Martie 2013, Publicaţia bilunară: "Q Magazine"
Interviu acordat de **Florian Coldea**, **prim-adjunct al Directorului Serviciului Român de Informaţii,** publicaţiei "Q Magazine"
Titlul: **"Suntem pregătiţi pentru războiul cibernetic?"**
Semnează: Floriana Jucan

"Atacurile informaţionale devin principala ameninţare la adresa securităţii unei ţări. Este şi motivul pentru care, în mod excepţional, **Florian Coldea, prim-adjunctul directorului SRI, a acceptat să vorbească pentru 'Q Magazine' despre Strategia de Securitate Cibernetică a României.**

Pentru a înţelege dinamica spaţiului virtual, amintesc faptul că radioului i-a luat 35 de ani pentru a ajunge la o audienţă de 50 de milioane de persoane, televiziunii 15, în timp ce internetul a ajuns la aceeaşi cifră de utilizatori în doar 5 ani. Astăzi, peste două miliarde de oameni sunt conectaţi sau dependenţi de net. Dincolo de beneficiile importante, spaţiul virtual s-a dovedit, în timp, şi generator de cybercrime şi de conflicte.

Scenariile cele mai pesimiste merg până la imagini apocaliptice, în care alimentaţia, energia, alimentarea cu apă, transporturile, finanţele şi tot ce derivă din acestea pot fi paralizate, chiar într-o ţară precum Statele Unite ale Americii.

In interviul pe care prim-adjunctul Directorului Serviciului Român de Informaţii, General-maior Florian Coldea l-a acordat revistei 'Q Magazine', acesta recunoaşte ca Romania este la fel de ameninţată precum orice alt stat NATO.

In anul 2000, doi hackeri din Filipine au lansat virusul Love Bug. 55 de milioane de calculatoare au fost atacate, iar prejudiciul s-a ridicat la 15 miliarde de dolari. A fost momentul în care lumea a înţeles cu adevărat că prejudiciile unui război neconvenţional, uneori asimetric, pot fi infinit mai mari decât cele provocate de armele clasice.

Bombele nu mai sunt convenţionale, ci se lansează printr-o simplă 'atingere' virtuală, în celălalt capăt al lumii. Inamicul este nevăzut şi adesea rămâne necunoscut chiar şi serviciilor de informaţii. Intregul fenomen al războiului cibernetic este învăluit într-un asemenea mister, încât Războiul Rece pare un timp al deschiderii şi transparenţei diplomatice.

Un posibil 'Pearl Harbour' cibernetic

Intr-un raport dedicat acestui nou tip de război, preşedintele CSBA, Andrew Krepinevicki Jr., după o experienţă de 21 de ani în Armata Americană, vede în armele cibernetice un potenţial de daune mai mare chiar şi decât cel nuclear, în timp ce fostul secretar al Apărării din SUA Leon Panetta nu a exclus un potenţial 'Pearl Harbour' cibernetic. Intrebat fiind ce se poate întâmpla, practic, printr-un atac cibernetic, Generalul Keith Alexander, şeful Cyber Command al SUA, a răspuns că 'un inamic poate paraliza puterea energetică a unei ţări, bursele, schimburile sale comerciale şi internetul... pentru o perioadă de timp' şi că această capacitate nu este circumscrisă doar unei entităţi statale, ci şi unor hackeri privaţi sau terorişti.

Nimic nu pare intangibil. In 2009, programul militar Joint Strike Fighter a fost compromis, fiind furaţi câţiva terabiţi de date privind sistemele electronice, iar sursa atacului pare să fi fost China.

Tot hackerii chinezi au reuşit de mai multe ori să pătrundă în reţeaua de calculatoare a Casei Albe, pentru scurt timp, reuşind să fure email-uri dintre oficiali guvernamentali înainte ca un expert informatic al Statelor Unite să repare sistemul.

