Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Understanding the drone epidemic

Roger Clarke[a,b,c,*]

[a] Xamax Consultancy Pty Ltd, Canberra, Australia
[b] Australian National University, Canberra, Australia
[c] University of N.S.W., Sydney, Australia

Keywords:
RPA
RPAS
UAV
UAVS
Drone control
Drone autonomy
Drone applications
Drone risks

ABSTRACT

Drones are aircraft that have no onboard, human pilot. Through the twentieth century, piloted aircraft made far greater progress than drones. During the twenty-first century, on the other hand, changes in both drone technologies and drone economics have been much more rapid. Particularly in the case of small, inexpensive devices, the question arises as to whether existing regulatory frameworks can cope. To answer that question, it is necessary to document the nature and characteristics of drones, the dimensions across which they vary, the purposes to which they are put, and the impacts that they appear likely to have. The analysis concludes that careful consideration is needed of the adequacy of controls over the impacts of drones on two important values – public safety, and behavioural privacy.

1. Introduction

During the twentieth century, people became used to seeing vehicles in the sky. As had been the case with horse-drawn carriages, train engines, trams and automobiles, a human in the airborne vehicle controlled its behaviour. The twenty-first century is seeing a rapid proliferation of aerial vehicles that do not have a human controller on board. In some cases, the pilot is nearby, and in others the pilot is remote and even half-a-world away. Large drones are being used for military purposes by various countries. Meanwhile, the capabilities of small drones have greatly increased, and their manufacturing costs have greatly reduced. So small drones are proliferating, the increase in market-size has attracted further investment, and a leap in the functionality-to-cost ratio has occurred. This multiplies the potential for benefits from drones, and exacerbates the risks.

In addition, a century of technological progress has resulted in at least some of the pilot's functions being performed automatically, particularly aircraft stability in response to turbulence. Autonomy may extend through various levels, under human supervision or otherwise, with or without automatic detection of out-of-scope conditions and auto-handover to a human pilot, and subject to over-ride by the human pilot or not. With such capabilities come risks.

Can existing regulatory frameworks cope with the challenges arising from increased capabilities, much greater usage, and higher degrees of drone autonomy? To answer that question, it is necessary to document the nature and characteristics of drones, the dimensions across which they vary, the purposes to which they are put, and the impacts that they appear likely to have.

Many parties have an interest in talking up drones and their capabilities and applications. Many media outlets are driven by the need for revenue, and subject to limited journalistic constraints, so a great deal of the media coverage of drones comprises lightly dressed-up versions of corporate sales brochures and media releases, with limited critical thought applied by the nominal author. The implications of drones are sufficiently significant that more careful analysis is needed.

[*] Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611, Australia.
E-mail address: Roger.Clarke@xamax.com.au.

http://dx.doi.org/10.1016/j.clsr.2014.03.002

The privacy impacts of civil applications of drones have already been subjected to analysis, e.g. in Finn and Wright (2012). The scope of the research reported on here is broader than privacy, extending across the wide range of security issues that the technologies give rise to. This is the first of a series of four papers, whose combined purpose is to identify the disbenefits and risks in the use of drones, and consider the extent to which they are subject to suitable controls.

The present paper lays the foundation for the series. The second paper reviews the existing literatures on computing, data communications, robotics, cyborgisation and surveillance, in order to bring past experience to bear on the drone phenomenon. The third and fourth papers examine the extent to which current regulatory frameworks for public safety and behavioural privacy appear likely to cope, and the prospects of adapted and new measures to address the problems that drones present.

The scope of the work is civilian applications and excludes theatres of war. Issues that are thereby out-of-scope include the ethics, politics and practices of remote-controlled delivery of armed explosives, the notion of ’war as video game’, the ’post-heroic’ age of warfare, the increasing acceptability of warfare with limited risk to the war-maker’s personnel, the role of drones in the quiet creep of war-making by countries’ executives outside the control of their parliaments, and violence committed by semi-autonomous devices on behalf of nation-states.

It is necessary, however, to keep warfare at least somewhat within the field of view. Military applications have been, and remain, a strong driver of drone developments. The vast sums of money available for research, IR&D and production of equipment that provides military advantage heavily biases progress in particular directions. A further factor is that the early years of the 21st century have seen a dramatic increase in the application of military technologies by nation-states not only to wage war on other nations that they perceive to be enemies at the time, but also to monitor activities along the country’s borders, to assist in the enforcement of domestic laws, and even to subjugate their own people. The scope of this series of articles accordingly encompasses not only individual, corporate and governmental applications of drones, but also law enforcement and national security uses within an individual country.

The industry prefers to use descriptive terms for the aircraft concerned, but this paper uses the popular term throughout. The paper commences by reviewing the emergence of drones, and their attributes. On the basis of a consideration of categories of drones and not-drones, and boundary-testing examples, a working definition is proposed. The opportunities and challenges that drones present are then considered within a wide range of current and proposed application-areas. This delivers insights into the question of the attributes of drones that challenge existing regulatory arrangements.

2. Drones

In order to develop an appropriate working definition for a drone, this section considers in turn their precursors and origins, and the attributes of effective drones, with particular attention paid to their control and the degree of autonomy from their controller.

2.1. *Emergence*

Many threads of technological development have fed into the notion of a drone. Artefacts have been airborne for several millennia (in such forms as sharpened stones, spears, boomerangs and kites). Humans have been achieving flight since at least 1783, using lighter-than-air balloons or ‘aerostats’. Powered flight was achieved by a French ‘dirigible’ balloon in 1852. The internal combustion engine was applied by 1872, with most of the early developments taking place in France and then Germany. Nearly 150 years later, aerostats were tethered 15,000 feet above Afghanistan, transmitting live battlefield-surveillance video (Bumiller and Shanker, 2011). Heavier-than-air craft were emergent through the nineteenth century in several countries. Following developments during the 1890s, the first fixed-wing aeroplane/airplane achieved sustained, manned, powered and controlled flight in the USA probably in 1901 and certainly in 1903. Rotorcraft (of which the helicopter is the most common form) had been emergent for centuries, with the first unmanned flight in 1877 in Italy, and the first manned flight in 1907, in France.

Flying artefacts have been applied to many purposes. One early use, at least 2000 years ago, in China, was to assist in communications by means of lanterns. Balloons were used to carry human observers by the French in 1794, and this use was revived during the American Civil War in 1861–65. Cameras were attached to balloons in France in 1858, to kites and rockets c. 1880–1900, and to pigeons in Germany in 1907–11. Drones were being developed as means of carrying weapons and delivering explosives as early as 1915 in the USA, and were used as targets as early as 1930 in the UK. Science fiction has played an interactive role with many technologies, including drones. The first major 20th-century anti-utopian novel – 25 years before Orwell’s ‘1984’ – imagined drones (‘aeros’) as the means by which the government observed and repressed the population (Zamyatin, 1922). The surveillance and security applications of micro-drones were investigated in Stephenson (1995).

Many forms of motive power have been the subject of experimentation, and some have been harnessed. A greater challenge in the development of drones has been the means of control of the aircraft. The early focus was on control by a human pilot on board the aircraft, and, for the first century of flight, pilotless aircraft were seen as exceptions and novelties rather than the mainstream.

Yet remote control of transport devices had emerged before the first manned flight, in the form of Tesla’s Teleautomaton – a radio-controlled boat, demonstrated in 1898. Automated stabilisation control of an aircraft was emergent in the USA in 1910–15. The first known pilotless rigid-frame aircraft was in testing in the USA prior to the end of the World War I.

Generally, discussions of drones refer to an individual, at distance from the drone, but in control of it. The term ’remote pilot’ is commonly used, not just for historical reasons, but also because the functions performed and the visualisation capabilities and the skills required continue to be closely related to those of an onboard pilot. That may change over time, however. In addition, the prospect of fully autonomous drones requires consideration.

Even such a brief review of the origins and early years of drones makes clear that the field is beset with considerable diversity. In order to settle on a satisfactory working definition of drones, and appropriate bases for categorising them, it is necessary to identify the range of attributes that they display. The most fundamental of these are the attributes associated with the craft's survival. The following section accordingly considers the means whereby drone behaviour is controlled.

2.2. *Drone control*

The term 'airworthiness' is commonly used to refer to an aircraft's suitability for safe flight. Each aircraft has an operating envelope, defined in terms of its attitude, inside of which it is flyable, and outside of which it is unstable and probably unrecoverable. An aircraft's attitude is its orientation about its centre of gravity. Attitude varies in three dimensions around the centre of mass:

- roll or bank refers to rotation around the aircraft's long axis
- pitch refers to the rise and fall of the nose of the aircraft, i.e. rotation around its lateral axis
- yaw or heading refers to port-starboard/left-right swing of the nose of the aircraft, i.e. rotation around its vertical axis

Safe operation of a drone is dependent on the aircraft's attitude being kept within its operating envelope, by conducting manoeuvres within that envelope, and by taking corrective action when the aircraft's attitude is changed by external factors, referred to as upset-conditions, such as a wind-gust or turbulence.

Key attributes that enable drone survival are:

- awareness of the drone's location within the operational space, of its attitude and of its direction and speed of movement
- sensors and/or remote data-feeds that enable maintenance of the awareness of location, attitude and movement in a sufficiently timely manner
- a sufficient set of controls over the drone's attitude, and direction and speed of movement, to enable flight to be sustained under a wide variety of atmospheric conditions
- sufficiently rapid response of the drone to the controls (manoeuvrability)
- sufficient power to maintain movement, to implement the controls, and to operate sensors and data-feeds, for the duration of the flight
- the ability to navigate to destination locations within the operational space
- the ability to monitor the operational space (situational awareness, threat detection)
- the ability to navigate with respect to obstacles (collision avoidance)
- sufficient physical robustness to withstand threatening events, such as wind-shear, turbulence, lightning and bird-strike

Control over drone-flight may be exercised by a human pilot or an auto-pilot. A review of remote control and auto-pilot functions for small drones is in Chao et al. (2010). In principle, either kind of pilot may be on-board or remote. However, there appear to have been insufficient advantages for remote auto-pilot technologies to emerge, and auto-pilots are almost always on-board. That may change, as the micro-drone market develops, and particularly as nano-drones emerge. A drone by definition does not carry a human pilot, and hence human pilots are always remote. This section considers firstly autonomous control and then control exercised by the remote human pilot.

