Resources. https://resources.infosecinstitute.com/topic/hacking-tor-online-anonymity/
12. Fossbytes. Tor Explained: What is Tor? How Does It Work? Is It Illegal? https://fossbytes.com/everything-tor-tor-tor-works/
13. The Irish Times. Darknet is 'like eBay' for drugs, hit men and child porn. https://www.irishtimes.com/business/technology/darknet-is-like-ebay-for-drugs-hit-men-and-child-porn-1.2143958
14. Bussiness Insider. Tech. The dark web turns 20 this month. From black market hotspots to facilitating the Arab Spring, here's how it changed the world. https://www.businessinsider.com/dark-web-changed-the-world-black-markets-arab-spring-2020-3
15. University of Central Arkansas. Political Science. Global Hacking Groups. https://uca.edu/politicalscience/cyber-security-and-international-relations-csir-project/global-hacking-groups/
16. Wired. Security. Your Guide to Russia's Infrastructure Hacking Teams. https://www.wired.com/story/russian-hacking-teams-infrastructure/
17. The New York Times. Chinese Army Unit Is Seen as Tied to Hacking Against U.S. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html
18. Reuters. Hunt for Deep Panda intensifies in trenches of U.S.-China cyberwar. https://www.reuters.com/article/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621
19. Mitre Attack. Groups. Lazarus Group. URL: https://attack.mitre.org/groups/G0032/
20. Computer Weekly. North Korean Lazarus Group hackers indicted in US. https://www.computerweekly.com/news/252496494/North-Korean-Lazarus-Group-hackers-indicted-in-US
21. Tribune. Shadow Brokers threaten to release Windows 10 hacking tools. https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools
22. Forbes. Boeing Is The Latest WannaCry Ransomware Victim. https://www.forbes.com/sites/leemathews/2018/03/30/boeing-is-the-latest-wannacry-ransomware-victim/
23. Bank Info Security. WannaCry Outbreak Hits Chipmaker, Could Cost $170 Million. URL: https://www.bankinfosecurity.com/chipmaker-tsmc-wannacry-attack-could-cost-us170-million-a-11285
24. Frankfurter Allgemeine Zeitung. Weltweite Cyberattacke trifft Computer der Deutschen Bahn. URL: https://www.faz.net/aktuell/wirtschaft/unternehmen/hacker-angriff-weltweite-cyberattacke-trifft-computer-der-deutschen-bahn-15013583.html
25. Central Intelligence Agency. CIA's Latest Layer: An Onion Site. https://www.cia.gov/stories/story/cias-latest-layer-an-onion-site/
26. Настоящее Время. "Следуйте простым инструкциям". Служба внешней разведки России открыла приемную в даркнете. URL: https://www.currenttime.tv/a/razvedka-darknet/31211594.html

27. Служба внешней разведки Российской Федерации. Report Information. http://svr.gov.ru/upload/iblock/0a4/manual.htm