STRATEGIKON
Innovative Strategies

RAPORT

Libertate, încredere și securitate în spațiul cibernetic național și european

Sumar

- Prezentul raport analizează în mod interdisciplinar parteneriatul public – privat în managementului datelor cu caracter privat în Statele Unite ale Americii, în Uniunea Europeană și în România. Această analiză vine ca o consecință a dezbaterilor pe seama Legii Securității Cibernetice și a riscurilor si amenințărilor asimetrice europene și euro-atlantice la adresa infrastructurii cibernetice.

- Strategikon urmărește trei dimensiuni importante atunci când analizează reglementările ce vizează spațiul cibernetic: trendurile internaționale, lecțiile de învățat și recomandările pentru factorii decizionali. Astfel, documentul poate contribui la optimizarea Legii Securității Cibernetice care pe de o parte trebuie să protejeze dreptul la viață privată și pe de altă parte trebuie să satisfacă nevoia de securitate cibernetică.

- Având cel mai rapid internet din UE și aproape niciun cadru de Securitate cibernetică, România este raiul haker-ilor. După ce Curtea Constituțională a decis că Legea Securității Cibernetice este neconstituțională (Decizia 17/2015), Ministerul Comunicațiilor și pentru Societatea Informaţională a publicat pe website un draft modificat al legii. Astfel, legea a redevenit un subiect fierbinte în dezbaterile publice.

București, IULIE 2016

RAPORT STRATEGIKON, *IULIE 2016, Copyright @ www.strategikon.ro . Report scris de Bebe-Viorel Ionică, Claudiu Săftoiu, Corneliu Vișoianu, Denis Kurunczi, Filofteia Repez, Florin Necula, Gabriel Mihăilescu, Mădălina Neacșu, Mihai Popa.*

CUPRINS

INTRODUCERE

Poate securitatea “angajată” să fie aplicată prin lege, astfel încât democrația să nu sufere, iar spațiul virtual să rămână liber, dar sigur? Nevoia de siguranță în cyber spațiu este acută, după ce amenințările teroriste ale ultimilor ani au pornit cu predilecție de pe www și au vulnerabilizat radical sistemele naționale de protecție online. Instituții de securitate, sisteme insituționale ale autorităților statale și servere ale companiilor private sunt expuse necruțător haiducilor iresponsabili ai netului. Teroriștii electronici utilizează libertatea cyber spațiului, pentru a îngenunchea libertatea internetului, națiunile și sute de milioane de cetățeni, logați online 24/24.

Cazul României este relevant: în fața riscurilor venite din lumea virtuală, opinia publică se luptă încă cu fantomele concentraționare ale poliției politice. Comparativ, SUA, Canada și țări importante europene fac front comun împotriva hoardelor care prăduiesc și se organizează online, împotriva criminalilor fără chip.

Strategikon expune provocările, etalează comparațiile semnificative și avansează recomandări, în ajunul trecerii prin parlamentul României a unei legi esențiale, sigure și democratice în egală măsură: Legea Securității Cibernetice.

1. Tendințe internaționale, evoluții și lecțiile acumulate

1.1. Statele Unite ale Americii

Puterile acordate de către Congres executivului în urma atacurilor din 9 septembrie 2001 au fost vaste însă în anii ce au urmat, curentul opiniei judiciare și a celei publice a devenit potrivnic față de ceea ce mulți au văzut ca fiind o depășire a atribuțiilor și o și mai mare incapacitate de a performa. În mai 2015, o Curtea de Apel americană a decis că programul prin care se colectau sistematic înregistrările telefonice ale cetățenilor americani nu a fost niciodată corect autorizat. Legea a fost lăsată să expire, iar în iunie 2015 Congresul a aprobat *USA Freedom Act*, care interzice activitățile de colectare. Chiar și în măsura în care NSA s-a străduit că ofere publicului și Congresului mai multă transparență asupra modului său de operare, evaluările indică că programul de colectare în masă a fost un eșec.[1]

Guvernul și industria vorbesc de mai bine de un deceniu despre mecanisme de transfer a informațiilor. Camera Reprezentanților a promulgat legea *Cyber Intelligence Sharing and Protection Act (CISPA*) în 2013, dar progresul legii a fost oprit când Președintele Barack Obama a amenințat că își va exercita dreptul de veto, acuzând o lipsă a protecției vieții private. În octombrie 2015, Senatul Statelor Unite a trecut controversata *Cybersecurity Information Sharing Act (CISA),* menită să încurajeze companiile și agențiile guvernamentale să împărtășească informații privind hackerii și metodele lor.

