ASIA PROGRAM

From safe product to secure product

A CHALLENGE FOR INTERNATIONAL RELATIONS: THE CASE OF DRONES

BY EMMANUEL MENEUT

PHD, CATHOLIC UNIVERSITIES LECTURER

FEBRUARY 2019

ASIA FOCUS #105

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

The "drone security challenge" is a key case that reveals the **continuity** from quality to safety through security after the shift from safety to quality that took place during the 1990s. This shift, triggered by Japan, revealed the main strategy levers of the globalization era: delocalization, just in time and total quality management. Briefly, after the mass consumption trend after World War II, the safety issue became the major challenge to the firm reputation with the consumer movement in the 1970s. Then, the rise of the Japanese economy as the 2nd world economy at the beginning of the 1990s, illustrated the shift from safety toward quality as a strategic tool to conquer foreign markets, for example by the Japanese automotive industry. Today, the large scale digital breakthrough introduces by reliable and affordable high tech products like the smartphone or the drone, rises the problematic of **security**, either personal data security or airspace security, as a strategic **challenge** for both the State and the firm. The security frame to address this challenge will make possible to reach the billions of dollars of wealth promised by the digital revolution underway. The case of the drone is particularly interesting as the Chinese company DJI, the main drone manufacturer, implements a security strategy that carry a strategic opportunity through the OBOR framework in order to mass produce « secure product ». The new shift toward secure products is highlighting the main feature of the mutation of the economic and liberal order. The **manufactured firms of digital products highly connected will be security provider to customers and States at a global scale**.

THE FACTS: THE DRONE SECURITY CHALLENGE

Following the American Federal Aviation Authority (FAA) the number of drone sightings reported by pilots is increasing with a nonlinear trend. Most of them, 78%, occurred during the approach phase near an airport. However, 7% occurred during *en route* phase at high altitude, some above 4 km. It is a threat to security of aviation, a necessary condition for airline businesses. Actually, the distance at which a drone is sighted and its size are the main features of the threat. The number of drone sightings illustrates the level of the collision probability because to be in sight a drone must be close to the aircraft, around less than very few hundred meters. About the drone size and weight, the spectrum

goes from few centimeters and grams to a fighter jet. For example, a Global Hawk drone has the size of a B737.

Today, Airline companies are facing an exponential growing threat, this kind of situation requires an efficient set of mitigation barriers without delay, however it would be a « no future » situation!

At the global level, the International Air Transport Association (IATA) purpose is to ensure the safe operation of drones, especially in close proximity to aircrafts within airports areas. The airspace will be share between an increasing number of commercial aircrafts and a high frequency drone operations. Definitely, the security issue is the main topic on the airspace agenda. The recent drone disruption at the Gatwick airport between December 19th and 21st concerned 120 000 passengers during Christmas holidays. It highlights the economic impact of this security issue for all airspace commercial users.

THE THEORETICAL FRAMEWORK OF THE SECURITY CHALLENGE

The contemporary security challenge is the continuity from quality to safety issues due to the increase frequency of dangerous drone/aircraft situations. It is a structural effect coming from the dynamic of a technological breakthrough. This challenge may be address by mass security means to mitigate the majority of the dangerous situations, non-intentional collision trajectory, and more discriminating tools for the last more specific cases of intentional collision trajectory. We examine this problematic through the analysis of the two components of security: the trend of the frequency of the risky situations and its gravity.

Classical risks management from an enterprise point of view in a market economy is driven by two independent variables, the frequency and the gravity. Actually, they defined four spaces for the risks management process issue:

Gravity		
High	c/ Safety management system	← d/ Security : no place for a firm, the State is required ↓
Low	a/ "Business as usual"	b/ Quality management system
	Low	**Probability** **High**

The low probability and low gravity situation defines a space (a/) where a firm could provide mass products or services without high level of cost to support a quality or safety management system. It is the economic area where business is driven by the price/cost criteria. For example, it was the case for car mass production of the 1920s and the 1950s.

The high probability and low gravity situation defines a space (b/) where a firm should invest into a quality management system to support mass production in order to satisfy its stakeholders. It was the case of the Japanese car industry during the 1990s.

The low probability and high gravity situation defines a space (c/) where the firm must invest into a safety management system to support its business processes, usually it is a requirement by the State in order to gain social acceptance of the economic activity. It is for example the case of the nuclear or airlines industry.

Finally, the high probability and high gravity situations defines a space (d/) where a firm could not survive. The security challenge could only be meet by a State actor with sufficient fungibles means to mitigate the risk (force, wealth, intelligence). A firm is a specialize actor without access to all the fungibles means required to tackle numerous catastrophic cases. Each time an activity fall within this area, a **security challenge** must be address in order to develop a profitable business field. Either the frequency or the gravity should be reduce, most of the time both dimensions will be address.

The drone revolution is actually falling within the security challenge area.

