



# Cyber-Telecom Crime Report 2019

Trend Micro Research  
Europol's European Cybercrime Centre (EC3)



# Foreword

Financially motivated cybercriminals will always find ways to exploit new and existing business processes and technologies. Telecommunications fraud is another example of criminals “hacking the system” in order to abuse legitimate enterprises for criminal gain. While this is not a new crime area, it does represent a new challenge for many law enforcement agencies throughout the European Union, emphasizing the need for law enforcement and private industry to build close working relationships to improve our capabilities and increase our effectiveness in preventing, prosecuting, and disrupting cybercrime related to telecommunications fraud.



**Steven Wilson**

Head of Europol's  
European Cybercrime Centre (EC3)



**Craig Gibson**

Principal Threat Defense Architect,  
Forward-Looking Threat Research Team,  
Trend Micro

Telecommunications has been with us for so long that we don't remember what it was like to not have it. We trust that our phones will work, that we can work from home, that we can be paid through our ATM accounts, and that we can shop online. We tend not to think about what is under the covers of the unseen global network we rely on so much, despite the fact that telecom carriers and their networks are the underpinning of modern society.

The vulnerability in a system of this size is in its humanity: the billions of family photos sent, the work emails sent at midnight, the ability to reach your child when they don't come home on time. A global always-on and always-present network is also always exposed. Like any system involving people, it has to evolve faster than we do or we will break it. The only way we can keep voices and pictures flowing is to work together and evolve together. We have to “watch each other's back.”

The message of this report is that collaboration, cooperation, and sharing are the ways to evolve the safety of this global network of humans in an era of 5G and the internet of things. Let's be ready.



## TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

## EUROPOL DISCLAIMER

©European Union Agency for Law Enforcement Cooperation, 2019. All rights reserved.

Reproduction in any forms or by any means is allowed only with the prior permission of Europol.

More information on Europol is available on the internet:

Website: [www.europol.europa.eu](http://www.europol.europa.eu)

Facebook: [www.facebook.com/Europol](https://www.facebook.com/Europol)

Twitter: [@Europol](https://twitter.com/Europol)

YouTube: [www.youtube.com/Europoltube](https://www.youtube.com/Europoltube)

Published by:

**Trend Micro Research**

Written by:

**Craig Gibson**

Principal Threat Defense Architect of Trend Micro

**Europol's European Cybercrime Centre (EC3)**

Stock images used under license  
from Shutterstock.com

*For Raimund Genes (1963-2017)*

# Contents

## 05

The Perpetrators of Telecom Fraud

## 09

From Physical Access to Network-based  
Frauds: How Telecom Fraud Has Evolved

## 13

Threat Model Components for  
Telecom Crime

## 22

Threat Modeling Telecom  
Infrastructure

## 28

Physical Telecom Infrastructure Attacks  
Facilitating Telecom Fraud

## 35

Network-based Telecom Fraud Attacks

## 41

Noteworthy Real-World Cases of  
Telecom Fraud

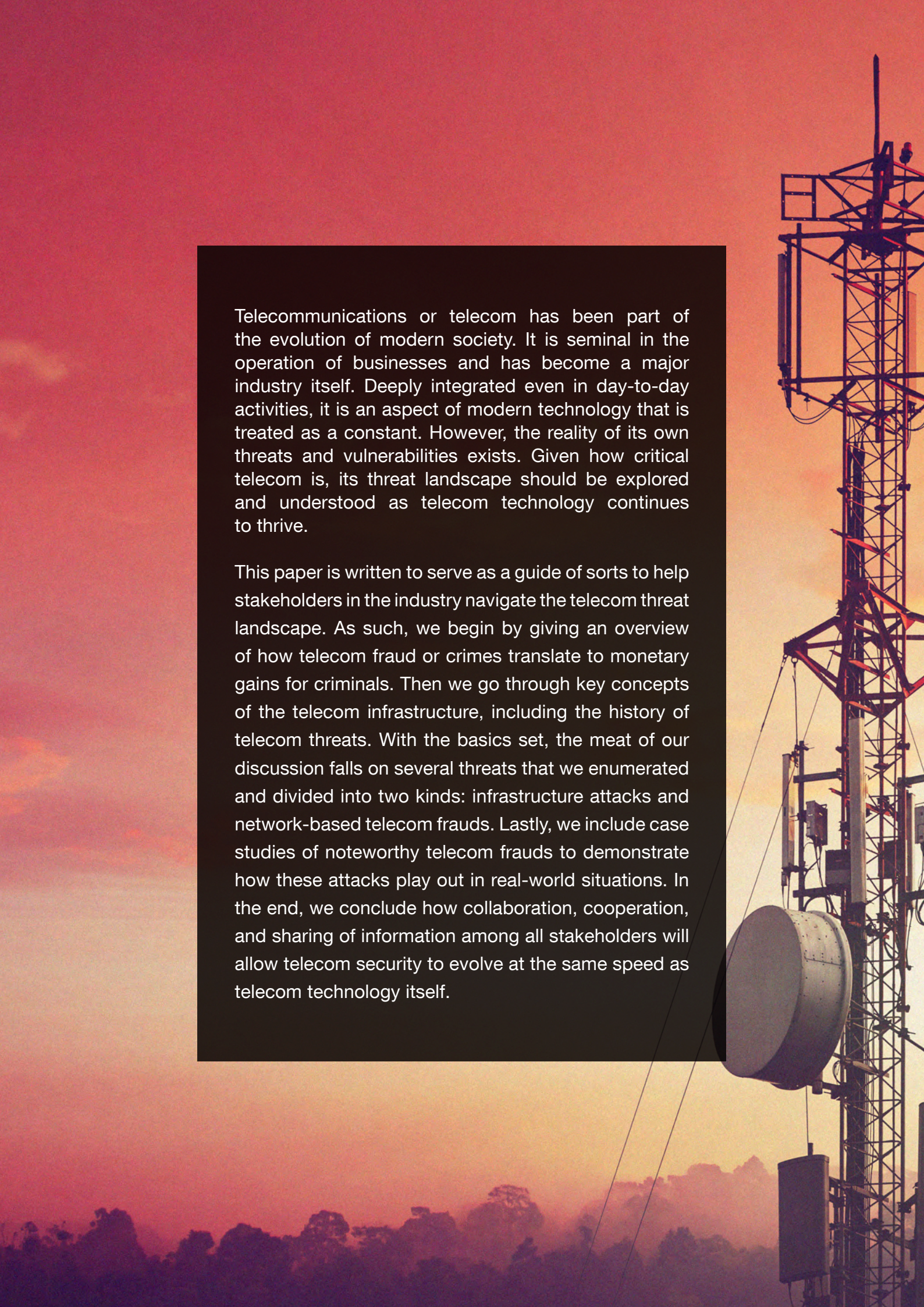
## 45

Conclusion

## 46

Appendix





Telecommunications or telecom has been part of the evolution of modern society. It is seminal in the operation of businesses and has become a major industry itself. Deeply integrated even in day-to-day activities, it is an aspect of modern technology that is treated as a constant. However, the reality of its own threats and vulnerabilities exists. Given how critical telecom is, its threat landscape should be explored and understood as telecom technology continues to thrive.

This paper is written to serve as a guide of sorts to help stakeholders in the industry navigate the telecom threat landscape. As such, we begin by giving an overview of how telecom fraud or crimes translate to monetary gains for criminals. Then we go through key concepts of the telecom infrastructure, including the history of telecom threats. With the basics set, the meat of our discussion falls on several threats that we enumerated and divided into two kinds: infrastructure attacks and network-based telecom frauds. Lastly, we include case studies of noteworthy telecom frauds to demonstrate how these attacks play out in real-world situations. In the end, we conclude how collaboration, cooperation, and sharing of information among all stakeholders will allow telecom security to evolve at the same speed as telecom technology itself.



# The Perpetrators of Telecom Fraud

Geopolitically, most telecom crime tends to be addressed by the telecom companies themselves. The costs are absorbed as the cost of doing business. This creates a kind of isolation however. Without thorough cross-border intelligence sharing and intelligence fusion with law enforcement, the source, investigative method, and evidence cannot be connected in a way that results in a meaningful number of arrests or a decrease in the acceleration of international cyber-telecom fraud.

Traditional financial crime involves banking and extensive bank-side Anti-Money Laundering Audit Controls (AMLAC).<sup>1</sup> These AMLAC controls that prevent many types of bulk financial crime are not present in telecom crime when SIM (subscriber identity module) cards are used in place of traditional banking methods. The relatively lateral criminal element present in nearly all countries is simultaneously reaching the concept of telecom crime as a low-risk alternative to traditional financial crime.

Telecom fraud is increasingly originating in countries normally considered “third world” or failed states. It is also increasingly being used to prop up failing economies. The normal sequence of events is that crime goes up to the point the military becomes government, but in this case the flow has reversed, being that a failing government has a failing military. Both entities rely on military-like trans-border crime as a supporting alternative to falling tax collections due to rising unemployment. This reverse sequence is complementary to what some coastal countries experience: they undergo the same de-evolution where they end up conducting ocean piracy and, in some cases, cross-border banditry as a means of supporting their government.

The drivers of this simultaneous awakening are the reduced cost and increased availability of telecom equipment capable of hacking intercarrier trust, the availability of information on the topic, and the flattening (homogenization) of telecom deployments in 4G. These drivers will continue in 5G, and be further multiplied by the effect of the nested tiers of automation (and attack effect amplification) contained in the core cost-reducing design drivers of 5G architecture.

---

<sup>1</sup> Financial Action Task Force (FATF). (n.d.). *The FATF Recommendations*. Last accessed 14 February 2019 at [http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)).

These trends also escalate due to the overlap of specific economies — the cost of telecom deployments drops due to economic commonalities driven by the need for automation. Examples of these include rising telecom costs, competition from nontraditional telecom providers, and market saturation.

This automation and commonality lends itself to criminal use. And if a network becomes 10 times more scalable, then it could mean that attacks using that infrastructure will have 10 times the effect, damage, and cost. Attacks involving this infrastructure also have the capability of using their speed against the carrier itself, enabling more cases of telecom fraud to be performed in the time that it takes people to respond to fraud gaps and security incidents caused by vulnerabilities attackers have newly discovered.

## Cashing Out Telecom Crime

### Overview

The annual cost of telecommunications subscription fraud is estimated by some to reach up to more than US\$12 billion, while others foresee the actual losses to be far greater, estimating it to be between 3 percent and 10 percent of the operators' gross revenues.<sup>2</sup>

The purpose of gaining access to the SIM or other billing portions of a network is to get to the customer or carrier account, where debt can be incurred in favor of the attacker (i.e., large volume fraud). This victim debt is criminal revenue. If the attacker has access to the carrier accounts with the global clearing house (the GPRS Roaming Exchange or GRX), the customer account itself (such as the web billing customer account), or the Smart City aggregated SIM account (responsible for 100,000 SIMs worth of monthly billing), then the attacker effectively has access to many “bank accounts.”

The most common methods of “cashing out” SIM card accounts can be broken into categories that range from low to high sophistication:

- **SIMs**

Premium phone numbers will bill the account “behind” a SIM card when called. If the attacker is in control of the premium number (under another carrier), then the attacker will be paid part of the cost of the call. The rest will go to the cooperating carrier. International revenue share fraud (IRSF) is one example of this arrangement.

---

<sup>2</sup> ThreatMetrix. (15 January 2019). *ThreatMetrix*. “Telco Fraud: Why this Industry is Unique in the Cybercrime Landscape.” Last accessed on 8 February 2019 at <https://www.threatmetrix.com/digital-identity-blog/cybercrime/telco-fraud-why-industry-unique-cybercrime-landscape/>.

- **Customer Self-Management Website Accounts**

Customer self-management websites are typically secured by a password chosen by the customer and, therefore, depending on password strength, may have little or no security. These telecom self-management accounts control SIM-related debt. Accessing the website to manipulate the SIMs effectively grants access to money. These websites also grant access to customer phone numbers and their ownership. Through a standards-based activity called wireless number portability, the phone number may be changed from one carrier to another. With this level of control over the customer account, the numbers may be pointed in any direction to facilitate nearly any telecom fraud. The true owner can be locked out of their account or even implicated in various non-fraud telecom crimes, for example, those involving death threats).

This level of control also redirects data and SMS (short message service) traffic, meaning true banking SMS transaction authentication number (TAN) codes can be captured, giving attackers access to true bank accounts and, consequently, allowing for further fraud and money laundering. One variety of this is SIM jacking.

If a carrier has “Autopay” credit card payments prearranged with the customer, the various instances of telecom fraud performed will also invoke debt against the customer’s credit card, which may go unnoticed for a time. In this way, SIM card fraud can enable credit card fraud.

- **Enterprise or Smart City Telecom Management**

This is very similar to the use of customer self-management websites; however, in this case the enterprise account manages many SIMs and other telecom accounts. Gaining access to this webpage will amplify the ability of the fraudster to create debt (criminal revenue) and likely allow the attacker to gain access to the functionality of non-human devices like those in the internet of things (IoT), smart factories, autonomous vehicles, and others. By controlling many accounts and many SIMs, the enterprise becomes, in part, the money laundering apparatus responsible for monetizing the attack on itself. This could be thought of as similar to ATM jackpotting, where malware is used or machine vulnerabilities are exploited to empty the machine’s cash safe.<sup>3</sup>

- **Insider Trading**

When gaining access to SIMs, and redirecting them across own infrastructure, fraud need not occur. If there is no fraud, there is nothing to detect and, therefore, an attack can continue unnoticed for some time.

When criminals redirect traffic across their own infrastructure, they can add themselves to the unencrypted “conversation” while allowing the traffic to continue to the intended recipient.

---

<sup>3</sup> Trend Micro Forward-Looking Threat Research Team & Europol’s European Cybercrime Centre. (5 September 2017). *Trend Micro*. “Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types.” Last accessed on 2 February 2019 at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/shift-in-atm-malware-landscape-to-network-based-attacks>.

By adding a voice capture appliance such as a voice-to-text device, the content of the target conversations or traffic can be caught. If this captured traffic is text-searched for hits against a glossary of insider trading keywords, the attacker can “beat the market” by engaging in a very profitable (but otherwise undetectable) investment.

- **Statecraft-Level Insider Trading**

When insider trading financial attacks are performed on a target by a state actor, the effect is much like that of industrial espionage, but rather than steal secrets to enhance competitiveness to help the economy of the actor’s country, the actor skips the middle steps and goes straight to the economic benefit. The actor’s investment portfolio improves, and at the same time, information of strategic value can be provided directly to the actor’s state industries.

This class of attack can be detected using advanced financial statistical quantitative analysis such as that used in actuarial banking techniques. However, this detection is of little value without both cybersecurity-telecommunications (CyTel) intelligence fusion and law enforcement collaboration necessary to justify any remedial action. In any event, the statistical anomalies that indicate this activity is occurring tend to be of obvious interest to intelligence agencies.

## **Cash-Out**

Cash-out and conversion are the last steps of any money laundering process. They are also of the highest risk since they are the most obvious to spot for law enforcement to capture the criminal. For this reason, actual cash is avoided by most criminals, and even laundered money is manipulated indirectly.

Aggregate telecom balances may be traded as passwords-with-value, making the account itself a financial instrument similar to fiat currency. In this way, a password representing US\$10,000 is considered equivalent to a “US\$10,000 bearer bond” guaranteed only by the financial stability of the backing carrier. Only at the smallest scale of organized crime does the value become true cash used to buy merchandise. In this way a password becomes a kind of digital asset similar to a Bitcoin address.

## **IRSF Chaining as Money Laundering**

International revenue share fraud is a means of transferring value from one carrier to another. This is similar to what is considered a wire transfer in international banking. Since carrier logs show the path a “live” call took, and those logs are kept for a short time, criminals can simply wait for the logs to expire before executing any further money laundering steps. The attackers can then perform IRSF on themselves to move the value from their own account under one carrier to an account under another carrier (they are unlikely to complain when they “victimize” themselves). This way, the connection to the victim is obscured by the expired log. After a few of these “hops,” patient fraudsters will have broken much of the chain of evidence that might connect them to the original crime.



# From Physical Access to Network-based Frauds: How Telecom Fraud Has Evolved

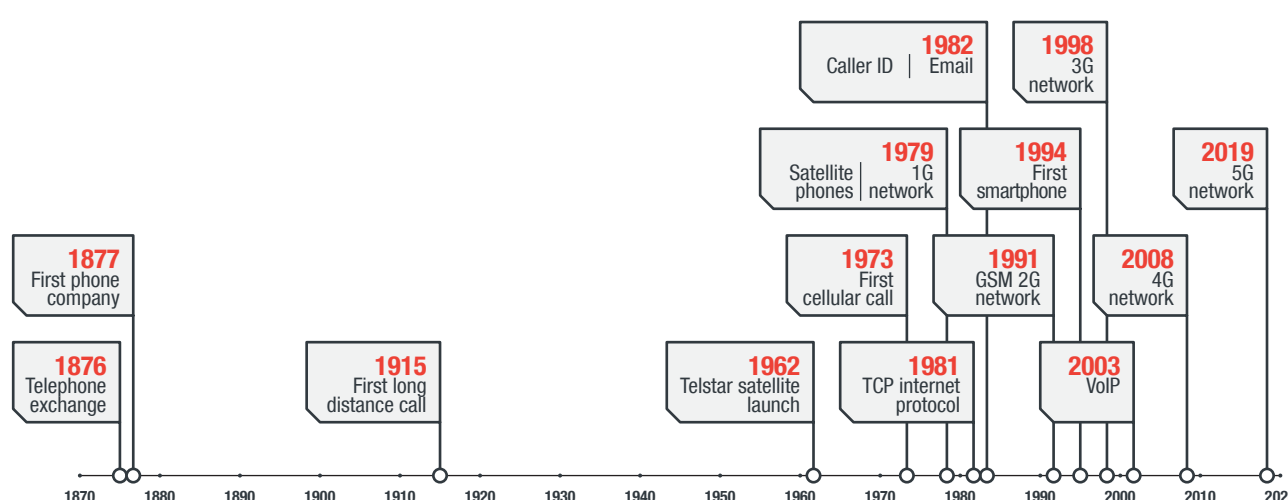


Figure 1. Timeline of telecom evolution to 5G<sup>4,5</sup>

## The Human-Defined Network—Circuit Switching

Telecom network design philosophies more than one hundred years old are still in use in many parts of the world. A name for one of the older types of this philosophy is circuit-switched technology, which is similar to what was once used by human switchboard operators. These switchboard operators would verbally ask who the call was for and manually plug cables into a switchboard to establish the connection (the circuit). This circuit switching required dedicated resources and was very resource-intensive. Eventually, the human switchboard operators were replaced by automated machines, but the technology design was effectively unchanged for a hundred years.

<sup>4</sup> Mitel. (n.d.). "The History of Telecommunication." Last accessed on 21 February 2019 at <https://www.mitel.com/articles/history-telecommunication>.

<sup>5</sup> Glen Kunene. (18 April 2017). *Nexmo Blog*. "A History of Telecommunications: How Telecoms Became Just Another Interface." Last accessed on 21 February 2019 at <https://www.nexmo.com/blog/2017/04/18/a-history-of-telecommunications-how-telecoms-became-just-another-interface>.



