MELROSE NETWORKS

Primer for Government and Regulatory Authorities

Mobile Network Signalling Analysis for Detection and Tracking of Cellular-Connected Drones

A policy and technical briefing for government departments, national security stakeholders, telecommunications regulators, and policy and legal teams

---

Executive Summary

This primer explains how analysis of mobile network signalling data can be used to detect and track drones that rely on cellular connectivity, and sets out the policy, legal and governance considerations relevant to its adoption. It is intended to inform decisions by government and regulatory authorities about how telecommunications infrastructure might contribute to national resilience against the rising threat of hostile and criminal uses of unmanned aerial systems.

Public mobile networks have become pervasive digital infrastructure in almost every jurisdiction. They are increasingly used, deliberately or incidentally, to provide command, control and data links for drones operating beyond the visual line of sight of their operators. Where such platforms attach to a public network, their behaviour produces observable signalling that is readily distinguishable from that of terrestrial devices. Appropriately governed analysis of this behavioural metadata can support both real-time alerting and retrospective investigation at national scale, complementing physical sensors such as radar and radio-frequency detection.

The principal recommendation of this primer is that signalling analysis should be treated as a practical, near-term component of layered counter-uncrewed-aerial-systems capability, pursued in close collaboration with network operators and within a clear legal, regulatory and privacy framework.

Uncrewed aerial systems are evolving rapidly in capability, accessibility and autonomy. Small, commercially available platforms are now used across a wide range of legitimate activities, including logistics, agricultural monitoring, emergency response, surveying and media production. In parallel, the misuse of such platforms by criminal groups, organised networks and state-aligned actors has become an established and growing concern for governments worldwide. Incidents affecting prisons, airports, public gatherings and critical national infrastructure have illustrated both the ingenuity of misuse and the limitations of detection frameworks designed for an earlier threat environment.

A defining feature of the modern drone is its reliance on wireless connectivity for command, control and payload operations. An increasing proportion of platforms now incorporate cellular modems, either as a primary means of communication or as a resilient secondary channel. Cellular connectivity

extends the operational envelope of a drone well beyond the visual line of sight of its operator, supports high-bandwidth telemetry and video, and provides a ubiquitous, low-cost control path that is difficult to disrupt without impact on legitimate services. This reliance simultaneously creates an operational opportunity for defenders, because any device that attaches to a public mobile network necessarily leaves behind a trail of observable signalling events.

1. Strategic Context

Drones are dual-use technologies. The same platforms that deliver medical supplies in remote regions can also deliver contraband into secure facilities or weaponised payloads against fixed assets. Recent conflicts have demonstrated how inexpensive commercial airframes, augmented with widely available components, can be employed at scale against targets of significant strategic value. The cost asymmetry between attacker and defender has become a defining challenge for national security planners.

Mobile networks are central to this evolving environment, although they are not themselves the target. They are enabling infrastructure: pervasive, reliable and nationally ubiquitous. In most developed economies, cellular coverage now extends across the full extent of inhabited territory and beyond, supported by hundreds of thousands of radio sites and serving many millions of connected devices. Where an unmanned platform uses a public cellular network for its control or telemetry link, that network becomes both part of the threat path and part of the potential solution.

Because cellular networks are designed to track the attachment and mobility of every connected device to route traffic correctly, they inherently generate a rich body of operational data. Appropriate analysis of that data, within suitable legal and governance frameworks, can yield insight into the presence and movement of cellular-connected aerial devices at a scale that no purpose-built sensor network could presently match.

2. Nature of Mobile Network Signalling

Modern mobile networks are conventionally described in terms of two logical domains: the control plane and the user plane. The user plane carries the content a subscriber sends or receives, such as voice packets, video streams and application data. The control plane carries the signalling that manages the network itself, including the procedures by which a device attaches to a cell, authenticates, establishes sessions, hands over between cells and reports its radio conditions. This distinction is fundamental to any policy discussion of the analytical techniques described in this primer.

