UDC 621.316.9

A. Alhaj Hasan

Review of the counter-drone systems and their efficiency against the UAV technology

Drones technology is not always a friendly technology, it might be a threat. These threats must be dealt with by security systems. Although with all the advancing technology nowadays, there is no fully effective defense system, where the type and extent of mitigation techniques depend on the environment and situation. Besides the effectiveness issue, there is the fact that the drone technology itself is not standing still. The counter-drones market will therefore have to constantly respond to new advances in drone's technology. There are no standards for insuring the performance and reliability of the C-UAS system so they might present a public safety threat like interference with emergency radio communications, or like missing the intended target by a kinetic system. So this paper is aimed at making a point on the anti-drones techniques and their efficiency and the most effective systems – the high power electromagnetic systems.
Keywords: technology, drones, unmanned aerial systems, counter-drones.

Counter-drone technology, also known as counter–unmanned aerial systems/vehicles, C-UAS or C-UAV technology, refers to systems that are used to detect and/or intercept UAS. As the potential security threats of drones to both civilian and military entities are growing, a new market is rapidly emerging for the counter-drone technology. To date, there have been at least 235 counter-drone products either on the market or under active development (Tab. 1) [1]. In a response to the growing interest in counter-drone weapons, a number of large defense firms are marketing existing products for counter-drone use. For example, Raytheon claims that its C-RAM air defense system, which is traditionally used to defend against mortars and other projectiles, is equally effective against slow-moving unmanned aircraft [2]. Also, the Russian enterprises are betting on electromagnetic suppression systems that help detect malicious drones, identify and disable them [1].

Table 1

C-UAS products [1]

Number of C-UAS products	235
Number of manufacturers	155
Systems capable of detection only	88
Systems capable of interdiction only	80
Systems capable of both detection and interdiction	67

Electronic identification is an alternative form of «counter-drone» technology, which allows one to remotely access information such as the exact location, model type, operator name, and registration number of the drones operating nearby. It is possible to use this information to establish whether a drone presents an immediate threat – something that traditional C-UAS systems cannot do. As in case if a drone is operated by a major broadcasting network, it is not a threat, probably. These systems could also provide users with the exact location of a drone's pilot, unlike many existing C-UAS products, which only locate the drone. AeroScope is an electronic ID system unveiled by the Chinese drone maker DJI, and it is likely that the other manufacturers are in the way to make their own systems. The problem of these systems is that they will only work on drones made by manufacturers that have willingly provided their communications protocol to the system manufacturer [3].

Many countries started to train large birds to catch drones in mid-flight, in an entirely different approach to C-UAS. According to one of these firms, the eagles which wear protective shin-guards in order to shield their legs from the drone's rotors have a 95-percent intercept rate, which is likely higher than many mechanical kinetic alternatives. For maximum effectiveness, it is advised to operate a secondary C-UAS system in tandem with eagles [1].

Different C-UAS systems rely on a variety of techniques for detecting and/or intercepting drones. The following tables describe the main detection (Tab. 2) and interdiction (Tab. 3) methods employed by products currently available on the market, as well as the classification of the C-UAS (Tab. 4) according to their platform [1].

Table 2

Detection and Tracking Systems [1]

Radar	Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters RF pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds
Radio-frequency (RF)	Identifies the presence of drones by scanning for the frequencies on which most drones are known to operate. Algorithms pick out and geolocate RF-emitting devices in the area that are likely to be drones
Electro-Optical (EO)	Detects drones based on their visual signature
Infrared (IR)	Detects drones based on their heat signature
Acoustic	Detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment
Combined Sensors	Many systems integrate a variety of different sensor types in order to provide a more robust detection capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements may also be intended to increase the probability of a successful detection, given that no individual detection method is entirely fail proof

Table 3

Interdiction [1]

RF Jamming	Disrupts the radio frequency link between the drone and its operator by generating large volumes of RF output. Once the RF link, which can include WiFi links, is severed, a drone will either descend to the ground or initiate a «return to home» maneuver
GNSS Jamming	Disrupts the drone's satellite link, such as GPS or GLONASS, which is used for navigation. Drones that lose their satellite link will hover in place, land, or return to home
Spoofing	Allows one to take control of the targeted drone by hijacking the drone's communications link. (Also known as protocol manipulation)
Laser	Destroys vital segments of the drone's airframe using directed energy, causing it to crash to the ground
Nets	Designed to entangle the targeted drone and/or its rotors
Projectile	Employs regular or custom-designed ammunition to destroy incoming unmanned aircraft
Combined Interdiction Elements	A number of C-UAS systems also employ a combination of interdiction elements: most commonly, RF and GNSS jamming systems that work in tandem

