

PERSONALITATEA HACKERULUI - MINOR

FLOREA Eugen

doctor în drept, conferențiar universitar
Universitatea Cooperatist-Comercială din Moldova

ORCID ID: 0000-0001-7236-0695

Summary. *Juvenile cybercrime is the problem that has received little attention in academic research. This study is dedicated to applicability of M. Gottfredson and T. Hirshi theory of self-control for explaining juvenile illegal hacking. The article also covers the applicability of T. Hirshi social bounding theory to this type of crime. The main author's conclusion it that the causes of juvenile cybercrime have cross-national nature. Weak self-control, as well as the lack of social ties with family and school, are the main factors contributing to teenager's illegal behavior in cyberspace, and factors such as place of birth, the degree of urbanization of the place of residence have a lesser effect on the likelihood of a teenager violating the law both in real and virtual world.*

This kind of research always has a number of limitations, which are associated with the correct understanding by the interviewed adolescents of the questions addressed, as well as their sincerity in answers provided. Nevertheless, the information received has a criminological value and can serve as a basis for further research, as well as practical steps in this area.

Keywords: *juvenile, cybercrime, hacker, hacking, cryptocurrency, self-control theory, social bounding theory, parent control, school control.*

În data de 15 iulie 2020, rețeaua populară de socializare Twitter pe pagina sa oficială a anunțat un atac de hacker asupra sa. Folosind metode de inginerie socială[1], atacatorii au reușit să spargă 130 de conturi. Printre acestea au fost sparte conturile mai multor persoane publice, politicieni, oameni de afaceri de rang înalt. În special, au fost sparte conturile fostului președinte american Barack Obama, CEO-ului companiei Tesla Elon Musk, CEO-ului companiei Amazon Jeff Bezos, co-fondatorului companiei Microsoft Bill Gates, candidatului la președinția SUA (în acel moment) Joe Biden, magnatului media Michael Bloomberg, bine cunoscutului investitor-miliardar Warren Buffett, precum și contul oficial al companiei Apple [2]. După ce au preluat controlul conturilor, atacatorii din numele vedetelor au publicat tweet-uri conform cărora oricine care ar transfera moneda virtuală Bitcoin către portofelul electronic indicat în mesaj ar primi înapoi aceeași sumă în dublu față de suma expediată. Potrivit KrebsOnSecurity, o companie de securitate cibernetică, au fost efectuate aproximativ 400 de transferuri în valoare totală de peste 100.000 USD către portofelele electronice ale infractorilor ciberneticici[3].

În luna martie 2022, poliția londoneză a arestat șapte adolescenți cu vârsta cuprinsă între 16 și 21 de ani, suspecți de activități criminale de hacking. Este vorba despre binecunoscutul grup de hackeri Lapsus\$, cunoscut pentru atacurile

sale cibernetice asupra Microsoft, Uber, Okta și implicat și în extorcare cibernetică folosind virusul Wannabe. Șeful organizației este considerat a fi un adolescent de 16 ani, cunoscut sub numele de „White”. Numele său real, adresa de domiciliu și fotografiile de pe rețelele de socializare au fost postate pe un forum specializat de hackeri de către persoane cu care adolescentul a avut un dezacord financiar. Tot pe acest forum a fost postată și o scurtă cronologie a atacurilor cibernetice efectuate de hackerul minor, în urma cărora în contul său s-au acumulat aproximativ 300 BTC (în aceea perioadă având o valoare de aproximativ 6 milioane de dolari). Conform datelor sursei, copilul are o tulburare de spectru autist și frecventează o școală specială din Oxford. Părinții nu cunoșteau nimic despre activitățile copilului lor, crezând că „se joacă” la calculator[6].

