GSD, 2019, 15(32): 691-711
DOI: 10.17752/guvenlikstrtj.668216

Araştırma Makalesi
Research Article

The Present Role of Anti-Drone Technologies in Modern Warfare and Projected Developments[*]

Modern Savaşta Anti-Drone Teknolojilerinin Mevcut Rolü ve Olası Gelişmeler

Tolga ÖZ[**] – Serkan SERT[***]

Abstract

As by many scholars pointed out "Autonomous drones are being called the biggest thing in military technology since the nuclear bomb". The idea behind MAD doctrine is that if both sides were to fight a full-scale war with nuclear weapons, there would be no winners and both would be mutually annihilated. This impasse has relatively kept the world from erupting into another all-encompassing war. In the matter of drones, continuing proliferation of them with their technological components that pioneered in 1917 with the first pilotless winged aircraft in history, ramped up by the first commercial drone permits by the FAA in the US recognizing the potential of non-military, non-consumer drone applications in 2006. Concordantly academic literature rather has been filled with the hypothesis of using drones; particularly armed ones can spark long term security and stability. But the snowballing use of contemporary drones is obviously inclined to make the world a more conflicting place both in civilian and military domains. This has been

[*] This paper was presented at 8th International Scientific Conference on Defensive Technologies (OTEH 2018) at 11-12, October 2018, Belgrade, Serbia.

[**] Ph.D., Lecturer, Colonel, Turkish National Defense University, Atatürk Institute of Strategic Studies, ORCID: 0000-0002-3608-2090, e-mail: toz@msu.edu.tr.

[***] Ph.D., Colonel, Turkish National Defense University, e-mail: ssert@msu.edu.tr.

Geliş Tarihi / Submitted : 20.01.2019
Kabul Tarihi / Accepted : 24.10.2019

progressing as a worldwide pain point that there's not been reached any forcible remedy like MAD doctrine in nuclear confrontation. Within this problematique margin, our study firstly provides awareness how growing number of increasingly capable drones in our skies poses obvious challenges. And as second, it enables the academics to familiarize recent types of counter drone technologies and instruments, and lastly outlines trajectory of counter-technology in times to come.

Keywords: *Drone, Anti/Counter UAS/Drone, Detection & Neutralization of Drones, Defense Management.*

Öz

Birçok bilim insanının belirttiği gibi, "Otonom dronlar, askeri teknolojide nükleer bombanın icadından bu güne en büyük buluş olarak nitelendirilmektedir. MAD doktrininin ardındaki fikir, iki tarafın da nükleer silahlarla büyük çaplı bir savaşta kazananın olmayacağı ve karşılıklı olarak yok olacağı yönündedir. Bu çıkmaz, göreceli olarak dünyayı, her şeyi kapsayan bir savaşa dönüşmekten alıkoymuştur. 1917 yılında tarihteki ilk insansız uçakla başlayan ve teknoloji ile birlikte sürekli gelişmeye devam eden dronlar 2006 yılında Amerikan Federal Havacılık Dairesi'nin ticari dron kullanılmasına ilk defa izin vermesi ile yaygınlaşmaya başladı. Buna paralel olarak akademik literatürde özellikle silahlı dronların uzun vadeli güvenlik ve istikrarı tehdit edebileceğine ilişkin dron kullanımı ile ilgili çok sayıda hipotez bulunmaktadır. Ancak, modern dronların hızla çoğalan kullanımı dünyayı hem sivil hem de askeri alanlarda açıkça daha çatışmalı bir yer haline getirme eğilimindedir. Bu husus, nükleer çatışmada MAD doktrinin aksine herhangi bir etkili çözüm bulunamamış evrensel düzeyde tanımlanamayan bir sorun olarak devam etmektedir. Bu sorunsal çerçevesinde, çalışma öncelikle giderek artan sayıda kabiliyetli dronların nasıl aşikar sorunlar yarattığı konusunda farkındalık sağlamakla birlikte literatüre en son anti-dron teknolojilerini ve araçlarını tanınması yönünde katkı yapmakta ve öngörülebilir karşı teknolojinin yol haritasını ana hatlarıyla belirlemektedir.

Anahtar Kelimeler: *Drone, Anti/Karşı Drone, Drone'ların Tespiti ve Etkisiz Hale Getirilmesi, Savunma Yönetimi.*

Introduction

Certain figures have played an significative role in geopolitics and world affairs. For instance, Pakistani nuclear scientist, Abdul Qadeer (A.Q.) Khan, built a network in the 1990s that smuggled technology and nuclear know-how to rogue regimes in Iran, North Korea and Libya, drastically complicating the global security landscape.[1] Again Edward Snowden, the former National Security Agency contractor responsible for copying and leaking vast troves of classified information, impacting security procedures for how other countries and notably the US handle classified information.[2] Individuals and small groups have the potential to use an array of new and emerging technologies, virtual currencies, encrypted communications, artificial intelligence (AI) and ever-increasingly drones. Given that, there is a steady drumbeat of warranted concern over the potential use of specific technologies by non-state actors. The combination of these technologies—as evidenced in the Saudi scenario, where a drone was used in conjunction with a deliberate disinformation campaign perpetrated through social media, individuals or small groups with nefarious intent will soon be able to modify and repurpose the technology to cause chaos.[3] As for drones, there is growing security concern among civilian and military sectors. As a consequence, a new market has already been boomed for countering existential and potential threats posed by Unmanned Aircraft Systems (UAS).

