Abstract: The most popular drone countermeasure techniques are described. Results of an analysis of literature sources show that contemporary technical solutions are focused on neutralization of drones either by electronic means (jamming) or by net-capturing systems, can be effective when the drone attack is executed by a limited number of drones. It is noted that manufacturers of countermeasure devices focus on the counteraction to civil threats (snooping, tracking by criminals). These means can be useful against amateurs or badly prepared terrorists because the available solutions do not take into consideration the possibility that the attack can rely on the coordinated action of a group of drones (a swarm).

In this paper, it is pointed out that development of unmanned technologies as well as countermeasures against these technologies, indicates the existence of an arms race directed towards achieving an advantage in this new kind of military action. A special feature of strategy for future combat missions will be the need for machines to fight against machines, not humans directly.

1 Introduction

There are many justifiable reasons for dealing with the topic of the inevitability of machine wars. The most important is the development of the so called Internet of Things (IoT). From that point of view even an autonomous vacuum cleaner (cleaning robot) can be regarded as a sensor in a security system and – if hacked – act like an enemy who spies. Which possibility is being executed in your house? To answer this question, one has to use a machine capable of controlling the vacuum cleaner. Because a human (housekeeper) does not have the tools to do it himself, only...
a machine can determine if the system is safe. But who checks the machine which checks the vacuum cleaner? – only another machine can … and a virtual circle is formed, so the self-propelled technology of IoT is also formed. In this paper, a view is presented regarding the most visible area of developing machine war technologies, i.e. Unmanned Aerial Vehicles (UAVs, drones) and the countermeasures against them. The reasons are:

a) In media reports, one can find information about the wars of drones [1].

b) There is information leading to the belief that the reason for the explosion at the Ukrainian army depot in March 2017 [2, 3] was caused by a drone attack, using a thermite grenade ZMG-1 [4]. This explanation is possible not only due to previous similar cases in Ukraine, which can be regarded as non-objective, but also upon the basis of many examples, posted by terrorists on the internet, of projectiles being released from drones, especially the use of a drone during an attack in 2017 on a Syrian army depot in Deir Ez-Zor [5].

c) The market for commercial drone countermeasures is well established and is growing because there is rapidly increasing evidence of their illegal use [6]. The more spectacular cases are:

- 2016: – violation of the protected zone of the Polish Prime Minister’s Office by a drone operated by a Russian (September 26, Warsaw) [7],
- 2015: – the first documented attack of the destruction (spray paint) of a billboard using a drone adapted by a perpetrator of graffiti painting [8],
  – a drone was crashed into the seating area during the U.S. Open Tennis Championships [8],
  – a drone landing on the White House lawn [9, 10],
  – flights of unidentified drones over critical national infrastructure facilities, like nuclear power stations and a submarine naval base in France [10, 11],
  – Enrique Iglesias hurt his hand when trying to catch a drone during one of his concerts [8],
  – a drone with traces of radioactive material was landed on the roof of a government building in Japan, by opponents of nuclear policy, [8],
  – use of drones for hacking WiFi printers [8],
- 2014: – use of drones for smuggling drugs into prisons in the USA [8],
  – a drone carrying a national flag appeared during a EURO 2016 qualifying match between Albania and Serbia, causing conflict between the players [8],
- 2013: – a drone was crashed 2 m from the German Chancellor Angela Merkel during her election meeting in Dresden, Germany [11].

As an answer to the large amount of illegal drone usage, one can point to research projects for ensuring the safety of e.g. air transportation [12], seminars [13, 14], as well as international fairs in Nuremberg, Germany in March 2018 [15], dedicated, among others, to unmanned countermeasure technologies.

The proposition of this paper is that preparation for a machine war is becoming an area for developing tools for a drone war. The reasons for this assessment are: a well established scientific record (see Section 1a), an easy to achieve and maintain technology gap between the top players in the world’s drone industry and the rest (see Sections 1b-1d), a continually growing number of commercial drone applications supplemented by an almost complete lack of limitation in size and possibilities, which seems to be a very useful test-field for the arms industry e.g. as dual use technologies [16], (see Sections 1e-1g) and finally, a reduction of the human factor and application of new technologies (3D printing) leading to significant reductions in manufacturing costs compared to pilot-onboard aircraft (see Section 1h), i.e.:

a) **Unmanned technologies and tools for their defeat have been known for at least 50-70 years.** The idea for launching a projectile containing a web (see Section 3.2.2) towards a flying object (a plane) was presented in the 1940s [17]. The required tools for the effective use of drones, like wireless guiding of unmanned objects, as well as jamming of communication channels with these objects (see Section 3.2.1) were developing abroad, e.g. in the case of cruise rockets, at least as early as the 1950s [18]. The application of optical cameras for guiding rockets has been known at least as early as the 1960s [19]. At the same time, concepts of drones known as VTOL (Vertical Take-Off and Landing) were developed, – as were concepts of supersonic ones using rocket propulsion systems [20]. On the other hand, also in the 1960s, research on countermeasures for defeating unmanned systems (rockets) using laser techniques, was started in the U.S. and China [21].
Abroad, the military applications of drones were being taken into consideration at the end of the 1970s [22].

