SCANDINAVIAN JOURNAL OF
MILITARY STUDIES

Guitton, M. J. (2021). Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms. *Scandinavian Journal of Military Studies,* 4(1), pp. 26–36. DOI: https://doi.org/10.31374/sjms.53

RESEARCH ARTICLE

Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms

Matthieu J. Guitton[1,2]

[1] Faculty of Medicine, Université Laval, Quebec City, QC, CA

[2] CERVO Brain Research Center, Quebec City, QC, CA

matthieu.guitton@fmed.ulaval.ca

The use of unmanned aerial vehicles (UAVs) or "drones" in military contexts has skyrocketed in the last two decades, with missions ranging from surveillance, reconnaissance, and intelligence to combat support. Technological advances have led to an increase in drone capabilities and reliability, on the one hand, and to a decrease of production costs, on the other hand. Furthermore, drone availability has also drastically increased, and equipment that was once the exclusive privilege of a few countries can now be obtained by all national armed forces – and, as evidenced by recent attacks, by non-official forces. In this context, drones can become part of any conflict, and military strategists have to include response to drones and to potential drone swarms in their operational scenarios. Therefore, defense against drones has to become a component of any full-fledged military strategy. This analysis explores the conceptual and operational changes for military forces triggered by the massive emergence of drones, including the theoretical and practical challenges related to training and implementing specific anti-drone units. First, the evolution of the threats related to drones and drone swarms is identified. We then summarize the different possible countermeasures. Finally, we propose practical solutions to deploy these countermeasures, notably by exploring the possibilities of development and deployment of specialized anti-drone units and examining some of the challenges associated with fighting high-tech unmanned enemies rather than fighting soldiers in conventional battlefields.

Keywords: drone; military training; military workforce; UAV; UCAV; unmanned aerial vehicle

Introduction

Drones – the colloquial name for unmanned aerial vehicles (UAVs) – are no longer found exclusively in science fiction and anticipatory novels. Indeed, they are becoming a more and more common component of modern cityscapes. Due to their versatility and accessibility, the popularity of drones for civilian uses keeps growing, both in terms of number of users and variety of purposes. The utilization of drones is being promoted to fields as diverse as research (Coops, Goodbody & Cao 2019) or emergency responses (He, Chan & Guizani 2017).

This visibility of civilian drones should not overshadow the fact that drones were initially developed by the military, for military purposes. Military applications of drones are numerous, ranging from tasks similar to what can be seen for civilian drones (e.g., surveillance and reconnaissance, yet directed to military or intelligence targets) to combat situations with UCAVs – unmanned combat aerial vehicles (Lucas 2014). In less than two decades, drones have come to play a significant role in supporting U.S. operations in Iraq and Afghanistan (Sharkey 2011). The September 14, 2019 attacks against the state-owned oil facilities at Abqaiq and Khurais in Saudi Arabia took the use of drones in war a step further (Hubbard, Karasz & Reed 2019). Indeed, in contrast to previous military uses of drones, the attacks were not openly launched by official armed forces. Although the Houthi movement (a Yemen-based Islamic armed movement) claimed the

attack, U.S. authorities asserted that the attacks originated from Iran (Said, Malsin & Donati 2019). The question of the real masterminds behind the Abqaiq-Khurais attacks is irrelevant here; what matters is that the recent events in Saudi Arabia epitomize the fact that drones are no longer an exclusive technology mastered only by a few nations. Drones can now be used for military purposes not only by legitimate armed forces, but also by a myriad of others, including terrorists or other non-state actors. The proliferation of drones that are cheaper, easier, and faster to produce not only recasts the way surveillance or reconnaissance is devised and performed, but also provides new ways to hassle or intimidate potential opponents. Furthermore, this proliferation of cheap and readily unmanned units clearly boosts the risk of conflict spirals across the world (Boyle 2015). The increased degree of autonomy of drones is also questioning defense forces responses. Indeed, drones can range from non-autonomous (requiring the constant control of a human pilot) to fully autonomous (programmed to carry on their mission without any further human intervention once launched). Of note, all the possible intermediate levels of autonomy can exist between the two ends of this continuum. Also, autonomy can be provided either by pre-programming (thus limiting the possibilities for adaption of the drones once launched) or through the use of artificial intelligence (AI) modules, providing the drones with more adaptability. Alongside increasing their own capacities by acquiring specialized fleets of drones, developing countermeasures will be critical for military forces. Thus, acquiring proper anti-drone response units will likely be one of the focuses of military leaders in the very near future.

Defense against drones has to become part of any full-fledged, long-term military dynamics. Thus, armed forces will have to adapt to this emerging reality. The changes required to answer unmanned threats are not purely conceptual; they will have to translate into operational changes. These changes must take place not only at the level of conventional forces defending against drones (notably at the land/sea interface) and drone-deploying forces preparing to counter drones, but also at the commanding and strategic levels of military staff. Furthermore, the reflection needs to be performed both by army, navy, and air force staff, as the issue of drone defense affects all the services. In this perspective, this text will analyze this question while keeping three operative challenges in mind: analyzing the context and identifying the threats, implementing effective countermeasures, and deploying these countermeasures with an appropriate military workforce – notably by exploring the possibilities and challenges related to the development, deployment, and maintenance of specialized anti-drone units.

