Mediul de securitate a cunoscut o schimbare dramatică în ultimii ani; provocările la adresa securității fiind cele mai diverse. Printre acestea se numără și cele la adresa securității cibernetice. Astfel de provocări pot fi abordate cu eficacitate printr-o colaborare coordonată, prin utilizarea de politici și instrumente care au la bază solidaritatea, asistența reciprocă și prevederile documentelor oficiale. În acest fel, se contribuie la îmbunătățirea rezilienței statelor în ceea ce privește răspunsul la provocările comune. Spațiul cibernetic are un impact enorm asupra tuturor componentelor. Atacurile cibernetice pot provoca perturbarea serviciilor digitale din întreaga lume. Îmbunătățirea rezilienței sistemelor de comunicare și informare este importantă pentru a sprijini piața unică digitală. În acest sens, cooperarea dintre toți actorii implicați în domeniul securității cibernetice (state, organisme etc.) este foarte importantă.

Se presupune că termenul **”terorism cibernetic”** a apărut în vocabularul IT în anul 1997. Agentul special FBI Mark Pollitt a definit acest tip de terorism ca “atacul premeditat, motivat politic impotriva informaţiei, sistemelor informatice, programelor informatice şi datelor, rezultând în violența împotriva țintelor noncombatante, de către grupări sub-nationale sau agenți clandestini".

***Definiții:***

● Terorismul cibernetic – influienţarea ilicită impotriva sistemelor informaţionale, în scopul de a amenința viața, sănătatea sau proprietățile persoanelor nespecificate prin crearea condițiilor pentru accidente și dezastre tecnogene sau amenințarea reală a unui astfel de pericol.

* Atacurile cibernetice sunt încercări de a folosi abuziv informațiile, prin furt, distrugere sau publicare cu scopul de a perturba sau distruge sistemele și rețelele de calculatoare.
* Securitatea cibernetică include securizarea datelor și comunicațiilor, tehnologia de operare și platformele informatice necesare asigurării securității sistemelor digitale.
* Apărarea cibernetică include securitatea cibernetică, analiza amenințărilor, precum și strategiile de protecție împotriva amenințărilor îndreptate împotriva cetățenilor, instituțiilor sau guvernelor.

Existenţa la nivelul fiecărui stat a unui cadru normativ în domeniul securităţii informaționale este necesară, în condiţiile în care nivelul ameninţării la nivel internaţional este în continuă creştere. În evaluarea nivelului ameninţării informaționale avem în vedere, pe de o parte, riscurile generate de interesul anumitor entităţi statale şi criminale de a compromite infrastructuri informaționale/cibernetice şi, pe de altă parte, vulnerabilităţile sistemelor informatice, fie software, fie de natură umană (pe fondul precarităţii culturii de securitate cibernetică). [Transformarea digitală a economiei și a societății](https://www.europarl.europa.eu/news/ro/headlines/society/20210414STO02010/transformarea-digitala-importanta-avantaje-si-politici-ue) a accelerat în ultimii ani, dând naștere la noi oportunități, dar și unor noi provocări, cum este securitatea cibernetică. Pe măsură ce viețile noastre depind tot mai mult de tehnologii digitale, atacurile cibernetice devin tot mai costisitoare. Securitatea cibernetică a devenit foarte importantă și o prioritate majoră pentru UE.

Calculatorul oricărei persoane fizice, care nu are un minimum de cunoștințe în domeniul securității informaționale/cibernetice, poate fi ținta unui atac sau poate fi folosit pentru un atac cibernetic, fără ca măcar să știe acest lucru. Educarea societăţii civile în sensul creşterii culturii de securitate, dar şi creşterea încrederii între stat şi societatea civilă sunt puncte esenţiale de atins în obţinerea unui deziderat privind spaţiul cibernetic.

În acest sens, modernizarea programelor de studii existente la nivelul învăţământului gimnazial, dar şi pregătirea personalului din administraţia publică şi formarea unor magistraţi cu competenţe în domeniul securităţii informaționale ar putea să soluţioneze câteva din problemele pe care le regăsim la nivelul societăţii civile.

**Atacuri cibernetice împotriva păcii și securității**

Atacurile cibernetice, desfășurate concomitent cu dezinformarea, presiunile economice sau atacuri armate convenționale, [pun la încercare reziliența statelor](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698032/EPRS_ATA(2021)698032_EN.pdf) și instituțiilor democratice, atentând în mod direct la pacea și securitatea UE. Conform ENISA, în timpul războiului rus în Ucraina atacurile cibernetice au loc în paralel cu acțiunile militare convenționale. Hackerii urmăresc să distrugă sau să perturbe funcționarea agențiilor guvernamentale și a entităților ce țin de infrastructura esențială, și de asemenea să submineze încrederea publicului în conducerea țării.

**Consecințe pentru serviciile esențiale și sectoarele critice**

**Serviciile esențiale și critice,**cum ar fi transporturile, energia, sănătatea și sectorul financiar, au devenit tot mai dependente de tehnologii digitale. Acest lucru, coroborat cu creșterea numărului de obiecte fizice conectate la internetul lucrurilor, poate avea consecințe directe, inclusiv transformarea securității cibernetice într-o problemă de viață și de moarte.

De la atacuri cibernetice asupra [spitalelor](https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis), forțându-le să amâne proceduri medicale urgente, la atacuri asupra rețelelor de electricitate și rezervelor de apă - atacatorii pun în pericol furnizarea de servicii esențiale. Atacurile cibernetice pot afecta milioane de oameni în același timp - de exemplu, un atac de tip ransomware din mai 2021 a blocat majoritatea serviciilor de sănătate din Irlanda pentru câteva ore, iar repercusiunile s-au resimțit câteva săptămâni după atac. Pe măsură ce automobilele și casele devin tot mai conectate, acestea ar putea fi la rândul lor amenințate sau exploatate în moduri neprevăzute.

Securitatea Republicii Moldova este o parte componentă a securităţii mondiale. Emergenţa ameninţărilor asimetrice în epoca globalizării contemporane implică necesitatea consolidării relaţiilor de parteneriat durabil în cadrul sistemului complex al comunităţii informative în scopul diminuării riscurilor ce pun în pericol securitatea naţională şi regională. Prevenirea şi contracararea ameninţărilor la adresa securităţii Republicii Moldova este un demers în care Serviciul de Informaţii şi Securitate cooperează cu serviciile speciale şi structurile partenere în plan regional şi internaţional. După anul 1991, odată cu fondarea instituţiei, evoluţia raporturilor de cooperare ale SIS a cunoscut o dinamică pozitivă, îmbrăcând varii forme: schimb de informaţii şi expertiză, participare la evenimente de profil şi realizare de operaţiuni comune cu partenerii externi.