THE DIMENSIONS OF THE DRONE SECURITY CHALLENGE: THE FREQUENCY AND THE GRAVITY

Indeed, the FAA estimated the small drone fleet in the US totaled around 1.2 million in 2017 and it will reach the 2.9 million level in 2022. From February 2017 through April 2018 the FAA collected 6 117 reports of sighting of potentially unsafe use of drones from civil aircraft pilots. The number of reported sightings increases about five fold from 233 in 2014 to 1 217 in 2015 and by another 51% in 2016 to 1 840. The 2 185 reported sightings in 2017 represented a 19% increase over 2016. It is an exponential rise of the collision probability of a drone with commercial aircraft. This trend is the natural consequence of the diffusion of a technological breakthrough following an "S-curve". In the case of the drones:

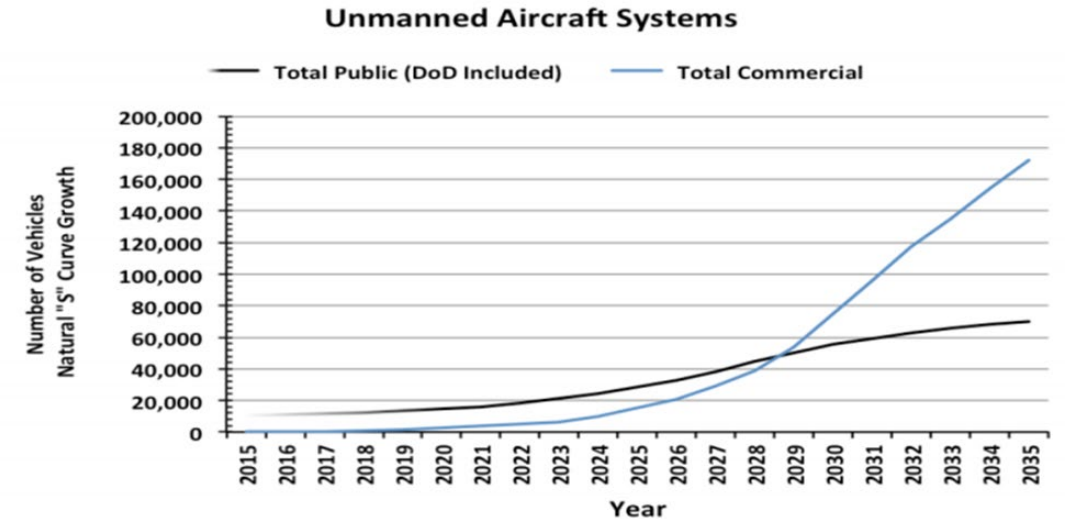

Fig. 1 : total drone forecast 2015 – 2035 following an exponential trend[1]

The number of drone in the airspace is rising at a nonlinear growth rate, the density of drone followed the same trend, hence the probability of drone sighting by aircraft pilots increase at an exponential pace. The increase of drone/aircraft near misses and collisions in the Chinese airspace between 2013 and 2017 and the consequences: air force shoot

[1] (US DOT, 2013) US Dpt of transportation, september 2013, Unmanned Aircraft system service demand 22015 – 2035, technical report version 0.1 at url https://fas.org/irp/program/collect/service.pdf

downs of errant drones, airport delays or shutdown and forced deviation is a key concerned for Chinese authorities[2]. (HUBER, 2017)

China examines the gravity of the consequences of an airplane/drone collision. China's CAAC conducts drone/aircraft collision tests mainly on the windshield and radome (the nose of the aircraft) of an airliner with a light DJI drone. Three academics institutions performed the tests. The results demonstrated the absence of catastrophic/major consequences. The result showed similar results encountered in a bird strike tests[3]. (HUBER, 2017) However, drone collision tests with heavier drone are missing to cover the full cases of gravity collisions.

WHAT MATTER IS THE GRAVITY!

The probability of collision will not decrease because the number of drones exponentially increases as well as the number of professional activities where drone is or will be use. Therefore, **gravity** is the critical variable of the security challenge.

In the commercial airline field, the last case of collision demonstrated that consequences might be catastrophic. On December 13th, 2018, a drone may have collided with a B737 as the aircraft was landing in Tijuana airport, Mexico. It leads considerable damage to the radome[4] (cf fig. 2)

Fig. 2 : The damaged nose of Aeromexico's 737 jet[5]

[2] (HUBER, 2017) Mark Huber, dec 14, 2017, China conducts drone-aircraft collision tests, Business aviation
[3] ibid
[4] (NAVARRO, 2018) (NAVARRO, 2018) Andrea Navarro, Alan Levin, dec. 14th, 2018,
Boeing 737 Passenger Jet Damaged in Possible Midair Drone Hit Bloomberg
[5] (NAVARRO, 2018) Andrea Navarro, Alan Levin, dec. 14th, 2018, Boeing 737 Passenger Jet Damaged in Possible Midair Drone Hit Bloomberg at https://www.bloomberg.com/news/articles/2018-12-13/aeromexico-737-jetliner-damaged-in-possible-midair-drone-strike

Following a study made by several American universities and laboratories for the FAA, it demonstrated the severity of drone collision impact with a commercial transport jet. It also highlights the influence of drone velocity and mass as key parameters of gravity. A collision with a quadcopter or fix wing in the horizontal tail plane reached the catastrophic level[6] (level 4 or red on fig. 3)

Severity	Description
Level 1	• Airframe undamaged. • Small deformations.
Level 2	• Extensive permanent deformation on external surfaces. • Some deformation in internal structure. • No failure of skin.
Level 3	• Skin fracture. • Penetration of at least one component into the airframe.
Level 4	• Penetration of UAS into airframe. • Failure of parts of the primary structure.

