ANCOM

National Authority for Management and Regulation in Communications of Romania

VIITORUL COMUNICAȚIILOR. 5G ÎNTRE BENEFICII ȘI PROVOCĂRILE DE SECURITATE CYBER

Virgilius Stanciulescu
ANCOM
Directia IT si Protectia Datelor

- Abordarea zilelor și mai exact obișnuințele zilnice se vor schimba substanțial odată cu dezvoltarea tehnologiei, care va conecta tot ceea ce ne înconjoară.
- **Cu ajutorul rețelelor 5G**
  - conexiunile vor fi mai rapide
  - lucrurile care joacă un rol în confortul de zi cu zi vor fi conectate
  - beneficii încă puțin înțelese sau cunoscute de către fiecare dintre noi.

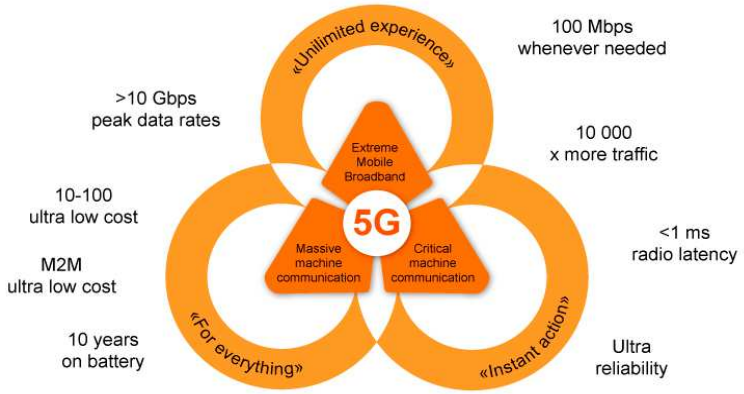
- Pentru operatorii de rețele de telecomunicații:
  - rețeaua de fibră optică
  - integrarea fix – mobil

  ⬇

  - conlucrează pentru a deschide calea către 5G și mai departe respectiv pentru a ține pasul cu:
    - vitezele necesare pentru transportul
    - unor cantități uriașe de date
    - cu întârziere minimală (de ordinul milisecundelor)
    - cu un număr masiv de elemente conectate.

5G: caracteristici tehnice

- Volumul de date transmis: de 1.000 de ori mai mare, decât în prezent
- Numărul de dispozitive ce vor putea fi conectate: de sute de ori mai multe.
- Viteza de procesare a datelor: 10Gbps, iar specialiștii estimează că se vor atinge viteze și mai mari.
- Latența redusă: timpul comanda – răspuns
  - în rețelele 4G este de aproximativ 50 de milisecunde,
  - în rețelele 5G de o milisecundă
- Consum redus de curent



5G: vulnerabilites

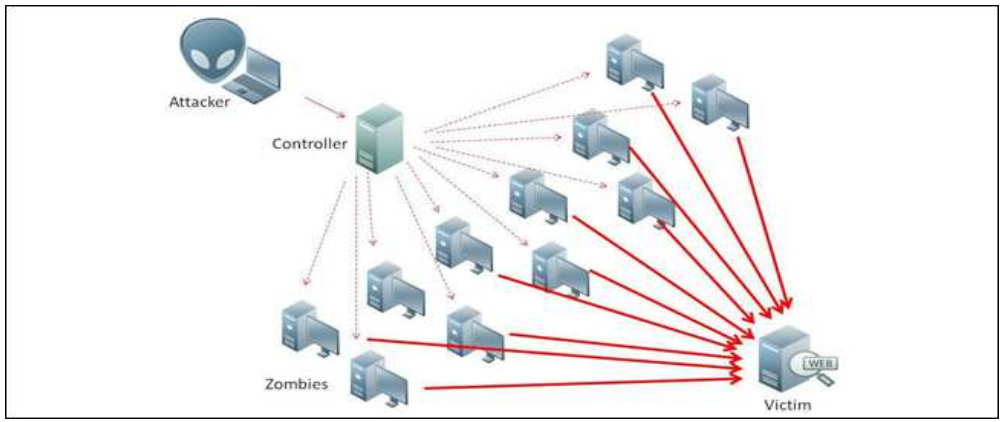
Speaking about vulnerabilities: at least 2 origins