Figure 2. Switchboard operators at work manually establishing voice circuits to carry voice calls  
(Photo used under license from Shutterstock.com)

A very common vulnerability in these networks was that the switchboard operators would listen to the conversations of all the most interesting people in the city and trade the content as gossip. A private investigator who knew a switchboard operator (and was willing to pay for information) would have had access to his own wiretap infrastructure.

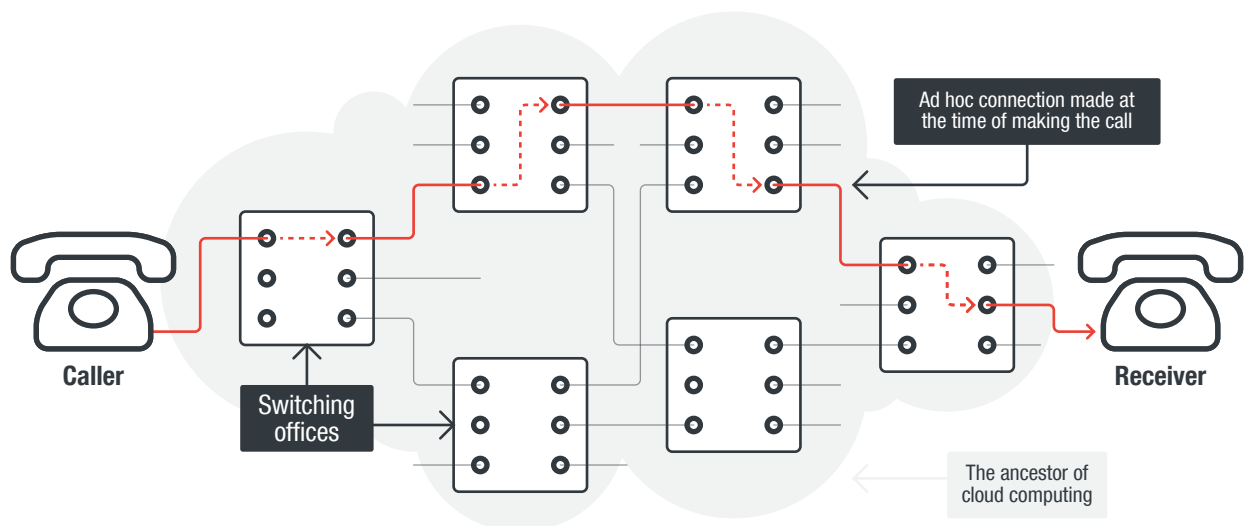


Figure 3. Switch paths establishing voice circuits to carry voice calls in a circuit-switched network<sup>6</sup>

<sup>6</sup> Computer Networking Demystified (n.d.). *Computer Networking Demystified*. "Overview of Circuit Switching and Packet Switching." Last accessed on 8 February 2019 at <http://computernetworkingsimplified.in/physical-layer/overview-circuit-switching-packet-switching/>.



# The Hardware Defined Network—Packet Switching

When the resource constraints and scalability limitations of circuit-switched networks became obvious, the emerging “new” information technology and circuit miniaturization became very attractive. The idea that the custom hardware required by telecommunications carriers could be mass produced while meeting their unique specifications drove the explosive growth of the internet. Many carriers identified how much their data transmissions cost and created or acquired internet service provider (ISP) capabilities. Knowing that mobile data speeds facilitated a growing richness of services, many acquired television media outlets to further control mobile television advertising revenue. Thus, carriers are on track to become content delivery networks (CDNs), replacing most methods people use to consume media content. For content delivery networks (voice and video), scalability and capacity are critical issues as these kinds of content consume large amounts of bandwidth and network resources compared to a traditional voice call.<sup>7</sup>

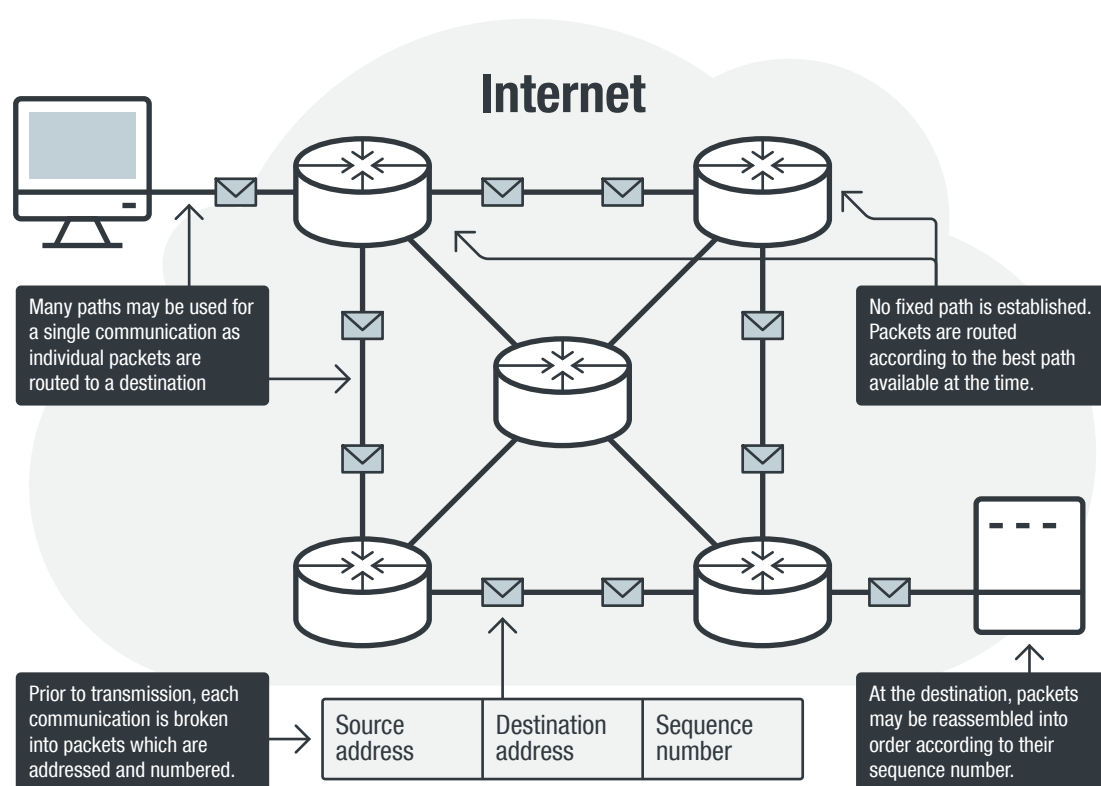


Figure 4. Telecom switching equipment responsible for “manually” establishing voice circuits to carry voice calls<sup>8</sup>

Since packet-switched networks combine many of the vulnerabilities and risks in circuit-switched networks (e.g., wiretap, roaming frauds, SIM card supply chain issues, etc.) with “traditional” IT security risks (e.g., hackers, spies, viruses, worms, etc.), the primary means of protecting these networks comes from an unscalable kind of network isolation in which every carrier attempts to replicate the IT security industry, often in isolation.

<sup>7</sup> Computer Networking Demystified (n.d.). *Computer Networking Demystified*. “Overview of Circuit Switching and Packet Switching.” Last accessed on 8 February 2019 at <http://computernetworkingsimplified.in/physical-layer/overview-circuit-switching-packet-switching>.

<sup>8</sup> Subina Khatri. (n.d.). *Study-for-exam Blogpost*. “Distinguish between circuit switching and packet switching.” Last accessed on 8 February 2019 at [https://study-for-exam.blogspot.com/2013/05/distinguish-between-circuit-switching\\_2.html](https://study-for-exam.blogspot.com/2013/05/distinguish-between-circuit-switching_2.html).

# The Software-Defined Network— The “Data-Switched Network” of Orchestration

In the development of cost-saving and revenue-generating efficiencies, new types of automation are needed to offset the costs of operating ever-more large and complex networks. Increasing regulation and technical complexity require increased throughput and technical sophistication to support the degree of the automation needed.

These nested tiers of automation require advanced management techniques called cloud orchestration or orchestrators.<sup>9</sup> These orchestrators handle the various hybrid circuit-like, packet-like networks called network slices.<sup>10</sup>

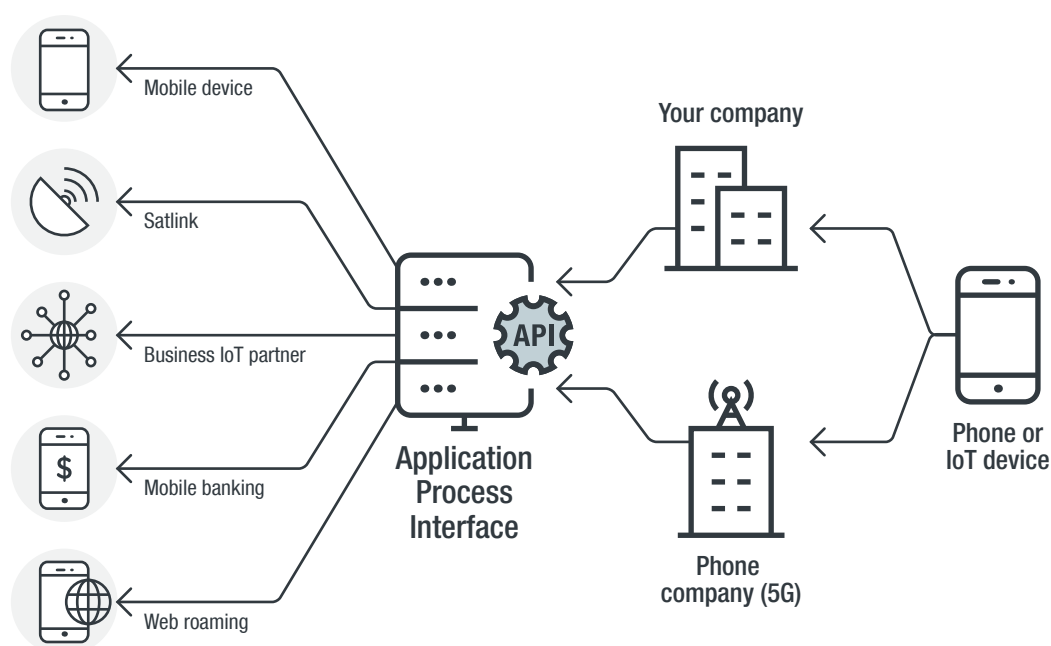


Figure 5. Software-defined networks are implemented across hundreds of identical low-cost computers, using software-based routing and nested tiers of automation to carry voice calls, data, and management traffic

Since these networks inherit the vulnerabilities of both circuit-switched and packet-switched networks while obsolescing many of the security and anti-fraud models used to secure each, the result is that the effects of old risks will be amplified due to the automation of their delivery media (the carrier amplifies the effect of the attack), or new hybrid attacks will become available (telecom fraud viruses and worms).

<sup>9</sup> Margaret Rouse. (n.d.) *Tech Target*. “Cloud orchestration (cloud orchestrator).” Last accessed on 8 February 2019 at <https://searchitoperations.techtarget.com/definition/cloud-orchestrator>.

<sup>10</sup> Sasha Kavanagh. (28 August 2018). 5G. “What is Network Slicing?” Last accessed on 8 February 2019 at <https://5g.co.uk/guides/what-is-network-slicing/>.



# Threat Model Components for Telecom Crime

When describing any complex attack (financial or otherwise), it is useful to create a threat model diagram. These diagrams describe the environment of the threat with enough detail to show what systems, people, and processes are NOT involved, allowing the threat assessment and investigation to move along much more quickly by reducing the space that needs to be examined. By sharing the threat model with others, everyone can have a common understanding and stay very crisply on topic. A threat model will likely become smaller as more is learned about the attack and possibilities are ruled out. This is key to handling an evolving threat quickly during the coordination of a large group containing many people from multiple backgrounds, skillsets, and languages.

Figure 6 shows a diagram of the telecom business and network model. It is a generic model and does not have a threat model (an attacker’s path) overlaid yet. The threat models will be added in the section discussing specific frauds.

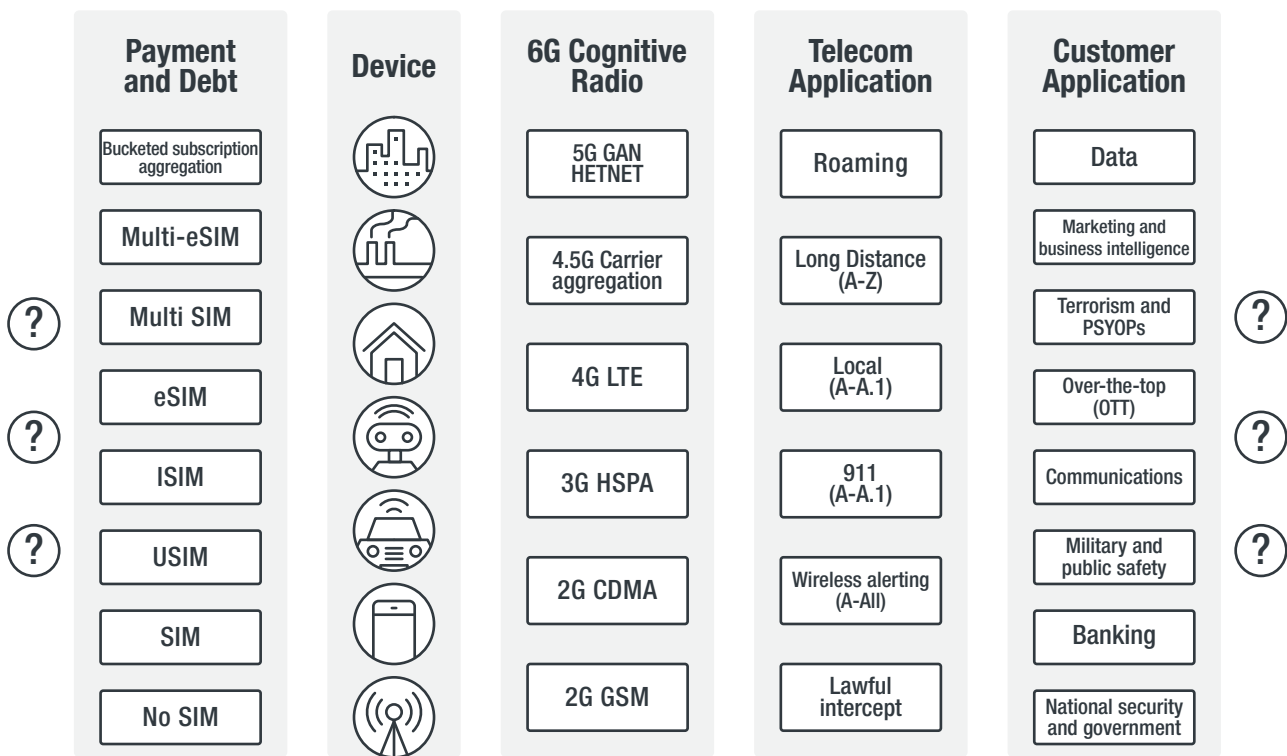


Figure 6. Combined network model and business case showing both ends of the telecom delivery “pipe” at far left and far right ends of the diagram, each represented as ???

# SIM Cards—Mobile Telecom Payment, Fraud, and Debt

A SIM is a card representing the identity of the subscriber. Like bank payment cards, it can be postpaid (like a credit card) or prepaid (like a debit card). Also, like with a payment card, it is often used to assure the identity of the device's user (as denoted by its name). Just like credit cards, SIMs can be the subject of a wide range of supply chain frauds, interception, hijacking, black flag communications forging, and other abuses. Since they are used to initiate transactions of all sorts, the transactions themselves can be falsified for criminal profit.

Unlike payment cards, SIMs of all types can be remotely updated with arbitrary information for the purpose of “efficient content delivery,”<sup>11</sup> which is a standards-based means of changing large numbers of SIM cards all at once, remotely. This can also constitute an attack if used maliciously.

The following are potential attacks for a SIM-less scenario and for different SIM types.

- **No SIM**

Emergency calls from a cellular device (including misconfigured IoT devices) do not require a SIM or any authentication at all. Calls (and crimes) made from devices without a SIM may result in deaths due to their impact on life-critical emergency systems such as those of the police, fire respondents, and paramedics. These dispatch points may have as few as eight long-distance lines, whose capacity can easily be consumed by the most small-scale automated cyber-telecom (CyTel) attacks.

- **SIM**

A common SIM is similar to a tiny credit card, and both SIM cards and credit cards are likely to be manufactured by one of only a few major trusted vendors such as Giesecke and Devrient (G&D) or Gemalto. SIM cards have two major parts: the metal and plastic universal integrated circuit card (UICC) hardware, and the software portion where encryption keys and onboard applications such as mobile wallets, contact lists, and the subscriber identity reside. SIMs (including USIM, ISIM, and eSIM) and others (like those in 5G, satellite phones, and IoT devices) are subject to many of the same frauds and risks that credit cards are. Since a SIM card behaves like a credit or debit card, and it is placed in a cellphone from which billing (like an expensive long distance call or roaming data) can be initiated, the combination of a SIM plus a cellphone can be thought of as a billing system. If viewed this way, a phone-and-SIM combination works like an ATM (automated teller machine) or the credit card purchase point of sale (PoS) terminal in a store. It becomes vulnerable to all the fraudulent and criminal activities that those credit-based and cash-based systems are vulnerable to as well. To be specific, SIMs refer to 2G technology, although the public commonly refers to all UICCs as SIMs regardless of generation (2G, 3G, 4G, 5G).

---

<sup>11</sup> Mohamed Sabt, Mohammed Achemlal, & Abdelmadjid Bouabdallah. (2015). *2015 First Conference on Mobile and Secure Services (MOBISERVICES)*. “Over-the-internet: Efficient remote content management for secure elements in mobile devices.” Last accessed on 12 February 2018 at <https://ieeexplore.ieee.org/abstract/document/7072873/authors>.



- **USIM**

UMTS SIM (USIM) is a 3G or 4G SIM with additional applications and functionality, allowing use in 3G and 4G portions of carrier networks.<sup>12</sup>

- **eSIM**

The embedded SIM (eSIM) is a tiny chip (the “SIM card” without the plastic casing, just its tiny engine operating its functions) which is soldered directly to the board of a phone or IoT device. Because SIMs can be updated remotely, the eSIM never needs to be physically swapped.<sup>13</sup> This ability is very important when IoT SIMs may prove difficult to extract, like inside the top of streetlights, traffic lights, or other areas spread across a smart city or smart country. This allows very large deployments of phones and/or IoT devices to move from one carrier to another in a cheap yet competitive way.

Like with all SIMs, this ability to move from one carrier to another is a vulnerability, especially when a carrier is cooperating with criminals, a carrier is a criminal organization, or criminals are operating their own CyTel War Rig (a “carrier in a box” discussed in an Appendix).

- **Multi-SIM**

Different carriers have different price plans, roaming agreements, and cellular coverage. When a subscriber moves from a region served by one carrier to another region serviced by another carrier, rather than take a SIM from the phone and replace it with one that has a cheaper mobile plan, a multi-SIM phone has the ability to use the cheapest path routing, with whichever SIM is cheapest at the moment. Since these devices use different SIMs based on where they are, many network logs will contain different information based on which SIM was active at that moment. For this reason it may be difficult for investigators to integrate logs for a single event from a single device, when the device was served by multiple carriers as the device moved. Generally, a multi-SIM device will have no more than four SIMs,<sup>14</sup> but in hacked cases may have up to 256 “SIMs” or more.