Generalul James Cartwright spunea că ar trebui să începem să vedem în armele cibernetice arme de distrugere în masă, în timp ce doi savanţi ai Armatei Liberării Poporului, Ye Zheng şi Zhao Baoxian, sunt de părere că 'la fel cum războiul nuclear a fost războiul strategic al erei industriale, războiul cibernetic a devenit războiul strategic al erei informaţionale, iar acest lucru a devenit o formă de bătălie masiv distructivă, având legătură cu viaţa şi moartea naţiunilor'.

China şi-a propus în politicile sale de strategie naţională ca în 2050 să stăpânească lumea prin puterea cibernetică. 1.500 de diplomaţi chinezi, operând din 70 de birouri, 15.000 de studenţi chinezi care vin în fiecare an în Statele Unite şi 10.000 de chinezi care sosesc în 2700 de delegaţii în fiecare an ar putea reprezenta o acoperire a spionajului de la Beijing în Statele Unite.

Un catalizator major în expansiunea activităţii cibernetice ilicite îl constituie crima organizată. Nicăieri acest fapt nu a fost mai evident decât în Rusia, unde Reţeaua de Business Rusesc (RBR/RBN), s-a ridicat ca 'cea dintâi organizaţie de crimă cibernetică, furnizor al bazei logistice pentru atacuri cibernetice.' Capacităţile de război cibernetic ale RBN sunt atât de formidabile încât este singura organizaţie criminală identificată de NATO drept o ameninţare majoră la securitate. Se bănuieşte că RBN controlează între 150 şi 180 de milioane de noduri de reţea. In anul 2007, aproximativ 40% din crimele cibernetice, dintre care unele erau estimate la peste 100 de miliarde de dolari la vremea aceea, au fost atribuite RBN.

Raportul Chatham House 'Cyber Security and Global Interdependence: What Is Critical?' are o abordare ceva mai temperată şi subliniază că posibilităţile oferite de spaţiul cibernetic sunt cu mult mai mari decât pericolele pe care le conţine - 'multe dintre acestea fiind încadrate în acest tip de limbaj dramatic şi apocaliptic care dezvăluie temeri mult mai adânci faţă de scăparea de sub control a tehnologiei'.

Cei care pot găsi un echilibru optim între libertate şi siguranţă în spaţiul virtual vor culege recompense care sunt cu mult mai mari decât costurile.

România, ţinta spionajului informaţional

Războiul cibernetic pare să fi ajuns şi în România care a fost ţinta mai multor astfel de atacuri în ultimul timp, unele fiind descoperite de Serviciul Român de Informaţii, altele nu. De pildă, atacul înregistrat la sfârşitul lunii februarie (ultimul raportat oficial) le-a fost semnalat ofiţerilor români de intelligence de servicii partenere şi a fost estimat ca având un impact cu mult mai mare decât Red October, datorită nivelului tehnologic superior şi exfiltrării de informaţii.

De altfel, compania Kaspersky Lab semnalase o campanie de spionaj asupra unor ţări din Europa de Est, între care şi ţara noastră, fiind vizate informaţii despre geopolitica naţională şi despre resursele naturale.

In mediile apărării şi securităţii statului, ameninţarea cibernetică a devenit una dintre cele mai mari şi mai dinamice la adresa siguranţei României, chiar dacă marea masă a populaţiei nu o percepe încă în adevăraţii ei parametrii.

In condiţiile în care acest război afectează atât persoane civile, companii private, cât şi instituţii publice, măsurile de prevenire pe care le instituie Strategia de Securitate Cibernetică a României, adoptată în ultima şedinţă a CSAT din 5 februarie, trebuie

dezbătute public, pentru conştientizarea pericolelor. In acelaşi timp însă, se naşte fireasca întrebare, mai ales într-o ţară obsedată de fenomenul 'big brother', până unde putem ceda controlul computerelor noastre entităţii care coordonează această Strategie, adică Serviciului Român de Informaţii.

Generalul-maior Florian Coldea, prim-adjunct al directorului SRI, a răspuns acestei întrebări în exclusivitate pentru Q Magazine.

Q Magazine: Care sunt obiectivele şi direcţiile naţionale ale Strategiei, în afara celor enunţate de Comisia Europeană?