- Application level, vulnerabilities associated to new applications and services
- Technical aspects, technologies, management modules, protocols

5G: vulnerabilities

- It can easily extrapolate the current known situation of DDoS attacks:
  - increasing the number of interconnected devices
  - will increase the critical mass of potential devices taken over in a Botnet network
  - to initiate stronger attacks
  - at a speed perhaps thousands times higher!

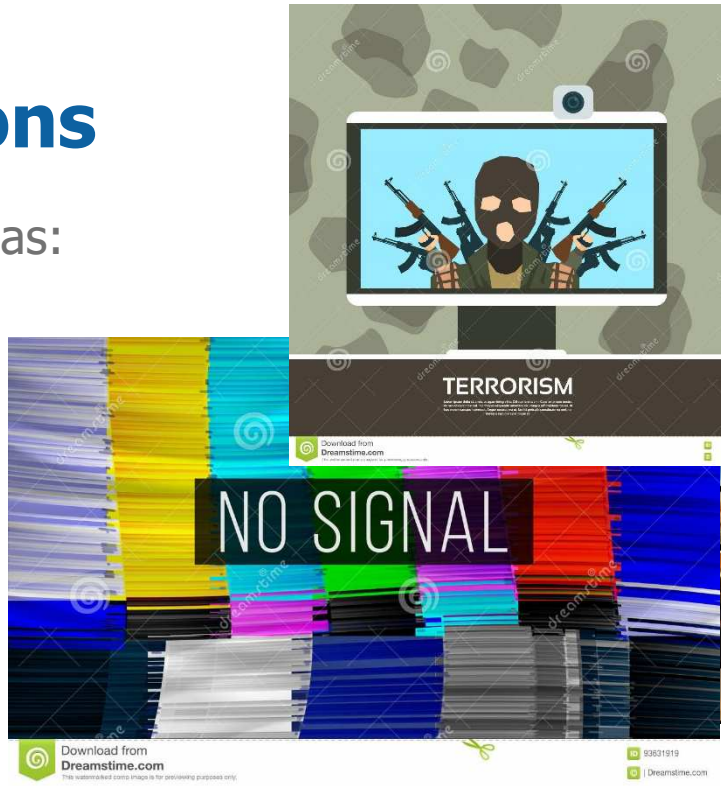
From a technological point of view, will need to have an adapted response capacity.



5G: applications

High-speed mobile internet even in crowded areas:

- concerts, festivals, sports events
- without being affected by
- speed limitations, interference,
- or signal instability.



- a download of 4K resolution movies
- will be a matter of seconds

- live TV shows and sports events will become real immersive, augmented or virtual visual experiences,

even for those who will not personally participate in real life,

- offering the possibility of virtual, sensory participation in real

5G: applications

In the testing period, an operator from Romania made an experiment with a rock concert with a hologram!

5G: Internet of Eyes

- Dynamic traffic monitoring, traffic management,
- public security (so-called Internet of Eyes concept)
- object detection and positioning in real-time,
- smart city, smart home, smart building,
- technology will be the backbone of IoT

