HACKING

THE NARCO BACKBONE

📚 Table of Contents

HACKING
THE NARCO BACKBONE

Alperen L. Ugurlu

Introduction

Drug cartels and other organized crime groups have developed their own private communication infrastructures to prevent law enforcement agencies from intercepting their communications and to maintain operational secrecy. These infrastructures encompass **a wide range of technologies, including privately deployed base stations, fake radio towers, satellite phones, internet-based encrypted communication networks, and advanced encrypted radio systems**.

This report examines the technical aspects of these systems, the security strategies employed within them, the methods used by law enforcement to detect and dismantle such **infrastructures, and potential penetration testing scenarios targeting these networks. Furthermore, it evaluates the vulnerabilities, threats, and lessons learned that these specialized communication systems present** for cybersecurity professionals.

Alperen L. Ugurlu

1.Technical Infrastructure

1.1 Private Base Stations and Cellular Networks

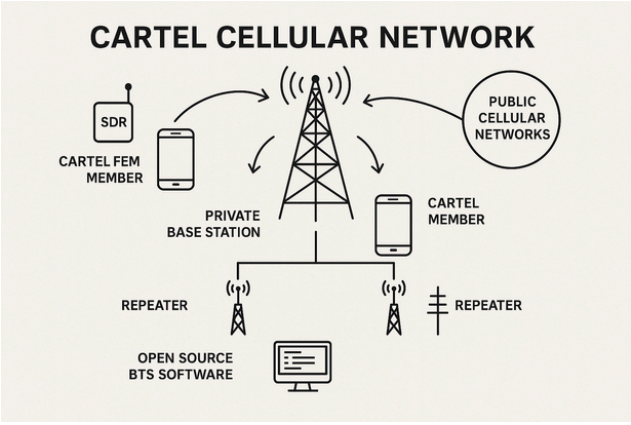
Cartels have deployed private base transceiver stations (BTS) and repeaters to establish their own cellular communication networks, independent of traditional telecommunications infrastructure. For instance, in Mexico, cartels such as Los Zetas built clandestine phone networks consisting of hundreds of antennas and transmitters. A network uncovered in 2011 spanned over 500 miles along the Texas border and extended another 500 miles into Mexico; the operation led to the seizure of 167 antennas and 150 repeaters.

These private mobile networks enabled cartel members in the region to communicate via mobile phone–like systems exclusively within the cartel's domain. In recent years, the decreasing cost of software-defined radio (SDR) technology has allowed cartels to build their own GSM networks using open-source BTS software such as OpenBTS.

For example, in 2021, during the dismantling of a cartel-operated network in the Tamaulipas region, authorities discovered an Ettus USRP-based SDR device running OpenBTS. These private base stations effectively decouple cartel communications from public telecom networks, minimizing the risk of interception and complicating metadata tracking by law enforcement.

Building and maintaining these systems has required a considerable level of engineering expertise. To meet this need, some cartels have reportedly kidnapped telecommunications technicians and forced them to work on these systems.

In conclusion, the ability to construct and operate their own cellular networks has provided cartels with a geographically widespread, relatively secure, and private communication environment.



Alperen L. Ugurlu

1.2 Use of IMSI Catchers (Fake Base Stations)

IMSI catchers, also known as fake base stations, are typically used by law enforcement as tools for mobile phone interception and tracking. However, criminal organizations have also begun repurposing this technology for their own operational needs. These devices trick nearby mobile phones into connecting to them instead of legitimate cellular networks.

