REȚELELE SOCIALE ȘI CRIMINALITATEA CIBERNETICĂ ÎN RĂZBOIUL INFORMAȚIONAL

Drd. Teodora Marin
Academia de Poliție ”Alexandru Ioan Cuza”

Abstract

The generalized spread of digital information technologies in all areas forms the basis of the changes of the security paradigms and their implementation in apparently disjoined aspects such as political revolutions like the Arab Spring and Euromaidan, the transformation of hacking into a weapon controlled by the state, the use of social networks in the strategies of electronic warfare.

All these features are common for the great powers, but also for emerging states, having both an aggressive component as well as a defensive one of identification and annihilation of these attacks.

The Russian Federation has developed an integrated system, which becomes obvious in a case study that we consider relevant in the analysis of its components for how it is centrally controlled.

Keywords: mail.ro, Wkontakt, Facebook, cybernetic systems, cyber-war

1. Preliminarii

Generalizarea tehnologiilor informațiilor digitale în toate domeniile constituie baza schimbărilor paradigmelor securității, implementarea sa în aspecte aparent disjunse, precum revoluțiile politice de tip Primăvara Arabă și EuroMaidan, transformarea hackerismului într-o armă controlată statal, folosirea rețelelor sociale în cadrul strategiilor războiului electronic.

Toate aceste caracteristici sunt comune marilor puteri, dar și statelor emergente, având atât o componentă agresivă, cât și una de apărare, de identificare și de anihilare a acestor atacuri.

Federația Rusă a pus la punct un sistem integrat, ceea ce devine evident în cadrul unui studiu de caz pe care îl considerăm relevant în analiza componentelor sale, modului în care este controlat în mod centralizat, astfel încât infrastructura cibernetică agresivă include majoritatea platformelor de socializare online, mail.ru și Wkontakt, dar și rețele globale, precum Facebook și Twitter în conexiune directă cu sisteme cibernetice de securitate, organizate conform structurilor militare.

Prin urmare, studiul nostru de caz subliniază ceea ce este tipic pentru statul totalitar, și anume rețeaua centralizată, atât economic cât și politic, și-a găsit o formă extrem de eficientă în spațiul cibernetic, implicând atât sistemele militare, cât și cele civile[75].

Ne vom ocupa mai întâi de modul în care s-a creat un sistem complex de includere a criminalității informatice în sistemul cyber-war.

O altă direcție majoră este cea de a crea structuri militar-civile, informatice, de viitor, în care sunt incluși tineri studenți și absolvenți, urmărindu-se crearea unui Silicon Valley rusesc, anunțat inițial ca urmând să fie dezvoltat lângă Moscova, iar ulterior în Crimeea.

Cea de-a treia componentă analizată vizează folosirea rețelelor de socializare pentru crearea mesajelor favorabile Kremlinului și contracarării celor externe.

[75] Studiul a fost realizat în cadrul lucrării de cercetare *"Social media – o nouă dimensiune a raporturilor dintre securitatea societală și mass-media"*- drd. Teodora Marin, finanțată în cadrul proiectului POSDRU/159/1.5/S/138822, cu titlul „Rețea Transnațională de Management Integrat al Cercetării Doctorale și Postdoctorale Inteligente în Domeniile "Științe Militare", "Securitate și Informații" și "Ordine Publică și Siguranță Națională" - Program de Formare Continuă a Cercetătorilor de Elită –" SmartSPODAS"."

În fine, în partea concluzivă a studiului vom evidenția modul în care toate aceste componente, departe de a fi epuizate, sunt controlate în mod unitar, centralizat, pe baza oportunităților oferite de un stat cu o componentă discreționară evidentă, ceea ce reprezintă esența strategiei de securitate cibernetică a Federației Ruse.

2. Sistem complex de includere a criminalității informatice în structura cyber-war

În această privință, inclusiv cyber-criminalitatea a fost atrasă, numeroși infractori informatici fiind incluși în sistemul războiului electronic.

Astfel, proiectul Skolkovo[76], care avea în vedere combaterea criminalității cibernetice prin integrarea infractorilor informatici, a condus la o structură ambiguă și la raporturi specifice activităților de intelligence, în cadrul cărora se admite o anume autonomie a celor vizați, în schimbul utilizării expertizei lor de către structuri statale.

Această formulă este cât se poate de utilă în disiparea responsabilității și a posibilităților de identificare a cyber-atacatorilor.

Așa se și explică faptul că frecvent atunci când se semnalează atacuri cibernetice se menționează doar suspiciunea că ele aparțin unui stat și unui grup de criminalitate informatică.

