ANALYSIS

ERROR 404: DRONE NOT FOUND SMARTPHONES AS UNMANNED AERIAL VEHICLE GROUND CONTROL STATIONS: AN OVERVIEW OF CYBER-RELATED VULNERABILITIES

GINEVRA FONTANA

Master's Student in International Security Studies at Scuola Superiore Sant'Anna & University of Trento. Selected Student at Collegio Clesio. Collaborator at the Center for Cyber Security and International Relations Studies of the University of Florence. Particularly interested in Armed Conflicts, Cybersecurity, Arms Trade and Terrorism Studies.

1. Introduction

The US Army began utilising Unmanned Aerial Vehicles (UAVs) in the 1980s. At the time of writing, it owns an extensive array of more than 7,000 of such devices – and seems set on acquiring many more in the future.

Reports from 2016 suggest that the US Army considered purchasing commercial off-the-shelf UAVs for intelligence, surveillance and reconnaissance (ISR) purposes. As such devices are usually controlled with a smartphone or a tablet, this article tries to answer the question of what cybersecurity threats such controllers bring into the picture, and how some of these vulnerabilities could be solved.

2. Framing the current situation

Unmanned Aerial Vehicles, commonly referred to as *drones*, are a specific type of technological device that, as the name suggests, is a flying robot that is either controlled by a human operator at a distance or is completely independent (Pullen, 2015). The latter typology is still undergoing implementation, but the former has been increasingly tested and used by military agents throughout the past decade. The technology grew more and more accessible, giving way in the past five years to a spill-over effect into the civilian market (Hsu, 2017). Especially when it comes to UAVs used for filmography and videography purposes, the costs became more and more approachable, therefore bringing an increase in their usage (Glaser, 2017).

The US army has used UAVs for ISR since the 1980s (Springer, 2013). At present, the US operate various types of UAVs in war zones: they have a fleet of more than 7,000 remotely piloted aircraft (RPA). A few hundred of these are the infamous MQ-1 Predator and its descendant, the MQ-9 Reaper (Walker, 2017). Used for both ISR and strikes in areas such as Iraq, Pakistan and Afghanistan, these UAVs have come under fire in the public opinion for the discrepancy between the official narrative and the actual outcome of their strikes. In fact, according to various sources, including official ones, Predator and Reaper strikes are not as effective and 'surgical' as they have been portrayed, causing numerous civilian deaths (Chamayou, 2014; Stanley, Fontana & Duraccio, 2017).

The US army has used UAVs for ISR since the 1980s. At present, the US operate various types of UAVs in war zones: they have a fleet of more than 7,000 remotely piloted aircraft. A few hundred of these are the infamous MQ-1 Predator and its descendant, the MQ-9 Reaper.

Although Predators and Reapers are the most talked about, the majority of the US UAV fleet consists of drones primarily used for ISR purposes. Among these, the most numerous are the RQ-11 Ravens, which are more than 7,000 units (Thompson, 2011; Air Force Technology, n.d.). Nonetheless, there has recently been a new addition to the catalogue.

In May 2016, an article published in the online magazine Popular Mechanics mentioned how the US armed forces were looking for new small UAVs (Hambling 2016). Particularly important were a few key elements:

The specifications also demands [sic] a drone that can be readied and launched in less than 60 seconds, from the prone position or under cover. This is in contrast to the Raven, which takes a few minutes to assemble and needs to be thrown into the wind – not so easy when you are under fire. (Hambling 2016)

Moreover, these UAVs needed to be easily operable in enclosed spaces, such as buildings, for ISR—an ability that the ones concurrently owned by the US armed forces did not have (Hambling, 2016).

In January 2017, Wired magazine first reported that the US Marine Corps were considering buying off-the-shelf UAVs to be used in the military field, especially for future 'urban reconnaissance'. More specifically, the article indicated Commandant Robert Neller's will to provide 'every deployed Marine infantry squad to have their own [UAV] for aerial reconnaissance by the end of 2017' (Hsu, 2017).

Off-the-shelf UAVs are usually operated via smartphone or tablet. I have, therefore, decided to analyse the issues that using such technologies to operate UAVs would bring into the mission from the cybersecurity perspective.

Unmanned Aerial Vehicles: the basics

Understanding the susceptibilities of UAV systems requires a general explanation of how these systems work. Figure 1 shows a simplified model of the basic elements of a UAV.