This paper firstly provides awareness how growing number of increasingly capable drones in our skies poses obvious challenges,

[1] The Guardian Website, "Pakistan releases 'father' of nuclear bomb from house arrest,", https://www.theguardian.com/world/2009/feb/06/nuclear-pakistan-khan (Access Date: 17.01.2019).

[2] Paul Szoldra, "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks", https://www.businessinsider.com/snowden-leaks-timeline-2016-9 (Access Date:17.01.2019).

[3] Colin P. Clarke, "A Terrorist's Dream: How Twitter and Toy Drones Could Kill a Lot of People", https://nationalinterest.org/blog/the-buzz/terrorists-dream-how-twitter-toy-drones-could-kill-lot-26288 (Access Date:17.01.2019).

including espionage and weaponization. And as second, it enables the academics to scrutinize different types of counter drone technologies, and outlines trajectory of non-kinetic counter-measures in times to come.

1. Security Threats Posed by Drones

A growing number of increasingly capable drones in our skies pose obvious challenges.[4] In spite of being relatively new technology, drones of varying types and sizes are readily available for consumer purchase. Where there were once one to two predator drones, now there are delivery drones, hobby drones and sightseeing drones. Some experimentation in taking a drone apart revealed that most ready-to-ship drones come with the same electronics as a smartphone or tablet.[5] Indeed drones have gained a huge popularity as toys among the general public. With ever-growing capabilities in performance, cameras, GPS, and radio links, the number of drone applications is rapidly expanding, stirring the imagination of inventors and hobbyists alike but with limited aeronautical knowledge.[6] To face the safety, security and privacy issues associated to the development of these UAS operations, many countries have already promulgated their national UAS regulation but hardly any action have been launched against small UAS flying at Very Low Level (VLL)- 500ft and below.[7]

[4] Jon Hegnares, "The Past, Present And Future Of Anti-Drone Tech", https://www.forbes.com/sites/forbestechcouncil/2018/01/26/the-past-present-and-future -of-anti-drone-tech/ (Access Date:17.01.2019).

[5] Kelly Yyver, "A Future Full of Drones — and the Advanced Threats They Present", https://securityintelligence.com/a-future-full-of-drones-and-the-advanced-threats-they-present/ (Access Date:17.01.2019).

[6] Rene Van Der Heiden, "NCI Agency helps protect NATO operations against drone attacks", https://www.ncia.nato.int/NewsRoom/Pages/180529-Drone.aspx (Access Date: 17.01.2019).

[7] Antoine Joulia, Thomas Dubot ve Judicael Bedouet, "Towards a 4D Traffic Management Of Small UAS Operating At Very Low Level", www.icas.org/ICAS_ARCHIVE/ICAS2016/data/papers/2016_0064_paper.pdf (Access Date:17.01.2019).

Even the cheapest drones have fully operational Wi-Fi, radio frequency and Bluetooth antennas or a combination of all three[8]. The ease of use and accessibility of the latest drone models opens the door to those who would use drones for unintended and malicious purposes. It would be irresponsible to ignore the need for counter-drone technology. One of the reasons counter drone/anti-drone e-technology has become such a big issue in 2018 relates to scenarios where drones could be used to threaten the privacy of people, protected places, large events or critical infrastructure.

In civilian domain the potential to use this cutting-edge technology against civilian populations is staggering. Nefarious drone uses within Industrial Domains based on recent past events in the world can be outlined as;

- Drones flying directly over nuclear cooling towers, where they can simply be shut off or drop while carrying an explosive payload,[9]
- Drones for reconnaissance on sensitive areas such as critical power units causing blackout,[10]
- They can watch and document security patrols in proximity of public venues, arenas, events national laboratories and governmental buildings by cooperating required hacking devices, spying cameras and sensitive microphones.[11]

[8] Rene Van Der Heiden, “NCI Agency helps protect NATO operations against drone attacks”, https://www.ncia.nato.int/NewsRoom/Pages/180529-Drone.aspx (Access Date: 17.01.2019).

[9] RT Website, “Unidentified drones flying over French nuclear power plants, probe launched”, https://www.rt.com/news/200887-france-drones-nuclear-plants/ (Access Date: 17.01.2019).

[10] India Ashok, “Drone crash: Rogue UAV knocks out power line causing widespread blackout”, https://www.ibtimes.co.uk/drone-crash-rogue-uav-knocks-out-power-line-causing-widespread-blackout-1625876 (Access Date:17.01.2019).