Organized crime groups may use IMSI catchers for two primary purposes:

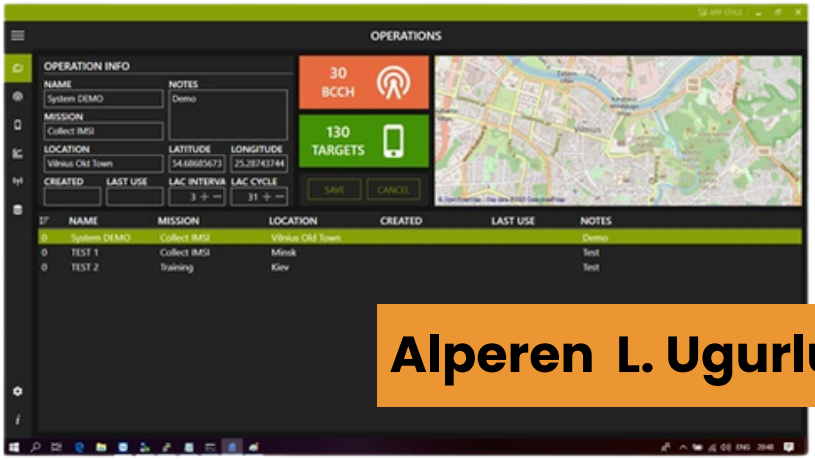
1. Offensively – to intercept third-party communications or send spoofed messages;
2. Defensively – to ensure their own communications remain secure and confined within a private environment.

For instance, in 2024, a fraud network in the UK constructed a homemade fake base station to send phishing SMS messages to thousands of people. This setup bypassed mobile carriers' suspicious message filters and was recorded as the first incident of its kind in the UK.

This case demonstrated that even consumer-grade radio equipment could be used to build functioning IMSI catchers. Similar incidents have been observed across East Asia and Europe, where portable IMSI catchers hidden in backpacks were used to push fake messages to nearby phones. One notable case in Paris in 2022 involved the discovery of a mobile IMSI catcher installed inside a repurposed ambulance.

Cartels may also use IMSI catchers for defensive purposes. If members do not want their phones to connect to public cellular networks, they can deliberately deploy a fake base station and configure it to accept only SIM cards issued internally by the cartel. This allows the group to create a closed, local GSM micro-network, ensuring all communications stay within a controlled environment — adding an extra layer of protection against external surveillance.

Moreover, cartels might monitor their cellular environment to detect anomalies that suggest a foreign IMSI catcher (e.g., one deployed by law enforcement) has been introduced into their territory. In such cases, anomaly detection tools could alert them to the presence of unauthorized surveillance equipment.



Alperen L. Ugurlu

1.2 Use of IMSI Catchers (Fake Base Stations)

IMSI catchers, also known as fake base stations, are typically used by law enforcement as tools for mobile phone interception and tracking. However, criminal organizations have also begun repurposing this technology for their own operational needs. These devices trick nearby mobile phones into connecting to them instead of legitimate cellular networks.

Organized crime groups may use IMSI catchers for two primary purposes:

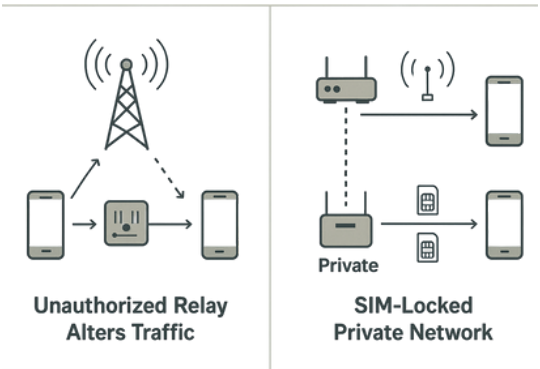
1. Offensively – to intercept third-party communications or send spoofed messages;
2. Defensively – to ensure their own communications remain secure and confined within a private environment.

For instance, in 2024, a fraud network in the UK constructed a homemade fake base station to send phishing SMS messages to thousands of people. This setup bypassed mobile carriers' suspicious message filters and was recorded as the first incident of its kind in the UK.