Altfel spus, este vorba de o complicitate ce vizează folosirea integrată a capacităților de atac, de rețea informatică, mărirea capacităților de influență cibernetică, încorporarea forțelor cibernetice civile în planificarea militară, includerea elementelor non-military în noua dimensiune cibernetică, astfel încât să fie consolidat conceptul extins de information war.

În acest concept, care nu este specific doar Federației Ruse, sunt incluse și războiul radioelectronic, operațiunile de influențare psihologică, operațiunile de propagandă prin intermediul mediei clasice și online, presa rusă în cadrul unui concept integrativ, holistic.

Ceea ce diferențiază acest construct în cadrul Federației Ruse este o conștientizare de masă a acestei strategii, folosirea fiecărui utilizator de internet, a fiecărui deținător de computer, ca pe un punct nodal al acestei concepții.

[76] Skolkovo Institute of Science and Technology, http://www.skoltech.ru/en

3. Structuri complexe militar-civile și crearea unei noi generații în strategia dezvoltării războiului

Deși nu există confirmări oficiale în această privință, numărul companiilor care au ca obiect cercetarea științifică ce își propun atragerea absolvenților și studenților în cadrul competițiilor și structurilor subordonate sistemelor informatice de sorginte militară a devenit o preocupare majoră la nivel central.

Astfel, se recunoaște că ”se urmărește lansarea unei recrutări extinse de programatori și experți IT, impusă de volumul mare de informații și tehnologii de securitate, care sunt destinate a fi integrate în logistica armatei în următoarea perioadă”.[77]

În mod declarativ, asumat, se recunoaște ”crearea unei noi generații de tineri care vor dezvolta știința războiului”.

Această afirmație aparține Ministrului Apărării rus și a fost făcută în anul 2014, din contextul în care a fost emisă această declarație-program reiese că este vorba de războiul informațional și că tinerii la care se referă nu vor fi neapărat incluși în structuri militare.

Cu toate acestea, se au în vedere și astfel de structuri militare, precum un Centru Special Cyber Defense în cadrul Statului Major General, precum și centre similare în cele patru districte militare, ceea ce vizează unei rețele ciber militară, care însă va funcționa fără conexiuni la internet, cu o protecție multilevel, destinată să prevină orice atac exterior, fiind așa cum se întrevede un sistem cyber militar ofensiv prin definiție.

4. Înregimentarea rețelelor sociale în războiul informațional

Pentru a avea o imagine exactă a ceea ce reprezintă atacurile informaționale prin intermediul rețelelor de socializare, relevante sunt dezvăluirile apărute în presa occidentală, în primul rând, în ziarul ”The Guardian”, care într-o serie de articole au dezvăluit modul cum este folosită ”armata de bloggeri” a Rusiei. Sute de bloggeri sunt plătiți de Moscova pentru a inunda internetul cu comentarii, a umple forumurile din Rusia și

[77] Gabriela Ioniță, *Federația Rusă – în topul agresorilor cibernetici?*, 7 aprilie 2015, http://powerpolitics.ro/rusia-si-amenintarile-cibernetice/

secțiunile de comentarii din publicațiile vestice cu punctele de vedere oficiale ale Moscovei.

În această privință se remarcă poziția total antioccidentală și antiucraineană, precum și cea de apărare a Republicilor Donețk și Lugansk, precum și în apărarea invaziei Crimeei.[78]

Potrivit acestei publicații, activitatea bloggerilor postaci se desfășoară la Sankt Petersburg într-o clădire de patru etaje, pe a cărei firmă scrie ”Business Center” de pe strada Savușkina.

În fiecare dimineață, la ora 9,00, o mulțime de angajați își încep programul care durează 12 ore, după care sunt înlocuiți de alții, care vin în tura de noapte.

Cei doi angajați care au făcut depoziții în fața reporterilor de la The Guardian arătau că trebuiau să mențină conturi false pe LiveJurnal și să răspândească comentarii favorabile Kremlinului, conform unei grile în care introduceau texte anodine spre a nu atrage atenția, în baza unor reguli sofisticate de manipulare.

Astfel, bloggerul care lucra pe Live Jurnal trebuia să scrie despre ”cele mai frumoase 20 de castele din Europa” sau ”zece semne care arată că te întâlnești cu fata care nu ți se potrivește”, intercalate cu postări politice cu privire la Ucraina, sau care să sugereze că liderul opoziției ruse, Alexei Navalni, este corupt.

Cel mai înfricoșător este atunci când observi că această modalitate de comunicare are efect extrem de ridicat, astfel încât partenerii, respectiv prietenii de blog, repetă lucruri pe care le-ai transmis prin sarcinile tehnice, fiind de acord cu ele și răspândindu-le mai departe în rețea.

