Terrorism: an answer to the drone challenge

Remotely piloted aircrafts (RPAs)[1] witnessed an exponential increase in sales during recent years[2]. Small-sized[3] RPAs for photography and videography purposes can now be afforded by an average consumer, as price is akin that of digital cameras with nearly identical specifics[4]. At factory settings, an RPA is equipped with an advanced image-capturing system and presents higher payload capacity, which allows for better stability and manoeuvrability.

At non-altered status it could already be used to infringe privacy and/or no-fly-zone legislation. In the United States, the problem of identifying people responsible for breaking flight law already manifested[5]; in Europe, the cases of drones hovering over Gatwick and Heathrow airports has highlighted their inherent potential to cause confusion and inconveniences[6].

Geofencing systems[7], with which RPAs are equipped, have proven fallible. Removing GPS components appears to be a simple process – the drone can then be manoeuvred solely basing on what the integrated image-capturing system transmits. It is also possible to disable the geofencing software through programmes which can be found online[8] – in some cases, it even appears to be virtually non-existent[9].

---

1 Colloquially referred to as "drones" and also known as UAVs (Unmanned Aerial Vehicles), UASs (Unmanned Aerial Systems), or – in the Italian version – APRs (Aeromobili a Pilotaggio Remoto).

2 European Commission (2014), "Remotely Piloted Aviation Systems (RPAs) – Frequently Asked Questions", p. 2 Link: https://bit.ly/2J2gmX9
European Aviation Safety Agency (2016). "Explanatory Note", *Prototype Commission Regulation on Unmanned Aircraft Regulation,* p. 13. Link: https://bit.ly/2IZFpKq

3 RPA Classification

Category	*Operative radius (km)*	*Flight height (m)*	*Flight duration (h)*	*MTOW (kg)*
Nano	< 1	100	< 1	< 0,0250
Micro	< 10	250	1	< 5
Mini	< 10	150 – 300	< 2	< 30

4 An entry-level Canon reflex, like the EOS 1300D, is sold on the Canon official website at € 470,99. In the same price range fall also cameras from other labels, such as the Nikon D3400. DJi, the Chinese company leader in drone-making, prices its drones from the Phantom and Mavic series between 500 and 1.200 dollars. They are the most sold worldwide. In 2017, DJi held more than 36% of the North American market.
Chandler, C. (2017). "For China's high-flying drone maker, the sky's the limit", *Fortune*. Link: https://bit.ly/2vt9BWr
Glaser, A. (2017). "DJi is running away with the drone market", *Recode*. Link: https://bit.ly/2nNIhkd

5 An example is Casey Neistat's case in Manhattan.
P.A. Aitken (2017) "Copy of FAA message sent. Casey Neistat investigation lacks conclusive evidence", *Taitkenflight*. Link: https://bit.ly/2W2f5SY;
Andy (2017) "EXCLUSIVE: Details of Casey Neistat's FAA investigations", *Andy's Travel Blog*. Link: https://bit.ly/2TfKoli.

6 BBC (2018), "Gatwick airport: Drones ground flights", *BBC*. Link: https://bbc.in/2EvX5uW
BBC (2019), "Heathrow airport drone investigated by police and military", *BBC*. Link: https://bbc.in/2Hs4768
BBC (2019), "Heathrow airport: Drone sighting halts departures", *BBC*. Link: https://bbc.in/2RokRAL

7 "Geo-fencing is the concept of restricting drone access by designating specific areas where the drone's soft- ware and/or hardware is designed not to enter, even if the pilot, without intent, instructs the drone to go" European Aviation Safety Agency (2015), "Concept of Operations for Drones…", *ibidem*.