Aceste exemple, la fel ca și multe alte cazuri, demonstrează că problema crimei cibernetice juvenile nu este una exagerată. Generația născută în secolul XXI încă din copilărie se confruntă cu produsele revoluției științifice și tehnologice și este de fapt modelată de influența Internetului și a dispozitivelor informatice. Prin urmare, nu este surprinzător faptul că minorii moderni sunt mult mai buni decât adulții în multe subtilități tehnice asociate cu tehnologia informațională. Și dacă pentru unii totul se limitează la jocuri și participarea activă la rețele sociale, atunci pentru alții computerele și Internetul devin o sursă semnificativă de venit. Trebuie de remarcat faptul că câștigurile în acest domeniu pot fi absolut legale. Deci, e-sportivii de succes care și-au perfecționat abilitățile într-un anumit joc pe computer pot câștiga sute de mii sau chiar milioane de dolari. Campionatele mondiale desfășurate în mod regulat în domeniul jocurilor de computer, precum *Dota 2*, *Counter Strike*, *Fortnite*, *League of Legends* etc. adună un public uriaș în întreaga lume și oferă premii bănești pentru câștigători care sunt comparabile cu recompensele pentru victorii în cele mai populare sporturi tradiționale din lumea reală. De asemenea, un adolescent care cunoaște bine tehnologia informațională poate face așa-numitul *white hacking* (sau *white-hat hacking*), care este munca de testare a securității cibernetice a unui obiect. Hackerii albi contra cost (*bounty*) oferă servicii pentru găsirea vulnerabilităților pentru a le elimina în continuare din sistemul clientului.

În literatura criminologică problema hackerilor minori este una dintre cele puțin studiate. Printre cele mai cunoscute se numără lucrările cercetătorilor americani *A. Bowker* [7, p. 40-43], *D. Verton* [8, p. 40-43], *J. De Marco* [9, p. 48-55], *J. Manchi* [10, p. 147-145], *M. Yar* [11, p. 387-399], *B. Sterling* [12]. Astfel *M. Yar* a atras atenția asupra implicării „disproporționat de mari” a minorilor în comiterea infracțiunilor informatice. La rândul său, *B. Sterling* susține că majoritatea hackerilor încep să facă hacking la vârsta de 11-18 ani, dar odată cu împlinirea vârstei de 20 de ani, entuziasmul lor în mare parte scade. Cercetătorii

atribuie principalelor factori care dau naștere comportamentului ilegal al minorilor în rețeaua cibernetică astfel de trăsături personale ca imaturitatea morală și impulsurile hedoniste [13, p. 97].

Pentru a explica mecanismul criminalității cibernetică criminologii cel mai frecvent fac referire la teoria autocontrolului dezvoltată de cercetătorii americani *A. Godfredson* și *T. Hirschi* [14]. Potrivit savanților numiți toți oamenii au interes să comită o infracțiune dacă aceasta poate satisface orice necesitate personală, dar prezența autocontrolului suprimă acest interes. Însă dacă autocontrolul este insuficient, persoana decide să încalce legea. Potrivit lui *A. Godfredson* și *T. Hirschi*, acest mecanism funcționează indiferent de contextul național, cultural sau geografic. Cu alte cuvinte, acest concept se bazează pe alegerea rațională a unei persoane între beneficiile unei infracțiuni și posibilele consecințe negative pentru sine în urma comiterii acesteia. Formarea unui nivel suficient de autocontrol, conform cercetătorilor menționați, ar trebui să fie efectuată în copilăria timpurie, de preferință înainte de vârsta de opt ani. Principalul factor în acest proces este comportamentul părinților. În primul rând, supravegherea copilului ar trebui să implice o apreciere negativă a comportamentului deviant al copilului și îndreptarea corespunzătoare a comportamentului în direcția corectă. În calitate de măsuri preventive eficiente, *A. Godfredson* și *T. Hirschi* susțin programe care vizează educația timpurie și supravegherea copilului, precum și programe de supraveghere a copiilor și de lucru cu familiile care se confruntă cu probleme psihologice.

Considerăm că teoria dată, care poate fi numită teoria prezenței/absenței frânelor sociale, este pe deplin aplicabilă criminalității informatice juvenile. În același timp, este necesar să se țină cont de specificul de vârstă al acestei categorii de persoane, care impune anumite trăsături în explicarea comportamentului infracțional al persoanelor sub vârsta de 18 ani.

În contextul celor relatate prezintă interes studiul cercetătorilor din Florida și Texas, care au intervievat 18.985 de adolescenți din opt țări (SUA, Venezuela, Spania, Franța, Germania, Polonia, Ungaria, Rusia) [15, p. 40-55]. În timpul studiului au fost testate următoarele ipoteze:

- 1) Scăderea autocontrolului crește probabilitatea de acțiuni ilegale de tip hacking din partea adolescentului;
- 2) Însemnătatea majoră a controlului parental pentru adolescent reduce probabilitatea de hacking ilegal din partea lui;
- 3) Însemnătatea majoră a școlii pentru adolescent reduce probabilitatea de hacking ilegal din partea lui.