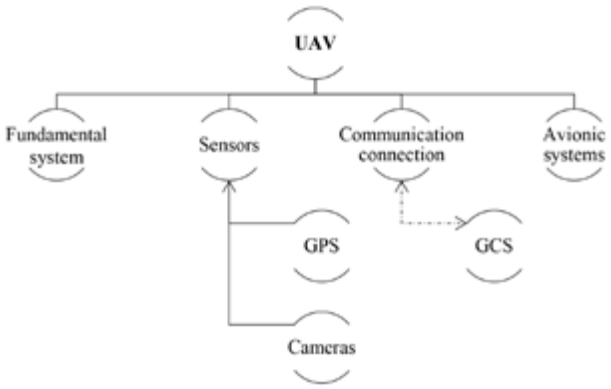

Figure 1. Simplified model of the basic elements of a UAV

The ***fundamental system*** connects all UAV elements: as Hartman and Steup (2013) effectively said, '[i]t may be considered an UAV "operating system"'. By controlling the other elements, the fundamental system permits the incorporation of other components; for instance, ISR UAVs' *sensors* usually include cameras and GPS (Hartman & Steup, 2013).

Avionic systems include all elements contributing to flight capability and allow the received commands to be translated into effective directives for the functioning of e.g. the engine (Hartman & Steup 2013).

The ***communication connection*** in UAVs can be, for evident reasons, wireless only. Hartman and Steup (2013) classified it into two categories: 'a) direct, line-of-sight (LOS) communication and b) indirect – mostly – satellite communication (SATCOM)'. For the purposes of this article, I am later going to focus more on the former case, as it is the one used most often in off-the-shelf lightweight UAVs.

Although some newer UAV models can operate autonomously, small offtheshelf lightweight UAVs are manoeuvred by an operator, which requires a Ground Control Station (GCS). Figure 2 shows a simplified model of the basic elements of a GCS.

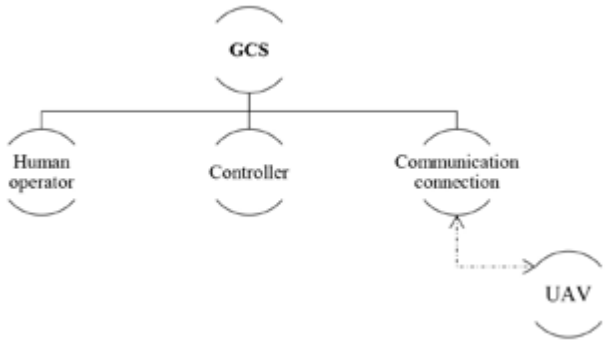

Figure 2. Simplified model of the basic elements of a GCS

The *communication connection* is, as previously mentioned, always wireless in the case of UAVs, and small off-the-shelf lightweight ones are no exception.

Originating from Hartman and Steup's (2013) graphs, I have extrapolated a threeelement GCS model that underlines the importance of the *controller*. In the case of off-the-shelf lightweight UAVs, the controller—usually a smartphone or a tablet—is the most important and, at the same time, vulnerable ring of the chain, alongside the communication connection.

3. Communication connection vulnerabilities

From an attacker's point of view, the communication connection, being wireless, is the element that is the most difficult to safeguard. It is composed of two flows: a bidirectional one between the UAV and the GCS, and a unidirectional other between the environment and the sensors (Hartman & Steup, 2013). These links can be exploited in various ways.

From an attacker's point of view, the communication connection, being wireless, is the element that is the most difficult to safeguard. It is composed of two flows: a bidirectional one between the UAV and the GCS, and a unidirectional other between the environment and the sensors.

Because Hartman and Steup (2013) analyse the communication connection indepth, I would only like to drive the reader's attention towards the aforementioned LOS communication. This communication can be implemented under either C-band or Wi-Fi. Both systems utilise omnidirectional antennas (Hartman & Steup, 2013), and are, therefore, more exposed to eavesdropping, especially if the communication is not encrypted. This was the case in 2009, when a terrorist group used a $26 program, called *SkyGrabber*, to record the video feed off of a US UAV (Gorman, Dreazen & Cole, 2009; Javaid et al., 2012), which had not been encrypted even though the vulnerability had been known to the US armed force for a long time (Arthur, 2009).