8 Ryan Whitman (2017) "Russian Company Is Selling Mods to Bypass DJI Drone Safety Features", *Extreme Tech*. Link: https://bit.ly/2YCHFj6

9 Interviews conducted with drone enthusiasts have highlighter how, at the moment in which a DJi drone flies in a no-fly zone proximity, the operator is alerted through a pop-up alert. Accepting the alert, the drone continues to function, and it is yet to be verified if and how the geofencing system would behave. The text of the pop-up alert appearing when using a DJi drone can be found here below —
"**No-Fly Zones.** There are 1 Authorization Zone(s) nearby. Authorization zone type: Military Facility(Military Zones). Your aircraft may experience RTH interruption, hovering, or Intelligent Flight Mode cancellation. Please fly with caution. Do you wish to apply for Self-Unlocking to access these zones? No / Yes"

In the Syrian and Iraqi theatres of operations, the first reports regarding use of 'drones' or 'armed drones' by ISIS[10] date back to 2014. They were used to spy on US and Kurdish lines' movements during the 2014-2017 battles, to drop explosives, and as 'kamikaze drones'[11]. Multiple reasons have allowed ISIS to include RPAs in its arsenal: notably, simplicity in purchasing second-hand products online. Their dimensions and flight altitude rarely trigger radars or protective shields; for the same reasons, they are also difficult to spot or engage by personnel on the ground[12]. Tampering with them is uncomplicated, and they can be weaponised in various ways. Last but not least, they can provide images of their activities: videos can be used for propaganda purposes, as has already been the case in late 2017[13].

RPAs for videography and photography purposes are the type exhibiting the biggest potential to turn into a national security issue. The role of the Defence is fundamental in identifying possible solutions for the short-, medium- and long-term to guarantee the protection of the civilian population. A concerted approach from Armed Forces and Law Enforcement would be desirable[14].

Identifying potentially sensible objectives –harder to determine than critical infrastructure[15]– is one of the first problems arising. 'Covering' the whole national territory with anti-drone systems is an objective currently lying out of reach for timing, costs and level of technology.

The necessity materialises to develop an integrated, fully automated *search, find and ID* system basing on two main motivations. The technologies presently available on the market do not present a satisfying cost-benefit ratio, considering the investment needed to acquire them; secondly, a fully automated system has the capacity to resist saturation by removing the man-in-the-loop element[16], pre-envisioning future attacks conducted by swarms[17]. Particular attention should be paid to rapidity of reaction and intervention, which interconnects with the engagement question.

10 "[ISIS] è un progetto politico di lungo termine con confini mobili […] Frutto delle idee di Abu Musab al-Zarqawi, proclamato "Califfato" il 29 giugno 2014 da Abu Bakr al Baghdadi, ha ridisegnato la geografia del Medio Oriente cancellando i confini di Iraq e Siria prodotti dagli accordi di Sykes Picot del 1916. Si proietta contro gli stati postcoloniali che sorgono all'interno della mappa di "Bilad al Sham", la leggendaria nazione araba del Levante che corrisponde agli attuali territori di Iraq, Siria, Giordania, Libano, Israele e Autorità nazionale Palestinese", cit. M. Molinari (2015), "Il Califfato del terrore. Perché lo Stato Islamico minaccia l'Occidente", *Rizzoli*, pp. 10-11.

11 Peter Bergen & Emily Schneider (2014) "Now ISIS has drones?", *CNN.* Link: https://cnn.it/2SMwMWm
Ben Watson (2017) "The Drones of ISIS", *Defense One*. Link: https://bit.ly/2YmIus0
Mike Peshmerganor (2018), *Blood Makes the Grass Grow: A Norwegian Volunteer's Fight Against the Islamic State,* Independently Published.

12 L. E. Davis et al. (2014) "Armed and Dangerous? UAVs and U.S. Security", *RAND Corporation*. Link: https://bit.ly/2LMqWUu

13 The video hereby referred was circulated on the internet through ISIS-affiliated Amaq agency and spread by ABC News (https://ab.co/2Ybr6en). It showed a drone dropping munitions over a Syrian arms depot. Although the author is skeptical regarding the authenticity of the images themselves, the potential for propagandistic use of these technologies remains undeniable. Link to the video: https://bit.ly/2Yxz9BH

14 Only two actors appear to be – at the time of writing – equipped with jamming systems in Italy: central Police services, as they are the ones involved in cases of specific necessity; and offices where classified information is discussed, which undergo periodic checks.

15 Legislative Decree n. 61, 11 April 2011, in actualization of Directive 2008/114/CE concerning individuation and designation of European critical infrastructures and evaluation of the necessity to implement their protection.
Legislative Decree, in Italian: https://bit.ly/2NRjMQj
European Directive: https://bit.ly/2Y6pUZ8

16 "*Human-in-the-loop* (HITL). A model that requires human interaction." Cit. USA Department of Defense (1998), "DoD Modelling and Simulation (M&S) Glossary", DOD 5000.59-M, p. 124 (emphasis in the original).