Mediatizatele breșe cibernetice din ultimul an de la Sony Pictures, Home Depot, Office of Personnel Management și de la zeci de alte organizații au ajutat CISA să ajungă până în Senat. Filosofia este că prin împărtășirea de informații părțile implicate se vor putea pregăti mai bine în vederea identificării și a

[1] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/.

auto-apărării împotriva hackerilor ce încearcă să sustragă informații. Cu toate aceastea, în forma sa actuală, CISA, nu definește clar modul în care informațiile vor fi împărtășite, cine le va gestiona și cum vor fi diseminate.[2]

Criticii atrag atenția asupra faptului că împărtășirea informațiilor are o eficiență scăzută în a preveni atacurile cibernetice. La nivelul guvernului federal exista deja o organizație care se ocupă de împărtășirea informației privind amenințările cibernetice. În cadrul *Department of Homeland Security* a fost stabilită *United States Computer Emergency Readiness Team* (*US-CERT*) în 2003 pentru a colecta, analiza, disemina și răspunde la informația împărtășită între agenții guvernamentale, sectorul privat și cercetători. Criticii CISA susțin că mecanismele de împărtășire a informației trebuie să fie combinate cu implementarea criptării, îmbunătățirea software-ului învechit și cu îmbunătățirea protecției cibernetice în general.[3]

În februarie 2015, Președintele Obama a semnat Ordinul Executiv 13691, care detaliază cadrul de extindere a mecanismelor de împărtășire a informațiilor privind amenințări și atacuri atât în mediul privat cât și între mediul privat și cel public. Numeroase inițiative publice și private au avut drept scop crearea unor astfel de programe.[4]

1.2. **O punte peste Atlantic – Uniunea Europeană**

Pentru companii, problemele internaționale referitoare la siguranța datelor au fost concluzionate în octombrie 2015, când Curtea Europeană de Justiție (CEJ) a anulat înțelegerea *Safe Harbor* dintre Uniunea Europeană și Statele Unite, în vigoare încă din 2000, ce permitea transferul de date cu caracter privat. Decizia Curții a venit pe un fond de incertitudine, accentuat de cazul Edward Snowden și de procesul intentat de Max Schrems. CEJ a concluzionat că *Safe Harbor* nu proteja în mod corespunzător drepturile de confidențialitate ale utilizatorilor, deoarece pe de o parte le permitea oficialilor americani să aibă acces la datele utilizatorilor chiar și în condițiile în care legea europeană o interzicea și pentru că pe de altă parte permitea ca informația să fie mutată în țări terțe în care înțelegerea *Safe Harbor* nu era în vigoare.[5]

În februarie 2016, Comisia Europeană și Statele Unite au căzut de acord cu privre la *Privacy Shield*, un nou cadru pentru fluxul transatlantic de date care impune obligații mai stringente pentru companiile din Statele Unite pentru a proteja datele personale ale europenilor și o monitorizare mai strictă de către *Department of Commerce* a SUA și a *Federal Trade Commission* (FTC), inclusiv prin cooperarea cu autoritățile europene cu competențe în protecția datelor.[6]

În 2015, șase dintre cele zece țări care au suferit în urma fraudelor pe internet au fost localizate în Europa de Est și în fosta Uniune Sovietică, iar cele mai pertinente activități criminale includ:

- Malware: În 2015, principalele categorii de malware folosite extensiv de către cybercriminalii europeni au fost: ransomware, viruși Trojan ce permit accesul într-un computer, de la distanță și virușii ce accesează informații confidențiale din computerul compromis.

[2] Larry Greenemeier, A Quick Guide to the Senate's Newly Passed Cybersecurity Bill, The basics of the controversial Cybersecurity Information Sharing Act (CISA), 28 October 2015, http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/

[3] Larry Greenemeier, A Quick Guide to the Senate's Newly Passed Cybersecurity Bill, The basics of the controversial Cybersecurity Information Sharing Act (CISA), 28 October 2015, http://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/

[4] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/.

[5] Cyber Risk Report 2016, Hewlett Packard Enterprise Security Research, http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/

[6] EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, Press release of the European Commission, 2 February 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm

- Piețe pentru Bunuri și Servicii: date din carduri de credit, spam-uri, pornografie infantilă, fraudă și phishing, extorcare cibernetică, divulgarea datelor personale și confidențiale, compromiterea resurselor și distrugerea site-urilor web, compromiterea sistemelor de rețea și a website-urilor, interzicerea accesului la anumite servicii, e-comerț și servicii ilegale.
- Bitcoin: Cybercriminalii din Estul Europei sunt activi în hackingul monedei Bitcoin, o valută criptată și imposibil de urmărit, folosită în mediul online.[7]

Securitatea cibernetică a avut un debut mai lent în anii 2000, atât în interiorul statelor membre, unde conștientizarea pericolului a crescut odată cu creșterea numărului de atacuri cibernetice și cu creșterea dependenței economiilor moderne de industria ITC, cât și la nivelul Uniunii. UE avea competențe cibernetice limitate, îndeosebi civile, cele militare fiind rezervate NATO.

