Observer Research Foundation
Building Partnerships for a Global India

HOME
ABOUT US
LEADERSHIP@ORF
PUBLICATIONS
ORF MONITORS
ANNUAL
ASSESSMENTS
EVENTS
CHAPTERS
CENTRES
PARTNERS
CAREERS
LIBRARY
ORF IN THE MEDIA
CONTACT US

Analysis

You are here: orfonline.org » Publications » **Analysis**

Search

Drones are welcome, but where's the policy framework?

R Swaminathan
15 January 2015

The recent rape of a young woman in an Uber taxi in Delhi has triggered off a slew of institutional responses. These range from usual suspects like increased patrolling by the police to the unusual ones like the use of drones to keep an eye on activities. It's interesting that the Delhi police are actively looking at deploying drones to augment and, in several cases, take over standard policing operations. At one level, it's almost an explicit admission that their existing system of patrolling and response mechanisms - the basic framework of law and order - are fraying at the edges, often getting overwhelmed comprehensively by the ugly underbelly of the city. At another, it indicates a desperate and naïve assumption that just throwing high end technology at a deep rooted and multidimensional problem, one that's as social and economic and it is gendered and political, will end up resolving it. By itself technology cannot be the sole solution to social issues. However, a robust ecosystem of technology-based solutions combined with the right administrative structure and a proactive policy environment can actually contribute to a better quality of life and a safer and more secure cityscape. A good example is the staggered manner in which New York mayor Michael Bloomberg set the stage for introducing drones for internal surveillance and law and order functions. Of course, it wasn't without its share of controversies, especially on issues of privacy, but the public debate it generated contributed a great deal in clarifying the operating profile and the policy framework for the use of drones on a daily basis. Seen in this context, the decision of the Delhi police to use drones seems like an ad-hoc and knee-jerk reaction

with no clear-cut thought process on how it will integrate with the existing systems of investigation, evidence gathering and recording and standard operating procedures. In order for drones to effectively augment existing police functions and create new ways of responsive intervention and action, instead of becoming yet another fancy and underutilised toy, there is a clear cut need for an enabling system. There are three fundamental pillars for creating this facilitating framework.

The first is to clearly reorient and redefine notions of airspace and air-corridors. A drone is an unmanned aerial vehicle first and an integrated digital system next. Indian policy makers tend to treat airspace as somewhat of a physical commodity, almost like a piece of land. It's necessary to look at airspace beyond its literal definition and as a 'collection of procedures, regulations, infrastructure, aircraft and personnel that compose the national air transportation system'. Airspace, by default, has also come to mean at least 10,000 feet. Except for the landing and take-off phase, for airlines, air traffic controllers, aviation authorities and policymakers airspace only refers to 25,000 to 35,000 feet (the standard cruising altitude for most civilian aircraft). Micro drones and small unmanned aerial vehicles, like the ones being sought to be used by Delhi police, redefine airspace with some cruising at less than 100 feet and others going up to almost 3000 feet. Though not many details are available, the drones expected to be used by the Delhi police will have the capability to transmit real time pictures to Quick Response Teams (QRTs), integrate with the existing network of CCTV cameras and fly at approximately 200 feet. The prevailing Air Traffic Control (ATC) system operates on the basis of ground level radars (a command centre) monitoring the movement of planes, and communicating directly with the pilots and co-pilots on direction, altitude, navigation, vehicle and traffic control and collision avoidance. Apart from the constant guidance and inputs from the ATC, pilots either visually try and spot aerial vehicle or use the Traffic Collision and Avoidance System (TCAS) to avoid untoward incidents. Unmanned aerial vehicles have to integrate with the current system, especially with the TCAS. This requires the current ATC system to introduce new generation radars that can track small and microdrones flying at extremely low altitudes. Additionally a system to physically and electronically identify drones has to be evolved. Since drones will increasingly become part of a networked environment, it's critical to give each drone a unique electronic code, something like an Internet protocol address, for quick, easy and clear identification. In this regard, the European Union's policy and approach document towards the regulation and management of unmanned aerial vehicles is an excellent starting point.

