ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXV/SUPLIMENT, ŞTIINŢE JURIDICE, 2019

Aspecte privind elaborarea profilului hackerului în cyberspaţiu

Aspects Regarding the Development of the Hacker's Profile in Cyberspace

Adrian Cristian Moise[1]

Rezumat:
Pornind de la noţiunile de hacker şi hacking, prezentul articol şi-a propus să prezinte şi analizeze aspecte referitoare la elaborarea profilului hackerului. *Cybercriminal profiling* reprezintă o tehnică ştiinţifică ce determină personalitatea şi caracteristicile comportamentale ale unei persoane în cyberspaţiu prin utilizarea unor metode de cercetare din domeniul ştiinţelor sociale, calculatoarelor şi criminologiei. Pentru hackeri, activitatea de hacking nu reprezintă doar o tehnică de accesare neautorizată în sistemele şi reţelele informatice, ci reprezintă mai degrabă un stil de viaţă. În vederea elaborării profilului hackerului, articolul subliniază importanţa motivaţiei, aptitudinilor tehnice şi manifestărilor tehnice de comportament criminal în cyberspaţiu. Articolul prezintă şi analizează şi principalele motive ale hackerilor de comitere a hackingului, cât şi cele mai cunoscute categorii de hackeri.

Cuvinte-cheie: hacker; hacking; cyberspaţiu; cybercriminal profiling; motivaţie.

Abstract:
Starting from the concepts of hacker and hacking, this article aims to present and analyze aspects related to the development of the profile of the hacker. Cybercriminal profiling is a scientific technique that determines the personality and behavioral characteristics of a person in cyberspace by using research methods in the field of social sciences, computers and criminology. For hackers, hacking is not just a technique of unauthorized access to computer systems and networks, but rather a lifestyle. In order to develop the hacker profile, the article emphasizes the importance of motivation, technical skills and technical manifestations of criminal behavior in cyberspace. The article presents and analyzes the main reasons for hackers to commit hacking, as well as the most popular categories of hackers.

Keywords: hacker; hacking; cyberspace; cybercriminal profiling; motivation.

[1] Conferenţiar univ. dr., Universitatea „Spiru Haret” din Bucureşti, Facultatea de Ştiinţe Juridice, Economice şi Administrative, Craiova, România; avocat, Baroul Dolj; E-mail: adriancristian.moise@gmail.com.

1. Introducere

Cybercriminal profiling reprezintă o tehnică ştiinţifică ce determină personalitatea şi caracteristicile comportamentale ale unei persoane în cyberspaţiu prin utilizarea unor metode de cercetare din domeniul ştiinţelor sociale, calculatoarelor şi criminologiei.

În literatura de specialitate există diferite tehnici ştiinţifice pentru a combate criminalitatea din spaţiul real, *criminal profiling* fiind una dintre aceste tehnici.

Cu toate acestea, aplicabilitatea unor astfel de tehnici criminologice la criminalitatea informatică reprezintă o provocare, determinată nu numai de mediul în care infracţiunile au loc, dar şi de alţi factori, cum ar fi, de exemplu, caracterul de anonimitate pe Internet, limitele geografice şi sistemele de drept diferite.

Spre deosebire de spaţiul real, în cyberspaţiu, când se conturează profilul unui infractor, este necesară o abordare interdisciplinară, fiind utile nu numai cunoştinţele din psihologie, criminologie şi alte ştiinţe juridice, ci şi cunoştinţele din domeniul noilor tehnologii.

Evidenţiem faptul că tehnicile de *criminal profiling* se pot aplica cu succes şi la lumea virtuală.

Potrivit literaturii de specialitate, în general, metodologia de *cybercriminal profiling* cuprinde patru etape[2]. Astfel, prima etapă se referă la profilul victimei şi identifică aspecte variate privind potenţialele ţinte ale infractorilor din cyberspaţiu. Totodată, în această etapă se stabileşte motivul referitor la alegerea victimei ca ţintă şi modul în care victima a devenit ţinta infractorului.