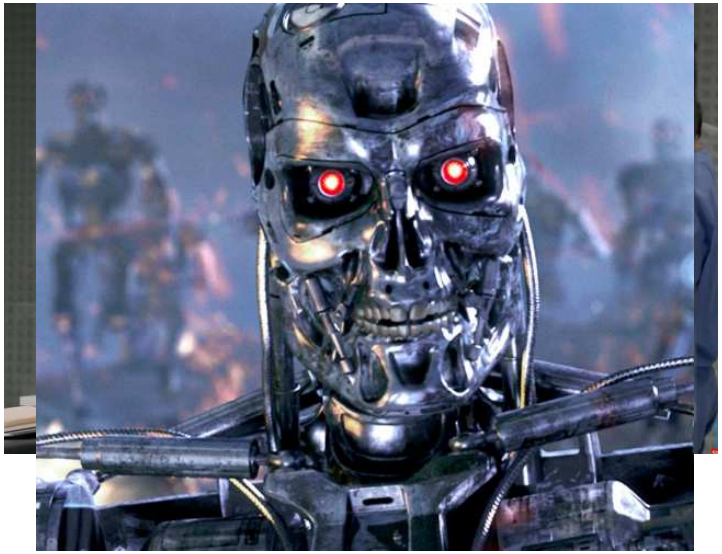
- independent vehicles will interact with traffic lights, infrastructure,
- communicate with each other, based on systems with AI or Augmented.
- sensors integrated into roads, railways and flight paths will communicate with each other and intelligent vehicles to improve infrastructure control and critical services.

5G: Internet of Eyes

VectorStock®
VectorStock.com/13699290

Internet of Skills vulnerabilities

- Robotics potential:
  distance controlled,
- Medical operations,
  - Combined with VR,
  - Tactile internet,
  - Real time touching sense at distance.
- Surgeons act at distance.
  - VR sets



- Agricultura:
  humidity sensors, etc

- Drone: control device

Immersive Gaming: intrusion

- AR for movies and games - visual virtual immersion experience 360 degrees

5G: vulnerabilities

- Information theft can reach immense levels:
- extortion of information and theft of personal data, traffic intercepts for password decryption or confidential information,
- in the case of the 4.0 industrial revolution that brings virtual prototyping and sending the online model directly on the manufacturing line,
- a man-in-the-middle attack could mean the theft of the model (intellectual property, industrial espionage) or worse, its distortion or replacement, the change of features before the physical execution begins.

- The results and negative effects can be non measured.

5G: vulnerabilități

Vorbind despre vulnerabilități și riscuri associate, identific cel puțin două origini ale acestora:

- una legată de nivelul aplicație, adică vulnerabilități asociate noilor tipuri de servicii și aplicații
- una legată de aspectele tehnice legate de tehnologii în sine, de module de management sau protocoale.

5G: vulnerabilități

- Deturnarea dronelor sau vehiculelor autonome
- Falsificarea sau furtul datelor personale
- Compromiterea operatiilor cu roboti la distanta
- Interceptarea datelor de la senzori

5G: vulnerabilități

- defectele de securitate ale rețelelor de internet 2G, 3G și 4G ar putea fi repetate și în cazul 5G.
- ENISA: studiu "Signalling Security in Telecom SS7/Diameter/5G"
- Protocoalele SS7 si Diameter: probleme de securitate
- atacurile SS7 pot fi complexe:
  - deoarece atacatorii câștigă tot mai multe cunoștințe și dezvolta scenarii de atac eficiente.
  - O protecție de bază va acoperi probabil majoritatea atacurilor, dar va lăsa loc pentru atacurile complexe sau orientate care pot provoca daune la nivel social, economic sau politic (de exemplu, spionaj etc.).
  - SS7: ENISA: majoritatea furnizorilor adoptă măsuri de securitate minime. Măsurile de securitate de bază oferă doar un nivel de bază de securitate. De asemenea, infrastructura SS7 este destul de veche în unele cazuri și nu toate echipamentele susțin adoptarea de măsuri de securitate, nici măcar cele de bază.
- Diameter: protocol de autentificare, autorizare
- Design: concepte împrumutate din SS7, împreună cu vulnerabilitățile sale.
- Protocol pur bazat pe IP: există un risc crescut de acces prin hacking.
- Acest lucru îl face teoretic, mai simplu de exploatat decât SS7

5G: vulnerabilități

- defectele de securitate ale rețelelor de internet 2G, 3G și 4G ar putea fi repetate și în cazul 5G.
- ENISA: studiu "Signalling Security in Telecom SS7/Diameter/5G"
- "The future use of this protocol or similar approached should be avoided"!
- "Carriers will need a new signalling architecture that can address the impact of introducing billions of roaming and static devices, the subscriber behaviour and bandwidth requirements, and new applications."
- "Nevertheless there is a certain risk of repeating history. Given the improvements that 5G will bring, having the same security risks can be extremely dangerous."

