Technology Trends

Drones

Enterprise Architecture, Chief Technology Officer Branch

Version 0.1
Date 2019-5-8

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Business Brief [1]

While drones can be referred to by various names[2], Transport Canada uses the technical term Remotely Piloted Aircraft (RPA). An RPA is defined as a navigable aircraft, other than a balloon, rocket, or kite that is operated by a pilot who is not on board. An RPA is considered a component of a Remotely Piloted Aircraft System (RPAS). An RPAS refers to a set of configurable elements consisting of a remotely piloted aircraft, its control station, the command and control links, and any other system elements required during flight operation. Essentially, a drone can be considered a flying computer that can be remotely controlled or fly autonomously through the use of software working in conjunction with various sensors. Transport Canada uses the term 'drone' interchangeably with RPAS.

Transport Canada classifies drones by weight into three basic groups, namely:

- Drones under 250 grams,
- Drones from 250 grams up to and including 25 kilograms, and
- Drones over 25 kilograms.

Transport Canada advises that drones weighing less than 250 grams (approx. ½ lbs.), also referred to as micro drones, must be "flown responsibly". Micro drones should not be flown near aircraft or airports. People and property must never be placed in danger and the operator/pilot should maintain visual-line-of-sight with the drone when in flight. A pilot certificate is not required to operate a micro drone.

Operators/pilots must obtain a drone pilot certificate for drones that weigh between 250 grams and 25 kg (approx. 55 lbs.). There are two types of pilot certificates available from Transport Canada and they are based on categories of operation. For example, a pilot conducting basic operations must always fly more than 30 m away from bystanders and only in uncontrolled airspace – requiring a basic operations certificate. A pilot conducting advanced operations may fly less than 30 m from and over bystanders and in controlled airspace – requiring an advanced operations certificate.

Additionally, drones that weigh over 25 kilograms require special permission (i.e. a special flight operations certificate) from Transport Canada before they are flown.

Drones can come in a wide variety of sizes and have just as many capabilities. For example, the United States Air Force uses large drones the size of normal manned aircraft (i.e. the Predator and Reaper drones used for surveillance and/or as a munitions

[1] Further information will be added to this document based on additional research and consultation during the fiscal year 2019-20.
[2] For example, UAV for Unmanned Aerial Vehicle.

platforms). The United States Army uses micro drones the size of a role of quarters (i.e. the Black Hornet Nano drone contains a tiny camera which provides troops on the ground with local aerial situational awareness). Drones can have fixed wings and require short runways to take-off (i.e. various types of radio-controlled model aircraft) or drones can have rotors like a helicopter and can take-off vertically, fly, hover, and land vertically (e.g. quadcopters). These are the types of drones that are commonly available to the public and are primarily used for recreational and commercial purposes.

Technical Brief

Drones, and the technology related to drones, are constantly evolving as new innovation and investment lead to advancements. A typical drone is made of light composite materials to reduce weight and increase maneuverability. Since drones do not have a need to accommodate human operators/pilots, the body of a drone typically contains the technology. Drone technology refers to everything from the aerodynamics of the drone, materials in the manufacture of the physical drone, to the circuit boards, chipset, software, and communications system. Drones can be equipped with additional technology such as various types of cameras, Global Positioning System (GPS), lasers, various types of sensors, and even weapons. Drones can also operate with various degrees of autonomy, either under remote control by a human operator/pilot or autonomously by on-board computers. The remote Ground Control Systems (GSC) that control drones are typically referred to as a ground cockpits.

