FORWARD DEFENSE

TACTERO

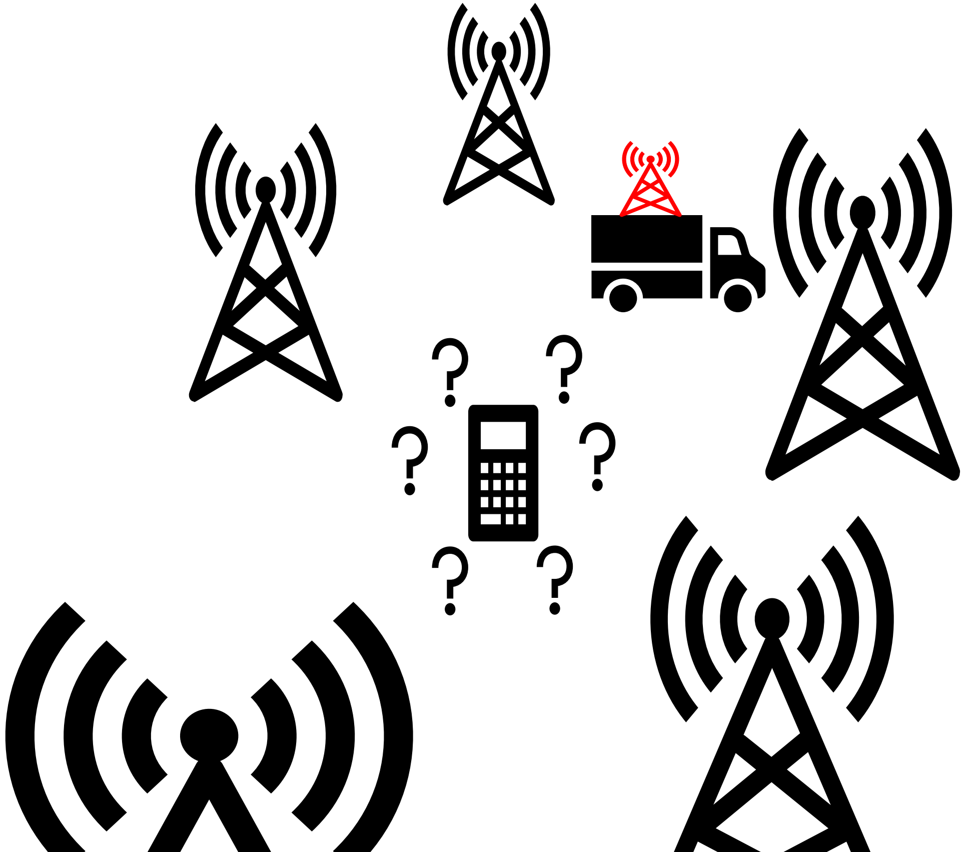
IMSI catchers’ detector

AGENDA

- The threat: IMSI catchers
- Objectives of IMSI catcher detection systems
- Overview of the Tactero approach
  - Special features of Tactero / strong points
- Future features
- Summary & conclusions

THE THREAT

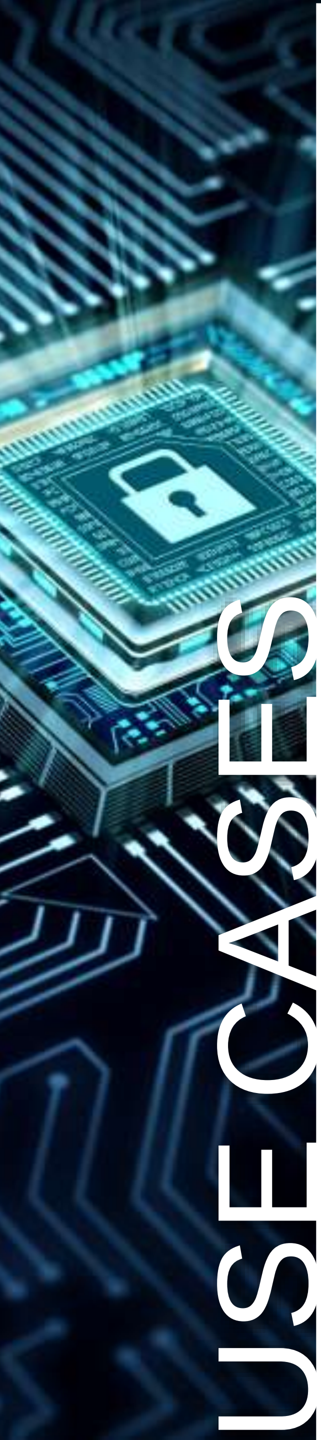
IMSI-catcher (dubbed a "*Cell-site simulator*", "*rogue mobile phone tower*", "*rogue cell*" or - after concrete models - "Stingray" or "Dirtbox") is a device used for intercepting mobile phone traffic and tracking location data of mobile phone users. Essentially IMSI-catcher is a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack.



Examples of IMSI catchers uses (the 'good guys' use cases)

- (Police, government agencies)
  To **help in police (criminal) investigations** (locating/finding criminals, acquiring their communication). Such scenarios have been reported among others in Canada, Norway, USA:
  - Identifying unknown phones currently used by a known target
  - Locating devices that cannot be found by the wireless carriers
  - Selectively blocking devices or dialed numbers (in specific areas, such as bomb attack, hostages taken or prisons areas)
- (Police, special forces, government agencies)
  To **find the wanted persons (incl. terrorists)**, the use case applied in many countries with notable examples from USA.
- (Police, government agencies)
  To disturb communication of protesters and to spam protesters during mass protests. This probably happened during the anti-police protests in Chicago (USA) and during anti-government protests in Kiev (Ukraine).
- (Law enforcement, prison officials)
  To **prevent the contraband cell phone use in prisons**. This requirement would require an appropriate cell phone management which can be done with IC (USA).

FORWARD DEFENSE

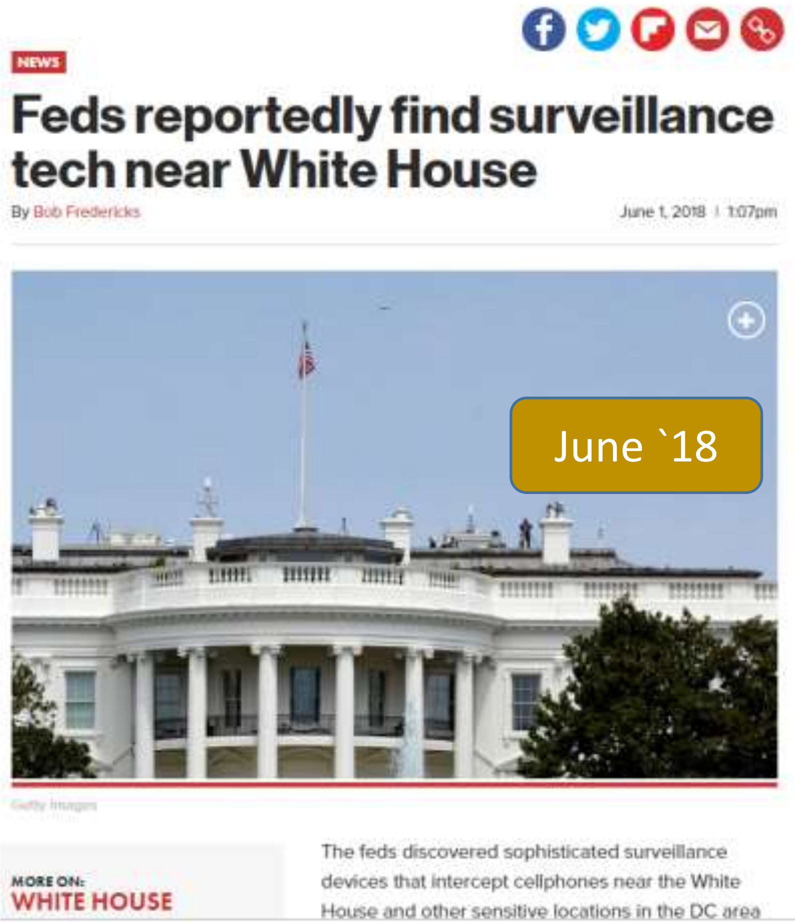


Examples of IMSI catchers uses (the ’bad guys’ use cases)