4. GCS: controller vulnerabilities

The US army considering buying off-the-shelf UAVs brings about a whole new set of problems that had never been previously tackled in the military field: the security of the smartphones and tablets used to control said UAVs. Since the two most popular smartphone OSs, which I will analyse in the following paragraphs, Apple iOS and Google Android, are also used for tablets, and considering that the related issues are exactly the same as in the case of tablets using a Wi-Fi + cellular line, I am going to only use the term *smartphone* for the sake of brevity from now on.

The US army considering buying off-the-shelf UAVs brings about a whole new set of problems that had never been previously tackled in the military field: the security of the smartphones and tablets used to control said UAVs.

4.1. Why commercial smartphones?

BlackBerry phones used to be the go-to device for government workers in many US departments and in the U.K., as they had scored the highest security accreditation. But in 2012, the British government dismissed them in favour of its competitors, Apple and/or Samsung devices (Dalton, 2012), whereas different US governmental agencies moved to either Apple (e.g. the Immigration & Customs Enforcement (Ribeiro, 2012)) or Google Androidrunning devices (e.g. the US Army (Milian, 2012)).

As with off-the-shelf UAVs, commercial devices usually exemplify the most cutting-edge technologies, with the added value of the government not having had to invest considerable sums for their development (Mansfield et al., 2013; Hsu, 2017). Moreover, using mass-market smartphones would be a cost and timeeffective choice, as soldiers are already familiar with the devices if they use similar ones in private (Mansfield et al., 2013).

Using commercial smartphones as GCS for off-the-shelf, lightweight UAVs in ISR missions could bring both advantages and disadvantages. These pocketsized devices mean that a single soldier can operate the UAV without needing the support of a comrade, hence making utilisation easier in hightension missions, e.g. if the soldiers are under fire or are conducting a surprise operation at night-time. On the other hand, smartphone screens are smaller than a regular laptop's, possibly making all information (realtime images, avionic stats and location, just to name a few) cramped (Mansfield et al., 2013).

Using commercial smartphones as GCS for off-the-shelf, lightweight UAVs in ISR missions could bring both advantages and disadvantages. These pocketsized devices mean that a single soldier can operate the UAV without needing the support of a comrade, hence making utilisation easier in hightension missions.

4.2. Vulnerabilities

The GCS is fundamental for the ISR missions, as it is not only the controller used to manoeuvre the UAV, but acquires data (in the form of images and videos), as well. By targeting the smartphone used as GCS, the attacker can jeopardise the mission itself. In order to do so, attackers can either acquire control of the GCS, or render it inoperative, even creating a denial of service. Fruitful attacks can be performed through communication network, hardware and/or software.

4.2.1. Communication Network

Using a smartphone as a GCS necessitates a communication network. As Mansfield et al. (2013) argue, wireless networks in war zones are set up with a stationary base station, which is a tempting target. Making it inoperative equals making the communication network inoperative, as well. In such cases, the soldiers could resort to unsafe civilian networks. Moreover, loss of the communication network can damage, if not disrupt, communication between the GCS and the UAV, making the device uncontrollable as well as allowing for data loss or dispersion, hence jeopardising the mission.

Threats to the communication network include network eavesdropping, spoofing, denial of service and jamming. (Mansfield et al. 2013)

Eavesdropping is the practice of capturing packets of data transmitted over the network and deciphering them (Mansfield et al., 2013). Spoofing consists in the transmission of manipulated data through a network, the access to which has been gained using false credentials (Tippenhauer et al., 2011; Mansfield et al., 2013). Denial of service (DOS) attacks hamper transmission of information between networked agents (Kwon, Liu & Hwang, 2013). In its most primitive form, jamming consists in causing a loss of signal (Giray, 2013)[1].

1 I would like to briefly draw attention to the fact that US Marines, as well as other armed forces around the world, have been reportedly equipped with jammers for at least a couple of decades (Schmitt, 1995; Mihelic, 2007; Rogoway, 2014; Military Aerospace Electronics, 2016; US Marine Corps, 2016).Analysing the use of such devices and their impact on UAVs operated by the same actors would far exceed the scope of this article, and is therefore left to further research to be conducted separately, AN.