[11] UK Progressive Website, “The flying of unauthorized drones at stadiums prompts

- Because of some prominent enterprises having developed technology that captures data on potential customers' characteristics by marking any individual's home of roof, driveway, landscaping etc. private individuals may experience drone incidences as it is unclear how this data will be used out of providing maximum customer satisfaction.[12]

The first threat came into public view in Turkey was a drone controlled by state television channel-TRT for recording Victory Day celebrations caused panic among statesmen and the public in August 2015. This date can be accepted as triggering milestone for Turkey to attach importance to drone threat from legal, technical and even sociopsychlogical context. Once more in February 2016, a hobbyist-drone landed by a student in presidential compound set second concrete case for Turkey thusly handheld RF and GNSS jamming ASELSAN anti drone equipment started to be full operational for governmental protection.[13]

Among dozen examples in the world that exposed to media from 2013 to date, probably the most strong effective incident occurred in August 2018, two drones packed with explosives flew toward Venezuelan President Nicolas Maduro in what the government has described as a failed assassination attempt. The Venezuelan military knocked one of the drones electronically. The second drone crashed into an apartment building about two blocks from where Maduro was speaking to hundreds of troops.[14]

safety concerns", https://ukprogressive.co.uk/the-flying-of-unauthorized-drones-at-stadiums-prompts-safety-concerns/article32097.html (Access Date:17.01.2019).

[12] Dedrone Website,"Worldwide Drone Incidents", https://www.dedrone.com/resources/incidents/all (Access Date:17.01.2019).

[13] Haber46 Website, "Anıtkabir töreninde drone paniği, askerler çekim yapan aracı vuracaktı", https://www.haber46.com.tr/politika/anitkabir-toreninde-drone-panigi-askerler-cekim-yapan-araci-vuracakti-h116581.html (Access Date:17.01.2019).

[14] Erin Kelly, "Venezuela drone attack: Here's what happened with Nicolas Maduro", https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas -maduro-assassination-attempt-what-happened/913096002/ (Access Date:17.01.2019).

Another matter introducing alarming security concerns is supposed to be airports and their airspace. Without any identifying factors on the drone itself, airports and flight operators must brace for any possibility or reason for an airspace interruption. The US airports have been experiencing about 600-700 drones incidents flying too close for comfort to airports and airplanes, according to a report from the Federal Aviation Administration and it is estimated that drone sales are expected to reach 7 million in 2020 which presumptively will skyrocket the drones around airports.[15]

Within the scope of legislation, the International Air Transport Association (IATA) warned that as of 2016, of the 191 states within the International Civil Aviation Organization (ICAO), 63 so far had regulations already in place for drones, nine states have pending regulations, while five have banned their use. Moreover, it is stated that there's not a consistency across the regulations, to help harmonize global rules.[16]

The first airport incident was reported in Turkey at Atatürk Airport in February 2015, affected air traffic security adversely.[17]

The inference is that since consequences of a too close encounter or potential airborne collision between a commercial UAV and an airplane would have a catastrophic outcome, controlling drones more efficiently and reducing the threat originating from them over airspace is an ongoing battle for civil aviation authorities.[18]

[15] Jonathan Vanian, "Drones Are Still Flying Dangerously Close to Airplanes and Airports", http://fortune.com/2016/03/28/drones-flying-too-close-airplanes-airports/ (Access Date:17.01.2019).

[16] Agence France-Presse, "Drones becoming 'real' threat to commercial aviation: IATA", http://2016.mb.com.ph/2016/02/15/drones-becoming-real-threat-to-commercial -aviation-iata/#rbZIqrCDIsztMMKl.99 (Access Date:17.01.2019).

[17] Hürriyet Website, "Atatürk Havalimanı'nda Drone için tabelalı önlem", www.hurriyet.com.tr/video/ataturk-havalimaninda-drone-icin-tabelali-onlem-122501 (Access Date:17.01.2019).

[18] Slavimir S. Nikolić, An innovative response to commercial uav menace – anti-UAV

In the military domain, small drones have been proliferating at a rate that has already alarmed battlefield commanders to ponder the issue of how to counter them since the beginning of 1990's. Related to this, one of the first publicly released academic documents dates back to 1992, a us naval post graduate school thesis titled with "Anti-UAV Defense Requirements For Ground Forces And Hypervelocity Rocket Lethality Models" by Joseph J. Beel., in which it analyzes the threat that unmanned aerial vehicles (UAVs) pose to U.S. ground forces. The study refers to the prophetically suggested need for counter-UAV measures, even though technological maturity of UAV's had not been reached to the level it already has been at present.[19]

But particularly as a corporate endeavor, the NCI (NATO Communications and Information) Agency has recently acquired a deep understanding of drone detection and countermeasures. As a centre of excellence for Electronic Warfare and sensor systems, the Agency's Joint Intelligence, Surveillance and Reconnaissance (JISR) team is well positioned to apply knowledge gained through the delivery of operational capabilities using similar technologies to help the counter-drone challenge.[20] The Agency also has a thorough grasp of the available counter-drone systems on the market, acquired through a recent market survey performed in the last quarter of 2017. As such, the Agency intends to release an Invitation for Bid (IFB) for NATO procurement, which had already been planned in mid-2018.[21]

Falconry, *VOJNO DELO, 4/2017.*, http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2017-4/69-2017-4-14-Nikolic.pdf (Access Date: 17.01.2019).