- (Criminal organizations/individuals) To **infect phones** of the end users with malware. In such scenarios, the fake base stations (ICs) are used to send specially prepared SMS messages, which look as if they were sent from legitimate mobile carriers. They contain a link to a malicious software. This can be, for instance an alternative SMS application, which will steal bank tokens etc. This happened to be a problem in China.
- (Cyberwarfare) To **send propaganda** messages in the war area (e.g., eastern Ukraine). The propaganda/hate messages are believed to be sent by means of ICs since they were sent to multiple phones within the same area.
- (Criminal organizations, foreign intelligence, industrial espionage) To **record confidential data** transferred by VIPs. Also, to identify are their phone numbers. Events of this type have been discovered both in Washington DC and in Canada.

Incidents - USA

FORWARD DEFENSE



NEWS

Feds reportedly find surveillance tech near White House

By Bob Fredericks June 1, 2018 | 1:07pm

Getty Images

MORE ON: WHITE HOUSE

The feds discovered sophisticated surveillance devices that intercept cellphones near the White House and other sensitive locations in the DC area

June `18

Mystery Stingray devices discovered Washington

4 April 2018

Undercover policing inquiry

April `18

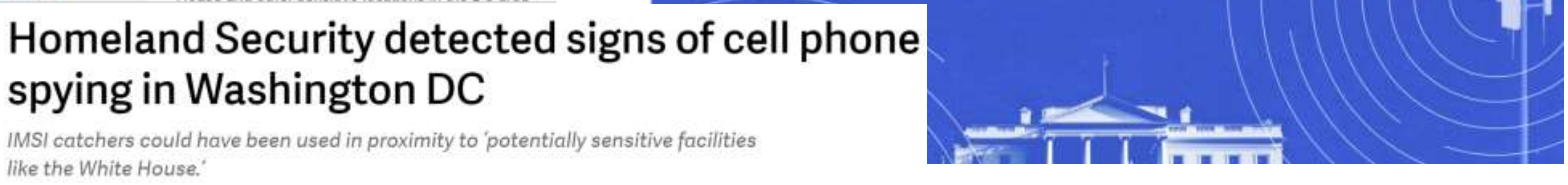
EXCLUSIVE

Israel accused of planting mysterious spy devices near the White House

The likely Israeli spying efforts were uncovered during the Trump presidency, several former top U.S. officials said.

By DANIEL LIPPMAN | 09/12/2019 05:14 AM EDT | Updated 09/12/2019 06:34 PM EDT

Sept `19

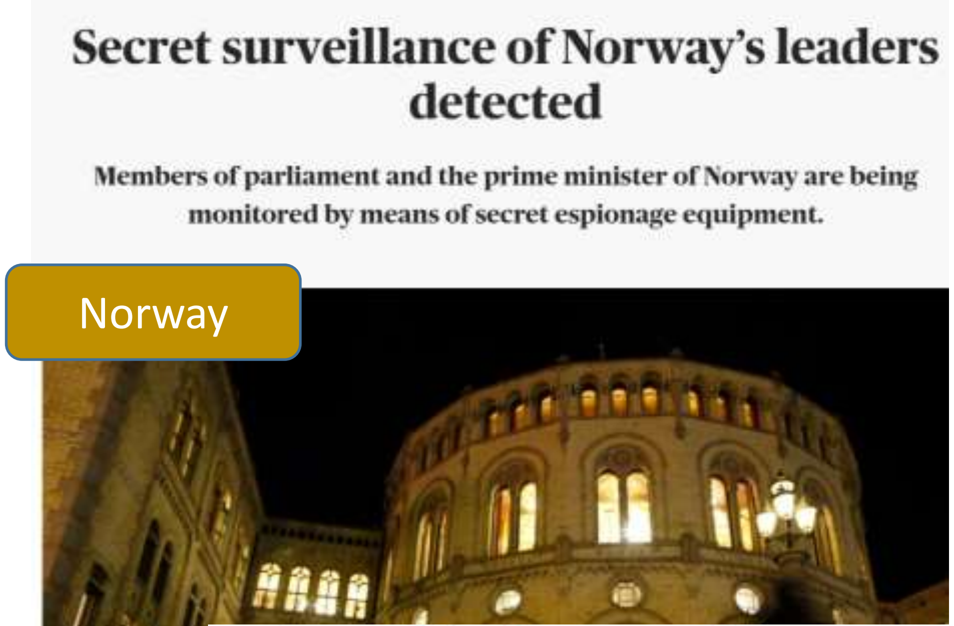


Homeland Security detected signs of cell phone spying in Washington DC

IMSI catchers could have been used in proximity to 'potentially sensitive facilities like the White House.'

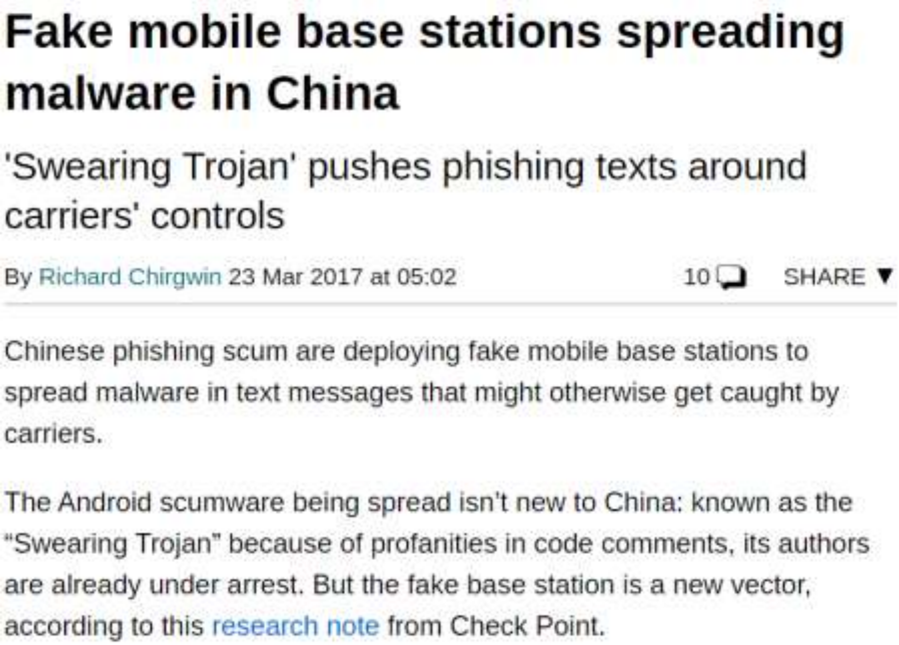
Incidents - world

Norway



Secret surveillance of Norway's leaders detected

Members of parliament and the prime minister of Norway are being monitored by means of secret espionage equipment.