Communication network vulnerabilities are for the most part solvable through bandwidth allocation and encryption (Mansfield et al., 2013). Bandwidth allocation consists in limiting network access requests to avoid multiple or excessive requests (Guérin, Ahmadi & Naghshineh, 1991; Mansfield et al., 2013). Encryption is the process by which information is codified, so that only authorised agents can decipher it (Skoudis, 2009; Mansfield et al., 2013).

4.2.1.1. Hardware

Smartphones and sensors inside them can be infected by malware software. The malware can enter the device through vulnerabilities in the OS's software or applications; there also exists a risk of malicious software being installed on these devices during the supply chain, which is particularly troublesome to inspect in today's era of transnational companies (Mansfield et al., 2013).

Understandably, the presence of such malware can jeopardise missions and put the soldiers' lives in danger. For instance, by infecting the smartphone's GPS system, the enemy could track the troops' movements, and therefore attack them when they are least expecting it, or provide them with false information.

Mansfield et al. (2013) identify other possible attacks that could impede the correct utilisation of the smartphone as a GCS; among these, I would like to highlight flooding, the practice of overwhelming the device with calls and messages, so that the system is overloaded and/or the human operator is unable to operate the UAV anymore; and battery exhaustion attacks, by means of which the GCS's battery drains exceedingly fast compared to normal battery capacity.

By infecting the smartphone's GPS system, the enemy could track the troops' movements, and therefore attack them when they are least expecting it, or provide them with false information.

An easy way to protect the hardware would be to utilise anti-virus software, which is designed to detect and remove malware immediately.

In war zones, smartphones could more easily fall into the hands of the enemy, thus giving access to information stored on the device. Two solutions to this problem could be the use of passwords and that of encryption, although both can impact the immediacy of use during missions (Mansfield et al., 2013).

4.2.1.2. Software

The OS is the inner foundation of the smartphone, as it controls hardware, sensors and software applications. The enemy, by infiltrating the OS, can acquire complete control over the device and proceed to infiltrate hardware and software applications. This includes acquisition of location, videos and images, as well as conversations (Mansfield et al. 2013). Since the software apps are used to manoeuvre the UAV, accessing them puts the UAV in the hands of the enemy.

As Mansfield et al. (2013) pointed out, smartphones are now vulnerable to the same threats as computers. Alongside the previously-mentioned malware, the software can be infected by viruses such as the 'keylogger' that infected the US UAV fleet's operating computers in a Nevada base in 2011, which registered every tapped key on the keyboard, therefore storing passwords as well (Lawrence 2011; Shachtman 2011).

Below, I will proceed by briefly analysing the three most popular smartphone OSs in light of their application as GCSs in military operations: BlackBerry, Apple iOS and Google Android.

4.2.1.3a. BlackBerry

As explained in the 'Why commercial smartphones?' section, BlackBerry phones were the go-to devices for governmental forces up to 2012, when they lost their position to Apple iOS and Google Android. Even though BlackBerry's devices had been given the highest level of security clearance, and were, therefore, fit to handle classified documents safely (Ribeiro 2012), they were outraced in the technological competition and fell behind. BlackBerry's spot was not single-handedly won by either of its two main competitors: Apple iOS and Google Android

both scored contracts with different US authorities and departments (Kerr, 2012; Milian, 2012; Ribeiro, 2012).

Nonetheless, it may be too soon to carve BlackBerry's epitaph in stone: in 2017, the company won the right to sell its tools to make phone calls and text messages secure through encryption to the US government (Sharp, 2017). So far, however, BlackBerry is still struggling behind its two largest competitors: Apple iOS and Google Android.

4.2.1.3b. Apple iOS

Apple iOS is Apple's unique OS. All updates and alterations to the OS are supervised and executed by the company itself, which allows for reinforced security of devices. On the other hand, all software applications running on Apple iOS need to undergo an App Review, which involves a thorough check and approval by Apple developers (Apple, n.d.). Another limitation involves applications being available only through the Apple store.

Although its devices are used by US governmental agencies, such as the ICE and the Defense Department (Kerr, 2012; Ribeiro, 2012), Apple has been on cold terms with the US government ever since it refused to unlock the San Bernardino shooter's iPhone (Holpuch, 2016; Lichtblau and Benner 2016). If this is considered alongside the difficulty that the US military would have in trying to customise Apple iOS-running products, it comes as no surprise that the Army has been apparently leaning more towards Google Android-running devices.

