TREND HUNTER #7. IDIS.

FENOMENUL DEZINTERMEDIERII ȘI REZILIENȚA DE CARE AVEM NEVOIE

Igor Munteanu

Efectele tranziției

Trăim o lume agitată care traversează mai multe tipuri de tranziții. Anumite tranziții sunt sistemice și se referă la trecerea de la societatea industrială la societatea post-industrială (confundată uneori cu ”economia bazată pe servicii”); altele se referă la schimbarea vechiului sistem internațional bipolar cu un sistem internațional multipolar mult mai instabil și expus la conflicte. Dar există și alte tranziții care se produc în organismul societăților umane ca urmare a unor adânci mutații structurale - consecințe directe ale globalizării schimburilor comerciale și impactul tehnologiilor moderne. Să ne imaginăm pentru moment ce schimbare uriașă o are asupra indivizilor posibilitatea de a călători într-o singură zi dintr-o emisferă în alta a planetei, sau cea de a elimina aproape integral achitările cu cash pentru orice bunuri, servicii, sau la imensele rețele on-line, pentru care demult nu mai există nici un fel de bariere naturale, după cum erau frontierele sau comunitățile naționale ocrotite de stat. Impactul acestor schimbări profunde asupra conceptelor de ”putere”, ”autoritate”, ”piață”, ”mass media” este atât de răvășitor încât mulți dintre noi își pun pe bună dreptate întrebarea dacă nu asistăm la o ruptură sistemică cu tipul de lume pe care o știam până la sfârșitul sec. XX. Această ruptură elimină multe nivele intermediare între cetățean și puterea formală a statului. oferind unor grupuri și indivizi resurse simbolice și conectivități colective enorme.

Sute de milioane de indivizi de pe mai mulate continente pot forma, în acest fel, comunități transfrontaliere, identități comune, interacționând și comunicând pe teme de interes comun, în ciuda frontierele care definesc statele lor naționale, în ciuda diferențelor de rasă, religie, limbă sau educație, accentuând astfel anumite mecanisme ale globalizării în marș și având drept efect dispariția intermediarilor în aceste schimburi. Aceste interacțiuni accelerate nu-și propun să fuzioneze națiunile, dar pun în discuție decalajul care se adâncește între formele pre-moderne ale statelor și nevoile emergente ale populațiilor afectate de noile tehnologii. Un concept nou care-și face tot mai activ intrarea în atenția lumii academice și a decidenților este ”dezintermedierea” – un fenomen pe cât de complex pe atât de prezent în schimbările din ultima vreme. Dezintermedierea reprezintă un fenomen care se referă la adoptarea și extindea rapidă a unor noi tehnologii digitale (”social media”), care devin tot mai populare și puternic integrate în majoritatea sectoarelor economiei și societăților moderne. Accesul la internet wireless a devenit brusc o necesitate cerută de clienții oricărui local care se respectă, deopotrivă cu echipamentul de navigație prin satelit pentru automobile(GPS), mobile banking, achitările on-line pentru cumpărăturile la distanță, digitalizarea datelor personale și plățile electronice pentru aproape orice fel de servicii. Comunicăm tot mai mult prin platforme digitale și păstrăm cele mai importante date personale în celule de memorie protejate de companii transnaționale ca Google, Amazon Web Services (AWS), Microsoft.

Practic, nici măcar bisericile, ca organisme conservatoare prin definiție, nu mai pot rămâne străine de aceste rețele de socializare activă, trecând în masă la difuzarea on-line a serviciilor divine, menținerea legăturilor cu credincioșii lor prin pagini web, group mail, cloud computing, înțelegând prea bine că ”cine le ignoră este ignorat de public”! Aceste noi instrumente social media pot conecta concomitent grupuri și indivizi fără nevoia unor intermediari numiți ori selectați de stat, fără autorizații speciale, doar pe baza manifestării de voință de a face parte din aceste grupuri virtuale. Noile tehnologii sunt accesibile și atractive pentru publicul larg și ușor de mânuit. Accesul la noile tehnologii extinde spre utilizator spații uriașe de conexiuni și date utilizabile în care indivizii își caută adepți, resurse, identități ideologice și religioase, date culturale, educaționale sau cunoștințe academice, pe care altminteri le-ar găsi mult mai greu. Deși sunt inițiative globale, fondatorii celor mai solide platforme de social media au grijă să angajeze publicul prin intermediul limbilor naționale, creând nevoi sociale despre care nici nu ne-ar fi păsat în epoca industrială. Businessurile create în jurul Amazon, Facebook, Skype, Twitter, Odnoklassniki, Vkontakte, etc, și multe alte programe reușesc să estompeze formele tradiționale de comunicare cu clienții, marketing, comunicare și socializare.