Fake mobile base stations spreading malware in China

'Swearing Trojan' pushes phishing texts around carriers' controls

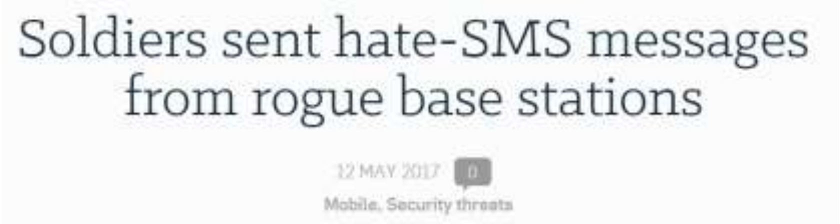
By Richard Chirgwin 23 Mar 2017 at 05:02 10 SHARE ▼

Chinese phishing scum are deploying fake mobile base stations to spread malware in text messages that might otherwise get caught by carriers.

The Android scumware being spread isn't new to China: known as the "Swearing Trojan" because of profanities in code comments, its authors are already under arrest. But the fake base station is a new vector, according to this research note from Check Point.

China

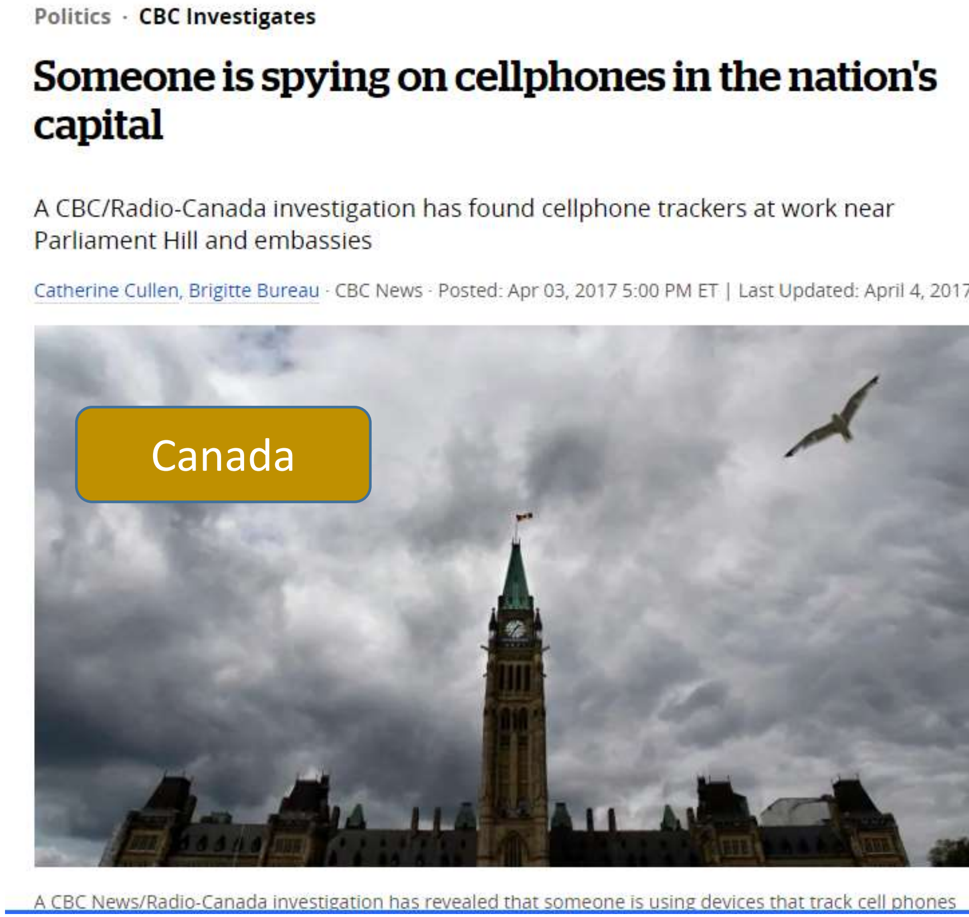
Ukraine



Soldiers sent hate-SMS messages from rogue base stations

12 MAY 2017 0

Mobile, Security threats



Politics · CBC Investigates

Someone is spying on cellphones in the nation's capital

A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies

Catherine Cullen, Brigitte Bureau · CBC News · Posted: Apr 03, 2017 5:00 PM ET | Last Updated: April 4, 2017

A CBC News/Radio-Canada investigation has revealed that someone is using devices that track cell phones