În contextul politicii de integrare a Republicii Moldova în structurile Uniunii Europene, Serviciul îşi propune ca imperativ aderarea la platformele informative regionale, stabilirea şi promovarea relaţiilor bilaterale şi multilaterale cu instituţiile de profil de pe arena internaţională. Scopul urmărit în această interacţiune este orientat spre realizarea intereselor fundamentale de securitate naţională şi implicarea activă a SIS în crearea unui climat adecvat de securitate regională şi europeană, având ca finalitate promovarea imaginii Republicii Moldova nu doar în calitate de consumator, dar şi generator de securitate.

La nivelul statelor din UE, platformele on-line sunt tot mai mult utilizate de mediul de afaceri pentru suportul serviciilor logistice, management sau comunicare, în special datorită capacității acestora de operare multilingvistică, anulând astfel una dintre barierele principale de colaborare care se manifestă între statele Uniunii. Cu toate acestea, acest potențial este din ce în ce subminat de riscuri digitale și vulnerabilități care se manifestă tot mai mult în spațiul virtual; fraudele on-line, atacurile asupra infrastructurilor critice sau utilizarea noilor tehnologii de către rețelele de criminalitate organizată sau cele teroriste sunt completate de operațiuni cibernetice complexe de spionaj industrial executate de către entități nonstatale sau care au ca sponsori diverse națiuni. Preocupările legate de securitatea acestui domeniu, abordate inițial la nivelul statelor membre ale UE, au început să capete importanță la nivelul instituțiilor europene. Astfel, Comisia Europeană a preluat inițiativa elaborării politicilor de securitate cibernetică la nivelul Uniunii, responsabilizarea uniformizării standardelor în domeniu, a modalităților de prevenire și răspuns la atacurile cibernetice, a colaborării între diversele organisme cu vocație în apărarea cibernetică. Uniunea Europeană lucrează la întărirea securității cibernetice. În noiembrie 2022, Parlamentul a adoptat [directiva privind securitatea rețelelor și a sistemelor informatice (NIS2)](https://www.europarl.europa.eu/news/ro/headlines/security/20221103STO48002/noile-norme-de-securitate-cibernetica-ale-ue-explicate), care stabilește reguli cuprinzătoare pentru a consolida reziliența la nivelul UE. Tot în noiembrie 2022 deputații europeni au adoptat legi pentru a crește rezistența sectorului financiar al UE la atacurile cibernetice prin actul privind reziliența operațională digitală (Dora).

Creșterea angajamentului Comisiei Europene de a extinde resursele industriale şi colaborarea cu actorii internaționali sunt considerate elemente critice, deoarece acestea joacă un rol determinant în realizarea rezilienței cibernetice, reducerea criminalității informatice şi consolidarea sistemului european de apărare cibernetică. În februarie 2013, Comisia Europeană a adoptat „Strategia de Securitate Cibernetică a Uniunii Europene”, denumită „Un spațiu cibernetic deschis, sigur și securizat”, în scopul de a reduce şi de a preveni mai eficient criminalitatea informatică. La elaborarea acestei Strategii, obiectivele principale ale Comisiei Europene în domeniul securității cibernetice și, implicit, a rezilienței cibernetice au fost:

* a) creșterea capacității securității cibernetice şi a cooperării în scopul prevenirii riscurilor şi amenințărilor. Prin acest obiectiv se urmărește a se aduce capabilităților de asigurare un nivel confortabil al securității cibernetice la același nivel de dezvoltare în toate statele membre ale UE şi de a dezvolta un cadru conceptual care să asigure eficiența schimburilor de informații și cooperării inclusiv la nivel transfrontalier. În acest domeniu, „Directiva privind Securitatea Sistemelor şi Rețelelor Informatice” (The Directive on security of network and information systems)2 , numită şi directiva NIS, este principalul instrument de susținere a rezilienței cibernetice în UE;
* b) transformarea UE într-un jucător puternic în securitatea cibernetică. Prin acest obiectiv se subliniază faptul că Uniunea Europeană trebuie să își amplifice eforturile în cultivarea unui avantaj competitiv în domeniul securității cibernetice, pentru a se asigura că cetățenii europeni, organizațiile comerciale, sistemul administrației publice şi componentele de apărare au acces la cele mai recente, interoperabile și competitive tehnologii de securitate digitală, având un nivel de încredere ridicat și care sunt dezvoltate şi implementate pe baza unor politici care respectă drepturile fundamentale ale cetățenilor, inclusiv dreptul la viață privată. De asemenea, prin acest document se susține dezvoltarea capacităților de cooperare economică, pentru a se profita de expansiunea pieței de servicii în domeniul securității cibernetice la nivel mondial. Pentru a realiza acest lucru, UE are nevoie să depășească fragmentarea actuală a pieței de securitate cibernetică şi să stimuleze industria europeană de securitate cibernetică. Comisia Europeană are ca obiectiv strategic consolidarea capacităților industriale din Uniune specifice domeniului;
* c) integrarea securității cibernetice în cadrul politicilor viitoare ale Uniunii Europene; practic se dorește asigurarea cadrului procedural necesar încorporării elementelor privind securitatea cibernetică în viitoarele inițiative politice ale UE încă din faza de elaborare, în special cele privitoare la noile tehnologii și sectoare emergente. „Strategia de Securitate Cibernetică a Uniunii Europene” oferă un cadru comun de cooperare, prin abordarea cuprinzătoare, care să reunească domeniile de politică de securitate a informațiilor, a rezilienței rețelelor, Politica de Securitate şi Apărare Comună a UE, justiția penală și afacerile externe. Se observă, însă, necesitatea existenței unui set omogen de instrumente politice care ar putea ajuta la focalizarea unui astfel de efort.