Signalling analysis is concerned exclusively with control-plane events and the behavioural metadata they produce. It does not involve interception, decryption or inspection of the content communicated by a device. The analyst observes that a device is attached, how it is moving between cells, what radio conditions it is reporting and how its behaviour compares to that of the population of devices. The content of any associated voice call, message or data session remains outside the scope of the analysis

and, in most jurisdictions, outside the scope of what may lawfully be accessed without specific additional authorisation.

The emphasis on metadata rather than content is an important point of principle. It shapes the legal basis on which such analysis may proceed, the protections that must be applied to the data and the proportionality considerations that must govern any operational deployment. It also aligns signalling analysis with established operational practices in fraud management, network planning and lawful interception support, where behavioural metadata is routinely used without reference to the content of communications.

3. Observability of Aerial Devices

Cellular networks are engineered for terrestrial users. Radio planning assumes that handsets and fixed wireless terminals operate at or near ground level, within buildings or vehicles, and within well-understood mobility patterns driven by road, rail and pedestrian movement. An aerial device departs from these assumptions in ways that are measurable through ordinary network signalling.

A drone in flight typically sees many more cells than a ground-level device at the same geographic location, because the radio signals that would normally be obstructed by buildings, terrain or vegetation reach the airborne antenna with little attenuation. This produces unusually rich neighbour-cell reports, above-average signal strength from distant sites and unusually frequent handover activity. The pattern of cells visible to the device, and the speed at which that pattern changes, provides a strong indication that the device is not behaving as a conventional terrestrial terminal.

Mobility characteristics reinforce this picture. Terrestrial devices move along constrained routes at speeds consistent with walking, cycling or motorised travel. Aerial devices move along trajectories that are not constrained by road networks, at speeds and altitudes that can produce distinctive ground tracks and handover sequences. Temporal features, such as the timing of session establishment relative to known flight patterns, can add further corroboration. Taken together, these characteristics form an identifiable behavioural signature that distinguishes aerial activity from the background of terrestrial traffic.

4. Analytical Approaches

Several complementary analytical methods can be applied to the signalling record of a mobile network to identify aerial devices. These are described here at a policy level, without reference to specific implementations.

Mobility analysis

Mobility analysis examines the sequence of cells with which a device communicates over time, together with the reported radio parameters of each cell. Trajectories that are inconsistent with a terrestrial path, such as direct routes across inaccessible terrain or between isolated rural cells, are characteristic of airborne operation. Inferred speed and turn rate can likewise be compared against typical ground-based distributions.

Radio geometry and multi-cell visibility

Because aerial devices enjoy line-of-sight conditions to many radio sites, they tend to be visible to, and report measurements from, a larger and more geographically dispersed set of cells than terrestrial devices. Analysis of this multi-cell visibility, sometimes described as the radio geometry of the device, can provide both a strong discriminator for aerial behaviour and an input for position estimation.

Temporal behaviour

Operational drones frequently exhibit patterns of session activity that differ from those of everyday handsets. Flights may be of characteristic duration, occur at unusual times, or coincide with periods of low background traffic. Temporal features, combined with mobility and radio observations, help to distinguish operational drone use from incidental aerial exposure of ordinary devices.

Anomaly detection

Statistical and machine-learning techniques can be applied to the aggregate population of devices to identify outliers whose combined behavioural features fall outside normal distributions. Such techniques do not require a predefined signature of a specific airframe; they can surface previously unseen patterns of behaviour for further investigation. As with any anomaly-based method, the outputs must be treated as leads rather than conclusions and combined with other sources before operational action is taken.

5. Tracking and Continuity

Once a cellular-connected drone has been identified in the signalling record, the same data supports both real-time and retrospective tracking. Real-time analysis can follow the device as it moves through the network, providing a continuously updated estimate of its location and trajectory. Retrospective analysis can reconstruct past flights from stored signalling data, which is valuable for incident investigation, pattern-of-life analysis and the identification of associated infrastructure such as launch sites or operator locations.