1. Emerging Technology, Emerging Problematic

1.1. A Dreadful Convergence of Technologies

The first two decades of the twenty-first century have witnessed a drastic acceleration in technological breakouts. These breakouts have touched upon numerous fields, including biological sciences (biotechnologies, genetic engineering, including genome editing, cognitive science, etc.), computer science and information technologies (big data, AI, social media and social engineering, Internet of things, quantum computing, etc.), and engineering (hardware progress, robotics, nanotechnology, new material technologies, cybernetic systems, wireless technologies, alternative fuel and energy systems, autonomous vehicles, etc.). These diverse and revolutionizing innovations are referred to as emerging technologies (Rotolo, Hicks & Martin 2015). The societal impacts of these scientific advances are so deep that some authors qualify the period we are living in as the Fourth Industrial Revolution (with its industrial subset, Industry 4.0) or the Second Machine Age (Brynjolfsson & McAfee 2014; Schwab 2017). In this context, drones are the pure representative of the various avatars of this revolution. Indeed, drones are at the crossroads of various technologies, ranging from AI to advances in material (including 3D printing) and energy sciences. They in fact embody the convergence and synthesis of emerging technologies.

Innovations already available or likely to be so in the near future can find their application for drones:

- Embarked electronics: Embarked electronic systems are the heart and the core of UAVs. Advances in electronic systems, including sensors, hardware, and software, are directly supporting the increase in drone performance and reliability.
- Real-time geolocalizing technologies: GPS and other satellite-based technologies have tremendously increased navigation capabilities. Although not flawless, these technologies can be used to guide both drones and the missiles they might carry. The emergence of multi-modal and combined geolocalizing technologies makes drones more and more resistant to jamming attempts.
- Connectivity, interconnectivity, and interoperability: Communication is central for drones, either to stay in contact with their pilots or to allow GPS-dependent or GPS-independent navigation. Wireless

technology has allowed drones to join the global Internet of things – drones can be connected to devices as common as regular cell phones. This massive connectivity of drones and interoperability with other systems is however a double-edged sword, as it may allow the enemy to penetrate the embarked systems.
- AI: One of the popular flagships of the emerging technologies, AI has major significance for drones. Supported by enhanced sensor capacities, task-specific AI will allow drones to move to fully autonomous units. Applying AI to drones will also trigger legal and ethical debates, magnified by the military use of UAVs.
- Energy science: Advances in battery engineering (both in terms of reduction of size and increase of capacity) directly impact the autonomy of drones, increasing their range and striking capabilities.
- Material science: Development of lighter and more resistant materials reduces the weight of drones while increasing their durability and their potential loading charge. Innovations in production systems such as 3D printing both make it easier to manufacture drones on a large scale and reduce the production cost.
- Warhead technologies: Advances in weapon sciences have allowed the development of small warheads considerably more lethal than past ones. Just like manned aircrafts, drones can carry missiles. Drones can act as a platform for bringing autonomous warheads within a closer range – much closer than a regular aircraft can, and without putting a human pilot within a threatening area.

1.2. Democratization of Drones

Drones are no longer an object of technological luxury. Indeed, their use has largely proliferated, and they are now fully democratized. Once led by just a few countries (originally the USA and Israel mainly), drone technology and the related expertise are now widespread. Although U.S. drones still dominate the international military market, more and more nations are developing their own models and the capacities to market UCAVs. This is notably the case of China, France, India, the United Kingdom, and Turkey. Regarding the civilian drones market, China and France are already in front of the USA in terms of global sales.

Manufacturing drones is no longer a challenge, and acquiring the necessary expertise to produce drones is easy nowadays. The emergence of technology such as 3D printing has been a game changer for numerous problems of production, and drone production is no exception (Hammes 2019). For instance, in 2014 U.S. academic researchers succeeded in producing a functional autonomous drone with a 50-kilometer range in less than 48 hours using 3D printing technology (Golson 2014). Further progress has been made since then. As production costs drop, prices of drones follow. While this is true for combat drones, the situation for civilian drones is even more marked, with civilian drones affordable for almost anyone and readily found in many regular retail shops. Not only are civilian drones readily found, they can also be reshaped for military purposes extremely easily. Converting a UAV into a UCAV can be done with but a few upgrades. In fact, civilian-grade drones can even be used without modification for short reconnaissance missions. International commercial competition pushes further applied research on drones, and drone reliability has considerably increased in the last few years. Given the light weight and small size of a lot of drones, they are easily delivered to buyers. U.S., Chinese, and Russian companies are already delivering ready-to-fight UCAVs in standard containers – with the added advantage of offering the possibility to use the shipment as a potential launching platform (Hammes 2019).

To face this drastic increase in the number of drones in circulation, developing normative and legal frameworks for drones will be necessary (Boyle 2015). Several countries have already taken steps in this direction. However, and that being said, given the ease of production, the ease of customization, the already important and constantly growing penetration of drones in civilian and military markets, and the increase of international tensions, attempts to try to slow down the global race for drones are simply illusory. Drones are part of the military landscape, and they are going to be even more so in the coming decades.

1.3. Drone Swarms

Among the various characteristics of drones, several of them have major implications for future military applications. This is notably the case for their small size and high maneuverability, their cheap production costs, the possibility for a single operator to simultaneously control several drones, and the possibility for drones to be semi-autonomous or even fully autonomous. When taken together, these characteristics make plausible the emergence of offensive strategies based on massive multi-unit assaults or, in other words, "drone swarm" attacks.