Cel de-al doilea angajat, conform declarațiilor sale, a lucrat într-un departament în care angajații postau în mod metodic comentarii pe forumuri. În acest departament, se lucrează în echipe de câte trei, primul posta plângeri de diverse probleme sau un link, în timp ce ceilalți doi postau linkuri către materiale în care Putin este elogiat sau fotografii în care Occidentul sau liderii ucrainieni sunt discreditați.

De exemplu, după masacrul din redacția publicației Charlie Hebdo, cititorul trebuia să rămână cu concluzia că Putin i-a trimis condoleanțe lui Francois Hollande, contactându-l imediat, în ciuda relațiilor proaste dintre Rusia și Occident.

[78] http://www.agerpres.ro/externe/2015/04/02/rusia-foloseste-o-armata-de-informaticieni-pentru-propaganda-pe-internet-the-guardian--20-14-04

Concluzia trebuia să fie că SUA încearcă în mod deliberat să slăbească Rusia, iar Ucraina este folosită pentru atingerea acestui scop.

Dacă în fiecare zi ești hrănit cu astfel de mesaje, începi să crezi în ele, desigur în primul rând fiind vorba de cei care le postează.

Dar e clar că cei aflați în această rețea sunt supuși unui proces de dependență și, la rândul lor, devin postaci din obișnuință sau chiar din convingere.

Acești foști angajați ai ”fabricii de mesaje rusești”, denumiți într-un limbaj internațional ”troli” sau postaci erau supuși unui regim draconic, primind amenzi dacă întârziau chiar și câteva minute sau dacă nu-și atingeau targetul de postări. Trolii lucrează în încăperi în care se aflau aproximativ 20 de persoane, fiecare grup fiind controlat de trei editori, care verifică mesajele și sancționează copi-paste-ul.

Ei erau plătiți cu 45.000 de ruble (790 dolari sau 520 euro) pe lună, fără însă să semneze vreun contract, singurul document fiind un acord de confidențialitate.

Fără îndoială, că astfel de sisteme nu funcționează doar în Rusia. Este însă un caz-școală, un adevărat studiu de caz relevant pentru modul în care social media este utilizat în domenii și cu scopuri care, până recent, erau în stadii experimentale.

5. Strategia de securitate cibernetică a Federației Ruse – vector agresiv de impact

Strategia de securitate cibernetică a fost elaborată sub semnătura președintelui Vladimir Putin în anul 2013 în care se arată că aceasta este îndreptată împotriva principalelor amenințări, și anume: ”folosirea tehnologiei cibernetice ca armă în scopuri militare-politice, teroriste și criminalte, precum și tentativele de intervenție prin internet în treburile interne ale altor națiuni”.

Strategia include cooperarea cu organismele internaționale și aderarea la Convenția ONU privind securitatea cibernetică internațională .

În spațiul cyber, atacurile informatice constituie o realitate greu de controlat.

Atât autoritățile de la Washington cât și de la Moscova acuză partea adversă că se confruntă cu până la 10.000 de atacuri cibernetice zilnic în nenumărate domenii, de o intensitate diversă, de la unele foarte puternice la altele ce au un impact mai redus.

Aceste atacuri pot atinge și blocarea infrastructurii de rețea în numeroase țări, pe diverse perioade, atât la nivel național, cât și pe diverse sectoare precis determinate.

Astfel, sunt cunoscute atacurile de rețea de tip DDoS[79] împotriva Estoniei (aprilie 2007), Georgiei (2008), Israelului și altora, care însă nu au fost revendicate.

Dacă în cazul Estoniei și Georgiei, existau suspiciuni că atacul a fost orchestrat sau, mai exact, în terminologia utilizată, ”sponsorizat” de statul rus, până în prezent nu s-au produs dovezi indubitabile.

O documentare precisă cu acuze clare întâlnim într-o poziție a lui George Maior, fostul șef al Serviciului Român de Informații (SRI), într-un articol publicat de ”The Financial Times” în aprilie 2015[80], în care arată că: ”Rusia duce de câțiva ani un război tăcut pe teritoriul țărilor europene prin intermediul spionajului cibernetic, fiind timpul ca NATO și Europa să contracareze aceste activități. Ofensiva spionajului rus, spune în continuare autorul, este dusă cu o determinare și sofisticare crescută”.