[19] Joseph J. Beel, Anti-Uav Defense Requirements For Ground Forces And Hypervelocity Rocket Lethality Models", March 1992, Naval Postgraduate School, Monterey, California. http://www.dtic.mil/dtic/tr/fulltext/u2/a252727.pdf (Access Date:17.01.2019).

[20] Rene Van Der Heiden, "NCI Agency helps protect NATO operations against drone attacks".

[21] NCI Agency, "Notification of Intent to Invite Bids", https://www.ncia.nato.int/Industry/Documents/NOI-IFB-CO-14685-UAS_Notification%20of%20Intent.pdf (Access Date:17.01.2019).

Particularly in the conflict in Syria and Iraq, many groups operate a wide variety of drones, which give even the most poorly funded actors an aerial command of battle space that can prove decisive in engagements.[22] Virtually Hezbollah and Hamas were pioneers of exploiting the possibilities offered by drone technology, but DEASH has presented very impressive development of the drone program. They initially used drones for surveillance and for propaganda purposes, but there has been a rapid increase of weaponised drones. There was a rapid increase in reports on DEASH's use of weaponised drones after the group announced the establishment of a separate drone unit in January 2017.[23] Also Turkey received her share from a bomb-laden mini drone attack by DEASH on Sept. 27, on the 35th day of Euphrates Shield operation in Syria.[24] As a result of domino effect among terrorist groups, Turkish security forces seized a bomb-laden drone reportedly made by outlawed Kurdistan Workers' Party (PKK) militants in the eastern province of Ağrı on November 11, Hakkari Çukurca September & November 18, Şırnak October 18. The bomb-laden drone, which is used as an air attack method by DAESH groups in Iraq and Syria, was reportedly seen used in a plot by the PKK for the first time.[25]

One striking example of events in military domain is an attack on Russian forces in Syria on January 5th executed by 13 home-made, GPS guided drones having 100 km range. The craft involved in these

[22] Arthur Holland Michel , "Counter-Drone Systems.", *Center for the Study of the Drone at Bard College,* February 20, 2018, http://dronecenter.bard.edu/counter-drone-systems/ (Access Date:17.01.2019).

[23] Truls Hallberg Tønnessen , "Islamic State and Technology – A Literature Review", *Perspectives on Terrorism,* Vol. 11, No. 6 (December 2017), pp. 101-111.

[24] Yeniçağ Gazetesi Website, "Yeniçağ: IŞİD, Drone ile Mehmetçiğe saldırdı!", http://www.yenicaggazetesi.com.tr/isid-drone-ile-mehmetcige-saldirdi-147012h.htm (Access Date:17.01.2019).

[25] Hürriyet Daily News Website "PKK's bomb-laden drone seized in Turkey's east", http://www.hurriyetdailynews.com/pkks-bomb-laden-drone-seized-in-turkeys-east-122299 (Access Date:17.01.2019).

attacks resembled hobbyists' model aircraft. They had three-meter wingspans, were built crudely of wood and plastic, and were powered by lawnmower engines. Each carried ten home-made shrapnel grenades under its wings. The craft may thus have been a cheap, garage-built copy of captured kit.[26] This event also illustrates the specter state- and non-state-sponsored package raid of swarm-drones implying being capable of flying autonomously in formation. As pointed out in CBS news "Autonomous drones are being called the biggest thing in military technology since the nuclear bomb", a new generation of drones is coming. Only this time they are autonomous -- able to operate on their own without humans controlling them from somewhere with a joy stick, can go about 10,000 nautical miles on a tank of gas, each of those tiny drones is flying itself.[27]

To put in a nutshell, in a Pentagon's official research publication, one military official very clearly highlights the drone-peril that. It is only a matter of time before drones will be used to carry chemicals, explosives, small arms or kamikaze into any facility, person or throng of crowds... The clock is ticking, and we don't want to wait until it's too late.[28]

2. Overview of Existing Counter Drone Measures and Challenges

As suggested above, sharp rise in incidences of security violation by unauthorized drones causing increased actions of nefarious and terror attempts worldwide has opened up evolution of counter drone measures. Recently counter-drone industry has been growing very rapidly. As of the beginning 2018, The Center for the Study of the

[26] The Economist, "Home-made drones now threaten conventional armed forces", https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces (Access Date:17.01.2019).

[27] David Martin,"New Generations of Drones set to Revolutinize Warfare", https://www.cbsnews.com/news/60-minutes-autonomous-drones-set-to-revolutionize-military-technology/ (Access Date:17.01.2019).

[28] Wim Zwijnenburg,"Terrorist Drone Attacks Are Not a Matter of 'If' but 'When'", https://www.newsweek.com/drones-isis-terrorist-attacks-453867 (Access Date:17.01.2019).

Drone at Bard College identified more than 230 C-UAS products produced by 155 manufacturers in 33 countries. These products range from detection, identification to neutralization purposes.[29]

At the present moment there are no such a system which could protect for hundred percent from the drones, because each object has different area, infrastructure, security policy or location issues.[30] However determining type of the target and its threat level is the backbone of defense logic with regards to establishing timely and proper reaction against any medium generated from air. In this sense the first step is to find and alert the presence of the threat, right after to classify the nature of it.