Fig. 3: The damage level categories and the aircraft consequence of a 1.2 kg quadcopter collision (left) or 1.8 kg collision with a fix wing (right) drone collision severity levels on commercial transport jet type aircraft

In the military fields, drone are widely used for all intelligence and shell missions. The Islamic State against the Russian aerial bases of Hmeimim and Tartous had used it in January 2018, 50 km from the bases. The Russian forces trigger all their available defense system from the electronic barrier, jamming etc. to the anti-missile Pantsir S1[7]. The development of recreational drones made them affordable and reliable for all parties of a conflict. The Islamic State used drone during several offensives, on an important scale with multiple drones (around 20 drones) to shell targets[8].

[6] (OLIVARES, 2017) Gerardo Olivares, nov 2017, FAAs UAS airborne collision hazard severity evalution, ASSURE (Missipi state university & al.) at url : http://www.assureuas.org/projects/deliverables/sUASAirborneCollisionReport.php
[7] (RED SAMOVAR, 2018) Red Samovar, 13/01/2018, Attaques sur les installations russes en Syrie, available online: https://redsamovar.com/2018/01/13/actu-attaques-sur-les-installations-russes-en-syrie/
[8] (WATERS, 2017) Nick Waters, February 10, 2017, Death From Above: The Drone Bombs of the Caliphate, Bellingcat, available online at https://www.bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/

The use of two explosive drones (cf. fig. 4) around the Venezuelan president Maduro on august 4th, 2018 may not be the last case of malevolent use of drone. According to official Venezuelan source, two DJI M600 drones (hexacopter) each loaded with 1 kg of C4 explosive covering a radius of 50 meters were used for this drone attack[9].

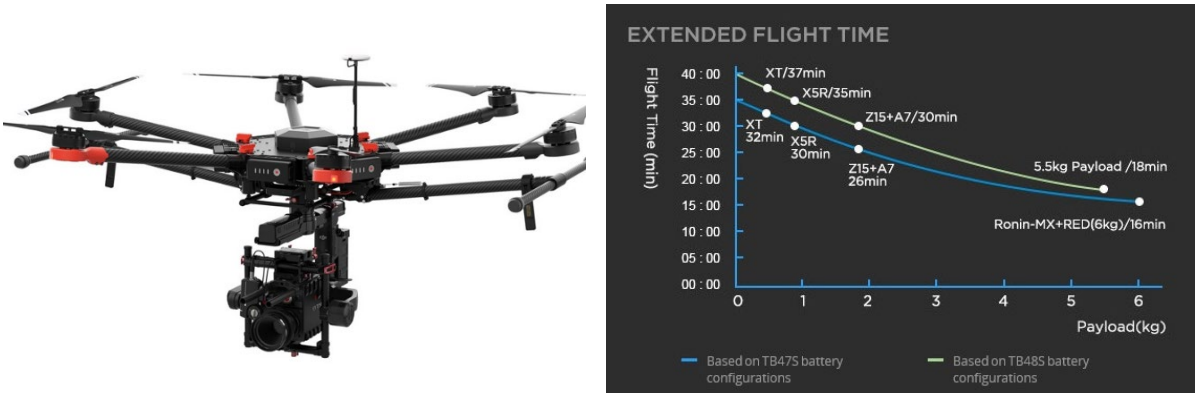

Fig. 4 : The DJI M600 is a professional drone primarily for filmmakers with a 5 km range until a 6 kg payload (from DJI available online at : https://www.dji.com/fr/matrice600-pro)

Gravity will not decrease because the functional domain of drone exponentially increases which entail the growth of their weight and speed. In addition to non-intentional intrusion, there are also a requirement to protect critical airspace like airport from intentional intrusion from sophisticated operators, which represent only few cases.

The drone collision risk is increasing due to the rise of the frequency of near collisions and the major or catastrophic collision consequences gravity. The drone business field is confronted with a security challenge, will it be a new economic sector or a dead end ? The answer will come from the risk management process. If there are low cost mitigations barriers that reduced either the probability of drone/aircraft collisions or the uncertainty on the collision gravity, then there is a place for private enterprises business. Otherwise, public opinion will have to choose between these two economic sectors. Hence, without a

[9] (BARRETT, 2018) Rian BARRETT, 8/04/2018, The explosive carrying drones in Venezuela won't be the last, WIRED

permanent set of efficient mitigation barriers, the security challenge won't be address. Especially for critical airspace with high density of commercial aircrafts.

THE MITIGATION PROBLEMATIC

The **mitigation problematic**, namely how to mitigate the collision risk with efficient barriers, rises the alternative either to promote the airspace segregation between aircrafts and drones or to focus on the actors, the aircraft and the drone pilots, by favoring the "see and avoid" principle in order to share the airspace.

Following IATA, the aircraft pilots have only few seconds to manage the situation of proximity with a drone. To detect a drone and to recognize a potential collision require around 6 second. The avoiding manoeuver delay adds 4 more seconds. Before the aircraft trajectory changes it requests 2 more seconds for a total of 12 seconds. At the current aircraft speed, this sequence requires more than 700 meters to be performed. It is much more than the drone visibility for human eyes! As a consequence, there is much less hope that the cockpit crew will be able to use the "see & avoid" barrier to handle the collision risk with a drone…

In Australia, the public sphere is focusing on certification of drones and their pilots. The Civil Aviation Safety Authority (CASA) licenses remote pilots to fly drones in Australia. However, critics highlights « unlicensed companies and individuals were increasingly using cheap drones from China by unqualified pilots, and were not flying in designated recreation flying fields[10]. »

For the FAA, a drone pilot should be trained and be responsible in order to mitigate the collision risk. The main pillars of the approach of drone risk mitigation rest on:

- ➔ Education of drone operators
- ➔ States regulatory frameworks shared by drone operators
- ➔ Enforceable sanctions for drone operators when using drone in dangerous manner

The purpose of the regulatory framework is to minimize the cost impact of new drones operations on all airspace users. The efficiency of a regulatory framework without enforcing capacities by an authority doesn't have any valuable results. The regulatory

[10] (MOSES, 2012) Asher MOSES, Flying drones a safety threat at airport, The Sydney morning herald

framework addresses the financial burden of security. It has the lowest level of impact on the cost of operations. So the alternative is between unreliable "see & avoid" mitigation barriers and costly automated detection and efficient neutralization barriers which may enforce segregation.