This case demonstrated that even consumer-grade radio equipment could be used to build functioning IMSI catchers. Similar incidents have been observed across East Asia and Europe, where portable IMSI catchers hidden in backpacks were used to push fake messages to nearby phones. One notable case in Paris in 2022 involved the discovery of a mobile IMSI catcher installed inside a repurposed ambulance.

Cartels may also use IMSI catchers for defensive purposes. If members do not want their phones to connect to public cellular networks, they can deliberately deploy a fake base station and configure it to accept only SIM cards issued internally by the cartel. This allows the group to create a closed, local GSM micro-network, ensuring all communications stay within a controlled environment — adding an extra layer of protection against external surveillance.

Moreover, cartels might monitor their cellular environment to detect anomalies that suggest a foreign IMSI catcher (e.g., one deployed by law enforcement) has been introduced into their territory. In such cases, anomaly detection tools could alert them to the presence of unauthorized surveillance equipment.



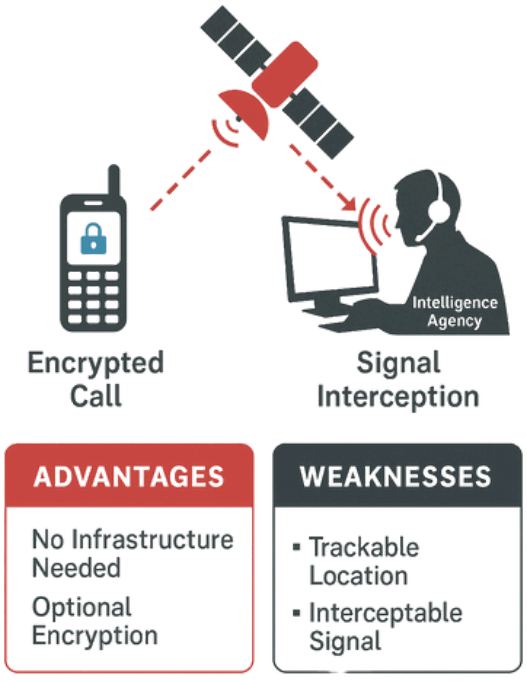
1.3 Satellite Communication

In geographically remote or infrastructure-deficient regions, criminal organizations often rely on satellite communication as a critical alternative. Satellite phones are particularly attractive because they can establish communication directly via satellite, even in mountainous terrain, dense forests, or across oceans. Cartels have historically used satellite phones for top-tier leadership communications, believing them to be more secure.

For example, the Mexican Sinaloa cartel leader "El Chapo" Guzmán reportedly used a satellite phone during his years on the run. U.S. intelligence agencies were able to track his location by monitoring satellite phone signals — a tactic that played a key role in his eventual capture.

During the operation, cartel members who were apprehended also turned over satellite phones. The contact lists and call logs contained within these devices proved extremely valuable for intelligence purposes, offering critical insight into the structure and communication flow of the organization. Similarly, the Colombian FARC, a guerrilla group active in dense jungle terrain, is known to have relied heavily on satellite phones for field communication.

One of the key advantages of satellite phones is that they do not depend on terrestrial infrastructure. Furthermore, many models can be equipped with scrambling or encryption devices. In fact, as early as the 1990s, some drug cartels had begun using encrypted satellite communication systems to make interception more difficult.



However, it is important to note that satellite communication is not entirely secure. Advanced intelligence agencies are capable of tracking satellite signals or gaining access to satellite service providers. For instance, an unencrypted satellite call, transmitted as a radio wave to the satellite, can be intercepted by any entity with sufficient technical capabilities.

To mitigate this, cartels often attempt to leverage built-in encryption features provided by satellite phone manufacturers (some modern devices now come with integrated, strong encryption by default). As a result, satellite communication remains a critical tool for cartels, especially for cross-border coordination, long-distance planning, or situations where local infrastructure is suspected of being compromised. Still, due to its limitations, this communication channel is often combined with additional cryptographic protections to increase operational security.