- **Multi-eSIM**

Similar to but more advanced than a multi-SIM device, a multi-eSIM is a mobile device with the ability to support as many as 256 eSIMs, allowing much more flexibility in roaming and travel. In the case of IoT devices, and certain 5G phones, this flexibility extends to the ability to late bind or “half-activate” devices in the backend network. When the devices are placed in inventory/bought/shipped/turned on, the remainder of the activation occurs in the customer’s home or remote IoT deployment (for example, a traffic camera installed on a traffic light and given power for the first time for instance). This concept of multiple SIMs introduces additional vulnerabilities, since both the data supply chain and vulnerability to both fraud and wiretap multiplies with the number of SIMs (therefore also the carriers/vendors/logs) involved.

---

<sup>12</sup> PC Mag. (n.d.). *PC Mag*. “Definition of USIM.” Last accessed on 12 February 2019 at <https://www.pcmag.com/encyclopedia/term/62422/usim>.

<sup>13</sup> PC Mag. (n.d.). *PC Mag*. “Definition of eSIM.” Last accessed on 12 February 2019 at <https://www.pcmag.com/encyclopedia/term/69396/esim>.

<sup>14</sup> PC Mag. (n.d.). *PC Mag*. “Definition of multi-SIM.” Last accessed on 12 February 2019 at <https://www.pcmag.com/encyclopedia/term/67497/multi-sim>.

- **Bucketed Subscription Aggregation**

Subscription aggregation is an IoT-driven topic becoming more common in smart city and smart country deployments. When a single customer procurement department obtains large numbers of SIM cards of any type, the billing for those SIM cards and the IoT devices they will be deployed in is paid by the procurement department or the department of finance of that customer. This means that the activity of a large number of SIM cards (tens of thousands or millions) is aggregated into a very small number of accounting line items, possibly a single line item for the entire smart city and all of its IoT devices regardless of type. Ultimately, when one or more SIMs are compromised (by stealing them for instance, or through a false cell tower's injection of IoT malware using radio), the fraud generated by the attack is invisible simply due to the accounting method involved. In effect, the fraud is whitelisted at the accounting level. Since the fraud goes undetected, the attack goes undetected as well.

## Device Types

- **Smart City (Network)**

A smart city is a collection of many different always-on radio connected civic devices such as smart traffic lights, smart streetlights, smart garbage bins, and others. Each of these has deeper communication abilities related to their functions. An example is how smart garbage bins can indicate that they are full and should therefore be emptied or not full, meaning the staff can work more effectively elsewhere. Traffic lights can take pictures of vehicles making traffic infractions and send the violation fine to the licensed owner. Streetlights could come on (and turn off) when they detect a person moving down the street. This connected visibility lends itself well to the automation of civic functions. Cost savings for city taxpayers is achieved in the form of increased efficiency and fewer required staff members. Another benefit is the ability to gain new insights that can be gathered for use in city planning (such as information on traffic congestion feeding how traffic lights manage traffic flow in real time). These smart city devices are part of the internet of things and are most likely SIM-card-equipped mobile phone-like devices regardless of whether or not the “cellular” traffic light they are installed in is, in fact, capable of motion.

- **Smart Factory (Network)**

Similar to a smart city, a smart factory performing smart manufacturing is a collection of centrally managed robots that compose part of an IT network. While many factories consider themselves isolated from the internet, the means by which factories meet disaster recovery requirements includes having a cellular data connection for performing backups to an offsite location. For fully automated “dark” factories and others, this cellular connection may also be used for remote maintenance of the factory robots and their management systems. While the robots may not necessarily have SIM cards or phone numbers like typical phones and IoT devices, the cellular device will have an internet connection that will allow backups or factory control. In this way the factory can be used for outbound fraud, and cyber-telecom vulnerabilities can be used to attack the factory.



- **Smart Home (Network)**

A smart home has a lot in common with a smart factory, although the automated devices (a smart oven, for instance) have reduced responsibilities (in the case of the oven, baking) as opposed to those of connected industrial equipment (laser-sinter-welding a car, for example). Unlike typical smart factory robots, smart home devices may in fact have a SIM card and may use either Wi-Fi or cellular data to connect to a home gateway (similar to the smart factory cellular backup device mentioned previously). From there, the devices can be reached from the networks of the manufacturer, the internet, the telecom domain, or even earlier in time through supply chain abuses.

- **Robot (Device)**

A robot is a device, often radio-enabled, that for the purpose of this report also has a SIM card and cellular radio. It is prone to all the attacks and abuses a phone is subject to, including hosting malware, sending telecom fraud messages, or relying on a SIM card subject to a variety of telecom and payment card frauds.

- **Smart Car/Autonomous Vehicle (Device)**

As a mobile device, an autonomous car is a (SIM-enabled) smart car with the ability to drive itself at least part of the time. Autonomous vehicles (e.g., drones, cars, agriculture vehicles, various large mining equipment) are subject to all the frauds and abuses typical phones are subject to, including telephony denial of service (TDOS), in which the car could become lost due to having no internet connection, or in which it gets hijacked and the passengers taken to an arbitrary location, among others.

- **Smartphone (Device)**

As small computers containing a payment card, smartphones are subject to a variety of frauds, malware, viruses, and worms, but aside from that, they also grant attackers access to the users themselves, thus, allowing verbal trickery in the form of voice phishing or “vishing.” There are several different kinds of vishing, including Wangiri scams, voicemail scams, and automated blackmail/ransom. The mass automation of kidnapping fraud/extortion (i.e., fake ransom or blackmail messages) also happens here.

- **Femtocell, Home Cell Tower, or Small Cellular Router (Device)**

Femtocell networks connect to the internet using devices that turn an IT network into a cellular network.<sup>15</sup> These gateways or bridges take the networks and protocols under them and enable them to connect to the internet using cellular data. The device itself will have a SIM card and is, thus, subject to all the frauds and attacks that both IT and telecom are subject to (e.g., hacking, fraud, wiretap). It is important to also note that these devices are normally placed inside the network security perimeter of a smart city, building, home, and so on, and may function as a backdoor into the network.

---

<sup>15</sup> PC Mag. (n.d.). *PC Mag*. “Definition of femcell.” Last accessed on 12 February 2019 at <https://www.pcmag.com/encyclopedia/term/59848/femtocell>.

# Network Types

- **2G – GSM**

Global System for Mobile (GSM) is the first class of phones that held a SIM card, and it allowed calls only.<sup>16</sup> It is vulnerable to wiretap due to old assumptions about criminal inability to buy telecom equipment.

- **2G – CDMA**

Code Division Multiple Access (CDMA) is a more secure version of GSM with a different radio network design.<sup>17</sup> It uses a security method similar to what is now called an eSIM, a configurable security chip in the device. In part, the security improvement occurs when the network identifies (authenticates) the device, and the device identifies the carrier.

- **3G – HSPA, HSPA+**

High Speed Packet Access (HSPA) and evolved HSPA (HSPA+) provide a means of moving both data and voice calls across the same phone, without interrupting one for the sake of the other.<sup>18</sup> HSPA+ uses twice as many data channels and is therefore twice as fast. Devices of this era use SIM cards in which CDMA-like two-way authentication is used, but also use a SIM card.

- **4G – LTE**

Long-Term Evolution (LTE) is a faster network in which many functions can occur at once. In LTE, the automation of the radio network and improvements in the backend network allow voice, data, and video (television and videoconferencing) to function. The mobile data quality becomes high enough that “over the top” entities like Skype and Netflix can function using cellular LTE. However, because of this speed, fraud also accelerates as the business case for telecom fraud becomes much more profitable.

- **4.5G – Carrier Aggregation**

Carrier aggregation refers to the use of cooperating radio algorithms to reduce interference and increase data speed. Devices contain multiple radio types (HSPA and LTE, for instance). The network improvements and integration can combine the transmissions of multiple radio types to add the data speed of all available networks and antennas together to a single network provider (i.e., a single carrier). At the network level, a device may now have multiple IP addresses (IP Volatility) for a single session as it moves from one cell tower to another, to Wi-Fi, and back while the owner walks down a sidewalk. This complicates billing, incident response, logging, and financial investigations.

---

<sup>16</sup> Lawrence Harte. (n.d.). *Engineering 360*. “Introduction to Global System for Mobile Communication (GSM).” Last accessed on 12 February 2019 at <https://www.globalspec.com/reference/66227/203279/introduction-to-global-system-for-mobile-communication-gsm>.

<sup>17</sup> Robert Sheldon. (2012). *Tech Target*. “Wireless carrier security risks: Keeping enterprise data safe.” Last accessed on 12 February 2019 at <https://searchmobilecomputing.techtarget.com/tip/Wireless-carrier-security-risks-Keeping-enterprise-data-safe>.

<sup>18</sup> Bradley Mitchell. (8 December 2018). *Lifewire*. “HSPA and HSPA+ for 3G Networks.” Last accessed on 12 February 2019 at <https://www.lifewire.com/high-speed-packet-access-817467>.

- **5G – HetNet including 5G New Radio**

A Hetnet or network of networks is the fusion of the various networks within a carrier to become one single unified core network serving all customers (a HETerogenous NETwork or HetNet).<sup>19</sup> A 5G HetNet is one in which many different types of radio are intelligently considered by the network, and the most cost-effective ones are chosen based on ever-changing criteria, for instance, routing may change if there is a nearby football game or rush hour is about to begin on a nearby highway

## Telecom Application Types

- **Roaming**

Roaming is the result of a user being the customer of one carrier who has made roaming agreements with another carrier whose service area (radio coverage network) the customer is in.

Roaming involves intercarrier trust, in which roaming partners are assumed to behave honorably. If a member of this global web of agreements does not behave honorably, that member is punished after the fact by having some of its phone numbers blacklisted or otherwise blocked from service.<sup>20</sup>

- **Long Distance**

Long distance is similar to roaming, but the connection to another carrier may reach either a mobile phone or a traditional landline phone. In both cases, intercarrier trust must be honored by the carrier to avoid being blacklisted. Both roaming and long distance may be abused through a variety of attacks explored later in this report.

- **Local**

Calls that are “local” calls are those that both originate and terminate within the same carrier and region. Abused calls are most often disguised as local calls.

- **Wireless Alerting, Broadcast, and Updating**

SMS messages (text messages) were originally meant to only configure and update mobile devices (“Control Plane SMS”). With unused capacity, “User SMS” became a source of revenue that was later used for sending broadcast messages about public safety (for example, hurricane alerts). SMS still updates and alters SIM devices and can route traffic across arbitrary criminal infrastructure to push IRSF telecom fraud malware, originate fraud SMS, and alter the security of devices and networks.

- **Lawful Intercept**

Lawful intercept and criminal wiretap are similar in that they involve the redirection of unencrypted traffic so it can be captured for later analysis. The means of redirecting traffic for the sake of fraud or malware are often very similar to those used to comply with national security wiretap and surveillance requirements.

<sup>19</sup> Lance Uyehara. (31 July 2019). *Electronic Design*. “What’s the Difference Between SON, C-RAN, and HetNet?” Last accessed on 12 February 2019 at <https://www.electronicdesign.com/communications/what-s-difference-between-son-c-ran-and-hetnet>.

<sup>20</sup> Craig Gibson. (23 October 2019). *Trend Micro*. “Toll Fraud, International Revenue Share Fraud and More: How Criminals Monetize Hacked Cellphones and IoT Devices for Telecom Fraud.” Last accessed on 12 February 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/toll-fraud-irsf-criminals-monetize-hacked-phones-iot-devices-telecom-fraud>.



# Customer Application Types

- **Data**

It is traditional bulk data, including everything from email, instant messages, and conversations to application updates and video streaming, when passed through a carrier or ISP infrastructure.

- **Marketing, Advertising, and Business Intelligence**

Very detailed intelligence is gathered through the collection of telemetry or detailed measurement of a target using a remote sensor (a phone or mobile device in this case). Device telemetry includes the browsing interests and time spent on advertisements, the time spent in specific locations, time and frequency for measurable activities such as drinking coffee or reading emails, frequency of people in a user's network viewing any website links sent to them by the user — all this and more are gathered for grueling analysis and action by advertisers. This information may be sold, aggregated, and resold hundreds of times.

- **Population Persuasion: Terrorism, Psychological Operations (PsyOps), and Fake News**

This mechanism is very similar to marketing, advertising, and business intelligence. A demographic is chosen by the malicious “advertiser,” who arranges, through various popular social media channels, to have specific content displayed to the chosen group. The design of this content (which could be a news story or actual advertisement) has the purpose of manipulating public sentiment to sway opinions or persuade people to take a certain action (for example, voting in an election) according to the attacker's desires.

- **Over-the-top**

When networks attain “4G levels of speed and stability,” the data quality is high enough that non-telecom providers can establish their own version of telecommunication “over the top” (OTT) of the carrier network's data. There are many examples of this, including Facebook chat, Skype, WeChat. These services can originate spam and other forms of telecom fraud if capable of making a voice call to or from a telephone number. Since OTT can leverage the programming and automation of IT and software, OTT attacks on telecom can be automated very simply to attack large numbers of victims in a short period of time.

- **Person-to-Person Communications**

One person calls another person. This communication has its own traditional risks: Humans making an otherwise legitimate phone call can make death threats, blackmail, or other abuses.

Additional risks include abuses of conference call membership and routing, allowing an arbitrary wiretap for the sake of insider trading. In this use case (one of many), every call a person makes becomes part of a criminal conference call, which the criminal records (using common conference call functions) and analyzes.

- **Military, Law Enforcement, and Public Safety**

Emergency services such as the 911 hotline are subject to forms of fraud specific to them, such as emergency number international revenue share fraud (EN-IRSF). While IRSF affects most telephone-number-enabled public networks,<sup>21</sup> different number ranges such as emergency numbering have different risk profiles. When a fraud scheme uses an emergency number, it is more likely to result in death (due to the consumption of available emergency calling resources), which is why it is unlikely for carriers to end up blocking this specific type of fraud. Since it is less likely to be blocked, criminals knowingly set up persistent attacks from within this infrastructure, “farming” for fraud revenue despite the deaths they will cause. This process is one of several types sometimes called “murder farms” or lethal persistent fraud.

- **Banking**

Telecom infrastructure is often used as an additional “second method” of securing banking, such as the method of authenticating transactions such as voicemail and SMS text messages. An example would be a TAN SMS or TAN code. These can be rerouted, intercepted, and manipulated for a variety of purposes, including bank account takeovers through SIM jacking. Voicemail and private branch exchange (PBX) (see Section 6) can be manipulated for the same effect.

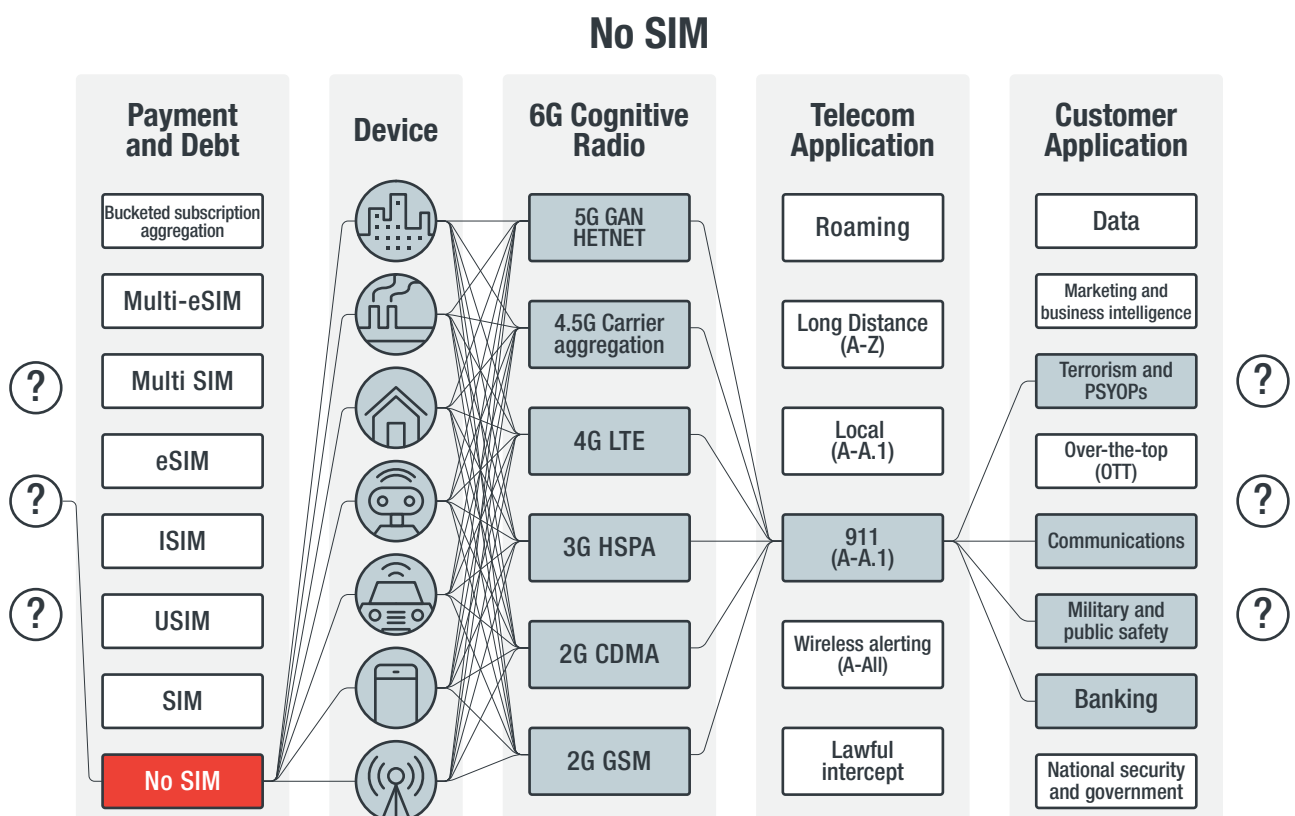
- **National Security and Government**

The methods used in fraud can also be used to manipulate government functions. Wherever telecom can be manipulated for the purpose of fraud, traffic can be manipulated to discover or hide from law enforcement, criminals, or intelligence officers. If the fraud includes a few forms of business process compromise (BPC), the attacker gains the ability to predict the movements of people and their groups (such as terrorists, hackers, police officers, politicians, journalists, or spies).

---

<sup>21</sup> Craig Gibson. (23 October 2019). *Trend Micro*. “Toll Fraud, International Revenue Share Fraud and More: How Criminals Monetize Hacked Cellphones and IoT Devices for Telecom Fraud.” Last accessed on 12 February 2019 at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/toll-fraud-irsf-criminals-monetize-hacked-phones-iot-devices-telecom-fraud>.

# Threat Modeling Telecom Infrastructure



Note: The lines represent the path that telecom attacks including fraud can take.