A doua etapă implică identificarea motivelor care au determinat atacul infractorului, cât şi modul de operare al acestuia. În această etapă, motivaţia infracţională este strâns asociată cu o victimă, prin urmare, stabilindu-se o relaţie între victimă şi infractor. De asemenea, această etapă implică efectuarea unei evaluări a riscului asupra victimei şi analiza criminalistică a probelor digitale în scopul determinării caracteristicilor comportamentale. La finalul etapei a doua se urmăreşte obţinerea unor posibile caracteristici comportamentale ale infractorului prin utilizarea parametrilor de identificare a profilului criminalului în cyberspaţiu.

Etapa a treia a metodologiei implică o analiză statistică privind datele obţinute în etapa a doua şi identifică modele care sunt comparate cu caracteristicile comportamentale posibile, obţinute în etapa a doua. În finalul etapei a treia se obţine o listă a caracteristicilor comportamentale ale infractorului.

Etapa a patra implică obţinerea profilului infractorului din cyberspaţiu din caracteristicile care au fost identificate în etapa treia.

Una dintre cele mai importante lucrări în domeniul profilului hackerilor în cyberspaţiu este lucrarea *Profiling Hackers. The Science of Criminal Profiling as*

[2] A. Warikoo, *Proposed Methodology for Cyber Criminal Profiling*, în Information Security Journal: A Global Perspective, Editura Taylor & Francis Group LLC, 23:4-6, 2014, pp. 174-178.

Applied to the World of Hacking, ce a fost elaborată în cadrul proiectului intitulat *Hackers Profiling Project - HPP* – ce a fost dezvoltat de Institutul pentru Securitate şi Metodologii Deschise (Institute for Security and Open Methodologies) - ISECOM[3] – şi de Institutul Inter-regional pentru Criminalitate şi Justiţie din cadrul Organizaţiei Naţiunilor Unite (United Nations Interregional Crime and Justice Institute) - UNICRI[4]. Autorii lucrării *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking*[5] utilizează atât metoda de criminal profiling deductivă, cât şi metoda de criminal profiling inductivă pentru a stabili profilul hackerului în cyberspaţiu. Datele obţinute din literatura de specialitate referitoare la cazurile reale de hacking şi din cadrul chestionarelor (metoda inductivă) sunt corelate cu datele obţinute de la scena infracţiunii (metoda deductivă). Obiectivele Proiectului *Hackers Profiling Project - HPP* au fost:[6] analiza fenomenului de hacking ca un fenomen tehnologic, social şi economic, prin utilizarea unei abordări tehnice şi psihologice; identificarea şi înţelegerea diferitelor motivaţii infracţionale; aplicarea metodelor de criminal profiling la datele colectate; prezentarea informaţiilor obţinute.

2. Noţiunile de hacker şi hacking

Noţiunea de *hacker* şi-a modificat de-a lungul anilor semnificaţia, odată cu dezvoltarea tehnologiei informaţiei şi comunicaţiilor. Termenul de *hacker* îşi are originea în domeniul programării calculatoarelor din perioada anilor 1970, fiind utilizat pentru a defini o persoană care are aptitudini pentru a dezvolta în mod creativ programe pe calculator[7]. De asemenea, cuvântul *hack* se referă la utilizarea inovatoare a tehnologiei informaţiei şi comunicaţiilor, mai ales la producerea de programe ce au condus la rezultate pozitive şi beneficii. Iniţial, termenul de *hacking* a avut semnificaţia unei activităţi de scriere şi de modificare a programelor pentru computer în scopul de a le face mai eficiente. Astăzi, termenul de *hacking* se referă la obţinerea accesului neautorizat într-un sistem informatic în scopuri multiple, cum ar fi, de exemplu, furtul de date informatice, alterarea datelor informatice etc.

În concluzie, termenii de *hacking* şi *hacker* sunt folosiţi pentru a denumi activităţile ilegale referitoare la accesul ilegal într-un sistem informatic şi pentru a indica acele persoane care sunt implicate în aceste activităţi ilegale.