Previous work can be confirmed by a patent [23], published in 1979 but filed in 1972, citing American and British patents from the 1960s. The application of drones in observation missions was analyzed in France in the middle of 1980s [24].

b) The definition of the word „drone” solely as a flying object is insufficient, including an assessment of the tactical possibilities of such platforms. Expressions such as “hovering” and “submersible” drones [25-27], can be regarded as short hand for unmanned objects, but for (flying) drones capable of moving in water, so called hybrid drones, it is not a question of simplifying the vocabulary. It is a very realistic component of revolutionary changes in military strategy and terrorist threats. At the upper end we are talking about distances expressed in kilometers for the range of effective defense, but it is enough for just one open body of water (reservoir, lake) close to a protected facility, to make the monitoring of airspace for drone intruders, ineffective. A drone intruder can arrive in a protected area and fly up into the air near the facility, to execute an attack .... Fantasy – from the point of view of „swimming pool” technologies [28] – certainly, but taking into consideration the possibilities of hybrid drones like CRACUNS (Corrosion Resistant Aerial Covert Unnamed Nautical System) [29, 30] and assuming that the most advanced technologies have not been disclosed, one can regard hybrid drones as a real possibility for use as combat platforms.

The concept of hybrid drones is not limited to hovering drones, but encompasses far reaching changes in the future, like the car-drone hybrid called Pop.Up [31]), or an integration of different power sources, enabling e.g. 2.5 h flights with 10 kg payloads for distances of up to 160 km, as is the case of a drone supplied with both, electric batteries and a gasoline engine [32].

c) One has to take into account the existence of a gap between technologies of the top players in the world and the rest, not only in the field of utilization of drones, but also in the field of ensuring their safe use. This conclusion can be drawn by analysing the parameters of radars and telecommunication technologies developed in average countries and those of the top players in the drone industry. This relationship is based on the observation that full control is the basic requirement for proper operation in unmanned technologies. One can also see differences in the state of drone technology development at other levels e.g. design in stealth technology, among others [33, 34].

A special type of threat arising from externally procured drones is the possibility of them being used for spying. At the end of 2017, the Department of Homeland Security of the USA informed about such a situation existing regarding the commercial drones and software of a Chinese company, D.J.I. (Da Jiang Innovations Science and Technology Company) [35]. This conflict between the giants is still pending and has had repercussions for smaller players, like Poland. In response to an objection about the procurement of D.J.I. drones by the Polish police, a statement was issued [36] which said that the Polish police understands that the procurement does not affect the security of police operations. The supporting information was that D.J.I.’s drones are in service in foreign police forces, e.g. in 2015, D.J.I. drones were tested by UK police forces for suitability in shooting scenes and searching for missing persons [37]. Accusations by U.S. officials met with firm opposition from D.J.I., however questions remain, like: - is the purchase of foreign, commercial drones by state services safe? - what tools are necessary to confirm the safety of purchased foreign technologies which are much more advanced than domestic ones?

d) One has to reckon with the existence of the technology gap, counted in the hundreds or thousands of drones, between the tactical possibilities of troops equipped by the top players and the others. According to initial plans, from the start of activities of the 12th Unit of Unmanned Aerial Vehicles in Mirosławiec, Poland [38], in 2016, the Unit was expected to have up to 45 drones [39]. Of course, there are many more drones in the Czech and Polish forces, it being fairly possible that the total number of drones is hundreds of times more. Having hundreds of drones is a prerequisite of the contemporary battlefield. The existence of the technology gap is obvious when comparing the funding of drone-related technologies in the U.S. to those of Poland or the Czech Republic. The U.S. Department of Defense allocated approximately 4.457 billion USD for drone-related tasks in the proposed budget for Fiscal Year 2017 [40] and, comparatively:

- according to plans from 2015 [41], the Polish military drones modernization program for 2013-2022
was set at over 37 million USD (apart from another program valued at least “several billion zloty”) with the total number of drones planned at 350,
- the Czech Army has plans [42] to purchase UAVs systems for about 46.4 million USD until 2025, and within this task, in 2019 it plan to purchase a system based on ScanEagle drones for about 9.3 million USD. Finally, one has to agree that leading countries are far ahead, i.e.:
- in 2017 [43], there is talk about the Russian Federation armed forces fleet having about 1800 new drones capable of conducting missions with ranges up to 500 km, and moreover, later on there is work on platforms with ranges up to 3000 km,
- U.S. armed forces had almost 11000 drones in 2013 [44].