Prim cadru comprehensiv în domeniu, Strategia pe Securitate Cibernetică a Uniunii Europene, din februarie 2013, elaborată de Înaltul Reprezentant al Uniunii și de Comisia Europeană a stabilit cinci arii prioritare pentru: reziliența cibernetică și securitatea infrastructurilor, reducerea infracțiunilor cibernetice, politici de apărare cibernetică și capabilități legate de Politica de Apărare și Securitare Comună, dezvoltarea de resurse specifice industriale și tehnologice și o politică europeană a spațiului cibernetic.[8]

Piața Unică Digitală este o prioritate a Comisiei Juncker și include o inițiativă cheie bazată pe un parteneriat public-privat în domeniul securității cibernetice. Cea mai importantă realizare de până acum, Directiva privind Securitatea Rețelelor și a Informațiilor (NIS) a fost adoptată formal de către Parlamentul European și Consiliu. Statele membre vor avea la dispoziție 21 luni pentru a implementa directiva în legile lor naționale și încă șase luni pentru a identifica operatorii serviciilor esențiale. Platforma NIS public-privată va reprezenta un mecanism cheie în asigurarea unui nivel comun înalt de securitate cibernetică în Uniunea Europeană. Directiva NIS construiește pe trei piloni: 1) creșterea capabilităților de securitate cibernetică în statele membre; 2) asigurarea cooperării între toate statele membre, prin înființarea unui Grup de Cooperare și 3) asigurarea unui nivel înalt în practicile de management de risc în sectoare cheie (ca energie, transport, sectorul bancar și cel sanitar).

Chiar dacă platforma NIS are obiective înalte, există încă discrepanțe mari între politicile de securitate cibernetică ale statelor membre, între cadrele lor legale și capabilitățile operaționale. Agenția Europeană pentru Securitatea Rețelelor (ENISA)[9] lucrează îndeaproapa cu statele membre și cu sectorul privat pentru a furniza sfaturi și soluții și pentru a facilita dialogul între actorii publici și privați implicați în securitatea cibernetică la nivel european.

Uniunea Europeană avansează către o integrare mai bună a politicilor sale și către o cooperare mai strânsă între statele membre. După atacurile teroriste de la Paris și Bruxelles a apărut întrebarea ,,cum s-a întâmplat asta?". Dacă europenii au cadrul pentru partajarea informațiilor, și sunt conștienți că amenințările trec frontierele și că deci soluția este cooperarea, atunci cum de am eșuat în a preveni atacurile, cum de am fost orbi și cum ar fi trebuit să procedăm? Urgența, atât a găsirii acestor răspunsuri cât și a nevoii ca instituțiile europene să umple golurile, nu a fost nicicând mai presantă.

[7] The Global Cyber Crime Underground: Russia and Eastern Europe, LookingGlass Cyber Solutions, 14 April 2016, https://www.lookingglasscyber.com/blog/the-global-cyber-crime-underground-russia-and-eastern-europe/

[8] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[9] ENISA is a European agency established in 2004 (with a renewed mandate in 2008) that has seen its role gradually expanded to become a major actor in the European cyber-security community.

Trecere în revistă a statelor europene cheie

Marea Britanie are o strategie comprehensivă de securitate cibernetică, care a fost lansată în 2011 și care e completată de un cadru legal puternic în domeniul securității cibernetice și de două echipe pentru intervenție cyber de urgență (CERT-uri). Mai mult, Marea Britanie are un sistem bine dezvoltat al parteneriatului public - privat, în care sectorul privat participă activ.[10]

Franța are o strategie elaborată în ceea ce privește lupta împotriva crimelor cibernetice (cu un accent puternic pe măsurile de securitate), dar se află în urmă în ceea ce privește parteneriatul public-privat. Franța are o strategie a securității cibernetice în vigoare din 2011, deși aceasta se concentrează mai mult pe apărare și chestiuni de securitate națională. Agenția Națională pentru Securitatea Sistemelor de Informații (ANSSI) este o autoritate cu vechime, dedicată securității informațiilor și este integrată cu echipa de intervenție cibernetică de urgență, a țării. (CERT-FR). Strategia de securitate cibernetică conține recomandări pentru o cooperare mai strânsă cu sectorul privat, dar această dimensiune nu a fost dezvoltată semnificativ. ANSSI a publicat măsuri de securitate specifice diverselor sectoare, făcând din Franța una dintre puținele țări europene care a adoptat o abordare atât de specifică în ceea ce privește gestionarea securității cibernetice.[11]

Germania poate fi considerată liderul european în securitatea cibernetică, din moment ce pune accent atât pe strategia guvernamentală, cât și pe parteneriatul public-privat. Germania a adoptat o strategie comprehensivă de securitate cibernetică în 2011 și a completat-o cu un puternic cadru legal. Existența Biroului Federal pentru Securitatea Informațiilor (BSI), responsabil de gestionarea securității computerelor și a comunicațiilor pentru guvernul german, dovedește importanța dată securității cibernetice la un nivel înalt guvernamental. Mai mult, Germania a dezvoltat parteneriatul public-privat, precum Alianța pentru Securitate Cibernetică și parteneriatul UP KRITIS, iar politicile sale naționale și cadrul legal reflectă accentul pus pe cooperare.[12]