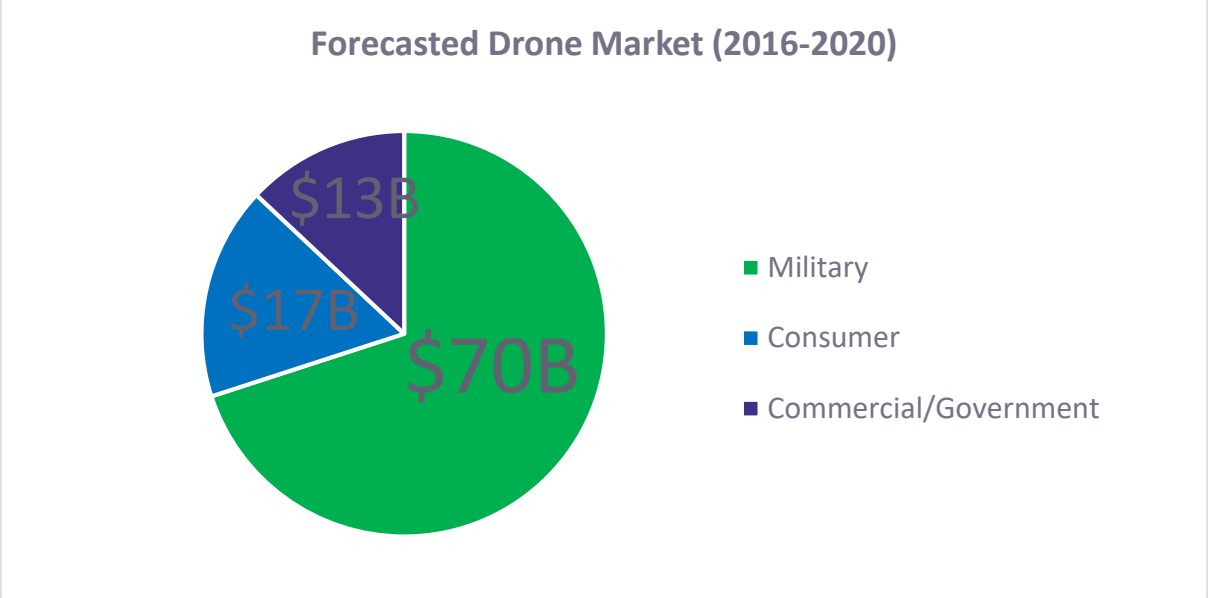
Drones can contain a multitude of technology, including:

- Satellite Positioning – the use of Global Navigational Satellite Systems (GNSS) such as GPS to aid in drone navigation.
- Obstacle Detection and Collision Avoidance – vision systems use obstacle detection sensors (e.g. ultrasonic, infrared, etc.) to scan surroundings in order to avoid objects.
- Gyro Stabilization, Inertial Measurement Unit (IMU) and Flight Controller – these technologies are components that work together in order to give drones their smooth flight capabilities.
- Drone Motor Direction And Propeller Design – these components enable drones to move through the air and to fly in any direction or hover.
- Internal Compass & Failsafe Function – enables drones to return to a safe location in case of a loss of signal between the drone and the ground control system.
- LED Flight Indicators – allows the operator/pilot to know the orientation of the drone in flight.
- Smartphone App featuring Ground Control System Function – many drones can be flown from a smartphone app connected to the drone via Bluetooth, Wi-Fi, or over cellular networks like 4G (LTE) or 5G.

- Cameras and Live Video Transmission – a video camera mounted on a drone can have the ability to broadcast live video to the operator/pilot on the ground.
- Gimbals & Tilt Control – allows for any vibration from the drone to not reach the camera and to create unique video angles while the drone is in flight.
- Drones with Sensors – can be used to create 3D models of buildings, landscapes, etc., to collect and provide precision data to users.
- Drone Security – in some ways drones are like flying computers and as such are susceptible to hacking and other cyber-attacks or interference.

Industry Use

According to a 2016 report by Goldman Sachs Research, between 2016 and 2020, the market opportunity for drones is forecast to grow to $100 billion. While the military share of this market will remain strong, further growth will be driven by further demand in the commercial and government sectors, specifically in construction, agriculture, insurance claims, oil and gas (aerial inspections), police, fire, search and rescue, journalism, boarder protection, and cinematography.



- Source: "Drones: Reporting for work". Goldman Sachs Research, 2016.