Mimicry of biological systems – also known as biomimicry – has been central to drone development. From the shape of the drone to sensor systems and in-flight behavior, drone technology has been heavily inspired by nature – typically insects and birds. The very name used colloquially for a UAV – a drone – comes from biology (a drone is a male honey bee), and the concept of a swarm, widely used in the field of robotics by analogy for what is seen among some highly social animals (Beni 2005; Brambilla et al. 2013; Garattoni & Birattari 2018), finds its natural continuity in drones. Interestingly, the concept of "swarming" has been foreseen as one of the most important challenges that military strategy will have to face in the future (Arquilla & Ronfeldt 2000), and it is likely to be operationalized in the coming years with drones. To push the comparison with biological systems even further, a drone swarm would be a pretty good example of a manifestation of the ancient locust swarms. This type of mechanical swarming would be as difficult to counter as was its biological counterpart.

The operationalizing of drone swarms in actual battlefields depends on at least three factors: the deployment of the drones of the swarm, their degree of autonomy, and their degree of coordination (Hammes 2019). As stated above, any basic container can be used as a launching platform for a large number of small drones, given their diminutive size compared to standard aircrafts and the ability of numerous drones to take off vertically. Even large drones typically require less space to be launched than a manned aircraft of equivalent size. A good example has been provided by the Chinese forces, who can deploy a battery of 18 nine-foot wingspan Harpy UCAVs from a two-men crew five-ton truck (Hammes 2019). Thus, quick deployment of large numbers of drones can easily be done with a fleet of just a few trucks or similar container-transporting vehicles. If massive deployment of drones is not an issue *per se*, operating them successfully in a combat situation may require significant logistic resources. Indeed, the number of drones a single pilot can handle is limited. The key parameter to overcome this limitation is to increase the degree of autonomy of the drones. At the end of the spectrum, fully autonomous drones do not even need to maintain contact with their human operator – thus incidentally decreasing the risk of jamming of their communication and electronic systems. On the other hand, once a mission and objectives have been assigned to fully autonomous drones, it is difficult to change the orders. In other words, providing autonomy to drones means for the sending forces to trade their ability to control their swarm once launched. Although it is quite possible to deploy a large number of autonomous drones, coordinating the drones within the swarm is another issue. Indeed, coordination would allow optimal use of the drones and drastically increases the chances for the drones to reach their target. Yet, coordination of large swarms would require important computational power – something that might soon be attained with the help of AI – and massive interactions between the drones as well as between the drones and their environment, increasing the potential vulnerability of the drones to external cyber-attacks. Non-coordinated drones, however, would not require that much work: The strategy would be to simply rely on the number of attacking units to get the desired effect – in this case, the destruction of the target. Yet, large, non-coordinated fleets of drones are likely to suffer important losses through fratricide, i.e., accidental destruction by drones from the same fleet (Hammes 2019). Therefore, within-swarm coordination is currently a challenge for the implementation of military drone swarms. That being said, given the pace of advances in computing sciences, this challenge is likely to meet solutions in a near future.

The questions of optimizing human-swarm communication and maintaining control over swarm navigation are central for operationalizing drone swarms in a military context. These questions have not been left unaddressed, though. Indeed, while having originally emerged from biology (with the study of social animals' collective behavior), the field of swarm research has extended to numerous other disciplines, including robotics, engineering, and computation (Beni 2005; Brambilla et al. 2013). The fact that swarm behavior research is highly translational positively influences the future implementation of military drone swarms. Indeed, as autonomous or semi-autonomous multi-unit systems, drone swarms can directly benefit from research advances in swarm intelligence and swarm robotics (Brambilla et al. 2013; Garattoni & Birattari 2018). Independently of research dealing with general robotics, research on drone swarms specifically is also currently taking place. For instance, new interfaces are being developed in order to allow human operators to guide larger drone formations more optimally, using various strategies such as impedance control and haptic feedback (Tsykunov et al. 2019). Although not presently seen in operational battlefields, drone swarms are a reality which military strategy will have to deal with in a foreseeable future.

2. Countermeasures

2.1. Passive Countermeasures: Protection and Detection

To some extent, passive protection against drones can be provided by the way physical infrastructures are designed and built or their location. Indeed, drones are aircrafts. Like for any airborne offensive, the target of a drone needs to be accessible from above to be reached. Underground facilities and heavily shielded targets are more challenging to destroy with the types of warheads a drone can carry. Sensitive military infrastructures used to be built in remote areas. Yet, this passive strategy is no longer so relevant. Indeed, with modern space-based Earth imagery, there is practically not a single place on Earth that could truly be considered as "remote". Thanks to satellite imagery, it is nowadays utopian to believe that a potential structural target can remain unlocalized, or that movements of military units can remain unnoticed. As unmanned vehicles, drones heavily rely on geolocalization systems to navigate from their launching base to their target. Thus, drones are vulnerable to technologies deteriorating GPS signals, specifically GPS spoofing and GPS jamming. There is however a limit to what can be done with purely passive infrastructural protection, and for the most part these limits have already been reached. Indeed, systems such as the military SAASM (Selective Availability Anti-Spoofing Module) can alleviate the effects of GPS spoofing produced by the U.S. military. Other systems can be developed to allow GPS receivers to detect spoofing or jamming attempts. Once GPS spoofing or jamming is detected, it is possible for drones to switch to other modes of navigation. Indeed, drones can use various other sensor methods to navigate in a GPS-denied environment, ranging from visual mode, infrared, radar, sonar (for underwater drones), electronic/electromagnetic detection to a combination of any of these methods. Even if relying solely on satellite-derived signals, solutions can be developed. Indeed, civilian researchers using non-military-grade technology and algorithms have been able to obtain complete and dynamic geolocalizing features despite being in an area of military GPS denial, practically defeating U.S. Army GPS signal alteration systems (Voosen 2019). Applying similar methods to drone navigation would basically render them immune to GPS spoofing and GPS jamming.