1.4 VoIP and Encrypted Mobile Networks

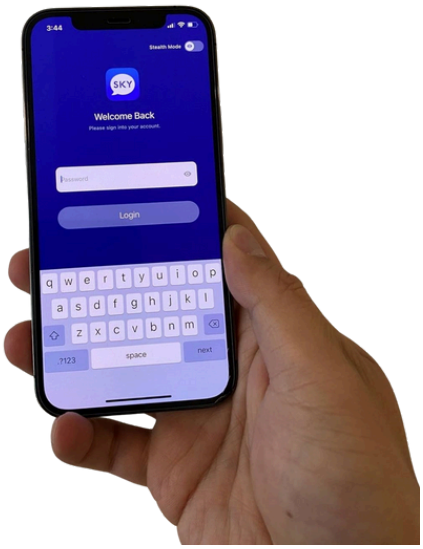
Private Voice over IP (VoIP) communication networks and encrypted messaging applications have become common tools for cartels and mafia organizations. With the widespread adoption of smartphones, the criminal underworld has increasingly turned to custom-built encrypted phone services. In recent years, several global encrypted communication networks have been exposed:

EncroChat was a Europe-based encrypted communication network offering hardened Android phones exclusively to its members. These devices had their cameras, microphones, GPS modules, and other tracking hardware disabled, and came pre-installed with only a secure messaging app.

Users could only communicate with others within the EncroChat network. All messages were end-to-end encrypted and routed through EncroChat's offshore servers. The system became highly popular among organized crime groups in Europe — so much so that in 2019, even leaders of the Sinaloa cartel were found to be using EncroChat phones.

In 2020, a joint European police operation compromised EncroChat's infrastructure. Authorities infiltrated the servers and decrypted tens of millions of messages, leading to hundreds of arrests across Europe and the network's eventual shutdown.

Sky ECC After EncroChat's collapse, Sky ECC rose in popularity among criminals. Based in Canada, Sky ECC also offered specialized encrypted smartphones. In 2021, coordinated operations by Belgian and French authorities dismantled its infrastructure. Investigators seized encrypted messages and made numerous arrests, significantly disrupting organized crime activities across Europe.



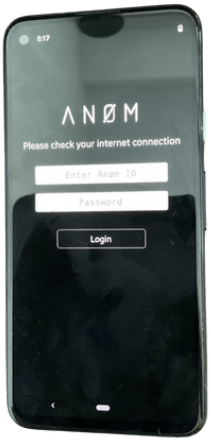
Phantom Secure This Canada-based company provided PGP-encrypted email and messaging services primarily via modified BlackBerry devices. Phantom Secure was widely used by international drug trafficking groups, including senior members of the Sinaloa cartel.

Clients were accepted only by referral, and devices were equipped with remote wipe (kill switch) functionality. In 2018, Phantom Secure's CEO and several employees were arrested by the FBI, and the network's servers and domains were seized. According to court testimonies, the company sold at least 20,000 encrypted devices, used globally to facilitate the trafficking of cocaine, heroin, and methamphetamine.

Alperen L. Ugurlu

ANOM was a honeypot network secretly developed by the FBI and its partners. Marketed as a secure communication platform, ANOM devices were covertly distributed to criminals worldwide. After the fall of EncroChat and Sky ECC, many criminal actors adopted ANOM.

In 2021, the operation was revealed: over 800 individuals were arrested globally, as law enforcement had been silently monitoring their encrypted communications the entire time. ANOM represents a rare example of how trusted communication technology can be weaponized as a large-scale trap by intelligence agencies.



Common Characteristics of Encrypted Phone Networks

These encrypted networks typically operate completely independent of traditional phone infrastructure, using internet-based end-to-end encryption. Users can only communicate with others on the same platform, and devices often feature:

- Disabled microphones and cameras
- Hardware encryption modules
- Panic wipe or kill switch functions

Communication is conducted via VoIP protocols and encrypted messaging, rather than SMS or regular voice calls. This bypasses lawful intercept systems like CALEA, allowing criminal groups to avoid traditional wiretaps.