Comerțul electronic domină rețelele retail din marile economii ale lumii (SUA, China). Presa tipărită și televiziunile clasice sunt astăzi sub un adevărat asediu din partea televiziunilor online, mult mai agresive și mai adaptabile la cerințele schimbătoare ale clienților. Voluntariatul și acțiunile de mobilizare (crowdfunding, petition on-line, etc) devine populare și creează noi mecanisme de interacțiune între public și grupurile politic și social active. Între timp noi industrii se profilează la orizont, care pot răsturna multe paradigme ale societății post-industriale (time-traveler).

Accesul la datele celor care se folosesc de comerț sau comunică on-line se transformă într-un nou produs analitic, Big Data, prin care marile companii transnaționale își pot optimiza vânzările și profiturile într-o lume tot mai puternic conectată digital. Și modul în care cetățenii interacționează cu statul devine tot mai digitalizat. Guvernele recurg tot mai frecvent la digitalizarea serviciilor furnizate populației sale, iar deciziile sale sunt tot mai des expuse atenției cetățenilor interesați și opiniilor critice (open data). Efectele dezintermedierii sunt uriașe, afectând dramatic dinamica și structura autorității prin faptul că multe dintre structurile ierarhice, care au apărut în susținerea acestor autorități tradiționale (statul, partidele politice, monarhul/președintele, autoritățile publice) în perioada epocii industriale sunt pe cale de a fi parțial sau complet revizuite. Indivizii își pot asuma în acest moment mult mai multe libertăți decât oricând în alte timpuri și, totodată, accesul la aceste tehnologii îi face mult mai dependenți de cei care le creează, le distribuie ori le reglementează. Fără să vrea, noile tehnologii declanșează un proces care reduce la zero utilitatea unor instituții, profesii și chiar sectoare întregi ale industriilor cu origini din epoca industrială. Se cuvine să menționez aici că accesul la tehnologiile de comunicare este domeniul cel mai puțin codificat în legislația națională și internațională dintre toate. Această schimbare bruscă a rolului pe care noile tehnologii l-au obținut la nivel de mase largi de oameni generează inevitabil multe incertitudini și fricțiuni / conflicte, multe dintre care nu și-au găsit răspunsuri.

Caracteristicile noilor realități moderne

O lume în care regulile se schimbă mai rapid decât autorii lor și instituțiile care le autorizează este periculos de volatilă. Această lume este tot mai fragmentată, mai segmentată de conflicte și incertitudini. Modelul de societate Westphalian desemna statul ca fiind autoritatea supremă a unei societăți, abilitată cu atribuția de a stabili și păstra sub controlul său crearea de reguli și instrumentul de aplicare a violenței în stat.

Responsabilitatea pentru asigurarea securității indivizilor și națiunii, colectivitatea politică reprezentată de stat în raport cu alte state prietene sau rivale, era transferată de la cetățeni/indivizi sau grupuri spre instituții specializate ale statului, cetățenia fiind liantul natural care lega prin loialități naționale cetățenii de stat. Statul definea condițiile necesare și suficiente pentru păstrarea ordinii interne, stabilea politici economice, educație, cultură, securitate și apărare, fiind responsabil de aplicarea acestor condiții pe plan intern și extern, apărându-și supușii de pericole externe mai mult sau mai puțin reale. Societatea nu era în mod necesar implicată în furnizarea de securitate, decât în anumite condiții în care statul era atac militar de agresori externi sau interni.

