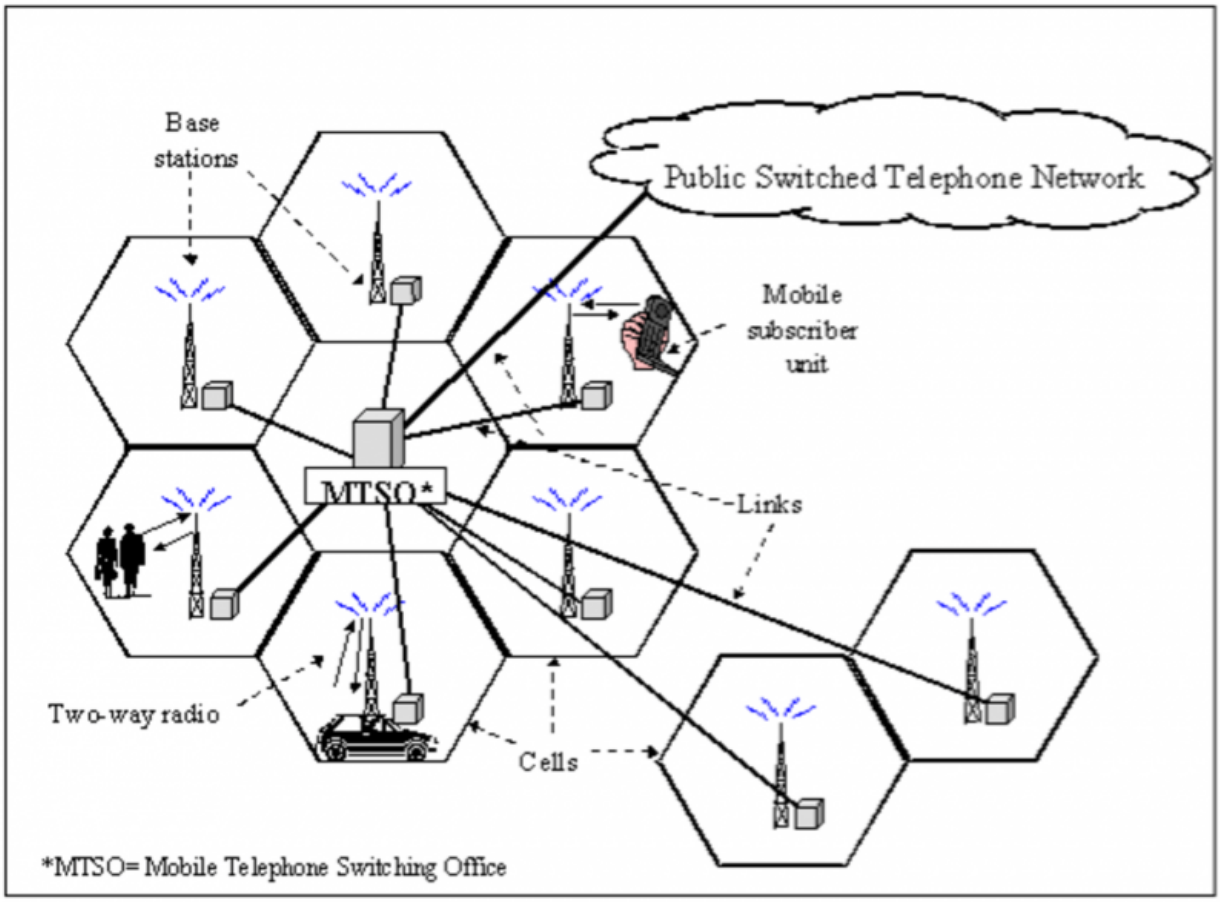
What police can learn from a terrorist's discarded mobile phone