Actually, the critical variable is the capacities developed to automatically deny the majority of the drone incursions, either involuntary of naïvely malevolent, in forbidden airspace and to manually neutralize the other cases of high tech and elaborate incursions. The goal is to find the security barrier means with the lowest cost in order to mitigate the majority of near collision events. The last cases will anyway requires coercive and expensive security barriers. For the investment challenge in security, the main question should be what will happen after a commercial aircraft would have been seriously damage by a drone with many casualties ? Indeed, security is a perception and the main actor is **public opinion**, which may become highly concerned after the first aerial catastrophic accident caused by a drone.

REMINDER: PUBLIC OPINION THE CONSUMER MOVEMENT OF THE 1970S

During the 1970s, after the increased of the mass consumption trend during the 1950s, a growing number of citizens questioned the safety of the « technologically advanced » products flooding the market. In an atmosphere of protest and overall distrust of authority, more and more buyers demanded product safety. The most notable figure of this new consumer movement was Ralph Nader, a young lawyer from Connecticut. In the early 1960s, Nader noted an alarming high number of automobile fatalities. He presented his findings in a 1965 book, *Unsafe at any speed*. Nader charged car manufacturers with putting market share quest ahead of safety[11]. He also challenged the auto industry's claims that drivers were to blame for auto accidents: « the american automobile is produced exclusively to the standards which the manufacturer decides to establish. It comes into the marketplace unchecked. When a car becomes involved in an accident, the entire investigatory, enforcement and claims apparatus that makes up the post-accident response looks almost invariably to driver failure as the cause. Accommodated by

[11] (the politics of protest), Ref : chap 26 the politics of protest, à l'url : http://misdtx.schoolwires.com/cms/lib/tx21000394/centricity/domain/112/ch26a.pdf consulté le 9/1/2019

superficial standards of accident investigation, the car manufacturers exude presumptions of engineering excellence and reliability, and this reputation is accepted by many unknowing motorists[12]. » (Unsafe at any speed)

As for the automotive industry, **public opinion** will helped spur Government to pass **Drone Security Act** after the first catastrophic accident. The act will set mandatory security standards and establish a procedure for notifying drone owners and aviation authorities about defects and vulnerabilities. The drone industry will be subject to federal security regulations. Drone makers will have to **incorporate security standards into their drone designs so that drone/aircraft collision would be extremely improbable and less devastating**. Requirements that called for the installation of anti-collision systems in order to prevent from injuries the millions of airline passengers. These anti-collision barriers would have to be efficient and affordable in order to enable the drone industry to fulfill all of its promise. Today, the main anti-collision systems are:

- ➔ Detection systems: all the electromagnetic spectrum may be used for a liable detection
- ➔ Electronic warfare: mainly used by air forces
- ➔ Kinetic defense: physical neutralization of a drone
- ➔ Geofencing: software limits implemented in the firmware by the manufacturer or by hacking of the drone near the forbidden area

The security drone framework to address the security challenge is a key example for risk management of large-scale digital and technological breakthrough following an S-curve (cf. fig 5). Drone's success may led to calls for a closer examination of numerous other digital goods. Organizations may lobbied Congress and state legislatures to pass laws regulating such products as high tech and connected products with flammable lithium batteries or cyber-attack capacities.

This kind of situations is structural. It is the result of the dynamic of a technological breakthrough following an S-curve. Indeed, the diffusion phase of a technological breakthrough is very short. Hence, there is a veil of ignorance about security issues during the incubation phase and it is quickly replace by a requirement for security and an

[12] (NADER, 1965),Ralph Nader, Unsafe At Any Speed the Designed Dangers, Pocket

acceptable level of risk for public opinion. The risk management challenge is a constraint from public opinion. There is a necessity for the State and the firm to answer such challenge by fungible security means, most of the time based on force, money and information. The duration of the diffusion phase is an amplifier of the security challenge. The more rapid is the diffusion, the more pressing is the security issue.