Italia și-a înnoit legile privind securitatea cibernetică în 2007 și a adoptat planuri pe securitate cibernetică în 2013 și 2014, rezultând într-un cadru legal puternic. De asemenea, strategia italiană pe securitate cibernetică face apel la parteneriatul public-privat, ca fiind o direcție dorită pe viitor. Cu toate acestea, nicio cooperare formalizată nu există încă.[13]

1.3. Vecinătatea periculoasă a României: Europa de Est

Întocmai ca omologii săi regionali, criminalitatea cibernetică europeană subterană operează ca o piață legitimă de afaceri, devenind din ce în ce mai comercializată și orientată pe servicii. Est-europenii și germanii sunt dintre cei mai activi în ecosistemul european al criminalității cibernetice. Potrivit Interpol în 2015, infractorii cibernetici est europeni au fost printre cei mai sofisticați. Ei folosesc software-ul creat de alți hackeri, dar implementează instrumente customizate, create pentru operațiuni speciale. Acești actori lucrează de obicei în echipe mici, concentrate pe proiecte la îndemână și sunt extrem de atenți la păstrarea anonomității.[14]

[10] *EU Cybersecurity Dashboard, Business Software Alliance (BSA),* http://cybersecurity.bsa.org/assets/PDFs/country_reports/Cs_unitedkingdom.pdft

[11] *EU Cybersecurity Dashboard, Business Software Alliance (BSA),* http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_france.pdf

[12] *EU Cybersecurity Dashboard, Business Software Alliance (BSA),* http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf

[13] *EU Cybersecurity Dashboard, Business Software Alliance (BSA),* http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_italy.pdf

[14] The Global Cyber Crime Underground: Russia and Eastern Europe, LookingGlass Cyber Solutions, 14 April 2016, https://www.lookingglasscyber.com/blog/the-global-cyber-crime-underground-russia-and-eastern-europe/

1.4.1. România - Context

România, în actualul context european este ideală pentru a fi folosită în atacuri cibernetice asupra altor ţinte, atât din interiorul țării cât și din afară, deoarece are cea mai mare viteză a internetului din UE şi o protecţie foarte slabă a calculatoarelor şi a reţelelor cibernetice. Inexistența unei legi care să traseze răspunderea privind o infrastructură cibernetică aflată în proprietatea unui operator privat, face ca avantajele ce derivă din capabilitățile superioare ale infrastructurii la nivel de țară să devină reale dezavantaje din punct de vedere cibernetic, la nivel local, regional și chiar global.

Statutul curent al incidentelor de securitate cibernetică în România:[15]

- 8% din alertele procesate de CERT-RO în 2015 se referă la sisteme vulnerabile, și anume servere care sunt expuse pe internet, fiind configurate prost sau care nu sunt actualizate și sunt folosite ca punct de tranzit pentru derularea atacurilor.

- 21% dintre alerte se referă la infecţii cu malware. Dacă un atacator vrea să îşi facă o reţea botnet, va alege cu siguranţă victime din România, in același context al performanțelor pozitive din punct de vedere tehnic. Odată ce ,,gazda" s-a instalat pe servere din România, nu mai există niciun impediment în a lansa atacuri sau activități ilegale în numele infrastructurii din România.

- Conform CERT-RO, de la finele anului 2015 şi până în prezent, a fost înregistrată o creştere a incidentelor care au afectat autorităţi publice locale din România. Cele mai întâlnite tipuri de incidente sunt: compromiterea site-urilor web cauzată de platforme neactualizate şi vulnerabile, infectarea staţiilor de lucru cu diferite variante de malware, în special ransomware.

- Atacurile cibernetice direcţionate cu un grad ridicat de complexitate şi potenţial de risc major, din categoria "APT – Advanced Persistent Threat", se vor manifesta, cu o tendinţă ascendentă, prin identificarea si exploatarea a noi vulnerabilități de securitate la nivelul aplicațiilor software sau resurselor hardware utilizate de catre instituțiile publice / private țintă.

- În general, instituțiile publice sunt afectate de lipsa personalului de specialitate pe linia securității sistemelor informatice. Această vulnerabilitate duce deseori la configurarea necorespunzătoare a sistemelor informatice precum și la securizarea necorespunzătoare a acestora în raport cu riscurile indificate în spațiul virtual;

Creșterea nivelului de securitate a devenit o prioritate. În acest scop, următoarele idei sunt luate în considerare:

- derularea unui exerciţiu de securitate cibernetică cu implicarea sectorului public şi privat;

- înfiinţarea şi operaţionalizarea Centrului de Inovare în Securitate Cibernetică;

- creşterea nivelului de securitate al infrastructurilor cibernetice aferente instituţiilor din teritoriu;

- demararea unui proiect privind extinderea „sistemului de alertă timpurie şi informare în timp real – SAT" al CERT-RO;

[15] Report on the cybersecurity alerts processed by CERT-RO in 2015, CERT-RO, https://www.cert-ro.eu/files/doc/1068_20160411140422094789700_X.pdf

- demararea unui proiect adresat elevilor privind educaţia în securitate cibernetică şi siguranţă online;

- elaborarea şi aprobarea criteriilor minime pe care trebuie să le îndeplinească o structură de tip CERT pentru a fi inclusă în comunitatea CERT din România;

- elaborarea şi aprobarea unei politici publice privind divulgarea responsabilă a vulnerabilităţilor.