The current air defense systems have traditionally been designated for protection of airspace from manned aircraft that are large and fast moving assets. They potentially present challenges in the fields of cost, efficiency, range and collateral damage. For Instance among other projects, the American army is hurriedly upgrading its shoulder-launched Stinger missiles, which are used to attack low-flying aero planes and helicopters, not designed to hit small drones. The upgrade adds a proximity fuse which detonates when the missile is close enough to destroy a drone without actually having to make contact with it. But the upgrades cost about $55,000 each (on top of the basic $120,000 cost of a Stinger), so only 1,147 are being purchased—about two per team, which is hardly enough to tackle a swarm of drones. Another emphasis focused by the armies is counter air operation to stop drones before they can take off. Any attempt for prevention drone threat in preparation or sustainment phase along with drone-assembly and storage facility is another story. But when there are no runways or hangars, and drones can be operated from houses

[29] Arthur Holland Michel, “Counter-Drone Systems.”, *Center for the Study of the Drone at Bard College*, (Access Date:17.01.2019).

[30] Anti-Drone Website “Anti-drone system overview and technology comparison”, https://anti-drone.eu/blog/anti-drone-publications/anti-drone-system-overview-and-technology-comparison.html (Access Date:17.01.2019).

and garages, finding bases to attack is far from easy.[31]

The main non-kinetic detection and identification technologies suggesting both opportunities and challenges for development of industrial counter drone measures can be encapsulated as bellows;

- ***Optical and Infrared***

Electro-optical systems can only operate during daytime, and might confuse a drone with a bird or an airplane. A camera scans the area to detect and identify a potential drone. The monitoring can be done on the visible or infrared spectrum. The issue is that drones are small and difficult to see. They also have a limited heat signature compared to traditional aircraft with combustion engines. These type of sensors are not very suitable for the detection phase.[32]

- ***Acoustic Sensors***

Drones emit a distinctive buzzing sound that can be picked up by sensitive microphones in order to give an estimated direction and distance of the drone. However acoustic sensors rely on a library of sounds emitted by known drones, and might therefore be deaf to drones not covered by the library. Besides they are not able to precisely identify threats because of noisy backgrounds (e.g., airport, city downtown), or drone tuning limiting detection capability.[33]

- ***Electronic Support Measures***

RF detection systems only detect certain frequency bands in a library that needs to be regularly updated considering the rapid growth of commercial drones. The key of detection is to adjust the right sensitivity, selectivity-frequency to detect the drone. If the system is attuned too sensitively, it may lower discrimination of drone from any

[31] The Economist, “Home-made drones now threaten conventional armed forces”, (Access Date:17.01.2019).

[32] Arthur Holland Michel, “Counter-Drone Systems”.

[33] Oliver Kmia, “The Technical and Legal Challenges of Anti-Drone Systems”, https://fstoppers.com/aerial/technical-and-legal-challenges-anti-drone-systems-193666 (Access Date:17.01.2019).

other flying object (e.g. pigeon). Adding the fact that the operating environment is becoming full of authorized and unauthorized drones, C-UAS systems must be able to have the capability to identify friend or foe. Most commercial drones are constructed of plastic and are difficult to spot electronically because they fly low to the ground and don't carry a transponder to signal their positions. But in comparison radar seems more promising than optical&infrared imaging for threat confirmation.[34]

When it comes to neutralization (Interdiction (soft kill) and/or destruction (hard kill), with small numerous drones, which are difficult to detect, identify and track, jamming could be an obvious measure by disrupting the radio links between the operator and the drone, or confusing its GPS navigation. But jamming is not effective against autonomous ones that are pre-programmed via GPS again.[35] In practice the destruction of drones can be done by firearms from ground or air requiring missile and laser but solutions are not cost effective. New technologies are under development such as electromagnetic pulse and high energy microwaves. But their promise are still in question whether they can be used in urbanized environment that can cause them falling into ground. And all these concerns influence in counter-drone industry.

3. Counter-Drone Market Scope

This rapidly emerging global Counter-Drone market might be segmented as below according to financial expenditure in the market via five orthogonal money trails, and these categories are: mitigation, defense, end-use, and region-based.

In the first level, the mitigation market segment has been split into destructive and non-destructive systems. Destructive systems are

[34] W.J. Hennigan, ”Experts Say Drones Pose a National Security Threat — and We Aren't Ready”, www.time.com/5295586/drones-threat/ (Access Date:17.01.2019).

[35] The Economist, “Home-made drones now threaten conventional armed forces”.

used completely to destroy the working components of drones. Destructive mitigation systems are sub categorized as; Laser Systems, Missile Effectors, and Electronic Counter Measure Systems.

In this section the data regarding this so-called segment has been provided by the publication of “Anti-Drone Market” by Grand View Research company which is currently accessible main and single open-source in related subject-matter.[36]

As the first categorization, mitigation systems occupied the leading market share in the global counter-drone market in 2016 in terms of revenue. Also, it is found out that destructive system global market is the fastest growing segment by providing market growth from $266.1 mn in 2015 to $1.733 bn by 2024, following an estimated CAGR 24.8% from 2016 to 2024.