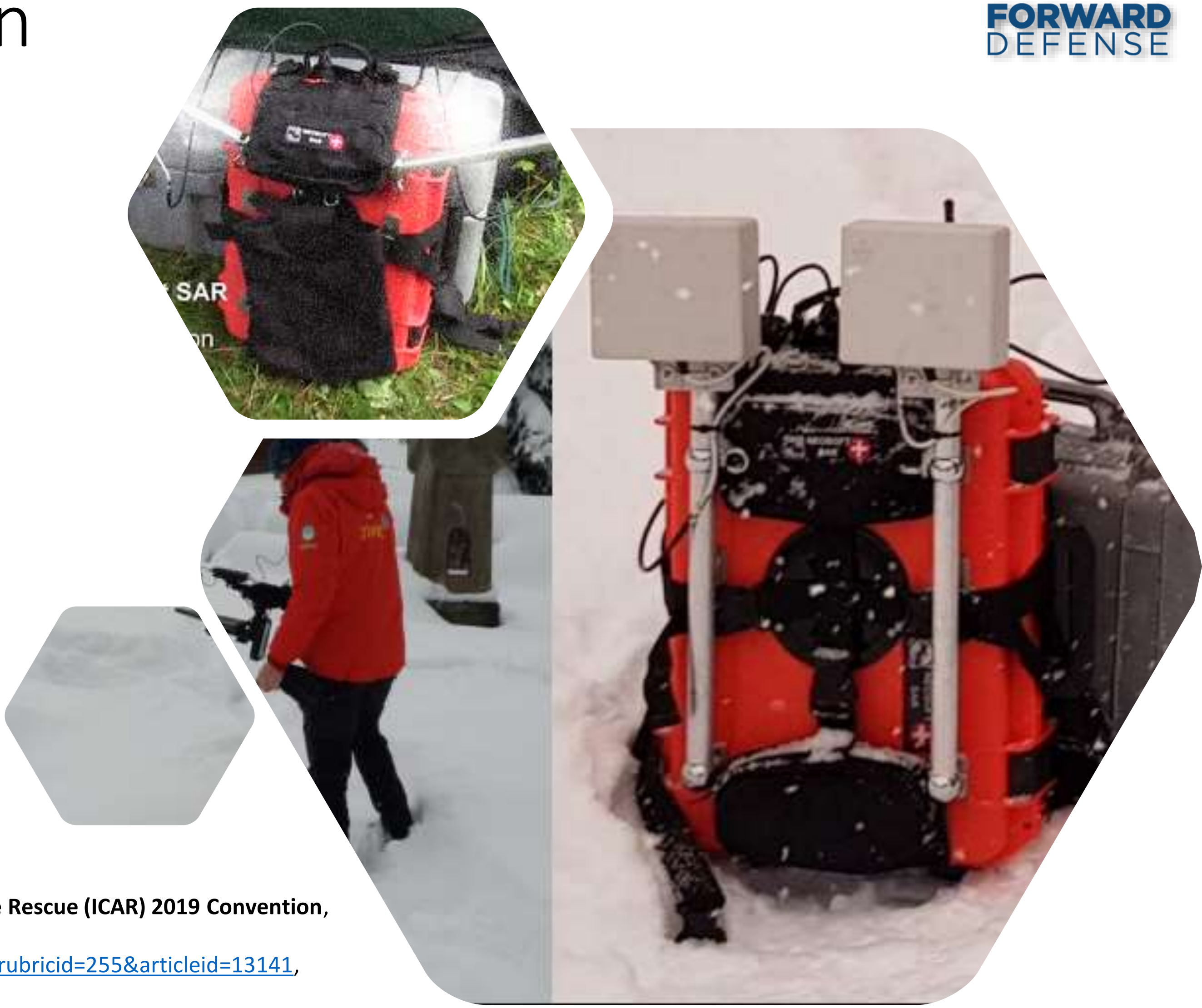
Canada

USE CASES

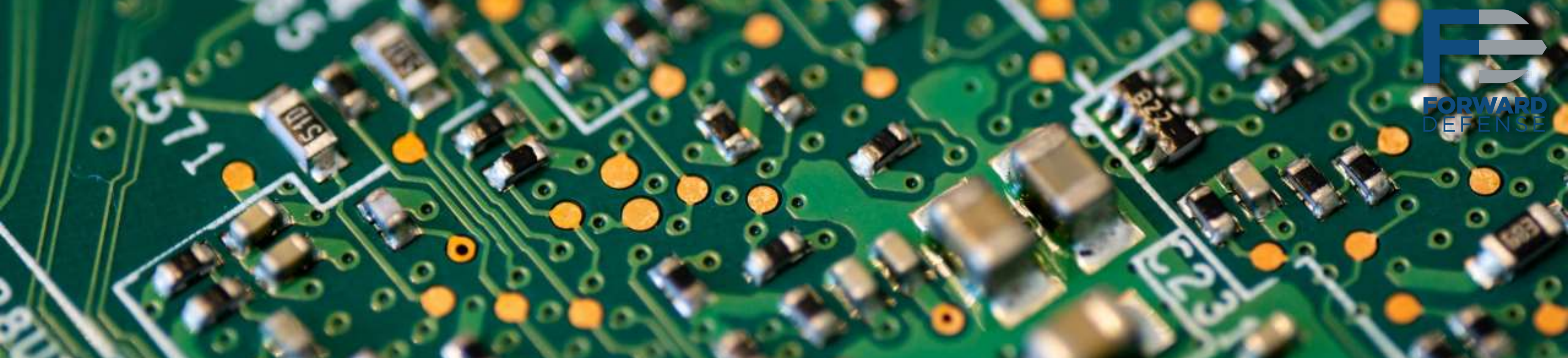
Non-standard application of IMSI catchers

(in fact, the ’very good guys’ use cases)

- In a search for:
  - a tourist lost in the mountains
  - an avalanche victim



* A system presented during the **International Commission for Alpine Rescue (ICAR) 2019 Convention**, **in Zakopane, Poland, Oct 2019,** http://www.alpine-rescue.org/xCMS5/WebObjects/nexus5.woa/wa/icar?menuid=1063&rubricid=255&articleid=13141, https://vimeo.com/showcase/6614072



FORWARD DEFENSE

TOWARDS AN IMSI CATCHER DETECTION SYSTEM

2021 Tactero

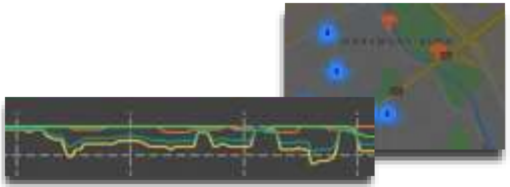
DETECTION SYSTEM -

- Detection of the presence of the threat in the current moment
  - If not sure – report an incident (about a ”suspicious anomaly”)

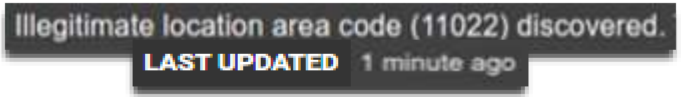
SECURE

DANGER

- Gathering information about the time and place of the activity
  - When it started, when it stopped, is it still active?
  - Where it is located?



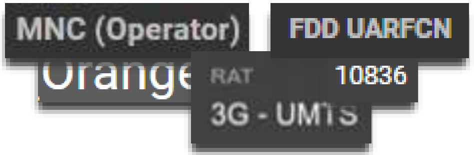
- Mode of operation
  - Does it behave according to a known pattern?
    - Does it change its settings during work?
    - Does it initiate some kinds of procedures?



Illegitimate location area code (11022) discovered.

LAST UPDATED 1 minute ago

- Who is potentially threatened?
  - What operator(s) are mimicked?
  - What RATs are used?