Noul tip de societate schimbă această piramidă prin intermediul dezintermedierii, care înseamnă o fuziune fără precedent a tehnologiilor fizice, digitale și sociale, declanșând discuții cu privire la loialitățile și identitățile cetățeanului, atras de libertatea de circulație și interacțiune cu alte spații vitale. Ipoteza noastră este că volatilitatea și conflictele din sistemul internațional nu sunt un accident. Ele reflectă modificări tectonice ale modelului istoric, accentuate de apariția noilor tehnologii digitale și sociale. Aceste noi tehnologii de comunicare și mobilizare cutremură pilonii economiilor moderne, scutură structurile vechilor societăți și modul în care erau luate deciziile în cadrul statele naționale. Promițând noi oportunități, acest proces aduce și provocări epocale, inclusiv o masă critică de noi riscuri sociale și politice. Extinderea comerțului electronic produce în mod implicit și riscuri uriașe pentru cei care se bucură de aceste servicii – fraudele electronice. Orice preferințe manifestate în spațiul cyber lasă urme și permite celor care procesează aceste date să intervină în folosul maximizării discursului politic. Pierderile globale datorate crimelor cibernetice au constituit în 2013 cca 113

mlrd $, conform rapoartelor Norton[1]. Riscurile majore afectează înainte de toate cetățenii neprotejați (accesarea neautorizată a poștei electronice, spionajul cibernetic), preluarea controlului asupra datelor personale bancare. Peste 379 de mln de persoane au fost victime directe ori colaterale a crimelor cibernetice în 2013, iar impactul atacurilor (malware) asuprautilizatorilor de telefoane mobile, tablete, laptopuri, calculatoare este în creștere. Potrivit datelor unui raport al Price Water House "Global cyber crime", fiecare a 3 companie pe plan global s-a ciocnit în 2016 cu tentative de sustragere ilicită a unor resurse și fonduri deținute, adică cu atacuri cyber, mai mult sau mai puțin prevenite. Hackerii pot deveni mai periculoși astăzi decât trupele de guerilă care atacau convoaiele militare pe timp de război, diferența fiind că acești activiști nocivi ai spațiului cyber acționează destructiv pe timp de pace contra unor instituții civile, de regulă. Actori non-statali și indivizi bine instruiți pot deveni agenți ai unor arme de distrugere în masă fără a mai avea nevoie de a accesa facilități de producere ori de stocare a armelor controlate de guvern. Acești agenți ai conflictelor pot ataca politici, societăți și economii prin canale care nu sunt controlate de autoritățile statului ori de sectorul privat (infrastructura cyber) sau pot ținti teme sensibile pentru populație (naționalismul isteric) ori sănătatea populației (bioatacuri). Grupuri mici de indivizi mobilizați în scopuri destructive pot mobiliza mișcări largi de protest, folosindu-se de mijloace populare de social media, aproape instant, fără a mai avea nevoie de rețele intermediare de emisie. Iar acestea nu mai sunt de ordinul exemplelor potențiale, ci fapte care s-au întâmplat sub ochii noștri.

Dezintermedierea pune la dispoziția unor grupuri și indivizi mijloace alternative de acțiune colectivă, care poate fi exploatate atât în scopuri pozitive cât și negative. Populismul modern, nealiniat unei anumite ideologii, dar în căutarea de oportunități politice pentru a obține controlul asupra puterii politice, apare ca urmare a schimbărilor în societate și a pierderii rolului tradițional pe care partidele l-au jucat în ultimii 150 ani de istorie. Naționalizarea discursului public și respingerea medierii internaționale sau transnaționale revine din nou pe agenda liderilor populiști. Liderii unor state influente pe plan global nu mai susțin cum o făceau acum câțiva ani modelul de extindere a beneficiilor globalizării, asociindu-se la rândul lor celor sceptici sau adversari ideii de cooperare internațională. Globalizarea înseamnă circulație și schimburi, inclusiv de ordin comercial. Oricare dintre noi poate avea acces astăzi la cele mai sofisticate mijloace de comunicare digitale, fizice și sociale, multe dintre acestea având și posibilități de a influența malign audiența, inclusiv prin puteri destructiv imposibil de imaginat în epoca industrială. Nu există răspunsuri clare asupra efectelor globalizării asupra națiunilor, asupra statelor, iar reacția instanță de protejare a identităților naționale, de rezistență contra expansiunii unor culturi străine reflectă clar apariția unei competiții ideologice pe care unii o pierd și alții o câștigă.

