SECURITY THREAT SCENARIOS OF DRONES AND ANTI-DRONE TECHNOLOGY

Yeon-Jun Choi, Kwangju Women's University

ABSTRACT

In the past, drones were only used in the military field, but in the age of the 4th Industrial Revolution, they are used in conjunction with a commercial purpose such as GPS and video transmission where they operate with the integration of terrestrial devices. In addition, they are actively utilized in a diverse range of industries through the fusion with many cutting-edge technologies such as Artificial Intelligence(AI) and IoT(Internet of Things). Also, with the increase in the output of the drones' motor and battery and better performance coming from the miniaturization of them, they have provided a variety of benefits to society and at the same time, they are setting a new paradigm of living-style. However, with the increase in utilization of drones, which has made it more common-place than before to normal citizens, it has also lead to more attacks by dirty drones: we have come to the situation where we need to respond to the onslaught of drones in the field of security in order for the safety of society. As drones are becoming more advanced as time goes past, they are not limited to physical attacks, but instead, they carry out operations such as scouting and information theft. Therefore, this research suggests counter-measurements, utilizing the anti-drone technologies, for the security threat of drones through the analysis of security threat scenarios on illegal footage taking, spoofing and attacks through malicious code and physical attacks of drones.

Keywords: Drone, Drone Security, Security Threat, Threat Scenarios, Anti-drone.

INTRODUCTION

In the age of the 4th Industrial Revolution, drones have gone beyond the meaning of *"independent bodies"*, but they are rather developing as miniature aviation devices with the ability to be utilized in integration with terrestrial devices such as GPS and video transmission. Simultaneously, it is setting the paradigm for a new life style as it exceeds the limits of the current industry standards and keeps on advancing by positioning itself as a core technology that connects to other new ones. Drones were initially used with military purposes such as combat, offence, surveillance, taunt and antiaircraft, but in recent days the variations and functions of them have become more diverse with commercial purposes such as aviation pest control, extinguishing fires, disaster surveillance, aviation footage-taking and logistics transportation. The current trend is now the development of multi-purpose drones that could be used in every-day life which can be seen from the higher utilization rate in varying industries with the increased output in the motors and batteries along with their becoming more lightweight and a decrease in price.

However, with the rapid rise in the usage of drones and the boundary of their usage extending to normal citizens, attacks from dirty drones have increased and in the field of security, we have come to the point where we need to seriously consider the 'onslaught of drones' (Lee & Kang, 2019). The following are examples of security threat cases that involved drones: crashing of a drone on a nuclear power plant in France in March 2015, illegal flying of a

Citation Information: Choi, Y.J. (2022). Security threat scenarios o*f drones and anti-drone technology. Academy of Strategic Management Journal, 21*(1), 1-7.

drone at the Gatwick Airport in December 2018, bombing of the ARAMCO oil refining facility in Saudi-Arabia in September 2019 where the reality is that the safety of society is under threat as the threats are not limited to terrestrial facilities but extends to large-scale occasions or targets particular individuals such as a drone-attack on the attendance ceremony of the Venezuela president in August 2018, attack on the government army parade by the Yemen insurgent army using drones.

As it can be seen, it can be predicted that the security threat from the misuse of drones will increase with the upward curve on the usage of drones. In addition, the ever-evolving drones for offence-use are not limited to physical attacks only, but are now equipped with the functions of reconnaissance and disclosure of confidential information. Therefore, in preparation of the developing drone attacks, we have analyzed the security threat scenarios and suggest counter-measures that involve anti-drone technologies against the drone security threats.

LITERATURE REVIEW

The Definition of Drones

Drones- also known as Unmanned Aerial Vehicle (UAV)- can be defined as an aircraft without a pilot onboard and flies automatically or semi-automatically along a pre-programmed route on ground and has an automatic aviation device built into the aircraft (Park, 2015). The scope of UAVs- aircrafts that operates without on-board human control- differs slightly according to the definition, but according to the Unmanned Systems Roadmap issued from the United States Department of Defense, UAV are defined as aircrafts that are operate autonomously or remotely without a pilot on the actual aircraft which can carry weapons or normal cargo and is driven by a power source that is consumed once or can be re-used. Hence, ballistic aircrafts, cruise missiles, torpedoes, landmines, artilleries, satellites do not fall under the category of UAVs (Shin et al., 2020). In the case of South-Korea, drones are defined as unmanned aerial vehicles under the banner of ultralight aerial vehicles while at the same time they are unmanned power aerial vehicles with their body weight being under 150 kg without taking into account the weight of the fuel- according to article 5 of the Enforcement Rules of the Aviation Safety Act.