---

3 Institute for Security and Open Methodologies, disponibil pe site-ul: http://www.isecom.org/about-us.html, consultat la 31.10.2019.

4 United Nations Interregional Crime and Justice Institute, disponibil pe site-ul: http://www.unicri.it/, consultat la 31.10.2019.

5 R. Chiesa, St. Ducci, S. Ciappi, *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking*, United Nations Interregional Crime and Justice Institute, Hackers Profiling Project, Editura Taylor & Francis Group, LLC, Boca Raton, Florida, 2009, p. 62.

6 R. Chiesa, St. Ducci, S. Ciappi, *op. cit.*, pp. 58-59.

7 M. Yar, *Cybercrime and society*, Editura SAGE Publications Ltd., Londra, 2006, p. 23.

3. Principalele tipologii ale hackerului în cyberspaţiu

Principalele categorii de hackeri sunt următoarele:[8]

▪ **Wannabe**

Hackerii Wannabe (aspiranţi) utilizează tehnici de hackeri fără să aibă cunoştinţe despre acestea şi nici curiozitatea de a învăţa cum funcţionează de fapt aceste tehnici. Hackerii Wannabe utilizează programe concepute de hackerii mai experimentaţi, ce pot fi descărcate gratuit de pe Internet, aceste programe putând automatiza diferite procedee pe Internet care altfel ar fi fost realizate manual. Aceste instrumente concepute de hackerii mai experimentaţi pot conţine greşeli sau programe backdoor. De asemenea, hackerii Wannabe pot posta o cantitate mare de mesaje pe diferite forumuri, solicitându-le celorlalţi hackeri să-i înveţe cum să devină hackeri experimentaţi;

▪ **Script Kiddie** reprezintă hacker-ul cel mai neexperimentat dintre hackerii care săvârşesc infracţiuni în spaţiul virtual. Această denumire este una peiorativă, fiind folosită de hackerii cu experienţă pentru a se referi la hackerii neexperimentaţi care utilizează programe realizate de alţii în scopul exploatării vulnerabilităţilor de securitate ale sistemelor informatice. Hackerul Script Kiddie nu este capabil să scrie propriile programe şi nu înţelege pe deplin programele pe care le execută;

▪ **Cracker-ul** reprezintă acea persoană care pătrunde neautorizat într-un sistem informatic sau într-o reţea informatică prin încălcarea măsurilor de securitate ale acestora. În general, crackerii posedă abilităţi tehnice bune ce le permit să-şi urmărească scopurile;

▪ **Hacker-ul etic** este o persoană cu abilităţi tehnice excelente care sprijină comunitatea să descopere deficienţele şi erorile existente în cadrul infrastructurii IT, protocoale şi aplicaţii;

▪ **Hacker-ul QPS (Quiet, Paranoid, Skilled Hacker)**

Acest tip de hacker pătrunde neautorizat în sistemele informatice fără a produce pagube acestora. Scopul atacurilor realizate de acest tip de hacker este de a dobândi experienţă şi noi cunoştinţe, nefiind interesat de faimă sau de bani. În cazul în care prezenţa sa în sistemele informatice este detectată, ceea ce este foarte greu de realizat, atunci hacker-ul QPS va dispărea imediat;

▪ **Cyber-warrior**

Hackerii cyber-warrior reprezintă persoane care fac parte din grupuri extremiste din mediul politic sau religios. Acest tip de hacker lucrează pe bază de comision, câştigând bani din săvârşirea unor atacuri asupra unor obiective specifice;

▪ **Spionul industrial** se referă la acele persoane care sunt infiltrate ca spioni în diferite companii, având abilităţi tehnice excelente şi experienţă, şi care

[8] R. Chiesa, *Hackers Profiling: Who Are the Attachers?*, în Freedom From Fear Magazine, Issue no.7/2010, United Nations Interregional Crime and Justice Institute, Max Planck Institute, Basel Institute of Governance, Torino, pp. 4-7, disponibil pe site-ul: http://f3magazine.unicri.it/, consultat la 31.10.2019.