17 "UAV swarms, inspired mainly by the swarms of insects, are groups of small independent unmanned vehicles that coordinate their operations through autonomous communications to accomplish goals as an intelligent group, with or without human supervision. It may be a heterogeneous mix of machines with dissimilar tasks but contributing synergistically to the overall mission objectives", cit. Puneet Bhalla (2015), "Emerging Trends in Unmanned Aerial Systems", *Scholar Warrior*, Autumn 2015, p. 89.

The long-term objective should be the development of systems acting upon control algorithms so as to "steal" the drone and land it in a safe zone. The danger, in fact, lies in an RPA armed not only with explosives, but CBRN[18] charges as well. Protocols including the creation of a quarantine zone are needed to safeguard both civilian population and specialised personnel.

Since the development of this system is not achievable in the short-term, existing possibilities need to be analysed on a costs-and-benefits basis. In conducting said analysis, problems relating to the TYPE OF COMMAND used for the drone (whether remotely controlled or with a pre-set route) and the TYPE OF ARMAMENT (whether the release of the charge is activated through the remote control; or automatically when the drone is above certain pre-set coordinates; or with a timer).

There are four possible outcomes. Having lost connection to the remote control, the drone incurs in a mid-air stalemate (is essentially *frozen*), automatically goes back to the last known remote-control position, or lands. If a *failsafe system*[19] is not in place, it crashes to the ground[20]: in this case, if armed with explosive charges, it could detonate; if armed with CBRN ones, it could contaminate the area.

A first option of anti-drone technology might regard the use of *jammers*, translating their established use as *counter-IED systems*[21] in conflict areas. Impact on civilian technologies and infrastructures, if used in urban environment, remains to be evaluated on a case-by-case basis[22]. Considering the relatively short distance and duration of drone flights with malevolent potential, absence of a jamming system *in loco*, whether portable[23] or fixed, could implicate missed engagement. Fixed systems in urban environments present problems regarding background noise, though.

18 Chemical, Biological, Radiological and Nuclear.

19 Definitions of "fail-safe" —
(American English): *adj*. "[D]esignating, of, or involving a procedure designed to prevent malfunctioning or unintentional operation […]".
(British English): *adj*. "Something that is fail-safe is designed or made in such a way that nothing dangerous can happen if a part of it goes wrong".
Collins Dictionary, link: https://bit.ly/2Y98T1i

20 In summer 2019, during a drone race in Turin, a hacker attack to the organisers' Wi-Fi made the operators lose control of their drones. This was caused by the fact that all remotely-controlled APRs were operating on the same Wi-Fi network, offered by the organisers – therefore, attacking this infrastructure was a cyberattack which had no direct effect on the drones (it did not intervene on them), but rather broadly speaking on their wireless communication. The causes of the reported "going crazy" of the APRs are to be found in the fact that these were homemade race drones, presumably with no fail-safe system, already launched at high speed at the time they were disconnected from their remote controllers.
Alessandro Contaldo (2019), "Attacco hacker alla drone race: i quadricotteri fuori costretti ad atterraggi di emergenza", *La Repubblica*. Link: https://bit.ly/2NPVGv

21 Here below follow a few definitions —
"An improvised explosive device (IED) is a type on unconventional explosive weapon that can take any form and be activated in a variety of ways. They target soldiers and civilians alike. In today's conflicts, IEDs play an increasingly important role and will continue to be part of the operating environment for future NATO military operations. NATO must remain prepared to counter IEDs in any land or maritime operation involving asymmetrical threats, in which force protection will remain a paramount priority." in NATO (2018), *Improvised explosive devices*, www.bit.ly/2Ykd4qb.
"**Electronic Warfare:** The use of electromagnetic (EM) or directed energy to exploit the electromagnetic spectrum. It may include interception or identification of EM emissions (es.: SIGINT), employment of EM energy, prevention of hostile use of the EM spectrum by an adversary, and actions to ensure efficient employment of that spectrum by the user-State. An example of electronic warfare is radio frequency jamming" in Michael N. Schmitt, editor (2016), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, p. 565.

