DRAFT
GSMA REGULATORY POSITION ON

JARUS OPS: Recommendations for UAS Operations Category A and B

December 2017

GSMA Messages to JARUS Consultation on ‘Recommendations for Unmanned Aircraft Systems Operations for Category A an B’

GSMA welcomes the opportunity to contribute to JARUS consultation on the ‘Recommendations for Unmanned Aircraft Systems (UAS) Operations for Category A and B’.

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series conferences.

In summary, this GSMA consultation response recommends that:

1) In order to ensure an operation-centric, proportionate, risk and performance based regulatory framework, the new EU regulatory framework should ensure that drones can, where required, be equipped with SIM cards and a communications modem so that the drone ecosystem can benefit from cellular connectivity.

2) The mobile industry should be engaged when implementing these regulatory requirements for drones. This includes relevant expert groups that advise the European Commission. Collaboration, research, learning and exchange of information is key at this early stage of this emerging market. GSMA would welcome the opportunity to continue to actively participate and contribute to this process.

3) Applicable spectrum regulatory authorities at national and European level, consulting with JARUS where necessary, should ensure that there are no undue barriers in relation to the use of existing licensed mobile spectrum for drone connectivity, so that the public safety, security and performance benefits associated with cellular can be realised.

1. Introduction

In the context of this GSMA position, ‘cellular connectivity’ means that the drone can interact with the mobile network when equipped with a SIM card and a communications modem using existing licensed mobile spectrum and networks. This brings two major benefits:

Firstly, the mobile infrastructure exists already which makes the fast growth of drones economically feasible, because no investment is necessary in the roll-out of a new infrastructure. Mobile infrastructure is also an essential driver to realise a multitude of commercial use cases, for example disaster response and package delivery.

Secondly, cellular connectivity can help to establish controlled and safe operation of drones by ensuring the connection of drones with their control centres. This connectivity leads to a number of capabilities that benefit the drone ecosystem:

- Cellular connectivity can be part of unmanned traffic management solutions and enable no-fly zones
- Identification and registration schemes can be made possible for drones with cellular connectivity
- Cellular connectivity can assist law enforcement by enabling identification and tracking of drones.
- Mobile networks have a track record and useful tools to ensure privacy and data protection.

These capabilities allow cellular technology to provide end-to-end solutions in the emerging drone market.

This consultation response will explain the benefits of cellular connectivity in more detail before identifying potential barriers to cellular connectivity of which regulators should be aware. Much technical work is happening in the drone ecosystem. In the last part of this response, the outlook, we will point to key technical work streams that are relevant from a mobile perspective so that regulators can involve all relevant stakeholders in the regulatory process going forward.

2. Benefits of Cellular Connectivity for Drones

2.1 Drones in the context of the Internet of Things (IoT)

The GSMA has, for many years, been at the forefront of the effort to accelerate the delivery of new connected devices and services in the context of the Internet of Things (IoT). Key features of mobile networks that support drones are:

- Mobile networks are global, ubiquitous, scalable and reliable. They provide for a global, interoperable and scalable platform for innovative services to develop and to benefit from the existing ecosystem. The drone market can benefit from this connected platform.

- Many mobile operators already run 4G LTE networks, which meet very high-bandwidth, low latency requirements with an exceptional quality of service which is designed to scale. This will allow the drones industry to create innovative services. Mobile technology is evolving and 5G is the next step of the evolution to meet the ever expanding need for more devices, faster transmission and lower latency.

- The GSMA and its members draw on their extensive experience in addressing data protection, privacy and security issues. They work collaboratively with their IoT partners throughout the value chain, from device manufacturers to service and application providers, to embed privacy and security into IoT technologies. The drones market can benefit from existing approaches such as the GSMA Security Guidelines or GSMA Privacy by Design Toolkit.

In this context, the GSMA believes that the emerging drones market will benefit from the capabilities that exist within the global mobile platform, communication networks and the inherent approaches towards data protection, privacy and security.

2.2 Cellular connectivity is an important enabler for drones

Cellular connectivity is an important enabler for the emerging drone market, because it supports key requirements of the drone ecosystem, such as control, security and law enforcement.

This brings major benefits to those who want to make use of this technology:

1) Drones can use the existing mobile infrastructure that supports secure, high quality connectivity. This makes the fast growth of cellular connected drones economically feasible because no investment is necessary to roll-out a new infrastructure. The communications market is already being driven by demand for widespread coverage and data. Drones will particularly benefit from this trend, as the quality of the signal improves for airborne devices, for example due to the absence of fixed obstacles.

2) Cellular connectivity can already support functionality related to the command of drones over 4G networks, including communications services such as telematics, sensor data and streaming data. This functionality will continue to evolve as we move towards 5G networks.

This will realise a multitude of commercial use cases for drones over existing and future networks, i.e. 5G networks.

3) Cellular connectivity can help to establish controlled and safe operations of drones by supporting the connectivity needs for a broad range of operational scenarios and in particular those operating beyond line of sight in the highest risk environments where there are people, manned aircraft and critical infrastructure, e.g. airports. The cellular network enables reliable communication, because the mobile operator can control and monitor the quality parameters of the connection. This allows appropriate service quality for drone support.