Comparatively, non-destructive system global market anticipated to witness a sluggish growth in the near future by providing lack of effective drone counter solutions by providing a market growth from $32.9 mn in 2015 to $117.4 mn by 2024.

As the second market categorization, defense segment has been split into Detection and Detection&Disruption systems. Amongst the defense systems market, Radar based and Active Optics systems are the leading sub-segments of the detection system. The low price factor of these technologies over RF emission or acoustics type detection system accounts for their lead positions. In parallel to electronic systems, the trend in the global counter-drone market by defense category is in favor of Detection segment with a market growth from $92.9 mn in 2015 to $616.1 mn by 2024, following a CAGR of 25.0% over the forecast. These data naturally makes the detection systems as the fastest growing defense category segment. Comparatively,

[36] PR News Wire Website "Counter-Drone Market & Technologies – 2018-2023", published by Homeland Security Research Corp., https://www.prnewswire.com/news-releases/the-global-counter-drone-market-is-forecast-to-grow-at-a-2018-2023-cagr-of-37-2-300710320.html (Access Date:17.01.2019).

Detection & Disruption market segment has a tendency of market growth from $206.1 mn in 2015 to $1.23 bn by 2024 with an estimated growth CAGR of 23.6% from 2016 to 2024.

As the third market categorization, End-Use Segment has been split into Military&Defense, Commercial, and Government sub-categories.

In terms of end-use market, the segments of both military and government are the key general end-users of counter-drone systems holding the leading share of the market in 2015.

The results of detailed analysis, regarding end-use market industry snapshot can be summarized as follows:

Military&Defense market by far anticipated to emerge as the leading predominant end-use segment due to increase in R&D activities by defense prime contractors; the market for counter-drone systems in military and defense applications is expected to cross USD 900 mn by 2024 with a market size estimated at $179.4 mn in 2015. Military&Defense segment is followed by government segment. Government Market size was $35.9 mn in 2015 and is expected to reach $284.5 mn by 2024 with a proportional increase in the near future.

Apart from military and government sectors, the commercial sector is also expected to contribute significantly to the counter-drone market having a tendency of market growth from $56.2 mn in 2015 to $388.9 mn by 2024 over the forecast period with growing at an estimated CAGR of 25.6% from 2016 to 2024. This involves use of counter-drone for protection of airports, government buildings, commercial buildings, places of public gatherings, etc.

As the fourth categorization of Region market segment, Market Breakdown Description of the global anti-drone market share by geographic regions is roughly as follows; Americas with the lead of USA has the %60, Europe %25, Asia Pacific (APAC) %10 and rest of the World (RoW) %5.

In Asia Pacific region it is anticipated to witness a CAGR of close to 30.0% over the forecast period owing to increasing government expenditure in development of aerospace infrastructure across emerging economies.

3.1. Overview of Primary Company Revenues in the Market

Based on key player company types on the market these proportions are as follows: Companies having more than USD 1 billion total revenue of 2015 as %55, having total revenue of 2015 between USD 500 million – 1 billion %25, and having less than USD 1 billion total revenue of 2015 as %10. In parallel to global market share the USA is forcing counter-drone market with 62 companies, and the UK (20 companies), Israel (13 companies), Australia, Germany, France, and Switzerland (10-13 companies) are the other leading stakeholder manufacturer countries shaping the industry. Turkey is also contributing with two companies having ground-based RF/GNSS Jamming detection and interdiction capabilities.

Conclusion

Drone technology is undergoing progressive evolution. The current technology has already been transforming from capabilities of improved safety modes, autopilot modes into multi-type platform and payload adaptability, and full autonomy facilitating airspace awareness. The next generation suggests promising benefits particularly in full airspace awareness and automatic execution of every type of package missions in swarm.

In parallel with advancement of drone technologies, all the benefits have already come with their share of risks and challenges that is leveling them up to national security concern. It would unhesitatingly come that individuals and small groups will exploit them for their own advantages. Accordingly, this paper aimed to outline how growing number of increasingly capable commercial drones in our skies poses obvious risks and challenges along with the current overview of platform-based defense solutions.

Part of the challenges is evident that new national and international regulations must be designed for this emerging threat getting more and more autonomous. It seems impossible to find complete solution from today to tomorrow. However, sectors with support of governments have to develop corporate programs regarding net of multiple sensors to offer wide area architecture of surveillance

of all drones mostly operating in urban areas where many strategists increasingly acknowledge that the future of war is in cities. From platform standpoint, defending against multiple drones requires launching multiple sensors and platforms. And practically considering the worst case, even downing drone with an explosive could be risky for safety. Thus, capturing and taking them away seems to be the best option. Anti-drone market for "*detection and disruption*" clearly shows that it is going to grow at the highest CAGR in five year-period of time. But it is likely that counter interdiction methods (jamming, laser, net, machine gun, electromagnetic pulse etc.) employing combination of multiple sensor types generated by drone-catcher drones, rather than ground based or hand held platforms will be in focus among companies.