(1) Autonomous control

In practice, drones generally exhibit at least some degree of autonomy, because such functions as stabilisation of attitude and altitude are readily delegated to electronic components. To perform these functions, an auto-pilot needs access to data, in real-time or close to it, to enable computation of attitude, location in space, and location in relation to obstacles. This data may be generated by onboard equipment such as gyros, accelerometers, magnetic sensors, electromagnetic sensors (in the visual, infra-red, microwave and radio ranges), or may be received as data-streams from remote sources including Global Positioning System (GPS) data from satellites. The reliability of autonomous performance of such functions is arguably better than that of humans, at least under conditions that are within predicted ranges and relatively stable. Even under more challenging conditions, autonomous performance may be of comparable reliability.

Some higher-order functions, such as maintenance of a previously-determined flight path, take-off, and even planning of the flight path, may also be delegated from a human pilot to an auto-pilot. It is also possible for landings to be performed entirely autonomously, which is referred to as 'autoland'. At least for large, fixed-wing drones, this requires considerable infrastructure at the landing site, triple-redundancy of multiple components aboard the aircraft, supervision by the human pilot, and occasionally resumption of control by the human pilot. Due to the equipment costs and training levels involved, it is currently a very expensive option. In addition, if an aircraft is only capable of autoland, it is inherently severely limited in its choice of landing location.

In the military drone environment, variously four and/or five levels of autonomy are distinguished:

- where all upper-level functions are human-controlled, the terms used include *’human-operated’* (USDoD, 2011, p.46) and ’human-in-the-loop’ systems (EP, 2013, p.6)
- where some upper-level functions remain in the hands of the pilot except during periods when the function is switched over to automatic, USDoD (2011) uses the term *’human-delegated’*
- where an upper-level function is by default in automatic mode, but the pilot is able to switch control back to manual, USDoD (2011) uses the term *’human-supervised’*
- EP (2013, p.6) recognises a *’mostly autonomous’* mode, also referred to as ’human-on-the-loop’ systems. This might be inferred as meaning that control of key actions (such

as those involving violence) remains in human hands. On the other hand, the text implies that the decision to launch an attack is fully delegated to the device, with the possibility of a human override (if the human exercises it in time). A similar approach might of course be adopted to surveillance drones used by police or paparazzi, by civilian interceptor drones, and, as they emerge, of pursuit drones
- *fully autonomous* drones are feasible, and are referred to in military circles as 'human-out-of-the-loop' systems (EP, 2013)

An alternative set of gradations between full pilot control and full autonomy is provided in Table 1.

Table 1 – Gradations between full pilot control and full autonomy. From Armstrong (2010, p.14), attributed to a BAE presentation.

Drone function	Pilot function
Full Autonomy	Interrupt
Act Unless Revoked	Revoke
Suggest Action	Authorise Action
Give Advice	Accept Advice
Give Advice if Requested	Request Advice
None	In Command

When control feeds from the pilot are interrupted, a drone of necessity drops into autonomous mode. Designs need to apply safety principles in order to minimise the risk of harm. The crash of a hobbyist drone into the Sydney Harbour Bridge in October 2013 provided a valuable case study (Kontominas, 2013; LL, 2013). It appears that the drone had dropped into autonomous mode and was auto-returning to its point-of-origin. Its lack of situational awareness resulted in it flying through the bridge pylons, colliding with three of them, lurching low across road traffic and crashing onto railway tracks. The industry uses the term 'fail-secure' for such features as 'remain in place', 'land immediately' and 'auto-return to origin'. The case study demonstrates that the term 'fail-secure' is materially misleading.

The reliability of fully autonomous operation generally decreases as the flight mission becomes more complex (e.g. target acquisition, camera control, release of munitions), and as the flight mission changes or is refined. Emergent so-called 'guided-bullet technology' is intended to include directional flight control at ballistic speed, but it appears unlikely that it will include a recall button or an ability to prevent impact or suppress explosion (Schachtman, 2008). Although these aspirations are in the military field, they have potential applications in para-military law enforcement and even in civilian fields.

Fully autonomous drones remain experimental. On the other hand, flights have already occurred within controlled airspace. For example, "on 18 August 2005, … the Herti-1A system (G-8-008) achieved the first CAA approved fully autonomous mission of an unmanned aircraft in UK airspace … from Campbeltown Airfield, Scotland … over Machrihanish Bay [600 m from the end of the runway] … [with] a fully autonomous landing back at the airfield" (UVS-Info, 2005). See also Prigg (2013).

At this early stage, designs of autonomous systems continue to appear very naive in comparison with the insights from the critical literature that are discussed in the second paper in this series. Discussions of possible architectures for autonomy fail to embody as a central feature of drone-with-pilot interactions an explanation of the rationale for action or advice.

(2) Remote human control

Effective remote human control of a drone can only be achieved if the following criteria are satisfied:

- the pilot has sufficient data-feeds, of sufficient quality, in sufficient time, to enable decisions to be made
- data communications are adequate
- the pilot has a sufficient instruction-set available
- communications of instructions are adequate
- the drone performs in accordance with the instructions provided by the pilot

Several categories of remote control need to be distinguished:

- Visual Line of Sight (VLOS) Operation

  The pilot relies on their sight and intuition, without visual aids or instrumentation.

  This has long been the primary mode of operation of model aircraft
- First Person View (FPV) Operation

  The pilot is aided by, or even entirely dependent upon, the transmission of images or video from one or more cameras mounted in the drone in ways that correlate with the view that an onboard pilot would have
- Instrument-Based Operation

  The pilot is aided by, and is generally entirely dependent upon, data-feeds and instruments to render the data

In practice, the range over which VLOS operation is practicable depends on the size of the drone, atmospheric conditions and natural and man-made obstructions. FPV operation in its current forms is regarded as error-prone, especially where the pilot depends on FPV to the exclusion of VLOS, e.g. by wearing goggles. Both FPV and instrument-based operations are heavily dependent on communications capabilities. Regulatory requirements apply, and are considered in the third paper in the series.

Significant challenges arise from the dependence of drones and drone-pilots on data-feeds and control-feeds, combined with the limited range of frequency choices for electronic communications. Airwaves are congested, especially in urban areas, but also in zones that have considerable electronic communications traffic for other reasons. Signals between drones and remote pilots, and between drones and GPS satellites, are subject to a considerable amount of interference – variously environmental, accidental and intentional. This may block or modify communications, and hence may result in drone behaviour different from that intended by the remote pilot.

The following section considers other dimensions, in addition to control of the drone's flight, across which drones differ.

2.3. *Other drone attributes*

Bento (2008) identifies factors that are conventionally regarded within the industry as being key characteristics of drones, such as size, maximum altitude, endurance, range of the device's data links, and intended missions. However, in order to identify the definitional attributes of drones, it is important to distinguish the primary functions of drones:

- control – as discussed in the previous section
- navigation, in order to follow a path and/or reach a location
- operational functions, such as load-carrying and surveillance
- capabilities that are ancillary to control, navigation and operations

The operational value of drones depends on a range of characteristics, including:

- the available payload, which reflects dimensions, engine-power and other limiting factors such as angles of tilt, and payload flammability
- operational range and flight-time, which depend on the power-source available to the drone, related to the power-demands for control, navigation and operational functions
- suitability to the operational context, e.g. ground-proximity/high-altitude/indoors

Throughout the history of manned flight, pilots have been sufficiently busy performing control functions that they have needed to be complemented by other specialist aircrew who can focus on other functions. Examples of specialised roles that are relevant to drone operation include navigators, to determine and continually re-determine current location, destinations and flight-paths, and facilities operators, in particular for cargo-handling, and for the operation of on-board equipment such as cameras.

Control, navigation and operation are dependent on the quality of onboard sensors, and on remote data-feeds and control-feeds. Remote feeds in turn depend on infrastructure to support the remote pilot and operators, communications between them and the drone, and communications between any other remote data sources and the drone. In a large proportion of cases, this includes access to GPS satellites. Where communications links may be interrupted, redundant communications channels and fail-safe performance are needed. Experience to date suggests that the range of circumstances in which communications links may be broken is considerable, and that they occur sufficiently often, that such features may be fundamental requirements, even for small and inexpensive drones. In addition, where the airspace may become congested, or where attacks can be expected, collision-avoidance appears likely to quickly become a critical capability.

The communications facilities that are available to the remote pilot and operator, and that are on board the drone, may significantly influence its usability. For example, different frequencies are differently subject to interference and to congestion. Some are limited to line-of-sight operation. Dual and even triple-redundancy of communications channels is accordingly an important safety-feature. In some circumstances, such as where very fine and carefully-timed movements need to be executed by the drone based on human instructions, signal-latency arising from the length of the path that the signals have to travel may negatively affect control, navigation and/or operational quality.

Prior to distinguishing those drone attributes that are definitional, those that are useful bases for distinguishing sub-categories of the general class, and those that are merely descriptive, it is necessary to consider other terms and concepts that intersect with the notion 'drone'.