The rapid growth of the drone industry has often outpaced the development of government regulations and systems to govern their use. This uncertainty weighs on innovation and commercial adoption, but anticipated regulatory clarity should lead to increased demand. For example, the National Aeronautics and Space Administration (NASA) is leading a multibillion-dollar effort to develop a United States airspace management system (often referred to as an Unmanned Traffic Management (UTM) system) capable of safely coordinating manned and unmanned flights, while the Federal Aviation Administration (FAA) is expected to further ease restrictions that are keeping commercial drones from reaching their full potential.

A 2017 market analysis report on drones by Business Insider (BI) Intelligence identified that the market for commercial and consumer drones will grow at a compound annual growth rate of 19% between 2015 and 2020, compared with 5% growth for the military market. BI Intelligence expects sales of drones to surpass $12 billion in 2021. That is up by a compound annual growth rate of 7.6% from $8.5 billion in 2016. BI Intelligence predicts future growth across the consumer, commercial, and government markets. The report concludes that the commercial market will be the segment that drives the industry.

The largest producer of drones for the consumer market is the Chinese-based company DJI Technologies Co. In 2017, DJI accounted for over 70% of the consumer drone market with revenues of approximately $2.7 billion.

As for military drones, Israel and the United States make up more than 80% of all military drone exports worldwide, according to the Stockholm International Peace Research Institute. Most military drones are for surveillance, but several countries already have military drones capable of carrying out combat missions – a number that is expected to rise in the coming years.

Research from Forrester (2017) also predicts that drone usage and deployment will be pervasive across all industries. Drone regulations will continue to evolve and will continue to introduce new opportunities for further applications.

Within the Canadian marketplace, Unmanned Systems Canada (USC) –a not-for-profit organization, acts as the national industry association representing entrepreneurs, businesses, students, academia, industry, and government organizations working in the aerial, ground, and marine remotely-piloted and unmanned vehicle systems sector. USC has the objective to strive for a strong, single voice that advocates for safety, high professional standards, industry collaboration and a stable, responsive regulatory framework. Transport Canada engaged with USC during the development of new regulations for drones, which are discussed in the following section.

Canadian Government Use

Drones offer almost endless use in their application to public service operations. From performing regular safety inspections on infrastructure such as roads, bridges, and power lines, to carrying out potentially life-saving public safety missions, the right drone can make all the difference in optimizing operations across a huge scope of different government uses.

Transport Canada estimates that the number of drones flown in Canada is approximately 193,500. By comparison, it is estimated that there are 37,000 aircraft in traditional aviation, including commercial passenger and cargo aircraft and general aviation aircraft in Canada. The growth in drone usage has brought new entrants to aviation. Transport Canada no longer deals solely with the typical industries such as aerospace manufacturers, airlines, and airplane pilots. New entrants include commercial drone operators/pilots, manufacturers, training providers, law enforcement, and academia. Unlike persons who are traditionally involved in aviation, such as commercial airline pilots and military pilots, new entrants have varying levels of aviation safety awareness, may never have flown traditional aircraft before, and may be unfamiliar with safety-related aviation rules and regulations.

Flying a drone has quickly become a pastime. As of 2018, the recreational drone community in Canada is estimated at 140,800 operators and is projected to increase to 225,500 operators by 2025.[3] That being said, the minimalistic requirements under the Canadian Aviation Regulations (CARs) for recreational operators/pilots has resulted in a number of incidents (which are often associated with a lack of user knowledge) and a growing risk to aviation safety as well as to people on the ground. Since 2014, the number of drone-related incidents reported to Transport Canada has risen over 200%.[4] Incidents have included risks to traditional aircraft while they are on take-off or landing near airports, high altitude flights, and risk of injury to people on the ground caused by events such as a 'fly-away', which generally means that a pilot cannot maintain control of the drone or that it ceases to follow pre-programmed procedures.

The growing drone industry has significant economic potential for Canada, however, until recent years there has been no specific set of regulations in place to require the safe operation of drones in Canada. Existing CARs did not provide a regulatory framework that promotes the economic potential of drones nor did it contain modern, risk- and performance-based regulations that can uphold aviation safety. To date,

[3] Using 11% of the U.S. FAA's 2018 RPAS forecast, which reflects Canada's population relative to the U.S. [Federal Aviation Administration. (2018). FAA Aerospace Forecast: Fiscal Years 2018-2038. Washington, D.C.: FAA.]