For a time, these networks provided near-total protection against law enforcement surveillance. However, in recent years, state-level actors have increasingly succeeded in infiltrating or dismantling them through advanced cyber operations and international cooperation.

Still, organized crime groups quickly adapt, often building their own private VoIP servers, VPN tunnels, or darknet-based communication channels, continuing the search for untraceable, anonymous communication systems.

Alperen L. Ugurlu

2. Penetration Testing Perspective

2.1 Passive Radio Recon & Traffic Decryption (SDR-Based)

Objective: Intercept unencrypted or weakly protected digital radio or VoIP communications and extract infrastructure data.

Tools: HackRF, RTL-SDR, GQRX, CubicSDR, GNU Radio, DSDPlus, OP25, Wireshark, kalibrate-rtl, gr-gsm

Threat Model: Cartel members communicate using unencrypted or weak digital radio systems. These channels can be intercepted from a distance, providing insight into operational details.

Tactic Flow:

1. Scan local RF spectrum with GQRX.
2. Identify signal types and protocols (e.g., analog, DMR, P25).
3. Use DSDPlus/OP25 to decode audio.
4. Scan for GSM BTS using kalibrate-rtl and grgsm_scanner.
5. Analyze VoIP RTP packets with Wireshark.

Sample Commands:

```
kalibrate-rtl -s GSM900 -g 40
# Output:
# chan: 124 (935.0MHz + 0.0kHz) power: 6200

grsms_scanner
# Output:
# MCC: 208, MNC: 10, LAC: 01F4, ARFCN: 124

dsdplus -i rtl_tcp://127.0.0.1:1234 -o decoded.wav
# Output:
# Playing decoded audio stream...

wireshark -Y "rtp || sip" -i wlan0
# Output:
# SIP Invite -> RTP Stream -> Audio Codec: G.711
```

2.2 IMSI Catcher Deployment

Objective: Harvest IMSI identities of cartel members and track local BTS behavior.

Tools: OpenBTS, YateBTS, srsRAN, SDR hardware (BladeRF, LimeSDR)

Threat Model: Fake BTS lures target phones into connecting, enabling identity collection and location triangulation.

Tactic Flow:

1. Start rogue LTE base station with srsenb.
2. Observe connection logs and extract IMSI/TMSI.
3. (Optional) Redirect or capture traffic.

Sample Commands:

```
sudo ./srsenb enb.conf
# Output:
# eNB connected on frequency 2680 MHz
# RRCConnectionRequest: IMSI 001010123456789

tail -f /OpenBTS/logs/OpenBTS.log
# Output:
# IMSI detected: 001010123456789
# TMSI: 0xF123ABCD
```

- IMSI Catcher detectors
- Randomized IMSI refresh protocols
- Carrier-side BTS location verification

2.3 Digital Radio Hijacking & Decryption

Objective: Intercept and/or spoof encrypted radio traffic.

Tools: OP25, DSDPlus, SDR#, UniTrunker

Threat Model: Cartel uses digital trunked radio with weak or no encryption; traffic can be decoded or mimicked.

Tactic Flow:

1. Use UniTrunker to follow talkgroups.
2. Capture audio and decode with DSDPlus.
3. Inject spoofed messages using recorded samples.

Sample Output:

```
dsdplus -i audio_input.wav -o audio_output.wav
# Output:
# Decoded voice stream saved to audio_output.wav

UniTrunker GUI:
Control Channel: 853.9125MHz
Talkgroup: 1015
Unit ID: 10023 -> Voice Grant to TG:1015
```

- Mutual radio authentication
- Rolling encryption keys
- RF anomaly detection on known talkgroups

2.4 VoIP & Encrypted Messaging App Compromise

Objective: Analyze traffic and perform MITM or reverse engineering on custom apps.