2.4. *Drone categories and boundary-tests*

In order to isolate the factors that determine which attributes of a drone are definitive, it is helpful to consider the varieties of artefact that are to be defined-in, but also the categories of things that are to be defined-out. The basic concept is of a single aircraft, whose pilot is elsewhere rather than on board. Alternative terms that appear in the literature include:

- Unmanned Aircraft (UA)
- Remotely Operated Aircraft (ROA)
- Remotely Piloted Vehicle (RPV)
- Unmanned Aerial Vehicle (UAV), commonly used in the USA, and in Australia since 1998
- Remotely Piloted Aircraft (RPA), commonly used in Europe, and in Australia since mid-2013

Another consideration is that a remotely-operated drone depends on facilities to enable the pilot to perform their functions, including:

- communication links to pass data to the pilot, from the drone and perhaps from elsewhere
- rendering of data to assist the pilot to make real-time decisions
- means for the pilot to express commands to change the drone's behaviour
- communication links to pass commands from the pilot to the drone

Terms in common use to refer to the drone together with its supporting elements, are:

- Unmanned Aerial System/Unmanned Aircraft System (UAS), primarily used in the USA
- Remotely Piloted Aircraft Systems (RPAS), adopted by ICAO and much-used in Europe

The two families of terms differ to the extent that RPA/RPAS logically excludes fully-autonomous drones, whereas UAV/UAS may include or exclude them.

A number of categories of not-drone are usefully identified. Generally, lighter-than-air craft are excluded, such as kites and balloons, including airships/dirigibles, blimps and zeppelins. So are artefacts that lack controls, including artillery projectiles (cannonballs, mortars, shells), and accidental projectiles (e.g. whose pilot is unconscious or dead). Largely unguided pilotless aircraft (such as the Nazi V1, buzzbomb or doodlebug, in 1944) and largely unguided rockets (such as the Nazi V2, in 1944–45) are generally excluded as well, even though they had simple auto-pilots.

A further category of flying artefacts that needs to be considered is what are commonly referred to as 'model aircraft'. Primitive forms had been evident for centuries. During the first three decades of the twentieth century, sophistication developed quickly, in parallel with manned flight. Model aircraft graduated from uncontrolled flight, to control by means of cables between the controller and the aircraft, and then to wireless control by means of radio signals that activate mechanisms to operate flight controls. Associations of enthusiasts emerged and have remained vigorous.

The distinction between model aircraft and drones is vague. For example under Australian Regulations, "a model aircraft is any unmanned aircraft, other than a balloon or kite, which is flown for sport or recreational purposes, weighing not more than 150 kg …" (CASA, 1998 at 101–3). CASA classifies a drone as a UAS/RPAS rather than a model aircraft if it is "flown for air work – this includes commercial tasks (hire and reward), demonstrations, training, R&D, flying for company internal purposes, etc.", as distinct from "for private or recreational use" (CASA, 2011). On that basis, drones used by neighbourhood and voyeuristic paparazzi are model aircraft, provided that no-one pays a fee for a service performed by the drone. In addition, a competition for, say, delivering a load, finding a missing object or person (e.g. UAVOC, 2014), or tracking a vehicle, is reasonably interpreted as 'sport', even if money does change hands. The distinction between model aircraft and drones is not functional, but essentially regulatory, and based on the purposes of use. Model aircraft are accordingly within-scope of this series of papers.

Size is significant to the analysis of the impacts of drones. The reasons include the need to carry equipment that performs a variety of engine, navigation, communications, computational, control and operational functions, but also because of marketplace realities and, significantly, historical regulatory thresholds. Consideration of the laws of various countries – which are addressed in the third paper in this series – suggests that thresholds of current legal relevance include 150 kg, 20 or 25 kg, possibly 7 kg and 2 kg, 1 kg and 0.1 kg. Some definitions also include reference to dimensions, however, and in at least Australia the weight and/or size threshold is contingent on the category of aircraft (airship, powered parachute, aeroplane, rotorcraft or 'powered lift device' – which is undefined, but presumably relates to hovercraft and perhaps rockets – CASA, 1998 at 101–240).

A design feature that is to at least some degree associated with size is noticeability. Some drones are designed to mimic desirable attributes of flying birds or insects. Some of those, particularly some in the nano-drone range, below perhaps 0.1 kg, may readily escape detection because of some combination of their size and their appearance. This may be incidental or arise from an endeavour to be 'hidden in plain view' (Whitehead, 2013).

A final factor to consider is the possibility that drones, rather than being used independently, may be applied in groups of two or more drones operating in an inter-dependent manner. One reason for such an arrangement is for mutual surveillance and protection, in much the same manner as static CCTV cameras are usefully positioned and oriented so as to include one another within their fields of view. Another example is the use of multiple surveillance drones in order to provide triangulated observations. Beyond small teams of drones, a considerable amount of research has been conducted into swarms of small drones (e.g. Bürkle et al., 2011). Marketers may prefer a collective term with more positive connotations, such as 'flock'. Large numbers of inexpensive drones can achieve redundancy, which is particularly useful in dangerous contexts. On the other hand, swarm-members that are no longer under the swarm-manager's control may create an increased risk of collateral damage.

2.5. *Definition*

One interpretation of a drone is "an unmanned aircraft that can fly autonomously" (Villasenor, 2012). On the other hand, many remotely-controlled aircraft have very limited independence, so it is inappropriate to specify the ability to fly autonomously as a mandatory attribute. The first use of the term 'drone' appears to have been by the US Navy in 1935. It commenced a program to produce remotely-controlled target aircraft. Following a visit to the Royal Navy's well-established program, including demonstration of the 'Fairy Queen' and 'Queen B' or 'Queen Bee' models, the US Navy adopted the word 'drone' for its own artefacts, on the basis that it related to Queen Bees (Mehta, 2013). The usage is traced by the Oxford English Dictionary to 1946, and it first appeared in Encyclopaedia Britannica in 1947.

An important reference-point for this analysis should be the terms and definitions used by relevant organisations around the world. For example, one document from the US regulator FAA defines a UAV as "A device used or intended to be used for flight in the air that has no onboard pilot. This devise [sic] excludes missiles, weapons, or exploding warheads, but includes all classes of airplanes, helicopters, airships, and powered-lift aircraft without an onboard pilot. UA do not include traditional balloons (refer to 14 CFR part 101), rockets, tethered aircraft and un-powered gliders" (FAA, 2013, p.A-5). Agencies' definitions are of course relevant to regulatory analysis. However, regulatory agencies are constrained by constitutional limitations and their own enabling legislation, and in many cases this results in warped definitions of limited value for policy assessment. They are accordingly not heavily weighted in the analysis reported on in this paper.

Of the various industry associations, the Association for Unmanned Vehicle Systems International (AUVSI) appears not to offer definitions of relevant terms, and the UK Unmanned Aerial Vehicle Systems Association (UAVS) merely has a discursive page on meanings of relevant terms (UAVS, 2013). However, Unmanned Vehicle Systems International (UVSI) provides a glossary (UVSI, 2013). It deprecates 'drone', 'UAV' and 'RPV' in favour if 'RPA', and defines RPA as a subcategory of unmanned aircraft “where the flying pilot is not on board the aircraft” (and notes that this is consistent with both ICAO Circular 328 and the definition of the UK regulator CAA, in CAP722). The only other subcategories of unmanned aircraft that UVSI distinguishes are based on size, or autonomy.

The definition used by the US Department of Defense (USDoD, 2011) is that an Unmanned Aircraft (UA) or Unmanned Aerial Vehicle (UAV) is a powered, aerial vehicle that does not carry a human operator, and uses aerodynamic forces to provide vehicle lift. It expressly declares several factors not to be definitional: a UAV can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. USDoD does not consider ballistic or semi ballistic vehicles, cruise missiles, and artillery projectiles to be UAVs.

Based on the above analysis, this paper identifies the elements of a definition of drone as being:

- the device must be heavier-than-air (i.e. balloons are excluded)
- the device must have the capability of sustained and reliable flight
- there must be no human on board the device (i.e. it is ‘unmanned’)
- there must be a sufficient degree of control to enable performance of useful functions

Other attributes that fall short of being definitional factors include size and weight, the nature of the airframe and propulsion, the particular functions performed, the degree of remoteness of control, the nature of the operating organisation, and the degree of autonomy. The definition provided here intentionally encompasses a great many variants; in particular it includes the full range of control options – human, semi-autonomous and fully autonomous; all sizes; and all purposes to which the device is put.

2.6. *Market and regulatory segments*

Beyond establishing a working definition, there is value in identifying categories of drones whose impact and management may be materially different. An approach adopted among regulators is to distinguish ‘model aircraft’ from UAV/RPA, on the basis of ‘private use for sport and recreation’ as distinct from ‘use for air work’. Until recent years, most ‘model aircraft’ were not used for air work. However, the capabilities of small drones are now such that the same model may be used for both purposes.

The single most important basis for recognising distinct categories of drones would appear to be an indicator of size, because this is likely to correlate sufficiently closely with other important factors such as the kinetic impact in the event of aerial collision or crash, payload, the sophistication of navigation and communications facilities, and the level of quality assurance involved in manufacture, maintenance and operation. A clear distinction exists in the marketplace, and in regulatory contexts, between large drones and other drones. In this series, the simple terms ‘large’ and ‘small’ are used.

However, there are also significant differences within the category ‘small’ drones. For example, the mass can vary by a factor of 1000 (Clothier et al., 2010), and the safety features from modest down to none at all. For the purposes of the analysis conducted in this series of papers, large drones are distinguished from three sub-categories of small drones, as follows:

- **large drones**
  These are commonly close to the size of conventional piloted aircraft. An indicative lower threshold, reflecting existing technologies, and aligned with thresholds used by many regulators, is 150 kg for aircraft, and 100 kg for rotorcraft

- **mini-drones**
  These are increasingly capable of performing similar functions to piloted aircraft but are smaller because of the space and weight savings arising from dispensing with pilot-related apparatus.
  An indicative size-range, based on existing regulatory frameworks and discussions, is between 20 kg (or 25 kg) and 150 kg/100 kg. In military contexts, some sources use a lower threshold of 30 kg, with a separate category in the range 5–30 kg. Some other sources have suggested that a maximum size of 1 m in the longest dimension might also be applied

- **micro-drones**
  These fall below whatever threshold is applied for mini-drones, down to some lower threshold of perhaps as much as 7 kg or 5 kg, or 2 kg or 1 kg, or as little as 0.1 kg. Disclosures from industry consultations conducted by the Australian regulator, CASA, during 2013, suggested that a separate category in the 2–7 kg range was being considered

- **nano-drones**
  These are smaller than the lower threshold of micro-drones, and could perhaps be as small as ‘smart particles’ or ‘Micro-ElectroMechanical Systems (MEMS) dust’ (Berlin and Gabriel, 1997), a notion that was subsequently popularised as ‘smart dust’.