Özet

2006 yılında Amerikan Federal Havacılık Dairesi'nin verdiği izinle birlikte hızla yaygınlaşan dronların 1917 yılında tarihteki ilk pilotsuz uçakla başlayan gelişimi ve günümüzde teknolojik yeniliklerle birlikte devam etmektedir. Bununla birlikte modern dronların hızla çoğalan kullanımı dünyayı hem sivil hem de askeri alanlarda daha çatışmalı bir yer haline gelmesi riskini de barındırmaktadır.. Bu husus, nükleer çatışmada MAD doktrininin aksine herhangi bir etkili çözüm bulunamayan ve evrensel düzeyde tanımlanamayan bir sorun alanı ortaya çıkarmaktadır. Makalede bu sorun kapsamında sırasıyla dronların neden oldukları güvenlik riskleri, mevcut anti-dron sistemleri ve anti-dron sistemleri pazarının durumu incelenmektedir.

Günümüzde geniş bir kullanıcı kitlesi, çeşitli boyut ve işlevlere sahip olan dronları hayatın birçok alanında kullanmaktadır. Dron kullanımının bu şekilde yaygınlaşması çeşitli riskleri de beraberinde getirmiştir. Günlük hayatta bu riskler kamu düzenine güvenliğe ve özel hayata yönelik olarak üç kategoride toplanmaktadır. 2018 yılı itibariyle yapılan ve bazıları gerçekleşen risk analizlerinde bu sistemlerin uçuş güvenliğinin riske atılmasında, kritik altyapılar ve hassas bölgelere saldırılarda, taşıdığı kameralar ve hassas mikrofonlar ve topladığı veriler aracılığıyla istihbarat elde edilmesi, özel hayatın

gizliliği ve kişisel verilerin korunması ihlallerinde kullanılabileceği değerlendirilmektedir.

Dronların askeri açıdan yarattığı risklere yönelik teorik tartışmaları 1990'lı yıllara gitse de esas olarak Suriye ve Irak'taki terör gruplarının saldırı amacıyla bu sistemleri kullanmasıyla gündeme gelmiştir. Suriye'deki terörist unsurlar ucuza mal ettikleri, uzun bir uçuş menziline sahip dronları kullanarak çeşitli saldırılar düzenlemişlerdir. Ülkemize de yönelik saldırı girişimleri mevcut olsa da 13 tane patlayıcı yüklü ve 100 km menzile sahip el yapımı dron ile Rusya'ya ait bir üsse yapılan saldırı dronların kullanıldığı en çarpıcı örneklerden biridir.

Dronlara karşı alınabilecek önlemleri değerlendirdiğimizde mevcut hava savunma sistemleri belirli bir büyüklükteki hava araçlarına yönelik olması sebebiyle yetersiz kalmaktadırlar. Alçak irtifada uçan hava araçlarına yönelik sistemler bulunsa da bunların çeşitli modifikasyonlara tabi tutulmadan dronlar için kullanılması mümkün değildir. Bu yeni tehdidin ortaya çıkardığı ihtiyaca yönelik geliştirilen hali hazırda 230'dan fazla anti-dron sistemi bulunmaktadır. Ancak bu sistemlerin hiç biri %100 koruma sağlamamaktadır. Bu sistemler kullandığı yöntemlere göre optik-kızıl ötesi sistemler, akustik sensörlü sistemler ve elektronik sistemler olarak üçe ayrılmaktadır. Ancak bu sistemlerin her birinin ciddi eksiklikleri bulunmakta ve sahada bazı durumlarda işlevsiz kalabilmektedirler.

Anti-dron sistemleri pazarına ilişkin elimizde son derece kısıtlı bilgiler bulunmaktadır. Bu pazara ilişki sunulan veriler sistemlerin etkilerine, kullanıldığı sektöre savunma açısından kullanımına, pazarın bölgesel olarak dağılımına ve pazardaki şirketlerin durumuna göre analiz edilmiştir.

Bu kapsamda etkinliğine göre yok edici sistemler en çok kullanılan ve pazarı en hızlı genişleyen sistemlerdir. Bu sistemlerin alıcıları incelendiğinde ise, en büyük payın devlet kurumlarına ve askeri kurumlara ait olduğu görülmektedir. Dron pazarına bölgesel olarak bakıldığında ise pazarın yarısından fazlasının ABD'ye ait olduğu görülmektedir. ABD'yi %25 ile Avrupa takip etmektedir.

Bu alanda faaliyet gösteren şirketlere baktığımızda ise yine ABD 62 şirketle ilk sırada bulunmaktadır.

Sonuç olarak hükümetler dronların takibine yönelik gerekli altyapıların kurulması için önlemler almalı ve gerekli düzenlemeleri yapmalıdırlar. Anti-dron sistemleri açısından ise tespit edip uzaklaştıran sistemler riski en aza indirmesi sebebiyle 5 yıllık süreçte pazar payında en fazla büyüme olacaktır. Ancak yerde kurulu sistemler veya elde taşınan sistemler yerine şirketler bu sistemlerin kullandığı müdahale yöntemlerine sahip avcı dronlar geliştirme yoluna gidecektir.