Because the relevant data is generated across the entirety of a national network, the resulting visibility is continuous and nationally scaled. A device that traverses multiple regions, or operates in sparsely instrumented rural areas, remains observable as long as it is attached to the network. This stands in contrast to localised sensing systems, which provide detection only within the footprint of a specific installation.

Cross-border considerations arise where aerial activity crosses national boundaries or where the device roams onto a foreign network. European experience demonstrates that coordinated frameworks can be developed to support lawful cross-border exchange of relevant information, provided appropriate legal bases, safeguards and operational protocols are in place. Such arrangements are likely to become increasingly important as drone operations extend across jurisdictions.

6. Position Within a Layered Detection Model

Signalling analysis is one component of a layered counter-uncrewed-aerial-systems model. Radar provides physical detection of airframes regardless of their connectivity, with performance governed by target size and deployment geometry. Radio-frequency sensing detects the emissions of the drone itself and, where possible, of its controller, allowing identification of known protocols. Electro-optical and infrared systems provide visual confirmation, classification and, in many cases, intent assessment.

Signalling analysis complements these capabilities rather than replacing them. It offers wide-area, persistent visibility of the subset of drones that use cellular connectivity, including platforms that may fall below the effective detection threshold of conventional radar. It can be used to cue localised sensors, to provide early warning of unusual aerial activity, and to support attribution by associating flights with specific subscriber identifiers subject to appropriate legal process.

The relationship between wide-area and localised detection is best understood as a hierarchy. Signalling analysis supplies national-scale situational awareness and prompts closer investigation. Localised sensors confirm, classify and, where authorised, support engagement. No single layer is sufficient in isolation; the combined picture is substantially greater than the sum of its parts.

Attribute	Signalling Analysis	Traditional Sensors (Radar, RF, EO/IR)
Geographic reach	National, wherever cellular service is available.	Localised to sensor coverage; requires physical deployment.
Detection trigger	Attachment, registration and mobility behaviour of a connected device.	Reflected radio energy, emitted RF signatures, or optical observation.
Data type	Behavioural metadata from control-plane events.	Physical measurements of the airframe or its emissions.
Coverage of non-connected drones	Not observable unless using cellular connectivity.	Observable if within sensor range, regardless of connectivity.
Deployment profile	Leverages existing national infrastructure; largely software based.	Hardware-intensive; site-by-site installation and maintenance.
Retrospective analysis	Supported where lawful retention of signalling data exists.	Limited to recorded sensor output at deployed locations.

7. Legal and Governance Considerations

Any use of mobile network data for detection purposes must be grounded in a clear legal basis, applied with proportionality and subject to effective oversight. The data involved, while behavioural rather than content-bearing, is nonetheless personal data in most jurisdictions and attracts corresponding protections.

In a European context, the General Data Protection Regulation establishes the overall framework for lawful processing of personal data, including requirements relating to purpose limitation, data

minimisation, retention and the rights of individuals. The ePrivacy Directive imposes additional obligations specific to electronic communications, including confidentiality of communications and restrictions on the processing of traffic and location data. National security and law enforcement activities fall within derogations, but those derogations are themselves subject to substantive and procedural conditions.

In the United Kingdom, the Investigatory Powers Act 2016 provides a detailed statutory framework for the acquisition of communications data and related interference with privacy, including authorisation regimes, independent judicial oversight and safeguards on retention and handling. Comparable frameworks exist in other jurisdictions, and the international trend is towards increasing formalisation of such regimes. Proportionality, necessity and targeting are recurring themes across all of them.

Programmes that apply signalling analysis to the detection of hostile drone activity should therefore be designed from the outset with these frameworks in mind. This includes clarity on the legal basis for access to operator data, on the purposes for which the data may be processed, on retention periods, on the control of derived intelligence, and on the mechanisms by which subjects may seek redress where errors occur. Governance arrangements should extend to independent oversight, periodic review and transparent reporting, to the extent that operational security permits.