1.4.2. Legea Securității Cibernetice

În România, Legea Securității Cibernetice a trecut prin furcile caudine ale abordărilor politice, poziționărilor ONG-urilor de securitate și comentatorilor și analiștilor mass-media, fiind un exemplu clasic de intenție bună, dar comunicată și tratată mai mult decât discutabil.

Legea Securității Cibernetice a fost una dintre cele trei Legi Big Brother, un pachet declarat neconstituțional. Prima lege prevedea ca furnizorii de telefonie și internet să păstreze timp de șase luni datele utilizatorilor lor, în timp ce a doua cerea ID-ul utilizatorilor înainte de achiziționarea cartelelor SIM pre-pay și utilizarea rețelelor de Wi-Fi publice.

Este a doua încercare a autorităților de a trece legea prin Parlament, după ce în 2014 și din nou în 2015, Serviciul Român de Informații (SRI) a încercat să treacă legea de unul singur.Greșeala SRI a întârziat într-o manieră nechibzuită dezbaterea publică și după aceasta, aprobarea unui set de legi de către Parlament, care erau create să abordeze riscurile și amenințările, să creeze un cadru național de cooperare între instituțiile relevante și sectorul privat și să ranforseze capacitatea de a reacționa la incidentele cibernetice.

În ciuda atât a asigurărilor din partea MCSI, cât și din partea SRI, că legea nu are nimic de a face cu datele cu caracter personal, publicitatea generată a prelungit retorica vehementă. Există mai multe motive pentru asta, toate provenind din trauma postcomunistă, care încă dăinuie în România. Există un sentiment de paranoia, un fel de legendă urbană despre interceptări ilegale ale oricui, oricând. Mass media, ONG-urile și liderii de opinie păstrează vie ideea că sistemul ascultă ilegal, interceptările sunt făcute fără mandat și la comanda politicienilor, și că serviciile secrete procedează cum vor, fiind stat în stat. Frica generalizată este bazată pe două aspecte. În primul rând, seria de interceptări scurse presei din cazurile procurorilor. În al doilea rând, importanța atașată interceptărilor până de curând, ca probe necesare și suficiente la tribunal. Au existat o serie de cazuri în care politicieni de rang înalt au acuzat instituțiile ce luptă împotriva corupției și serviciile de informații care desfășurau munca operațională, că fac nu atât munca lor cât poliție politică.

Prin politizarea rolului și a importanței serviciilor de informații, aceste instituții au fost demonizate într-o perioadă în care subiectele de mare importanță de pe agenda internațională sunt războiul hibrid și terorismul.

Controversele asupra pachetului de legi pe securitate cibernetică subliniază trei probleme, încă foarte actuale:

1. Cultura slabă de securitate a mass media, a liderilor de opinie, a decidenților și a politicienilor cu mandate limitate și cu puțin interes în a-și îmbunătăți înțelegerea noilor concepte de securitate.
2. Modul în care, prin politizarea unei probleme, rivalitățile cresc, în timp ce eforturile comune pentru inițiative de interes național scad.
3. Lipsa încrederii cetățenilor în instituțiile de securitate și inițiativele lor.

Din acest motiv, în ultima variantă a Legii Securității Cibernetice, corecturi importante au fost aduse privind mandatul judecătorului în investigarea incidentelor de securitate cibernetică:

- Informațiile cu caracter personal, necesare pentru activități specifice vor fi accesate doar după primirea ordinului judecătoresc.
- În cazul identificării de activități ce indică un incident cibernetic, biroul procurorului va fi anunțat.
- Supraveghetorul sistemului a fost schimbat din militar (SRI) în civil (MCSI).

În termeni de imagine publică, un pas important a fost acela de a delimita dezbaterea publică de-a lungul liniilor fiecărei legi Big Brother. Este un semn bun faptul că guvernul a promovat separat Legea Securității Cibernetice și că a permis două sesiuni de dezbatere publică.Un pilon cheie în promovarea Legii Securității Cibernetice a fost decizia de a promova ideea că aceasta nu vizează utilizatorul individual, ci entități naționale, deținători de date personale sau informații legate de infrastructura de securitate națională. Prin abordarea hotărâtă a acestei probleme, frecvența cu care legea a fost acuzată de a se amesteca în viața privată a fost redusă.