În conformitate cu mandatul său, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) deține un rol important în facilitarea consolidării rezilienței cibernetice în cadrul UE, în special în ceea ce privește reducerea decalajelor între capacitățile tehnice şi operaționale ale statelor membre. ENISA a fost creată inițial, la 10 martie 2004, ca o entitate pur complementară a Comisiei Europene, în scopul de a ajuta la prevenirea, analiza şi răspunsul Comisiei la probleme de securitate cibernetică în spațiul UE. Această Agenție este un centru de expertiză pentru securitatea informațiilor şi a rețelelor ITC pentru organismele UE, pentru cele ale statelor membre, pentru cele care aparțin sectorului privat transeuropean şi individual și pentru cetățenii Europei. În acest sens, ENISA cooperează cu aceste grupuri pentru dezvoltarea normativelor şi a recomandărilor cu privire la bunele practici în securitatea informațiilor. În domeniul rezilienței cibernetice, ENISA este instituția principală din cadrul UE, având atribuții în studiul şi elaborarea strategiilor pentru reducerea fragmentării existente în abordarea europeană a securității cibernetice, prin derularea de programe de dezvoltare pentru reducerea decalajelor de capacități ale statelor membre. Nevoia unei înțelegeri comune a securității cibernetice este unul dintre obiectivele principale asumate de către ENISA, fapt dovedit și prin publicarea, în decembrie 2015, raportului „Definiția Securității Cibernetice ‒ Lacune şi suprapuneri în domeniul standardizării” (Definition of Cybersecurity ‒ Gaps and overlaps in standardization). Din cauza naturii vulnerabilităților cibernetice, care se pot manifesta în întreg spațiu virtual și care generează mecanisme de risc care până în prezent s‑au dovedit neguvernabile, consolidarea rezilienței cibernetice şi atenuarea impactului riscurilor diverse necesită o abordare multilaterală. În această privință, ENISA, prin forma sa de organizare, îmbunătățește schimbul de informații între diverși actori, acționează ca intermediar între diversele echipe de experți pentru evaluarea capabilităților de apărare şi răspuns la incidente de securitate cu manifestare dominantă în spațiul cibernetic, identifică lacunele strategice sau operaționale ale acestor capabilități şi evaluează politicile pentru modelarea schemelor de apărare şi elaborarea unui răspuns la nivel național și european. În același timp, ENISA este agenția europeană responsabilă pentru elaborarea, revizuirea anuală şi propunerea spre avizare de către Comisia Europeană a „Listei Cadrul de Certificare Cloud” – CCSL (Cloud Computing Certification), document care reunește sub un cadru unic de compatibilitate, schemele de certificare ale autorităților recunoscute pe teritoriul UE.

La 22 martie 2021, Consiliul a adoptat concluzii privind Strategia de securitate cibernetică, care subliniază că securitatea cibernetică este esențială pentru **construirea unei Europe reziliente, verzi și digitale**. Miniștrii din UE au stabilit ca obiectiv-cheie atingerea autonomiei strategice, menținând în același timp o economie deschisă. Aceasta include consolidarea capacității de a face alegeri autonome în domeniul securității cibernetice, cu scopul de a consolida **poziția de lider a UE în domeniul digital** și capacitățile sale strategice.

Credeți că există o soluție care poate răspunde tuturor nevoilor? Probabil ca nu, însă sunt de părere că există modele care funcționează corect și care pot inspira orice profesionist în domeniul educației cibernetice. Voi încerca să prezint aceste modele din unghiul de analiză al practicianului. Și anume:

1. • Modelul de cooperare globală care stă la baza campaniei de advocacy Cyber Security Awareness Month.
2. • Modelul de cooperare europeană care stă la baza European Cyber Security Challenge.
3. • Modelul de cooperare globală care stă la baza Safer Internet Day.
4. • Modelul de cooperare globală care stă la baza Girls in ICT Day.
5. • Modelul de cooperare europeană care stă la baza Code Week.
6. • Modelul de cooperare globală care stă la baza Data Protection Day.

**1)** Această inițiativă a fost creată în urma unui parteneriat public-privat între Guvernul american și o Asociație de profil din Washington, urmând să se dezvolte progresiv în SUA prin implicarea reprezentanților din companiile de tehnologie din Silicon Valley, apoi la nivel internațional prin parteneriate guvernamentale și evenimente ca Internet Governance Forum. În Uniunea Europeană parteneriatul transatlantic a fost stabilit abia în 2010, când strategia menționa cooperarea pentru luna de advocacy și organizarea de exerciții cibernetice. În Europa campania a crescut pas cu pas, în 2011 a fost editat un raport de fezabilitate, în 2012 a fost organizat un pilot, apoi în 2013 au fost implicate peste 20 de țări. După câteva ediții campania crește exponențial deja, urmând pașii bine stabiliți de la prima ediție în 2013 și anume: coordonator de țară, activități în parteneriat publicprivat, întâlniri frecvente online între principalii actori. Este important de adăugat că partenerii sunt susținuți prin advocacy și lobby, mijloace nemateriale. În acest caz, principalul atu este menționarea acestei inițiative în strategia europeană de cyber security din februarie 2013, fiind element definitoriu pentru implementare la nivel european.

**2)** Această inițiativă implementată din nou în parteneriat public-privat a fost dificil de inițiat ținând cont de factori ca o piață bogată de companii de cyber security. Aceste companii erau/sunt foarte active și interesate exclusiv de atragerea de noi talente. După o coordonare dificilă la început, în momentul de față inițiativa a devenit un mare succes, susținută de un buget din ce în ce mai mare. Voi scoate în evidență două aspecte: parteneriatul public a adus coerență în coordonarea actorilor prezenți și coordonarea cu politicile publice în domeniu. Apoi organizațiile private au fost motivate de crearea de competențe digitale avansate de care piața/companiile au nevoie.

**3)** Această inițiativă s-a dezvoltat într-un ritm impresionant fiind inițiată de un proiect academic finanțat de Uniunea Europeană. În momentul de față a depășit orice indicator de succes stabilit în prealabil și este o inițiativă globală pentru activități punctuale de educație online. Cred că este important de menționat suportul primit de o rețea academică de profesori, coordonarea centrală de către o echipă unică.

**4)** Pentru modelul de față, două aspecte sunt de interes pentru acest articol. În primul rând efortul instituțional pentru promovarea inițiativei. În al doilea rând implicarea centrată pe țările membre ITU. Statistica arată că inițiativa crește în susținere, însă observația mea este că obiectivul sau misiunea declarată de la început se schimbă pe parcurs. În momentul de față promovarea ICT în rândul fetelor este o misiune globală, fără corelare geografică sau economică pentru publicul țintă.

**5)** Această inițiativă lansată la nivel european și devenită mișcare internațională a început în 2013 într-o întâlnire de lucru în dialog instituțional. Rețeaua Young Advisors convocată de comisarul european pentru Digital Agenda Europe a constituit laboratorul perfect. Comisia Europeană a sprijinit această idee prin planificare multianuală și o libertate de implementare pentru toți voluntarii implicați. În plus, încă de la primele ediții inițiativa a beneficiat de ambasadori pentru fiecare țară implicată, acest lucru participând la creșterea motivării și implicare. Un alt punct forte al inițiativei consider că este descentralizarea coordonării. Acest element crește semnificativ implicarea, însă pierde structura comună a activităților.

**6)** În contextul acestei inițiative merită să observăm corelarea proiectului cu strategia politicii publice existente. Sărbătorită în fiecare an în ianuarie, inițiativa a crescut în importanță odată cu adoptarea GDPR în UE și nu numai. Însă campania nu este susținută de o coordonare centrală sau resurse educaționale relevante.

Concluzie: Prin prezentarea acestor exemple oferite de peisajul de cyber security la nivel internațional îmi doresc să evidențiez diferențele și asemănările dintre acestea. Modelul de bază care funcționează eficient nu este neapărat promovat de resurse financiare abundente ale unui singur actor, ci mai degrabă de o strategie de conținut și un model de coordonare pentru actorii implicați. Pașii de urmat în dezvoltarea unei bune cooperări internaționale în domeniul educației securității cibernetice sunt:

**a.** Planifică o strategie cu obiective măsurabile și comunică către toți actorii implicați același mesaj. O singură voce coordonată!