Figure 7. Emergency call threat model

## SIM Card Supply Chain, Procurement, and Customer Accounts

SIM cards are, as previously discussed, payment cards that can be procured from specific high-trust suppliers, who also make other payment cards, including credit cards and debit cards. Typically, SIM cards are bought by a carrier and transported under medium to high security to a central area, where they are distributed as needed and activated (become capable of billing) when assigned to a specific named customer. As in most forms of fraud, the person requesting the SIM (and therefore access to money) may use a false identity. The criminal may also buy SIM cards from phone thieves, driving robbery, physical assault, and violent crime in the area.



An example of an attack on a telecom customer’s supply chain is when criminals add themselves to the customer’s account using the self-management web portal and making themselves the primary contact, dropping the true owner, reassigning the number, and then using the compromised traffic flow to receive the customer’s transmissions. These may include their computer network permission, two-factor authentication (2FA) codes, banking TANs, etc.

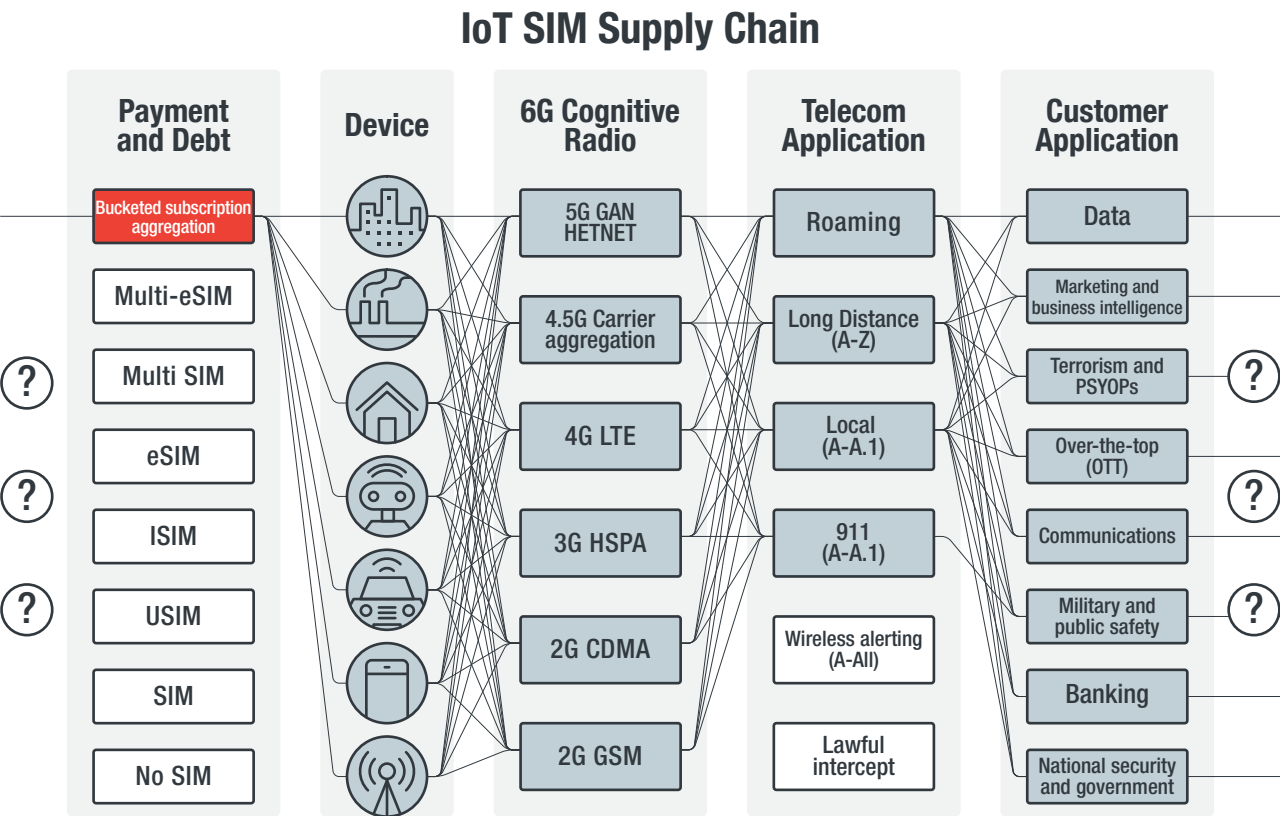


Figure 8. IoT SIM supply chain compromise threat model

## SMS and Premium SMS

SMS can be directed to criminal-operated premium numbers, where billing is inflated by criminal traffic. There are various means for this, including malware (worms and viruses), and can be implemented to create very large traffic volumes and subsequent bills for the true owner of the phone number.

SIM cards used in IoT can be removed often from the IoT device and used in fraud. Famously, a case of IoT SIMs being removed from traffic lights for the sake of being placed in SIM boxes involved criminals committing long distance fraud.<sup>22</sup> Even if the device is capable of only recording digital video and storing that video locally while receiving one management SMS per month, the features enabled on a common IoT SIM card typically include everything a person could or would use (i.e., more features than a “paying user” would activate). This means a common “smart” IoT trash can can place long distance calls, send spam, function as a gateway, launder (bridge) data and SIM-based financial transactions, and many others.

<sup>22</sup> BBC News. (n.d.). BBC News. “South African thieves hit traffic lights for Sim cards.” Last accessed on 13 February 2019 at <https://www.bbc.com/news/world-africa-12135841>.

A common error in providing access privileges and billing authority is that a relatively “dumb” IoT device has a feature set unknown to the procurement department buying it, and so the buying carrier or their customer essentially “enables all telecom features” by not changing the configuration as this is a very common default configuration.

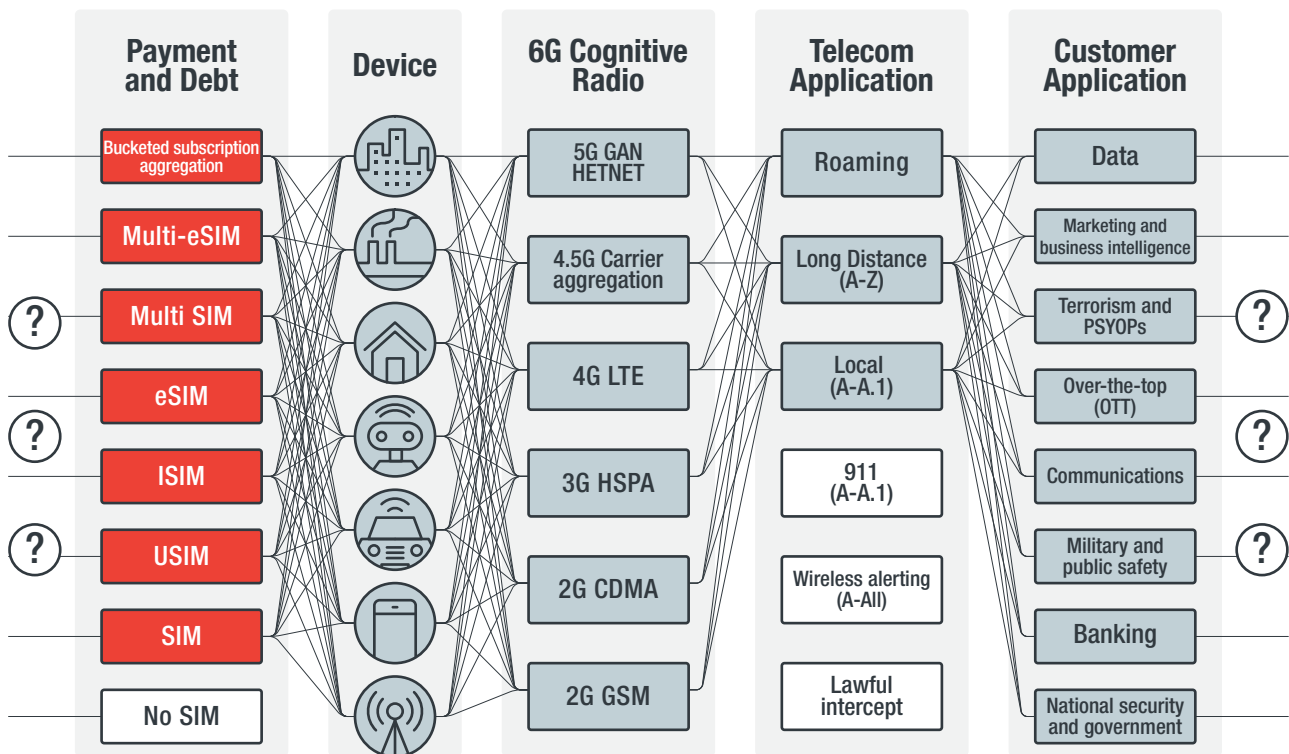
This leaves cellphones or IoT devices open to exploitation for fraud. Aside from being used to send large volumes of fraudulent billable traffic, they could even be subject to attacks such as a cellular data malware infection to attempt the creation of an opportunistic pass-through Bluetooth malware infection of every device walking by the infected IoT device (for example, via phishing malware using, among others, fake free coupon links).

## Trunking

Trunking is the establishment of bulk call management routing (called trunks). Routing of calls occurs across a number of methods typically sorted by “labels” in a technical process called MPLS (Multiprotocol Label Switching), determined at the billing, radio network, core network, and/or others. Logical compromise of the design models used in any of these will compromise the traffic as well, resulting in fraud, wiretap, and potential service outage.

An example of abuse of trunking is the use of telecom routing to perform a telephony DNS hijack to execute fraud and wiretapping. Since control of routing using telecom-side roaming controls is inherited by the device from the network (i.e., the device takes its orders from the network), the redirection of the device to a criminal network allows the criminal network (or criminal portable cell tower) to perform forcible routing of the device across the criminal network by changing its configuration to temporarily receive malware or surveillance from the criminal network. This can also be arranged to persist for a prolonged period of criminal control.

## Trunking



Note: The lines represent the path that telecom attacks including fraud can take.

Figure 9. Emergency call threat model

## Roaming

In roaming, intercarrier billing agreements for local or long distance traffic routing extend to cellular radio devices such as IoT devices and cellphones. Roaming is also a routing condition in which the device is told that the home network is unavailable, such that the device registers it as unavailable and then requests guidance from the closest network it can detect. If this guidance comes from a criminal network, the device will accept any criminal guidance it is told, if that criminal guidance is arranged correctly.

One example of fraud enablement is a man-in-the-middle (MitM) attack on the telecom path and/or mobile data path. This gives an attacker the ability to add to or modify the content of the transmission. This allows wiretaps, delays of online trading transactions (allowing arbitrage attacks on stock trades), insertion of data traffic (such as telemetry or malware), insertion of information (such as fake news), and others. This attack could be thought of as the telecom version of remote code execution.



## Roaming

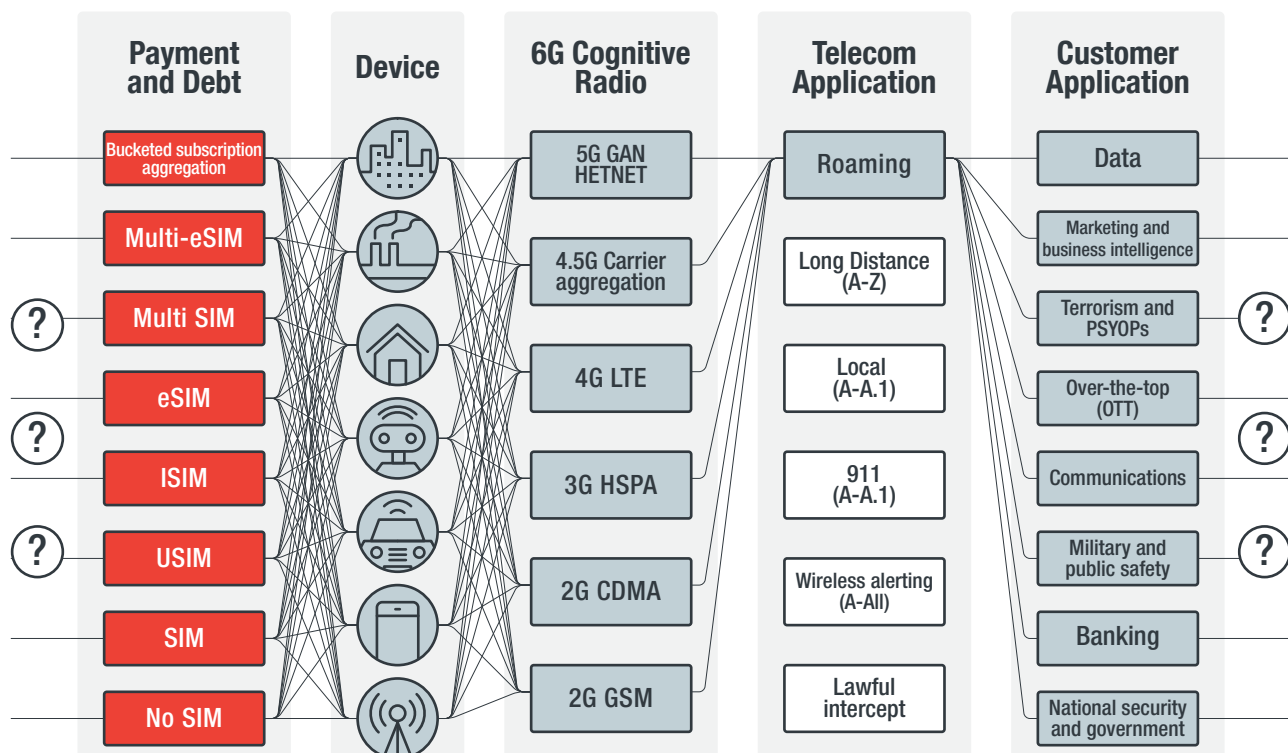


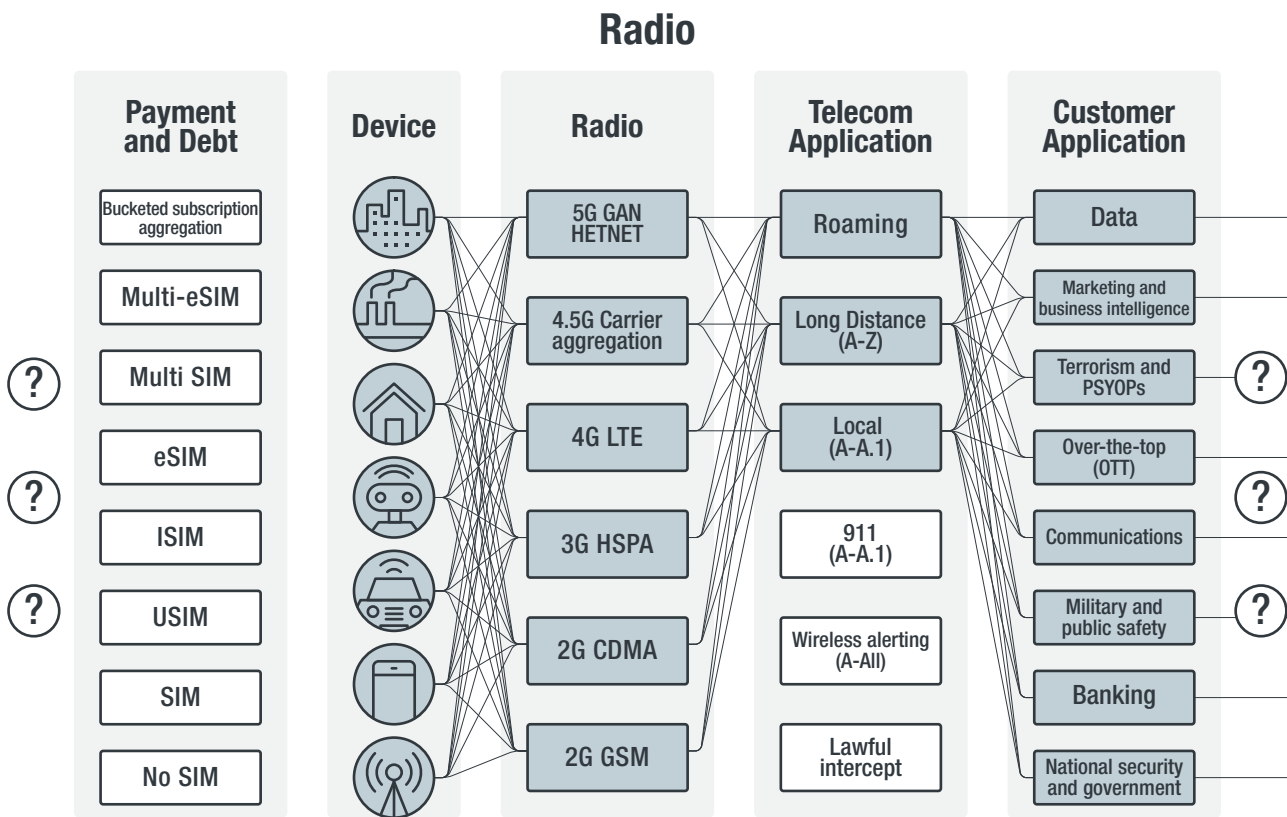
Figure 10. Roaming threat model

## Radio

Radio networks including cellular networks have much of their security designed for an era when criminals did not have financial or logistic access to cell towers and telecom equipment, the technical sophistication to operate them, or a strong enough criminal business case to sufficiently monetize their use. Attacks on telecom infrastructure were typically performed by state actors using intelligence techniques.

In the present day, however, the availability of equipment, training, staff, and money (criminal revenue) have all increased to the level that telecom hacking devices are available on the internet and capable of a degree of self-configuration. Furthermore, small book-sized cell towers can be bought from within the security domain of any of the most insecure telecom providers in the world, and then carried to the physical location of any other carrier in the world. These devices can be used to simultaneously hack roaming, trunking, IT, and radio while routing across a criminal network located anywhere in the world. (see the Appendix on war rigs). By purposely buying these devices from the least secure telecom deployments in the world, the security of the attack is low, but the network attack may be performed in a region from which high volumes of revenue can be obtained.

One example of this is the combination of the evil twin radio attack (increasing criminal broadcast power to drown out the real tower) and the anti-steering trunking attack (exploit of a roaming standard's loophole), combined with normal hacking methods. This combination uses a standards-level intercarrier trust vulnerability. This exploit of intercarrier trust forces radio edge roamers into a special case in which arbitrary (i.e., criminal-controlled) roaming is allowable. When criminals control roaming, they also control billing, allowing revenues to be stolen by either the fraudster or another carrier. By extension, when this attack is used on customers as individuals or groups, it results in the criminal gaining access to both the traffic of the customer and likely increases the debt the customer is intended to pay.



*Note: The lines show the path that telecom attacks including fraud can take.*

Figure 11. Radio and Roaming Anti-Steering threat model

# Physical Telecom Infrastructure Attacks Facilitating Telecom Fraud

The infrastructure of telecom networks is maximized for throughput, meaning it pushes massive amounts of very efficient high-speed traffic (calls and data). The means of accessing global telecom infrastructure is restricted at the “customer edge” by SIM cards. When attackers use a variety of basic frauds to gain control of SIM cards, they gain access to all the billing capabilities of the global telecom network.