Dezintermedierea are efecte profunde în domeniul securității pentru că poate genera nu doar riscuri noi de securitate, dar poate resuscita și riscuri mai vechi. Drept exemplu servește faptul că digitalizarea unor servicii publice atrage inevitabil și concedierea unui personal care, anterior, servea statului drept interfață în procesul de furnizare a unor servicii de stat cetățenilor săi. Digitalizarea serviciilor publice reduce de regulă numărul angajaților într-un stat prin intermediul platformelor Open Government. Un alt efect al dezintermedierii este însă că statele (și guvernele lor) devin dintr-odată dependente de anumite entități private care își contractează serviciile legate de noile tehnologii în materie de comunicare, apărare, securitate și reziliență, fie la protejarea infrastructurii critice, prevenirea radicalizării unor grupuri contestatare ori apărarea publicului contra unor tentative de manipulare a discursului. În aceste condiții, rolul statului va depinde puternic de buna credință cu care aceste entități private își vor îndeplini obligațiile contractate, influențând în consecință unul din scopurile centrale ale statului în materie de furnizare a securității pentru cetățenii acestuia. Este evident că capacitatea statului de a face față provocărilor în aceste materii, numită și reziliență, devine astfel o parte componentă a politicii de apărare și securitate. Deloc întâmplător că reziliența reprezintă conceptul de bază al Strategiei Globale de Securitate a Uniunii Europene (EUGSS)[2].

De multe ori, decalajul între capabilități, alocarea de sarcini și responsabilități, finanțarea necesităților de apărare și securitate, vorbește limpede despre caracterul funcțional al unui stat. Indeciziile sau lipsa de capacitate de a face față propagandei rusești descurajează populația unei țări și o face vulnerabilă în fața unui război hibrid, care înlocuiește și completează confruntări reale în geopolitica lumii moderne. Din acest motiv, statele trebuie să facă față provocărilor noi în spațiul cibernetic (cyberspace), în care sarcinile și capabilitățile sunt încă slab conturate, iar cadrul legal este și mai slab dezvoltat. Cine-și mai aduce aminte de "revoluția Twitter" de la Chișinău? Peste 2 ani, publicul revoltat se mobiliza în Tunisia folosindu-se pe rol de declanșator de uciderea unui simplu vânzător stradal de legume. În 2016, hackeri ruși au atacat bazele de date ale Partidului Democrat (SUA) la indicația serviciilor de securitate rusești, conform datelor comunităților de intelligence. Astăzi, atunci când China capturează o dronă subacvatică americană, Președintele Trump va

[1] www.enisa.europa.eu/activities/resilience-and-CIIP/national-cyber-security-strategies-ncssss/national-cyber-security-strategies in the world

[2] The EU Global Strategy. http://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union

răspunde (probabil) printr-un mesaj revoltat pe Twitter, sfidând canalele obișnuite anterior de președinții americani. Și în RM, actualul Președinte I.Dodon se străduie să mențină atenția publicului cu o prezență hiperactivă pe Facebook și alte rețele sociale, deși adeseori, efectul atins de mesajele sale sunt insipide sau chiar ridicole. Mulți ambasadori comunică activ pe Twitter fără a se simți inhibați de protocoalele rigide ale școlilor diplomatice tradiționale. Abia la începutul mandatului său, Ambasadoarea Indiei la Washington DC anunța că are 50 mln de followers într-o discuție publică la Brookings (2013).

Inovațiile nu sunt accesibile doar actorilor bine-intenționați. Statul Islamic (SI) a folosit pe larg accesul la rețele de social media pentru a-și recruta luptători străini și la crearea unei imagini eroice pe plan extern. Se știe cum acești teroriști ai lumii moderne se folosesc de social media pentru a-și planifica și coordona atacurile teroriste, multe dintre care rămân imposibil de prevenit. Aceiași tactică o au grupurile separatiste, care-și revendică recunoaștere externă pe baza exploatării loialităților afecte prin social media și a manipulării de simboluri istorice. Separatiștii de la Tiraspol folosesc pe larg portaluri făcute la standarde moderne, care au angajat vorbitori nativi de limbă engleză, pentru a-și promova ideologia și elementele unei ”statalități” pe care nici un stat din lume nu a recunoscut-o. Ghidați de patronii politici de la Moscova, separatiștii transnistreni au investit resurse exorbitante în ”ancorări” de publicații occidentale și chiar a unor diplomați acreditați în Republica Moldova, înțelegând cât de important este să cultivi loialități informale. La rândul lor, separatiștii pro-Kremlin din Donbas gestionează zeci de website-uri prin care-și recrutează mercenari, pe lângă sprijinul militar pe care-l primesc în mod uzual din partea Federației Ruse.