reuşesc să obţină informaţii confidenţiale utilizând noile oportunităţi oferite de tehnologia informaţiei şi comunicaţiilor;

▪ **Agentul guvernamental** reprezintă acel tip de hacker care desfăşoară activităţi de spionaj, contraspionaj şi monitorizare a informaţiilor referitoare la guverne, persoane, grupuri teroriste şi industrii strategice, cum sunt, de exemplu, sectorul de apărare, furnizorii de energie, apă, gaz etc.;

▪ **Hacker-ul militar**

Dezvoltarea tehnologiei informaţiei şi comunicaţiilor a condus la apariţia unui nou tip de război, *războiul informaţional*, care se realizează prin intermediul unor atacuri cibernetice sponsorizate de guverne şi conduse de hackeri militari;

▪ **Hacktivist-ul** reprezintă acea persoană care săvârşeşte hacking-ul din motive politice. *Hacktivismul* reprezintă o activitate combinată între hacking şi activism[9]. Hacktivist-ul îşi desfăşoară activismul în mediul online în speranţa de a evidenţia ceea ce el consideră a fi cauze nobile, cum ar fi, de exemplu, acţiunile instituţionale imorale sau penale şi politice. Hacktivismul cuprinde, de asemenea, actele de nesupunere civilă prin utilizarea cyberspaţiului. Tacticile utilizate în hacktivism s-au modificat în timp datorită dezvoltării tehnologiei informaţiei şi comunicaţiilor[10].

La fel ca în spaţiul real, în care activiştii utilizează diferite abordări pentru a transmite mesajul, în cyberspaţiu, hacktiviştii folosesc diferite abordări, cum sunt, de exemplu, bombele automate de e-mail, site-urile virtuale şi programele maliţioase.

4. Motivaţia hackerului

Motivaţia reprezintă una dintre cele mai importante caracteristici ale comportamentului uman. Motivaţia este o construcţie teoretică, alcătuită dintr-un ansamblu de factori dinamici care determină comportamentul unui individ[11].

De cele mai multe ori, hackerii, când au fost chestionaţi, au declarat că sunt pe deplin implicaţi în activităţile lor de hacking şi nu urmăresc obţinerea vreunui câştig[12]. Pentru hacker, computerul în sine este un divertisment ce semnifică un exerciţiu mental obţinut prin intermediul unei activităţi intrinsece interesante şi stimulatoare[13]. Astfel, având în vedere cele prezentate, putem concluziona faptul că motivaţia hackerilor poate fi privită ca fiind o una intrinsecă. Motivaţia

---

9 R. Russell, *Politics*, în K.L. Poulsen (ed.), *Hack Proofing Your Network: Internet Tradecraft*, Editura Syngress Publishing Inc., Rockland, Massachusetts, 2000, p. 8.

10 J. Migga Kizza, *Computer Network Security*, Editura Springer Science+Business Media, Inc., New York, 2005, p. 142.

11 A.C. Moise, *Dimensiunea criminologică a criminalităţii din cyberspaţiu*, Editura C.H. Beck, Bucureşti, 2015, p. 263-268.

12 Al.E. Voiskounsky, O.V. Smyslova, *Flow-Based Model of Computer Hackers' Motivation*, în CyberPsychology & Behavior, April 2003, Vol. 6, no. 2, Editura Mary Ann Liebert, Inc., New Rochelle, New York, pp. 171-173.

13 Th.J. Holt, *Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures*, în Deviant Behavior, Volume 28, Issue 2/2007, pp. 171-198.

intrinsecă reprezintă dorinţa proprie de a căuta lucruri şi provocări noi, de a analiza capacitatea cuiva şi de a observa şi dobândi cunoştinţe. Totodată, motivaţia intrinsecă este condusă de propria plăcere şi există în persoană mai degrabă decât în constrângerile exterioare sau dorinţa pentru recompensă.