Poland can obtain a much larger and faster strategic potential in the range of loitering munitions. The technologies of these are well known throughout the world [45], e.g. drone Harop was presented at Air Fair 2017 in Bydgoszcz, Poland [46]. In 2017, the Polish army and WB Electronics (WB Group) signed a contract for the supply of 1000 Warmate loitering munitions. Warmate [47] is in fact a projectile which can be regarded as a special (singe use only) kind of drone. Warmate can be used on its own or as an armament of a typical drone, e.g. Manta (WB Electronics) [48]. The number of Warmate drones has to be assessed with respect to a statement presented in [49], which states that the best strategy for this kind of loitering munition is through massive attack using a swarm. The concept of a swarm was put forward in [50] with respect to a swarm of 100 drones. However, the necessity to incapacitate, preferably simultaneously, a swarm of 100 drone-intruders is not a question for the future. In 2016, such a swarm size was tested in the U.S. [51]. Today’s requirement for an effective defense of particularly important strategic objects against swarm attacks, is more realistic with regard to swarms of at least 500 drones. In 2016, a swarm of 500 drones, each of 280 g, operated by one pilot with a laptop, was used for a light show by Intel Corporation [52]. The simultaneous use of 1000 Warmates is a significant achievement but it would be necessary to use swarms consisting of at least 100 drones because a smaller number may be ineffective. … thus 1000 drones is sufficient for 10 attacks.

From the point of view of demonstrating the technology gap, one has to take dimensions into consideration. Although much larger drones are used as loitering ammunition, e.g. the British drone Fire Shadow is 4 m long where as the Warmate is only 1.1 m long, the gap is visible when these are compared with the Perdix drone, which can fit in the palm of a hand. This is why the release of 103 Perdix was carried out by 3 F/A-18 Super Hornets [51]. Another aspect of the technological advantage of Perdix, connected with the advantage in dimensions, is presented in Section 1h.

e) A little bit of an exaggeration, but it is better to be safe than sorry …., one has to reckon that in the foreseeable future, drones will be almost as commonly-used as cars. In 2015, the value of the global commercial drone market was rated as 127 billion USD [53]. Of course, the Polish market is much smaller, but it is growing significantly, from 164 million PLN in 2015 to 201.31 million PLN in 2016 [54a]. The Americans estimate that the number of drone hobbyists (each of them has at least one drone weighing up to 28 kg) will grow in the U.S. from 1.1 million in 2016 [51] to 3.5-7 million approaching 2021 [6, 51]. In the same period in the U.S., the number of commercial drone flights will grow from 42,000 to 42,000 per year [8]. Reports of the possibilities, conditions and perspectives of the development of this industry have been prepared by, among others: the European Commission [55], European states [56], the U.S. Army [57, 58] and other international organizations [53]. According to [54b], analysis can be found that closer to 2025 in the U.S., on-board piloted aircraft would be regarded as having no future and that the introduction of unmanned air transportation, and passenger aviation, could possibly start.

Domestic interest in military drones is very significant, so further development is assured. This regards not only military applications [59, 60]. Their use in agriculture is quite new but well established with broad perspectives for the utilization of unmanned technologies. Technologies for ground, autonomous (driverless) agriculture machinery [61] are currently available in Poland [62]. According to the EU Communication Research and Development Information Service (CORDIS), in the years 2010-2014, systems were tested combining drones and ground robots for agricultural work, within a projected worth of approximately 8.9 million EUR [63]. The
most developed unmanned technologies concern the so-called agriculture drones or ‘ag-drones’, dedicated for precision agriculture [64, 65]. From the point of view of potential threats arising from the use of an agriculture drone with the aim of causing a dangerous situation to the public, one has to cite:

- the implementing of planned observation activities during a flight executed, usually at an altitude up to about 100 m, at a distance from the operator of up to 2 km, over an area of up to 30-200 ha (Parrot Bluegrass [66], eBee SQ [67]), with a duration of about 50 min (AgDrone [63], AgEagle [68], PrecisionHawk Lancaster 5 [63], Quantix™ [69]),
- the monitoring of a given area using different sensors e.g. optical, thermal (InfraRed), multispectral, hiper spectral, as well as LIDAR (Light Detection and Ranging) [63],
- the rapid spreading of particulate materials (e.g. pesticides and fertilizers) over a given area, although this feature is already used for testing drones as tear gas carriers for riot control purposes [70],
- hand take-off, i.e. without a launcher (AgEagle [68], Quantix™ [69]),
- the collection and storage of data in computing clouds (Parrot Bluegrass, AIRINOV First+ software [66]),
- the control by mobile applications such as Android and iOS (Parrot Bluegrass [66]),
- the availability of swarm technologies (see Section 1d) for agricultural ground platforms [61].