The second is to reconceptualise connectivity and infrastructure. Drones are, for all practical purposes, the first autonomous peer-to-peer connective infrastructure that does not need a hub. Though each drone is an independent hub and a spoke at a same time, nonetheless they require adequate docking and charging stations. If the Delhi police is serious about integrating drones as part of its law and order maintenance and surveillance system then it has to first establish specifically earmarked docking and recharging stations. Most of these drones are either electrically and battery operated or work on alternative energy means like solar energy. The docking and maintenance stations will require their own power sources, an entire band of unmanned aerial vehicle engineers, maintenance crew and a complete supply chain system for parts, electronics and networking solutions. There is also a need to support and evolve a domestic drone industry that understands specific Indian challenges. Today, most of the drones are imported and then customised. These two aspects, of a evolving a docking and maintenance infrastructure and a robust domestic industry, cannot be achieved till all aspects of civilian drone management and regulation is integrated into one single department. The issues of integration of unmanned aerial vehicle with existing systems of law and order transcend boundaries of civil aviation, internal security, privacy and safety and external security. A crucial component of resolving this challenge to satisfaction is to reorient the role of DGCA from an agency focusing exclusively on providing various forms of certifications for flight operations, air worthiness and the final Certificate of Authorisation (COA), and to become a true regulator on the lines of a Securities Exchange and Board of India (SEBI) and Telecom Regulatory Authority of India (TRAI). In this respect it would be a good idea to look at the policy measures being taken in the United States of America to expand the regulatory mandate of the FAA to slowly integrate drones with the existing manned aviation network. Today, FAA has a separate division that's exclusively mandated to look and manage the integration of drones into various daily aspects of social, political and economic life.

The third issue is one of privacy. Taken together with CCTVs, web monitoring programmes and real time satellite imagery, drones complete the picture of 360 degree surveillance. Drones require an absolutely new human thinking: one that has to acknowledge and understand that the set of interconnected technologies of today constitute an artificial intelligence of tomorrow that will no longer be completely in our control. It is in this context that there are two fundamental challenges that are worth considering and debating. The first challenge confronting Indian policy makers is to substantially rework the Information Technology Act of 2000, which was amended in 2008, to be ready for a future that's going to be increasingly based on an Internet of things. Drones are at the cutting edge of this phenomenon. Attention has to be paid to Section 66A of the IT Act, especially its wordings **'computer resource'** and **'communication device'**, which embeds the possibility of any land or air vehicle, whether manned, semi-autonomous and completely autonomous, using any form of digital technology, which for all practical purposes is a computer resource, to come within the purview of the Information Technology Act. The second challenge is to redefine existing legal framework with reference to what constitutes the correct way of collecting evidence, especially its admissibility in a court of law in the context of Indian attempts to define a comprehensive and proactive policy and regulatory framework for privacy. The Information Technology (Amendment) Act, 2008 has two sections -- 43A and 72A -- providing for civil and criminal liabilities relating to Privacy. Section 43A focuses on the nuts and bolts of 'reasonable security practices' for sensitive personal data and information, while Section 72A provides for a jail term and a fine to anyone, a person, a body corporate or an institution, who causes 'wrongful loss or wrongful gain' by divulging the personal information of another person. These two sections specifically defined personal data as any information that is capable of singularly identifying the person. Everything from birth registry details, hospital records, financial and census information, mobile number, social networking details, educational records to death certificate and even a person's sexual orientation can possibly be interpreted to mean personal data and information. The introduction of drones for law and order introduces a completely new dimension to the debate and it's within this context that the draft Privacy Bill 2011 needs to be located. In this context, it would also not be a bad idea examine the case history relevant to drone surveillance and the American Fourth Amendment, especially how the Katz vs United States (1967) case, which established a legal and juridical standard for the interpretation of the Fourth Amendment, has been used in recent times to redraw and reorient 'constitutional protections' of the United States of America.

(The author is a Senior Fellow with the Observer Research Foundation, a Fellow of the National Internet Exchange of India (NIXI) and Contributing Editor of Governance Now)