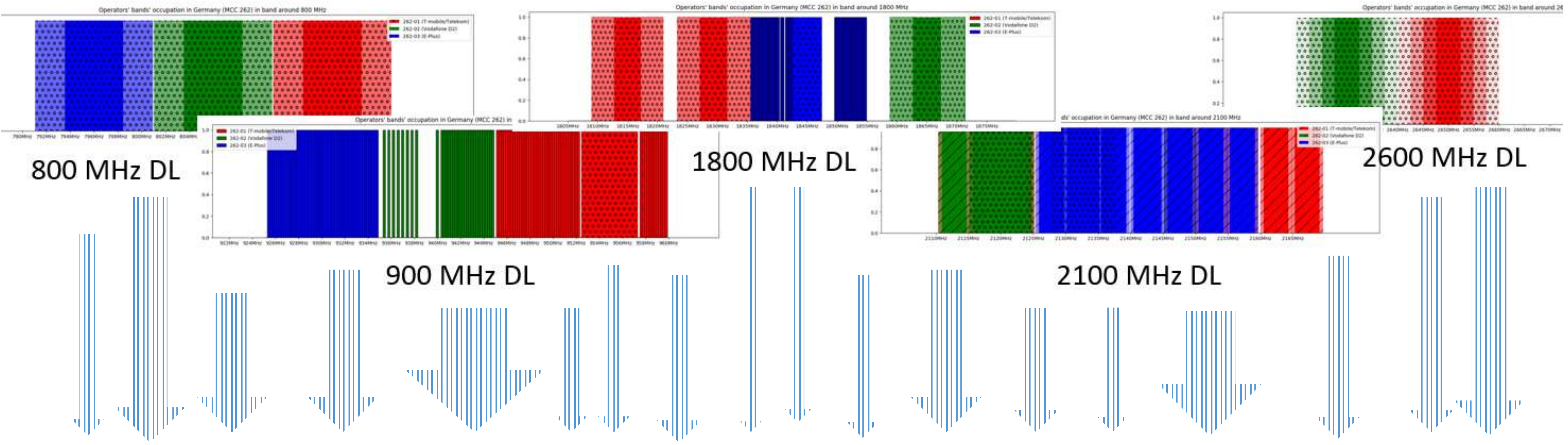


MNC (Operator) Orange

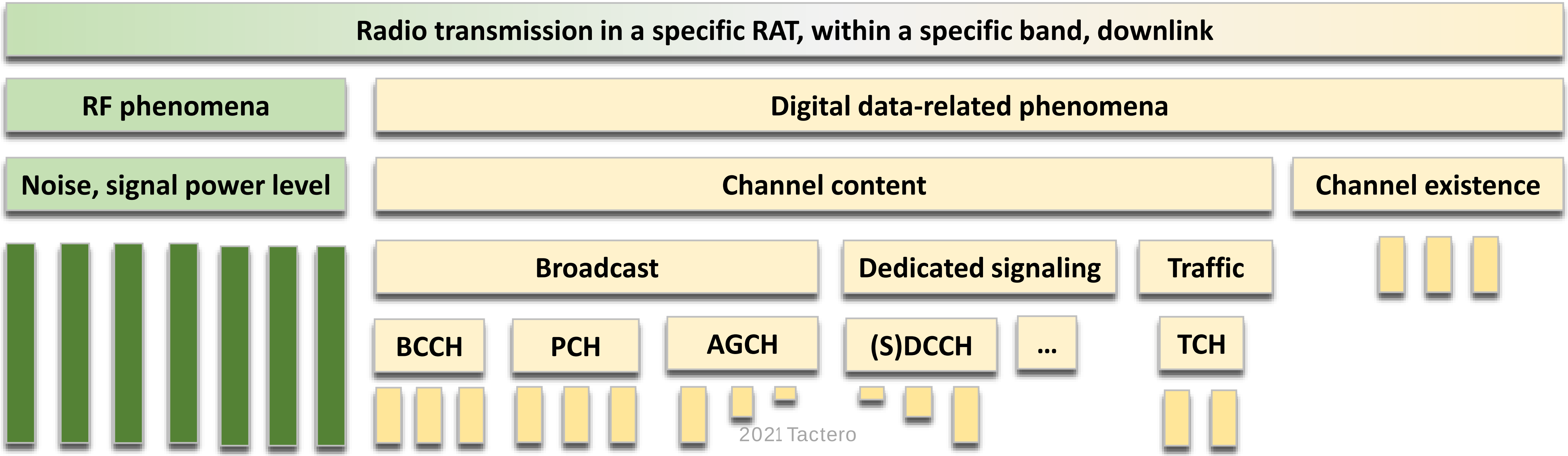
FDD UARFCN 10836

RAT 3G - UMTS

DETECTION SYSTEM – CHALLENG



DETECTION SYSTEM – CHALLENG



Radio transmission in a specific RAT, within a specific band, downlink

RF phenomena

Digital data-related phenomena

Noise, signal power level

Channel content

Channel existence

Broadcast

Dedicated signaling

Traffic

BCCH

PCH

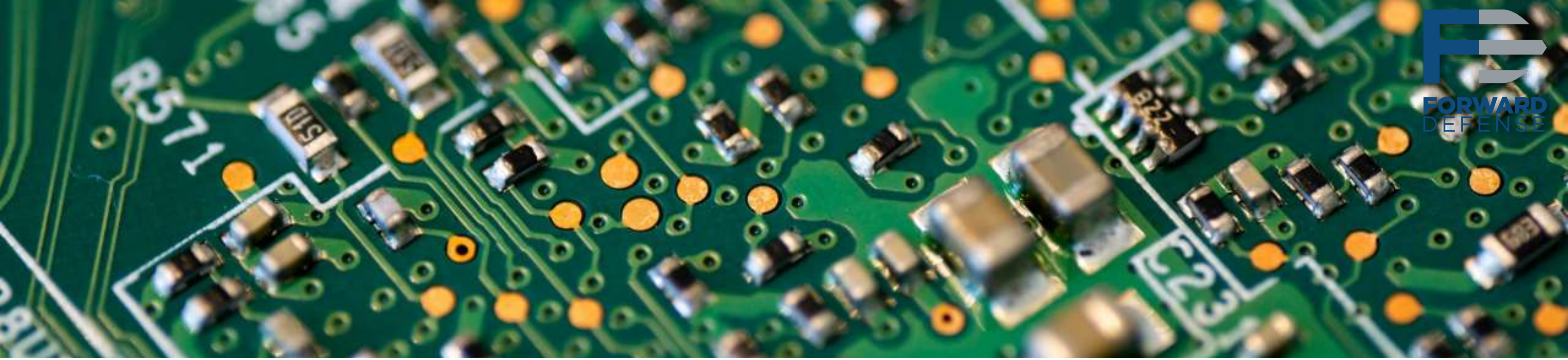
AGCH

(S)DCCH

...