The physical infrastructure of the network is most easily accessed through the use of a customer-edge device for the management of traffic. When criminals make their own criminal telecom infrastructure and route it across SIM cards, the intent of the infrastructure is effectively “authorized” by the carrier trust in their SIMs. This way, any criminal collection of devices pushing traffic across SIMs will be successful merely by being normally billable under one carrier, while any fraud performed is executed against another carrier in another country.

Since the domestic law enforcement agencies of the victim country cannot directly arrest the citizens of the country where the attack originates from, the criminals are effectively exporting crime and importing the financial/economic benefits of the crime, especially when the criminals spend locally. If the criminals are successful and spend a lot of money locally, their local government may even turn a blind eye to the activity while actively resisting international law enforcement efforts.

For these reasons, cultivating a relationship with international law enforcement is desirable since security response will always have a limited effect against infrastructures implicitly designed to look like customer traffic and trusted mobile carrier roaming partners.

## SIM Box Fraud

A SIM box device or simbox can hold hundreds of SIM cards and can route inbound traffic across voice over IP (VOIP) MitM to change arbitrary carrier metadata and forward the laundered call back out into the telecom domain and to the target burner phone. If each SIM is used only once, it defeats Lawful Access Production Order 1:1 paperwork procedures and approvals. Since these SIMs are used only once, this arrangement also functions as something of a one-time pad, which uses a one-time key. This method bypasses processes such as legitimate law enforcement wiretaps and Production Orders. SIM boxes are also capable of performing Intermarket Bypass Fraud similar to the above, defeating carrier surveillance that relies on a similar logic, as discussed below.



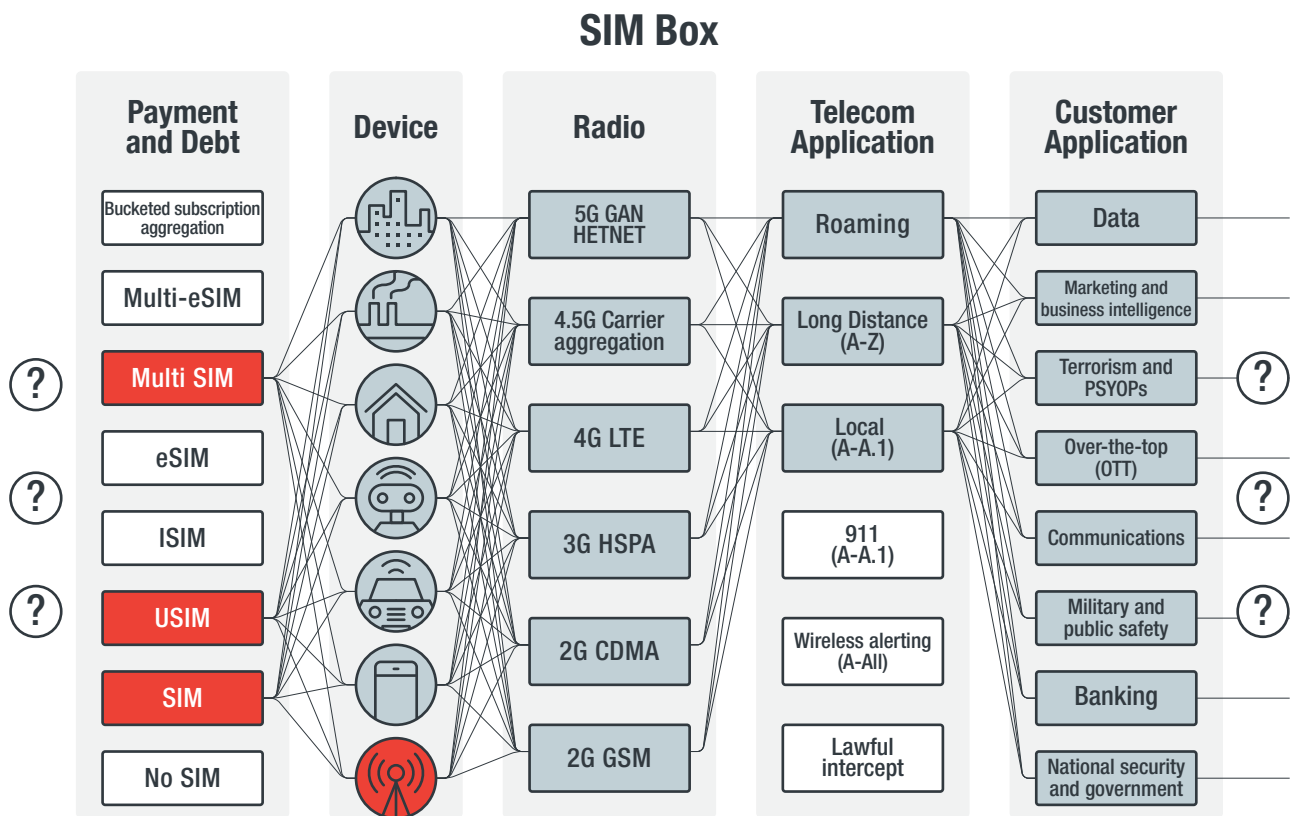


Figure 12. SIM box threat model

## International Revenue Share Fraud (IRSF)

IRSF is a general term for a number of frauds. Generically, the frauds in this group are characterized by the involvement of three parties: a) one victim from whom fraudulent billing or criminal revenue is taken through a variety of methods, and b) two sets of criminals, b1 being the “grey or white” money laundering function group for stolen billing or revenue, and b2 being a “black” function driving the CyTel hacking (or other functions including collusion or coercion) originating the fraud.



Figure 13. Money recovered by the Spanish National Police during an IRSF takedown

(Photo courtesy of the Spanish National Police)

Figure 14 shows the generic process followed in IRSF.

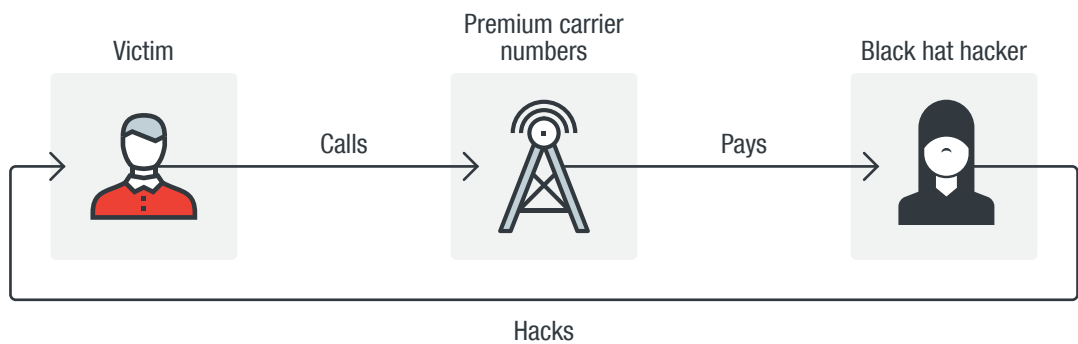


Figure 14. Generic IRSF

Within the telecom domain, IRSF follows a narrower group of practices, as shown in Figure 15.

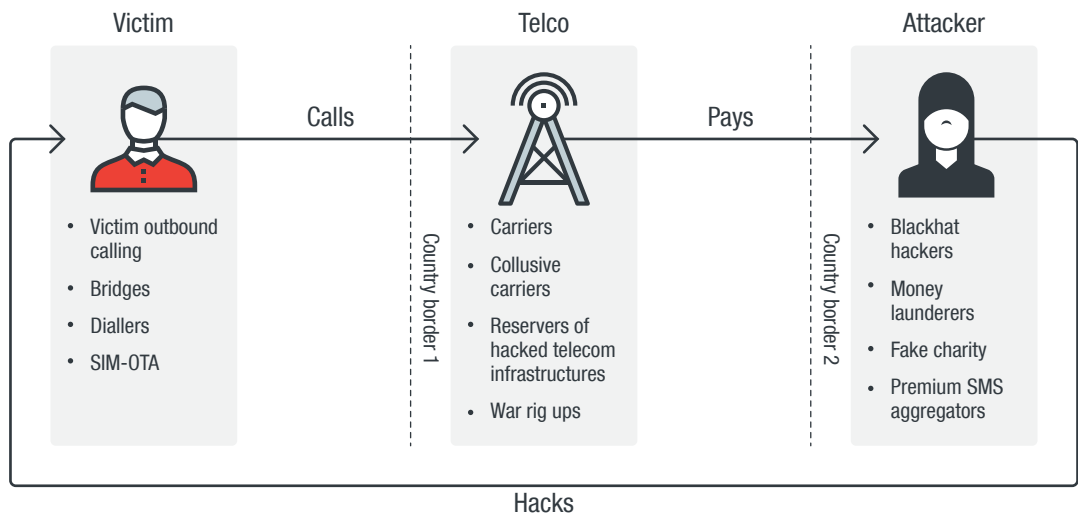


Figure 15. Generic telecom IRSF

The most common type of IRSF relies on BPC with the types of systems and their billing shown in Figure 16.

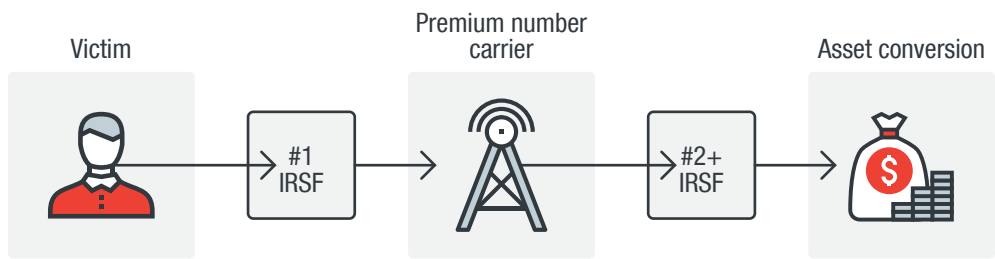
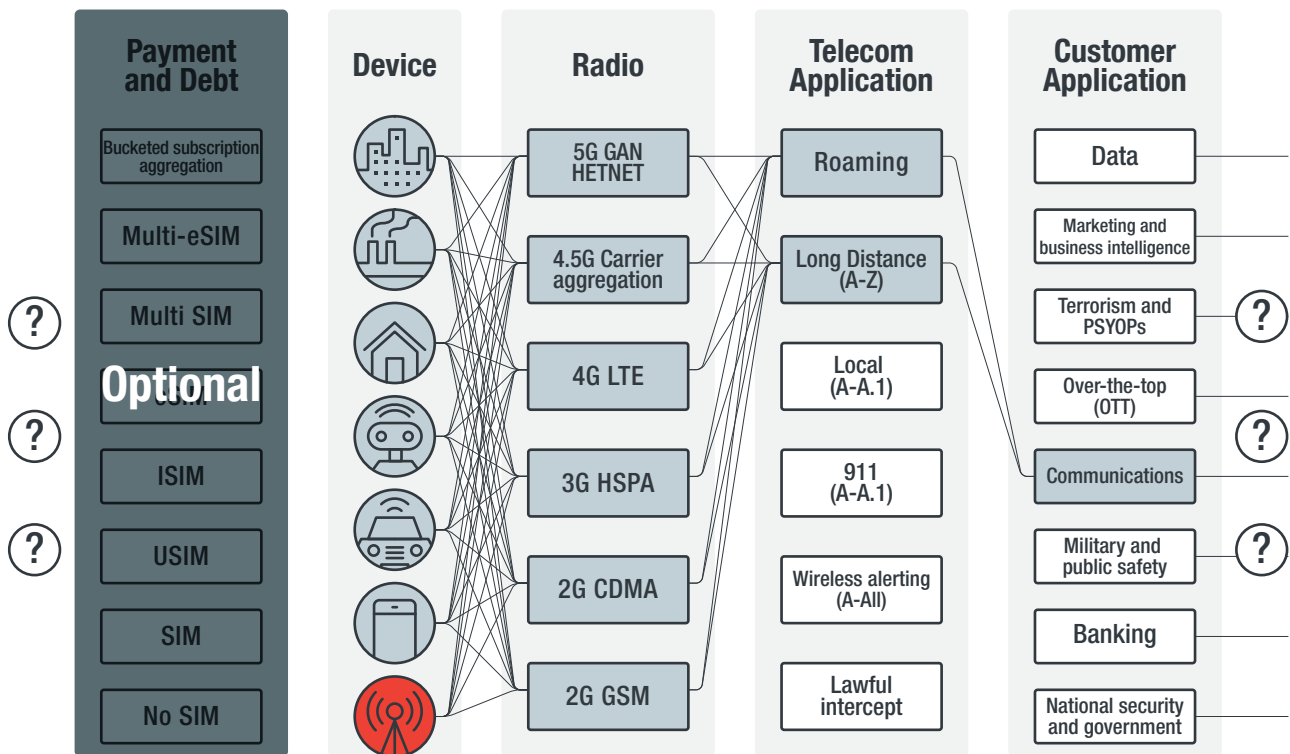


Figure 16. IRSF chaining obscures the provenance of criminal revenue, supporting money laundering

The origins of IRSF may be from one jurisdiction, and it can cross others and terminate in yet another, while being monetized across yet others.

## International Revenue Share Fraud (IRSF)



Note: The lines show the path that telecom attacks including fraud can take.

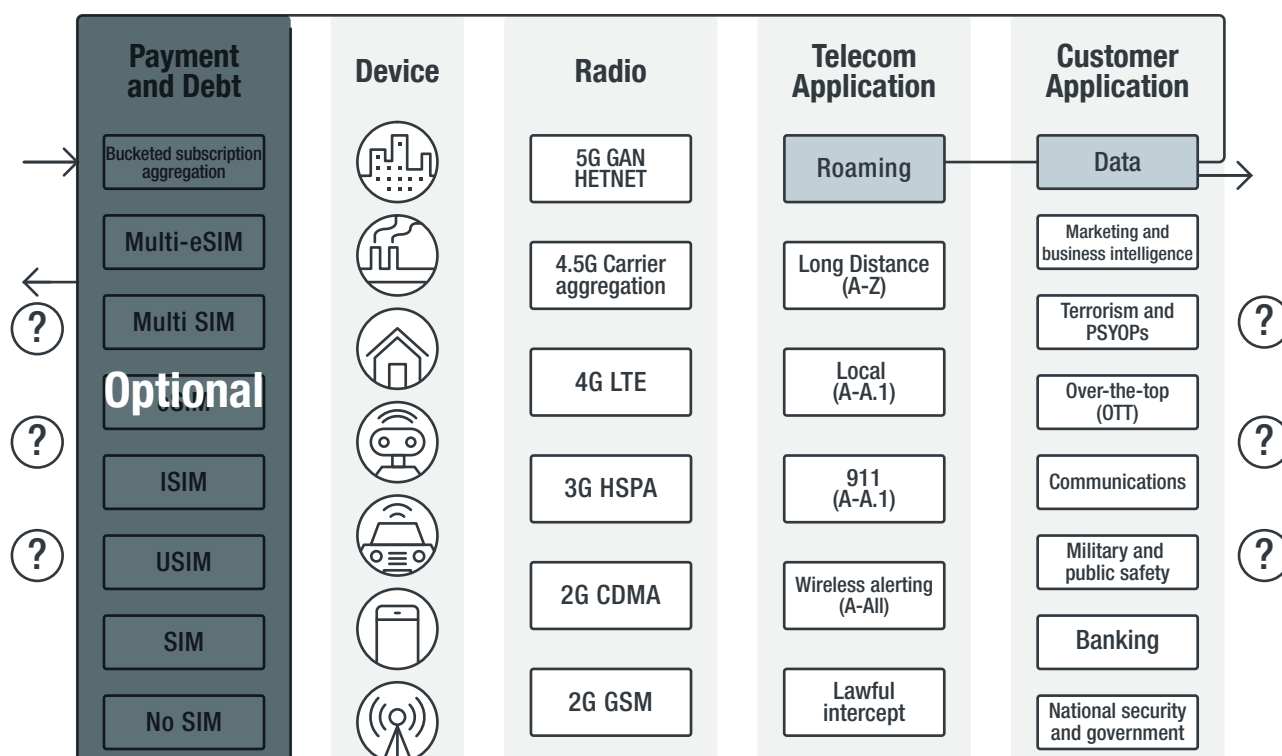
Figure 17. International revenue share fraud (IRSF) threat model

## Prepaid Charging Abuse

SIM cards are like credit cards and can be either *postpaid* or *prepaid*. As prepaid payment cards, the financial value represented by the card can be drawn down through use, and credited or “topped up” (using credit cards, or stolen credit cards for instance). Since the telecom sector is unregulated by money laundering controls, the value represented by SIM cards is invisible to the international banking and finance sector’s anti-money laundering audit controls (AMLAC).

Prepaid SIM cards are portable and anonymous means of transporting large amounts of criminal revenue. These prepaid accounts can be accessed from anywhere in the world using websites or telecom business process compromise (i.e., doing remote fraud against yourself as a means of money laundering), or by physically carrying a bag of topped-up high-value SIMs. SIMs are also small enough that many can fit in the base of a coffee cup or a gutted cellphone body. Obviously, they can also be carried in a phone or other IoT device in the proper slot.

## Prepaid Charging Abuse



Note: The lines show the path that telecom attacks including fraud can take.

Figure 18. Prepaid charging abuse threat model

## Intermarket/Interconnect Bypass Fraud

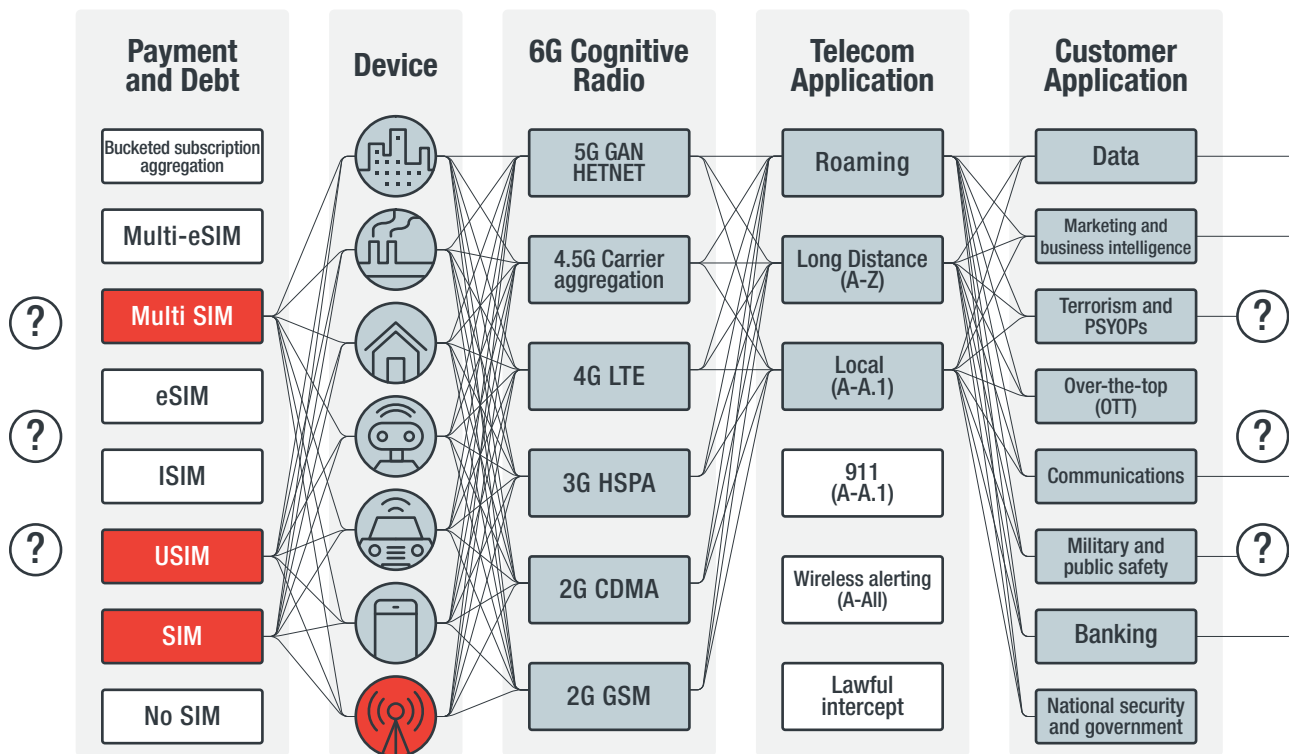
SIM boxes are devices capable of using many SIMs at once. A SIM box can be used for making calls, originating data, or sending SMS. When used to perform criminal activity, this device and its management are controlled by the criminal and it passes only the information the criminal intends, which does not necessarily include various identifiers and other login information used in typical IT security or antifraud filters.

