**ROMÂNIA**

**MINISTERUL APĂRĂRII NAȚIONALE**

**ACADEMIA TEHNICA MILITARĂ**

**„FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializarea: Calculatoare și sisteme informatice pentru apărare**

**și securitate națională**



***Aplicație destinată telefoanelor mobile în vederea detecției conectării acestora la stații de***

***bază false care se interpun între terminalul mobil și stațiile de bază ale furnizorilor oficiali***

***de servicii GSM (IMSI CATCHER DETECTOR)***

CONDUCĂTOR ȘTIINȚIFIC:

**Col. conf. univ. dr. ing. BĂDOI ION**

ABSOLVENT:

**Ștefan OLTEANU**

Conţine \_\_\_\_\_\_\_\_\_\_\_ file

Inventariat sub nr\_\_\_\_\_\_\_

Poziţia din indicator: \_\_\_\_

Termen de păstrare: \_\_\_\_\_

**BUCUREȘTI**

**2020**

**ABSTRACT**

**REZUMAT**

**CUPRINS**

[1 INTRODUCERE 10](#_Toc37336095)

[1.1. Importanța temei alese 10](#_Toc37336096)

[1.2. Scopul și obiectivele lucrării 10](#_Toc37336097)

[1.3. Prezentarea metodologiei de cercetare 11](#_Toc37336098)

[1.4. Rezumatul lucrării pe capitole 11](#_Toc37336099)

[2 Clasificarea stațiilor de bază în funcție de legalitate 12](#_Toc37336100)

[2.1. Reglementări cu privire la *Imsi Catcher* 12](#_Toc37336101)

[6 BIBLIOGRAFIE 13](#_Toc37336102)

**LISTĂ DE FIGURI**

# INTRODUCERE

## Importanța temei alese

Dispozitivele de tip *Imsi Catcher* există încă din anul 1993(1)însă erau mari, greoaie și mai ales scumpe. Datorită acestui lucru și a faptului că existau puțini producători, aceste dispozitive nu au fost folosite decât de unele agenții guvernamentale. În zilele noastre, apariția SDR-urilor[[1]](#footnote-2) a permis crearea unor proiecte de acasă și astfel înmulțirea atacurilor asupra rețelelor GSM. Mai mult, dacă inițial aceste atacuri au fost dezvoltate pentru a putea captura codurile IMSI[[2]](#footnote-3) de la telefoanele din apropiere – de unde vine și numele atacului -, versiunile actuale oferă posibilitatea de a intercepta atât apeluri telefonice cât și mesaje.

Prin urmare, această temă este cu atât mai importantă, cu cât nu există modalități de detectare a acestor atacuri, disponibile publicului larg. De asemenea, intrucât numarul acestora a fost în continuă creștere, este necesară informarea persoanelor cu privire la riscurile la care se expun în momentul în care telefonul se conectează la o stație de bază ce nu aparține unui furnizor de servicii local. Un articol realizat de cei de la Washington Post arată că numărul dispozitivelor de interceptare ilegale, găsite în oraș pe parcursul a mai puțin de două zile, este de aproximativ 18 (2). Așadar, nevoia unei aplicații care să ajute la detectarea acestor atacturi ce pun în pericol drepturile societății, este mai mult decât evidentă.

## Scopul și obiectivele lucrării

Scopul acestei lucrări de licență este acela de a expune problematica atacurilor de tip *Imsi Catcher*, de a evidenția modalități de detecție și nu în ultimul rând de a crea o aplicație Android funcțională care să pună în practică modalitățile precizate mai sus.

Printre obiectivele care trebuiesc atinse pe parcursul rezolvării acestei teme se numără un număr de informații cu ajutorul cărora cititorul iși poate face o idee complexă despre modul de funcționare atât a dispozitivului cu care se realizează atacul cât și a dispozitivului de interceptare. De exemplu:

* informații despre modul în care o rețea GSM functionează și ce puncte slabe are;
* prezentarea pe larg a modalităților prin care un dispozitiv *Imsi Catcher* exploatează rețeaua și reușește să capteze atât locația utilizatorului cât și mesaje sau apeluri telefonice;
* descrierea metodelor folosite în cadrul aplicației pentru a detecta atacul;
* s.a.m.d.

Obiectivul principal este ca la finalul lucrării să se poată demonstra cum se realizează atacul și detecția prin simularea unei stații de bază GSM care să preia semnalul telefonului mobil. Acesta din urmă va trebui să detecteze că celula[[3]](#footnote-4) la care este conectat nu aparține furnizorului de telefonie mobilă la care utilizatorul este abonat.

## Prezentarea metodologiei de cercetare

## Rezumatul lucrării pe capitole

# Clasificarea stațiilor de bază în funcție de legalitate

## Reglementări cu privire la *Imsi Catcher*

Aceste dispozitive folosite în mare parte de agențiile de securitate statală au ridicat probleme în legătură cu libertatea și intimitatea civilă. De aceea folosirea acestora se realizează numai conform regulilor scrise în *Codurile de Procedură Penală* (3)*.*

Orice utilizare a unui dispozitiv de tip *Imsi Catcher* se realizează sub jurisdicția *Convenției Europene a Drepturilor Omului,* care stabilește un nivel minim de protecție atât pentru viața privată a individului cât și pentru corespondența acestuia (4). Toate aceste legi ar trebui să analizeze foarte bine comportamentul dispozitivelor, întrucât acestea nu sunt folosite numai pentru monitorizarea prezenței telefoanelor mobile într-o anume zonă, având ca scop identificarea locației pe hartă a acestora, ci și pentru a aduna informații despre utilizatori sau despre dispozitivele pe care aceștia le folosesc.