Classification of Drones

The method as to how drones are classified differs according to the standard that is used from the miniaturization and development of the devices as a result of the advancement in technology. The classifications can be divided according to their performance parameters such as flight radius, flight altitude, flight duration and size. Flight radius wise, close range drones are less than 50 km, short range drones fly from 50 km to 200 km, medium range drones are between 200 km and 650 km and 650 km to 3000 km for the long-distance drones. Grouping them according to flight altitude, low-altitude drones fly below 6,200 m, medium-altitude drones operate below 13,950 m while anything above that is considered high-altitude drones. According to flight duration, anything within 5 hours is a brief-flight drone, less than 10 horus makes it a short-flight drone, if it is between 10 and 30 hours then it is labelled as a medium-flight drone and anything that flies for an extended period of time is a long-flight drone. Sorting the drones according to size results in: miniature drones that are smaller than 15 cm, below 1.5 m makes it a sub-compact drone, smaller than 5 m is a compact drone, a medium-size drone is between 5 m and 10 m while a large-size drone is bigger than 10 m (Oh & Kang, 2018).

Security Threat Scenarios from Drones

Not only are drones equipped with cameras for aviation footage taking, but the necessary software for the exchange of information between the pilot and the drone for achieving various tasks is installed. This software allows network and radio communication which leaves the opening for different attacks in the case of malicious motivations of the pilot including the possibility of a hacker taking control of the drone. In addition, there have been villainous instances for being the starting point of IT attacks such as accessing the wireless network of the target without authorization through the drone or carrying out malignant actions via electromagnetic waves. In consideration of having entered the 4th Industrial Revolution, much more intelligent and advanced attacks are possible with the combination of AI and IoT technology with drones. Furthermore, inserting malicious code within the software that drones run on infects the subject and leads to information leakage. This can mean destruction of foundational facilities and serious repercussions for smart factories and smart cities where there are incorporations of technology from the 4th Industrial Revolution (Park et al., 2018). Security threats with the utilization of drones allows for easy attacks in numerous ways by swiftly driving the drone to the location of the target. Therefore, we have attempted to analyse the various security threat scenarios of drones.

Illegal Footage Taking

Incidents such as the *"Busan High-Floor Apartment Internal Illegal Footage Taking"* and *"Near-Incheon International Airport Illegal Footage Taking"* are indications that illegal footage taking via drones occur frequently. The indiscriminate illegal footage taking via drones do not only infringe the privacy in everyday-life and the publicity rights-also known as *"portrait rights"* in South-Korea- but also creates the problem of internal illicit surveillance. reconnaissance, information leakage of internal data in the access control areas such as the major national facilities (Kim, 2018). It is a challenge to detect the smaller sized drones such as the miniature drones when one is not on an active lookout for it and with the immergence of drones with the appearance of small insects or other small objects, the danger of privacy violation and disclosure of confidential information is on the rise (Park, 2015).

Spoofing and Malicious Code Assaults

Spoofing means to deceive and it is a type of attack where it modifies the access control by pretending to be a valid user and deluding the system and the network. Hackers, being ill-willed, attempt a spoofing attack on the drones and makes them mistake their location so that the hacker is able to fly and land the drones at places. such as no-flight zones. as the hacker wishes, thereby disclosing the drones' information (Kim et al., 2020). They also utilize the drones as a hacking tool by infecting the drone's software with malicious code so that they can hijack and incapacitate them. The drones will then be able to give out malicious commands to cause system failures which then causes a freeze in network communication. A security threat also exists with the interception of the remote control commands and the collection and leakage of the information from it (Cho & Seo, 2020).

Physical Assaults

Initiating physical attacks on the foundational facilities and targets by using the drones itself is one of the methods of assault. Physical attacks from drones equipped with firearms, explosives, biological weapons or radioactive materials have easy access, and incidents continue to occur through the world because of their extensive effectiveness (Kim & Shin, 2020). With the increased output of the drones' motors and batteries along with their becoming lighter and smaller- not to mention their getting more affordable- it is now easier to obtain them and actively utilize them for physical attacks. Also, it is extremely difficult to detect them if the light-weight and small drones were to approach at a fast pace from a high altitude which compounds to the challenge of defending in midair since the attacks also happens within a short time-frame. Therefore, it can be said that there is the necessity for effective counter-measurements (Shin et al., 2020).