Florian Coldea: Vă enumăr succint câteva dintre acestea. Trebuie să adaptăm cadrul normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic, să securizăm infrastructurile cibernetice naţionale, relevante din punct de vedere al funcţionării corecte a infrastructurilor critice si să asigurăm rezilienţa (rezistenţa la şoc - n.r.) infrastructurilor cibernetice.

De asemenea, asigurarea stării de securitate presupune cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor. Avem în vedere promovarea şi dezvoltarea parteneriatului public-privat, precum şi a cooperării în plan naţional şi internaţional în acest domeniu, creşterea culturii de securitate a populaţiei prin conştientizarea faţă de vulnerabilităţile, riscurile şi ameninţările provenite din spaţiul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii.

Pentru atingerea acestor obiective, în cadrul Strategiei de securitate cibernetică a României sunt câteva direcţii de acţiune la nivel naţional, între care, daţi-mi voie să evidenţiez stabilirea cadrului conceptual, organizatoric şi acţional, dezvoltarea capacităţilor naţionale de management al riscului şi de reacţie la incidente cibernetice în baza unui Program naţional, promovarea şi consolidarea culturii de securitate în domeniul cibernetic, dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice.

Chiar dacă poate părea puţin cam tehnic, ţin să subliniez exact aceste obiective, întrucât este pentru prima dată când România adoptă Strategia Naţională în domeniul Securităţii Cibernetice şi este un document important din care vor deriva toate celelalte pentru reglementarea acestui domeniu.

Q Magazine: Recent, instituţia a recunoscut, prin vocea purtătorului de cuvânt, că 'Octombrie Roşu' a fost un atac cibernetic care a vizat obţinerea de informaţii despre resursele naturale româneşti. Câte atacuri cibernetice au fost la adresa entităţilor de securitate româneşti în ultimii ani, ce au vizat acestea şi câte a reuşit SRI să prevină?

Florian Coldea: Ultimul atac, pe care l-am anunţat la începutul lunii martie, a fost, din estimările SRI, mult mai puternic decât 'Octombrie Roşu'. Zilnic înregistrăm zeci până la sute de incidente cibernetice, însă doar o parte dintre acestea se pot califica drept atacuri informaţionale şi numai un număr foarte redus intră în competenţele SRI, care are atribuţii pe linia cunoaşterii şi informării instituţiilor publice şi private ce deţin Infrastructuri Critice Informaţionale (ICI) sau sisteme informatice de interes naţional, cu privire la ameninţările cibernetice.

SRI acţionează pentru investigarea ameninţărilor cibernetice şi punem accentul pe identificarea scopului şi motivaţiei atacurilor. Acest proces necesită, de regulă, perioade de timp mai îndelungate, având în vedere caracterul asimetric al ameninţării cibernetice, respectiv, dificultatea de atribuire a atacului. Uneori analizăm şi un an-doi un atac.

Serviciul a monitorizat şi documentat în mod constant agresiunile cibernetice la adresa unor sisteme informatice ale unor entităţi publice şi private desfăşurate de persoane aflate în conexiune cu reţele de criminalitate informatică transfrontalieră, care vizau preluarea sub control a sistemelor respective. Agresiunile cibernetice în care a existat un caracter transnaţional al faptelor au făcut obiectul cooperării SRI cu servicii partenere din state pe teritoriul cărora atacurile au produs efecte.

De asemenea, SRI a informat instituţiile statului cu privire la mai multe atacuri la adresa acestora derulate de membri ai grupării Anonymous. Astfel, în 29 mai 2012, procurorii DIICOT - cu sprijinul Jandarmeriei şi suportul tehnic şi informativ al Serviciului Român de Informaţii - au efectuat o serie de acţiuni menite să destructureze gruparea Anonymous România, care accesa ilegal şi exfiltra baze de date din sisteme informatice aparţinând unor instituţii publice.

Q Magazine: Cum colaboraţi cu celelalte instituţii? Există o conştientizare profundă a acestor pericole?