[4] Number of incidents: in 2014, there were 41 incidents; in 2015, there were 86 incidents; in 2016, there were 148 incidents; and in 2017, there were 136 incidents.

Transport Canada has been overseeing commercial drone operations on a case-by-case basis using certain CARs provisions that were not designed specifically for drones in order to mitigate aviation safety risks. This approach has been complex, inefficient, and in some cases overly restrictive. Transport Canada recognized that in the absence of any regulatory change, risks to aviation and public safety would continue to rise in step with the growth in popularity of drones.

Canadian civil aviation is the responsibility of the Minister of Transport under the *Aeronautics Act* (the Act). Under the Act, the Minister is responsible for the development of regulations governing aeronautics and the supervision of all matters connected with aeronautics. In 2017, the Minister of Transport made an Interim Order (IO) under the Act to address the growing number of incidents related to drones. The objective of the IO was to improve aviation safety, to protect the public and to ensure the safe operation of aircraft. It was a temporary measure (renewed in June 2018) until new regulations could be put in place to require the safe operation of drones.

In an effort to address on-going issues, in January 2019, Transport Canada published new regulations for flying drones in Canada. These regulations will come into effect on June 1, 2019, will amend existing CARs and are intended to provide improved regulatory predictability for businesses and to reduce risks related to aviation safety. These regulations will move away from the case-by-case treatment of non-recreational drone operations by eliminating a number of Special Flight Operations Certificates (SFOC) requirements for drone operations. This will create a predictable and flexible regulatory environment conducive to long-term planning while reducing costly administrative burdens on businesses. The amendments are also intended to reduce risks to public safety through pilot certification and will also introduce drone safety-based manufacturing requirements intended for certain operations.

These new regulations are not intended to impede innovations in the use of drone technology, such as Amazon's drone parcel delivery to residential areas. Transport Canada has indicated that these regulations do not touch upon privacy related issues since Canada already has in place laws that protect privacy. Enforcing these new regulations will be carried out by the Royal Canadian Mounted Police (RCMP), as well as other provincial and local police forces.

Implications for Shared Services Canada (SSC)

Value Proposition

Broadly speaking there are a number of value propositions in terms of drones and drone technology that federal organizations should be aware of, namely:

- Drones could offer improved monitoring:
    - As video monitoring and analytics capabilities are growing, drones and drone technology has the potential to upend traditional modes of video

surveillance. This could reduce installation costs and maintenance of traditional fixed systems. SSC should look to supporting drone technology as a means to improve/augment legacy systems.
    - Drones could also become a new vehicle for data collection. Analysis of this new data gathered by drones could provide new perspectives and insights to government departments. SSC should consider how best to handle an increased volume of data.
-
- Drones could automate and augment physical security:
    - The mobile nature of drones has its advantages over fixed physical security options. SSC should consider customer requests to upgrade existing systems that afford greater flexibility and reduced cost options.

With respect to the growth of drones and drone technology, there are a number of positive aspects to note for SSC. As the information technology (IT) infrastructure service provider for the Government of Canada, SSC is ideally positioned to capitalize on existing strengths and to seize opportunities.

Internal to SSC, the Department has an existing depth and breadth of IT expertise. SSC has over 5,800 employees, the majority of which are computer systems experts. These experts have specialized education, experience and training in various aspects of information technology and computer systems. These experts work to provide a modern, reliable, and secure information technology infrastructure for the Government of Canada. SSC maintains new, large, state-of-the art enterprise data centres that serve the entire government. These data centers enable SSC to protect the IT infrastructure that is the IT backbone of the safety, security, and well being of Canadians, 24 hours a day, 356 days a year. Additionally, SSC also offers public cloud computing services for its customers. Cloud computing improves services to Canadians by increasing the responsiveness, flexibility, and value for money of the applications used to deliver programs and services. All combined, these positive elements position SSC nicely to face the challenges of delivering on future customer requests for drone support.