2. Sfaturi pentru decidenți

Articolul 19 din Convenția Internațională a Drepturilor Civice și Politice prevede libertatea de exprimare, sub diferite forme și manifestări. Am putea susține că internetul a devenit un instrument inidspensabil pentru libertatea de exprimare. Astfel, am putea concluziona că libertatea de exprimare online este garantată. Și dacă adăugăm faptul că o parte din ce în ce mai mare din viețile noastre este dependentă de internet, putem spune că **dreptul de a fi conectat, cu alte cuvinte dreptul la internet, trebuie să fie garantat.**

Când au loc evenimente îngrozitoare, cu impact asupra unui număr considerabil de vieți, există o reacție naturală de a acționa astfel încât evenimentul să nu se mai repete. De prea multe ori, acel ceva (legislația) atrage consecințe nedorite. Este cazul unui număr de reglementări care vizează guvernarea securității cibernetice. În timp ce intenția de a proteja este corectă, reglementările trebuie să țină cont de imaginea de ansamblu.

2.1. Motivația: de ce?

Când vine vorba de spațiul cibernetic, restricțiile nu pot fi impuse asupra internetului ca întreg. Spațiul cibernetic este un sistem și, prin urmare, nu se află sub autoritatea unei anumite instituții. Așadar, singurele restricții care pot fi impuse se referă la efectele acestui spațiu și la efectele relațiilor create în interiorul acestui spațiu. În final, aceste restricții pot fi impuse doar la nivelul dimensiunii fizice. Un stat poate bloca geografic accesul la o anumită informație, singur sau prin intermediul furnizorilor de internet. Chiar și așa, acea informație este blocată, nu ștearsă de pe internet și continuă să fie accesată de alți utilizatori.

Când se crează o politică, guvernul trebuie să clarifice obiectivul acelei politici. Când vine vorba de legile privind securitatea cibernetică, obiectivul statuat este cel de aproteja integritatea infrastructurii și a informației care se găsește și tranzitează această infrastructură. Acest obiectiv este unul corect și onorabil. În cazul implementării politicilor de internet există câteva mecanisme clare: Legea, Normele Sociale, Piața și Arhitectura, care trebuie toate să funcționeze împreună.[16] Prin urmare, politicile de Internet trebuie să utilizeze legi, norme sociale, piața și arhitectura pentru a securiza conexiunile și informațiile, fără să afecteze modul actual în care ne exprimăm și comunicăm online.

Pentru ca limitele să fie percepute ca fiind rezonabile și pentru ca implementarea lor să fie posibilă, statele trebuie să se asigure că aceste limite sunt în concordanță cu principiile legalității (tot ce nu este interzis este permis), ale legitimității (încrederea că autoritățile, instituțiile și acordurile sociale sunt adecvate, potrivite și corecte) și ale proporționalității (echilibrul dintre ceea ce se

[16] Regulating the Internet, 19 February 2015, http://mysmartcity.ro/en/regulating-the-internet/

impune și valoarea care trebuie apărată prin intermediul acestei impuneri).

2.2. **Mijloace: cum?**

Guvernele ar trebui să adopte și să păstreze la zi un cadru legal și de politici comprehensiv, bazat pe o strategie națională de securitate cibernetică solidă, construită pe următoarele principii cheie:

1. **Bazat pe risc și prioritizat:** Amenințările cibernetice vin în multe forme și dimensiuni, cu grade variate de gravitate. Stabilirea unei ierarhii a priorităților - bazată pe o evaluare obiectivă a riscurilor - cu activele cruciale și/sau sectoarele cruciale în top.
2. **Neutru din punct de vedere tehnologic**: O astfel de abordare a securității cibernetice va crea cadrul în care controalele de securitate și bunele practici să evolueze și să țină pasul cu amenințările care avansează continuu.
3. **Practicabil:** Orice strategie este pe atât de eficientă, pe cât este adoptată de cel mai mare grup posibil și implementată cât mai larg. Supravegherea excesivă a guvernului a operatorilor privați sau intervenția disproporționată de reglementare în gestionarea operațională a riscului de securitate cibernetică e de cele mai multe ori contraproductivă, deturnând resurse de la protecția eficientă și progresivă, la conformitatea administrativă și fragmentată.
4. **Flexibilă:** Gestionarea riscului cibernetic este o funcție trans-disciplinară și nu există o abordare singulară pentru toate cazurile posibile. Fiecare industrie, sistem sau afacere se confruntă cu provocări distincte, iar gama de actori trebuie să fie flexibilă pentru a adresa nevoile lor unice.
5. **Respectuos față de viața privată și de libertățile civile:** Cerințele de securitate ar trebui să fie în mod corespunzător în echilibru cu nevoia de protecție a vieții private și a libertăților civile. Considerații importante în orice cadru de securitate cibernetică sunt: proporționalitatea dintre cerințe și obligații, faptul că acestea nu reprezintă o mai mare intruziune în drepturile fundamentale decât ceea ce e strict necesar și că ele sunt urmate de un proces echitabil și sunt susținute de o supraveghere judiciară corespunzătoare.
6. **Parteneriatul cu sectorul privat:** Cea mai mare parte a infrastructurii este deținută de sectorul privat, făcând cooperarea public-privată esențială. Cooperarea eficientizează gestionarea riscului prin eficientizarea partajării de informații, experiențe și perspective. Eforturi speciale sunt necesare pentru a cultiva încrederea și pentru a evita obstacolele legale care o pot împiedica.
7. **La nivel global, mai degrabă decât izolat:** Dat fiind faptul că amenințările sunt globale, politicile efective de securitate cibernetică și strategiile trebuie să mențină o perspectivă internațională, construindu-se pe eforturi comune cu partenerii și aliații. De asemenea, acestea trebuie să valorifice standardele internaționale, voluntare și din piață, pentru a maximiza scuritatea și partajarea de informații pan-regionale și globale.
8. **Cultivarea educației și a conștientizării despre riscul de securitate cibernetică**: Creșterea conștientizării, educația și formarea în legătură cu prioritățile clar articulate de securitate cibernetică, principiile, politicile, procesele și programele sunt componente esențiale oricărei strategii de securitate cibernetică.
9. **Stabilirea unui cadru potrivit pentru partajarea de informații importante:**