România, mai spune fostul șef al SRI, a fost o țintă a cyber spionajului rusesc în mai multe atacuri succesive, care însă au putut fi detectate și blocate de către Serviciul Român de Intelligence. În continuare, analiza fostului șef al SRI detaliază care sunt aceste direcții utilizate de spionajul rusesc în războiul informatic.

Mai întâi, este vorba de capacitatea hacherilor ruși de a accesa rețelele informatice până la nivelul celor al Departamentului de Stat al SUA și Casei Albe – ceea ce denotă sprijinul din partea autorităților.

De pildă, un atac asupra site-urilor guvernamentale din Germania în 2015 a fost revendicat de grupul autointitulat CyberBerkut, care și-a afișat scopul propagandistic în favoarea Moscovei, acuzând sprijinul acordat de Berlin Kievului.

În final, diplomatul român inventariază operațiunile ce fac parte din strategia purtată de Federația Rusă împotriva țărilor occidentale, începând

[79] A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

[80] http://blogs.ft.com/beyond-brics/2015/04/15/russias-silent-war-against-the-west/

http://www.hotnews.ro/stiri-esential-19937611-george-maior-cyber-spionii-rusi-atacat-romania-2013-pentru-afla-informatii-secrete.htm

de la finanțarea unor partide și platforme politice, crearea de bloguri și site-uri proruse, manipularea în rețelele de socializare, folosirea agenților de influență, toate vizând manipularea și dezinformarea, reconstruirea unei sfere de influență europeană în cadrul unui război informațional, care tinde spre un nivel de intensitate din ce în ce mai ridicat, cu un grad tot mai sporit de determinare și sofisticare.

Concluzii

Tehnologia informațiilor digitale și-a găsit cel mai fertil teren, cum era de așteptat, în domeniul securității, intelligence și războiului informațional.

Infrastructura cibernetică cu scopuri defensive și agresive include majoritatea platformelor de socializare aflate în conexiune directă cu sistemele cibernetice de securitate organizate conform structurilor militare.

Acest proiect de militarizare este o direcție majoră de viitor prin includerea tinerilor studenți și absolvenți, dar și a minorilor prin jocurile electronice, ceea ce denotă preocuparea pentru utilizarea rețelelor de socializare ca platforme permanente pentru continuumul război-pace pe care îl reprezintă războiul informațional cu subspeciile sale, război cibernetic, mediatic și electronic.

Dacă într-o primă fază, repede depășită, rețelele de socializare au fost folosite în special pentru culegerea de informații și monitorizarea utilizatorilor, în etapa actuală preponderentă devine transformarea acestora în vectori de multiplicare a mesajului și de folosirea lor ca agenți voluntari sau involuntari înrolați de cele mai multe ori fără acceptul lor în continua activitate de agresiune pe care statele, dar în primul rând marile puteri, o poartă împotriva celorlalte entități, nu doar statale.

Este, altfel spus, un război al tuturor contra tuturor, în care structurările cele mai vizibile aparțin statelor și sistemelor totalitare, care au creat deja un complex ce acționează integrat după paradigme militare cu scopuri distructive față de adversar și, evident, defensive în privința propriilor sisteme.

Rețelele de socializare, după ce au creat posibilitatea ca fiecare individ să fie interconectat în orice moment cu oricare altă persoană, a creat și riscul ca fiecare să devină un potențial adversar prin îndoctrinarea și manipularea sa, prin mijloacele pe care le reprezintă înalta tehnologie a comunicării online.

Conștientizarea acestor riscuri, dar și demonstrația că există posibilitatea contracarării, nu doar la nivel general, ci mai ales la nivel individual, este o opțiune dezirabilă.

Bibliografie selectivă

- Ioniță, Gabriela, *Federația Rusă – în topul agresorilor cibernetici?*, 7 aprilie 2015
- Pătruț, Bogdan, Monica, Pătruț, *Social Media in Politics, Case Studies on the Political Power of Social Media*, Springer International Publishing, Switzerland, 2014
- Messier, Ric, *Collaboration with cloud computing: Security, Social Media and Unified Communications*, Elsevier, 2014
- Skolkovo Institute of Science and Technology, http://www.skoltech.ru/en
- http://blogs.ft.com/beyond-brics/2015/04/15/russias-silent-war-against-the-west/
- http://www.hotnews.ro/stiri-esential-19937611-george-maior-cyber-spionii-rusi-atacat-romania-2013-pentru-afla-informatii-secrete.htm
- http://www.agerpres.ro/externe/2015/04/02/rusia-foloseste-o-armata-de-informaticieni-pentru-propaganda-pe-internet-the-guardian--20-14-04
- http://powerpolitics.ro/rusia-si-amenintarile-cibernetice/