With a reasonable degree of clarity about the scope of the drone concept, it is now feasible to identify and discuss drones’ benefits, disbenefits and risks with a minimum of diversions and ambiguities.

3. Drones as opportunity and challenge

This section identifies the aspects of drones that give rise to benefits, and that represent limitations on their use. It then offers a structured overview of the categories of applications to which they can be put.

3.1. *Generic capabilities*

During recent decades, a number of technological advances have combined to enable substantial increases in the capabilities of drones. Lightweight energy sources enable flight and onboard facilities to be powered. GPS chips enable the aircraft to be aware of its location. Inexpensive inertial devices enable the sensing of attitude and direction and the inference of location through de(a)d-reckoning. Miniaturised computers perform computations and maintain communications. The functionality of small model aircraft used to be limited to vicarious joyrides. Now small drones are capable of carrying payloads, and these may be delivered, or used to perform functions such as gathering information.

Small drones may be able to be navigated into locations that are otherwise difficult to gain access to, such as areas that are shielded from view, or that are congested at ground level. A drone also has an advantage where the target may move following paths that preclude pursuit on foot or in a terrestrial vehicle.

In the case of large drones, a key factor has been the savings arising from the absence of an airborne pilot. This changes several aspects of aircraft design:

- it removes the need for space and carrying-capacity:
  - for a pilot
  - for data displays and controls
  - for support facilities for the pilot, such as air-pressure controls, an oxygen supply, and means to bale out of a doomed aircraft
- it enables a much larger proportion of the space and weight-bearing capacity to be applied to:
  - fuel, hence greatly increasing flying-time and range; and/or
  - the functions to be performed
- it may enable lower investment in features that ensure the safety of the onboard pilot

Fixed-wing drones have advantages in relation to speed, range, endurance and robustness. Rotorcraft, on the other hand, requires less space for take-off and landing, can hover, and are more manouevrable.

Large drones remain expensive, but are attractive to the military and to some extent to national security and law enforcement agencies. In the smaller drone-segments, on the other hand, the rapid improvements in functionality have been accompanied by reduced costs. Production volumes have increased, lowering unit costs still further. Small drones are sufficiently inexpensive that they are offering promise not only to hobbyists but also to business enterprises and government agencies generally.

Small drones enjoy a regulatory advantage over large drones, in that many features that are requirements of both manned aircraft and large drones for safety reasons are not (to date) imposed on small drones. As the capabilities of small drones have increased, new possibilities have emerged. In addition, some substitution has occurred, whereby small drones perform functions that previously required large aircraft. A mature example is weed-spraying, at least for small areas, particularly in Japan.

Purchase prices for small drones are currently of the order of, for hobbyist devices USD/EUR 100–1000, and for low-end professional use USD/EUR 5000–10,000. For some applications, the indicative costs per hour of flight are currently of the order of USD/EUR 25 for small drones compared with USD/EUR 750 for manned fixed-wing aircraft and USD/EUR 1350 for manned rotorcraft. For applications for which the limitations are acceptable, such as the gathering of moderate-quality image and video, small drones are now vastly more economic than aircraft, and much more economic than large drones. This is naturally giving rise to both substitution effects and new customers.

3.2. *Generic limitations*

Small drones are subject to a range of very substantial technical limitations, in relation to load-capacity, flight-duration (currently 15–30 min), flight-range, flight-speed, reliability and safety. In countries that permit their use for commercial purposes, the light-handed regulatory framework that is applied to them places restrictions on such factors as where they can be operated, how close to people, and how far from the remote pilot.

Large drones also have technical limitations, but these are much less substantial than is the case with small drones. They are dependent on more sophisticated supporting infrastructure for the remote pilot than is the case with small drones, and this cancels out a lot of the cost-savings that arise from no longer having a pilot on board. In practice, most applications require facilities operators in addition to the pilot, and they also require supporting infrastructure. Moreover, if the infrastructure fails, the reliability of the drone may plummet. The safety of large drone operations is as yet nowhere near the same level as has been achieved, and is sustained, with commercial aviation services. Incidents occur far more frequently than in civilian operations, and remotely piloted passenger services are barely at the experimental stage.

In identifying the categories of opportunity for applying drones, the following further considerations also need to be taken into account:

- particular features are needed for effective operation at particular altitudes
- particular aircraft characteristics are important for particular applications, such as the ability to hover, to quickly re-orient the aircraft or a device that it carries, to sustain a very steady flight along a pre-determined bearing, to remain airborne for long periods, and to offer flexibility in the choice of take-off and landing locations and conditions
- weather frequently plays havoc with the aerodynamics of all forms of airborne devices
- weather sometimes plays havoc with both line-of-sight visibility and electronic communications
- fire, smoke and heat create serious challenges
- in a variety of circumstances, a remote pilot is unlikely to have all of the desirable situational information available, and hence may make decisions that are less good than the decision an on-board pilot would have made. (In other circumstances, however, a remote pilot may have better access to relevant data, and may be better placed to make good decisions)

3.3. *Generic applications*

The following section considers a range of specific applications, in order to gauge drones' impacts and implications. First, however, a general framework is suggested within which the wide range of potential applications can be placed.

Although the focus of this series of papers is on civilian applications, a great deal of the momentum, particularly in the large drone segment, has been generated in the military domain, and some of the categories of application that have arisen there may spill over into more widespread use. A US-centric history of combat drones is in Chapter 1 of Yenne (2004), and a broader international perspective is in Newcombe (2004). The following are specifically or at least primarily military uses:

- as a target, since the 1930s
- as a means of annoyance and attention-diversion. Drones are reputed to have been successfully used by Israel to draw enemy fire, during the Yom Kippur War in 1973
- as a communications-relay device
- as an electronic warfare platform, to disrupt opponents' communications
- as a means of performing assaults:
  - on ground and maritime targets, conceived no later than 1915 in the USA, described in hobbyist magazines (PM, 1940), and implemented at latest by the USA in Yemen in 2002 (Bowden, 2013)
  - on airborne targets, including other drones. Examples are currently lacking due to parties that have access to such technologies not yet having entered into conflict with one another

Multiple US defence sector documents identify as key prospects for drone work the kinds of “dull, dirty, or dangerous missions” in which a human pilot is a limiting factor in performance. That principle is equally applicable outside the military context. Examples of dangerous civilian purposes include:

- searches for missing persons and vessels, particularly in severe weather or over or within difficult terrain, but also for long periods of time and over long distances
- emergency management, including surveys of fires, volcanic activity, earthquake zones, flood zones, and malfunctioning nuclear reactors
- fire-fighting
- monitoring of atmospheric conditions shortly prior to and even during ’heavy weather’

Categories of ‘dull’ civilian missions include:

- staying within a tightly-defined zone, e.g. in order to provide a communications link or perform a static surveillance function
- staying on tightly-defined flight-paths, e.g. search-patterns for lost bush-walkers/hikers/sea-farers/surfers, aircraft wreckage, and missing sea-vessels, and during the conduct of ground surveys
- other routine activities in which limited human intelligence is required, such as conducting surveillance of the electromagnetic spectrum and the collection of other kinds of data
- goods transportation

A widespread use of drones is as a platform for surveillance devices, to enable observation, recording and transmission. This dates as far back as the end of the 18th century (using leashed balloons), and has been used increasingly intensively by various countries since the 1960s. The kinds of data that can be gathered are diverse, and include:

- electromagnetic-spectrum data:
  - image and video in the human-visible range
  - near-human-visible image and video (in particular, in the infra-red spectrum)
  - radio transmissions
  - other electronic transmissions
- other kinds of data:
  - sound in the human-audible spectrum
  - air-pressure waves of other frequencies
  - biological measures
  - magnetic and other geophysical data
  - meteorological data

It is noteworthy that 25 of the 26 commercial drone operators that had been approved to April 2013 by the Australian regulator (CASA, 2013a) had nominated surveillance uses (specifically aerial photography, aerial spotting, aerial survey, powerline inspection and surveillance), with just a single instance of a target drone. By the end of 2013, there were 69 operator certificate holders, of which 1 was approved as a target drone, and 1 was approved for training only, but 68 were approved for the various surveillance functions (CASA, 2013c).

Surveys of the formal literature and media sources give rise to a vast array of specific applications, some real, some emergent and some yet to be realised. Table 2 provides a framework for categorising those applications, based on the function performed and the party that sponsors the activity.

4. Specific applications

The purpose of this series of papers is to identify impacts and implications of the drone epidemic that give rise to the need for policy and regulatory responses. This section considers a number of specific applications that are evident within the framework provided by Table 2, and that were selected because of their apparent relevance to that purpose.

A wide range of current and potential civil applications exists. The following sections outline the primary application areas, with deeper consideration given to those that raise key issues in need of attention. The application areas discussed below are:

- Load-Delivery
- Passenger Transport
- Hobby and Entertainment Uses
- Journalism
- Voyeurnalism
- Law Enforcement
- Community Policing, Voyeurism
- Hostile Load-Delivery

Table 2 – Generic application categories.

Load delivery – Of what? And why?

- Consensual cargo carriage, point-to-point (books, medications, pizzas)
- Consensual cargo carriage, point-to-area (weedicides, pesticides, fertiliser, water to fires)
- Non-consensual cargo carriage, point-to-point (projectiles, explosives, inflammables)

Surveillance – Of what? And why?