Florian Coldea: In calitate de autoritate naţională în domeniul cyberIntelligence, SRI a constituit Centrul Naţional CyberInt. Aici identificăm atacurile cibernetice produse asupra Infrastructurilor critice Naţionale (ICN) şi limităm eventualele consecinţe ale acestora. Colaborăm cu toate celelalte instituţii cu responsabilităţi în domeniul securităţii cibernetice, precum şi cu instituţiile deţinătoare de ICN.

Cred că este necesară consolidarea cooperării Serviciului cu entităţile de la nivel naţional avâmd atribuţii în domeniu, inclusiv prin operaţionalizarea parteneriatului public-privat.

Q Magazine: Care va fi autoritatea română însărcinată cu securitatea reţelelor informaţionale?

Florian Coldea: Asigurarea securităţii reţelelor informaţionale proprii revine fiecărei persoane juridice de drept public sau privat în parte. In vederea coordonării acţiunilor în acest domeniu la nivel naţional, în cadrul Strategiei a fost prevăzută constituirea Sistemului Naţional de Securitate Cibernetică ce reprezintă cadrul de cooperare interinstituţională destinat asigurării securităţii cibernetice. Coordonarea tehnică a Sistemului i-a revenit SRI-ului.

Q Magazine: România a participat la Cyber Europe 2012 prin CERT-RO, SRI şi STS? Care sunt concluziile?

Florian Coldea: Dincolo de concluzii, exerciţiul a reprezentat o excelentă oportunitate pentru schimbul de informaţii la nivel internaţional între entităţile prezente. A fost o ocazie de a analiza, înţelege şi evalua mecanismele existente de cooperare interinstituţională la nivel european şi de consolidare a comunităţii europene de gestionare a incidentelor informatice. Exerciţiile paneuropene în domeniu reprezintă un instrument important pentru evaluarea şi îmbunătăţirea relaţiilor între ţări şi sunt un factor esenţial în vederea rezolvării unor crize informatice reale.

Q Magazine: Cât de vulnerabilă este România în războiul informaţional?

Florian Coldea: Faptul că activităţile guvernamentale şi comerciale se desfăşoară tot mai mult prin intermediul Internetului a oferit agresorilor cibernetici noi oportunităţi de materializare a intenţiilor lor, potenţate de o dependenţă din ce în ce mai crescută de sistemele de comunicaţii şi informaţii produse de o piaţă internaţională şi globalizată, care au adus cu sine vulnerabilităţile şi riscurile lor.

Traversăm o criză economică mondială care a generat puternice contradicţii sociale. In plus implementarea stadardelor tehnologice şi legislative europene în România este încă în stadiu incipient. Toate aceste realităţi au oferit motivaţii în plus pentru derularea unor atacuri informatice asupra sistemelor informatice aparţinând autorităţilor publice şi entităţilor private, şi a favorizat racolarea unui număr din ce în ce mai mare de specialişti IT în activităţi infracţionale informatice.

SRI consideră că România are un nivel de securitate cibernetică ce trebuie neapărat îmbunătăţit. Pentru a limita atât riscurile unui incident sau atac cibernetic de proporţii, cu un evident impact asupra securităţii naţionale, prin consecinţele economice, sociale şi instituţionale, România trebuie să fie suficient de puternică şi determinată să parcurgă cu consecvenţă o serie de paşi.

Q Magazine: Care ar fi aceştia?

Florian Coldea: Intâi de toate trebuie consolidat cadrul legislativ naţional. Legea privind identificarea şi desemnarea infrastructurilor critice şi Strategia de Securitate Cibernetică a României trebuie să fie urmate de iniţierea şi adoptarea Legii Securităţii Cibernetice, care să reglementeze juridic atât concepte precum securitatea cibernetică naţională sau incident/ atac cibernetic, cât mai ales cadrul instituţional naţional şi atribuţiile autorităţii naţionale în domeniu şi ale altor instituţii care au responsabilităţi în constituirea securităţii cibernetice şi în reacţia la producerea unui incident sau atac cibernetic. Trebuie operaţionalizat parteneriatul public-privat, iar la nivel european gtrebuie continuată relaţionarea cu organismele responsabile în acest domeniu. Tot la nivel naţional este extrem de important un efort susţinut pentru elaborarea şi implementarea unui plan naţional de gestionare şi reacţie la incidente cibernetice, care să prezinte metodologia de urmat de fiecare instituţie în cazul producerii unui incident/ atac cibernetic. Trebuie promovată şi consolidată o cultură de securitate în domeniul cibernetic, trebuie dezvoltate programe de conştientizare în rândul populaţiei, al administraţiei publice şi al sectorului privat cu privire la ameninţările, vulnerabilităţile şi riscurile specifice utilizării spaţiului cibernetic.