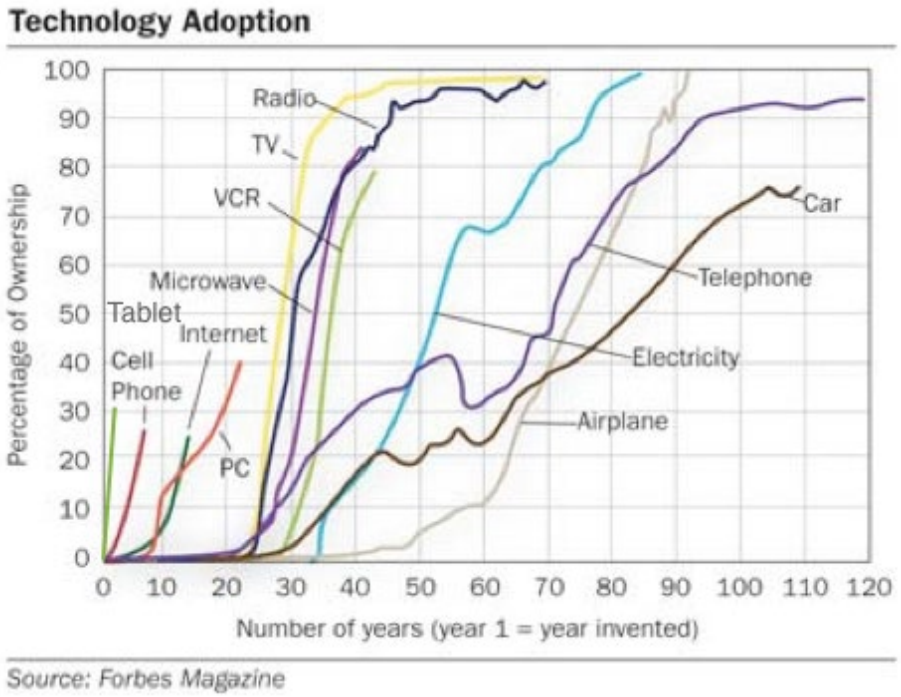

Fig. 5 : the technological S-curve duration of a set of innovations

The rise of the security issue by the pressure of the drone diffusion is revealed by the last 2018 report released of the American Government Accountability Office (GAO) suggesting the FAA needs to improve its risk management process[13].

As for the automotive industry and the driver during the 1950s, the classical manufacturer risk management process will focus on the aircraft and the drone pilots. It will be the main barriers to reduce the frequency of collisions. However, such approach is not able to handle rapid growing threat coming from the gravity of the drone/aircraft collision. Especially when neither mitigation operational barriers for pilots and air traffic

[13] GAO, May 2018, Small unmanned aircraft systems : FAA should improve its management of safety risks, US GAO-18-110

controller exists nor neutralization tools are available for security forces against malevolent use of drones.

Without a permanent and efficient mitigation barriers social acceptance of the risk will be the main obstacle to drone business development after the first catastrophic accident. A low cost permanent and efficient mitigation barriers is « in design » of the drone product, like for the car or aircraft industries. Whatever is the actor at the origin of the risk, drone pilot, either terrorist or unaware civilian; what matters are the consequences of the risk. If it is catastrophic, the security management system will have to address all potential users without free riding possibility. The **reputation of the drone producers' trademark** is under the threat of inducing an unacceptable risk on the airline sector.

WHAT ARE THE PERSPECTIVES?

In order to manage such a complex airspace with so many commercial aircrafts and drones, detection and neutralization systems must be implemented. Systems such as radar, acoustic sensors, radio frequency localization, optical sensing may contribute to a potential mixed solution. However, the number of flying objects to monitor may be very high and induced high infrastructure cost. The cyber space and the digital aviation by focusing on information, geographical coordinate and speed of flying objects may reduce the cost of the monitoring systems. Hence, digital aviation should impose as the main component to manage the flying objects and mitigate the majority of collision risk cases. It means hundreds of thousands of connected flying devices in the sky managed both by air traffic controller and automated devices to forbid part of the airspace to non-authorize flying objects, like airspace above an airport but also sports stadiums, government buildings, military bases, nuclear power plants[14], etc.

In addition, from the military air strategy, electronic warfare is a critical lever to neutralize the adversary defense system, which is a pre requisite in order to reach air domination[15]. Air domination is also a necessary condition for a low death toll in military intervention on ground. Henceforth, electronic warfare is a strong component of air forces

[14] (GETTINGER, 2018) GETTINGER D, Domestic drone threats, available online at : https://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats/ (last access date 1/2/2018)
[15] (CHAMAGNE, 2006, p115) Régis Chamagne, L'art de la guerre aérienne, Esprit du livre éditions

and armies are competing to reach a high level of efficiency[16]. Given the fact that one of the main vulnerability of a drone is the communication between the remote pilot and its drone, this kind of electronic warfare may find its way toward a civilian version for airport and critical areas. It is like the existing link between civil and military nuclear technological know-how. The cost of the technology is spread over military and civilian applications. Iranian demonstrated their ability to take control of a RQ-170 American drone in their airspace by simply spoofing it[17].

In summary, **in design anti collision** system, the monitoring of identified drones and **the military detection/neutralization** of unidentified drones are the main components of a drone security system, which address the security challenge.

ONE THE MOST PROMISING TOOLS FORM THE MANUFACTURER IS GEOFENCING.

An electric fence with the use of a cloud and a box inside drones to supervise drones in real time and to contain licensed drones within authorize and secure airspace is a feasible system. By registering drones with the help of a cloud system, it is possible to track the drones and the owners[18]. The mandatory registration is the necessary condition of such mitigation barrier. It could be reach through in design production of critical electronic components in the drones. DJI, one of the biggest drone manufacturers, has embedded geo fencing electronics and software in its drones that prevents them from flying over thousands of sites worldwide where drone operation is illegal. The electronic and software functions: “GEO” limits flights into zones that raise security concerns (cf. Fig. 6)

[16] ibid, p137
[17] (RAWNSLEY, 2011), Adam RAWNSLEY, Iran’s alleged drone hack, tough, but possible, WIRED
[18] (GETTINGER, 2018) GETTINGER D, Domestic drone threats, available online at : https://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats/ (last access date 1/2/2018)