Una dintre cele mai importante teorii din literatura de specialitate care se referă la motivaţia intrinsecă este Teoria Fluxului[14], elaborată de profesorul de psihologie Mihaly Csikszentmihalyi**,** de la Universitatea din Chicago. Fluxul reprezintă o stare mentală în care o persoană este cuprinsă de un sentiment de concentrare puternică într-o activitate, implicându-se total şi cu dorinţa de succes în desfăşurarea acelei activităţi. Fluxul este însoţit de emoţii pozitive şi de satisfacţii proprii.

Totodată, fluxul poate fi definit şi ca o stare în care toate faptele, gândurile, motivaţiile şi sentimentele interacţionează şi lucrează împreună fără probleme, atât pentru nevoile interne ale indivizilor, cât şi pentru a face faţă provocărilor lumii exterioare[15].

Caracteristicile fluxului sunt următoarele: obiective clare de urmărit; echilibru între cerinţele externe şi capacităţile personale ale subiectului; reacţia imediată în urma efectuării unei acţiuni; controlul deplin asupra situaţiei fără a fi necesară o monitorizare proprie; modificarea percepţiei timpului.

Mecanismul de funcţionare a fluxului se realizează în următorul fel: după experienţa unui flux, individul dezvoltă o complexitate psihică crescută şi, prin urmare, caută provocări mai mari. Această situaţie conduce la o creştere suplimentară a nivelului de competenţe necesar pentru a face faţă provocării. Aşadar, alegerea unei provocări mai dificile conduce la o creştere a competenţelor individului. După o perioadă de învăţare, provocarea şi competenţele personale se potrivesc din nou exact şi o stare de flux este încercată din nou.

În literatura de specialitate[16] s-a elaborat un model de motivaţie a hackerilor bazat pe Teoria Fluxului ce presupune faptul că un hacker care are o pregătire profesională superioară atinge o stare de flux mult mai des decât hackerii care au o pregătire profesională inferioară. Acest model se bazează pe potrivirea între nivelul de competenţe referitoare la utilizarea computerului şi nivelul de provocări ale hacking-ului întreprinse de hacker. Un hacker începător găseşte o potrivire între competenţele şi provocările sale şi începe să experimenteze fluxul. Motivaţia este una puternică, iar hacker-ul începător încearcă o senzaţie de bunăstare.

Prin urmare, observăm faptul că hacker-ul începător ar putea sta la acest nivel mulţi ani, întrucât acesta nu caută provocări mai mari, şi nici nu obţine competenţe profesionale superioare.

Unii autori au subliniat faptul că Teoria Fluxului explică evoluţia carierei hackerului, dar singură aceasta nu poate oferi un model complet pentru

[14] M. Csikszentmihalyi, *Beyond Boredom and Anxiety: Experiencing Flow in Work and Play*, Editura Jossey-Bass Inc. Publishers, San Francisco, California, 1975.

[15] R. Chiesa, St. Ducci, S. Ciappi, *op. cit.*, p. 45.

[16] Al.E. Voiskounsky, O.V. Smyslova, *op. cit.*, pp. 173-179.

criminalitatea din cyberspaţiu. Aceştia propun un model de dezvoltare a carierei hacker-ului, ce cuprinde şi alţi factori, cum ar fi, de exemplu, ideologia şi vandalismul, pentru a determina dacă tipul de persoană este un hacker etic sau un hacker maliţios[17].

În concluzie, principalele motive ale hackerilor sunt următoarele:[18]

▪ **Curiozitatea intelectuală**

Hackerii doresc să înveţe cum funcţionează reţelele şi sistemele informatice şi, de asemenea, să dobândească noi cunoştinţe referitoare la securitatea informatică;

▪ **Pasiunea pentru tehnologie**

Când motivaţia hackerilor se bazează pe pasiunea pentru tehnologie, activitatea de hacking se referă la explorarea sistemelor informatice, însă fără a avea ca scop afectarea acestora;

▪ **Amuzamentul**

Hackerii care accesează neautorizat sisteme informatice pentru amuzament nu urmăresc obţinerea unor avantaje financiare, ci doar simpla pătrundere neautorizată în sistemul informatic al unei persoane;