Hackeri faimoși au pus în pericol infrastructuri civile și militare prin atacuri concertate din mai multe colțuri ale lumii. Unii dintre ei au scris istorie (Guccifer) prin spargerea unor rețele guvernamentale arhisecrete. Tot ei capturat sute de milioane de dolari din conturi private ori au pus în pericol servicii vitale pentru populații largi, ca urmare a tehnologiilor de hacking de date, mult mai greu de interceptat ori de combătut. Există și alte forme de exploatare malefică a social media fie prin propagandă și manipularea - așa cum se întâmplă în raport cu Finlanda și Suedia (ținte ale atacurilor cu rachete rusești dacă acestea ar anunța că doresc să adere la NATO) ori demonizarea unor oponenți politici incomozi (zvonul despre aducerea celor 30.000 Sirieni în RM dacă va câștiga candidatul PAS la scrutinul din 2016).

Propaganda reprezintă din această perspectivă un instrument reinventat de social media. Dintr-o perspectivă utilitaristă, cetățenii care cunosc și practică aceste tehnologii pot participa mai activ și sunt mai bine reprezentați politic, ceea ce s-ar numi o formă de înzestrare cu putere, sau ”empowerment”. Cetățenii pot avea acces la mai multe resurse vitale (financiare, economice, tehnologii de generare a energiei curate/verzi, acces politic) prin social media. Nu putem ignora însă că această înzestrare cu putere cere și răspunsuri de reziliență, cel puțin la fel de complexe. Ieșirea Marii Britanii din UE se datorează impactului deosebit al folosirii social media în promovarea de către liderii UKIP a ideii de separare politică de Brussels, incapabil să-și apere imaginea și interesele contra unui grup minoritar. În mai 2015, UKIP a obținut în alegerile generale doar un singur mandat în Camera comunelor, suficient însă pentru a declanșa panică în biroul PM Cameron și decizia conservatorilor de a da satisfacție celor nemulțumiți printr-un plebiscit. A urmat o catastrofă politică a PM Cameron. Anterior Brexit-ului am urmărit bătălii politice intense pe principalele portaluri de social media din această țară, generate de referendumul din Olanda contra semnării Acordului de Asociere al UE cu Ucraina. Și alegerile americane (Trump for President) au fost marcate de etape de intensă volatilitate și convulsii sociale. Manipularea poate inspira mobilizări ostile chiar și printre cetățeni loiali ai unor democrații de tip occidental. Altminteri, tactici subtile sau acțiuni agresive cu caracter sistematic pot manipula discursul public și pot influența logica procesului politic prin acțiuni subversive ori conflicte care sparg societatea.

Cum construim reziliență în fața noilor pericole

Prima reacție pe care un bun cetățean informat o poate avea la aceste provocări ar fi logic legate la ideea de a educa publicul. Mai multă cultură strategică și informare asupra securității cibernetice va spori capacitatea de prevenire a riscurilor individuale și colective. Un cetățean care se informează și are acces la cele mai importante tehnologii moderne este, fără îndoială, mult mai pregătit să-și servească mai bine scopurile într-o lume dependentă de tehnologii, fiind la rândul