Anti-Drone Technologies

Anti-drone is a concept that encompasses the technology and the diverse range of methods used from it in order to detect, identify and incapacitate the illegal drones with the purpose of preventing and countering the crime and terrorism from them where the methods can be classified as either *"passive"* or *"active."* A passive method does not consort to physical methods to neutralize the drones, but instead regulates the usage of drones through the legislation and involvement in the process of their production. An active method involves neutralizing the illicit drones that have entered unauthorized areas through physical or technological methods.

Passive Methods

Geo-fencing technology

Geo-fencing technology stops the drones from approaching specific areas by establishing 'no-flight zones'. This is achieved by entering the restricted zones onto the GPS- thereby setting up a virtual fence- and then the drones are software-locked during the design and production stage where the flying of drones in specific locations are forestalled through the pre-entered GPS values of the no-flight zones. Geo-fencing technology provides a primary method of control over a wide area making it highly useful. However, the legal obligation for geo-fencing technology is not in place in South-Korea and it has the characteristic of not being compulsive since the blockade from it can be bypassed through illegal modifications of the software lock (Jung & Chun, 2021).

Management and restriction through legislation

With regards to the management and restrictions of drones through the legislation, there needs to be an effective reform about the illegal flying, illegal footage-taking and physical assaults from drones. In order to resolve the constant security threat of drones, South-Korea is preparing the necessary legislation in accordance to the flying of drones from the perspective of national security through the Aviation Safety Act and the National Intelligence Service Act in addition to implementing the policy of *"Drone Registration System."* However, a management structure for a more methodical aviation system needs to be in place. By analyzing the management and restrictions that countries such as America and China have in place, we need to respond to the various security threats with improvements in the following areas: registration system of drones, verification of the safety of them, restriction on the altitude, location and speed of aviation (Im & Choi, 2021).

Active Methods

Drone apprehension

Apprehending and incapacitating drones that have approached the access control areas minimizes secondary accidents and human damage where the two main methods are using nets or utilizing eagles. For the method of apprehension by firing nets on-ground or from drones, the Skywall 100 net-firing gun from OpenWorks Engineering in Britain exists (Unmanned Systems News, 2016), while the Drone Interceptor MP200 that Malou Tech in France invented uses drones for net-apprehension (Moseman, 2015). This method allows for the log record analysis of the captured drones thereby being able to identify the operators. However, there is a limit to the distance the nets are able to reach when they are fired from ground while the difficulty of hitting drones moving at high speed with a net-firing gun attached to the controlled drone also exists. Moreover, the results of utilizing eagles for the apprehension of drones vary significantly depending on the level of training they had received while also they are able to apprehend only light-weight drones in danger of injury from the propellers (The Telegraph, 2016).

Electromagnetic wave interruption of drones

Neutralizing drones that approach access control areas through electromagnetic wave interruption is done with jamming technology where the drones are denied of the waves they need for operation-use. Two leading examples in this area are electromagnetic wave interruption devices and drone guns. Jamming technology involves the discharge of interruptive electromagnetic waves at the 2.4 GHz Industrial Scientific Medical spectrum- necessary for receiving the control signals for the flying of drones- and the Global Navigation Satellite System spectrum- allowing for the receiving of the altitude and location. The Jammer, developed by Dedrone, is a device that releases electromagnetic waves so that the connection between the pilot and drone is lost when it comes within the area-of-effect (Atherton, 2016). A single device such as this has the characteristic of being able to deny the entrance of multiple drones in access controlled areas thereby providing a means of control and prevention in large-scale which makes it a suitable method for nuclear-related facilities and airports. Another method of using drone guns- such as the Drone Defender, developed by Battelle in America, or the DroneGun MKIII by DroneShield, neutralizes the drones by firing electromagnetic wave noise at the spectrum needed for information communication. It has the advantage of being convenient like normal firearms and the ones equipped with the latest technology even has the trait of preventing unauthorized drones from returning to their take-off zone by blocking the GPS (Choi, 2016).