Table 4

Platform types [1]

Ground-based	Systems designed to be used from either stationary or mobile positions on the ground. This category includes systems installed on fixed sites, mobile systems, and systems mounted on ground vehicles
Hand-held	Systems that are designed to be operated by a single individual by hand. Many of these systems resemble rifles or other small arms
UAV-based	Systems designed to be mounted on drones, which can come into proximity with the targeted unmanned aircraft in order to employ interdiction elements at close range

Table 5

C-UAS interdiction methods [1]

Jamming (RF, GNSS, or Both)	96
Net	18
Spoofing	12
Laser	12
Machine Gun	3
Electromagnetic Pulse	2
Water Projector	1
Sacrificial Collision Drone	1
Other	6

Table 6

Market survey-detection/classification [4]

System Name	Modality	Range	Notes
Falcon Shield	Radar/Optical/ (Unknown)	Unknown	Used at 2012 Summer Olympics
Liteye	Radar/Optical/ Jamming	Up to 6 Km	
SRC	Radar/Optical/ Jamming	Up to 50 Km	Used at 2012 Summer Olympics, G8 Summit, and US Marine Corp.
DeTect	Radar	3 Km for Styrofoam UAS	Machine learning capability

There are a lot of challenges that face the counter-drone systems at the level of performance, practicality, legality, and policy. These issues are important to consider hoping to use the technology. They are also important to those seeking to establish the role that the technology could play in the broader integration of drones into the airspace system [1]. Danger is the most obvious drawback of kinetic counter-drone systems like missiles, rockets or bullets. Even less risky commercial options (Tab. 5) which include nonlethal projectile weapons that fire blunt force rounds, such as bean bags or rubber bullets, or small portable net guns that can ensnare drones, or laser systems or net guns, may not successfully destroy a hostile drone and require line of sight. By interrupting the drones during their flight by physical means, they will fall down at a considerable speed. Even the net-based systems with a parachute to bring the drone down in a safety way are risky, so the kinetic interdiction systems are likely to be inappropriate for civilian safety [5].

All of the detection systems have drawbacks. It is hard sometimes to detect drones by radar, and the electro-optical systems may confuse a drone with a bird or an airplane and they can only operate during daytime, and EO and IR systems, as well as certain RF systems, must have a direct line of sight with the drone [1]. Acoustic systems might be deaf to some drones because sensors rely on a library of sounds emitted by known drones. As for RF detection systems, they can only detect certain frequency bands in their library which needs to be regularly updated, and with the speedy proliferating of the drones, the libraries will never cover 100 percent of all the drones. As a result, the systems that are not sensitive enough might generate false negatives, which is not desirable from the operator's standpoint [1]. Moreover, jamming systems can also interfere with the legitimate communications links nearside; so the airports are not advised to use the jammers since they can interrupt air traffic management operations [6].

A new technology started to emerge on the market as advanced jamming systems that only block the frequency on which the targeted drone is operating, as well as directed jamming antennas, which may reduce interference with legitimate communications, but it has not yet been certified entirely safe [1]. This is not all the problems in the non-kinetic systems. RF jamming depends on disrupting the drone's communications link with the operator, but it is possible to program some drones to operate autonomously without an active RF link, or to operate in GPS-denied environments, which makes the GNSS jamming systems useless [7]. Technically it is very difficult to build and implement the spoofing systems, and they might be not effective against drones that have been built with protected communication links. In general, all electronic warfare tactics are subject to countermeasures which may make them ineffective [1].

There are some of the detection and interdiction systems used in new counter-drone systems, which, in fact, are based on existing products. For example, the Babcock's LDEW-CD system incorporates the Raytheon's Phalanx unit. Some radars and jamming units are likewise derived from existing products (Table 6),

and are just repackaged as counter-drone systems [1]. International standards for the proper design and use of C-UAS systems are absent, which raises questions about the safety of these systems [1]. In Table 7, there are C-UAS known in Russia, and the most interesting systems in Germany.