22 The use of (civilian) jammers is legal in Italy, as long as the limits set by law concerning emissions and exposure are respected and they do not cause an interruption of public service (art. 340, Italian Penal Code). Armed Forces and Law Enforcement can use them in exceptional cases, hence when they operate *in deroga* (lit. notwithstanding the current regulation), e.g. for public safety reasons, protection of personalities, public order *et simili*.

23 As could be, e.g., the Wilson handgun jammer.

A second hypothesis would be the use of conventional ballistic weapons with the intent of shooting the drone down, or eventually armed with net projectiles[24]. This should only be considered as a last resort option, because of the aforementioned risks concerning typology of armament. Undoubtedly, a danger for the civilian population persists if the menace materialises in crowded areas.

A third option would be using predator birds. The reactivity of these animals and their economic impact make them a competitive short-term solution. A falconry nucleus is estimated to have a maximum cost of around fifty thousand euros – that would mean that, with a budget of three million euros[25], the installation of circa sixty falconry nuclei could be feasible. The costs for maintaining a single nucleus appear not to be above the few tens of thousands of euros per year[26].

A fourth option would involve weapons emitting radio frequencies. The specifics of an American-manufactured system appear quite interesting, yet it falls within the category requiring prior authorisation by the Federal Communications Commission to be sold or rented to non-federal users[27].

Lastly, direct-energy systems are increasingly attracting interest: an example would be the Counter Unmanned Aerial System (C-UAS) provided to the Italian Air Force's *Fucilieri*, *16° Stormo* during Russian President Vladimir Putin's visit to Rome in July 2019. It was described as a detection system equipped with devices to electronically interdict flight[28].

In the short term, the most feasible solution would be the constitution of a pilot experiment using a falconry nucleus to monitor exceptional situations involving a high concentration of people and, if need be, intervene – for example, Sunday Mass at the Vatican or the future Winter Olympics in Milano-Cortina 2026.

Information exchange amongst Armed Forces, intelligence and Law Enforcement should be accentuated. To predict possible future trends, attention should be on alterations, which can be found online, defined as "feasible" by hobbyists, enthusiasts and/or ill-intentioned actors. One should avoid the reasoning by which a possible modification, being it non-functioning, does not represent a future menace: when an idea concerning malevolent use of an RPA is put out, it should be considered as feasible, either in the short-term or in a more distant future.

24 COMFOTER SPT (2018), "Sperimentazione antidrone del COMACA", *Esercito*. Link: https://bit.ly/2HeeZnR
Stato Maggiore Esercito (2018), "Sperimentazione antidrone del COMACA", *Difesa Online*. Link: https://bit.ly/32Xf9b5
Maurizio Tortorella (2019), "Abbattete quel drone", *Panorama*. Link: https://bit.ly/2GwHUBF.
According to indiscretions, these exercises have been conducted using a Beretta rifle, caliber 12.

25 This amount has been chosen on purpose. Apparently, the Israeli 'Drone Dome' system, used at Gatwick airport – against the drone which caused the stop of air traffic – costed the United Kingdom 2.6 million pounds (at the moment of writing, equivalent to nearly 2.9 million euros).
Joe Pinkstone (2018), "The £2.6m Israeli 'Drone Dome' system that the Army used to defeat the Gatwick UAV after the technology was developed to fight ISIS in Syria", *Daily Mail Online*. Link: https://dailym.ai/2T4PKXb

26 As experts estimated during interviews.

27 Reference is hereby made to the DronekillerTM, a product of IXI Technology. Company website: https://bit.ly/30ZSOaU
IXI Technology, document on Dronekiller specifics: https://bit.ly/2Ykc5ax

28 "[…] sistema radar di rilevamento munito di dispositivi e ottiche diurne e notturne per l'interdizione elettronica del volo". Cit. Ministero della Difesa / Stato Maggiore della Difesa (2019), "Le Forze Armate concorrono alla cornice di sicurezza per la visita del Presidente Putin", *Difesa. Link:* https://bit.ly/2YzxkF4
All web links indicated in the present document have been last accessed on September 27, 2019.