Bibliography

Articles

NİKOLİĆ, Slavimir S., An innovative response to commercial UAV Menace – anti-UAV Falconry, *VOJNO DELO, 4/2017,* http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2017-4/69-2017-4-14-Nikolic.pdf (Access Date:17.01.2019).

TØNNESSEN, Truls Hallberg, "Islamic State and Technology – A Literature Review", *Perspectives on Terrorism*, Vol. 11, No. 6 (December 2017), pp. 101-111.

Online Sources and News Web Sites

Agence France-Presse, "Drones becoming 'real' threat to commercial aviation: IATA",

Anti-Drone Website "Anti-drone system overview and technology comparison", https://anti-drone.eu/blog/anti-drone-publications/anti-drone-system-overview-and-technology-comparison.html (Access Date:17.01.2019).

ASHOK, India, "Drone crash: Rogue UAV knocks out power line causing widespread blackout", https://www.ibtimes.co.uk/drone-crash-rogue-uav-knocks-out-power-line-causing-widespread-blackout-1625876 (Access Date:17.01.2019).

BEEL, Joseph J., Anti-Uav Defense Requirements For Ground Forces And Hypervelocity Rocket Lethality Models", March 1992, Naval Postgraduate School, Monterey, California. http://www.dtic.mil/dtic/tr/fulltext/u2/a252727.pdf (Access Date:17.01.2019).

CLARKE, Colin P., "A Terrorist's Dream: How Twitter and Toy Drones Could Kill a Lot of People", https://nationalinterest.org/blog/the-buzz/terrorists-dream-how-twitter-toy-drones-could-kill-lot-26288 (Access Date:17.01.2019).

Dedrone Website, "Worldwide Drone Incidents", https://www.dedrone.com/resources/incidents/all (Access Date:17.01.2019).

Haber46 Website, “Anıtkabir töreninde drone paniği, askerler çekim yapan aracı vuracaktı”, https://www.haber46.com.tr/politika/anitkabir-toreninde-drone-panigi-askerler-cekim-yapan-araci-vuracakti-h116581.html (Access Date:17.01.2019).

HEGNARES, Jon, “The Past, Present And Future Of Anti-Drone Tech”, https://www.forbes.com/sites/forbestechcouncil/2018/01/26/the-past-present-and-future-of-anti-drone-tech/ (Access Date:17.01.2019).

HEIDEN, Rene Van Der, “NCI Agency helps protect NATO operations against drone attacks”, https://www.ncia.nato.int/NewsRoom/Pages/180529-Drone.aspx (Access Date:17.01.2019)

HENNİGAN, W.J., ”Experts Say Drones Pose a National Security Threat — and We Aren’t Ready”, www.time.com/5295586/drones-threat/ (Access Date:17.01.2019)

http://2016.mb.com.ph/2016/02/15/drones-becoming-real-threat-to-commercial-aviation-iata/#rbZIqrCDIsztMMKl.99 (Access Date:17.01.2019).

Hürriyet Daily News Website “PKK’s bomb-laden drone seized in Turkey’s east”, http://www.hurriyetdailynews.com/pkks-bomb-laden-drone-seized-in-turkeys-east-122299 (Access Date:17.01.2019).

Hürriyet Website, “Atatürk Havalimanı’nda Drone için tabelalı önlem”, www.hurriyet.com.tr/video/ataturk-havalimaninda-drone-icin-tabelali-onlem-122501 (Access Date:17.01.2019).

JOULİA, Antoine, Thomas Dubot ve Judicael Bedouet, “Towards a 4D Traffic Management Of Small UAS Operating At Very Low Level”, www.icas.org/ICAS_ARCHIVE/ICAS2016/data/papers/2016_0064_paper.pdf (Access Date:17.01.2019).

KELLY, Erin, “Venezuela drone attack: Here's what happened with Nicolas Maduro”, https://www.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/ (Access Date:17.01.2019)

KMIA, Oliver, “The Technical and Legal Challenges of Anti-Drone Systems”, https://fstoppers.com/aerial/technical-and-legal-challenges-anti-drone-systems-193666 (Access Date:17.01.2019).

MARTİN, David, “New Generations of Drones set to Revolutionize Warfare”, https://www.cbsnews.com/news/60-minutes-autonomous-drones-set-to-revolutionize-military-technology/ (Access Date:17.01.2019).

MİCHEL, Arthur Holland, “Counter-Drone Systems.”, Center for the Study of the Drone at Bard College, February 20, 2018, http://dronecenter.bard.edu/counter-drone-systems/ (Access Date:17.01.2019).

NCI Agency, “Notification of Intent to Invite Bids”, https://www.ncia.nato.int/Industry/Documents/NOI-IFB-CO-14685-UAS_Notification%20of%20Intent.pdf (Access Date:17.01.2019).

PR News Wire Website "Counter-Drone Market & Technologies – 2018-2023", published by Homeland Security Research Corp., https://www.prnewswire.com/news-releases/the-global-counter-drone-market-is-forecast-to-grow-at-a-2018-2023-cagr-of-37-2-300710320.html (Access Date:17.01.2019).