Electronic C-UAS, which are also known as electronic counter measures (ECM), high power microwave (HPM), and high power electromagnetic weapons (HPEW) are designed to transmit electromagnetic signals somewhere in the frequency range from 10 kHz up to several GHz. The power levels range from several watts up to gigawatts, depending on the technology. ECM is mostly dedicated to interfering with any RF receiver. The vulnerable systems are the avionics systems (e.g. altimeters), data and command links, SAR and D/GMTI radar, commercial mobile telephony, personal mobile radios (AM/FM), and global positioning systems (GPS). Their goal is to prevent successful reception or transmission of data [11].

The commercial ECM is similar to a cyber style attack as it aims to exploit information contained within the data-link, but in this case the time durations of such attacks must be considered, especially in case of an intelligent attack strategy using a swarm attack, where isolating individual targets may be too difficult. It might be difficult also to penetrate altimeters because they are more likely to be used by nation organizations. As already mentioned, personal communication devices are very vulnerable to simple jamming techniques but this will likely interfere with any civilian or friendly systems nearby. Due to the weakness of GPS signals, GPS ECM consisting of jamming or spoofing (which is noted as more effective but also more difficult) is simple, and there are available protection techniques to amplify the satellite signal and attenuate it in the direction of the jamming signal. As a result, ECM technologies are effective only against low-cost consumer grade low, slow, and small drone's threats [11].

As the last barrier of defense, kinetic counter-drone systems capable of destroying hostile drones can be deployed against drones that still represent a threat despite non-kinetic systems being employed by blocking the controller frequency and GPS [5].

Theoretically, the HPEM can be very effective, with effects ranging from temporary disruption to physical destruction of unprotected electronics. There are also many external factors which influence this method's effectiveness, such as the electric field strength in the target area, the frequency, and the target shielding capabilities. Unlike the previous systems and methods, this mitigation strategy has low directivity and thus has an advantage as it does not need tracking or precise target location, but of course, the low directivity also means that it will likely affect the other friendly systems if left unprotected. There is no public data available for the operational range for this strategy and it has never been included in the Ground Based Air Defense (GBAD) systems [11].

Table 7

Counter-UAS products

Manufacturer	Product Name	Country	Detection	Interdiction	Platform
Kalashnikov/ZALA Aero Group	REX 1	Russia	Without	RF Jamming, GNSS Jamming	Handheld
LocMas	STUPOR	Russia	Unknown	RF Jamming, GNSS Jamming	Handheld
NNIIRT	1L121-E	Russia	Radar		Ground-based
Rostec	Shipovnik-Aero	Russia	RF, Unknown	RF Jamming, GNSS Jamming	Ground-based
SC Scientific and Technical Center of Electronic Warfare	Repellent-1	Russia	RF	RF Jamming	Ground-based
esc Aerospace [8]	CUAS	Germany	RF, Radar, Acoustic, EO	RF Jamming, GNSS Jamming, Electromagnetical pulse	Ground-based
Diehl Defence [9]	HPEM counterUAS GUARDION [10]	Germany	Unknown	Electromagnetic pulse	Ground-based

Table 8

Counter-UAS products.

Product name	Company	Weight	Applied temperature C	Analog Signal Suppression Radius	SNS suppression radius	Interfering at frequencies	Uptime
REX-1	ZALA AERO GROUP Unmanned Systems	4.5 kg	– 40 to + 50	0.5 km	2 km	900 MHz, 2.4, 5.2–5.8 GHz	3 hours
GARPUN-2	LLC SCIENTIFIC-PRODUCTION ENTERPRISE «NEW TELECOMMUNICATION TECHNOLOGIES»	unknown	unknown	up to 300 m	433–868–900 MHz – 1.17645 GHz; BeiDou (1.20714 / 1.26852 / 1.5750 GHz); GPS (1.17645 / 1.2276 / 1.5754 GHz); Glonass (1.202025 / 1.246 / 1.602 GHz) 2.4 – 5.8 GHz		40 minutes

Backing to the electronic C-UAS, depending on the power of the emitted pulse, shotguns are classified according to the frequency ranges at which they are able to jam the UAV communication channels. These devices are also capable of blocking GSM, 3G, LTE signals at a distance of one kilometer and interfering at different frequencies. However, the drone loses touch with the control panel and lands, but is not physically destroyed. Different companies in Russia offer their own solutions and products. In Tab. 8, there are examples of products like these in Russia (Figs. 1, 2) and some of their characteristics and features [12, 13].