Detecting a drone is quite a challenging task. Due to the small size of most UAVs, drones have a radar signature not different from that of a bird. In addition, some drones have stealthy characteristics, either stealth configuration (such as the U.S.-built Kratos QX-222 Valkyrie) or coating, meant to reduce their radar signature. So since relying solely on radar is not a viable option, alternative methods have to be devised to detect approaching drones. With their embarked systems and their use of wireless or satellite signals, drones produce specific and sometimes important electronic signatures. Yet, Faraday cages can reduce the electronic noise. Furthermore, wireless or satellite communication can be turned off when approaching a target if the drone switches to alternative guiding modes – especially for fully autonomous drones that do not need to stay in contact with their human operator. Visual recognition (for instance, with task-specific AI or deep-learning strategies) can be used to identify drones. Yet, their features can be designed to make pattern identification challenging, particularly since drones are typically in motion.

Drones performing aerial maneuvers generate noise, and their acoustic signature can thus expose them. Various audio processing methods are currently being developed to solve the problem of drone localization (Rascon, Ruiz-Espitia & Martinez-Carranza 2019). However, several important issues limit acoustic drone detection in real-life situations. Indeed, drone-generated noise is dynamic as drones are usually in motion. Furthermore, drone-generated noise typically has a very low signal-to-noise ratio. In other words, detecting drones in a noisy environment is quite difficult. Thus, as for other detection strategies, a lot more research will have to be done before acoustic methods can be used as a reliable source of drone detection. Just like passive protection, drone detection has its limits. Once drones are detected nearby a restricted area or a potential target, the next step of a drone defense strategy is the destruction of enemy units. This is what the next sections will explore.

2.2. Active Countermeasures: Destruction

Drones are not without weaknesses. Several strategies can be used by soldiers to disable or destroy enemy drones. However, no solution is perfect, and countermeasures can be developed to counter these countermeasures. Thus, optimal anti-drone strategies should combine several approaches in order to insure maximal efficiency of anti-drone units (**Table 1**).

– *Direct fire*
  Direct fire is typically the primary type of response to UCAV attacks. Of note, direct fire can be conducted either by human shooters or via automated counter-air defense systems. This solution presents

Table 1: Countermeasures against drones, and their limitations.

Countermeasure	Effect on target	Limitations/vulnerability
Direct fire	Destruction	Size of targets Number of targets Visibility
Hunting drones	Destruction	Number of targets Visibility Inherent drone weaknesses Deployment time
Missiles	Destruction	Costs
Laser weapons	Destruction	Atmospheric conditions Smokescreens Target's coating
Microwave weapons	Disabling	Sealing of electronics
Electronic jamming	Disabling Control taking	Sealing of electronics
Defending drone swarm	Individual destructions Swarm disruption	Lack of accurate response Deployment time

several limits, though. First, drones can be relatively small, and the size of the target may represent a marksmanship challenge. Second, direct fire can be hindered by lack of visibility (due to the day/night cycle, obstacles in the line-of-sight, or atmospheric conditions). Third, direct fire is easily overwhelmed by a drone swarm attack.

– *Hunting drones*
Defenders can use drones to hunt enemy drones. In such situations, defenders have several major advantages when operating their drones. Since defending drones typically operate very close to their launching point, autonomy is not an issue – in contrast to attacking drones that have to cover longer distances before reaching their target. Furthermore, while a defending drone can be used as a flying firing platform if equipped with appropriate weaponry, it can also be used in "suicide mode", aiming at destroying attacking drones by direct collision. Finally, defending drones are considerably less vulnerable to issues related to guiding and navigation. In fact, a drone can be operated visually from a direct line-of-sight of around 245 meters (Li et al. 2019). This distance – depending on human characteristics rather than on the type of drone – is still reasonable to counter the attack of a drone equipped with a relatively small warhead. This strategy still presents several limitations, though. All limitations related to direct fire apply to hunting drones. In addition, hunting drones have the usual weaknesses of drones (including the vulnerability of their embarked electronic systems to destruction or to hijacking). Furthermore, the time it takes to deploy hunting drones might render them difficult to use in a timely manner in the context of a surprise attack from enemy UCAVs.

– *Use of missiles*
Missiles and other autonomous warheads can be used to destroy drones. Missiles are fast and accurate enough to destroy UAVs. However, this is literally like using a hammer to kill a fly. Although theoretically possible, using autonomous missiles to destroy drones is not a cost-effective solution. While drones are getting cheaper and cheaper, the costs related to missiles remain important. The fact that autonomous missiles are single use weapons also contributes to making this solution too expensive to be realistically deployed on a large scale.