Cea mai bună modalitate de a reduce numărul incidentelor și de a le răspunde adecvat, este schimbul și partajarea de informații potrivite la momentul potrivit. Totodată, acest schimb crează premisele unui efort coordonat între actorii relevanți.

În consecință, întrebarea cheie este cum să ajungi la o partajare de informații eficientă și importantă între părțile interesate. În timp ce câteva țări au luat în considerare sistemele obligatorii de notificare în caz de incidente, acestea singure nu sunt suficiente pentru a adresa problema conștientizării și a pregătirii colective. Când vine vorba de acest lucru, schimburile de informații voluntare bazate pe încredere s-au dovedit a fi cea mai eficientă cale de a atinge partajarea cu succes a informațiilor importante. Fundamentele unui asemenea context sunt:

- **Crearea unui mediu al încrederii reciproce:** partajarea informațiilor, la fel ca raportarea incidentelor, cer garanții și stimulente.
- **Asigurarea unui nivel înalt de confidențialitate:** Dată fiind natura sensibilă a informației partajate în legătură cu un incident sau cu o amenințare cibernetică ce afectează infrastructură, este esențial ca securitatea și confidențialitatea comunicațiilor dintre operatorul de infrastructură și autoritățile supervizoare să fie respectate, menținute și supuse raportării transparente către autorități.
- **Construirea unui dialog aprofundat** între entitățile care suferă un atac și autorități, înainte de a dezvălui date despre atac, pentru a evita propagarea atacului, multiplicarea impactului incidentului, crearea panicii sau momentul dezaprobării publice nejustificate.
- **Asigurarea reciprocității:** În timp ce sectorul privat deține și operează cea mai mare parte a infrastructurii importante a țării, partajarea de informații nu ar trebuie să fie privită ca o furnizare unidirecțională de date, din partea sectorului privat, către entitățile publice. Aceasta ar trebui privită ca un schimb comun și adevărat de informații, bazat pe încredere și beneficii comune.
- **Stabilirea unor cerințe clare și coerente între jurisdicții:** dat fiind faptul că cerințele de notificare obligatorii acoperă un număr tot mai mare de domenii și zone geografice, probabilitatea ca obligațiile legale să intre în conflict crește. Cum varii organizații operează în sectoare multiple, în diferite țări și regiuni, problemele legate de ce se raportează, când și cui ridică deja provocări importante de conformitate. Așadar, în măsura în care un sistem de notificare obligatoriu ar fi introdus, este imperativ să lucrăm spre cît mai multă consistență posibilă, nu doar din punct de vedere al diferitelor obligații de notificare, dar și din perspectiva diferitelor cerințe naționale și regionale.
- **Definirea clară a termenilor:** privind amenințările cibernetice și standardizarea lor în contextul unei interpretări similare și uniforme (printre instituții), probabil prin crearea unui limbaj internațional standardizat al securității cibernetice.
- **Armonizarea prevederilor și principiilor** legilor pe securitate cibernetică cu cele din legile naționale (constituții) și din documentele oficiale (strategiile naționale).
- Pe măsură ce tehnologia evoluează, efectele și întrebuințarea ei trebuie înțelese pentru ca aceasta să fie corect reglementată. Prin urmare, **cercetarea** ar trebui încurajată în domenii precum: criptare, psihologie comportamentală a grupului, inginerie socială și studii de dezvoltare efectuate pe evoluția noilor tehnologii în relație cu atitudinile și dialogul cu cetățenii.

Anexă

Termeni

Următorii termeni și concepte se regăsesc de-a lungul acestui raport. Pentru o mai bună înțelegere, oferim aici definițiile acestora, așa cum experții Strategikon le înțeleg în contextul discutat. Se face o distincție între termenii conceptuali și cei tehnici. Primii trebuie definiți din cauza sensurilor largi și uneori înșelătoare, pe care le implică. Cei tehnici trebuie definiți pentru înțelegerea unei persoane ce nu activează în domeniul IT.