8. Policy Considerations

The implications of cellular-connected drones extend beyond operational countermeasures into the broader policy environment in which telecommunications operators function. Telecommunications infrastructure is a critical national asset, and the question of how that infrastructure contributes to, and is protected from, emerging security risks is a legitimate matter of public policy.

Structured collaboration between operators, regulators and security stakeholders is essential. Operators hold the data and the operational expertise. Regulators define the legal and commercial environment within which that data may be used. Security authorities understand the threat landscape and the decisions that analytical outputs must support. No one of these actors can deliver effective capability unaided, and ad hoc arrangements tend to be brittle and difficult to scale. Durable arrangements require shared governance structures, agreed data-handling standards and clear lines of accountability.

Cross-border coordination is a further policy consideration. Drone operations, criminal supply chains and the activities of hostile actors do not respect national boundaries. Mechanisms for the lawful exchange of relevant signalling-derived information between allied states, modelled where appropriate on existing telecommunications and law-enforcement cooperation frameworks, will become increasingly valuable. Early engagement with international partners can help to avoid fragmentation and to ensure interoperability of governance arrangements.

Policymakers should also differentiate between immediate and emerging capabilities. Analytical approaches that work with existing operator data can be deployed relatively quickly, subject to

governance, and can provide meaningful capability today. Emerging technologies, including the integration of sensing functions within future radio access networks, hold considerable long-term promise but will mature over network upgrade cycles. A realistic roadmap combines near-term adoption of analytical approaches with longer-term investment in the capabilities of next-generation networks.

9. Limitations

It is important to be clear about what signalling analysis cannot do. The approach is predicated on the use of cellular connectivity by the drone. Platforms that communicate exclusively via direct radio control, dedicated licensed spectrum, satellite links or pre-programmed autonomous flight generate no corresponding signalling in public mobile networks, and are therefore invisible to this technique. Adversaries may also employ measures to obscure their presence.

Devices that interact only intermittently with the network, such as those using short bursts of connectivity, present a reduced observational surface. Urban radio environments, with their complex propagation and dense traffic, introduce further ambiguity. Any operational use of the technique should therefore incorporate mechanisms for corroboration, ideally drawing on the other layers of the counter-uncrewed-aerial-systems model described above or deeper inspection of the device on the network.

Analytical confidence varies with geography, time of day, network configuration and the behaviour of the specific device. Well-designed systems communicate this uncertainty explicitly to decision makers and avoid presenting probabilistic outputs as deterministic facts. Human review remains an essential component of any workflow that may lead to operational action.

10. Conclusion

The rise of cellular-connected unmanned aerial systems presents both a challenge and an opportunity for national security authorities and telecommunications regulators. The challenge is evident in the evolving use of public networks as enabling infrastructure for hostile and criminal drone activity. The opportunity lies in the fact that the same networks are uniquely well placed to observe that activity at national scale, through analysis of the signalling they already generate during normal operation.

The approach described in this primer is practical, scalable and, in significant measure, immediately available. It draws on data that operators already collect and on analytical techniques with clear antecedents in fraud management and network analytics. It complements rather than replaces traditional counter-uncrewed-aerial-systems capabilities, and it fits naturally within a layered detection model that combines wide-area awareness with localised sensing and response.

Realising this potential requires deliberate action. Legal and governance frameworks must be clarified and applied. Operational relationships between operators, regulators and security stakeholders must be formalised and sustained. Expectations about performance, and about the limits of the technique, must be managed with candour. With these foundations in place, signalling analysis can make a

substantive contribution to national resilience against a class of threats that will only grow in importance over the coming years.

Melrose Networks
Edinburgh, United Kingdom
melrosenetworks.com

For further discussion or engagement: contact@melrosenetworks.com