External to SSC, the demand for drones from SSC's customers is still in its infancy. Requests from SSC's customers for support of drones and drone technology has been minimal. Therefore, there is still time for SSC to begin to ramp-up for an increased demand for support from its customers. Additionally the nature of drone technology has the potential to generate efficiencies and reduce costs. Drones can be more effective for the GC to use in environments where it is difficult and/or dangerous for humans to operate. For example, there could be potential efficiencies to use drones with cameras in place of helicopters with human observers. While there could be other net efficiencies for the Government of Canada, it is unclear if this could mean increased costs to SSC in terms of IT service support.

Challenges

Broadly speaking, there are a number of high-impact challenges in terms of drones and drone technology that federal organizations should be aware of, namely:

- Drones could be compromised:
  - Drones are vulnerable to hackers and significantly increase the attack surface that organizations must defend. SSC should view drones as another integrated hardware and software endpoint that requires essential security controls, access management, monitoring, patching, and updating.
- Drones could crash and/or impact critical operations:
  - With the increased use of drones, so too is there an increase in the number of drone crashes. SSC and its customers should be aware of the potential liabilities that can result from a drone incident and the potential impact on critical operations.
- Drones could create privacy concerns:
  - There are numerous issues surrounding aerial surveillance and privacy rights. SSC and its customers should be aware of the legal and regulatory landscape and act in accordance with it.

With respect to the growth of drones and drone technology, there are also a number of negative aspects to note for SSC. Internal to SSC, the Department continues to face challenges related to the modernization of the Government of Canada's IT infrastructure. The on-going replacement of aging IT systems could have an impact on SSC's ability to deliver services. While SSC is currently working diligently to modernize legacy systems, the Department has acknowledged that improvements are not progressing as rapidly as desired. SSC's capacity and tools for service management may not be sufficient to support excellence in the delivery of services to partner organizations. Additionally, SSC's capacity and tools for project management may also be insufficient to complete projects on time, on scope, and on budget, considering the operational burden already borne by SSC's workforce. Taken as a whole, these weaknesses could have a negative impact on SSC's ability to deliver on future customer requests for drone support.

Gartner (2018) has indicated that the growth of drone adoption will continue to be driven more by the establishment of clear regulations rather than by technology advancements. With Transport Canada's 2019 announcement of new regulations for flying drones, it is expected that the rate of drone adoption within Canada will continue to increase. External to SSC, it could be expected that federal organizations such as the RCMP, the Department of National Defence (DND), Canada Boarder Services Agency (CBSA), Fisheries and Oceans (including the Canadian Coast Guard), and others, will increase their use of drones in operations such as patrols, investigations, and search and rescue efforts. Hand-in-hand with the increased use of drone technology will be

the need to support the IT infrastructure related to these technologies. It is reasonable to assume that SSC will be called upon to support the use of drones in many of these operations.

Additionally there may also be challenges in terms of managing drone traffic. At this time, there does not exist a complete air traffic management solution (or a UTM system) that will keep drones and other aircraft from having accidents. Even in countries with established drone regulations (e.g. China was one of the first countries to introduce drone regulations but has not yet implemented a UTM system), many are still testing and searching for optimal UTM solutions. In Canada, NAV Canada is currently exploring options to address the management of drone traffic.[5] Whatever the end solution for a UTM is in Canada, SSC should be prepared to ensure functionality and interoperability of its IT infrastructure.

Considerations

Looking forward, SSC has a number of things to consider in terms of drones and drone technology.

Firstly, SSC should consider how the increased use of drones and drone technology will impact its role as an IT service provider for the Government of Canada. While Transport Canada has laid out new regulations for the safe use and enjoyment of drones, SSC should examine closer the potential impact of increased demand for support from its customers. SSC should consider how an increased demand in the use of drones might impact on its ability to deliver services. Should SSC support its customers in terms of the types of drones to procure or should SSC operate a drone-based on-demand service such as a Drones-as-a-Service (DaaS). At this point in time it may be difficult to determine the best approach and the precise amounts but it is reasonable for SSC to plan for increased requests for support from partner organizations. This in turn could lead to an increased need for SSC to allocate funding and resources to meet an increased demand.