f) Drones can be used in any form of attack or intelligence gathering effort, because both, dimensions and field of application seem to be limited only by human ingenuity. The contemporary measure of the lower size limit is a human fingertip. Dimensions of the smallest commercial VTOL are 3 cm × 3 cm × 2 cm [71]. Drones which fit in the palm of a hand are called mini drones and have very useful features, e.g. drone DJI Mavic Pro – is equipped with GPS (Global Positioning System), GLONASS (Global Navigation Satellite System), obstacle avoidance system and 4K camera, enabling a flight lasting up to 27 min up to a distance of 7 km [72]. A practical example of the smallest operational drone (length 10 cm, width 2.5 cm) is the PD-100 Black Hornet Nano (a VTOL produced by Prox Dynamics AS [73]), in use by the armed forces of Norway, Germany, Australia and the U.S. and formerly by the British Army (over 300 drones in 2013, but retired in 2017) [74].

At the other end of the scale, in terms of size and operational area - are observation and telecommunication unmanned platforms called HAPS (High Altitude Pseudo-Satellites). According to HAPS designers these will be powered by solar energy, the duration of the mission being counted in months and operating at a height of 20 km, like Thales Alenia Space’s Stratobus, in 2021 [75]. Other technical boundaries for the Thales Alenia Space’s Stratobus are: the capability of carrying a 250 kg load, an observation area up to 500 km, and a maximum length of 100 m for the commercial version of [76].

Also, the available operational distances between a drone and its operator seem to be unlimited. A test has shown than the GUA V7 drone [77] can be controlled from a distance of 7500 km using a personal computer equipped with the mobile network LTE (Long Term Evolution) [10].

g) Development of unmanned technologies is and will continue to be stimulated by very dynamic grow of global demand, created by commercial applications, so this development cannot be stopped or abandoned. This conclusion comes from the general rule that the development of contemporary technologies depends directly on the size of capital invested in them. The most important factors which show that the size of the drone market will be driven by commonly available solutions are: a limited number of producers and users of military drones (high quality and top secret technologies necessary) and unlimited possible applications of commercial drones and many users all over the world, as was shown by the example of precision agriculture in Section 1e.

Of course, funds for military applications are much bigger even in medium-size European drone manufacturers. In addition to the loitering munition Warmate in Poland and plans of the Czech Army, mentioned in Section 1d, there are a few modernization programs in the Polish Army directed towards the procurement of drones. New, own military projects can be confirmed by the awarded topics in a competition „Innowacje dla Sił Zbrojnych RP”, (eng. trans. Innovations for Polish Armed Forces), in 2017, which shows strong support from the Polish Ministry of Defense in the development of unmanned technologies [78], e.g:
1) a stratospheric platform as an element of a reconnaissance and protection system for the Polish Armed
Forces and the infrastructure,
2) a miniature supercavitating torpedo with rocket propulsion for manned and unmanned systems for naval combat.

On the other hand, funds for commercial R&D cannot be overlooked and it has to be underlined that significant support for national unmanned technologies is being given within the framework of:
1) Competition results of 4/1.2/2016/POIR, within the Framework of the sectoral Program INNOSBZ, funded under Measure 1.2 „Sectoral Programs R&D” POIR 2014-2020 implemented by National Centre for Research and Development (pl. NCBiR) for Priority I POIR 2014-2020 [79], according to which, with total costs of the project worth 61.6 million PLN, the NCBiR recommended that the amount of funding is 42 million PLN. Among the winning projects for special attention, were:
   – Industrial Research Institute for Automation and Measures (PIAP): 1) Development of a highly mobile unmanned hybrid platform for rapid response tasks. 2) A system of smart, mobile shooting targets with advanced systems for hit detection and modern composite protective armour MOBITARGET. 3) A mobile toolbox for supporting forensic procedures.
2) Another example contributing to the development of unmanned technologies in Poland (enabling the acquisition of experience in conducting environmental research in the use of drones) is a project started in 2017 and co-financed by the National Science Centre (pl. NCN) of 0.5 million PLN [80].

![Figure 1. VTOL with structural elements printed using 3D printer (fot. Rafał Szymaniuk, WAT)](image)

h) **Unmanned technologies allow a reduction of the so called human factor, which is crucial in providing a constant readiness for action.** At the moment, the presence of many people working in the manufacture and use of drones is inevitable. However, in the future, in the same way as happens in car factories, automated production lines can be the most effective and cheapest way for manufacturing drones, especially in large scale production. Meanwhile, production lines and test sites of drones operated by personnel at Flytronic company, can be viewed on the internet [81].