**b.** De la o ediție la alta, îmbunătățește conținutul educativ și participarea actorilor interesați. Încurajează parteneriatele de orice natură!

**c.** Îmbunătățește interacțiunea printr-o coordonare flexibilă. Dă dreptul la acțiune fiecărui actor implicat!

**Importanța cooperării în aria securității cibernetice**

Spațiul cibernetic este considerat al cincilea câmp de luptă, la fel de important pentru operațiile militare ca și domeniile terestru, maritim, aerian și spațial. Este un domeniu care cuprinde totul, de la rețelele de informații și telecomunicații, infrastructură și datele pe care le sprijină până la sistemele informatice, operatori și persoanele împuternicite de operatori.

UE cooperează în domeniul apărării în spațiul cibernetic prin activitățile **Agenției Europene de Apărare** (AEA), în colaborare cu Agenția UE pentru Securitate Cibernetică și cu Europolul. AEA sprijină statele membre în construirea unei forțe de muncă militare competente în domeniul apărării cibernetice și asigură disponibilitatea unei tehnologii proactive și reactive în domeniul apărării cibernetice.

**Strategia de securitate cibernetică a UE**, adoptată în decembrie 2020 de Comisie și SEAE, consolidează:

* coordonarea apărării cibernetice
* cooperarea și consolidarea capabilităților de apărare cibernetică

**Politica pentru apărarea cibernetică a UE**, adoptată în noiembrie 2022 de Comisie și SEAE, urmărește să stimuleze capabilitățile de apărare cibernetică a UE și să consolideze coordonarea și cooperarea dintre comunitățile cibernetice militare și civile.

La 23 mai 2023, Consiliul a adoptat **concluzii privind politica UE în domeniul apărării cibernetice**, subliniind importanța consolidării în continuare a rezilienței UE pentru a face față amenințărilor cibernetice.

Complexitatea sistemelor dezvoltate în ultimii ani în majoritatea domeniilor reprezintă o consecință directă a diversității subsistemelor și a elementelor componente ale acestora, ce au condus la creșterea gradului de interacțiune dintre diversele tehnologii și arhitecturi utilizate în implementarea unui sistem informatic. Asigurarea securității sistemelor a devenit un proces decizional complex, care necesită dezvoltarea unor instrumente manageriale aplicate cu privire la procesul de adoptare a deciziilor. Ca o consecință directă, informațiile referitoare la comportamentul unui sistem complex și interacțiunile dintre subsisteme nu pot fi ușor observate și controlate de un singur operator. Prin urmare, comportamentul sistemelor complexe sau al unor părți componente poate fi uneori imprevizibil în timpul funcționării, în contradicție cu funcțiile și obiectivele pentru care acestea au fost proiectate. Dezvoltarea unui sistem care să îndeplinească misiunea pentru care a fost proiectat, în prezența unei amenințări la adresa performanțelor și securității (defect, atac cibernetic, dezastru natural etc.), precum și asigurarea funcțiilor critice ale sistemului inițial, sunt reunite în conceptele de reziliență și survivabilitate (caracteristica de supraviețuire a unui sistem).

Principalele caracteristici asociate conceptului de survivabilitate, implică integritatea și disponibilitatea. Aceasta include luarea în considerare, la proiectarea sistemelor, a întrebărilor „cum” și „cât”, precum și o evaluare a riscurilor speciale. Astfel de riscuri pot fi limitate, având în vedere resursele și abilitățile sistemului pentru a oferi un nivel optim al serviciilor, prin definirea unei capacități de apărare și răspuns, cunoscute în momentul respectiv. Având o viziune de perspectivă, se presupune că provocările referitoare la performanța sistemului vor avea loc și se caută în mod activ noi modalități de combatere a amenințărilor. Importanța domeniului calității și fiabilității sistemelor complexe critice, în special a securității și dependabilității, este subliniată de numeroasele programe și proiecte aflate în derulare la nivelul Uniunii Europene, prin Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor. Obiectivul central este de a stimula și sprijini dezvoltarea unui nivel ridicat al capacității de reacție și răspuns, de securitate și de reziliență, atât la nivelul statelor membre (național), cât și la nivel european. Această abordare a fost aprobată în linii mari de către Consiliu începând cu anul 2009.

Strategia europeană și planurile de acțiune ale statelor membre, de protecție împotriva amenințărilor din spațiul cibernetic, cuprind direcții de acțiune cum ar fi pregătire și prevenire, detecție și reacție și reziliența infrastructurilor. Una din direcțiile care a căpătat o importanță deosebită este reprezentată de cooperarea la nivel național și internațional în domeniu. Astfel, începând cu anul 2013, încă de la versiunea de lucru a Directivei NIS - Network and information security across the EU - 2013/0027(COD), se stabilește ca măsură prioritară „crearea unui mecanism de cooperare între statele membre și Comisia Europeană pentru a împărtăși / distribui avertismentele timpurii privind riscurile și incidentele, pentru a face schimb de informații și a combate amenințările și incidentele NIS”. În versiunea finală a Directivei NIS este pus accentul pe „creșterea cooperării în domeniul securității cibernetice între statele membre ale UE” și se introduce necesitatea adoptării „măsurilor de securitate și a obligațiilor de raportare a incidentelor pentru furnizorii de servicii digitale și operatorii de servicii esențiale care dețin infrastructură națională critică”.

Numărul tot mai mare și complexitatea amenințărilor cibernetice necesită măsuri și acțiuni în vederea consolidării cooperării internaționale pentru a contribui la dezvoltarea de tehnologii, produse și servicii inovatoare și sigure. Cu toate acestea, nivelul de amenințare este în continuă evoluție, iar gestionarea unui incident cibernetic la scară largă, care implică simultan mai multe state, va fi o provocare.

Cooperarea la nivelul european este, prin urmare, esențială pentru a face față atât atacului cibernetic pe scară largă (în mai multe state), cât și incidentelor cibernetice mai mici, dar potențial mai frecvente. Astfel, este necesar un plan pentru o reacție coordonată, bazat pe schimbul transfrontalier de informații, pentru a aborda incidentele cibernetice în cel mai eficient mod. În acest sens, domeniul securității cibernetice trebuie integrat în mecanismele și procedurile existente pentru gestionarea situațiilor de urgență, în scopul de a obține o coordonare cu celelalte sectoare potențial afectate de un incident cibernetic. Principalele mecanisme de cooperare la nivel european sunt: - Grupul de cooperare - sprijină cooperarea strategică și schimbul de informații relevante privind incidentele cibernetice în rândul statelor UE; - CSIRT - rețeaua de echipe de răspuns la incidentele de securitate a calculatoarelor, care promovează o cooperare operațională rapidă și eficientă privind incidente specifice în domeniul securității informatice și al schimbului de informații.