According to an estimate by LATRO Services, fraudsters can easily generate over US\$100 per modem in a SIM box, and since one SIM box can contain 30 to 60 modems, this adds up to a US\$6,000 revenue loss per day or over US\$2 million per year.<sup>23</sup>

<sup>23</sup> Technology Research Institute & LATRO Services Inc. (2015). "Network Protocol Analysis: A New Tool for Blocking International Bypass Fraud Before Revenue is Lost." Last accessed on 13 February 2019 at <http://www.simprotection.com/MethodsUsedByOperators.aspx>.



## Intermarket Bypass Fraud



Note: The lines show the path that telecom attacks including fraud can take.

Figure 19. Intermarket/interconnect bypass fraud threat model

## Tromboning and Reverse Bypass Fraud

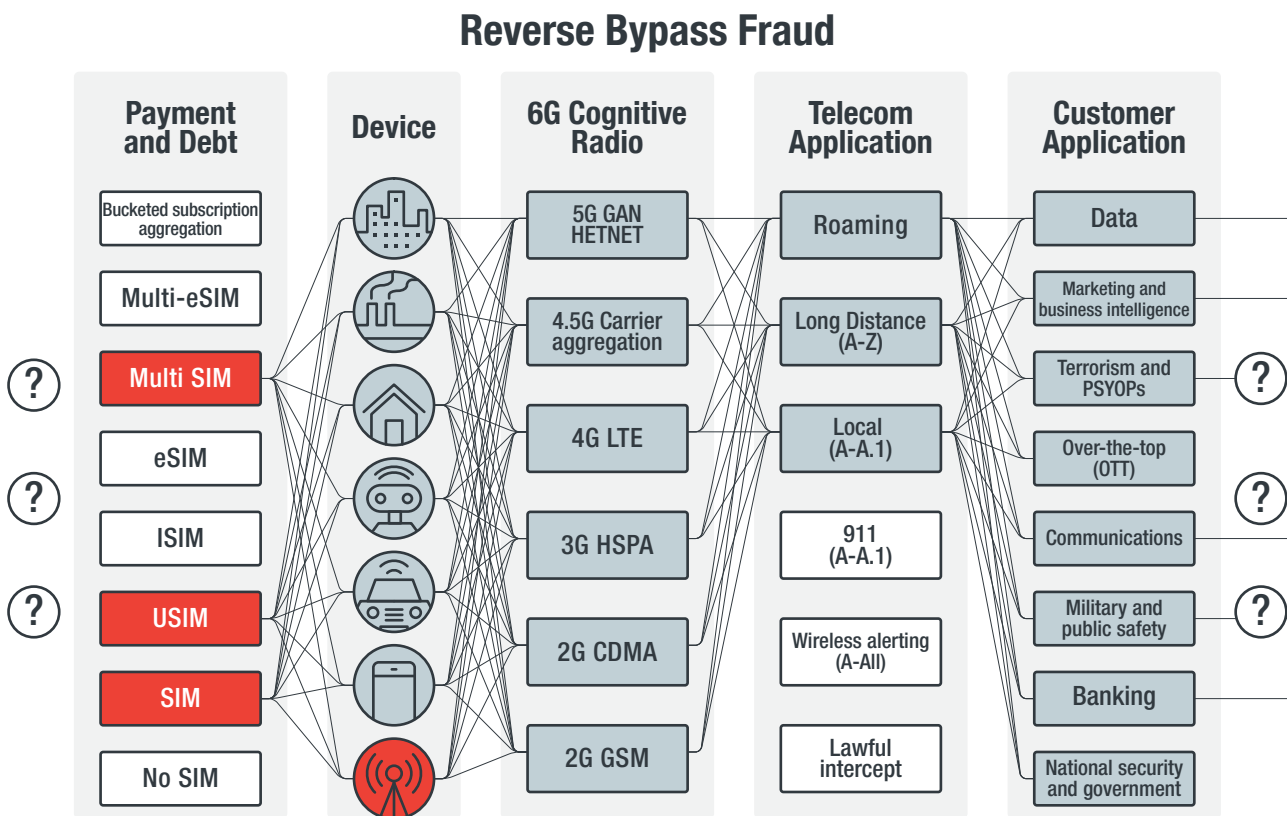
Within carriers are a number of ways of managing traffic to reduce cost and improve customer experience. These may happen before a call or during a call, and some of these may result in fraud.

Complication occurs when these call and (pre-call) network management techniques occur at the same time. If you as a reader have ever heard echoes of your own voice on a call, it could be true that you have been re-invited to a separate session of the same call, on a slightly different carrier network segment with a lower cost (i.e., is shorter and therefore faster). If the first (slower) call is not dropped properly by the network, you will have two calls going at once: a faster one and a slightly slower, original one. You will hear this as an echo. This practice of modifying a running call to make it faster/better is called tromboning, similar to moving the slide of a musical instrument toward its body to make the distance moved by the air inside shorter.

Tromboning occurs when a traditional circuit-switched network has a call set up by the public branch exchange (a switchboard-like router). After this call is set up in the circuit-switched part of the network, network resources may become available, allowing other, better routing (such as computer-based IP calls). As this is a cheaper method, this VoIP approach is preferred by the network's traffic management algorithms.

When attackers use publicly available CyTel hacking tools to “invite” themselves to a call, they can use the telecom infrastructure to call themselves or anyone else. If they use this functionality to call into an IRSF or other fraud operation, it will result in criminal revenue.

A wide range of hacker tools, for example, SIPvicious, which can audit VoIP systems that are SIP based,<sup>24</sup> are used in this attack, along with a range of legitimate telecom equipment.



*Note: The lines show the path that telecom attacks including fraud can take when reverse bypass is used.*

Figure 20. Reverse bypass threat model

<sup>24</sup> SIPvicious Pro. (n.d.). *SIPviciousPro*. Last accessed on 13 February 2019 at <https://sipvicious.pro>.

# Network-based Telecom Fraud Attacks

## Private Branch Exchange or PBX Hacking

A PBX is a computer responsible for routing revenue-generating traffic and, therefore, represents money to any attacker. Through the use of online searches or lists purchased from hackers, PBXs can be found and attacked using common methods. They are often protected by nothing but a default or potentially weak user-generated password.

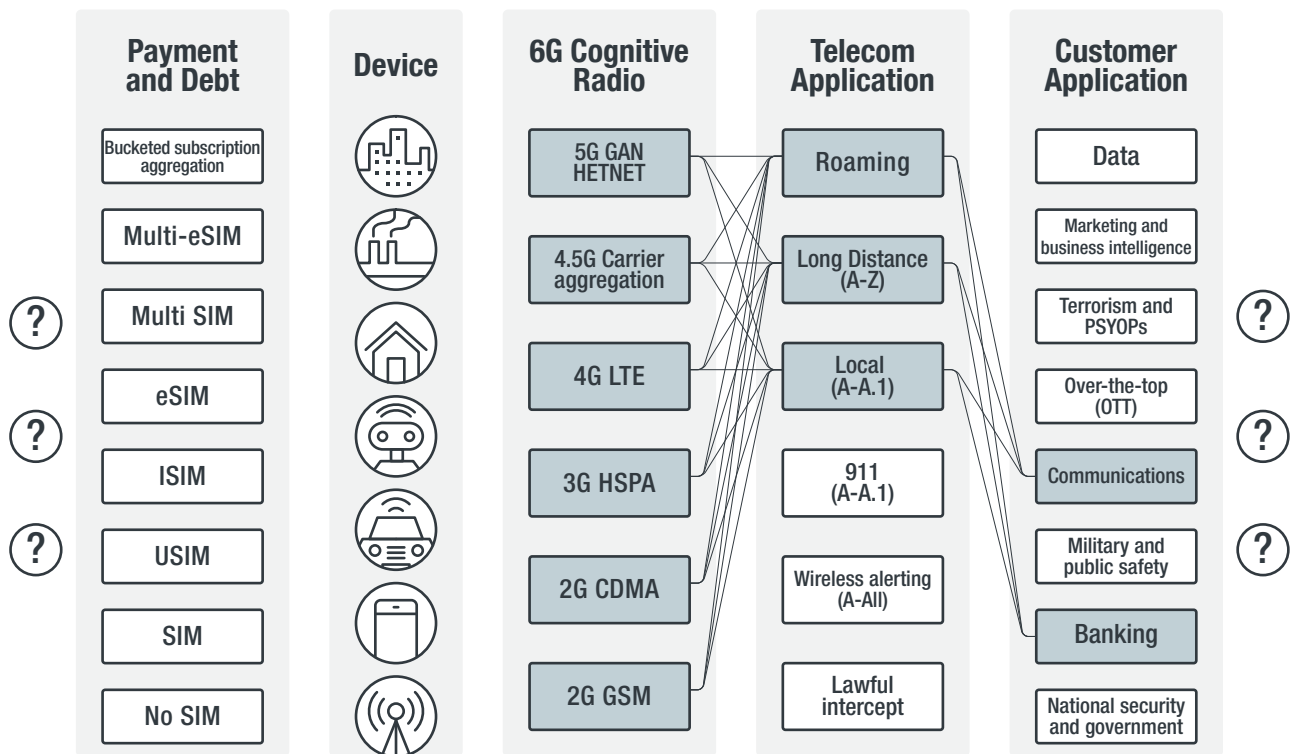
When this password is cracked, the attacker will have control over all the traffic passing through the system. CyTel hackers usually attack during off-hour periods to prolong the duration of the attack and therefore increase how much revenue they can gain.

The usual fraud method is for the attacker to redirect the calls initiated from within the PBX-controlled network to premium numbers controlled by the attacker such as those offered in certain online forums.<sup>25</sup> To keep the premium number from being cancelled and their revenue seized, criminals normally maintain these premium numbers in a separate country from the one being attacked, purposely leveraging gaps in CyTel carrier and law enforcement collaboration. Since the carrier providing premium number services and billing generates revenue from the attack, they are financially motivated to allow it to continue for as long as possible. In this way the attack becomes IRSF.

---

<sup>25</sup> Karlatama. (24 February 2014). *Black Hat World*. "Are you working with international premium rate numbers?" Last accessed at 13 February 2019 at <https://www.blackhatworld.com/seo/are-you-working-with-international-premium-rate-numbers.652902/>.

## PBX Hacking



Note: The lines show the path that telecom attacks including fraud can take.

Figure 21. Private branch exchange (PBX) hacking threat model

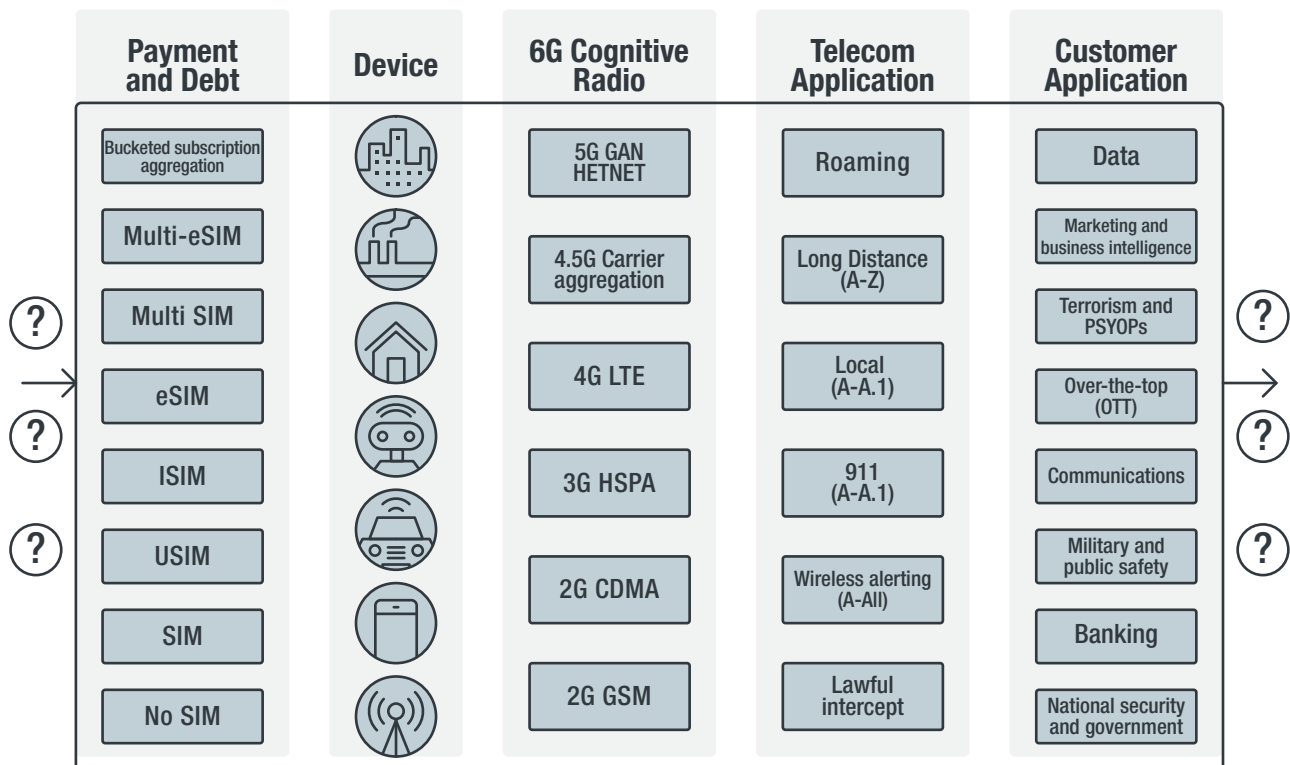
## Subscription Fraud

Subscription fraud is the use of BPC to gain access to the same level of control over a customer subscription as the customer's. This control of a consumer or enterprise subscription is then used to control the billing relationship between the customer and the carrier. It is common that the first action taken with this newfound control is to change the account password and remove the true customer from the account.

Subscription fraud involves hijacking an existing account, while the subset called initial subscription fraud involves creating brand-new fake "customers" from nowhere. Initial subscription fraud (also called synthetic subscription fraud) is very insidious since it exploits the fact that a carrier knows nothing at all about a brand-new, never-seen customer and has no method of establishing the reputation of someone the carrier has never met before. Initial subscription fraud is one use for stolen identities and identity information stolen as the result of privacy breaches and the hacking of customer databases. This identity information may be sold many times for a variety of purposes and reused across multiple carriers to originate a variety of frauds.



## Subscription Fraud



Note: The lines show the path that telecom attacks including fraud can take.

Figure 22. Initial subscription fraud threat model

## Wangiri

The word “wangiri” is a Japanese cultural reference to the samurai feat of skill in which a blade is drawn from the sheath and in the same single motion, the samurai cuts down his enemy. Wangiri literally means a “one cut win.”

In Wangiri fraud, an automated fraud infrastructure or autodialer calls many people, allowing the victim’s phone to ring a single time only. The victim, without looking at the number, calls it back and becomes the originator of the call (and therefore the one who has responsibility to pay for it). The number the victim calls is typically a premium number, which may trigger immediate billing, or if combined with other scams, keeps the caller on the line for as long as possible.

## Wangiri

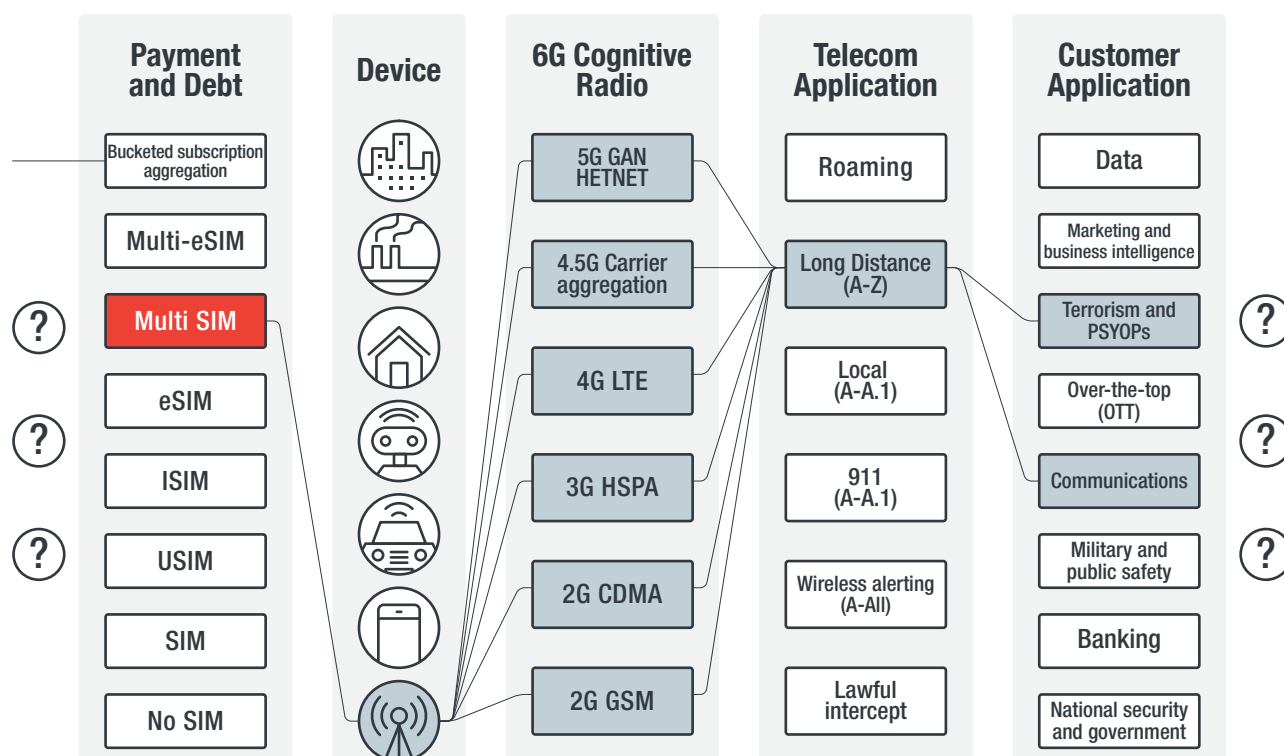


Figure 23. Wangiri threat model

## Voice Phishing/Vishing

Phishing is a social engineering technique used to trick people in a large-scale campaign of repeated and often automated messages. When targets respond to the trick, they respond by giving money, resources, or access to the phisher. These messages might be an SMS, email, instant message, paper mail, voicemail, human callers, or even voice chatbots that will speak back to the victim. Voice phishing or vishing specifically refers to phishing carried out verbally.