- Of a scene, for reconnaissance and situational awareness (crime and emergency scenes for service personnel safety and tactical response decisions)
- Of an area, for search (missing people, poachers, livestock, feral animals)
- Of an area, for imagery (photographs, videos, infra-red)
- Of an area, for measurement (geophysical variables, atmospheric variables, flora and fauna counts)
- Of infrastructure, for inspection and audit (cables, pipes, towers, borders)
- Of individual animals including humans (for activity monitoring, pursuit)

For whom?

The following categories of application sponsor can be mapped across the above sets:

- law enforcement agencies, emergency services agencies, physical environment agencies (atmospheric, environmental, maritime), other government agencies
- media organisations, other corporations
- communities, individual hobbyists
- organised crime organisations, individual criminals

4.1. *Load-delivery*

Among the recent flights of fancy have been drones used for ammunition re-supply, the rescue of injured people, and the delivery of medicines, pizzas and books. Many characteristics of drones generally, and of contemporary drone technologies act as major limiting factors on realistic uses for load-shifting. The special case of delivering loads in ways that are hostile to people and property at the delivery location is addressed in a later section.

An indication of the more likely candidate applications is provided by a longstanding use of drones in Japan, where, through the 1990s, over 1000 aerial devices weighing 50–60 kg and with a payload of 20–30 kg, were used for crop-spraying. According to some sources, the practical capacity of such drones is limited to about 1 ha per day per drone; but in the particular context it appears to be highly cost-effective.

The application involves constrained areas, populated by few people, few buildings, little high infrastructure such as electricity lines, and no other aircraft. The absence of such threats to the drone's operation, combined with high degrees of computer-mediation embodied in the aircraft's control, has greatly reduced the skill-levels demanded of pilots (Wong, 2001). Where such threats exist, on the other hand, the limited safeguards available give rise to substantial residual risks to people and property.

4.2. *Passenger transport*

To date, all passenger aircraft carry a human pilot. Although pilots depend on a great deal of technology, and autonomous flight, take-off, and with qualifications autoland, are all in use as individual elements, no passenger aircraft to date operate fully autonomously. Ross (2011) discussed factors that need to be addressed before passenger aircraft can be controlled by remote pilots, emphasising collision avoidance technology and public acceptance. In the UK, a modified commercial aircraft has conducted a flight through shared airspace, controlled after take-off and before landing by a remote pilot (Prigg, 2013). It is apparent that safety levels, even among large drones, are to date so far below existing civil aviation norms that public acceptability is decades away.

4.3. *Hobby and entertainment uses*

The majority of personal use of model aircraft has long been by individuals acting with considerable care and responsibility, typically as members of a club that sets constraints, arranges insurance cover, and uses dedicated and somewhat isolated airfields. The costs involved in acquiring and operating aerial devices has plummeted, however, and the less expensive models have now come within the price-range of adolescents' Christmas presents. The rash of remote-controlled model cars terrorising neighbourhoods may be about to give way to a rash of remote-controlled devices that are not terrestrially-limited, that may exhibit many additional failure-modes, whose impact-velocity when falling out of the sky may be rather greater than that of out-of-control model cars, which include rapidly-moving propellers that give rise to high levels of threat of injury and property damage, and whose operators may exhibit little responsibility and have little in the way of assets and no insurance.

The international regulatory regime does not appear to distinguish uses of these kinds from other uses. In some jurisdictions, however, the regulatory framework applicable to 'model aircraft' is different from that applicable to drones. In Australia, the key difference is that, to qualify as a model aircraft and not as a 'UAV', a device must be "flown for sport & recreation and education" and/or "for private use", as distinct from "for air work, including commercial operations, in activities such as aerial photography, surveying and law enforcement" and/or "for commercial 'hire and reward'" (CASA, 2013b).

CASA has approved an association, the Model Aeronautical Association of Australia (MAAA), to "govern the operation of" model aircraft, within the terms declared in CASR 101 (CASA, 1998). However, that apparent delegation is only applicable to club members operating from an MAAA-approved location. And in any case, MAAA has virtually no enforcement mechanisms. CASA, meanwhile, is casual about the regulation of small drones (CASA, 2012), to the point of declaring that they are not amenable to regulation: "significant technological advances and associated cost reductions have made RPAs more accessible, including at the very small end of the RPA scale – equivalent to the hobby level have made the application of this regulation somewhat ineffective … [Under forthcoming proposals,] RPA that are very small, for example less than 2 kg would not require any approval as RPA of this size are considered to pose a low risk and low potential for harm" (CASA, 2013d).

4.4. *Journalism*

Journalism is the preparation of news, current affairs and documentaries, by means of disciplined collection, analysis, cross-checking and presentation of information regarding events and issues that are 'in the public interest'. Journalism includes 'opinion', but opinion needs to be clearly distinguished as such. Inexpensive drones have been applied to journalism at least since early in the new century (Corcoran, 2012). It becomes possible to afford views from perspectives that were previously unprocurable without using expensive aircraft. This greatly increases the scope for the observation platform to hold position and monitor, rather than just to over-fly and produce snapshot imagery and video. Pursuits become more feasible, less expensive, and less dangerous – at least for the chaser, if not for the fugitive and bystanders.

Early examples of constructive uses by the media include by News Corp in the US in 2011 to film flood damage, and by Australia's 60 Minutes, which filmed while over-flying the Christmas Island immigration detention centre in May 2011 (Corcoran, 2012). Use at sporting venues in Australia has attracted considerable attention (Corcoran, 2013). The new capabilities give rise to a range of issues. For assessments of policy issues arising from journalistic uses of drones, see Goldberg et al. (2013) and Clarke (2013).

Over the last 50 years, while parliaments have been asleep at the wheel, the costs involved in data-collection have given rise to a balance between media intrusions and personal seclusion – a balance that is often markedly against the interests of some individuals, but nonetheless some kind of balance. The emergence of inexpensive surveillance technologies, including drones, is shifting that balance considerably, in such ways as the following:

- the perspective of the observation is lifted up and away from the limited point-of-view of a human being: drones add another dimension, literally as well as metaphorically. This may provide a sense of greater authority in the imagery than it actually warrants
- multiple sources and live feeds can be used at the same time
- a much greater degree of automated monitoring is feasible, including a notification service to a reporter or photographer when something interesting may be happening – enabling what are, in effect, automated stake-outs
- a much greater degree of surveillance extensiveness is feasible, approaching pervasiveness, e.g. by in effect being at each of the locations associated with a target at the same time
- a much greater degree of surveillance – intensiveness is feasible, approaching continuous monitoring, unrestricted by time of day, length of wait and human attention-span
- the notions of 'informant' and 'research assistant' expand from a party who observes and then describes from memory, to anyone who can support their description with evidence

A number of additional implications are readily foreseeable, including potential conflict with law enforcement and emergency services, and increased attractiveness to law enforcement agencies of access to media sources. Instances of irresponsibility have arisen in relation to the use of surveillance tools by journalists. In most such instances to date, however, the behaviour of the media personnel has lacked the justification of being 'in the public interest'. They are accordingly treated as a distinct application area, in the following section.

4.5. *Voyeurnalism*

A form of debased or corrupted journalism is widespread, in which information regarding events and issues is gathered and presented that is not 'in the public interest', but rather is 'what the public is interested in', or 'what the public may be able to be made to be interested in'. In some cases, the practices depart further from journalism by presenting information in a constructively misleading manner, or inventing pseudo-information or 'fantasy news'. A century ago, this category of media was referred to in the USA as 'yellow press' and 'yellow journalism', and the term 'sensationalist media' is used in the UK. The word 'voyeurnalism' is a concoction by this author, to deal with the absence of an established term (Clarke, 2012).

A representative set of media abuses of privacy is catalogued in Clarke (2012), almost all of which involve voyeurnalism, not journalism. Helicopters and fixed-wing aircraft have been too expensive for any significant use by paparazzi, whereas drones are creating a 'Paparazzi Aloft' problem. Drones enable barriers in the line of sight to be overcome, and imagery to be captured. Vertical and angled shots can be achieved. Continuous monitoring can be undertaken of bottleneck locations such as the target's front door. Tracking becomes much easier. Paris Hilton was filmed, and tracked, by drones, on the French Riviera as long ago as 2010. A 2013 story arose from drone use at Tina Turner's wedding in Switzerland.

Given the dedication of paparazzi, and the money that can be made from 'scoop' pictures of celebrities and notorieties, it is readily predictable that there will be frequent abuses of the power of drone-borne cameras. In September 2012, there was considerable coverage of photos of Kate Middleton (the Duchess of Cambridge), captured from long distance by means of a telephoto lens. The increased scope afforded by drones leads to the conclusion that she, and many other celebrities, can rest assured that their bare breasts are fair game, anywhere, anytime. More dangerously, the prospect of ill-judged pursuits is much-increased, as is the risk of encouraging ill-judged avoidance manoeuvres.

4.6. *Law enforcement*

An area of high payback from drones is emergent in relation to relatively very safe and quick reconnaissance at emergency scenes, resulting in effective and relatively safe tactical responses.

On the other hand, the scope for using drones as a form of highly-mobile, remotely-managed CCTV was apparent to law enforcement agencies at an early stage, e.g. Page (2007). Some false starts have been experienced, however, with the application of drones in Liverpool appearing to have taken three years to achieve an arrest, and then being found to be itself in breach of the law (Lewis, 2010). Drone-based surveillance is confronted by much the same challenges that have seen almost all CCTV schemes prove to be abject failures (e.g. Edwards, 2008; Groombridge, 2008). Successes will seldom arise from random image-capture. They will depend on professionalism, commitment and above all sufficient human resources applied to an investigation.