Fig. 1. REX-1 Russian weapons against drones. Protection against unmanned aerial vehicles [12]

Fig. 2. The commercial type «GARPUN-2». Protected from UAV [13]

Conclusions

The HPEM are still under development, and countries must do more effort toward it. The focus should also be on the EC-UAS and increased funding for the research and development of more effective systems. The most effective and cost efficient systems should be prioritized [5]. There may be ambiguity concerning which bodies of law apply depending on the context, as noted in UNIDIR's 2017 study. Establishing the facts and assessing the legality of the use of force has been challenging due to the limited transparency surrounding these operations [14,15,16].

Detection, identification, and mitigation of the LSS UAS are a challenging problem. The systems exist in the commercial domain that likely solve a limited piece of the larger LSS UAS problem, but no complete system appears to exist with evidence of acceptable performance [11].

The reported study was funded by Russian Science Foundation (project № 19-19-00424) in TUSUR University.

References

1. Michel A.H. Counter-drones systems. Center for the Study of the Drone, 2018. – https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf

2. Raytheon company. To down a Drone // Raytheon, October 13, 2017. – https://www.raytheon.com/news/feature/anti_drone_technology.html.

3. Daniel K. Letter from Small UAV Coalition to Hon. Elwell, Acting Administrator, Federal Aviation Administration. – February 2, 2018. – http://www.smalluavcoalition.org/wp-content/uploads/2018/02/Small-UAV-Coalition-Letter-to-FAA-re-Remote-Identification-and-Tracking-2.2.18.pdf

4. Daniels J. Russia says it killed rebels behind swarm drone attack in Syria, but experts see more such strikes ahead. CNBC. – January 12, 2018. – https://www.cnbc.com/2018/01/12/ russia-says-iteliminated-rebels-behind-swarm-drone-attack-insyria.html

5. Abbott C. Hostile Drones: the Hostile Use of Drones against British Targets. Remote Control Project. – January 2016. – http://statewatch.org/news/2016/jan/uk-org-hostile-use-of-drones-jan-2016.pdf

6. Michael J.O'Donnell, A.A.E. Director of Airport Safety and Standards. – U.S. Federal Aviation Administration. – October 26, 2016. – https://connect.ncdot.gov/resources/Aviation%20Resources%20Documents/faa-uas-detection-testing-letter.pdf.

7. Balamurugan G., Valarmathi J., Naidu V.P.S. Survey on UAV navigation in GPS denied environments / 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016. – P. 198–204.

8. Esc Aerospace group. – https://www.esc-aerospace.com/Projects/cuas/

9. Diehl Defence. Reliable protection against drone, 2017. – https://www.diehl.com/defence/en/press-and-media/news/reliable-protection-against-drones-esg-diehl-defence-and-rohde-schwarz-cooperate/.

10. Diehl Defence. GUARDION. – https://guardion.eu/

11. Birch G.C., Griffin J.C., Erdman M.K. UAS Detection, Classification, and Neutralization: Market Survey. Sandia National Laboratories, 2015. – https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/156365.pdf

12. ZALA AERO GROUP Unmanned Systems. – https://zala.aero/rex-1/

13. LLC scientific-production enterprise «new telecommunication technology». – http://www.nppntt.ru/produktsiya/

14. Woodhams G. Weapons of Choice? The Expanding Development, Transfer, and XVI Use of Armed UAVs. UNIDIR, 2018. – https://www.unidir.org/publication/weapons-choice-expanding-development-transfer-and-use-armed-uavs

15. Borrie J., Finckh E., Vignard K. Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles, UNIDIR, 2017. – https://www.unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles

16. United Nations Secretary-General, Securing Our Common Future: An Agenda for Disarmament, 2018. – https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf

Alhaj Hasan Adnan
Postgraduate student,
Department of Television and Control, TUSUR
Email: alhaj.hasan.adnan@yandex.ru