Pe lânga drepturile descrise mai sus, pe care un astfel de atac ar putea să le încalce, se mai adaugă și încălcarea dreptului la libertatea întrunilor pașnice. Există numeroase modalități prin care acest lucru este posibil, cum ar fi (5):

* persoanele ce cunosc modul de operarare ale acestor tipuri de dispozitive, nu vor mai participa la întalniri, proteste sau orice altă manifestare pașnică deoarece vor ști că prin captarea comunicațiilor mobile, aceștia pot fi urmăriți;
* prin captarea, editarea și rutarea comunicațiilor, abilitatea persoanelor de a comunica între ele va fi alterată;
* în unele cazuri, este chiar posibil ca unele guverne să trimită mesaje tuturor telefoanelor mobile aflate în zona în care se desfășoară o întalnire pentru a intimida, manipula sau pentru a împrăștia utilizatorii.

Deși există o lege europeană care face referire la protejarea individului, nu există legi specifice pentru utilizarea acestor dispozitive. Guverne din Statele Unite ale Americii și Germania au stabilit legi și politici care limitează modalitățile în care agențiile statatale pot utiliza în mod legal dispozitive de tip *Imsi Catcher.* Mai mult, Judecătorii din SUA au impus restricții suplimentare. Câteva exemple referitoare la legile adoptate de Ministerul de Justiție din SUA cu privire la utilizarea *Imsi Catcher* vor fi expuse mai jos: (6)

* limitarea folorii acestor dispozitive numai pentru identificare;
* cererea supervizării interne pentru utilizarea acestora;
* nevoia unui mandat pentru utilizarea acestora în situații care nu sunt urgente sau excepționale.

În cazul Germaniei, *Imsi Catcher-urile* au fost supuse legilor federale încă din anul 2002, atunci când utilizarea acestora a fost autorizată ca urmare a atacurilor de pe 9/11 din Statele Unite ale Americii. Curtea de Justiție Germană are dreptul de a autoriza folosirea unui astfel de dispozitiv numai în cazul în care există dovezi clare că o crimă serioasă are loc. Mai mult, persoanele care sunt vizate de aceste dispozitive trebuie anunțate că au fost subiecții unui *Imsi Catcher*, fără a pune în pericol anumite aspecte ale investigației (6).

* + 1. **Utilizarea IMSI Catcher în afara legii**

Deși atât în Europa cât și în Statele Unite ale Americii există reglementări în legătură cu utilizarea acestui tip de dispozitive, guvernele, agențiile de securitate și anumite persoane rău intenționate le utilizează fără un mandat. Spre exemplu, în 2014, poliția din Florida a recunoscut că a folosit *Imsi Catcher-uri* de cel puțin 200 de ori fără a recunoaște acest lucru în fața judecătorilor sau a avea un mandat care să le permită folosirea acestui dispozitiv (7).

Ideea care ridică probleme în acest sens, este aceea că poliția nu folosește acest tip de dispozive numai pentru prindere criminalilor dar și pentru spionarea populației. Deși în SUA exista numeroase state care dețin astfel de dispozitive, utilizarea lor nu este una transparentă, fapt care a ridicat multe semne de întrebare, deoarece nu se știe dacă acestea au fost folosite cu un mandat sau nu (8).

# BIBLIOGRAFIE

1. *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers.* **Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Edgar Weippl.** 2014, ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference, p. 10.

2. **Ashkan Soltani, Craig Timberg.** Tech firm tries to pull back curtain on surveillance efforts in Washington. *The Washington Post.* [Online] The Washington Post, 09 17, 2014. [Cited: 04 09, 2020.] https://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f\_story.html.

3. **Wikipedia.** Imsi-catcher. *Wikipedia.* [Online] 03 11, 2020. [Cited: 04 09, 2020.] https://en.wikipedia.org/wiki/IMSI-catcher.

4. **Naarttijärvi, Markus.** *Swedish police implementation of IMSI-catchers in a European law perspective.* Umeå : Computer Law & Security Review, 2016.

5. **International, Privacy.** *Privacy International’s contribution to the half-day general discussion on Article 21 of.* s.l. : Privacy International, 2019.

6. **Tamir Israel, Christopher Parsons.** *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada.* Toronto : Telecom Transparency, 2016.

7. **Wikipedia.** Stingray phone tracker. *Wikipedia.* [Online] Wikipedia, 04 10, 202. [Cited: 04 13, 2020.] Stingray phone tracker.

8. **Lee, Timothy B.** The police are secretly using fake cellphone towers to spy on people. *Vox.* [Online] Vox, 04 22, 2015. [Cited: 04 13, 2020.] https://www.vox.com/2015/4/22/8463239/stingray-fbi-secret.

9. **Wikipedia.** GSM. *Wikipedia.* [Interactiv] 13 09 2019. [Citat: 09 04 2020.] https://ro.wikipedia.org/wiki/GSM.

1. Software Defined Radio – sistem de comunicare radio. Componente care în mod normal ar fi implementate hardware, precum amplificatoare, modulatoare sunt implementate pe partea de software. [↑](#footnote-ref-2)
2. International Mobile Subscriber Identity – cod alocat utilizatorului de către operatorii de telefonie, ce le permite să identifice abonatul in funcție de numărul de telefon. [↑](#footnote-ref-3)
3. Celulă – releu GSM ce deservește o mică suprafață, mai mult sau mai puțin rotundă si cu diametrul de aproximativ 8-10 kilometri. (9) [↑](#footnote-ref-4)