La nivel internațional, țări ca Statele Unite ale Americii, Japonia sau China au adoptat strategii de cooperare în domeniu, prin definirea de mecanisme dinamice pe mai multe niveluri de colaborare cu alte state în vederea partajării informațiilor și a modalităților de contracarare a incidentelor. Schimbul de informații privind criminalitatea informatică și colaborarea cu instituții din alte state trebuie reglementate prin stabilirea unui cadru privind cooperarea internațională pentru asigurarea securității în spațiul cibernetic. Atacurile cibernetice sunt de obicei transnaționale și dificil de atribuit, țările ar trebui să colaboreze pentru a asigura securitatea cibernetică prin cooperare constructivă și consultare continuă. În prezent, cunoștințele și expertiza privind securitatea cibernetică sunt disponibile într-un mod dispersat și nestructurat. În acest sens, apare necesitatea unui cadru internațional agreat privind o cooperare consolidată împotriva unui atac cibernetic de scară largă prin colaborarea structurilor de specialitate naționale (CERT, CSIRT etc.). Mecanismele dezvoltate trebuie să pună accent pe partajarea cunoștințelor despre vulnerabilități și amenințări, utilizarea de proceduri și standarde comune în atenuarea acestora, valorificarea bunelor practici și a lecțiilor învățate ale altor state și încurajarea unei culturi a încrederii reciproce. Distribuția pe domenii de activitate a CSIRT-urilor active în spațiul european arată o dezvoltare în special în zona societăților comerciale, a administrației publice și în mediul educație academică - cercetare.

În domeniul securității cibernetice, cooperarea se realizează prin acorduri punctuale între organizații, pe orizontală (sectoriale naționale) sau verticală (structuri internaționale / naționale). Cele mai recomandate modalități de realizarea a unei cooperări eficiente este prin acorduri bilaterale (organizații internaționale sau punctual cu alte țări) și multilaterale, cum ar fi modelul de colaborare a CERT-urilor naționale din țările nordice Danemarca, Finlanda, Islanda, Norvegia și Suedia prin NORDUnet CERT și NCIRC CC - NATO Communication and Information Agency’s Cyber Security. Un alt plan necesar a fi dezvoltat este cel al cooperării între părțile civilă și militară și examinarea modalităților prin care ambele domenii pot învăța unele de la altele în ceea ce privește formarea și exercitarea, pentru a spori capacitățile de reziliență și de reacție la incidente. Câteva direcții care pot fi urmate sunt: - dezvoltarea unor platforme de educație, poligoane pentru exerciții cibernetice comune având ca obiective exersarea și evaluarea modului de gestionare a incidentelor cibernetice, răspunsul la nivel operațional, tactic și strategic; - optimizarea procesului de cooperare în vederea identificării și limitării impactului incidentelor prin abordări simplificate. Provocările și amenințările din spațiul cibernetic ignoră granițele naționale și au schimbat percepția asupra securității la nivelul unei societăți prin dependența din ce în ce mai mare de infrastructurile naționale. Interdependența economică și alte aspecte ale coexistenței moderne ar trebui să conducă și să ajute la dezvoltarea unei comunități internaționale și a unei culturi solide de cooperare în domeniul securității cibernetice.

**Combaterea criminalității informatice**:

Evoluția crimei organizate în R. Moldova, în ultimii ani este strâns legată de evoluția criminalității informatice și de folosirea tot mai intensă a tehnologiei informației și comunicațiilor, în comiterea de infracțiuni. Dezvoltarea fenomenului criminalității informatice se manifestă sub mai multe aspecte:

- creșterea numărului de cazuri înregistrate privind criminalitatea informatică;

- preocuparea infractorilor pentru identificarea de noi moduri de operare;

- reorientarea grupărilor criminale către infracțiuni de natură informatică.

Principalii factori care au determinat orientarea grupărilor criminale către infracțiuni informatice sunt obținerea de câștiguri materiale mari într-un timp relativ scurt și cu riscuri relativ mici, caracterul transfrontalier al infracțiunilor, accesul facil la echipamente IT moderne, precum și la instrumente software și tutoriale ce pot fi descărcate ușor din zona neindexată a Internet-ului - DarkNet.

La nivelul R. Moldova, criminalitatea informatică se manifestă sub următoarele aspecte: atacuri cibernetice, ce urmăresc compromiterea diferitor rețele și sisteme informatice prin multiple moduri și instrumente (malware, ransomware, atacuri de tip DDoS sau Defacement), fraudele informatice, constând în licitații fictive de bunuri, compromiterea conturilor utilizatorilor pe site-uri de comerț electronic sau realizarea unor site-uri de phishing pentru colectarea datelor bancare și fraudele cu cărți de credit, constând în compromiterea bancomatelor și extragerea unor informații confidențiale din cardurile clienților.

Persoanele implicate în activități de criminalitate informatică folosesc metode complexe de inginerie socială, conving victimele să divulge informații confidențiale sau să desfășoare acțiuni care să ducă la infectarea sistemelor informatice pe care le folosesc sau administrează. În foarte multe cazuri, sistemele informatice astfel infectate devin părți componente ale unor rețele de tip botnet, care sunt folosite la executarea unor atacuri cibernetice coordonate de tip DDoS împotriva unor infrastructuri cibernetice administrate de instituții publice. Se observă un trend îngrijorător al implicării tot mai multor persoane de vârste fragede și chiar minore în săvârșirea infracțiunilor informatice, acestea neavând o viziune clară asupra consecințelor juridice ce decurg din astfel de acțiuni. În acest sens se impune o mai bună informare a publicului și chiar campanii derulate în școli cu privire la combaterea și prevenirea criminalității informatice în rândul copiilor și tinerilor. Unele din cele mai frecvent întâlnite atacuri cibernetice în R. Moldova, ca de altfel și în Europa, constau în infectarea sistemelor informatice cu malware de tip ransomware. Acest ransomware criptează datele de pe sistemul informatic utilizat de victimă, iar singura modalitate prin care datele se pot recupera este plata unei chei de decriptare. Atacurile ce distribuie ransomware au devenit o problemă enormă pentru securitatea cibernetică în ultimii ani. Numărul de utilizatori infectați cu ransomware crește constant.

Poliția nu poate lupta împotriva singură împotriva acestor forme de atacuri, în special a răscumpărării, deoarece plățile către infractorii cibernetici sunt realizate în moneda virtuală Bitcoin. Lupta împotriva ransomware-ului la nivelul Europei necesită un efort comun între poliție, departamentul de justiție, Europol și companiile de securitate IT. În acest sens, pentru conștientizarea pericolelor reprezentate de răspândirea diverselor forme de ransomware, Centrul European de Criminalitate Informatică EC3, în parteneriat cu Poliția olandeză, două companii de securitate cibernetică (Kaspersky Lab și McAfee) și cu alți parteneri fondatori și asociați, au dezvoltat portalul No More Ransom. Lansat în iulie 2016, acest exemplu de parteneriat public-privat internațional are ca scop nu doar lupta împotriva fenomenului ransomware, ci și educarea utilizatorilor din întreaga lume cu privire la modul de prevenire a atacurilor de acest tip.