TCH

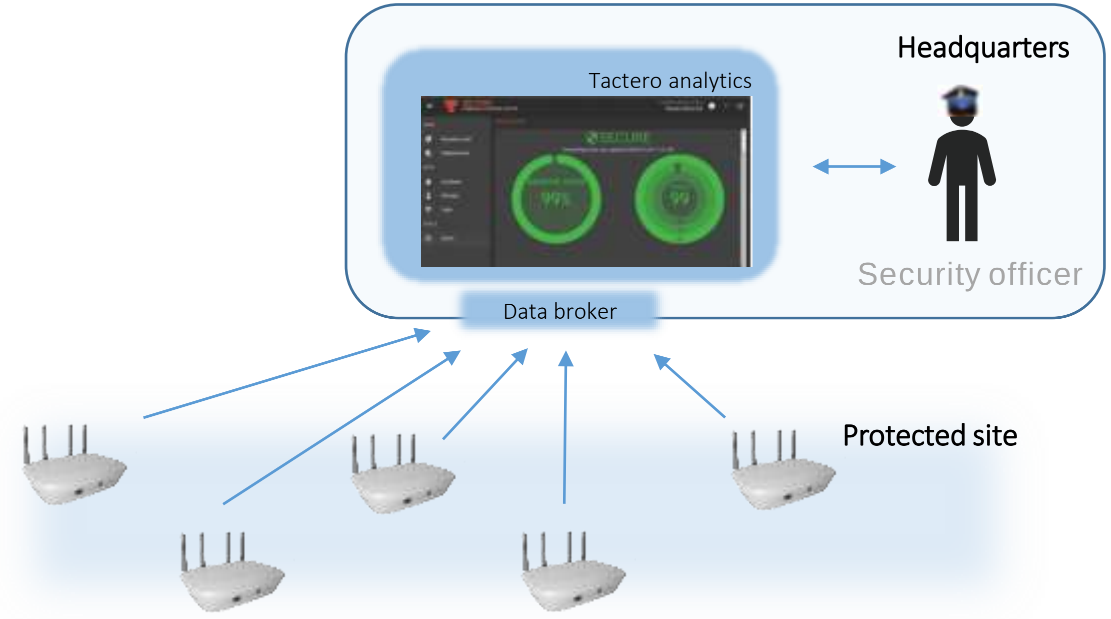
2021 Tactero



TACTERO

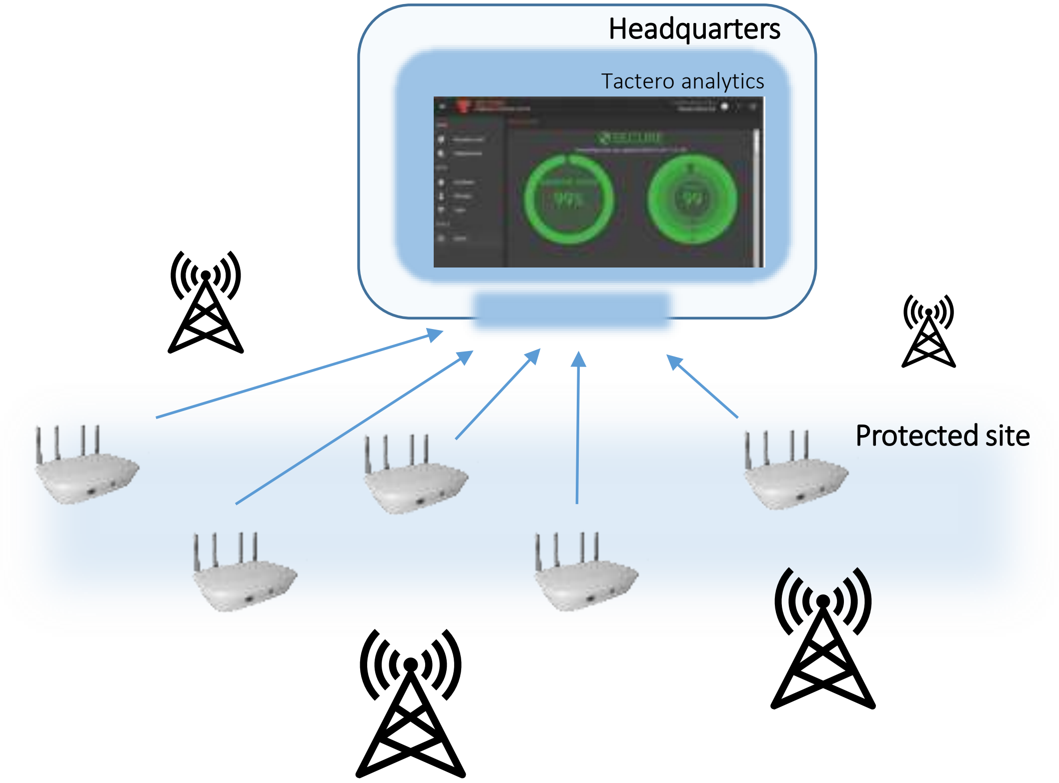
TACTERO – INTRODUCTION

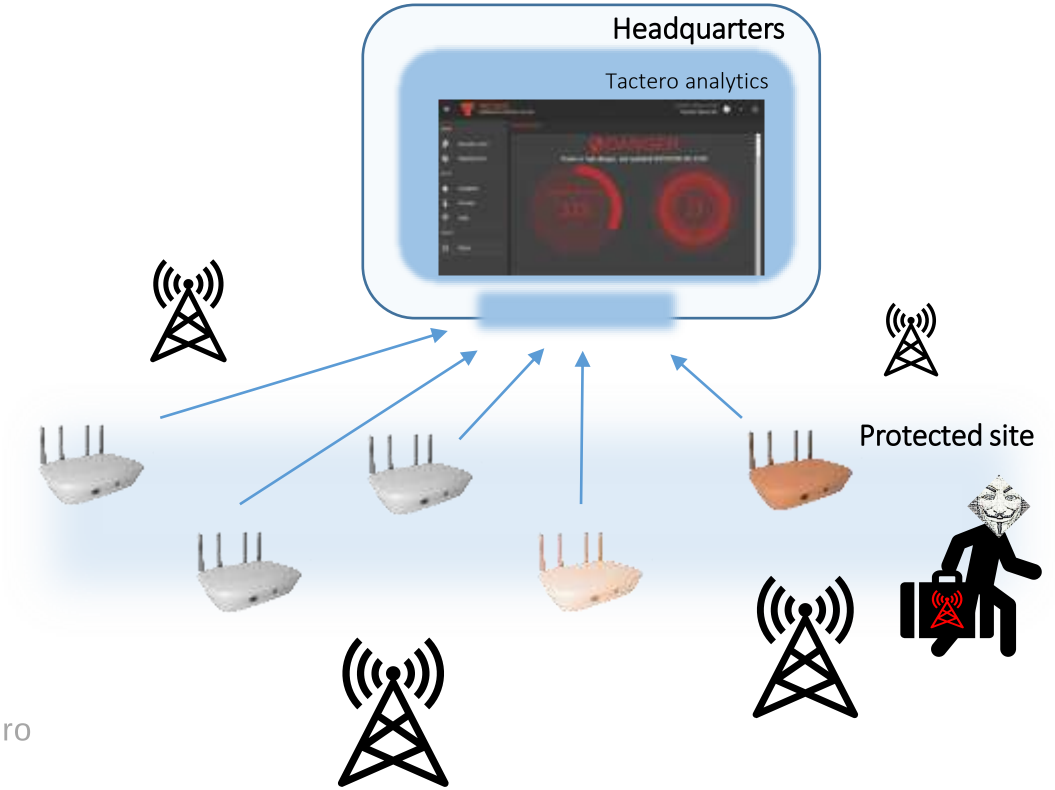
Tactero is a system which collects and analyzes radio signals in the cellular telephony bands in order to monitor mobile network security and to warn about potential threats such as like fake base stations (IMSI catchers), user tracking and over-the-air updates.



FORWARD DEFENSE

OPERATION





KEY FEATURES

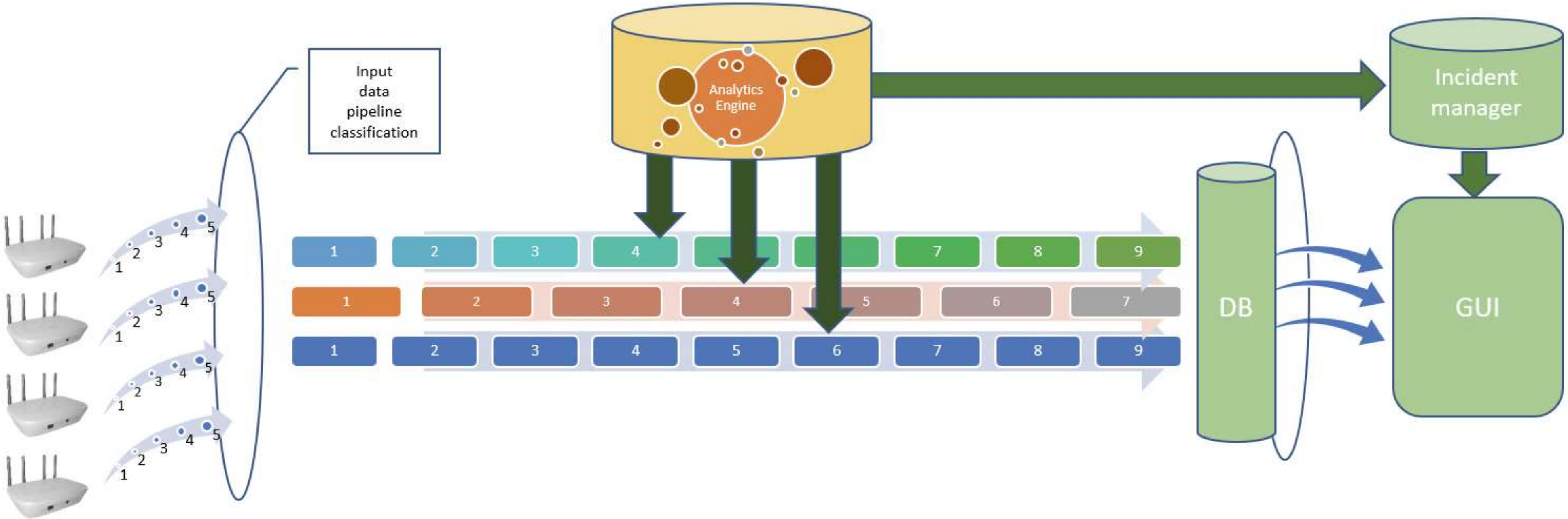
Core features:

- Multiple sources of real-time input data (collected by ’Tactero probes’)
- Knowledge of the environment and telco networks settings
- Central element to store and analyze data: analytics engine

Additional features:

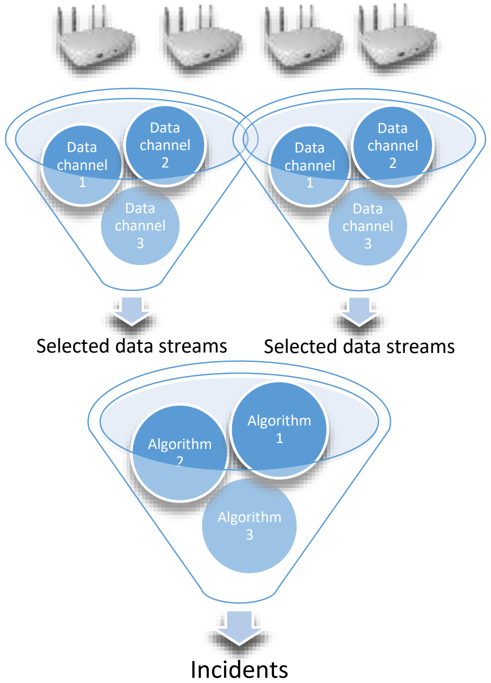
- Self-learning and self-adaptation
- Flexibility of configuration and features, incl. anomaly detection algorithms
- Heterogeneity of probes

TACTERO: ANALYTICS ENGINE

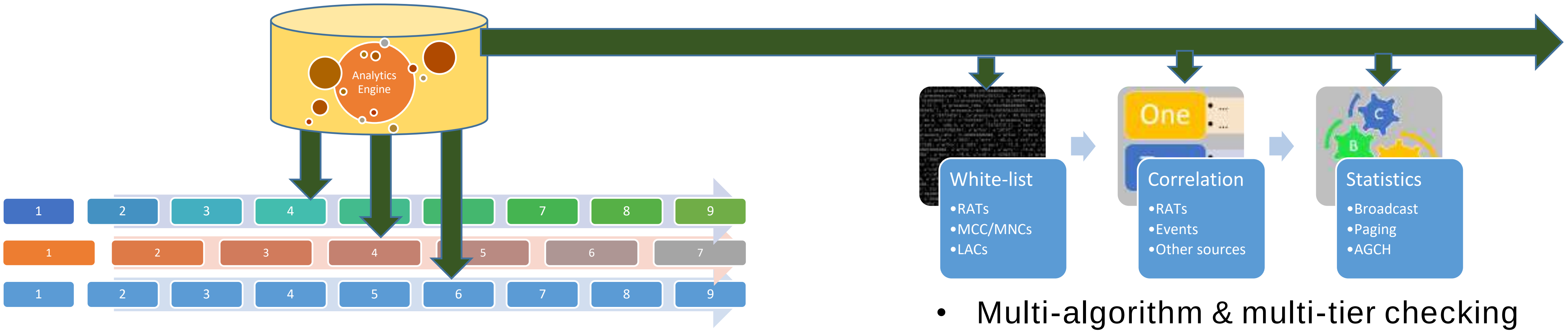


DATA ANALYSIS APPROACH [1]

- Radio environment is rich of heterogeneous data
- **It’s expensive to analyze everything**
- To solve it the filtering of data pipes is made
  - Decision of what to analyze is done on two layers:
    - Hardware layer – focus on most suspicious data channels so we need to select elements to analyze (probes can focus on specific radio RATs and channels)
    - Software layer – execution of selected algorithms are started upon lower the discovery of lower level anomalies



DATA ANALYSIS APPROACH [2]