Logistics is one of most important factors indicating that we have to be prepared for machine wars. Unmanned platforms are cheaper to produce not only because of lower costs of materials but also because of more efficient and easier manufacture and assembly of parts. Production of structural elements using 3D printers is generally known, as shown on websites [82, 83], research work [84, 85], as well as examples of applications. Structural elements of Perdix, mentioned in Section 1d, as well as of drones of the Polish company Harbot [86] and a VTOL designed and manufactured by the Science Club at the Military Technical Academy (pl. WAT) (Fig. 1), were produced using 3D printing technology.

From the point of view of terrorist threats, the possibility of 3D printing of plastic drone elements is a threat, however this possibility opens another area in which the competition (war) of machines can decide the outcome.
of a military action, especially when faster printing can result in faster combat readiness or a faster restoration of combat operational capability.

The above considerations show that drones are no longer one of many components of an armed force’s structure known from previous conflicts. Drones have to be regarded as the testbed for the foundation of an army of the future, i.e., an army of machines. If there is an army of machines, suitable means for defeating this are necessary. The aim of this paper is to present the most important drone countermeasures, because their existence and development clearly indicate that the arms race for gaining an advantage in machine wars has already started.

2. Drones in Poland and their countermeasures

Nowadays, despite the above mentioned technology gap, direct contact with drone technologies in countries like Poland is quite widespread. Just in the year 2017, between March and November, it is worth mentioning the following 11 public events held in Poland:

a) “Robomaticon 2017” Warszawa 04.03.2017 [87],
c) Drone Race Gdynia, the FAI Drone Racing World Cup 2017. Gdynia 13-14.05.2017 [89],
d) “Air Fair 2017”, Bydgoszcz 26-27.05.2017 [46],
e) “Pro-defence” Fairs, Ostróda 01-04.06.2017 [90],
f) “Parada Robotów Droniada”, Kraków 16-18.06.2017 [91],
g) “Air Show”, Radom 27.08.2017 [92],
h) “International Defence Industry Exhibition” (pl. MSPO), Kielce 05-08.09.2017 [93],
j) “DroneTech 2nd World Meeting Torun 2017” Fair, Toruń 5-6.11.2017 [95],
k) “Warsaw Industry Week” Fair, Nadarzyn 14-16.11.2017 [96].

At the last of these (“Warsaw Industry Week”), four national entities – 2 research centers (WAT and the Air Force Institute of Technology (pl. ITWL)) and 2 private entities (Dron House and Harbot) – exhibited their own drones. The scope of the drones varied from experimental [97] (Figure 1), a drone based on a model aircraft [86], to commercial drones like Bielik [98] and finally, to military drones like Rybitwa (eng. trans. Tern) (WAT) [99] (Fig. 2a) and AtraxM (ITWL) [100] (Fig. 2b).

In Poland, development of unmanned technologies has been clearly visible for many years. Milestones achieved up to 2014 like the Proteus system (3 ground autonomous vehicles cooperating with a drone) and the ILX-27 drone are described in [101], among others. Nowadays, in Poland there are not only drone producers but also training centres located at dedicated military bases, such as Mirosławiec (see Section 1d) as well as at military academies, e.g. the Polish Naval Academy [102] and the Polish Air Force Academy [103]. However, defense systems against drones are still a novelty, and are trying to gather interest, as indicated by:

a) “Pro Defense 2017” Fairs, Ostróda 01-04.06.2017, where there was presented:
   – an exhibition of drone command, detection and neutralisation [90],
   – Electromagnetic Lance [104, 105] by Military Electronic Works S.A., which will be the governing element in a mobile system for the disruption of drones. This system is being developed by some of the companies in the Polish Armament Group (led by Wojskowe Zakłady Uzbrojenia in Grudziądz, Poland). Lance is intended to jam drone communication bands in the 100-6000 MHz (25 W) range with an effective distance up to 900 m,

b) “Eastern Conference” and Border Protection Fair “BORDERS” Event, Lublin 25-26.10.2017, there was presented [94]:
   – drone Vector V8, of the Spartaaq company [106], intended for the catching of drones with a net,
   – system “Jastrząb” (eng. Hawk) [107], of Hertz Systems Ltd. Sp. z o. o., which includes, among others: radar with camera (effective up to 5 km) and a neutralizer effective up to 1 km,
   – non-kinetic radio-frequency anti-drone gun of the DPIDEA company,
c) awards in a competition „Innovations for Polish Armed Forces” (pl. „Innowacje dla Sił Zbrojnych RP”), in 2017, for the following projects [78]:
- The concept of portable and mobile electromagnetic weapons utilising advanced superconducting materials and strong impulse magnetic fields (50T) for the Army and the Navy.
- SafeSky - a multisensor system for drone detection.
- Hand-held carbine for non-kinetic overpowering of unmanned aircraft.