Cellular connectivity leads to a number of capabilities that are of benefit to the drone ecosystem that will be described below. We will describe each capability first in general terms and then support with more detailed technical information to explain the technical background.

2.2.1 Cellular connectivity supports Unmanned Traffic Management (UTM) and enforcement of no-fly zones

The cellular connection is fully secure and encrypted. Using mobile connectivity between the drone and the control centre, the drone is able to report and to get updates on its objectives and status (such as flight height, destination and flight path monitoring). Furthermore this connection also allows links between drone operators and authorities. This means new services can be supported beyond line of sight such as disaster response and package delivery.

Mobile operators can provide a service to set up geo-fenced areas and to detect when a drone flies within these areas, using network-based location techniques to verify the GPS location. This can also be used to trigger alerts to the drone operator and appropriate enforcement authority, for appropriate action to be taken. Where a drone operator needs temporary permission to fly in a no-fly zone, the request for authorisation can be forwarded via the mobile network to the relevant authority and the approval can be communicated directly back to the drone.

With the development of the mobile network towards 5G, the ability to control an increasing number of drones in any specific area will also increase.

Supporting evidence:

- The Third Generation Partnership Project (3GPP), which is a telecommunications standards development organisation, offers well established identification, authentication and authorisation standards for mobile devices and network. In addition, the GSMA has a dedicated group for sharing and solving potential security issues that arise. Further groundwork is currently being undertaken that will benefit the drone ecosystem.

- GSMA has also developed the IoT Security Guidelines, which are applicable for drones.

- In case of a drone entering a no-fly zone, a UTM or trusted authority could request the drone to remain outside the no-fly zone. The secure cellular connection can authorise and grant access for trusted parties with the appropriate credentials to communicate with the drone.

- A drone equipped with GPS could communicate current coordinates together with network based location based services for verifying the provided coordinates to counteract GPS spoofing and jamming. This could be as simple as checking the cell id, i.e. checking whether the serving cell is consistent with the reported GPS location. Higher accuracy methods based on triangulation of signals from multiple cells are also possible.

- Vehicle-to-Vehicle communication technology using LTE protocols is being tested at the moment. It is currently being standardised in land vehicle use cases. Similar approaches may support the development of collision avoidance in drones.

2.2.2 Cellular connectivity supports the identification and registration of drones

Many countries require registration of SIMs in handsets. Mobile operators therefore have experience of applying customer and device registration requirements.

Supporting evidence:

- The mobile industry has two ways of identifying cell phones and the subscriber. The mobile device is uniquely identified by the International Mobile Equipment Identity number (IMEI) and the subscriber is identified via the SIM by the unique International Mobile Subscriber Identity (IMSI). Both are very secure standards. The device IMEI system can be used for drone registration and the SIM IMSI can be used for drone operator registration.

- A cellular based solution could be an effective way to enable drone identification / authorisation services, as identity verification and management is already a key component of a cellular service.

2.2.3 Cellular connectivity can support law enforcement

Cellular networks can provide secure authentication and authorisation for law enforcement while following the appropriate data protection and privacy rules.

Supporting evidence:

- With cellular technology, the drone can be lawfully intercepted (similar to the mobile device). If the drone has cellular connectivity then it can communicate its position and the flight path of the drone can be intercepted in the same way as the communication between the users. Law enforcement can find out what the drone has done recently (via network, via GPS).

- Laws designed to protect national security and public safety or to prevent or investigate crime and terrorism typically include obligations to comply with, where required, the provision of lawful interception assistance and the disclosure of communications data (e.g. certain subscriber, line identification and data). Mobile operators could add dedicated APIs for this purpose which would be only for use by law enforcement into the networks, i.e. for identity, location, insurance information.

2.2.4 The mobile industry understands how privacy and data protection can be implemented

With the number of global mobile subscribers set to surpass five billion during 2017[1], GSMA members have significant experience with regard to privacy.

For example, the GSMA Mobile Privacy Principles were developed in 2011 to give consumers confidence that their personal data is properly protected irrespective of the device or type of mobile service they are using. They underpin the mobile industry's responsible approach to the use of personal data and help the GSMA and its members to develop further guidance in specific areas. For example, the principles laid the foundation for the Privacy Design Guidelines for Mobile Application Development (2012) which articulate how the Mobile Privacy Principles function in the context of mobile platforms, applications and devices. The GSMA's IoT Security Guidelines and the integral IoT Security Assessment also specifically incorporate data privacy considerations to ensure that developers design data privacy into new products and services.

This year the GSMA published a set of commitments aimed at increasing consumer confidence in its report Safety, Privacy and Security across the mobile ecosystem.

The body of knowledge and experience that the mobile industry has acquired during the evolution of new technologies such as the smartphone and the Internet of Things will also benefit the drone ecosystem.