– *Laser weapons*
Laser weapons are directed-energy weapons based on laser, i.e., on systems emitting electromagnetic radiation-amplified light coherently under the form of a narrow beam. When reaching its target, the laser beam will transfer a considerable amount of energy to the target, making it burn, or otherwise triggering significant damage (Coffey 2014). The possibility to follow the movements of the target

("tracking" the target) and the focalized area where the beam reaches its maximal intensity makes laser weapons perfectly suited for small moving targets such as drones. Thus, it is not surprising that several anti-drone laser weapons are currently being developed worldwide. However, since laser weapons are based on light beams, they are very sensitive to atmospheric conditions and smokescreens. Furthermore, the impact of laser can be considerably degraded if the light is reflected away from the target. Thus, coating the UAVs with ablative materials or covering them with mirrors can effectively counter most laser weapons, or at least significantly reduce their efficiency (Hambling 2016).

– *Microwave weapons*
Drones' functioning relies on the work of a lot of embarked systems, from sensors to autonomous processing systems. Destroying the embarked electronics equals disabling the drone. Microwave-based weapons aim at doing just that. Like laser weapons, microwave weapons are directed-energy weapons. However, while some laser weapons are already operational, microwave weapons currently remain mostly experimental. Furthermore, using Faraday cages to protect embarked electronic systems (something which is already possible to implement, even with 3D printer technologies) may represent a strong countermeasure against this type of weapon.

– *Vulnerabilities of electronic and communication systems*
Instead of trying to destroy the embarked electronic systems, using microwave weapons, for example, another anti-drone strategy is to take advantage of these systems and of their inherent connectivity. Even the most autonomous drones need to access external sources such as GPS signals for navigation purposes. Thus, drones are connected through Wi-Fi, GPS, radio waves, etc. – each of these communication channels representing a potential entrance to their internal systems. Even without military-grade technology, it is easy to exploit the transmission protocols, and then the vulnerabilities of their hardware/software (Dey et al. 2018). Drones are susceptible to GPS spoofing, GPS attacks, jamming, drone-specific malware ("maldrones"), and wireless attacks (Kerns et al. 2014). Although military drone systems are typically more protected than civilian drones (for instance, by using encrypted GPS signals for navigation), they are far from invulnerable to hacking. Attacks on the electronic systems or functions of a drone can have various aims: 1) feeding erroneous information to the drone's navigation systems, inducing drone "blindness" and disorientation, leading to rerouting or a crash, 2) hacking the drone systems, either to corrupt the hardware/software systems or to obtain information or data, or 3) taking control of the drone. Making a drone crash instead of simply destroying it can have advantages, for instance to recover components or information related to the navigation, sensors, or weapon systems of the drone (notably through reverse engineering). Hijacking is done by disconnecting the drone from its initial controller and replacing this connection. Of note, drone hijacking can be done using another drone as a platform. The hijacking drone will take control of nearby drones while flying among them, creating a fleet of enslaved drones. However, attempts to disrupt a drone using the weakness of its electronic systems can also be countered. As for microwave-based attacks, methods focusing on electronics can be countered by securing the electronic parts of the drone in Faraday cages (structure designed to block electromagnetic fields). Cybersecurity and software-based techniques can also be implemented in order to make the drone systems more difficult to hack, including using encryption to protect library files, using obfuscators to prevent decompiling, checking GPS latency and subframe data, securing Wi-Fi and open ports, or improving radio communication security (Dey et al. 2018).

– *Defender drone swarms*
None of the approaches mentioned above are sufficient to deal with attacks conducted by drone swarms. Indeed, whatever the system selected, the capacity of the defenders would simply be overwhelmed by the sheer number of autonomous attacking units. An interesting response strategy here could be to deploy another drone swarm, i.e., to have a high number of drones ready to take off in case of an assault. Defending drones do not necessarily need to be coordinated. Indeed, while uncoordinated, autonomous or semi-autonomous drones would clearly miss some of their targets or catch sister drones (i.e., drones belonging to the same swarm) into "friendly fire", the elevated number of potential targets from the swarm coupled with the elevated number of defending drones would make the probability of destruction of a significant proportion of the attacking drones high enough, leading to major disruption of the attacking swarm. Although using a drone swarm to counter another drone

swarm is a valid strategy, this would not lead to the total destruction of the attacking fleet. Thus, this approach would likely need to be combined with other methods (typically direct fire) to eliminate the remains of the swarm. Yet, the efficiency of direct fire would increase considerably if the number of attacking drones was initially drastically reduced by the defending swarm. That being said, the collision of the two swarms might create additional smokescreens and some degree of confusion, which might in turn reduce the marksman capacities to eradicate the last attackers. Like individual defending drones, defending drone swarms deployed for operational purposes might face the issue of speed of drone deployment. This point should be kept in mind when deciding the location of UCAV storage areas and launching platforms.

3. Development of a Specific Workforce

From an operative perspective, the response to the present and future increase in drones in military battlefields will require the development and deployment of specialized anti-drone units. The soldiers who will be part of these units will face a reality different from that of other soldiers; fighting high-tech unmanned enemies is not the same as fighting soldiers in conventional battlefields.

3.1. Technological Expertise

Even if anti-drone units remain limited within armed forces, the training of their members will face important challenges. Indeed, members of anti-drone units must display a large array of technical expertise, not just related to the drones, but also in operating and maintaining specific anti-drone equipment, which is unconventional for regular troops (e.g., laser weapons or microwave systems). Thus, from a training perspective, members of anti-drone units must receive both combat training and technological training. While combat expertise is obviously widespread within military forces and military education and training infrastructures, this is not the case for science and technology. It is important to note that these problematic interactions between conventional combat mastery and expertise in emerging technologies – and the related issue of training personnel in both fields – are not specific to operational military units. This is indeed a more global issue for modern security, as exemplified by the strategic and practical challenges related to building an intelligence and counterintelligence workforce with expertise in biotechnology capable of answering current international threats (Guitton 2020). Therefore, the solution to insuring that soldiers are able to acquire specific scientific and technical knowledge is not necessarily found in the exclusive training of a single unit. Instead, the solution is, by nature, multidisciplinary. The training of small, specialized units could thus be shared across different military specialties. In the case of anti-drone units, some of the specific technical knowledge which should be acquired by soldiers might be similar or at least somewhat similar to that of scouting units specializing in long-range detection. For a given nation, finding enough specialized units to undergo shared or cross-disciplinary training would certainly contribute to reducing costs related to formation, help build a larger human resources base for recruitment, and thus make a stronger workforce available to anti-drone units.

3.2. Invisibility Training

As for any specialized unit aiming at countering a specific type of enemy, the training of anti-drone soldiers needs to take into consideration the characteristics of their target. One of the main characteristics of drones is their very high degree of mobility. Due to their small size and autonomy, UCAVs can deploy extremely fast and deeply penetrate advanced lines before being detected. Therefore, in order to neutralize UCAVs, anti-drone units need to be extremely mobile as well. Anti-drone units must be able to engage their target quickly. Yet, given the versatility of drones, they also need to be able to disengage quickly to shift from one battlefield to the next. Furthermore, drones are at home in all types of battlefields, including high-density urban areas or even water/land interface areas. Mobility of anti-drone units should not be understood simply as spatial mobility, but also as conceptual mobility, though. Indeed, anti-drone units need to be able to switch from one battle modality to another, depending on the specific resistance of the UCAVs they are targeting.

Another characteristic of drones is their massive use of diverse sensors. Thus, anti-drone units maneuverability should be accompanied by a certain level of stealth. Anti-drone units should be able to move quickly, and to do so while remaining as unnoticed as possible. Such "invisibility" should extend outside of the battlefield as well. Indeed, drone war is a type of war heavily based on information. As drones are typically partially autonomous, directing drones requires at least some level of knowledge of the enemy's defense system. While the existence of anti-drone units can have a valid dissuasive impact, such units should remain

as secretive as possible regarding their exact equipment and deployment information, as this will make them more difficult to counter – and will help them achieve a maximum effect if faced with enemy UCAVs. Of note, this relationship between stealth in the battlefield and discretion outside of the battlefield is not something new. Indeed, historically, it was already conceptualized in conflicts where information gathering was critical. For instance, Hensōjutsu, which grouped the techniques of disguise of feudal Japan's shinobi, was part of the Jintonpō, the "methods to attain invisibility". In the digital era, invisibility goes a step further: Members of anti-drone units should remain cautious when using virtual spaces to avoid publicizing sensible content or publishing items that could provide either direct or indirect information. If identified as such, members of anti-drone units might become the privileged targets of manipulation by foreign intelligence services (Guitton 2019).

3.3. Psychological Support

The emergence of unmanned fights has created new forms of battle stress for all those exposed to drones – both for soldiers and civilians. Military drone pilots have repeatedly been reported to experience important levels of psychological stress from combat events (Sharkey 2011). Given that anti-drone units, by definition, mainly fire at unmanned drones rather than at humans, this might seem less relevant for operators of defending drones. Yet, the way strikes are delivered through UCAVs is an accentuating factor for the occurrence of psychological stress (Sharkey 2011), regardless of whether the target is human, making the risks for defending drones pilots to suffer similar outcomes real. Although post-traumatic stress disorder (PTSD) is often seen as the flagship of mental health issues among drone pilots, UCAV operators report a wide range of mental health problems, including hazardous alcohol use, depression, moderate or severe anxiety, and sub-clinical PTSD symptoms (Chappelle et al. 2014; Phillips et al. 2019). While in the U.S. Air Force UCAV pilots typically operate drones remotely, i.e., from the safety of the U.S. territory rather than directly on the battlefield, the incidence of PTSD among this population is significant, although lower than for military personnel returning from deployment (Chappelle et al. 2014). UCAV operators are not necessarily at increased risk of mental health problems compared to other soldiers, yet a higher proportion of drone pilots suffer from significant mental health-related functional impairments (Phillips et al. 2019).

Besides factors related to working hours and difficult positioning between military and civilian spheres, studies based on U.S. Air Force experience – arguably representing the largest population of combat UCAV operators – have demonstrated that the number of combat-related events in which UCAV operators have felt shared responsibility for the injury or death of bystanders was a significant predictor for the occurrence of PTSD symptoms (Chappelle et al. 2019). Especially in the context of drone swarms, some drones might succeed in crossing the defenses of the target. Thus, operators of defending drones or, for that matter, soldiers specifically tasked to defend against drones would likely be exposed to similar situations regarding potential harm to bystanders (in this case, the soldiers or civilians they were tasked to protect against the drone attack), with potentially similar outcomes on their mental health. Topping this increased exposure to risk factors, other elements are likely to enhance the psychological vulnerability of soldiers in anti-drone units. This is notably the case of high levels of stress, increased in the case of anti-drone units compared to regular troops, notably due to the fact that reaction time to a drone attack (time between the moment the drone is detected to the moment a response takes place) is shorter than for most conventional military reactions or the risks associated with disruptions of control of drone swarms.