November 20 2015, by David Stupples



Cellular network diagram. Credit: ITU

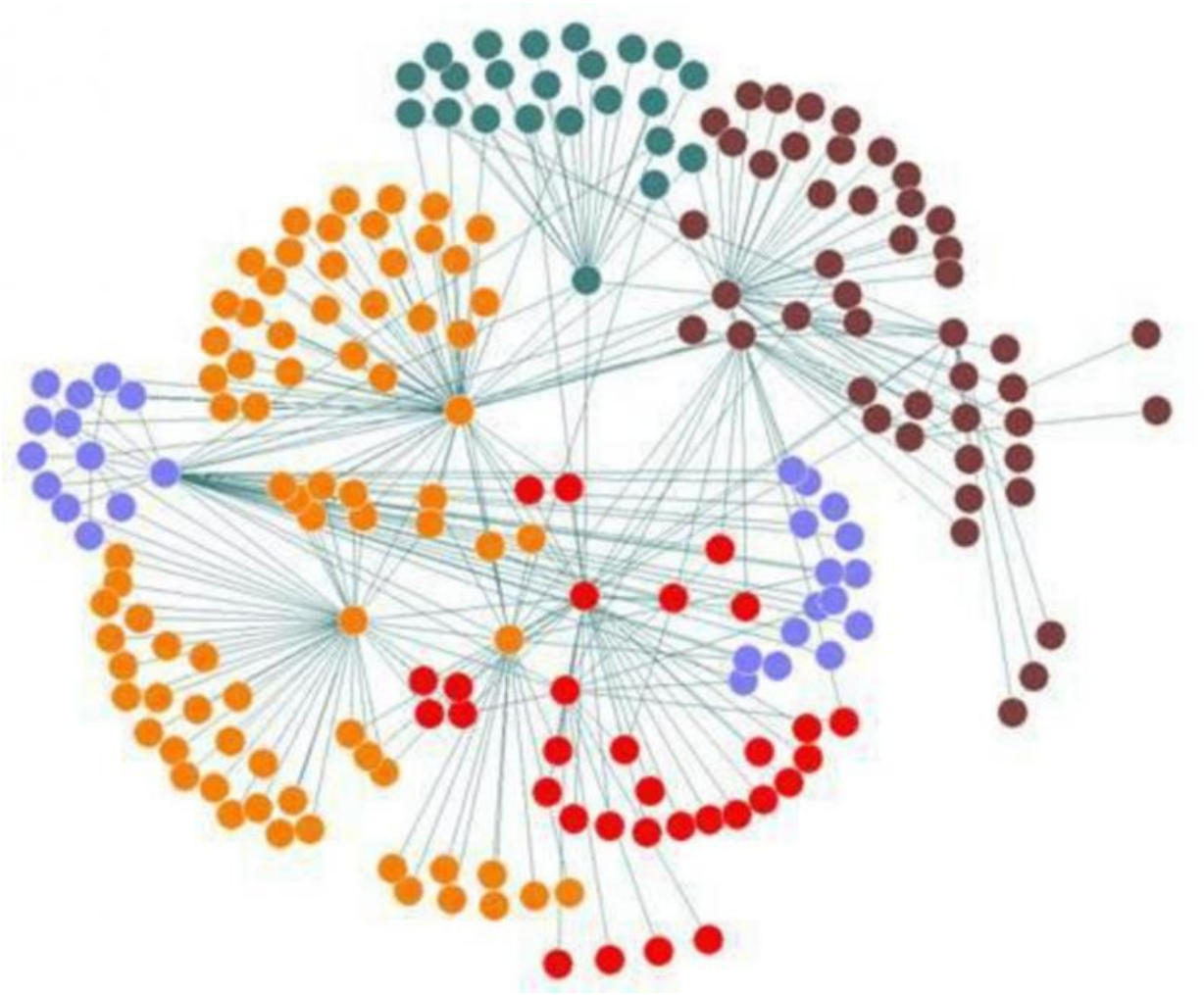
The dramatic raid on an apartment in the Paris suburb of Saint Denis that left two dead and eight arrested followed the discovery of a mobile

phone by police that was discarded by the terrorists who days earlier had launched their bloody attack. It's understood that the data police were able to extract from the phone led them to the apartment where others of the gang were hiding.

What information can be recovered from a mobile phone? Each mobile phone has a unique identifier called its IMEI number, and almost all modern phones also contain a SIM card containing an IMSI number which uniquely identifies a customer. From these two identifiers alone, the authorities will have been able to trace the registered owner of the phone and the calls made and received, by requesting this information from the telecoms company. But phone call records are just the start.

Mobile phone networks are cellular networks, constructed from a mesh of cells, each of which is an area of coverage provided by a radio transceiver base station. When switched on, a phone connects to and registers with a base station using its IMEI number, and the transceiver and handset will send paging messages between each other at frequent intervals to keep the connection established and detect if the phone is still within range.

As the phone moves beyond the base station's range and into a neighbouring cell then the process of registering and paging messages is repeated. Base stations are connected to each other through networks under the control of a Mobile Telephone Switching Office, which routes calls between different regions of the network. Different telecoms firms and network providers – for example EE, Vodafone and Three in the UK – are interconnected to form a single virtual network that spans an entire country.



A network of associations built from phone records can be revealing.

The network knows

This means the system will know the approximate location of any mobile phone device at any particular instant, so long as it's switched on and in contact with a base station – it needs to, in order to connect callers almost instantaneously. In the countryside a cell area may be as wide as 30km, but in towns and cities this will shrink to less than a kilometre, and in densely populated areas such as Paris the radius may be as little as

100 metres or less.

This information can provide a remarkably close approximation of where the phone is, or has been in previous seconds, minutes hours, days or weeks. And since all mobile phone networks interconnect at some point, this information can be recovered across Belgium and France, certainly, but also through most of the world. In densely populated cities the investigators will almost certainly have been able to locate the phone and its use to only a handful of addresses or apartment buildings.

Combined with intelligence from police investigations it will have been possible to hone down the search to a small number of apartments using only the mobile phone network records. If however the phone was a smartphone with Wi-Fi capabilities that had been used to connect to Wi-Fi access points, these would provide investigators with an even quicker and more exact pinpoint to where the terrorists were hiding as the IP address is normally associated with a physical address.

A treasure trove

Recovering the mobile phone would also have provided the Paris police with a treasure trove of other intelligence information relating to the planning of the attack, and perhaps to future attacks. From text messages and the phone's call log, a record of every incoming or outgoing call for the previous 12 months, investigators can request the records for each of the numbers that appear. With the times and dates of the messages, and locations indicated from the cell registration records of the mobile phone network operator, intelligence services can start adding names and addresses to numbers, building lists of associates and expanding the network of people of interest to come under further investigation.

Once names have been identified they can be used to investigate networks on social media such as Facebook, Twitter or location-driven

sites services such as food and entertainment directory Foursquare. The resulting network of associations are key to identifying active terrorist groupings, the logistics and financial support they receive, and even those individuals that may be reluctant participants who could be persuaded to become informants – an absolutely vital part of intelligence and policing.

It's likely that this discarded mobile phone will not only help the Paris police with their current investigation, but will provide information that will help prevent future attacks. Some of those identified in the association networks will not be aware that they've appeared on the intelligence services radar and will continue as before, unaware that their telecoms metadata is being monitored. Even if they purchase new phones, they will be betrayed by their associations to others in the network – and this is why this find by the Paris police is so important.

Source: The Conversation