Figure 2. Polish military drones: a) Rybitwa (eng. trans. Tern) (fot. Rafał Szymaniuk, WAT); b) AtraxM (fot. ITWL)

3. Machines fighting machines

3.1. Signaling zone violation

The first stage of drone countermeasure is detection, followed by tracking. There are patents on drone-intruder tracking, with one of the newest using its own drone, [108]. Detection is possible when one can recognize [8]:

a) movement, which can be ascertained using radar systems and optical devices (direct sight by a human, as well as visible light and infrared image cameras and binoculars). The disadvantages [109] of these techniques are: a rather short range of protected area for the optical techniques (a few hundred meters) and difficulties with detection of drones with poor thermal signatures e.g. electric propulsion. Radar is best, although radars are not usually designed for distinguishing between a small drone and a bird.

b) detection of communication bands, which can be ascertained using radio systems. An important advantage of systems monitoring radio frequency is the possibility of determining the GPS position not only of the drone-intruder but also of its operator [109]. Another goal of such systems is the possibility of far-reaching miniaturization, the transponder “Wingman” WM1000 [110] being an example of a hand-held detection system useful, for example, to the police.

A disadvantage of this kind of detection is blindness when there is radio silence, e.g. when the drone-intruder is operating on the basis of pre-programmed commands, without direct contact with its operator.

c) sounds generated by a drone, which can be determined using acoustic systems. Acoustic verification, utilising sound signature databases, seems to be difficult in urban areas, where many everyday noises can mask the presence of sounds coming from a drone. A big challenge is the identification of known drones with modified i.e. unknown sound signatures, e.g. those using a non-standard propelling system. Also, effective sound detection distances are limited [109, 111]. However, the fundamentals of acoustic detection technology dates from the 1980s [112], so it cannot be excluded that much more advanced acoustic systems are available which can overcome such restrictions.
3.2. Destruction and defeat

Termination of the operational activity of a drone-intruder can be carried out in several ways, for instance by:

a) overpowering (cutting off operator access to the drone or hacking into the on-board computer [113]),
b) interception (physically catching the drone),
c) destruction (physical disintegration).

Each of these has pros and cons. One can find analysis in the literature focused on the comparison of some of them, like [114], indicating that the preferred method is net-throwers (a very popular method of interception) compared to jamming (the most popular method of overpowering). Similarly, one can compare destruction techniques like traditional barreled vs. laser weapons [114, 115] and come to the conclusion that lasers are better. However, in general, in contrast to kinetic guns, the effectiveness of laser systems is lowered e.g. by air humidity and the presence of clouds [51]. On the other hand, energetic munitions can be dangerous to one’s own resources and troops, should the shooter miss the drone. Also, hacking into the on-board computer can bring differing results. It can lead to an immediate landing, a change in the flight course or the forcing of the drone to return to its base.

The best solution seems to be a combination of various countermeasures, i.e. possessing only one means of defense is not the solution. Clear confirmation for such thinking can found in a statement by the technical director of the Russian company Aerokon, which states that jammers are effective tools only for drones up to 200 kg [5]. The conclusion that multi-tool solutions are the future of anti-drone systems, together with observations that, usually, a human can operate one tool whereas a computerized system (machine) can operate many tools simultaneously. Only a machine with as large a number of countermeasures as possible can defend itself successfully against a drone attack.

Undoubtedly, it is wrong to limit an analysis to commonly known solutions. As weapons are not the subject of this paper, some possible solutions are omitted, but one has to remember that weapons designed for destroying or jamming electronic devices (among others, drones) area part of a huge family of so-called non-lethal weapons [116]. So, in general, the well known anti-drone techniques presented below are not the only possible solutions.

3.2.1. Overpowering by jamming communication and navigation channels

Jammers operate at the same channels and bands as are used for communication between an operator and a drone [117-119], i.e.:

a) military drones, radio frequencies (Band C – obsolete designation is NATO C-Band – 500-1000 MHz) and satellite communication (part of frequency Band J – obsolete designation is Band Ku – 10.95-14.5 GHz). Jamming of Band C has been well known since the 1980s [120].
b) commercial drones, bands for drones with a range of 3-5 km use 2.4 GHz WIFI, GPS L1, and 5.8 GHz; whereas up to 1 km - 433 MHz, 928 MHz, and GPS are used.