Note: This was one of twenty similar vishing call centers taken down in Spain in which the predominantly Taiwanese criminals launched vishing crime from Spain into China.

Figure 24. A vishing call center part of the WALL Operation

(Photo courtesy of the Spanish National Police)

Voice phishing is relatively a costly and laborious crime, and requires some sophistication and carrier knowledge to automate. For this reason, it is typically reserved for gaining access to high-value resources. Vishing is used to gain access to credit card numbers, but more commonly it is used to gain access to the victim's phone account or bank account. It may also be combined with identity theft for even more invasive and damaging attacks.



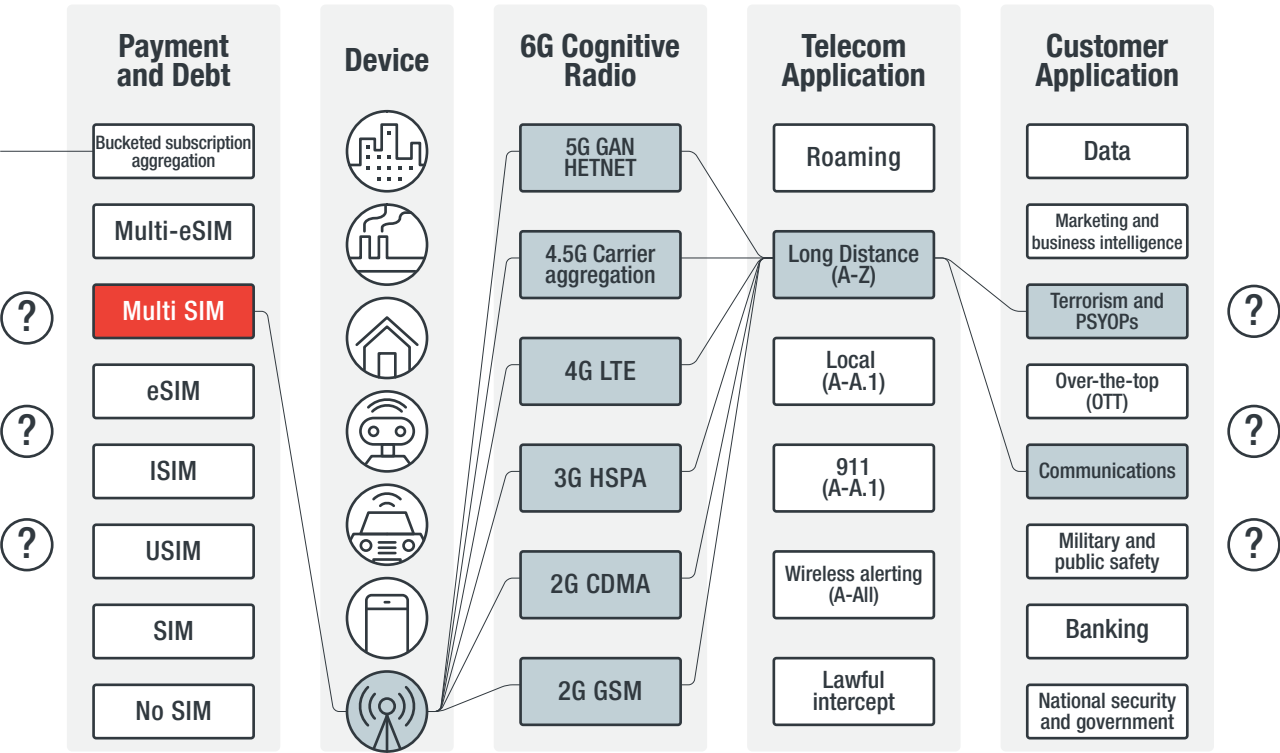
*Note: The writing on the side of the pistol reads "Desert Eagle,"  
a powerful .50 calibre handgun capable of piercing most body armor.*

Figure 25. A firearm recovered by the Spanish National Police during a vishing sting  
(Photo courtesy of the Spanish National Police)

Surrounding techniques such as caller ID spoofing (also called CLID spoofing) allow the calling attacker to look as if the call is coming from the victim's bank, a government office, a reputable private company, or a local number. By posing as one of the aforementioned, the suspicious "international" component of the fraud is hidden, until the fraud manifests as one — or as crimes such as IRSF or domestic revenue share fraud (DRSF).

Black flag voicemail spam and secondary blacklisting is also a concern. This refers to the breach of a carrier's voicemail that allows the sending of large-scale vishing or fraud, knowing the activity will get the carrier's number range blacklisted. If the criminal's intent is to get the numbers of a specific victim blocked, using fraud to manipulate carrier call-blocking procedures would achieve this.

# Voice Phishing/Vishing



Note: The lines show the path that telecom attacks including fraud can take.

Figure 26. Voice phishing threat model



# Noteworthy Real-World Cases of Telecom Fraud

Each of the following real-world cases has been anonymized and made generic to reflect that the fraud schemes work in most countries and under most carriers, to protect ongoing investigations, and to protect the identities of minors.

## Case A: Radio Shadow Ring (IRSF Fraud)

### Background

When an RF engineer suspected human interference (i.e., criminal activity) she notified her carrier's corporate security. Due to the complex nature of the event, a corporate enterprise security architect was assigned to look deeper.

The phone numbers dropping calls were analyzed, and all dropped calls belonged to a single phone number—a nontraditional telephone device fax-modem-like IoT device. The customer was also a wholesaler.

Consultations with the police identified the need for evidence from the “victim” phones that were attempting 911 calls and failing, under circumstances likely to have resulted in the death of the 911 callers. At a deeper level, this resulted in the need to go undercover and perform a “cold buy” of several cellphones and SIMs from the suspected organized crime office.

The architect partnered with a carrier fraud investigator and both visited the site using assumed undercover identities.

When customer onboarding paperwork began, other points of interest were found:

- The contract required “employees” (customers) to use the phone in making long distance calls. The customers were charged inflated fees, including long distance fees for international calls. The fees for these international calls were inflated using several fraud methods, including DRSF relay, IRSF, wholesale fraud, supply chain fraud, vendor fraud, subscription fraud, complex kiting, and other fraud techniques.

- The carrier sales staff (the employees of the national carriers) received enough sales volume for the activity that they were financially motivated to resist requests to sever the relationship with the suspect organization. A consequence of this resistance allowed their sales revenue, sales quotas, and personal bonuses to grow. Real financial benefit was a consequence of resisting the shutdown of the suspect accounts. It can be argued the intent to benefit from fraud through lack of cooperation with the investigation (before or after the fact) was itself criminal.

After gathering the information above, it was discovered the attack had followed the model below.

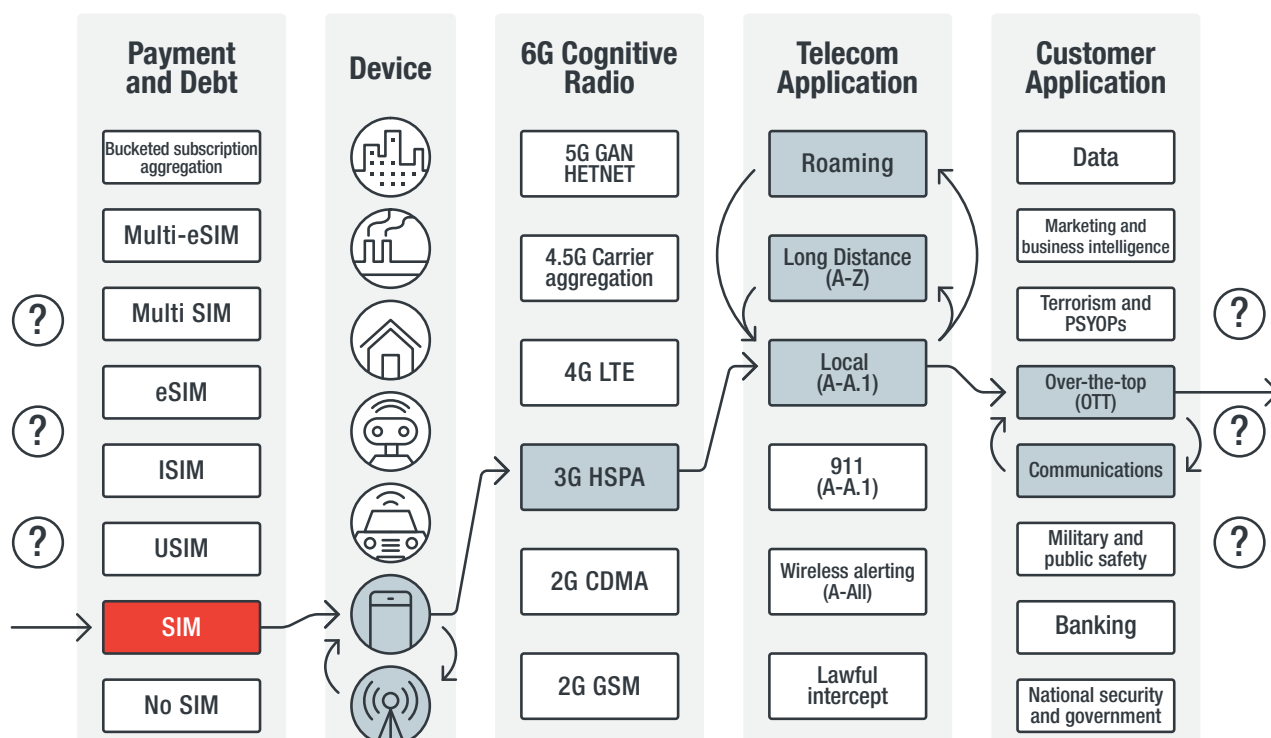


Figure 27. Radio shadow ring threat model used in the series of attacks

## How is this IRSF and/or DRSF?

Three parties are involved in a revenue share fraud scheme: the victim (A), the carrier (B), and the black hat or criminal organization (C). In this case, the customers (A) were targeted with social engineering to participate in a BPC scheme for the purpose of gaining illicit funds for the criminal organization (C), which pays part of the stolen funds to the carrier (B).

When the victims are local, they participate in DRSF. Much of the crime performed by the organization in this case was DRSF. When the victims travel to or are located in another country, they participate in IRSF. The victims travel to other countries and originate calls for which they have been social engineered through the use of this BPC (the fraudulent onboarding process), or are compromised directly through the use of voice phishing, Wangiri, or IPRN fraud, and others.

# Case B: International Fraud by a Teenage Drug Cartel

## Background

A business analyst in a Canadian telecommunications company noticed a large amount of duplicate data in a corporate production system, specifically customer street addresses. A carrier's corporate enterprise security architect was approached. An innovative and scalable model for an international drug cartel was discovered, one that was being operated by a 15-year-old boy.

It was eventually learned that the criminal was using a variety of frauds, including IRSF and money laundering, for the sake of realizing the criminal revenue from the group's tiny cartel. It is assumed from the elegance of the cartel's design that it was a part of an undiscovered whole.

## The Story

Customer data records indicated that many SIMs were registered to phones whose owners lived in a single address. Further fraud investigation into the results of the cyber-telecom intelligence fusion showed several findings.

A telecommunications investigator visited the occupant of the residence at the suspicious address. The resident apparently knew nothing of the nature of the crime or its details. The logged locations were compared to a street map. The resulting "pin map" matched three specific transit bus routes. It was observed that each address was immediately beside a bus stop.

Further investigation and intelligence analysis showed the owner of all the drug addresses to be a single person whose false Facebook profile led to a true Facebook profile identifying the individual as a 15-year-old boy who was using the pattern of crime he had designed to create "drug dealer starter kits" as a kind of anonymous "franchise."

Each starter kit was composed of a freezer bag containing a prepaid card, a SIM card, a phone, money to use for small drug buys (small bills), and a commercial amount of the requested drugs.

Further intelligence synthesis showed that the suspect made extensive use of online gambling (a common means of money laundering). Many small balances from various SIM accounts were aggregated into these online gambling accounts. Results of the high-volume gambling were transferred to PayPal and other online payment methods. These were used to perform prepaid top-ups, and outbound SMS charitable "donations" were made from these SIM accounts. Many large charitable SMS donations were made to charitable SMS aggregators in the U.K.<sup>26</sup>

**NOTE:** Charities and fake charities are also means of money laundering. Short-code SMS charity premium numbers are also used to move money out of financial systems into telecom systems, where it can then be moved around the world in a way invisible to bank-side anti-money laundering controls.

<sup>26</sup> Marco Giannangeli. (25 April 2005). *The Telegraph*. "Mobile firms 'take quarter of text charity donations'." Last accessed on 13 February 2019 at <https://www.telegraph.co.uk/news/uknews/1488624/Mobile-firms-take-quarter-of-text-charity-donations.html>.

In the U.K., the SMS charity payment aggregator gathered multiple phone numbers of inbound criminal revenue, tallied them, and transferred them to financial accounts. This was another step in the money laundering process and also had the criminal benefit of allowing the money to cross from one country to another (from Canada to the U.K.), and one technology regime to another (banking to telecom to banking).

The bank accounts attached to the charity aggregator had been attached to new phone numbers. IRSF was used against these new phone numbers to again draw the balance of the accounts across technologies (banking to telecom to banking) and across borders (in this case, from the U.K. to Dakar).

From this point, the carrier investigator lost the trail due to a lack of cooperation between the Canadian carrier and the bounce carrier in the U.K. and, more specifically, insufficient investment in relationship building with international law enforcement agencies.

## Conclusion

Telecommunications investment is critical in supporting proactive law enforcement relationships, a collaboration of the kind that can support investigations like this. Without this investment, specialized law enforcement support will not be available to provide guidance in carrier intelligence fusion to produce the needed evidence, as was the case here. For example, when the investigation terminated in Dakar due to decreasing carrier support, there were no other allies to draw on and the investigation failed — something investment in law enforcement agency collaboration by the carrier would have addressed.



## Conclusion

Current trend indicates larger and more scalable attacks, the solidification of threat actors, decrease in the sophistication and cost of necessary telecom equipment, and the substantial increase in telecom fraud. As proof, these are key topic at top-tier hacker conferences.

The emphasis at hacker conferences are on the low-risk ease of attacks, the financial revenue from attacks, interesting information learned as a side effect of attacks as all motivators for this uptick in cyber-telecom attacks. Additional motivators drawing attention to this class of attack are the very lucrative employment opportunities for individuals with CyTel security/hacking/fraud skills. At the time of writing, a senior individual might be offered US\$250,000 and an additional US\$150,000 in bonuses and equity, for a total of US\$400,000 in salary. In Europe, a consultant might be offered 2,000 euros daily. With the ubiquity of telecom networks and the inability of gaining legitimate access by anything but employment, the obvious approach (in a hacker's mind) would be CyTel fraud.

Telecommunications companies should provide the needed types of support, training, and investment to engage entities like the Europol EC3 CyTel working group. In this group, intelligence and techniques can be shared for the greater good. Non-European entities and national law enforcement groups have joined as well, and benefit from the reduced effort and complexity in performing law enforcement actions. Telecommunications companies use this forum to reduce the effects of fraud and CyTel crime both in Europe and abroad.

The concept of a global telecom network with unified threat intelligence between telecommunications service providers, between law enforcement, and between providers themselves, is a critical part of the Cyber-Telecom intelligence fusion. It doesn't stop there, however — these frauds are often complex. Other Europol criminology- and intelligence-sharing groups such as Airline Fraud (Global Airline Action Days) and Euro Money Mule Action (EMMA) operations overlap as well. These kinds of collaboration are necessary to keep telecommunications networks functional in an era of escalating voice telephony abuse costs. When multibillion dollar classes of fraud both proliferate among criminal groups and become scalable due to the abilities of 5G, the need to work together for the benefit of all will have never been greater.

# Appendix

## War Rig

A telecom war rig is a network of interconnected hacker war boxes (sanitized “hacking only” computers) composed of different controlling telecom equipment types. Recently, the cost of telecom equipment has decreased to the point that individuals can launch such attacks. These devices are connected as shown below, with the dotted lines indicating a man-portable container. The below could be considered a miniaturized Cell on Light Truck (COLT) or Cell on Wheels (COW), with additional hacker functionality. This additional functionality allows it to mimic the functions of a satellite ground station as needed to facilitate portions of many of the attacks described in this document as well as others.

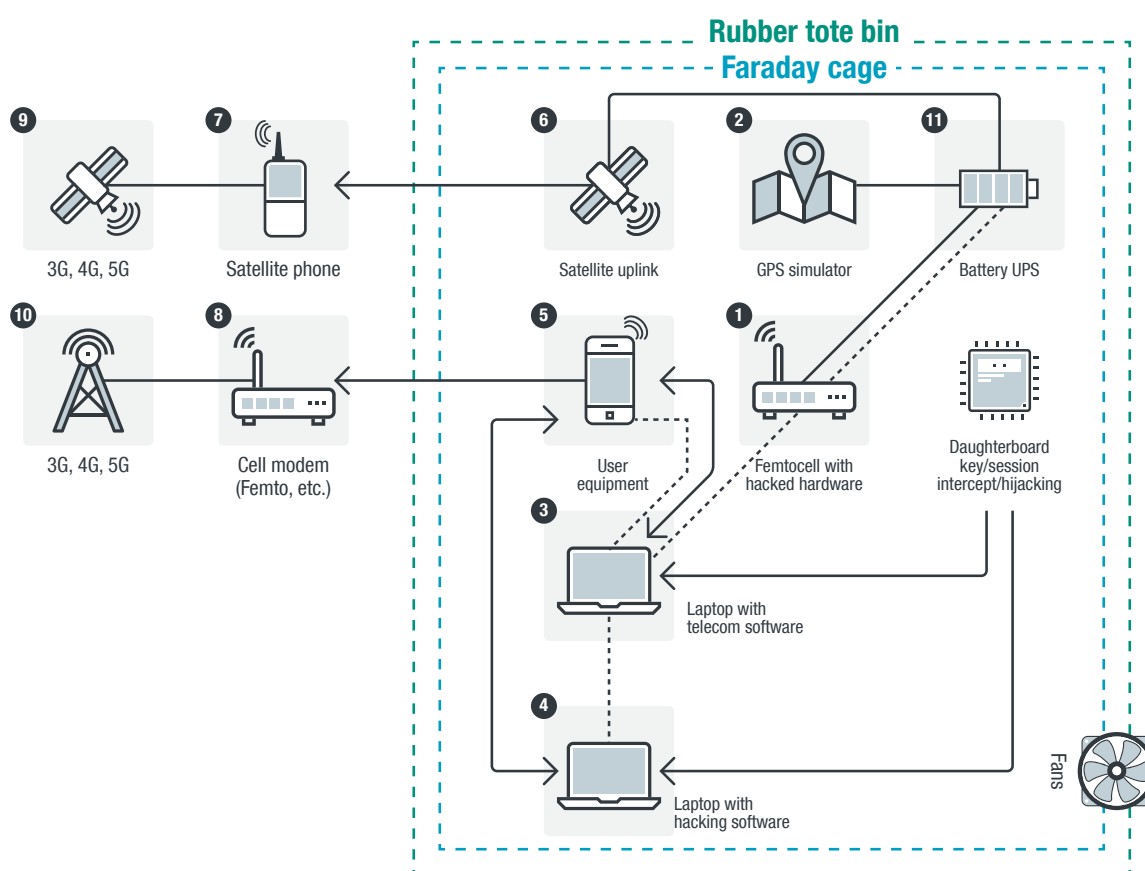


Figure 28. War rig supporting many voice telephony abuses

War rig elements and war box components include the following:

1. Radio war box – A femtocell with hacked hardware, which allows arbitrary information to be fed to and from the user equipment (UE) such as a phone or IoT device. This arbitrary information can be carrier-specific, radio-specific, or device-specific. The development of the war boxes can be very specific to a particular carrier, region, fraud, or victim demographic. It can also be made to be very open and capable of opportunistically attacking everyone who is within its range of targets (frequency and radio broadcast range).