Secondly, SSC should pursue a coherent policy in terms of drone acquisition and use. A consistent approach, with space for customization, would enable customers to acquire and use drones while maintaining interoperability. This would allow SSC to support the IT infrastructure of drones in a more cost-effective fashion. Coordination with Public Services and Procurement Canada (PSPC) in determining the roles and responsibilities

[5] Gartner analysts call January 30, 2019.

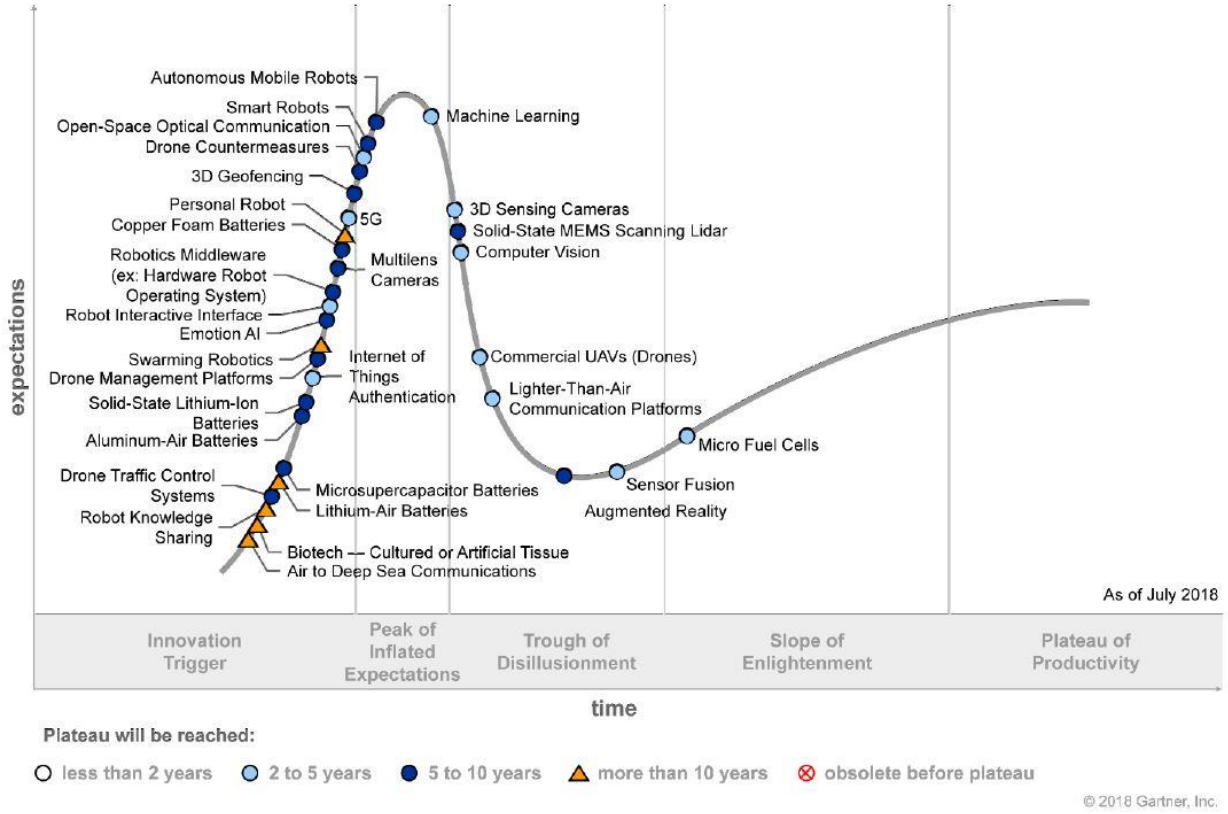
of procuring and servicing drones may be required in order for clear parameters to be established.