Rezultatele studiului au confirmat concluziile teoriei lui *A. Godfredson* și *T. Hirschi*. Autocontrolul scăzut din partea adolescenților crește probabilitatea

implicării lor în hacking ilegal cu 80% [15, p. 48]. De asemenea, rezultatele sondajului au demonstrat o dependență strânsă a hacking-ului ilegal de sexul persoanei. Adolescenții de sex masculin sunt mult mai predispuși la hacking decât fetele.

O altă teorie care a fost testată prin intermediul adolescenților în cadrul aceluiași studiu, fiind numită ”conceptul de control social sau de legături sociale” (*social bonding theory*), propusă în 1969 de *T. Hirschi* [16]. În literatura criminologică se remarcă faptul că specificul cercetării lui *T. Hirschi* este acceptarea criminalității ca a unui rău firesc, fiind pus accentul pe studierea motivației celor care se abțin de la încălcarea legii [17, p. 428-457]. Teoria controlului social nu face excepție de la aceasta ipoteză. Potrivit lui *T. Hirschi*, comportamentul antisocial este rezultatul legăturilor insuficiente ale unei persoane cu societatea convențională. Această conexiune constă din patru elemente:

- atașamentul sau legăturile emoționale ale individului cu alte persoane semnificative pentru el (*attachment to significant others*);
- angajamentul față de obiectivele tradiționale, cum ar fi studiul sau cariera (*commitment to traditional types of action*);
- participarea la activități convenționale (*involvement in traditional activities*);
- acceptarea normelor și moralității generale (*beliefs in the moral values of society*).

Cu cât conexiunea unei persoane cu societatea prin aceste patru elemente este mai puternică, cu atât este mai puțin probabil ca el/ea să se abată de la normele sociale. Conform prezentei teorii, cele patru elemente ale sale sunt interdependente și efectul cumulativ al acestor conexiuni este mai mare decât impactul lor individual. De asemenea, dacă una dintre cele patru legături este slăbită, individul intră într-o stare de probabilitate crescută de a se implica într-un comportament antisocial [16]. Cu alte cuvinte, potrivit lui *Hirschi*, cu cât un adolescent este mai atașat de părinți, școală și colegii săi, cu atât este mai puțin probabil ca acesta să încalce legea. Opusul, este, de asemenea, adevărat: cu cât un adolescent acordă mai puțină importanță opiniilor rudelor, prietenilor și profesorilor despre el însuși, cu atât este mai mult probabil ca acesta să fie implicat într-un comportament criminal. Trebuie de remarcat faptul că teoria legăturilor sociale a fost mult mai rar folosită de specialiștii în domeniu pentru a explica criminalitatea cibernetică decât teoria autocontrolului slab [15, p. 44].

Rezultatele studiului realizat de către *S. Back* cu colegii săi au demonstrat că conexiunile sociale au capacitate predictivă în raport cu hacking-ul ilegal comis de minori, însă, corelația este mai puțin evidentă decât în cazul teoriei autocontrolului slab. Astfel, prezența unor legături emoționale stabile între un

adolescent și părinții săi reduce probabilitatea participării acestuia la hacking ilegal cu 22%, iar importanța mare acordată școlii, în medie, reduce probabilitatea unor astfel de acțiuni cu 21% [15, p. 48-49].

În urma celor expuse, remarcăm importanța deosebită atât teoretică, cât și practică a unor cercetări ulterioare în acest domeniu, inclusiv prin atragerea participării adolescenților din Republica Moldova. Cu toate acestea, chiar și în baza rezultatelor unor studii realizate de savanții străini, se poate concluziona că complexul causal al criminalității cibernetice în rândul adolescenților este de natură transnațională. Considerăm, că slăbirea autocontrolului, precum și lipsa legăturilor sociale ale adolescentului cu familia și școala, sunt principalii factori care contribuie la comportamentul ilegal, iar așa circumstanțe, precum locul nașterii, gradul de urbanizare a locului de trai au o influență mai ne semnificativă asupra probabilității că minorul va încălca legea penală atât în lumea reală, cât și în spațiul virtual.