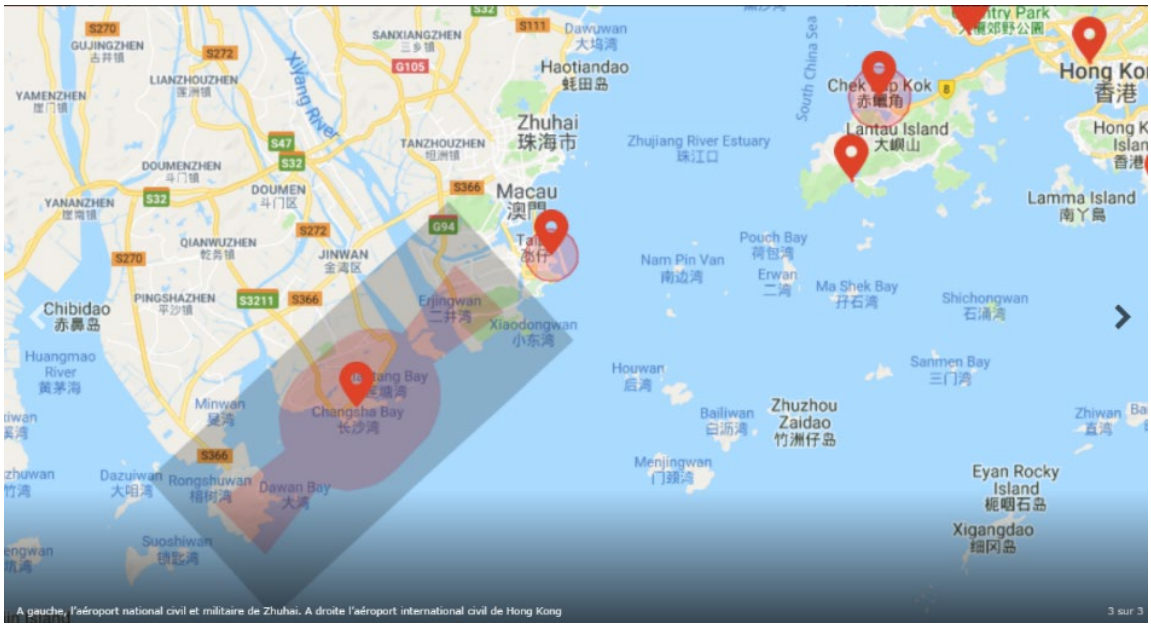

Fig. 6 : A gauche l'aéroport national civil et militaire de Zhuhai, à droite l'aéroport international civil de Hong Kong[19]

The existing DJI GEO system has been put in place since 2013, it enables the definition of circle then polygonal shape aeras to forbid drones or to constraint the maximum altitude a drone may reach. Severals kind of aeras may be defined. There are « Restricted area » which required a writen demand to DJI to get a fly authorization. These areas may be temporary. The « Enhanced warning zone » defined an area where the remote pilote get a warning. The « Altitude zone » simply limits the drone maximum fly altitude, 60 or 120 meters. 32 countries are covered by this GEO system.

There are severals economic and political consequences to this system. DJI customers will be protected from illegal incursion and the associated penalties. Airsapce users will be automatically protected from dangerous airspace incursions from all DJI drones.

But, as a dominant manufacturer it is a **barrier to the entry of potential competitors** (cf. fig. 7). Because of its market share, DJI will decrease the cost of security on all its customer basis. It will take advantage of **the scale factor**. All the customers and airspace users will be satisfy by sharing a low cost security system. Competitors will find very difficult to compete directly on security cost. The customers and airspace users may also

[19] (FRED, 2018) FRED, 23/10/2018, DJI verrouille temporairement les vols à Shenzhen, HelicoMicro at url : https://www.helicomicro.com/2018/10/23/dji-verrouille-temporairement-les-vols-a-shenzhen/

lobbied to insert this system insides the regulatory framework of their countries to limit overhead security cost.

DJI will get the precise knowledge of all the permanent and temporary areas where there are security matters. In the US, the initial provider of area definition data has shift from Airmap to Precision Hawk without legal concerned by the government. The drone manufacturer is becoming the drone **airspace security provider**.