3. Supporting action to be taken by other regulators in relation to the use of cellular connectivity for drone use

To harness the benefits of cellular technology it is important that relevant spectrum authorities, work in conjunction with JARUS as required to ensure that there are no undue barriers to the use of licensed mobile spectrum for drone use.

The GSMA recognises that this is a topic that does not form part of JARUS' regulatory remit. We outline it in this response as the use of licensed mobile spectrum will be a critical factor in establishing a global market for drone operations. The GSMA believes it is vital that all relevant authorities work together to ensure that applicable spectrum regulations evolve as necessary to permit the operation of drones in existing licensed spectrum.

Licensed mobile spectrum enables widespread, high quality connectivity for drones with sufficient capacity to support competitive services and rising usage levels. Mobile operators typically have exclusive access to spectrum for coverage (i.e. below 1 GHz) and capacity (i.e. above 1 GHz bands) which enables very safe, reliable, high speed LTE services over wide areas.

[1] See https://www.gsma.com/newsroom/press-release/number-of-global-mobile-subscribers-to-surpass-five-billion-this-year/

Mobile spectrum bands are typically harmonised, either regionally or globally, so the economies of scale already exist to support affordable radio equipment for commercial drones. This will help reduce barriers to entry helping the commercial drone market to grow rapidly. Where mobile spectrum is harmonised internationally, networks can also support reliable drone flights in border areas as well between countries where permitted.

However, regulatory decisions that restrict the use of mobile spectrum licences to support drone connectivity could damage the significant benefits cellular connectivity deliver. For example, if regulators choose to classify LTE-based services for drones as an 'aeronautical mobile service'[1] then the bands mobile operators can use may be restricted. These limits would adversely affect the coverage and capacity of the resulting LTE services as well as market competition to provide such services. It is not clear that such a classification would be justified given there is no evidence that drone-based LTE connectivity using these bands present interference concerns to other wireless services. Nevertheless, the GSMA is happy to discuss and support coexistence studies for specific bands as required by regulatory authorities.

[1] Aeronautical mobile service restrictions are listed in the ITU's Radio Regulations which allocate frequency bands to various types of wireless services. These restrictions are more common in ITU region 1 (ie. Europe, the Middle East and Africa).

4. Specific comments on the JARUS recommendations

General Assumptions

The GSMA proposes a new General Assumption at paragraph 1.2 (4).

“In adopting AMC with recommended rules, JARUS and NAA will assess the benefits of licensed mobile technology and its associated functionalities.”

Article 5 – Registration and identification

1. The operator of an UA in category A or B, shall register in the manner established by the NAA display identification marks on all the UA it operates for them to be easily identifiable, when required by UAS.OPA30 and UAS. OPB.40.

2. The operator of a UA in category A shall ensure that UA are equipped with an identification means, when required by UAS.OPA70 and UAS. OPA.80

GSMA comment:

The mobile industry has two ways of identifying cell phones and the subscriber. The mobile device is uniquely identified by the International Mobile Equipment Identity number (IMEI) and the subscriber is identified via the SIM by the unique International Mobile Subscriber Identity (IMSI). Both are very secure standards. The device IMEI system can be used for drone registration and the SIM IMSI can be used for drone operator registration.

Such a cellular based solution could be an effective way to enable drone identification / authorisation services, as identity verification and management is already a key component of a cellular service.

Article 2 and Article 11 – Acceptable Means of Compliance

We note that the definition of Acceptable Means of Compliance (AMC) means "non-binding standards adopted by NAA, to illustrate means to establish compliance with the Civil Aviation Law and its implementing acts. If no such applicable AMC have been adopted by NAA then AMC adopted by JARUS or guidance developed by industry.

We note that, according to Article 11, AMC and certification specifications (CSs) published by NAA or, when acceptable to the NAA, published by JARUS, other aviation authorities or standard making bodies may be used to establish compliance with the Civil Aviation Law and this Regulation. When AMC or CS are complied with, the related requirements of this Regulation are presumed to be met.

GSMA comment:

For the reasons set out in this document, the GSMA considers that licensed mobile network and the functionality that can be offered by mobile networks will be well placed to meet any AMC standards adopted by an NAA or JARUS.

5. Outlook

Cellular technology is a true differentiator for the evolution of the drone ecosystem. It is ubiquitous, and it is also evolving. This brings many advantages for both the regulators and the industry, compared to many singular solutions offered by non-cellular providers. Cellular technology is standards based. Therefore all solutions for drone communication (identity, tracking and law enforcement, for example) benefit from a well-established standards mechanism that is unique to cellular communications.

Moreover, the GSMA is working with a dedicated interest group of mobile operators and mobile ecosystem stakeholders to define recommendations for drone operations. The work of this group can be used to help regulatory bodies and other stakeholders to ensure that the benefits of the mobile industry are used for the development of this regulatory framework for drone operation.

The activities of 3GPP are also relevant. 3GPP is a global standards body that defines mobile network communications for all mobile operators. 3GPP is currently working on expanding the features (including maximum throughput and reliability) of the mobile network to be able to support drones better. Further information will be provided to regulators when available.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601