Jamming of communication channels between an operator and the drone have been known for many years, e.g. the Silent Archer C-UAS system was brought into service in 2005 [51]. Recently, the Russian company Kalashnikov started to produce a jammer Stupor, which operates in the GPS and WiFi bands, and is being tested in Syria [5]. The leaders of the market in anti-drone jammers and systems which combine jammers with different techniques, like detection (see Section 3.1), are, in alphabetical order: Aaronia AG (AARTOS DDS) [121], Battelle (DroneDefender®) [122], Blighter® together with Liteye Systems (AUDS Anit-UAV Defense System) [123], CTS Technology (CTS Drone Jammer [124], CUAS and ADIS [125]), Dedrone (DroneTracker Software) [126], Department 13 (D13’s MESMER® Counter Drone System) [127], DeTect (DroneWatcher APP, DroneWatcher RF, HARRIER DSR) [128], Drone Defence (Dynopis E1000MP, SkyFence) [129], DroneShield (DroneGun Tactical, DroneGun MKII, DroneSentinel, and DroneSentry) [130], MCTech (MC-Horizon) [131], Prime Consulting and Technologies (Grok mobile Gun, as well as Jammers: GROK, Meritis, and Phantom) [113], Sensofusion (Airfence) [132].

3.2.2. Interception

Nets can be fired from the ground, as well as fired or towed by a flying drone. As can be seen from online shops’
offers [133, 134], commercial technologies based on net-throwing systems seem to be useful for individual defense, at a range of about 15 m and – beside drones – against criminals and animals (like attack dogs). However, there are available professional systems proposed for use in maritime conditions, like Net Gun X1 [135]. Knowledge of drone interception using nets can be found in patents, recently published ones are [136-138] among others.

Leading manufacturers of anti-drone net systems are, in alphabetical order: DroneDefence (Net Gun X1) [139], MALOU Tech (MPI 200) [140], OpenWorks Engineering (SkyWall100, SkyWall300) [141], and Theiss UAV Solutions (Excipio Aerial Netting System) [142].

**Birds of Prey** are trained by the Danish police [143] and the Air Force in France [144], to catch drones. Life Cycle Analysis [6] has shown that the costs of implementation and maintenance of a defence system based on these birds is about $157,000 USD, taking into consideration the service life of a bird being about 40 years. Development of this technique is limited by these high costs, because the very likely premature loss of a fully trained bird will have a significant effect on the functioning of the system. Also, the application of this method seems to be limited to small VTOLs and to average life spans (non-combat and non-terrorists attacks), so for defense against other kinds of drones, other techniques are necessary.

Company Guard from Above [145] provides a drone interception using birds of prey.

### 3.2.3. Destruction by direct energy weapons

In less than 10 years, the USA plans to introduce into service **Directed Energy Weapon (DEW)** systems capable of destroying a swarm of drones. The most desirable features, which can be realized solely by machines, *ipso facto* leading to machine wars, are [51]:

a) **scalable DEW**, *i.e.* adjusting the amount of energy emitted for each shot, with respect to distance and the structural material of a target,

b) **fused DEW C2 system**, *i.e.* transferring data collected in a DEW system to other battlefield systems, with the aim of developing an optimal defense strategy,

c) **open DEW system**, *i.e.* connecting new devices, like radar, to a DEW system’s architecture can be carried out easily and automatically.

**Laser weapon:**

In 2015, in a public demonstration, Boeing [146] tested the infrared 200 W Compact Laser Weapon System designed for destroying drones. In static conditions, this laser burnt a hole in the drone’s composite fuselage in 2 s. It is an improved (much smaller) and much more convenient for transportation version (only two people are necessary) of the High Energy Laser Mobile Demonstrator (**HEL MD**), presented in 2014. The U.S. 30 kW laser system, ready for combat use in 2014 and capable of destroying a swarm of drones is the chemical laser Kratos Defense and Security Solutions AN/SEQ (XN-1) Laser Weapon System (**LaWs**) [21]. Other U.S. land and sea mobile lasers tested as countermeasures against single drones and swarms are the High Energy Laser Mobile Test Truck (**HELMTT**) and the Mobile Expeditionary High Energy Laser (**MEHEL**) [51].

Also in 2015, MBDA Deutschland [11] conducted a successful test, shooting down a small drone at a range of 500 m, a few seconds after its take off. Ultimately, this system has to cover 360°, has to be effective at distances up to 3 km and be able to engage mini-drones, rockets and mortar shells.