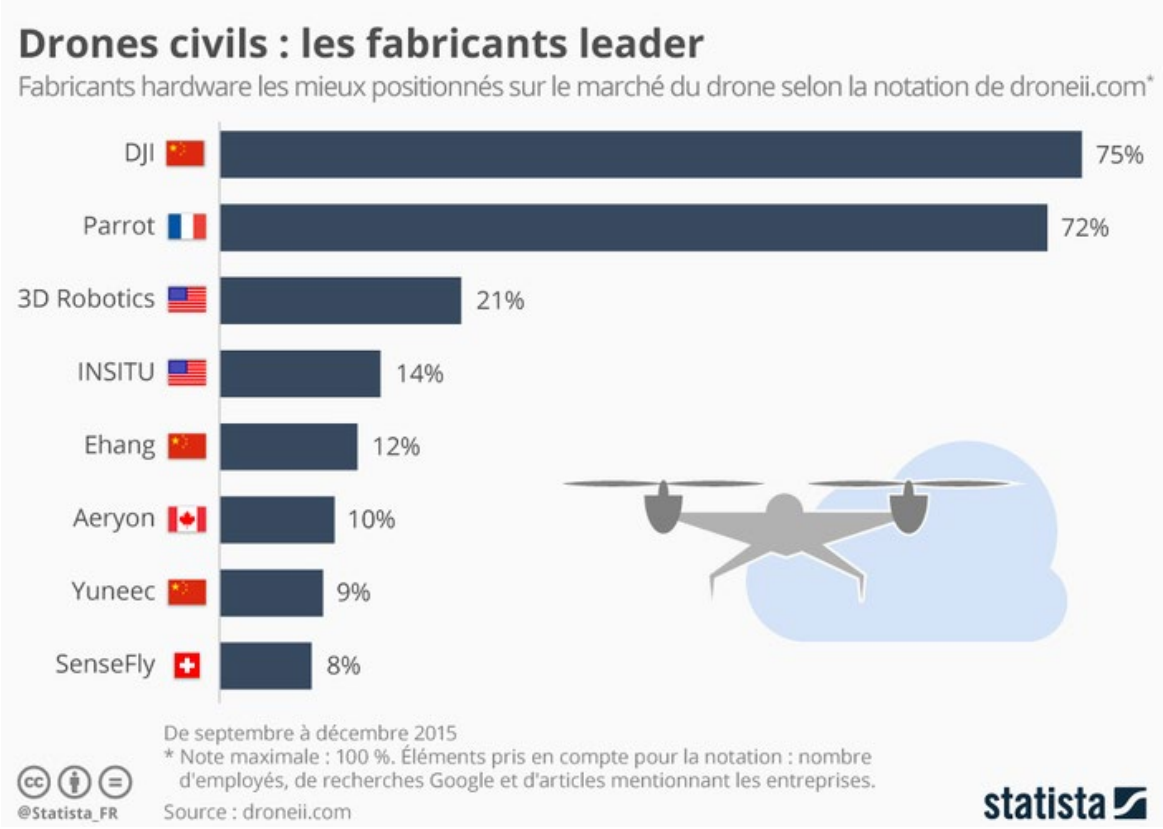

Fig. 7: The drone main producer is the chinese company DJI which dominate the market

As illustrated by the visit of pdt Xi Jinping in Hong Kong on july 2017 and october 2018 where the drone threat was managed with the help of DJI which defined temporary restricted area covering Hong Kong but also Macao and Shenzhen. All DJI drones were pinned to the ground. This functionnal capacities is also a coercive diplomacy tool as it was illustrated by the same Restricted area put in place in Syria to forbid permanently the

use of DJI drone for terrorist activities[20]. The first version of GEO is integrated in the type of drone used against president Maduro, but the drone threat of this particular events was not managed by DJI !

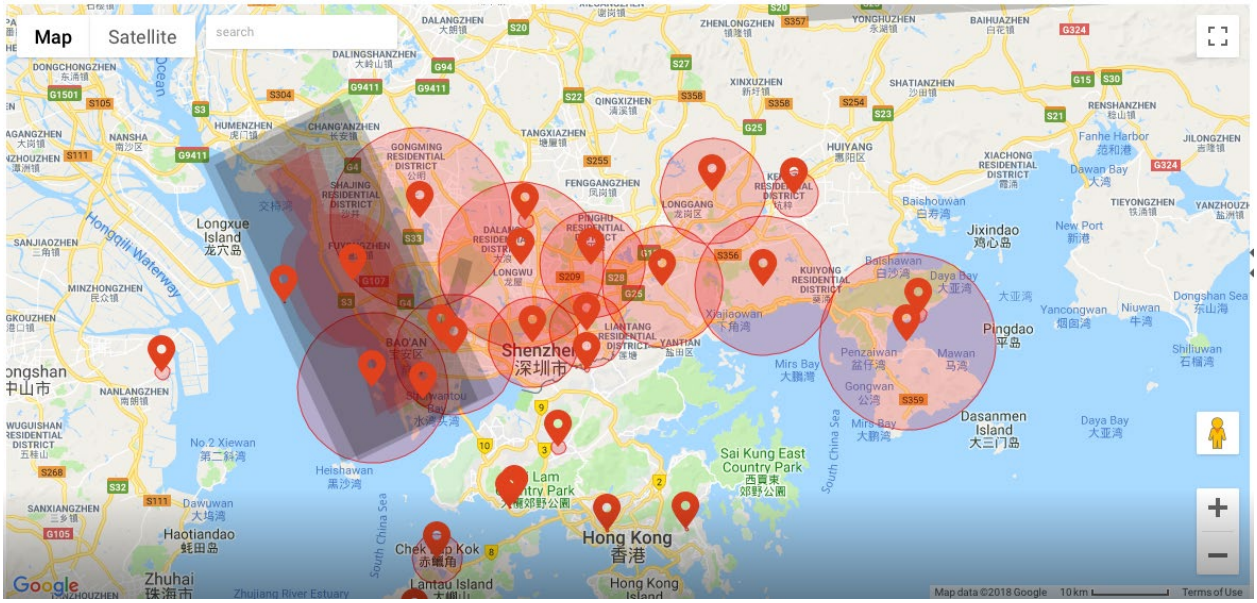

Fig.: temporary forbidden aeras or 80 km x 20 km near Shenzhen[21]

The manufacturer may also access to data concerning all sales drones, where, when and how they are used by commercial and non-commercial customers. It is also a mean to identify all the critical area of a country and the associated activities. Finaly, **the drone manufacturer is a security provider for outside territories**.