**Divulgarea coordonată a vulnerabilităților informatice**

Numărul incidentelor de securitate cibernetică ce exploatează vulnerabilități ale programelor, serviciilor și sistemelor informatice este în continuă creștere din cauza lipsei unei metodologii de testare a vulnerabilităților. Vulnerabilitățile sunt defecte în codul software ce pot fi exploatate pentru a compromite confidențialitatea, disponibilitatea sau integritatea sistemelor afectate. Remedierea vulnerabilităților este, prin urmare, crucială pentru asigurarea securității cibernetice, iar un proces de divulgare a vulnerabilităților reprezintă un element semnificativ în reducerea riscurilor de securitate. Însă vulnerabilitățile informatice, în special cele de tip zero-day, sunt căutate pentru comercializare pe piața neagră, pentru a fi exploatate în atacuri cibernetice, ducând astfel la pierderi însemnate și punând în pericol datele cetățenilor și funcționarea sistemelor și serviciilor în spațiul cibernetic. În procesul de divulgare a vulnerabilităților pot fi implicate numeroase părți interesate, cum ar fi producători/furnizori de software, furnizori de securitate IT, cercetători, publicul larg, dar și infractorii cibernetici. Aceste părți interesate pot avea interese conflictuale, ceea ce poate duce la provocări privind rezolvarea vulnerabilităților descoperite, cum ar fi constrângerile legale sau lipsa de încredere.

Cooperarea dintre instituții, organizații și comunitatea online creată în jurul topicului „securitate cibernetică” poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilității (CVD - Coordinated Vulnerability Disclosure) sau divulgarea responsabilă. În esență, aceasta este o formă de cooperare în care un raportor informează proprietarul sistemului informatic, permițându-i acestuia posibilitatea de a diagnostica și remedia vulnerabilitatea înainte ca informațiile trecute cu privire la vulnerabilitate să fie divulgate terților sau publicului larg.

Obiectivele unei politici coordonate privind divulgarea vulnerabilităților includ:

- asigurarea abordării vulnerabilităților identificate;

- minimizarea riscului de securitate provenit de la vulnerabilitățile identificate;

- furnizarea unor informații suficiente pentru evaluarea riscurilor legate de vulnerabilitățile sistemelor;

- stabilirea așteptărilor privind comunicarea și coordonarea pozitivă între părțile implicate.

O politică eficientă de divulgare coordonată a vulnerabilităților poate minimiza șansele ca actorii rău-intenționați să profite de vulnerabilitățile informatice, construi încrederea clienților în ceea ce privește securitatea datelor acestora, aduce informații suplimentare despre noi vulnerabilități relevante și contribui la sporirea nivelului de securitate cibernetică.

Procesul de divulgare a vulnerabilităților implică de obicei următorii pași:

- descoperirea unei vulnerabilități de către un raportor;

- notificarea proprietarului sistemului informatic afectat;

- investigarea vulnerabilității potențiale și a impactului acesteia;

- confirmarea a vulnerabilității (dacă este cazul);

- oferirea de soluții pentru remedierea sau eliminarea vulnerabilității;

- divulgarea publică a informațiilor despre vulnerabilitate.

În practică pot exista multe varietăți ale procesului de divulgare. Descoperirea unei vulnerabilități poate duce la vânzarea acestei informații unei terțe părți sau la dezvăluirea imediată în spațiul public, oferind dezvoltatorilor de software foarte puțin sau deloc timp pentru a rezolva vulnerabilitatea. Între aceste două situații se poate face o divulgare coordonată a vulnerabilității, în care raportorul și producătorii/furnizorii coordonează acțiunile și termenele înainte de divulgare. În ultimii ani a crescut dorința de a contribui la creșterea nivelului de securitate cibernetică, fiind tot mai frecvent întâlnite raportarea vulnerabilităților descoperite unei terțe părți neutre, precum echipele de tip CERT.

Având în vedere caracterul complex al divulgării coordonate a vulnerabilităților și interesele conflictuale ale părților interesate implicate, există multiple provocări asociate cu dezvăluirea vulnerabilităților: - raportorii se pot confrunta cu amenințări legale atunci când descoperă o vulnerabilitate (răspundere civilă, răspundere penală sau alte legi); - pot apare conflicte între părțile interesate implicate, ducând la lipsa de încredere între părțile interesate; - producătorii / furnizorii și organizațiile de utilizatori pot să nu aibă procese de raportare a vulnerabilităților, putând astfel acționa incorect; - raportarea în spațiul public a vulnerabilităților descoperite poate introduce noi riscuri pentru organizații, cum ar fi daune de reputație sau litigii; - utilizatorii ar putea vinde vulnerabilitățile identificate pe piețele negre, în vederea unor câștiguri financiare; - comunitățile de utilizatori pot fi reticente în a aplica direct patch-urile furnizate pentru vulnerabilitățile raportate, lăsând astfel produsele software-ul nesigure.

Încrederea și cooperarea sunt esențiale pentru divulgarea coordonată a vulnerabilităților cibernetice. În contextul necesității de a primi ajutorul publicului pentru menținerea securității cibernetice, un prim pas pe care toate organizațiile și instituțiile îl pot face este cooperarea prin mecanisme de raportare coordonată și responsabilă a vulnerabilităților sistemelor și serviciilor informatice. Guvernele au un rol de facilitare în introducerea și punerea în aplicare a unei politici privind divulgarea coordonată a vulnerabilităților. Astfel, ar fi necesară: - stabilirea unei terțe părți de încredere, ca de exemplu un CSIRT; - implementarea unui mecanism de armonizare internațională a divulgării coordonate a vulnerabilității și a legislațiilor relevante; - stimularea unei culturi mai deschise în care vulnerabilitățile sunt acceptate și recunoscute; - stimularea platformelor on-line de partajare a informațiilor; - implicarea comunității cercetătorilor de securitate; - sprijinirea sectorului juridic în identificarea posibilităților și reducerea riscurilor în ceea ce privește divulgarea coordonată responsabilă; - includerea divulgării coordonate a vulnerabilităților în cerințele de achiziții publice.

Interesul pentru dezvoltarea domeniului divulgării coordonate a vulnerabilităților este demonstrat de diversele programe și abordări în cadrul companiilor producătoare de software și corporațiilor din domeniu (Microsoft Security Response Center, Vendor Vulnerability 63 Reporting and Disclosure Policy – Cisco) și în mediul academic - Software Engineering Institute - Carnegie Mellon University.