Termeni conceptuali

- **Cultură a securității =** înțelegerea generală a populației cu privire la, pe de o parte, amenințările cu care se confruntă când utilizează dispozitive cibernettice și servicii și pe de altă parte a asumării modalităților și mijloacelor de protecție cibernetică. O cultură a securității este o modalitate de a obține utilizarea corectă a informației, de a crește transparența și încrederea în sistemele IT și în reglementările cibernetice și de a facilita conformitatea cu legi și reglementări.
- **Infrastructură cibernetică deținută de entități private =** active, sisteme și rețele, fizice (serverele) sau virtuale (internetul), ce furnizează servicii esențiale unui număr considerabil de utilizatori. Infrastructura este deținută de entitățile private, dar reglementată de stat, din cauza magnitudinii unei posibile perturbări.
- **Drepturi și libertăți în spațiul cibernetic =** utilizarea nerestricționată și sigură a infrastructurii cibernetice, libertatea garantată de exprimare, accesul la informații și spațiu privat în momentul folosirii infrastructurii cibernetice.
- **Protecția cibernetică =** metode de asigurare o utilizării sigure a dispozitivelor și a serviciilor cibernetice, fie prin mijloace IT (software) fie prin legi și reglementări (legea privind securitatea cibernetică).
- **Lege privind securitatea cibernetică =** o reglementare acceptată de societate ca impunând restricții legale și sigure asupra drepturilor și libertăților, în vederea asigurării utilizării sigure a dispozitivelor și serviciilor cibernetice.
- **Mecanisme de partajare a informațiilor =** parteneriate publice-private care crează protocoale transparente și sigure ce au ca scop informarea reciprocă privind amenințările și acțiunea comună pentru atenuarea riscurilor, evaluarea amenințărilor, intervenție și prevenție.
- **Date personale =** anumite informații care pot identifica o persoană, fie singure, fie prin coroborarea lor cu alte informații.
- **„Securitate" =** agenția de poliție secretă a României comuniste.

Termeni tehnici

- **Malware =** o varietate de forme de software ostile sau intruzive
- **Remote Access Trojans (RATs) =** software-ul, care odată intrat pe un computer oferă acces la informații sau pentru a instala un alt software de virusare
- **Ransomware =** malware care restricționează accesul la sistemul infectat pentru a obţine o răscumpărare.
- **Amenintari Persistente Avansate (APT) =** un set de atacuri cibernetice invizibile și continue, care adesea urmăresc o entitate specifică.
- **Phishing-ul =** încercare de a dobândi informații sensibile (nume de utilizator, parole, detaliile cardului de credit), dându-se drept o entitate de încredere în comunicare electronică.
- **Atacul DoS (Blocarea serviciului) =** o încercare de a face un computer sau o rețea indisponibil/ă utilizatorilor săi de drept
- **Blocarea Distribuită a Serviciului (DDOS)** = sisteme infectate, folosite pentru a viza un singur sistem care cauzează un atac DoS

- **Botnet =** calculatoare interconectate infectate cu malware, fără știrea utilizatorului și controlate de hackeri

Despre autori:

Bebe-Viorel Ionică este un specialist în sisteme IT. A lucrat ca secretar de stat în cadrul Ministerului Comunicațiilor și Societății Informaționale, unde a fost responsabil cu direcția generală, coordonarea și supravegherea activităților legate de TIC.

Claudiu Săftoiu este specialist în comunicare și campanii politice. A fost director al Serviciului de Informații Externe și consilier al președintelui, pe politică internă.

Corneliu Vișoianu este doctorand în cadrul Universității Naționale de Apărare, fost consilier al Primului Ministru și Vice-Președinte fondator al Strategikon

Denis Kurunczi este absolvent de drept cu expertiză în guvernare și în drepturi și libertăți civile. În prezent, este consilier juridic al Institutului Național de Cercetare şi Dezvoltare în Informatică.

Filofteia Repez este profesor asociat în cadrul Facultății de Securitate și Apărare a Universității Naționale de Apărare, unde predă operațiuni comune, securitate națională și euro-atlantică, doctrina politico-militară și studii strategice.

Florin Necula este consilier în Ministerul Economiei, Comerțului și Relațiilor cu Mediul de Afaceri. Înainte, a deţinut calitate de consilier la Ministerul Comunicațiilor și Societății Informaționale

Gabriel Mihăilescu este un profesionist IT cu experiență în administrarea sistemelor, dezvoltarea și implemantarea strategiilor IT. Înainte de a se alătura Departamentului IT din cadrul Ministerului Afacerilor Externe, a fost şeful IT pentru Roche România.

Steluța Mădălina Neacșu este președinte fondator al grupului de analiză agrostrategică - Agrointelligence Sistemul de Informatii al Securitatii Alimentare (SISA). Expertiza acoperă securitatea internațională și reglementările internaționale în domeniu.

Mihai Popa este expert în drept corporativ, cu expertiză în practicile de conformitate, dreptul internațional și european și reglementările de conformitate a companiilor și a contractelor.

Despre raport: