Case Study

SMS Blaster Detection in the Field

Lessons from the Yettel Serbia incident

Convergent Fraud Analytics · SMS Blaster Detection and Protection

heksagon

Learn more at heksagon.com

In late 2025, Serbian law enforcement arrested two Chinese nationals operating an improvised IMSI catcher from a moving vehicle in Belgrade. The device impersonated legitimate base stations, forced nearby devices onto unsecured 2G, and delivered smishing messages to harvest payment card data without any traffic passing through the operator network. Below, we analyze how Yettel Serbia detected it and suggest strategies for MNOs in a similar situation.

The Incident at a Glance

- **Location:** Belgrade, Serbia
- **Attack window:** Q4 2025
- **Method:** Rogue base station in a moving vehicle
- **Payload:** Smishing for payment card data
- **Resolution:** Two suspects arrested
- **Investigated by:** Police High-Tech Crime Unit

Suspects arrested for stealing citizens' data via fraudulent SMS; improvised equipment found in the vehicle

Photo: Ministry of Internal Affairs Serbia
Source: Nova.rs, Dec 10, 2025

How SMS Blasters Work and Why They Evade Traditional Defenses

1 Lure

Simulate a legitimate 4G cell to attract nearby devices.

2 Downgrade

Use RRC redirection to force connections to unsecured 2G.

3 Inject

Push SMS directly. No SMSC, billing record, or firewall event.

4 Release

Hand devices back to the real network and move on.

15s to 5 min

Window to capture, target, and release a device, fast enough to look like normal cell reselection (100K+ SMS/hour blaster capacity).

Invisible

Zero records in CDRs, billing, or SMS logs. The attack never touches the network.

Global Threat

SMS Blasters reported in 20+ countries across the EU, APAC, MEA, and Canada. Many telcos are still unaware of the attack vector.

How the Attack Was Detected

Invisible to conventional controls

SMS firewalls and CDR-based rules see nothing, because the attack never touches the network. It surfaces only one layer deeper, in radio network signaling.

Two sources, working together, surfaced the campaign:

Radio network signaling

Invalid location area codes and a spike in handover signaling as captured devices rejoin the network expose the rogue cell.

Subscriber complaints

Reports of unsolicited messages gave the trigger; paired with signaling anomalies, they anchor the analysis.

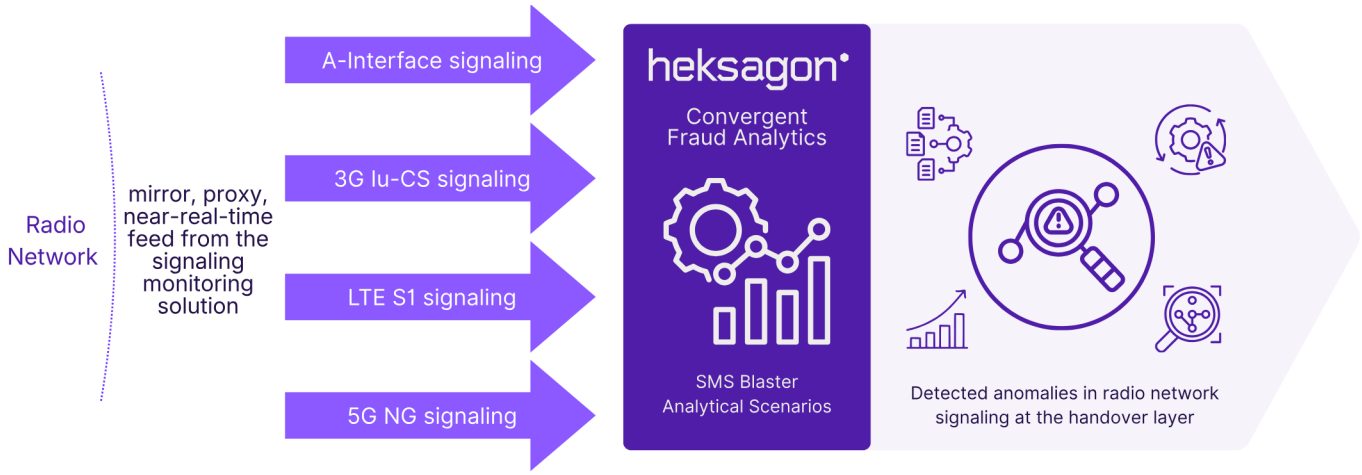
How MNOs Can Handle This Scenario

The incident exposed a readiness gap. Detection was reactive and manual, with no pre-configured scenarios, and it depended on Fraud, Information Security, Core Network, and RAN teams coordinating in real time. To close that gap, you need to:

- **Automate detection**
- **Pre-configure scenarios tied to SMS Blaster fraud**
- **Establish cross-team paths**
- **Instrument the right data**
- **Connect detection to positioning**
- **Build the full response chain**

How Heksagon Helps

Heksagon's **SMS Blaster Detection and Protection**, a module within the Convergent Fraud Analytics platform, detects SMS Blaster activity by analyzing the signals that rogue base stations do leave behind: anomalies in radio network signaling at the handover layer.



Heksagon Capability	Effect
Radio signaling analysis	Continuous monitoring of A-Interface, Iu-CS, LTE S1, and NG, with automated detection of handover anomalies and invalid parameters.
Multi-stream AI / ML correlation	Cross-stream processing raises detection confidence and cuts false positives below what any single signal can reach.
Subscriber impact response	Affected subscribers are identified, warned before they act, and optionally data restricted, closing the window between attack and harm.
E-CID location estimation	RSRP and RSRQ positioning from the E-SMLC module gives law enforcement actionable location data.
Case management	Signaling history, subscriber impact lists, and geographic data packaged for analyst review and LEA reporting.

Your network will be targeted sooner or later.
Stay ahead of emerging fraud schemes with Heksagon.

Presented the topic at GSMA FASG #34 · GSMA SMS Blaster briefing paper contributor · 600M+ subscribers protected daily
15+ years of market leadership · 0.01% false positive rate · 99.99% network uptime · ISO 9001 & ISO 27001 certified

info@heksagon.com www.heksagon.com

heksagon