▪ **Îmbunătăţirea sistemelor informatice**

Mulţi hackeri doresc să contribuie la îmbunătăţirea performanţelor sistemelor informatice. De asemenea, aceştia doresc să crească şi nivelul de securitate al sistemelor şi reţelelor informatice;

▪ **Lupta pentru libertate**

Mulţi hackeri consideră activitatea de hacking ca fiind un instrument de luptă împotriva problemelor politice şi sociale. Hacking-ul este folosit în special împotriva eventualelor încălcări ale principiilor care guvernează lumea online şi împotriva atacurilor săvârşite în lumea fizică, pe care hackerii o consideră coruptă. Hackerii doresc să apere dreptul la informare al oricărei persoane, determinând ca informaţia să circule liber şi să fie accesibilă pentru oricine;

▪ **Spiritul de revoltă**

Hackerii, prin acest tip de motivaţie, doresc să-şi demonstreze superioritatea faţă de autorităţile publice prin pătrunderea neautorizată în sistemele şi reţelele informatice ale acestora;

▪ **Atragerea atenţiei şi faima**

Unii hackeri simt nevoia să facă cunoscute succesele obţinute în activitatea lor, în scopul de a deveni celebri şi de a atrage atenţia mass-mediei;

---

[17] L. Rennie, M. Shore, *An Advanced Model of Hacking*, în Security Journal, no. 20/2007, pp. 236-251.

[18] R. Chiesa, St. Ducci, S. Ciappi, *op. cit.*, pp. 147-159; R. Russell, *op. cit.*, pp. 15-19; A. Hutchings, *Hacking and Fraud. Qualitative Analysis of Online Offending and Victimization*, în K. Jaishankar, N. Ronel (eds.), *Global Criminology. Crime and Victimization in a Globalized Era*, Editura CRC Press, Taylor & Francis Group, Boca Raton, Florida, 2013, p. 95.

▪ **Furia şi frustrarea**

Furia şi frustrarea îi pot determina adesea pe hackeri să săvârşească anumite fapte, pe care în mod normal nu le ar săvârşi, din cauza acestor tulburări emoţionale;

▪ **Motive politice**

Unii hackeri încearcă să implice comunitatea hackerilor în politică;

▪ **Evadarea din mediul familial şi din societate**

Pentru a scăpa de un mediu familial conflictual, de o viaţă de izolare şi singurătate şi pentru a se detaşa de realităţile sociale, hackerii îşi găsesc un refugiu în pasiunea lor pentru computere;

▪ **Motive profesionale**

Există hackeri care desfăşoară activităţi de hacking nu numai din pasiune, ci şi ca urmare a unor motive profesionale, cum ar fi, de exemplu, hacker-ul cyber-warrior, spionul industrial, agentul guvernamental, hacker-ul militar etc.

▪ **Profiturile financiare**

Majoritatea hackerilor au ca motivaţie infracţională obţinerea de câştiguri financiare.

5. Concluzii

Pe baza studiilor criminologice realizate la nivel naţional şi internaţional care au urmărit fenomenul hackingului, s-au obţinut o serie de informaţii şi date utile în investigarea criminalităţii informatice, cum sunt datele personale, datele relaţionale şi datele tehnice şi criminologice referitoare la profilul hackerului în cyberspaţiu.

Evidenţiem importanţa Teoriei Fluxului în stabilirea motivaţiei infracţionale a hackerului, această teorie încercând să explice concentrarea într-o anumită activitate, unde experienţa, ea însăşi, este dorită mai degrabă decât orice scop final specific, reprezentând o explicaţie pentru activitatea intensă ce se desfăşoară pe Internet. Când se confruntă cu fluxul, utilizatorii simt concentrarea, curiozitatea, interesul intrinsec şi controlul asupra activităţii desfăşurate. Emoţiile constatate de hackeri sunt asemănătoare cu cele constatate de alte persoane care se confruntă cu fluxul, iar unele dintre motivele oferite ca explicaţii de către hackeri, cum sunt, de exemplu, interesul intrinsec şi curiozitatea, pot fi susţinute de Teoria Fluxului.