THE CONSEQUENCE: A SECURITY PRODUCT AS A STRATEGIC LEVER

A secure product like a DJI drone carry a very low risk of accidental incursion, which represents most of the cases. The mitigation barrier will represent low cost due to the economy of scale of the market share of the first drone manufacturer. Therefore, the dominant producer will be a security provider. The mitigation of intentional intrusions by rudimentary operators may also come under this mitigation system by such manufacturer

[20] (FRED, 2018) FRED, 23/10/2018, DJI verrouille temporairement les vols à Shenzhen, HelicoMicro at url : https://www.helicomicro.com/2018/10/23/dji-verrouille-temporairement-les-vols-a-shenzhen/
[21] ibid

when it will cover all drones through regulatory framework and civilian neutralization capacities.

The drone market is mainly focusing on infrastructure monitoring, agriculture and transport (cf. fig. 8) :

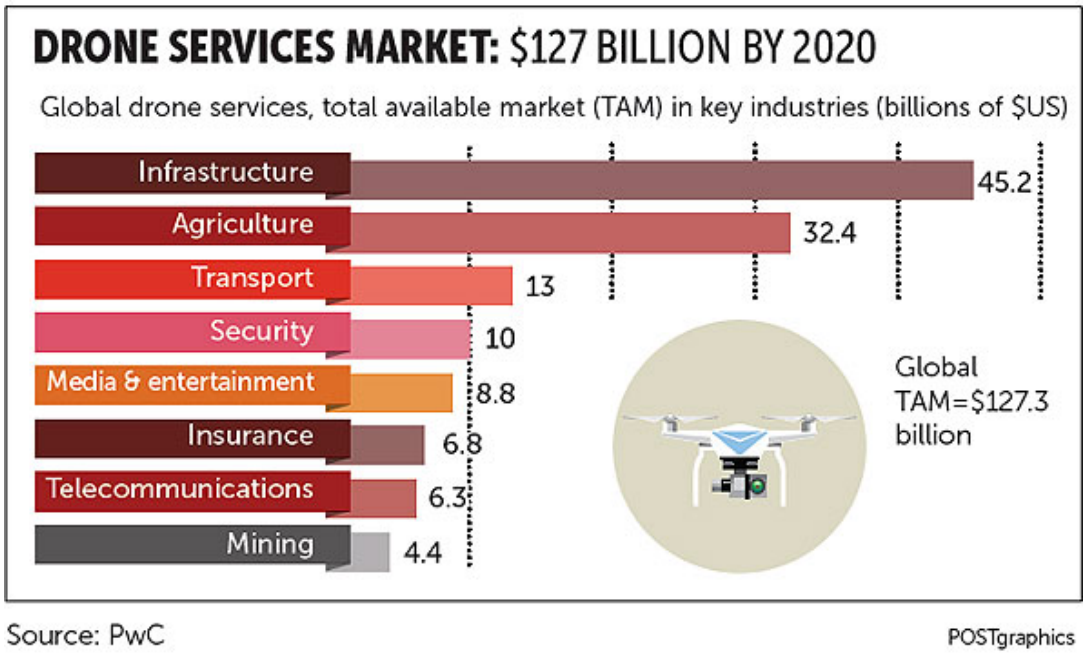

Fig. 8 : The applications and the revenue are on infrastructures.

Consequently, drones will be use on the short term in activities where the size of the territories is important and the security issue is high. These projects will discriminate the trademarks of the drone market between those that provide low cost and efficient anti-collision and anti-incursion systems and the others.

The One Belt One Road (OBOR) strategic program is mainly concerned by infrastructures projects, especially land infrastructures such as roads, railroads, airports, ports, pipelines, etc. The issues for each kind of infrastructure are specifics, for example regarding their maintenance requirements. But, they are crossing dangerous territories where security is the main success criteria. These projects and infrastructures will face migrations, local conflicts, terrorism threat, climatic stress, etc. with the requirement to constantly monitor infrastructures and quickly detect and intervene in case of deterioration. Infrastructures had always established a critical link between territories, private companies and the State sovereignty.

It will be a critical market for the Chinese drones manufacturers. DJI may simply become the airspace security provider for the areas along the OBOR infrastructures covering key territories on the Eurasian continent ; like the Navy which provide security on global sea lane !

This strategy of producing **secure products** with a **private company** as the main **security provider** for the users of the products is a key strategy to become a **global power**. The digital revolution diffusion requires in design security barriers and permanent monitoring of the material infrastructures of any advanced society. The secure product strategy and the rising function of security provider by the firms is a structuring feature of the next decade. ■

ASIA FOCUS #105

FROM SAFE PRODUCT TO SECURE PRODUCT; A CHALLENGE FOR INTERNATIONAL RELATIONS: THE CASE OF DRONES

BY EMMANUEL MENEUT / PHD, CATHOLIC UNIVERSITIES LECTURER

FEBRUARY 2019

ASIA FOCUS

Collection supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille, and Emmanuel LINCOT, professor at the Institut Catholique de Paris – UR "Religion, culture and society" (EA 7403) and Sinoligist.

courmont@iris-france.org – emmanuel.lincot@gmail.com

ASIA PROGRAM

Supervised by Barthélémy COURMONT, research director at IRIS, lecturer at the Université Catholique de Lille.

courmont@iris-france.org

THE FRENCH INSTITUTE FOR INTERNATIONAL AND STRATEGIC AFFAIRS

2 bis rue Mercoeur

75011 PARIS / France

T. + 33 (0) 1 53 27 60 60

contact@iris-france.org

@InstitutIRIS

www.iris-france.org