**CONCLUZII:**

Atacurile cibernetice, noi și sofisticate din punct de vedere tehnologic, pot perturba sau chiar distruge funcții economice și societale vitale din cadrul UE. Pentru a face față acestora, UE construiește cooperarea cu alți parteneri internaționali atât la nivel bilateral, cât și prin alte instrumente şi organizații regionale. Exemple, în acest sens, sunt: „Grupul de lucru UE-SUA” privind securitatea cibernetică și criminalitatea informatică; angajamentele bilaterale cu India, Brazilia și China. Politica de apărare cibernetică, dezvoltată prin „Politica Cadru pentru Apărare Cibernetică” (EU CYBER Defence Policy Framework ‒ ECDPF), din anul 2014, este menită să consolideze în continuare cooperarea cu Organizația Tratatului Nord-Atlantic, o organizație care, în calitate de furnizor de securitate pe plan internațional, și-a construit capacitățile de apărare cibernetică folosind un concept specific adaptat unei plaje largi de amenințări cibernetice prin folosirea unui plan de acțiune coerent şi detaliat.

Cooperarea internațională joacă un rol-cheie în acest domeniu, deoarece provocările privind securitatea cibernetică depășesc granițele, extinzându-se până la nivelul sistemelor interconectate la nivel global. Amenințările și vulnerabilitățile cibernetice continuă să evolueze și să se intensifice, ceea ce va necesita o cooperare continuă, mai strânsă, în special în ceea ce privește gestionarea incidentelor de securitate cibernetică transfrontaliere de mare amploare. Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale. Cooperarea operațională și gestionarea crizelor în domeniul cibernetic ar trebui să se bazeze pe consolidarea capabilităților operaționale de prevenire existente, în special prin modernizarea exercițiilor paneuropene de securitate cibernetică.

Prin activitățile desfășurate destinate a face față amenințărilor cibernetice, Uniunea Europeană intensifică eforturile de îmbunătățire a rezilienței cibernetice, continuând să promoveze valorile europene de libertate și democrație și de garantare a creșterii economiei digitale în condiții de siguranță.

Este necesară instituirea unei cooperări structurate cu ENISA, CERT-EU, Centrul European de Combatere a Criminalității Informatice (EC3) și cu alte organisme relevante ale U.E. Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților. O politică eficientă de divulgare coordonată a vulnerabilităților poate minimiza șansele ca actorii rău-intenționați să profite de vulnerabilitățile informatice, construi încrederea clienților în ceea ce privește securitatea datelor acestora, aduce informații suplimentare despre noi vulnerabilități relevante și contribui la sporirea nivelului de securitate cibernetică. Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune / cooperare trans-sectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar.

Cercetarea și educația în domeniul securității cibernetice trebuie să reprezinte priorități ale politicilor publice. Consolidarea cercetării în domeniul securității informatice, îmbunătățirea educației și dezvoltarea forței de muncă instruite sunt esențiale pentru atingerea obiectivelor generale ale politicii privind securitatea cibernetică. Politicile în cercetare și educație vor fi eficiente doar dacă includ natura multilaterală și multidisciplinară a securității cibernetice ca element fundamental și omniprezent în cultura, abordările, procesele, sistemele și infrastructurile tehnice. Finanțarea cercetării și dezvoltării în domeniul securității informatice este indispensabilă pentru a aduce inovare și a dezvolta noi tehnologii.

Accesul extins la educația privind securitatea cibernetică la toate nivelurile (pre-universitar, universitar și post-universitar) este necesar pentru pregătirea, construirea și îmbunătățirea forței de muncă. Numeroasele posibilități pentru universități, cadre didactice și studenți de la toate ciclurile de studii (licență, master, doctorat) de a se implica în cercetări de ultimă oră, de mare impact, sunt importante pentru dezvoltarea unei puternice comunități științifice.

Colaborarea cu entități europene și internaționale este absolut necesară, fie că este vorba de unități de învățământ, centre de cercetare, companii private sau instituții guvernamentale. Cooperarea dintre instituții, organizații și comunitatea de securitate cibernetică poate fi utilă în găsirea și stabilirea vulnerabilităților. Un mecanism de cooperare dovedit în acest sens este divulgarea coordonată a vulnerabilităților. Adoptarea unor politici publice unitare la nivelul statelor membre privind divulgarea coordonată a vulnerabilităților și a unor mecanisme coordonate de acțiune/cooperare transsectoriale vor asigura ecosistemul necesar asigurării securității în spațiul comunitar. Deschiderea canalelor de comunicare, crearea de grupuri de lucru și consultare publică, implicarea societății civile și parteneriatul public-privat devin direcții cheie pe care politicile publice trebuie să se axeze. Importanța domeniului securității cibernetice în contextul global al securității unui stat, este evidențiată de multitudinea de direcții de dezvoltare a domeniului. Evoluția tehnologică și automatizarea diverselor sectoare de activitate ale unei societăți, califică domeniul securității cibernetice ca fiind o dimensiune prioritară de acțiune în dezvoltarea strategiilor naționale de apărare a statelor. Securitatea cibernetică necesită un cadru legislativ, adaptat atât la noile amenințări tehnologice, cât și la necesitatea de respectare a drepturilor civile, aliniate ca principii de bază în strategiile naționale de apărare ale statelor.

Reglementările legislative existente, precum și gradul de operaționalizare al acestora la nivelul instituțiilor publice din R. Moldova nu permit, în prezent, prevenirea și contracararea cu maximă eficiență a unor amenințări cibernetice de nivel mediu și ridicat. Actualizarea Strategiei de securitate cibernetică a RMoldova trebuie să includă obiective clare cu indicatori de monitorizare și evaluare a liniilor strategice din domeniu, definirea de responsabilități pentru instituțiile implicate în asigurarea securității, măsuri privind protecția datelor și proprietatea intelectuală.

Concluzionând, adoptarea unei legislații comprehensive și actualizate în domeniul securității cibernetice, care să sprijine dezvoltarea capacităților de apărare ale statului, reprezintă o prioritate națională. Asigurarea unui spațiu cibernetic sigur este responsabilitatea atât a statului, cât și a autorităților competente, a sectorului privat și a societății civile. Pentru dezvoltarea culturii de securitate cibernetică, cele mai importante pârghii sunt educația și cercetarea, parteneriatele public-private și mecanismele de cooperare la nivel european.

**BIBLIOGRAFIE:**

Cyber security month SUA [Online]. Disponibil: https://web.archive.org/ web/20140731143707/http://www.staysafeonline.org/ncsam/about.

Cyber security month UE [Online]. Disponibil: https://www.enisa.europa.eu /topics/cybersecurity-education/european-cyber-security-month.

Cyber security challenge UE [Online]. Disponibil: https://europeancyber securitychallenge.eu/about.