In 2016, Chinese presented a 30 kW fibre laser Low-Altitude Laser Defending System (**LASS**), useful in combating swarms of small plastic drones up to a distance of 4 km [21]. One of the development versions of LASS, (< 100 kW), called Silent Hunter, was to be used for the protection of the 2016 G20 Hangzhou summit. Silent Hunter, functioning in stationary and mobile versions, is able to penetrate 5 mm steel from a distance of 1 km [21]. From the point of view of overcoming the high mobility of drones, the most important disadvantages of laser cannons are size and the need for highly efficient energy supply systems. Miniaturization of laser systems ought to bring greater acceptance of such types of gun, especially as no projectiles or explosives are necessary and energy requirements can be reduced.
Electromagnetic impulse

According to [21], the Chinese and Americans are interested in using electromagnetic impulse technology, among others, for defeating drones. One can point out the two inter-related demonstrators developed by Raytheon and Boeing [51, 147, 148], i.e. a ground-based Phaser, tested in 2013, and a weapon for air-launched missiles developed within the Counter-electronics High-power Advanced Missile Project (CHAMP), tested in 2012. This is a worldwide topic, developed, for example in the U.S. [149], Russia [150], Germany [151], Czech Republic [152], Poland [152-154], as well as within the framework of international projects [151, 155]. There are many patents, like [156], as well as commercial products [157] based on wireless energy transfer.

3.2.4. Destruction by kinetic energy

Advanced Ballistic Concepts (SKYNET) [158] and Snake River Shooting Products (Dronemunition) [146, 159] are two of the most popular manufacturers of anti-drone munitions of rifle-like systems. The deployment of mortar shells dedicated to destroying drones has been analysed in [160].

In 2017, the anti-drone mobile system ZRN-01 Stokrotka (eng. trans. *Daisy*) was presented at MSPO in Kielce, Poland [93]. The system is based on two air launchers B8W20 with non-guided 80 mm air missiles (RS-80P with programmable fuse). Stokrotka destroys drones at distances up to 4 km. It was developed in cooperation between the Polish company Arex (a member of the WB Group) and the Ukrainian company Artem (consortium Ukroboronprom).

4. Summary

In this paper, confirmation for the hypothesis put in the title is given. Proof that, before our eyes, the idea of machine wars has become a reality, is shown. It is presented as examples of drone-related technologies, the range of drone development, as well as the countermeasure techniques developed against them. The most significant examples are:

a) Drones are commonly used in many areas of interest, both military and commercial. Moreover, not only is the number of these areas growing rapidly, but also commercial applications, especially agricultural ones, can be regarded as a very useful learning and developing method for improving the technologies involved.

b) The factors mentioned in the paper show that the global drone-related market is very strong, meaning that unmanned technologies are unlikely to be abandoned in the future, especially as contemporary development of electronic and telecommunication systems enables the problems present in this field for the last 50-70 years, to be overcome. Also, unmanned technologies enable increases in economic profits, especially by reducing or eliminating the human factor, as the most expensive and/or unreliable component.

c) Unmanned technologies give new possibilities in combat strategy, which are impossible to execute using on-board-piloted platforms, especially when hybrid drones as well as swarms composed of hundreds of very small drones, manufactured on demand, on the battlefield, by 3D printers, are taken into consideration.

d) Because the demands of present battlefield and antiterrorist protection systems need an effective and as fast a response as possible to an enemy’s multipronged attack, the most advanced technologies are not broadly presented, especially those related to electromagnetic field deployment. Finally, systems like net throwers, jammers, and lasers are available commercially for protection against drones in everyday situations. However, the human factor remains.

e) Countermeasure techniques are based mainly on combining real-time electronic and telecommunication technologies with decision-making procedures. Disclosed development of all of these components is not currently sufficient for eliminating the human factor. But it cannot be excluded that the most advanced classified systems are fully automated.

Of course, the state of real combat possibilities in this field can be presented not earlier than during the first attack in a machine war. If we do not want to be surprised, the only possible conclusion is that we have to be able to deal with fully automated detect, attack and defense systems now. One needs to remember that the
broad beginnings of elimination of the human factor from the decision-making process goes back to the chess tournaments of Gary Kasparov vs. Deep Blue, in 1996 and 1997. Taking into account the 30 year period of improvement of systems like Deep Blue, i.e. artificial intelligence, one can regard this as conclusive evidence that machine wars are not a question for future generations, but machines (at least drones) are waiting their turn and are very close to being ready for action, now.

Literature

[3] Ukrainian arms warehouse storing 138,000 tonnes of rockets and tank ammunition is blown up by saboteurs forcing 20,000 to be evacuated. http://www.dailymail.co.uk/ [accessed 19.10.2017].
theguardian.com/ [accessed 20.11.2017].


[41] Pina F.D. 2017. Ideal directed-energy system to defeat small unmanned aircraft system swarms. Air Command and Staff College, Air University.


[43] Study analysing the current activities in the field of UAV. European Commission, Enterprise and Industry Directorate-General, ENTR/2007/065.


[63] RHEA: Robot Fleets for Highly Effective Agriculture and Forestry Management. NMP2-LA-2010-245986 (FP7 2010-2014) CORDIS.


Machine wars – no longer science fiction


Received: October 19, 2017
Accepted: December 22, 2017
Published: December 28, 2017