A particular concern is the extent to which law enforcement drones will be more like those designed for military or for civilian purposes. Since 2001, police forces in hitherto relatively free nations have adopted more aggressive approaches, and have begun to resemble the militarised police forces common in un-free nations. There is a serious risk that law enforcement drones and supporting systems will have characteristics in common with military facilities – including designs intended for unconstrained surveillance of an enemy, and lightly-constrained violence against an enemy, and which generate vast quantities of stored data that require integration and interpretation and hence produce information overload which may materially affect the quality of operators' judgements (Drew, 2010). The much higher cost of products for the military compared with those for civilian uses is a counter-balance against this risk. On the other hand, funding for law enforcement drones will almost inevitably be provided during periods in which law and order issues dominate common sense, and hence occasional large sums of money may be made available, enabling (de-militarised?) versions of military products to be acquired.

A sci-fi author provided some detailed scenarios for security drones: "[micro-drones] programmed to hang in space … watching and listening, so that nothing got through [undetected]" (Stephenson, 1995, pp. 56–57). Those (imaginary) surveillance drones were complemented by 'tagger' nano-drones, which attached themselves to a person immediately after they committed a criminal act. Together, the recorded video and the identification of the suspect delivered conclusive evidence to the courts (pp. 97–98, 127, 139).

That is 'visionary' or 'speculative'. However, whether or not such specialised security micro-drones and nano-drones actually eventuate, the prospect exists of a 'Panoptic Aloft'. The social, cultural and political risk is that many more people will cease to perform lawful behaviours, whereas there will be only limited deterrence of criminal behaviour, particularly crimes of violence. Another sci-fi author projected current surveillance capabilities a much shorter distance into the future, and included a key role for micro-drones (Bear, 2010). He concluded that, in the emergent world of coordinated little brothers, "Vengeance is everywhere. Nobody gets away with anything. We're terrified of our neighbors [and] forgiveness and forgetfulness become conveniences of the past". In the bleak view of the cyberpunk genre, "In an era when everything can be surveilled, all we have left is politeness" (Stephenson, 1995, p. 192).

4.7. *Community policing, voyeurism*

In addition to formal policing, drones have potential application by communities themselves, by individual, 'responsible citizens', by vigilantes, and by individuals and groups seeking to impose their own morality on others. A positive aspect of this is early recognition of trouble-spots, enabling early arrival of calming influences. The scope also exists for communities to monitor suspected polluters. There have been reports of use by groups seeking to protect wild animals (T&D, 2012) and to expose abusive chicken-farming practices (Murphy, 2013). A surf life saving association and various beachside local government agencies have considered and experimented with drones for shark-spotting (SLSA, 2012; RCC, 2013).

A less positive prospect is 'nagging aunty' drones, identifying what an algorithm – or an inference from an example-base or from a neural-net – determines to be misbehaviour, and then using recorded or synthesised voice to reprimand the computed perpetrator, and perhaps using intense sound or light to encourage the undesirables to leave the area (Stephenson, 1995). Another possibility is a permanent drone-enabled 'neighbourhood watch' of people regarded as strangers or aliens, such as 'gypsies', newly-settled refugees, and sex offenders.

Another potential is for individuals and groups to use the guise of community protection to indulge in voyeurism – i.e. sexual gratification through observation. CCTV operators are well-known to indulge in opportunistic observation of people within their cameras' fields of view (Smith, 2004), and instances abound of cameras installed in locations where titillating scenes may be able to be observed. Drones provide considerably greater empowerment to the voyeur than installed cameras, because of the flexibility of location and angle.

4.8. *Hostile load-delivery*

Drones offer prospects as a means of perpetrating violence, in such ways as:

- carriage of weaponry (e.g. pistols, cannon, missiles)
- delivery of explosives and inflammable materials (bombs)
- use of the drone itself as a guided weapon (pilotless kamikaze missions)
- interdiction of other aircraft's flight paths (attack swarms)

This section begins by considering what has been learnt from military uses for hostile purposes, and then applies it in the contexts that are within the scope of the present analysis: applications by law enforcement agencies and commercial security services, and by terrorists, criminals and thrill-seekers.

Military applications have given rise to a great deal of experience, particularly use by the US in Yemen, Iraq, Afghanistan and Pakistan, in many cases with the pilots on the US mainland, remote from the region, the battle-zone, the time-zone and local culture (Bowden, 2013). Some of this experience is relevant beyond the military sphere, in particular:

- malperformance arising from information overload on analysts

  A substantial literature exists on the challenges faced by those seeking to extract information from the flood of surveillance data transmitted by drones (e.g. Drew, 2010)

- malperformance arising from cognitive overload on pilots

  Even with the advantages of being ground-based, the standard of performance required of a drone pilot, and the degree of performance stress placed on them, can approach that of an on-board pilot. Cognitive overload can result in dangerously slow or dangerously erroneous commands. It may also reduce the ability of the drone pilot and facility operators to empathise (Coker, 2013), and, it has been surmised, even to perform their functions (Sterling, 1994, p. 78, 81)

- dehumanisation

  The controls used by remote pilots bear a relationship to games technologies. A range of techniques being developed in the context of Point of View Surveillance (PoVS) technologies are potentially applicable as well, such as image intensity manipulation and colouration, augmentation of displays with infra-red imagery, vision-width greater than that of natural human vision, multiple eyes pointing in different directions, warning overlays, and 'action replays'. The risk arises of facilities operators becoming detached from the real-world impacts of their actions, resulting in breaches of the rules of engagement, and the potential for extra-judicial murder, and low valuation of collateral damage to civilians.

A further important insight from the military sphere, however, is that controls can be designed into the use of drones to prevent some negative impacts and to mitigate others. The military use of 'killer drones' is argued to involve highly articulated structures and processes, rules of engagement, monitoring, and reviews. Will such controls be applied in civilian contexts? Will pre-evaluation and review processes be 'a closed shop' as they are in military contexts, or will they be transparent, as befits democratic governance?

Between the military and civilian categories lies a grey area of 'para-military' use. Observation and pursuit of individuals reasonably suspected of criminal behaviour is a civilian matter. In many countries, civilian police are armed, at least when they are in a context in which violent confrontations may occur. Is it appropriate to apply military drone capabilities in a free society for even border protection functions, let alone civilian policing? Will law enforcement drones also carry arms, controlled remotely, or perhaps even autonomously? Will law enforcement agencies purchase second-hand, or even new, military drones? At this stage, "Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program" (IACP, 2012). But will this nominal discouragement abate, once the public has come to accept police use of drones?

Law enforcement was for many decades considered to be a function of the State, delegated to agencies with specific functions and powers, performed by staff of those agencies, and at least nominally subject to controls by the Executive. In recent years, however, law enforcement has been outsourced to business enterprises that would have earlier been called 'mercenaries'. Such controls as exist are largely contractual rather than legislative, and law enforcement agencies are subject to inevitable constraints on the manner in which they exercise control over sub-contractors to whom they have outsourced much of their expertise, their resources and their power. The concerns about inappropriate usage of drones by law enforcement agencies escalate when private security companies are involved.

The virtual reality aspects of drone controls are relevant because they offer advantages and hence are likely to migrate into the civilian realm. The concern exists that a law enforcement officer's or civilian security employee's physical remoteness from the real world in which the drone is operating may be compounded by the air of unreality arising from additional information overlays. A person's detachment from physical reality might lead to decisions and actions that are inconsistent with the individual's normal morality, or that indulge fantasies that are normally kept under control by social norms. The detachment, combined with the thrill of live entertainment, can be expected to lead to enthusiastic voyeurism, which constitutes harassment, and will on occasions cross the boundary into stalking, and in some cases may culminate in acts of violence. The likelihood is that the social and institutional controls will be looser than is argued to be the case in military contexts, and in the case of micro- and nano-drones, perhaps almost entirely ineffective.

Inexpensive but useful remote-controlled aircraft are available beyond the law enforcement arena. Whereas the armed forces of States use large devices with substantial payloads and sophisticated custom-built electronics to deliver expensive explosives, terrorists make do with low-grade and readily available explosives. The payloads available with cheap, small drones may be sufficient for them to achieve their aims.

Commercial and even hobbyist drones are capable of being 'weaponised' in various ways. A small payload of explosives or incendiary materials, delivered at an appropriate location, could act as a detonator for a much larger explosive potential. Or it might exacerbate a bottleneck or cripple a control element within critical infrastructure (an electricity or water supply, an airport, a data communications facility, a data processing centre). Or an individual drone could be deployed against an aircraft during takeoff or landing, perhaps through a jet-engine air-intake. Where the perpetrators want to cover their tracks, they might avoid the use of their own drone, and instead hijack a hobbyist or commercial drone to perform the task. Beyond the prospect of an individual drone, a swarm of micro-drones floated across a flight-path could be relied upon to paralyse air transport, and probably also ground transport in the vicinity, for many hours.

Although media attention is easily gained for terrorist uses, less dramatic criminal enterprises can readily apply drones to activities such as extortion, the neutralisation of security infrastructure, and the diversion of law enforcement resources while a crime is being committed. Meanwhile, individuals with no specific criminal intent may conduct experiments and enjoy the spectacle or the feeling of achievement.

The almost complete absence of the once-touted threat of anthrax infiltrated into city water-supplies suggests that attacks of such kinds are far less simple to effect than they are to dream about. On the other hand, the theoretical existence of the threat is sufficient to ensure nervousness on the part of national security apparatus and a convenient excuse when justifications are sought for further repressive measures. Whether real or imagined, these potential implications of the drone epidemic add to existing tensions within contemporary societies.

4.9. *Conclusions*

The sample of drone applications considered in this section has identified a range of impacts and implications that call for policy responses and adaptation of regulatory frameworks.