2. GPS war box – A GPS simulator, which allows arbitrary information to be fed to the UE and provokes a change of state such as roaming and falsification of the apparent location that the attack is originating from (hiding the location of the attacker). Its primary use is commercial, where it is used for a variety of purposes including the calibration of high-performance equipment, including competitive race cars, fighter jets, and commercial airliners, among others.

There are two classes of this device, simulators and spoofers. GPS spoofers are devices that follow the format but not the context of a true GPS satellite's Wide Area Radio Network (WARN) feed.

Certainly, even the most basic sanity testing will detect a basic device like a GPS spoofer. They may be very simple and low-cost devices made from parts such as cookie tins or other metal food containers. GPS simulators, on the other hand, are sophisticated devices worth tens of thousands of euros. Simulators are used for calibrating other even more expensive equipment, including battleships. A simulator provides the attack with all of the information it needs, including arbitrary information such as:

1. Arbitrary date and time (back to mid-1980s)
2. Point in time location (target is at location A)
3. Time series location (target went from location A to B to C to D)
4. A combination of the above-mentioned information creating “a story in time and space.” When the above are combined, the attack can say (falsely or accurately at will), that portions of the attack:
  - Originated in a particular place (provoking roaming behaviors or arbitrary network routing across known-as-insecure telecommunications networks).
  - Travelled at a particular speed down a particular road, and stopped at specific locations (like intersections or traffic lights), which lends credibility to the technical story told by the activity of the war rig.
  - Continued to another location far away from the attacker's location (possibly to support an alibi).
  - Further location-based authentication and billing. Simulators have been used to falsify telemetry for the purpose of inflating location-based advertising revenue.
  - Breaking connection to a location. Even GPS spoofers can falsify house arrest bracelet location restrictions.<sup>27</sup> More advanced bracelets are defeated by simulators.

---

<sup>27</sup> Lorenzo Franceschi-Bicchieri. (9 August 2015). *Motherboard*. “How Hackers Could Get Out of House Arrest.” Last accessed on 13 February 2019 at [https://motherboard.vice.com/en\\_us/article/ypw7yv/how-hackers-could-get-out-of-house-arrest](https://motherboard.vice.com/en_us/article/ypw7yv/how-hackers-could-get-out-of-house-arrest).

Note that GPS is an American Military proprietary network with both an encrypted military channel and an unencrypted channel often thought of as the “civilian” channel (despite also being military, but ubiquitous and free). Devices that do not use GPS use other types of global navigation satellite systems (GNSS) such as GLONASS,<sup>28</sup> Galileo of Europe,<sup>29</sup> BeiDou of China,<sup>30</sup> or other satellite location-based services (LBS).

5. Telecom war box – A laptop with telecom software, which provides a sense of “reality” and technical consistency to the changed state of the mobile device. This device will vary slightly with the nature of the target network but will generally carry telecom software such as Asterisk,<sup>31</sup> OpenBTS,<sup>32</sup> and base station controller<sup>33</sup> software.
6. Traditional IT war box – A laptop with hacking software, which collects, sorts, and manages data generated by the attack. The content of this war box may vary with the preference of the attacker, but generally will have suites of operationalized hacker intelligence, network management, and security software. Other software related to planning -and strategy will be located on a separate external non-operational system.
7. Victim (“user equipment”) – One or more mobile devices such as those connected to the IoT. Note that the victim phone or IoT device (UE) can be outside the war rig’s radio-proof shield (Faraday Cage) (represented by the dotted line) to perform bulk attacks against people or devices within range.
8. Satellite war box – A satellite uplink, which routes the attack across satellite infrastructure to provoke a telecom billing response from the telecom network on the other side of the satellite. The satellite war box uses native functionality of the uplink and satphone (along with legitimate credentials if needed for a specific attack) to force the path of the attack across telecom network infrastructure for which standards-based security infrastructure may not exist, or for which the means of exploit may have been public for years or decades.

Note also that the involvement of satellite functionality and routing includes features specific to satellites, such as the ability to broadcast across a broad geographic area without identifying specific targets. This way, victims may be spread across a large area. More specifically, the location of the war rig itself may be very hard to geolocate since it not only can be situated anywhere under the satellite but also may move from place to place between uplink transmissions.

---

<sup>28</sup> Hexagon. (n.d.). Hexagon Positioning Intelligence. “GLONASS.” Last accessed on 13 February 2019 at <https://www.novatel.com/an-introduction-to-gnss/chapter-3-satellite-systems/glonass/>.

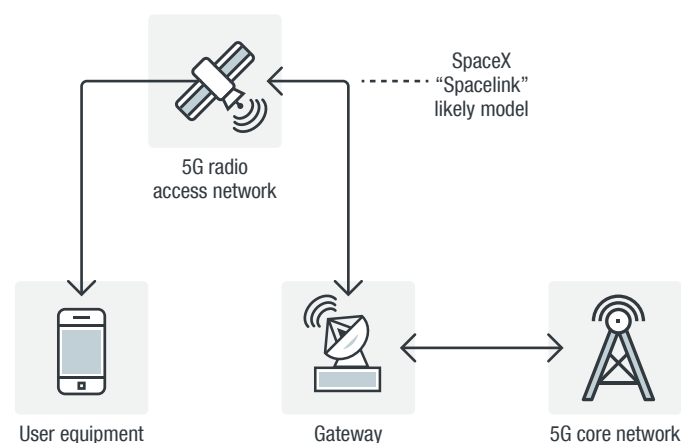
<sup>29</sup> European Global Navigation Satellite Systems Agency. (n.d.). *European Global Navigation Satellite Systems Agency*. “Galileo is the European global satellite-based navigation system.” Last accessed on 13 February 2019 at <https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system>.

<sup>30</sup> BeiDou Navigation Satellite System. (n.d.). *BeiDou Navigation Satellite System*. Last accessed on 13 February 2019 at <http://en.beidou.gov.cn/>.

<sup>31</sup> Asterisk. (n.d.). *Asterisk*. Last accessed on 13 February 2019 at <https://www.asterisk.org/>.

<sup>32</sup> OpenBTS. (n.d.). *OpenBTS*. Last accessed on 13 February 2019 at <http://openbts.org/>.

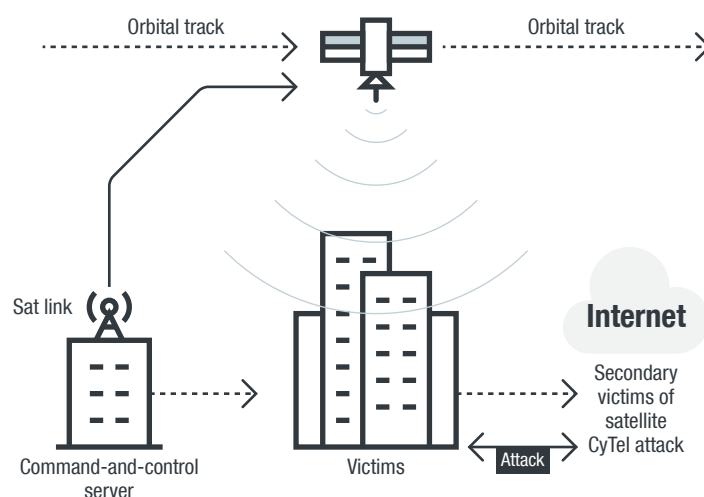
<sup>33</sup> Gartner. (n.d.). Gartner. “Base Station Controller (BSC).” Last accessed on 13 February 2019 at <https://www.gartner.com/it-glossary/bsc-base-station-controller>.



*Note: The gateway in this case may be a telecom war rig initiating attacks directly on satphones and therefore conducting satphone billing as well as other attacks including fraud.*

Figure 29. One path an attack on satellite phones may take for the sake of creating direct impact<sup>34</sup>

The means of exploiting this has been seen in the wild through a variety of vectors. Perhaps the most well-known of these is Turla.<sup>35</sup>



*Note: The Turla threat actor group uses satellite routing to hide the point of origin of the attack, allowing precise but distributed control of many victims.*

Figure 30. Turla CyTel attack threat model using satellite telephony abuse

<sup>34</sup> Craig Gibson. (11 June 2018). *Trend Micro Security Intelligence Blog*. Last accessed on 13 February 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/>.

<sup>35</sup> *Ars Technica*. Last accessed on 13 February 2019 at <https://arstechnica.com/information-technology/2017/06/russian-hackers-turn-to-britney-spears-for-help-concealing-espionage-malware>.



9. Satellite phone — A point to launder data as it goes back to the telecom network. Satellite phones or satphones are the large cellphone-like devices capable of communicating directly with space. Satphone operators are subject to the same frauds that cellphones are, although the various telecom names and devices may have different names. For example, hardware at the base of a cell tower is called a base transceiver station (or BTS) while the same device in the satellite domain would be called an Earth station or ground station. The IoT device in the cell tower example would be either a cellphone or an IoT device, while the IoT device in the satellite example would be the satellite itself (similar to a “mobile hotspot” passing traffic through itself).

Example satphones are those using the Iridium<sup>36</sup> telecom satellite network. These satphones are intended for primary use with satellites when cellular coverage is unavailable or undesirable in the case of people frightened of the local government’s wiretap capabilities, such as journalists, intelligence officers, or criminals. These satphones may use SIM cards from traditional telecommunications providers, which may also support traditional roaming using other internal traditional cellular telecom antennas which are used whenever a traditional (cheaper) terrestrial telecom cell tower is available.<sup>37</sup>

10. Cell modem, femto, etc. — These allow arbitrary information to be fed to the telecom network. The attacker may include some or all of these in their war rig. Cell towers are designated by the size of their broadcast “bubble,” with book-sized femtocells being most physically convenient for an attacker to use. These are consumer-grade devices that may be obtained from anywhere in the world and are typically chosen from the least secure carrier for the sake of easy manipulation of global routing.

The target networks drive what interface to obtain from the target network operator. The networks are described here, arranged from largest to smallest):

- A global area network (GAN) is for the global satellite network covering the Earth, and the broadband global area network (BGAN) specifically describes the part of that network capable of serving satellite data.
- A wide area radio network (WARN)) usually describes the coverage area of a single satellite.
- A public land mobile network (PLMN) consists of the combined land-based cell tower coverage of all the mobile service providers in the world. The coverage is similar to land mobile radio (LMR) and the radios commonly used by police and armed forces.
- A macro cell tower is a common true cell tower, fixed to the ground, in full control of a legitimate carrier. The typical functionality of a typical macro tower is used to carry the manipulated traffic back into the carrier network. Once it hits the true cell tower, the device gains some of the credibility of the carrier and can begin the process of more thoroughly hiding itself (a process sometimes called “data laundering,” of which the most famous type is money laundering).

<sup>36</sup> Iridium. (n.d.). Iridium. Last accessed on 13 February 2019 at <https://www.iridium.com/>.

<sup>37</sup> Craig Gibson. (11 June 2018). Trend Micro Security Intelligence Blog. Last accessed on 13 February 2019 at <https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/>.

- A typical, true telecom satellite with common attributes. Similar to the true macro cell tower, the satellite is in full control of the telecom carrier that owns it or pays for traffic to cross . Satellites may be used for several means of deploying an attack and hiding behind satellite infrastructure. There are two major satellite network types, GAN and WARN, which were described earlier. Both are used for telecom fraud and other attacks.

11. Rubber tote bin and Faraday shield combined with UPS battery and cooling fan — These allow the entire war rig to be mobile (setup in a car for instance) and function for an indefinite period, if charged by a car inverter. Note that if the target devices are low-power IoT devices, the overall size of the rig and its power requirements decreases significantly. The entire rig can fit in a backpack or the back of a motorbike and still function for a prolonged period. The rig may still fit in a backpack for cellular attacks, but its power demand will limit its operational effectiveness.



# Glossary

Acronym	Description
3G	Third generation of mobile
ACM	ISUP Address Completion Message
ANM	ISUP Answer Message
ANSI-41	American National Standards Institute #41
ATI	Any Time Interrogation
BCSM	Basic Call State Model
BSC	Base Station Controller
BOIC	Barring Outgoing International Calls
BOIC-EX-Home	Barring Outgoing International Calls except to home country
CAMEL	Customized Application for Mobile Enhanced Logic
CAP	Camel Application Part
CB	Call Barring
CC	Country Code
CDMA	Code Division Multiplexed Access
CdPA	Called Party Address
CDR	Call Detail Record
CF	Call Forwarding
CgPA	Calling Party Address
CIC	Circuit Identification Code
CLI	Calling Line Identification
CSD	Circuit Switched Data
CSI	Camel Subscription Information
DPC	Destination Point Code
DSD	Delete Subscriber Data
DEA	Diameter Edge Agent
DRA	Diameter Routing Agent
DTMF	Dual Tone Multi-Frequency
ERB	CAP Event Report Basic call state model
EU	European Union
FPMN	Friendly Public Mobile Network
FTN	Forward-To-Number
GLR	Gateway Location Register
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GMSC-F	GMSC in FPMN
GMSC-H	GMSC in HPMN
GPRS	General Packet Radio System
GSM	Global System for Mobile
GSMA	GSM Association
GSM SSF	GSM Service Switching Function
GsmSCF	GSM Service Control Function
GT	Global Title
GTP	GPRS Tunnel Protocol
HLR	Home Location Register
HPMN	Home Public Mobile Network
IN	Intelligent Network
IOT	Inter-Operator Tariff

Acronym	Description
GTT	Global Title Translation
IAM	Initial Address Message
IDP	Initial DP IN/CAP message
IDD	International Direct Dial
IMSI	International Mobile Subscriber Identity
IMSI-H	HPMN IMSI
IN	Intelligent Network
INAP	Intelligent Network Application Part
INE	Interrogating Network Entity
IP	Internet Protocol
IREG	International Roaming Expert Group
IRS	International Revenue Share
ISC	International Service Carrier
ISD	MAP Insert Subscriber Data
ISG	International Signal Gateway
IST	Immediate Service Termination
ISTP	International STP
ISTP-F	ISTP connected to FPMN STP
ISTP-H	ISTP connected to HPMN STP
ISUP	ISDN User Part
ITPT	Inbound Test Profile Initiation
ITR	Inbound Traffic Redirection
IVR	Interactive Voice Response
LU	Location Update
LUP	MAP Location Update
MAP	Mobile Application Part
MCC	Mobile Country Code
MCC	Mobile Country Code
MD	Missing Data
ME	Mobile Equipment
MGT	Mobile Global Title
MMS	Multimedia Message Service
MMSC	Multimedia Message Service Center
MMSC-F	FPMN MMSC
MMSC-H	HPMN MMSC
MNC	Mobile Network Code
MNP	Mobile Number Portability
MO	Mobile Originated
MOS	Mean Opinion Score
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number
MSISDN-F	FPMN MSISDN
MSISDN-H	HPMN MSISDN
MSRN	Mobile Station Roaming Number
MSRN-F	FPMN MSRN
MSRN-H	HPMN MSRN
MT	Mobile Terminated
MTP	Message Transfer Part
NDC	National Dialing Code



Acronym	Description
NP	Numbering Plan
NPI	Numbering Plan Indicator
NRTRDE	Near Real Time Roaming Data Exchange
O-CSI	Originating CAMEL Subscription Information
OCN	Original Called Number
ODB	Operator Determined Barring
OPC	Origination Point Code
OR	Optimal Routing
ORLCF	Optimal Routing for Late Call Forwarding
OTA	Over The Air
OTPI	Outbound Test Profile Initiation
PDP	Protocol Data Packet
PDN	Packet Data Network
PDU	Packet Data Unit
PRN	MAP Provide Roaming Number
PSI	MAP Provide Subscriber Information
QoS	Quality of Service
RAEX	Roaming Agreement EXchange
RI	Routing Indicator
RIS	Roaming Intelligence System
RDN	Redirecting Number
RNA	Roaming Not Allowed
RR	Roaming Restricted due to unsupported feature
RRB	CAP Request Report Basic call state model
RSD	Restore Data
RTP	Real-Time Transport Protocol
SAI	Send Authentication Info
SC	Short Code
SCA	Smart Call Assistant
SCCP	Signal Connection Control part
SCP	Signaling Control Point
SF	System Failure
SG	Signaling Gateway
SGSN	Serving GPRS Support Node
SGSN-F	FPMN SGSN
SIM	Subscriber Identity Module
SIGTRAN	Signaling Transport Protocol
SME	Short Message Entity
SM-RP-UI	Short Message Relay Protocol User Information
SMS	Short Message Service
SMSC	Short Message Service Center
SMSC-F	FPMN SMSC
SMSC-H	HPMN SMSC
SoR	Steering of Roaming
SPC	Signal Point Code
SRI	MAP Send Routing Information
SRI-SM	MAP Send Routing Information For Short Message
SS	Supplementary Services
SS7	Signaling System #7
SSN	Sub System Number

Acronym	Description
SSP	Service Switch Point
STK	SIM Tool Kit Application
STP	Signal Transfer Point
STP-F	FPMN STP
STP-H	HPMN STP
TADIG	Transferred Account Data Interchange Group
TAP	Transferred Account Procedure
TCAP	Transaction Capabilities Application Part
VT-CSI	Visited Terminating CAMEL Service Information
TP	SMS Transport Protocol
TR	Traffic Redirection
TS	Traffic Steering
TT	Translation Type
UD	User Data
UDH	User Data Header
UDHI	User Data Header Indicator
USSD	Unstructured Supplementary Service Data
VAS	Value Added Service
VIP	Very Important Person
VLR	Visited Location Register
VLR-F	FPMN VLR
VLR-H	HPMN VLR
VLR-V	VPMN VLR
VMSC	Visited Mobile Switching Center
VoIP	Voice over IP
VPMN	Visited Public Mobile Network
ATI	Access Transport Information
UDV	Unexpected Data Value
USI	User Service Information



## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)



Securing Your  
Connected World