Finally, in a battle context where drones would play a major role, anti-drone units might quickly become a priority target, thus generating more stress for their members. Therefore, it is critical for military forces wishing to develop anti-drone units to take these factors into consideration and to implement strong programs of mental health monitoring in order to identify potentially vulnerable soldiers and strong psychological and psycho-medical support to be deployed when the need arises.

Conclusion

Once confined to the armed forces of a few countries, drones are now widespread. With an increased range of missions, from surveillance and intelligence to combat, the capacity of drones for operating both in urban and non-urban environments, and their growing availability, the presence of drones in operative fields will only increase in the near future. Emerging technologies are making drones more and more reliable, and more and more difficult to counter.

As drones become more and more prevalent, nations increase their research efforts in the area. The motor of this game of hide and seek is technology. Yet, winning the arms race against drone developers is a never ending game. Indeed, for the few elements of which we still have control, the evolutions of technology are

likely to render current defenses massively obsolete. Yet, counter-UAV defense is not just about technology, but about people and organizations as well. Therefore, solutions are not to be found on the purely technological side, but have to include the human dimension. Counter-drone optimal strategies will rely on small, specialized units with a hybrid expertise in technology and combat skills, highly mobile, and able to rapidly respond to crisis. Such units should be able to quickly deploy on the battlefield. This would not only increase the efficiency of the response, but also allow major economies of scale – as deploying a specialized unit is more cost-sensitive than mobilizing a large, but unspecialized battalion. Being able to deploy anti-drone multi-modal responses and acquiring the human expertise to do so is critical for any country, independently of its size and its relative military strength. Smaller countries may even have more relative advantages doing so than the largest military forces.

What we have seen in the last decades is just the tip of the iceberg. We are at the dawn of technology-induced massive societal changes. Technology is going to massively alter warfare. AI and combat robotics are soon going to inhabit battlefields. In this context, anti-drone units might be our first glimpse of what future war will be like from an operational perspective. Therefore, anti-drone units might well become a template for future war forces' organization, training, and implementation.

Competing Interests

The author has no competing interests to declare.

Author Information

Matthieu J. Guitton is Secretary of the Faculty of Medicine and Full Professor at the Faculty of Medicine and at the Graduate School of International Studies of Université Laval (Quebec City, QC, Canada). He is Senior Researcher at the CERVO Brain Research Center (Quebec City, QC, Canada). A graduate from the University of Rouen and Université Pierre et Marie Curie – Paris VI, he obtained a PhD from the University of Montpellier (France) and was a Koshland Scholar/Postdoctoral Fellow of Excellence at the Weizmann Institute of Science (Rehovot, Israel). He is a Fellow of the Royal Anthropological Institute. He is the Editor-in-Chief of Computers in Human Behavior *and of* Computers in Human Behavior Reports*, and he serves on several other editorial boards, such as* Current Opinion in Behavioral Sciences.

References

Arquilla, J., & **Ronfeldt, D. F.** (2000). *Swarming and the Future of Conflict*. Santa Monica: RAND Corporation.

Beni, G. (2005). From Swarm Intelligence to Swarm Robotics. In E. Şahin & W. M. Spears (Eds.), *Swarm Robotics* (pp. 1–9). Berlin, Heidelberg: Springer. DOI: https://doi.org/10.1007/978-3-540-30552-1_1

Boyle, M. J. (2015). The Race for Drones. *Orbis*, *59*(1), 76–94. DOI: https://doi.org/10.1016/j.orbis.2014.11.007

Brambilla, M., Ferrante, E., Birattari, M., & **Dorigo, M.** (2013). Swarm robotics: A review from the swarm engineering perspective. *Swarm Intelligence*, *7*(1), 1–41. DOI: https://doi.org/10.1007/s11721-012-0075-2

Brynjolfsson, E., & **McAfee, A.** (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York City: W.W. Norton and Company.

Chappelle, W., Goodman, T., Reardon, L., & **Prince, L.** (2019). Combat and operational risk factors for post-traumatic stress disorder symptom criteria among United States air force remotely piloted aircraft "Drone" warfighters. *Journal of Anxiety Disorders*, *62*, 86–93. DOI: https://doi.org/10.1016/j.janxdis.2019.01.003

Chappelle, W., Goodman, T., Reardon, L., & **Thompson, W.** (2014). An analysis of post-traumatic stress symptoms in United States Air Force drone operators. *Journal of Anxiety Disorders*, *28*(5), 480–487. DOI: https://doi.org/10.1016/j.janxdis.2014.05.003

Coffey, V. (2014). High-Energy Lasers: New Advances in Defense Applications. *Optics and Photonics News*, *25*(10), 28–35. DOI: https://doi.org/10.1364/OPN.25.10.000028