A further consideration is the likelihood of defensive measures being taken by organisations and individuals who are concerned they may be subject to unwelcome observation or to attack. In addition, some individuals and organisations that are targeted by drone-based activities may move beyond defensive measures to actively pre-counter threats or retaliate against the perpetrator. Counter-measures against drones include:

- jamming of control signals and/or data transmission
- interference with geo-location data, such as the GPS data reaching the drone (BBC, 2012)
- hacking of software
- ground-based interdiction of the drone
- predator-drones
- defensive drone-swarms
- interference with the infrastructure on which remote pilots and facilities operators depend
- interference with remote pilots and facilities operators themselves

Any action that undermines a drone's operation increases the risk of malfunction, and hence of damage not only to the drone but also of anything it collides with as a result of the malfunction. Any item that is used to target a drone (a bullet, a water-jet, another drone) may have that effect, but with the added feature that the projectile itself becomes an additional threat to other objects and individuals in the vicinity. To date, there appear to have been few ill-judged defensive measures, pre-counters or acts of retaliation. However, an animal rights group in South Carolina reported that a drone that they used to video a live-pigeon shoot was shot down by hunters, in close proximity to a highway (T&D, 2012); and Deer Trail, Colorado was reported as playfully considering paying bounties for the shooting-down of unmanned drones (Coffman, 2013). Over-reactions of these kinds need to be factored into the policy and regulatory discussions.

Serious events involving drones are newsworthy. In addition, less serious events are likely to be misrepresented by some sections of the media. For example, a sober report of a micro-drone crashing into the Sydney Harbour Bridge (Kontominas, 2013) was dramatised in London and Milan by reference to the presence in the Harbour of international naval vessels and of the UK's Prince Harry. Media reports of this nature inevitably escalate the perceived significance of such events. They can be expected to give rise to knee-jerk reactions by politicians, resulting in additional 'safeguards' being put in place. Many such measures are likely to prove to be wasteful and ineffective, and to involve collateral damage to civil liberties.

5. Implications for risk management

Many of the attributes of drones that have been discussed in this paper have the potential to create challenges for existing regulatory regimes. This section identifies several aspects that appear to be of particular significance for the assessments of regulatory arrangements in the third and fourth papers in the series.

Care is required in defining what it and is not a drone. The devices evidence considerable diversity across multiple dimensions. Not only do their capability profiles vary, but so do their risk profiles. One categorisation of particular relevance is the drone's size. Large drones have large payloads, and with that come high expectations of redundant designs and quality assurance. On the other hand, small drones – including mini-, micro- and nano-drones – may be subject to correspondingly lower safety-design expectations, yet they are still capable of causing considerable harm. Controls need to reflect the scale of the disbenefits and risks, rather than just the costs-of-manufacture, but there is bound to be opposition to setting minimum thresholds for safety and liability.

Two primary themes have emerged from the analysis. One is the potential for harm to property and people. That is the focal point of the third paper in this series. Some of the controls that are effective in the context of piloted aircraft may be less effective for drones, not least because existing institutions, from the Convention on International Civil Aviation downwards, are structured on the assumption that aircraft have an onboard pilot. The much-lowered personal risk faced by a remote pilot is bound to affect concentration and decision-quality. An additional factor is that the quality and safety levels that apply to piloted aircraft bring with them high costs that are not sustainable in many segments of the drone market. In the mini-drones segment, there is the risk of compromise of safety features. In the micro-drones segment, on the other hand, there is the risk of manufacture and operation with very little regard for safety. Drone costs have fallen, particularly for micro-drones for the consumer market; and, from the outset, nano-drones have been conceived as very inexpensive, mass-produced items. It can be reasonably anticipated that drones that have the attribute of expendability will have less care taken in relation to both the drones themselves and their negative impacts, particularly after they have ceased to fulfil a useful function for the party that is (in some sense) responsible for them.

A particular concern is the wide array of 'failure modes' that afflict drones. After a large drone being used for border patrol purposes crashed in New Mexico in 2006, a large number of causal and contributory errors were identified (Carrigan et al., 2008). The earliest UK use for law enforcement purposes culminated in the drone's loss in the Mersey River off Liverpool (BBC, 2011). The earliest media use identified in Australia ended with the drone crashing, fortunately for those in the detention centre that had been filmed, in the adjacent Indian Ocean (Corcoran, 2012). A similar cautionary tale arises from the demonstration of what was claimed to be the first police-owned drone, in Texas – a large and expensive drone rather than a micro-drone. It crashed into a police vehicle which was, fortunately, armoured (Biddle, 2012). Then, in Incheon, South Korea, a large, commercial drone crashed into its control truck, killing an engineer and injuring two pilots who were 'remote', but insufficiently so (Marks, 2012). In May 2013, video emerged of an accident in August 2004, when a small drone, a German Luna weighing about 40 kg, crashed as a result of being caught in air turbulence from a commercial passenger aircraft on approach to Kabul airport. A major disaster would have been likely had the two collided instead of having a near miss (Spiegel, 2013). There have been crashes of micro-drones in the central business districts of Auckland (Mortimer, 2012) and Sydney (Kontominas, 2013).

Accident investigation reports for these incidents have not been located, but media reports have suggested that the causes have often been interruptions to GPS or control-flow transmissions, coupled with inadequate fail-safe designs to cope with signal-loss. At least one arose because the drone was in congested airspace but did not have a collision avoidance system (Spiegel, 2013). It appears that, to date, even the largest and most expensive drones do not carry such equipment (Harvey, 2013). These accidents give rise to ample cause for concern about the potential for harm to people and property, and highlight the need for an assessment of the adequacy of existing regulatory frameworks for public safety.

The other theme that has emerged is the surveillance of individuals and its impact on behavioural privacy. Significantly different issues arise in the case of journalism, voyeurnalism, law enforcement community policing and voyeurism. These are considered in the fourth paper in this series.

6. Conclusions

The first requirement for a calm assessment of the impacts and implications of drones is clarity about the scope of the notion, their attributes, and the opportunities and challenges that their applications embody. This paper has identified the definitional factors for a drone as comprising (a) a heavier-than-air device, (b) flight reliability, (c) the absence of an on-board pilot, and (d) sufficient control that useful functions can be performed. Attributes that are important in determining the impacts that need to be managed include above all size, but also functionality, the nature of the operating organisation, the remoteness of the pilot, and the degree of autonomy.

As discussed in the third paper in this series, large drones are widely perceived as being within-scope of existing regulatory frameworks, as having navigation and communications capabilities comparable to piloted aircraft, and as being manufactured, maintained and piloted within quality assurance frameworks similar to those applying to the manufacturers, maintenance organisations and pilots of manned aircraft. Critically, however, the same does not apply even to mini-drones, let alone to the burgeoning population of micro-drones and the rapidly-emergent category of nano-drones.

Some of the impacts and implications depend not only on drone-size, but also on the category of application to which the drone is put. In particular, surveillance applications need to be differentiated according to the purpose and the operator. Harm will also arise from intentional actions by drones and their operators, including acts of direct violence against people and property, including other drones.

This paper has delivered a comprehensive framework within which the later articles in the series are able to analyse the issues in depth, assess current regulatory frameworks, identify areas in which those frameworks are deficient, and evaluate the prospects of effective reform.

REFERENCES

Armstrong AJ. Development of a methodology for deriving safety metrics for UAV operational safety performance Measurement report. Master of Science in Safety Critical Systems Engineering, Department of Computer Science, York University; 2010. January 2010, at, http://www-users.cs.york.ac.uk/~mark/projects/aja506_project.pdf.

BBC. 'Police drone crashes into River Mersey' BBC News, 31 October 2011, at http://www.bbc.co.uk/news/uk-england-merseyside-15520279; 2011.

BBC. 'Researchers use spoofing to 'hack' into a flying drone' BBC News, 29 June 2012, at http://www.bbc.co.uk/news/technology-18643134; 2012.

Bear G. Little brother is watching. Commun ACM Sep 2010;53(9):111–2.

Bento MdeF. 'Unmanned aerial vehicles: an overview' inside GNSS (Jan–Feb 2008) 54–61, at http://www.insidegnss.com/auto/janfeb08-wp.pdf; 2008.

Berlin AA, Gabriel KJ. Distributed MEMS: new challenges for computation. IEEE Comput Science Eng Jan–Mar 1997;4(1):12–6.

Biddle S. 'Police drone crashes into police' Gizmodo, 6 March 2012, at http://www.gizmodo.com.au/2012/03/police-drone-crashes-into-police/; 2012.

Bowden M. The killing machines: how to think about drones. The Atlantic [at], http://www.theatlantic.com/magazine/print/2013/09/the-killing-machines-how-to-think-about-drones/309434/; September 2013.

Bumiller E, Shanker T. War evolves with drones, some tiny as bugs. The New York Times; 2011 [19 June 2011, at] http://agriculturedefensecoalition.org/sites/default/files/file/constitution_1/1W_2011_War_Evolves_With_Drones_Some_Tiny_as_Bugs_for_Spying_Other_Purposes_U.S._Air_Force_NYTimes_June_19_2011_Entire_Article.pdf.

Bürkle A, Segor F, Kollmann M. Towards autonomous micro UAV swarms. J Intell Robot Syst 2011;61(1–4):339–53.

Carrigan G, Long D, Cummings ML, Duffner J. 'Human factors analysis of predator B crash' Proc. AUVSI: Unmanned Systems North America, at http://www.web.mit.edu/aeroastro/labs/halab/papers/Carrigan_AUVSI.pdf; 2008.

CASA. Civil Aviation Safety Regulations (CASR). Civil Aviation Safety Authority; 1998 [1998, at] http://www.austlii.edu.au/au/legis/cth/consol_reg/casr1998333/.

CASA. Differences between Unmanned Aircraft Systems (UAS) and model aircraft. Civil Aviation Safety Authority; 2011 [February 2011, at], http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_100375.

CASA. Intruder in the circuit' aircraft. Civil Aviation Safety Authority; 2012 [17 December 2012, at], http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_101298.

CASA. List of UAS operator certificate holders. Civil Aviation Safety Authority; 2013a [26 Apr 2013, at], http://web.archive.org/web/20130426094414/http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_100959.

CASA. Differences between Unmanned Aircraft Systems (UAS) and model aircraft. Civil Aviation Safety Authority; 2013b [undated but presumably of 2013, at], http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_100375.

CASA. List of UAS operator certificate holders. Civil Aviation Safety Authority; 2013c [31 December 2013], http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_1009595.