Tools: mitmproxy, Frida, Objection, Burp Suite, Wireshark

Threat Model: Cartels deploy their own encrypted VoIP solutions. If reverse-engineered, vulnerabilities may expose metadata or message content.

Tactic Flow:

1. Bypass certificate pinning using Frida.
2. Hook mobile app functions via objection.
3. Capture and manipulate VoIP traffic.

Sample Output:

```
mitmproxy -p 8080
# Output:
# Intercepted HTTPS request to /auth/token
# Header: Authorization: Bearer xyz...

frida-trace -n com.securechat
# Output:
# Hooked function sendEncryptedMessage(): ciphertext length = 1024 bytes
```

- Strong TLS pinning
- Encrypted push notifications
- Non-trivial session key derivation

2.5 Infrastructure Hijack & Firmware Analysis

Objective: Reverse engineer seized equipment such as routers, repeaters, SDR nodes.

Tools: Binwalk, Ghidra, Radare2, JTAGulator

Threat Model: Equipment used by cartels may contain logs, hardcoded credentials, or encryption keys.

Tactic Flow:

1. Dump firmware from device.
2. Extract file systems using Binwalk.
3. Disassemble and analyze logic with Ghidra.

Sample Output:

```
binwalk -e firmware.img
# Output:
# 0x00000040 gzip compressed data, has original file name
# Extracted: ./_firmware.img.extracted/squashfs-root/etc/config/network

Ghidra:
Function Disassembly: checkAuthToken()
Referenced Strings: 'admin', 'root', '/etc/shadow'
```

- Secure boot and firmware encryption
- Anti-tamper mechanisms
- Device self-wipe on breach

2.6 Social Engineering & Spoofing Devices

Objective: Trick cartel members or systems using fake identities and communications.

Tools: Custom SDR scripts, Asterisk, SIP proxy tools, spoofed radios

Threat Model: Spoofed messages or devices mimic trusted sources, manipulating behavior or extracting intel.

Tactic Flow:

1. Replay known communication patterns.
2. Simulate a repeater or field unit.
3. Observe reaction or redirection.

Extended Technical Enhancements

- **Lab Scenarios:** OpenBTS on Docker, dummy VoIP apps, simulated trunked networks.
- **Red Team Chain:** Recon > Decrypt > Pivot > Persist > Exfil.
- **MITRE ATT&CK:** T1583.006, T1030, T1008.
- **Zero-Day Focus:** Frida/Objection reverse flows, TLS bypass, protobuf data leaks.

Conclusion

Transnational criminal cartels are no longer simply users of secure communication — they are builders of covert infrastructures. The evolution from burner phones to air-gapped GSM cells, encrypted radios, and self-hosted VoIP platforms reveals a trend: organized crime now operates as a shadow IT ecosystem. This study demonstrated how red team operators and cybersecurity professionals can simulate, deconstruct, and exploit these clandestine systems using:

- SDR-based signal interception,
- Rogue base stations (IMSI catchers),
- Digital radio decryption tools,
- Mobile app reverse engineering platforms,
- Firmware-level hardware analysis.

Each technique in this report is not theoretical — it is derived from practical tools and lab simulations that can be replicated in field-grade red teaming environments.

💬 *"The future of cartel disruption is not purely legal or tactical — it is technical."*

Law enforcement agencies and cybersecurity units must:

- Develop automated, AI-assisted SDR sweeps for pattern detection,
- Use proactive pentesting on seized cartel equipment,
- Create signature libraries of cartel-specific RF and software fingerprints,
- Establish cross-border forensic networks with integrated toolkits.

Finally, this paper illustrates a key cybersecurity truth:

💬 *"You cannot defend against what you do not understand."*

To dismantle underground infrastructure, we must first mirror it, model it, and outmaneuver it — at wire speed.

Alperen L. Ugurlu