Coops, N. C., Goodbody, T. R. H., & **Cao, L.** (2019). Four steps to extend drone use in research. *Nature*, *572*(7770), 433–435. DOI: https://doi.org/10.1038/d41586-019-02474-y

Dey, V., Pudi, V., Chattopadhyay, A., & **Elovici, Y.** (2018, January). Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. *Paper presented at the 2018 31st International Conference on VLSI Design and the 2018 17th International Conference on Embedded Systems (VLSID)*, Pune, India. DOI: https://doi.org/10.1109/VLSID.2018.97

Garattoni, L., & **Birattari, M.** (2018). Autonomous task sequencing in a robot swarm. *Science Robotics*, *3*(20), eaat0430. DOI: https://doi.org/10.1126/scirobotics.aat0430

Golson, J. (2014, September 16). A Military-Grade Drone That Can Be Printed Anywhere. *Wired*. Retrieved from https://www.wired.com/2014/09/military-grade-drone-can-printed-anywhere

Guitton, M. J. (2019). Manipulation through Online Sexual Behavior: Exemplifying the Importance of Human Factor in Intelligence and Counterintelligence in the Big Data Era. *The International Journal of Intelligence, Security, and Public Affairs*, *21*(2), 117–142. DOI: https://doi.org/10.1080/23800992.2019.1649122

Guitton, M. J. (2020). Using Biotechnology to Build a Workforce for Intelligence and Counterintelligence. *International Journal of Intelligence and CounterIntelligence*, *33*(1), 119–134. DOI: https://doi.org/10.1080/08850607.2019.1676038

Hambling, D. (2016, November 4). Drones Fight Back Against Laser Weapons. *Popular Science*. Retrieved from https://www.popsci.com/laser-guns-are-targeting-uavs-but-drones-are-fighting-back

Hammes, T. X. (2019). Defending Europe: How Converging Technology Strengthens Small Powers. *Scandinavian Journal of Military Studies*, *2*(1), 20–29. DOI: https://doi.org/10.31374/sjms.24

He, D., Chan, S., & **Guizani, M.** (2017). Drone-Assisted Public Safety Networks: The Security Aspect. *IEEE Communications Magazine*, *55*(8), 218–224. DOI: https://doi.org/10.1109/MCOM.2017.1600799CM

Hubbard, B., Karasz, P., & **Reed, S.** (2019, September 14). Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. *The New York Times*. Retrieved from https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & **Humphreys, T. E.** (2014). Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics*, *31*(4), 617–636. DOI: https://doi.org/10.1002/rob.21513

Li, K. W., Jia, H., Peng, L., & **Gan, L.** (2019). Line-of-sight in Operating a Small Unmanned Aerial Vehicle: How Far Can a Quadcopter Fly in Line-of-sight. *Applied Ergonomics*, *81*, 102898. DOI: https://doi.org/10.1016/j.apergo.2019.102898

Lucas, G. R. (2014). Automated Warfare. *Stanford Law Policy Review*, *25*(2), 317–340.

Phillips, A., Sherwood, D., Greenberg, N., & **Jones, N.** (2019). Occupational Stress in Remotely Piloted Aircraft System Operators. *Occupational Medicine*, *69*(4), 244–250. DOI: https://doi.org/10.1093/occmed/kqz054

Rascon, C., Ruiz-Espitia, O., & **Martinez-Carranza, J.** (2019). On the Use of AIRA-UAS Corpus to Evaluate Audio Processing Algorithms in Unmanned Aerial Systems. *Sensors*, *19*(18), e3902. DOI: https://doi.org/10.3390/s19183902

Rotolo, D., Hicks, D., & **Martin, B. R.** (2015). What is an emerging technology? *Research Policy*, *44*(10), 1827–1843. DOI: https://doi.org/10.1016/j.respol.2015.06.006

Said, S., Malsin, J., & **Donati, J.** (2019, September 14). U.S. Blames Iran for Attack on Saudi Oil Facilities. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/drone-strikes-spark-fires-at-saudi-oil-facilities-11568443375

Schwab, K. (2017). *The Fourth Industrial Revolution*. New York City: Crown Publishing Group.

Sharkey, N. (2011). The Automation and Proliferation of Military Drones and the Protection of Civilians. *Law, Innovation and Technology*, *3*(2), 229–240. DOI: https://doi.org/10.5235/175799611798204914

Tsykunov, E., Agishev, R., Ibrahimov, R., Labazanova, L., Tleugazy, A., & **Tsetserukou, D.** (2019). SwarmTouch: Guiding a Swarm of Micro-Quadrotors with Impedance Control Using a Wearable Tactile Interface. *IEEE Transactions on Haptics*, *12*(3), 363–374. DOI: https://doi.org/10.1109/TOH.2019.2927338

Voosen, P. (2019). Satellites see hurricane winds despite military signal tweaks. *Science*, *364*(6445), 1019. DOI: https://doi.org/10.1126/science.364.6445.1019

How to cite this article: Guitton, M. J. (2021). Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms. *Scandinavian Journal of Military Studies,* 4(1), pp. 26–36. DOI: https://doi.org/10.31374/sjms.53

Submitted: 28 October 2019 **Accepted:** 30 September 2020 **Published:** 13 January 2021

SCANDINAVIAN MILITARY STUDIES

Scandinavian Journal of Military Studies is a peer-reviewed open access journal published by Scandinavian Military Studies.

OPEN ACCESS