Q Magazine: Un pas în acest sens îl facem acum, prin acest interviu. China pare să-şi fi setat ca obiectiv militar să câştige lupta informatică în acest secol, în timp ce oficiali americani au admis că SUA au lansat un atac cibernetic la adresa unei alte ţări, probabil Iranul. Care sunt ţările de care România se poate teme în acest război?

Florian Coldea: Având în vedere că suntem membri ai NATO şi UE, ameninţările la adresa statelor membre ale acestor organisme reprezintă implicit ameninţări pentru România.

Q Magazine: Am putea spune că viitorul sună... ameninţător!

Florian Coldea: Nu fiţi atât de pesimistă! Spaţiul cibernetic nu presupune însă numai ameninţări, ci şi oportunităţi pentru promovarea intereselor, valorilor şi obiectivelor naţionale şi valorificarea acestora este un alt obiectiv al Strategiei.

Q Magazine: SUA au anunţat recent că doresc angajarea unui număr de 5000 de specialişti IT pentru o 'armată digitală'. Instituţia pe care o reprezentaţi are o strategie de atragere similară?

Florian Coldea: Chiar dacă trecem printr-o perioadă de austeritate care a condus la resurse materiale limitate şi la restricţii în ceea ce priveşte angajarea de resurse umane la nivelul instituţiilor din sectorul bugetar, am întreprins tot timpul demersuri în vederea formării unei echipe de specialişti în domeniul cibernetic, cu care s-au obţinut

rezultate operaţionale deosebite, atât în plan naţional, cât şi internaţional, între care aş aminti cazurile Anonymous, Păunescu, Red October, Pene.

Q Magazine: Suntem recunoscuţi pentru o serie de hackeri români care au reuşit performanţe incredibile, desigur, în mod ilicit. Are în vedere instituţia o recuperare, o convertire a acestora în interes naţional?

Florian Coldea: Pentru a-şi putea îndeplini misiunea de asigurare a securităţii cibernetice a sistemelor informatice şi a infrastructurilor critice de interes naţional, SRI va fi preocupat în permanenţă de identificarea de specialişti de înal nivel în domeniu. O prioritate în acest sens o reprezintă selecţia acestora atât din mediul academic, cât şi din cel privat, precum şi expertiza dobândită de Serviciu din activităţile de cooperare interneţională.

Q Magazine: SRI coordonează Strategia de Securitate Cibernetica deci va impune masuri de prevenţie atât entităţilor private, cât si instituţiilor statului. In condiţiile in care trăim într-o ţară şi aşa obsedata de faptul ca SRI ne asculta, ne urmareste,ne intercepteaza, pana unde vom putea ceda controlul asupra computerelor noastre?

Florian Coldea: Nu se pune problema cedarii controlului competentelor, ci a constituirii unui sistem de măsuri preventive şi reactive pe linia implementării de politici, standarde şi ghiduri de securitate. Va asigur ca toate reglementarile in acest domeniu vor fi aliniate la standardele se securitate europene si se vor realiza prin responsabilitatea si cunoasterea totala a proprietarilor si administratorilor sistemelor informatice.

Toate masurile de prevenire sau contracarare a atacurilor cibernetice pe care Serviciul Roman de Informatii le-a luat pana acum si le va lua de acum inainte in baza Strategiei adoptata de CSAT se realizeaza cu respectarea stricta a legilor, inclusiv cu respectarea drepturilor si libertatilor fundamentale ale cetaţeanului."