său o piesă importantă într-un plan de reziliență națională. Dar, crearea de reziliență este o sarcină complexă și migăloasă peste tot în lume, dar mai ales în regiunile încărcate de tensiuni geopolitice. Ea derivă din fragilitatea sistemelor de prevenire a atacurilor cyber și lipsa unui sistem de management integrat al securității cibernetice. Misiunea de a preveni acest gen de incidente în domeniul securității sistemelor informaționale naționale este alocată, de regulă, unor centre naționale pentru securitatea cibernetică, așa zisele CERT-uri guvernamentale. Din 2010, există un CERT și în Republica Moldova ca o platformă specializată în securitatea informațională, angajată prin răspundere guvernamentală la supravegherea funcționării sistemelor IT guvernamentale, care-și asistă beneficiarii la implementarea măsurilor pro-active și reactive la reducerea riscurilor de incidente a securității IT[3]. În 2009, RM a ratificat Convenția Consiliului Europei privind criminalitatea informatică, operând modificări în codul Penal în corespundere cu standardele europene, dar progresele în vederea creării unui cadru legal privind delimitarea și armonizarea competențelor și responsabilităților instituțiilor statului și a celor private în domeniul securității cibernetice, deficitul de resurse, lipsa de progres în auditarea riscurilor de securitate cibernetică a diminuat impactul pozitiv pe ansamblu în RM.

Este evident că instituirea unei politici de reziliență nu se rezumă doar la ”incidente IT” și reprezintă o sarcină mult mai complexă în condițiile proliferării noilor tehnologii moderne. Absența unui cadru legal adecvat afectează siguranța datelor publice și private, menține riscul penetrării rețelelor guvernamentale, bancare, de grupuri bine echipată, care pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice. Sarcina se dovedește a fi dificilă și din cauza fragmentării societăților moderne și diluări a definiției clasice a puterii politice, după cum se recunoaște și în Programul Național de Securitate Cibernetică a RM pentru anii 2016-2020[4]. Programul de securitate cibernetică este corelat cu strategia națională de dezvoltare a societății informaționale ”Moldova Digitală 2020”, având drept agenții de implementare Ministerul Tehnologiei Informației și Comunicațiilor. Programul prevede identificarea unor acțiuni prioritare specifice: Procesarea, stocarea și accesarea în siguranță a datelor, Securitatea și integritatea rețelelor și serviciilor de comunicații electronice, Dezvoltarea capacităților de prevenire și reacție urgentă la nivel național (CERT), prevenirea și combaterea criminalității informatice, consolidarea capacităților de apărare cibernetică, Educația, formarea și informarea continuă în domeniul securității cibernetice, etc. Costurile estimate pentru implementarea tuturor acestor obiective individuale se ridică la numai 9,5 mln lei până în anul 2020, ceea ce reprezintă foarte puțin în raport cu marile provocări ale domeniului.

Mai mult, Programul pornește de la aceiași carență instituțională în care statul este actorul central care evaluează și intervine în situațiile unor pericole și situații de riscuri cibernetice, cu o implicare insuficientă a sectorului privat și mediului asociativ. Or, adevărata reziliență în sectorul de asigurare contra riscurilor cibernetice ar trebui să pornească de la o mai mare inclusivitate a societății active, luând în considerație fenomenul dezintermedierii. Este total eronat să încerci a răspunde provocărilor derivate din noile tehnologii fără a înțelege tabloul general al acestor riscuri, vulnerabilitățile existente și mijloacele prin care societățile pot fi protejate contra unor intenții ostile. Astfel, dezastrul din sistemul bancar pune cu acuitate necesitatea unui CERT sectorial în sistemul financiar, care s-ar ocupa cu stocarea și utilizarea expertize necesare la prevenirea, analiza, identificarea și reacția la incidentele de securitate cibernetică din sectorul atacat anterior de forțe ostile. Supravegherea sectorului bancar solicită BNM un sistem care să asigure supravegherea tuturor operațiilor financiare, în condiții de prudențialitate. Fără un sistem performant de gestionare a datelor bancare, nici măcar administratorii băncilor nu ar putea ști cum să evite diverse incidente bancare, similare cu cele care au condus la ruinarea și falimentul celor 3 bănci din RM (2015). Mai multe sectoare cer în acest moment sisteme de alertă timpurie și informare în timp real, în scopul prevenirii unor dezastre similare, fie că vorbim de incidente tehnogene în sistemul energetic, al sistemelor critice (apă, gaze, utilități) și alte servicii de care depind comunitățile urbane mari. Este evident că aceste riscuri în sistemul securității cibernetice nu nu pot fi gestionate exclusiv de către agențiile guvernamentale abilitate.