Safer Internet Day [Online]. Disponibil: https://www.saferinternetday.org/ about.

Girls in ICT Day [Online]. Disponibil: https://www.itu.int/en/ITU-D/ Digital-Inclusion/Women-and-Girls/Girls-in-ICT-Portal/Pages/Portal.aspx.

EU Code Week [Online]. Disponibil: https://codeweek.eu/.

Data Protection Day [Online]. Disponibil: https://www.coe.int/en/web/dataprotection/data-protection-day.

14 th International Conference on Cyber Conflict: Keep Moving, CCDCOE Publications. 2022. https://ccdcoe.org/uploads/2022/06/CyCon\_2022\_book.pdf 1.

ENISA a publicat un raport cu referire la tehnicile de securitate cibernetică pentru protecția datelor <https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>

ENISA a organizat prima conferință de politică în domeniul securității cibernetice <https://www.enisa.europa.eu/news/supporting-policy-developments-to-achieve-a-high-common-level-ofcybersecurity>

Parteneriatele NATO și Republica Moldova în fața noilor amenințări la adresa securității regionale. Chișinău, 2014, p. 47-49.

A. Miroiu, Introducere în analiza politicilor publice, Editura Punct, 2001.

A.D. Householder, G. Wassermann, A. Manion, C. King, The CERT Guide to Coordinated Vulnerability Disclosure, August 2017, CMU/SEI-2017-SR-022.

Anexă la comunicarea Comisiei către Parlamentul European și Consiliu. Valorificarea la maximum a NIS - către punerea în aplicare eficace a Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, Consiliul Uniunii Europene, 14 septembrie 2017.

C. Jugastru, „Proceduri și autorități în noul drept european al protecției datelor cu caracter personal”, Revista Universul Juridic nr. 6, iunie 2017, pp. 112-129.

Comisia Europeană - Comunicat de presă, 5 iulie 2016, <http://europa.eu/rapid/pressrelease_IP-16-2321_ro.htm>

Comunicat de presă, https://politiaromana.ro/ro/comunicate/politia-romana-si-bitdefender-contribuie-la-lupta-globala-impotriva-ransomware

Comunicat de presă, https://www.pwc.ro/en/press\_room/assets/2017/cybersecurityreport-ro.pdf

Coordinated Vulnerability Disclosure, Global Forum on Cyber Expertise (GFCE), www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

CyberWISER - Cartography of EU cyber security strategies, www.cyberwiser.eu/ cartography D. Clark, T. Berson, and H.S. Lin, At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work, 2014.

Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, Jurnalul Oficial al Uniunii Europene, 19 iulie 2016.

Directiva 2008/114/CE - identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.

Divulgarea Coordonată a Vulnerabilităților - componentă esențială a securității cibernetice, CERT-RO, https://cert.ro/citeste/divulgarea-coordonat-a-vulnerabilitilor-component-esen-ial-a-securit-ii-cibernetice

Divulgarea Coordonată a Vulnerabilităților - CVD, https://cert.ro/pagini/CVD

E.M. Hutchins, M.J. Cloppert, R.M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation, 2010.

ECONOMICA.net, http://www.economica.net/ici-vrea-sa-atraga-investitii-de-5- milioane-dolari-pentru-un-centru-de-cercetare-in-cyber-security\_135842.html

I.C. Mihai, G. Petrică, C. Ciuchi, L. Giurea, Provocări și strategii de securitate cibernetică, Editura Sitech, 2015.

I.C. Mihai, G. Petrică, Securitatea informațiilor. Ediția a II-a, îmbunătățită și adăugită, Editura Sitech, 2014.

I.C. Mihai, L. Giurea, Criminalitatea informatică. Ediția a II-a, îmbunătățită și adăugită, Editura Sitech, 2014.

International Strategy of Cooperation on Cyberspace issued by the Ministry of Foreign Affairs of the People’s Republic of China on March 1, 2017, <http://www.scio.gov.cn/32618/Document/1543874/1543874.htm>

International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity - October 2, 2013, Information Security Policy Council, Japan

L. Vasiu, I. Vasiu, „Riscul de atac electronic asupra sistemelor de informații”, capitol în Fenomene și procese cu risc major la scară națională, Editura Academiei Române, București, pag. 145-165, 2004.

„Legile pământești ale lumii virtuale”, Revista Intelligence, http://intelligence.sri.ro/ legile-pamantesti-ale-lumii-virtuale/

Luna europeană a securității cibernetice, https://www.enisa.europa.eu/news/enisanews/cybersecmonth-2017/2017-10-02%20ENISA%20Press%20Release%20- %20European%20Cyber%20Security%20Month\_RO.pdf

M. Troutt, „IT Security Issues: The Need for End User Oriented Research”, Journal of End User Computing, pp. 48-49, 2002.

Metarankingul universitar 2016, <https://www.edu.ro>

National Institute of Standards and Technology (NIST), „Special Publication 800-30: Risk Management Guide for Information Technology Systems”, July 2002.

No More Ransom, https://www.nomoreransom.org/ro/

OECD Digital Economy Outlook 2017, ISBN 9789264276284, October 11, 2017, OECD Publishing, https://books.google.ro/books?id=PIQ5DwAAQBAJ

Pan-European Status of the NIS Directive, https://geistwert.at/en/status-der-nisrichtlinie-in-den-eu-mitgliedstaaten/

Politica de raportare a vulnerabilităților, www.cisco.com/c/en/us/about/securitycenter/vendor-vulnerability-policy.html

Privacy and Data Protection by Design - from policy to engineering, ENISA, January 12, 2015.

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48.

R. G. Wilsher, and H. Kurth, „Security Assurance in Information Systems”, Sokratis K. Katsikas and Dimitris Gritzalis (Eds.), Information Systems Security: Facing the information society of the 21st century, Chapman and Hall, 1996.

Regulament al Parlamentului European şi al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

„Război hibrid și atacuri cibernetice”, Revista Intelligence , http://intelligence.sri.ro/ razboi-hibrid-si-atacuri-cibernetice/

Rezoluția Consiliului din 18 decembrie 2009 privind o abordare europeană a securității rețelelor și a informațiilor bazată pe colaborare (2009/C 321/01).

Security Updates, <https://technet.microsoft.com/en-us/security/dn440717.aspx>

United Nations Security Council resolution 2341, Physical protection of critical infrastructure against terrorist attacks, 2017, https://www.un.org/sc/ctc/wpcontent/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

V. Spiridon, Tendințe în criminalitatea informatică, Cybersecurity Trends, 1/2015.

V.V. Patriciu, M.E. Pietrosanu, I. Bica, J. Priescu, Semnături electronice și securitate informatică, Editura All, 2006.

V. Vlad, Strategia de dezvoltare a României în următorii 20 de ani, vol. II și III, Editura Academiei Române, 2016, http://www.acad.ro/strategiaAR/strategiaAR.htm