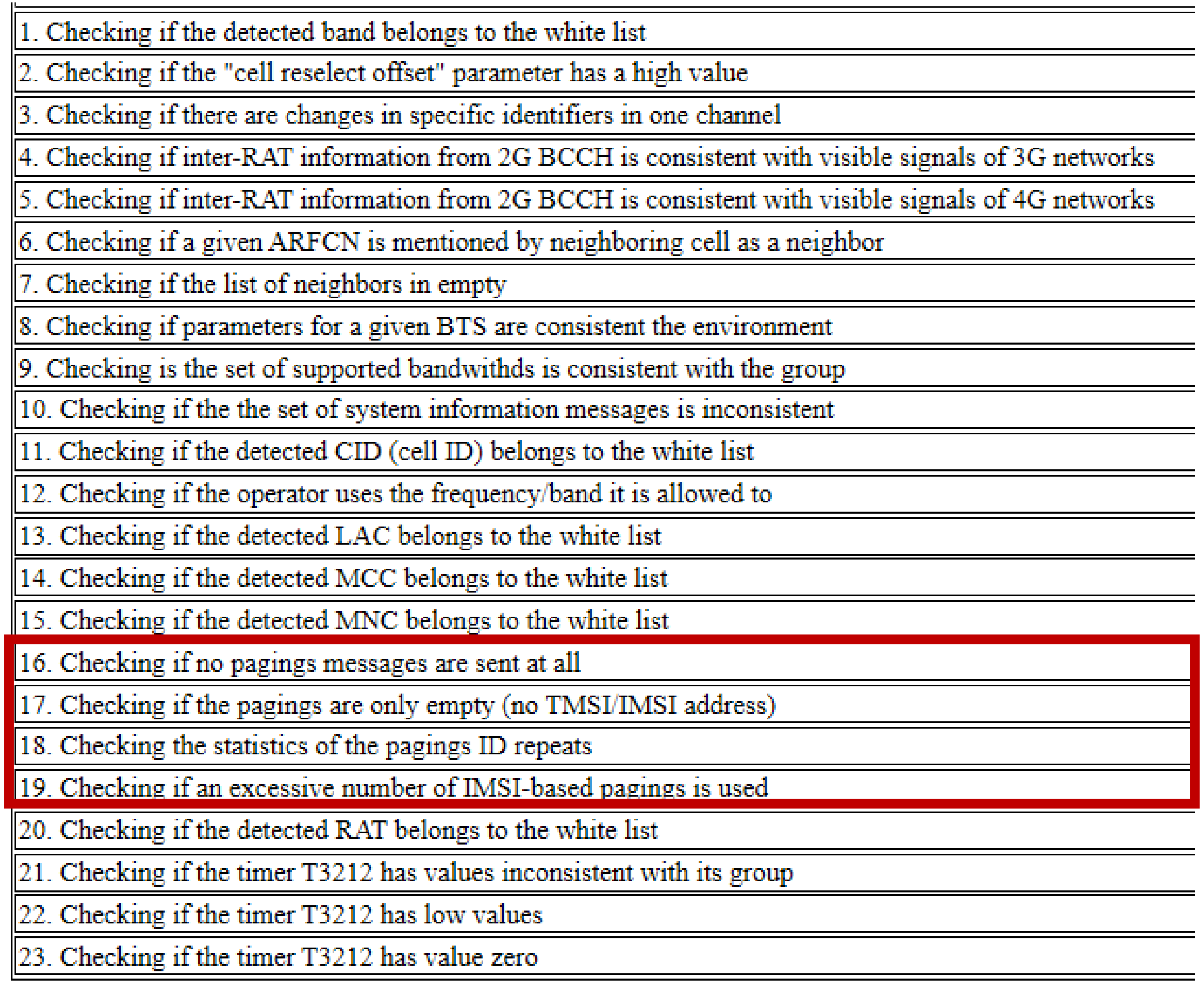
White-list
- RATs
- MCC/MNCs
- LACs

Correlation
- RATs
- Events
- Other sources

Statistics
- Broadcast
- Paging
- AGCH

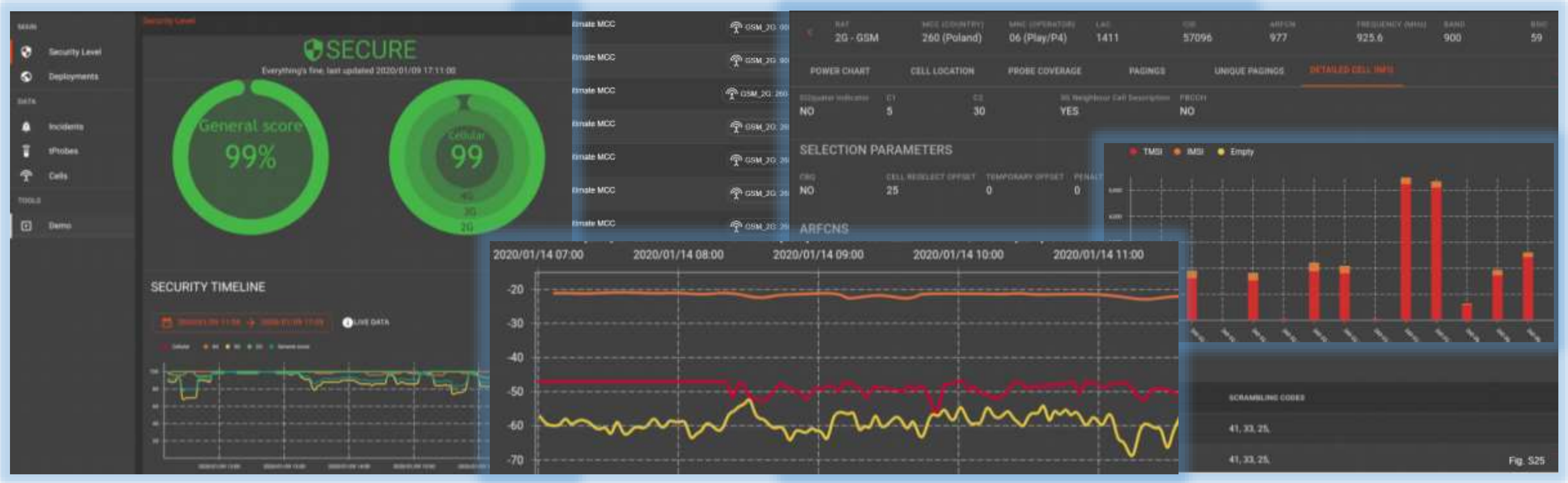
- Multi-algorithm & multi-tier checking
- Ability to turn on and off flexibly
- Expandability – new functions easily added

EXAMPLE CHECKS



1. Checking if the detected band belongs to the white list
2. Checking if the "cell reselect offset" parameter has a high value
3. Checking if there are changes in specific identifiers in one channel
4. Checking if inter-RAT information from 2G BCCH is consistent with visible signals of 3G networks
5. Checking if inter-RAT information from 2G BCCH is consistent with visible signals of 4G networks
6. Checking if a given ARFCN is mentioned by neighboring cell as a neighbor
7. Checking if the list of neighbors in empty
8. Checking if parameters for a given BTS are consistent the environment
9. Checking is the set of supported bandwithds is consistent with the group
10. Checking if the the set of system information messages is inconsistent
11. Checking if the detected CID (cell ID) belongs to the white list
12. Checking if the operator uses the frequency/band it is allowed to
13. Checking if the detected LAC belongs to the white list
14. Checking if the detected MCC belongs to the white list
15. Checking if the detected MNC belongs to the white list
16. Checking if no pagings messages are sent at all
17. Checking if the pagings are only empty (no TMSI/IMSI address)
18. Checking the statistics of the pagings ID repeats
19. Checking if an excessive number of IMSI-based pagings is used
20. Checking if the detected RAT belongs to the white list
21. Checking if the timer T3212 has values inconsistent with its group
22. Checking if the timer T3212 has low values
23. Checking if the timer T3212 has value zero

USER INTERFACE



Everything's fine, last updated 2020/01/09 17:11:00

RAT	MCC (COUNTRY)	MNC (OPERATOR)	LAC	CID	ARFCN	FREQUENCY (MHz)	BAND	BSIC
2G - GSM	260 (Poland)	06 (Play/P4)	1411	57096	977	925.6	900	59

NO · 5 · 30 · YES · NO

SELECTION PARAMETERS

CBQ	CELL RESELECT OFFSET	TEMPORARY OFFSET	PENALT
NO	25	0	0

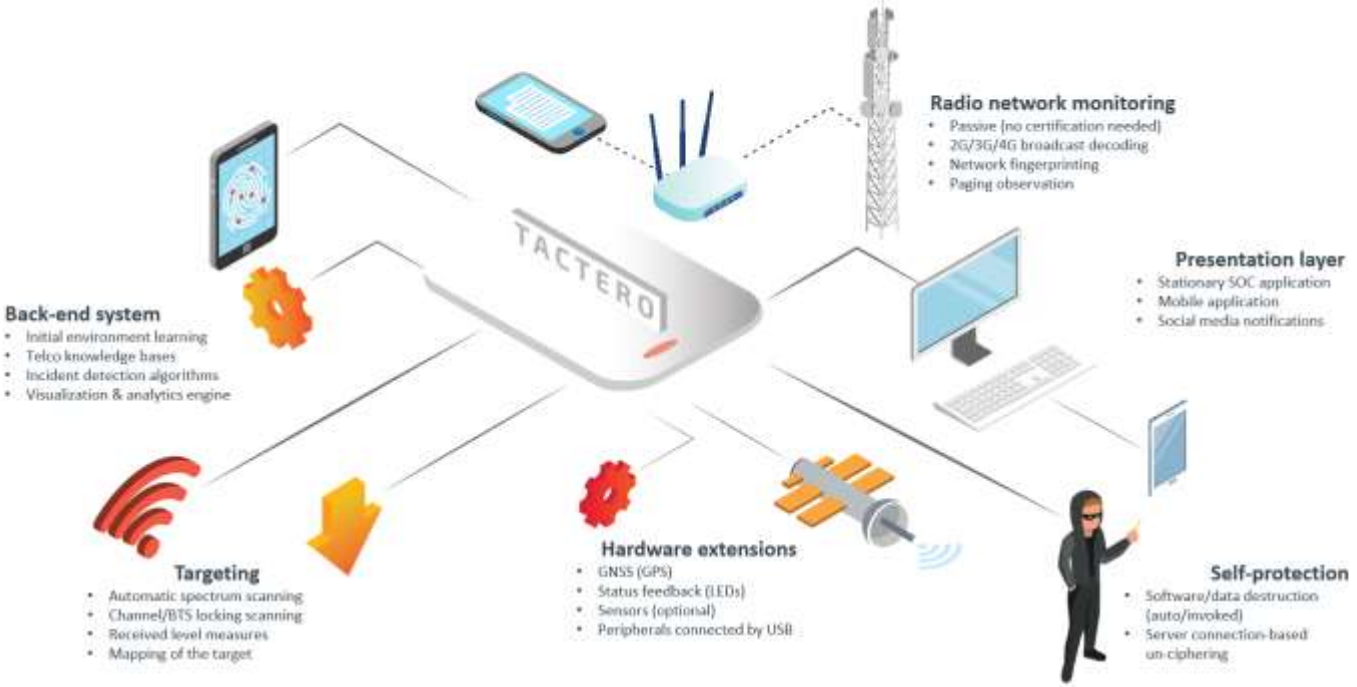
ARFCNS

41, 33, 25,

41, 33, 25,

2021 Tactero

SUMMARY & DEVELOPMENT



Radio network monitoring
- Passive (no certification needed)
- 2G/3G/4G broadcast decoding
- Network fingerprinting
- Paging observation

Presentation layer
- Stationary SOC application
- Mobile application
- Social media notifications

Back-end system
- Initial environment learning
- Telco knowledge bases
- Incident detection algorithms
- Visualization & analytics engine

Targeting
- Automatic spectrum scanning
- Channel/BTS locking scanning
- Received level measures
- Mapping of the target

Hardware extensions
- GNSS (GPS)
- Status feedback (LEDs)
- Sensors (optional)
- Peripherals connected by USB

Self-protection
- Software/data destruction (auto/invoked)
- Server connection-based un-ciphering

Future developments:

- Future wireless cellular technologies support
- More advanced self-learning and autonomy
- GUI with more detail explained
- More use cases

FORWARD
DEFENSE

Contact:
David Michaux
dmichaux@forwarddefense.com
+971 50 455 4031