Thirdly, SSC may wish to consider what type of drone management platforms should be used across the Government of Canada. Drone management platforms refer to capabilities by which organizations manage their drone fleets. Technologies will be required to facilitate drone operations using common or interoperable platforms. Any government organization that would maintain a comparatively large fleet of drones should use a management platform to make their operations safer and more efficient. More broadly, SSC should also be in consultation with regulatory organizations like Transport Canada and NAV Canada regarding drone traffic management systems. Wireless technologies used to track, control, and manage drones in our skies should be securely interoperable with GC infrastructure.

Lastly, SSC should consider if additional or new security measures are required for drones that are connected to or interact with Government of Canada networks. SSC takes cyber and IT security seriously and should consider if the protocols needed to secure GC supported drones are sufficient and properly followed. Additionally, SSC may need to consider how and to what degree support is required by customers in terms of drone countermeasures. Drone countermeasures are systems and devices designed to neutralize or retaliate against threats from drones. SSC should expect to work with Government of Canada security departments and agencies to determine how best to support their IT infrastructure security needs.

Appendix A – Hype Cycle for Drones and Mobile Robots, 2018 (Gartner)

Figure 1. Hype Cycle for Drones and Mobile Robots, 2018



Source: Gartner (July 2018)

This Gartner (2018) Hype Cycle provides visibility of robot/drone innovations that will benefit organizations that are two years or beyond in adoption of drone and mobile robots. Many of the platforms, technologies and components (such as semiconductors, sensors, motors/actuators, networks, software/algorithms and materials) that will improve performance, costs and capabilities in these systems, leverage development in other markets. However, there remain many challenges in making drones better, such as artificial intelligence, semiconductors and battery technology. As more and more countries establish regulations governing the operation of drones, Gartner is predicting that this will result in an increased demand for drones that will continue to proliferate in many use cases across markets. Many of these technologies related to drones are still in the innovation phase and will not reach a more mature plateau for another 5 to 10 years (and in some cases more than 10 years).

References

- "Regulations Amending the Canadian Aviation Regulations (Remotely Piloted Aircraft Systems): SOR/2019-11." Canada Gazette. Part II, Vol. 153, No 1. December 21, 2018.
  http://www.gazette.gc.ca/rp-pr/p2/2019/2019-01-09/html/sor-dors11-eng.html
- "Regulations Amending the Canadian Aviation Regulations (Unmanned Aircraft Systems)". Canada Gazette. Vol. 151, No. 28 — July 15, 2017
  http://www.gazette.gc.ca/rp-pr/p1/2017/2017-07-15/html/reg2-eng.html
- "Drones: Reporting for work". Goldman Sachs Research. 2016.
  https://www.goldmansachs.com/insights/technology-driving-innovation/drones/
- "How Do Drones Work And What Is Drone Technology". Fintan Corrigan. January 7, 2019.
  https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/
- "Business Insider's Latest Drone Industry Analysis". Miriam McNabbon. July 13, 2017.
  https://dronelife.com/2017/07/13/business-insiders-latest-drone-industry-analysis/
- "World's top drone seller DJI made $2.7 billion in 2017." Masha Borak. January 3, 2018.
  https://technode.com/2018/01/03/worlds-top-drone-seller-dji-made-2-7-billion-2017/
- "Unmanned Aircraft System Traffic Management." June 6, 2018. NASA.
  https://www.nasa.gov/ames/utm
- "What is UTM?" Mariam McNabb. February 12, 2018.
  https://dronelife.com/2018/02/12/utm-conversation-amit-ganjoo/
- "Drones as a Service (DaaS)." Dibbern Consulting. 2019.
  https://www.dibbern.biz/drones-as-a-service-a-professional-it-service-provision/
- "Hype Cycle for Drones and Mobile Robots, 2018." Gartner (Analyst: Brady Wang). July 18, 2018.
- "Forrester's Guide to Drone Security Risks." Forrester (Analysts: Merritt Maxim and Salvatore Schiano). May 30, 2017.