ENISA

5G: probleme

- SDN centralizeaza platforma de control al retelei si permite programabilitate si usurinta in administrare
- Conform studiilor: creeaza oportunitati pentru hacking-ul retelei, favorizand DDos, si expunerea API-urilor catre exterior.
- Controlerul SDN permite modificare software de rute si fluxuri, exista posibilitatea expunerii vizibile a acestuia, ce poate duce la Ddos sau la bottleneck.

Masuri:

- Arhitectura SDN permite monitorizare a securității reactiva si proactive
- Analiza de traffic si modificarea politicilor de securitate și introducerea serviciilor de securitate.
- Politicili de securitate consistente ale rețelei: pot fi implementate datorită vizibilității globale a rețelei,

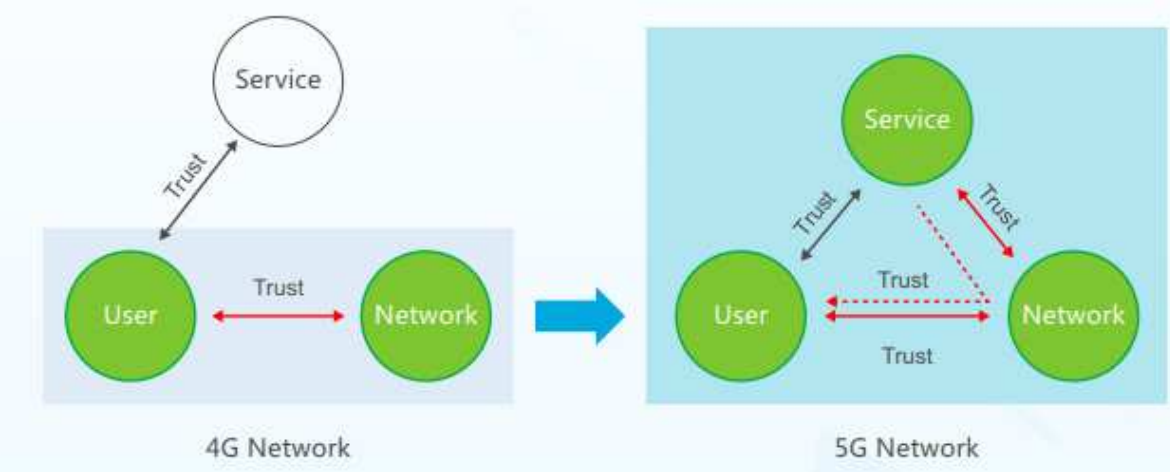
5G: probleme

- VNF (Virtual Network Functions): platformele curente au probleme cunoscute: nu ofera izolare si securitate serviciilor de comunicatii virtualizate

- Masuri:
- Securitate printr-un orchestrator de securitate în corespondență cu arhitectura care asigură securitatea nu numai a funcțiilor virtuale într-un mediu multi-tenant, ci și a entităților fizice ale unei rețele de telecomunicații.