Desigur, acest gen de cercetare are întotdeauna o serie de limitări, care sunt asociate cu înțelegerea de către adolescentul intervievat a întrebărilor adresate, precum și cu sinceritatea respondentului în răspunsurile oferite. Cu toate acestea, informațiile primite au valoare incontestabilă din punct de vedere criminologic și pot servi drept bază pentru cercetări ulterioare, precum și pentru realizarea unor pași practici eficienți în acest domeniu.

Referințe:

1. În teoria securității informaționale ingineria socială este definită ca orice manipulare care direcționează victima către acțiuni care nu sunt (sau pot să nu fie) în sfera intereselor sale. Printre cele mai frecvente manipulări, trebuie menționate, cum ar fi prezentarea de către un atacator ca o altă persoană, precum și utilizarea de link-uri rău intenționate (phishing). *Vezi:* Social Engineering Defined. În: Security Through Education. [Accesat: 29.10.2022]. Disponibil: <https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/>
2. An update on our security incident. În: Twitter Inc. – 18 July 2020. [Accesat: 24.10.2022]. Disponibil: https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident
3. Three Charged in July 15 Twitter Compromise. În: KrebsOnSecurity – 31 July 2020. [Accesat: 24.10.2022]. Disponibil: <https://krebsonsecurity.com/2020/07/three-charged-in-july-15-twitter-compromise/>
4. Three Individuals Charged for Alleged Roles in Twitter Hack / Official press-release. În: United States Attorney's Office, Northern District of California – 31 July 2020. [Accesat: 26.10.2022]. Disponibil: <https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack>
5. Alleged second teen mastermind behind Twitter's 'Bitcoin giveaway' hack. În:

- Cointelegraph – 02 September 2020. [Accesat: 26.10.2022]. Disponibil: <https://cointelegraph.com/news/alleged-second-teen-mastermind-behind-twitter-s-bitcoin-giveaway-hack>
6. Lapsus\$: Oxford teen accused of being multi-millionaire cyber-criminal. În: BBC News – 24 march 2022. [Accesat: 27.10.2022]. Disponibil: <https://www.bbc.com/news/technology-60864283>
 7. BOWKER, A. L. Juveniles and computers: Should we be concerned? În: Federal Probation Journal. US Courts Publishing. Washington 1999, № 63(2).
 8. VERTON, D. The hacker diaries. New York, NY: McGraw-Hill, Inc. 2002.
 9. De MARCO, J. V. It's not just fun and war games - Juveniles and computer crime. În: United States Attorneys' Bulletin. Executive Office for United States Attorneys Publishing. Washington 2001, № 49(3). - P. 48-55.
 10. MUNCIE, J. Institutionalized intolerance: Youth justice and the 1998 Crime and Disorder Act. În: Critical Social Policy. Sage Publishing. Thousand Oaks 1999, № 19(2).
 11. YAR, M. Computer hacking: Just another case of juvenile delinquency? În: The Howard Journal of Crime and Justice. The Howard League for Penal Reform. London 2005, № 44(4).
 12. STERLING, B. The hacker crackdown: Law and disorder on the electronic frontier. Penguin Publishing. London 1994.
 13. HOLLIN, C. Criminological psychology. În: The Oxford Handbook of Criminology. Editors M. Maguire, R. Morgan, R. Reiner. Oxford University Press. Oxford, 2007.
 14. GOTTFREDSON, M. R., HIRSCHI, T. A general theory of crime. Stanford, CA: Stanford University Press, Stanford 1990.
 15. BACK, S., SOOR, S., La PRADE, J. Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory. În: International Journal of Cybersecurity Intelligence and Cybercrime. # 1 (1), Bridgewater State University, Bridgewater, Massachusetts 2018.
 16. HIRSCHI, T. Causes of delinquency. CA: University of California Press. Berkeley 1969.
 17. MATSUEDA, L. R. The dynamics of moral beliefs and minor deviance. În: Social Forces. Vol. 68, Issue 2. University of North Carolina. Chapel Hill 1989.