CONCLUSION

There is no doubt that drone technology, being the forefront of the 4th Industrial Revolution, will be more actively implemented in various sectors of society through the amalgamation of other latest technologies such as AI and IoT and with the sustained increase in performance, a diverse range of benefits will be brought to society. As it can be seen, drones are evolving in different areas of the industry and they are developing as a technologically, conventional platform, but since they have become common-place for everyday users, the safety of society is under threat from the dirty drones' assault. From an offensive perspective, drones are a feasible method of assault which is why a wide spectrum of security threats have occurred such as illegal footage taking, spoofing, malicious code and physical attacks.

A more active research than before on anti-drone technologies needs to be conducted in order for the pertinent measurements against the different security threats from drones. In addition, guidelines for the response measures with regards to the management and restrictions on illegal drones as well as anti-drone systems needs to be established. Once the guidelines have been set-up institutionally, the relevant facilities need to implement the anti-drone facilities so that they are able to respond effectively to the security threats of drones in a physical and technical manner.

Henceforth, one needs to be conscious of the up-coming drone security threats such as illegal footage taking, spoofing, malicious code and physical attacks with the emergence of drone technology. On top of that, under the analysis of security threat scenarios, passive methods such as geo-fencing technology, management and restrictions through legislation as well as active methods such as drone apprehension and electromagnetic wave interruption of drones should be utilized in response to the security threats from drones so that derivative crimes and terrorism could be effectively prevented and countered.

REFERENCES

Atherton. (2016). Airbus partners with anti-drone startup popular science. Retrieved from: http://www.popsci.com/airbus-partners-with-anti-drone-startup

Cho, S.M., & Seo, S.H. (2020). Status of cryptographic technology applied to drone security. *Review of KIISC, 30*(2), 11-19.

Choi, H.H. (2016). Anti-drone technology detection, which has become important for security beyond facility security: Development of various technologies from stealing control to shooting down. *Defense & Technology*, 451, 38-45.

Im, D., & Choi, Y.J. (2021). Counter measures on drone terrorism and cyber terrorism in national important facilities in the era of the fourth industrial revolution. *Korea Terrorism Studies Review, 14*(2), 108-123.

Jung, J.Y., & Chun, Y.T. (2017). A study on the trend of anti-drone technologies and their applications, *Korean Security Journal,* Drone special issue, 33-55.

Kim, M. S. (2018). A study on regulation reform for the safe operation of drone and the privacy protection. In *Legislation Forum* 188-221.

Kim, M.S., You, I.S., & Yim, K.B. (2020). Trends in analyzing vulnerabilities and responding technologies of unmanned vehicle drones. *Review of KIISC, 30*(2), 49-57.

Kim, S. I., & Shin, J. (2020). A study on the countermeasures against the threats of small-scale inertia using the M&S. *Convergence Security Journal*, *20*(1), 77-84.

Lee, D., & Kang, W. (2019). A study on the establishment of anti-drone concept and effective response system. *Korean Security Journal, 60,* 9-31.

Moseman, A. (2015). This drone interceptor captures your pathetic puny drone with a net. Retrieved from http://www.popularmechanics.com/flight/ drones/a14032/francedispatches–a-net-carrying-bully-drone-to-catch/

Oh, I.S., & Kang, C.G. (2018). *Unmanned multi-copter drone pilot textbook.* Bogdoo, Seoul.

Park, J.H. (2015). *Drone unmanned aerial vehicle operation theory*. Goldenbell, Seoul.

Park, K.S., Cheon, S.P., Kim, S.P., & Eom, J.H. (2018). Security threats and scenarios using drones on the battlefield. *Convergence Security Journal*, *18*(4), 73-79.

Shin, J.H., Oh, I.S., Kang, C.G., & Kim, K.W. (2020). *An introduction to drone*. Bogdoo, Seoul.

The Telegraph. (2016). French Air Force turns to eagles to fight terror drone threat. Retrieved from: http://www.telegraph.co.uk/news/2016/11/18/french-air-force-turns-to-eagles-to-fight-terror-drone-threat

Unmanned Systems News (2016). OpenWorks engineering announces skywall drone capturing technology. Retrieved from: http://www.unmannedsystemstechnology.com/2016/03/open works-engineering-announces-skywall-drone-capturing-technology/