Evoluția contextului regional și geopolitic solicită eforturi sporite în vederea educării unei culturi a securității naționale, capacitatea efectivă de a evita riscurile cibernetice de către toți actorii implicați. Din păcate, RM încă nu a atins o linie de ireversibilitate a reformelor, deși a obținut din partea UE finanțări generoase și accesul rapid la regimul liberalizat de vize, fiind primul stat din Parteneriatul Estic în această privință. RM a suferit un declin neașteptat în ultimii ani, ca urmare a jocurilor de putere și poziționări între câteva grupuri de clanuri oligarhice, ceea ce a afectat grav imaginea elitelor și direcția de aplicare a reformelor, timorând populația, care s-a simțit în consecință vădit descurajată de trădări politice, lipsuri economice și de absența unui leadership credibil.

---

[3] Centrul pentru securitatea cibernetică (CERT-GOV.md) a fost înființat prin Hotărârea Guvernului RM No.746 din 18.08.2010 „cu privire la aprobarea Planului Individual de Acțiuni al Parteneriatului RM-NATO”, în cadrul întreprinderii de stat ”Centrul de telecomunicații speciale”. Sursa: www.cert.gov.md

[4] Hotărârea Guvernului RM No.811 din 29.10.2015 cu privire la programul Național de securitate cibernetică a RM pt anii 2016-2020. Monitorul Oficial No.306-300, Nr.811, 29 octombrie 2015.

O dificultate obiectivă ține de instinctele nedemocratice al unei elite care respinge reformele structurale și modernizarea societății ori de câte ori acestea îi amenință status-quo-ul. Multe dintre aceste reforme susținute de UE pornesc de la ipoteza că elitele ar putea sprijini schimbările pe baza unor raționamente logice. Această ipoteză s-a dovedit a fi în general falsă. S-a crezut mult timp că aceste societăți în tranziție vor opta în mod necesar pentru valorile liberale, iar elitele se vor mobiliza pentru a crea mai multă bunăstare socială și economică, în folosul populațiilor reprezentate de ele. Din păcate și această ipoteză s-a dovedit a fi falsă. În realitate, diviziunile adânci din societate și stratificarea accelerată a societății pe grupuri de ”profitori ai tranziției” și ”pierzători ai tranziției” au creat condițiile unei împotriviri la schimbare. Interesele unor carteluri politice au frânat importante reforme sistemice, cum ar fi – reforma sistemului judecătoresc, reforma proprietății publice, reforma sistemului de administrare publică, expulzând puținii lideri reformatori din sistemul politic și administrativ al statului și prăbușind, în rezultat, susținerea populară pentru reforme.

Crizele politice au făcut ca investițiile în noile tehnologii de asigurare a securității cibernetice să fie neglijate, iar protecția datelor de interes național să fie privită ca o povară, și nu ca o prioritate. Deloc întâmplător că de aceste omisiuni s-au folosit infractorii care au atacat în mai multe rânduri serverele guvernamentale în RM prin diseminarea mesajelor spam-phishing de tip ransomeware, criptând și încercând să preia datele existente în anumite instituții sau chiar șantajând victimele prin răscumpărări care li s-au cerut în schimbul remedierii problemelor cauzate. Și alte sectoare, nu doar cel guvernamental, au fost supuse atacurilor în ultimii ani – băncile, societățile de asigurări, dar și multe companii private, s-au trezit cu grave spargeri de securitate cibernetică, în mare parte datorită neglijării ori subestimării pericolelor în acest domeniu. Multe dintre aceste riscuri cibernetice sunt exploatate de grupuri transnaționale de crimă organizată. Uriașele fraude bancare, schemele de spălare a banilor din ultimii ani, rolul activ pe care l-au avut anumite grupuri politice cu origini înfipte adânc în labirinturile nomenclaturii sovietice și a rețelelor rusești de contrainformații și intelligence, întăresc nevoia strategică de a regândi pilonii unei politici de reziliență în RM, pe baza unor estimări realiste a șanselor și instrumentelor de întărire a sistemului democratic și a speranței că odată și odată RM ar putea deveni parte din lumea occidentală. Acest traseu cere răspunsuri adecvate și la noile tipuri de riscuri în domeniul securității cibernetice, a datelor, rețelelor și cunoașterii amenințărilor existente, care reprezintă un proces continuu și nu doar o atestare formală a riscurilor.