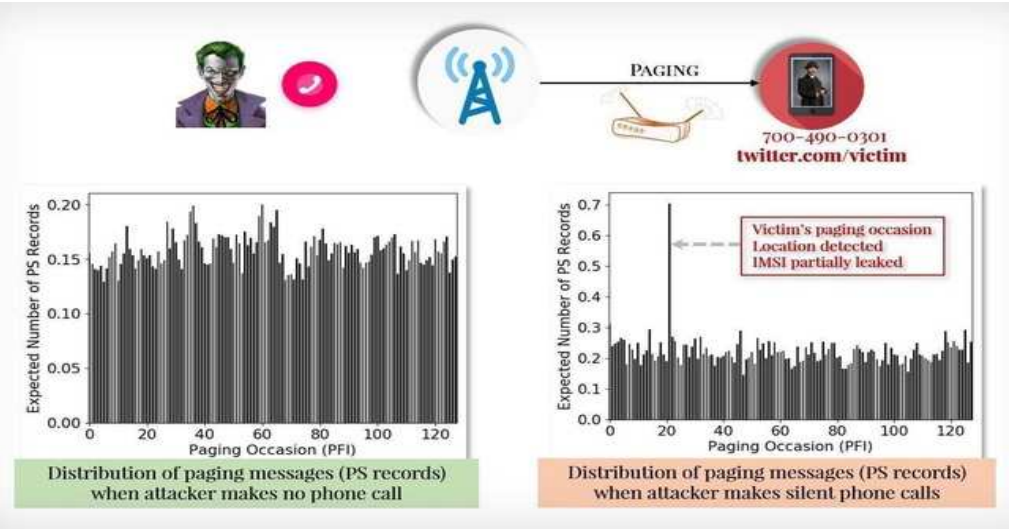
5G: probleme

- Trimiterea cheilor de criptare pt interfetele radio prin canale nesecurizate
- Se impun:
- Masuri de securitate sporita si data privacy pentru furnizorii de cloud
- cresterea relatiei de incredere,
- abordari de securitate frontend, back-end si network based.
- Izolarea si segmentarea retelelor in functie de serviciile oferite pentru a oferi protectie suplimentara
- Noi modele de trust si identity management care sa includa si furnizorul de servicii
- Securitate End 2 End



5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- 26 februarie 2019: Cercetatori ai Universitatilor Purdue si Iowa au dat publicitatii o lucrare in cadrul "Network and Distributed System Security" in care demonstreaza noi vulnerabilitati in retele 4G si 5G
- Atacul numit „Torpedo": apelează şi anulează apelul către ţintă de mai multe ori consecutiv, ducând astfel către o vulnerabilitate în sistemul de paginare al reţelei.
- Practic, iniţiatorul atacului poate trimite un mesaj către dispozitivul ţintei, fără ca acesta să înregistreze un apel. De aici, poate fi cu uşurinţă urmărit apelul şi pot fi trimise mesaje noi false, sau blocate alte mesaje care ar putea să vină.



5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- Atacul Torpedo deschide calea către alte două tipuri de atacuri.
- Piercer: poate fi folosit pentru a detecta identitatea dispozitivului prin dezvăluirea codului unic IMSI, atac valabil doar pe reţele 4G
- IMSI-Cracking, care poate să afle codul IMSI prin „brute force" atât pe reţele 4G, cât şi pe cele 5G, în ciuda faptului că acesta este criptat pe ambele tipuri de reţele.
- Reţelele 5G ar trebui să fie mult mai bine securizate decât cele 4G, dar acestea sunt în continuare vulnerabile la atacuri care funcţionau şi pe generaţia veche de antene telecom.
- Dispozitivele Stingray ar putea fi cu uşurinţă adaptate pentru atacuri pe reţele 5G, si se poate afla geolocaţia utilizatorilor de telefoane sau alte echipamente 5G. Dar ce ne facem cand nu sunt folosite doar de fortele de ordine? Un astfel de dispozitiv poate fi produs cu 200$

5G: noi vulnerabilitati
Atacurile Torpedo, Piercer, IMSI-Cracker

- GSMA, alianţa mondială care reprezintă operatorii de telefonie mobile a fost informata
- GSMA a recunoscut aceste probleme, însă nu este clar dacă vor fi sau nu rezolvate.
- Întrucât reţelele 5G încă nu sunt pornite, există şansa ca acestea să poată fi modificate înainte de lansarea oficială.
- Vulnerabilitatile au fost demonstrate si publicate, însă nu şi codul folosit pentru a demonstra vulnerabilităţile, Torpedo, Piercer şi IMSI-Cracking fiind mult prea periculoase în mâinile utilizatorilor.
- În timp ce IMSI-Cracking şi Torpedo pot fi rezolvate exclusiv de GSMA, vulnerabilitatea care duce la atacul Piercer poate fi „reparată” exclusiv de către operatori.

Va multumesc!