CASA. RPAs (drones) in civil airspace and challenges for CASA. Civil Aviation Safety Authority; 2013d [3 July 2013, at], http://www.casa.gov.au/scripts/nc.dll?WCMS: STANDARD::pc=PC_101593.

Chao AY, Cao YC, Chen YQ. Autopilots for small unmanned aerial vehicles: a survey. Int J Control, Automation, Syst 2010;8(1):36–44.

Clarke R. Privacy and the Media – a platform for change? Uni WA Law Rev June 2012;36(1):158–98 [at], http://www.rogerclarke.com/DV/PandM.html.

Clarke R. The new meaning of 'Point of View': media uses and abuses of new surveillance tools [Notes for a presentation to the Australian Press Council, Sydney, Xamax Consultancy Pty Ltd, February 2013, at], http://www.rogerclarke.com/II/APC-130225.html; 2013.

Clothier RA, Palmer JL, Walker RA, Fulton NL. Definition of airworthiness categories for civil Unmanned Aircraft Systems (UAS) [Proc. 27th Int'l Congress of the Aeronautical Sciences (ICAS), September 2010, at], http://eprints.qut.edu.au/32789/1/c32789.pdf; 2010.

Coffman K. Don't like drones? Folks in Deer Trail, Colorado mull paying citizens to shoot them down [Fairfax Media, 18 July 2013, at], http://www.theage.com.au/technology/technology-news/dont-like-drones-folks-in-deer-trail-colorado-mull-paying-citizens-to-shoot-them-down-20130718-2q5rd.html; 2013.

Coker C. Technology is making man the weakest link in warfare. The Financial Times; 2013 [9 May 2013, at]http://www.ft.com/intl/cms/s/0/cb0d02d0-b894-11e2-869f-00144feabdc0.html.

Corcoran M. Drone journalism takes off. ABC News [21 February 2012, at], http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616; 2012.

Corcoran M. Drones set for commercial take-off. ABC News [24 May 2013, at], http://www.abc.net.au/news/2013-03-01/drones-set-for-large-scale-commercial-take-off/4546556; 2013.

Drew C. Military is Awash in data from drones. The New York Times; 2010 [11 January 2010, at] http://csce.uark.edu/~jgauch/library/Video/Drew.2010.pdf.

Edwards R. Police say CCTV is an 'utter fiasco'. The [London] Daily Telegraph; 2008 [6 May 2008, at] http://www.telegraph.co.uk/news/uknews/1932769/Police-say-CCTV-is-utter-fiasco-as-most-footage-is-unusable.html.

EP. Human rights implications of the usage of drones and unmanned Robots in warfare. Directorate-General for External Policies, European Parliament; 2013 [May 2013, at] http://www.europarl.europa.eu/committees/en/droi/studiesdownload.html?languageDocument=EN&file=92953.

FAA. National policy – Unmanned Aircraft Systems (UAS) operational approval N 8900.227. Federal Aviation Administration; 2013 [30 July 2013, at], http://www.faa.gov/documentLibrary/media/Notice/N_8900.227.pdf.

Finn RL, Wright D. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput Law Secur Rev April 2012;28(2):184–94.

Goldberg D, Corcoran M, Picard RG. Remotely piloted aircraft systems & journalism: opportunities and challenges of drones in News gathering. Reuters Institute for the Study of Journalism; 2013 [June 2013, at] https://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Working_Papers/Remotely_Piloted_Aircraft_and_Journalism.pdf.

Groombridge N. Stars of CCTV? How the Home Office wasted millions – a radical 'Treasury/Audit Commission' view. Surveillance Soc 2008;5(1) [at], http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3440/3403.

Harvey A. GA-ASI completes first flight tests of SAA onboard Predator B UAV, integrates other sensors. Military Embedded Sensors; 2013 [13 December 2013, at], http://mil-embedded.com/news/ga-asi-completes-first-flight-tests-of-saa-onboard-predator-b-uav-integrates-other-sensors/#.

IACP. Recommended guidelines for the use of unmanned aircraft. International Association of Chiefs of Police; 2012 [August 2012, at], http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

Kontominas B. Security scare as drone hits bridge. The Sydney Morning Herald; 2013 [5 October 2013, at] http://www.smh.com.au/nsw/mystery-drone-collides-with-sydney-harbour-bridge-20131004-2uzks.html.

Lewis P. Eye in the sky arrest could land police in the dock. The Guardian; 2010 [16 February 2010, at] http://www.theguardian.com/uk/2010/feb/15/police-drone-arrest-backfires.

LL. Drone crash into Sydney harbour bridge causes security incident. Liveleak.com; 2013 [26 November 2013, at] http://www.liveleak.com/view?i=661_1385456831.

Marks P. GPS loss kicked off fatal drone crash. New Scientist [18 May 2012, at], http://www.newscientist.com/blogs/onepercent/2012/05/gps-loss-kicked-off-fatal-dron.html; 2012.

Mehta A. History Tuesday: the origin of the term drone [Drones, 14 May 2013, at], http://blogs.defensenews.com/intercepts/2013/05/the-origin-of-drone-and-why-it-should-be-ok-to-use/.

Mortimer G. Multirotor hits skyscraper and burns, Auckland NZ. s UAS News; 2012 [27 October 2012, at] http://www.suasnews.com/2012/10/19348/multirotor-hits-skyscraper-and-burns-downtown-auckland-nz/.

Murphy S. Animal Liberation activists launch spy drone to test free-range claims. ABC News; 2013 [30 August 2013, at] http://www.abc.net.au/news/2013-08-30/drone-used-to-record-intensive-farm-production/4921814.

Newcombe LR. Unmanned aviation: a brief history of unmanned aerial vehicles. American Institute of Aeronautics and Astronautics; 2004 [2004].

Page L. Liverpool police get mini-black helicopter. The Register; 2007 [21 May 2007, at] http://www.theregister.co.uk/2007/05/21/black_helicopters_over_merseyside/.

PM. Robot television bomber. Popular Mechanics 1940;Dec 1940:805–6.

Prigg M. 'Welcome to drone air: first passenger plane piloted remotely flies across the UK in pioneering trial' [London]. Daily Mail [14 May 2013, at], http://www.dailymail.co.uk/sciencetech/article-2324358/Welcome-drone-air-First-passenger-plane-pilot-flies-UK-pioneering-trial.html; 2013.

RCC. Unmanned drones for shark patrols; 2013 [Works Report No. W50/13, F2008/00609, Randwick City Council, 12 November 2013].

Ross PE. When will we have unmanned commercial airliners? IEEE Spectrum [at], http://spectrum.ieee.org/aerospace/aviation/when-will-we-have-unmanned-commercial-airliners; 29 November 2011.

Schachtman N. Pentagon Shoots $22 Million Into Guided-Bullet Tech; 2008 [Wired 26 November 2008, at] http://www.wired.com/dangerroom/2008/11/what-if-a-snipe/.

SLSA. World first 'Eye in the sky' boosts beach safety. Surf Life Saving Australia; 2012 [23 February 2012, at], http://sls.com.au//content/world-first-'eye-sky'-boosts-beach-safety.

Smith GJD. Behind the screens: examining constructions of deviance and informal practices among CCTV control room operators in the UK. Surveillance Soc 2004;2(2/3):376–95 [at], http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3384/3347.

Spiegel. Drohne "Luna": Bundeswehr verheimlichte Beinahe-Crash mit Airbus. Der Spiegel; 2013 [2 June 2013, at] http://www.spiegel.de/politik/deutschland/drohne-luna-bundeswehr-verheimlicht-beinahe-crash-mit-airbus-a-903337.html.

Stephenson N. The Diamond Age. Bantam Books; 1995 [1995].

Sterling B. Heavy Weather. Phoenix; 1994 [1994].

T&D. Animal rights group says drone shot down. T&D; 2012 [14 February 2012, at], http://thetandd.com/animal-rights-group-says-drone-shot-down/article_017a720a-56ce-11e1-afc4-001871e3ce6c.html.

UAVOC. UAV Outback Challenge; 2014 [2014, at]http://www.uavoutbackchallenge.com.au/.

UAVS. UAV or UAS?. Unmanned Aerial Vehicles Systems Association; 2013 [2013, at], http://www.uavs.org/index.php?page=what_is.

USDoD. Unmanned systems integrated roadmap FY2011-2036. US Department of Defence; 2011 [October 2011, at] http://info.publicintelligence.net/DoD-UAS-2011-2036.pdf.

UVSI. RPAS glossary 130815. UVS International; 2013 [August 2013, at], http://uvs-info.com/phocadownload/03_9_Survey-on-RPAS-Civil-Operations-2012-2013/3_UVSI_RPAS-CivOps_Glossary_V03_130815.pdf.

UVS-Info. Developing the next generation of UAV systems. UVS-Info; 2005 [undated, but apparently of 2005, at], http://uvs-info.com/phocadownload/05_3f_2006/113-114_UK_NextGenUAVs.pdf.

Villasenor J. 'What is a drone' anyway? Sci Am [12 April 2012, at], http://blogs.scientificamerican.com/guest-blog/2012/04/12/what-is-a-drone-anyway/; 2012.

Whitehead JW. Roaches, mosquitoes, and birds: the coming micro-drone tevolution. The Rutherford Institute; 2013 [15 April 2013, at] https://www.rutherford.org/publications_resources/john_whiteheads_commentary/roaches_mosquitoes_and_birds_the_coming_micro_drone_revolution.

Wong KC. Survey of regional developments: civil applications. School of Aerospace, Mechanical and Mechatronic Engineering, University of Sydney; 2001 [February 2001, at] http://www.aeromech.usyd.edu.au/wwwuav/papers/UAV_civil_app.PDF.

Yenne B. Attack of the drones: a History of unmanned aerial combat. Zenith Press; 2004 [2004].

Zamyatin E. We. Penguin; 1922 [1922, 1990].