4.2.1.3c. Google Android

The most popular OS, Google Android's software code is available to the public in order to permit customisations – yet, this liberty equals a downfall in security. Software updates are not as consistently implemented as by Apple, since the customisations have resulted in innumerable variations of the OS itself (Mansfield et al., 2013).

Software applications are available through Google Play, Android's equivalent of the Apple Store, as well as through applications created by developers outside the company. Although developer's responsibility is in force, applications do not undergo the same scrutiny as in Apple iOS, therefore allowing malicious software to enter the Android sphere undisturbed. In order to tackle this vulnerability concerning both OS and software apps, regular updates seem to be the easiest and most costeffective solution (Mansfield et al. 2013).

I would like to hereby suggest that the possibility to easily customise this OS, even though it is the cause of its major vulnerabilities, is also its major strength.

Already in 2011, the US Army began testing a modified version of Google Android in order to make it secure enough to handle classified documents (Milian, 2012).

In 2015, the Army's Experimentation Force tested a Samsung Galaxy II-based system: the Nett Warrior Future Initiative, which was a 'special software package' (Cox, 2015). This was also the first time that the InstantEye UAS (Unmanned Aircraft System, a USonly synonym of UAV) was mentioned, as the article states:

"[…] Nett Warrior Future Initiative is equipped with a special software package […] [s]o a platoon leader can share […] video streams from a company-level Raven UAS and a platoon-level *InstantEye UAS* with his squad leaders." (Cox 2015, emphasis added)

5. InstantEye: the game-changer?

The following year, an article mentioned that, among other UAVs, the InstantEye had been tested by the Army (Hambling, 2016; InstantEye, Robotics 2016). In February 2018, it became official: the US Marine Corps purchased 800 quadcopters from InstantEye Robotics (InstantEye Robotics, 2018) in order to realise what Commandant Robert Neller had envisioned in 2017 (Hsu, 2017). The company worked with the Navy and the Marines to develop the best device for the soldiers' needs (InstantEye Robotics, 2018).

The characteristics of the InstantEye Mk-2 GEN3-A0, the most affordable product from the InstantEye range, include: all-weather and day/night functioning, the possibility

for a single operator to launch it in circa 30 seconds, a twokilometre line-of-sight (LOS) video range, and an endurance of up to 30 minutes (InstantEye Robotics, n.d. a; n.d. b). Moreover, with both UAV and GCS weighing little more than two kilograms (the UAV and the GCS weigh respectively 1.2 and 3.4 lbs (InstantEye Robotics, n.d. b)), it is light enough to be carried by soldiers in their backpacks.

From the GCS's vulnerabilities perspective, it is unknown whether the GCS is a smartphone or a tablet, and if the system runs a modified version of a commercial OS or a specifically-developed one. This is to be expected, as sensitive information such as what OS the GCS is running could compromise the safety of the missions, as I argued previously.

From the GCS's vulnerabilities perspective, it is unknown whether the GCS is a smartphone or a tablet, and if the system runs a modified version of a commercial OS or a specifically-developed one.

Nonetheless, the company has made the following facts public:

The InstantEye Mk-2 GEN3-A0 utilizes a hybrid communication with encrypted, digital link for C2[2] and an analog video link. The aircraft does not store any data onboard, and therefore, there is no data at risk if the aircraft is lost. (InstantEye Robotics n.d. a)

Following my previous analysis, it is clear that the US Marines have solved a few of the afore-mentioned possible problems. First and foremost, the UAV communicates with the GCS via an encrypted connection, substantially disrupting any chance of easy eavesdropping. Moreover, the fact that apparently there is no data storage on board eliminates the threat that, were the UAV to fall in the hands of the enemies, it could provide them with valuable information.

Regardless, I would argue that the analogue video link between the UAV and the GCS should be further analysed in order to rule out potential eavesdropping threats. Because further details on this link are unavailable at the moment, and because this analysis would far exceed the object of this article, I will limit myself to pointing it out.

6. Conclusions

The US Army has utilised drones for ISR purposes since the 1980s. At the moment of writing, its UAV arsenal surpasses the 7,000 devices. Yet, the rush towards using such devices will apparently not end any time soon.

In 2016, it was announced that the US Army was considering buying offtheshelf UAVs: to keep up with the developing technology, it seemed best to tap into the ever-growing civilian market. However, because commercial UAVs are often operated through smartphones or tablets, this introduced an entirely new set of vulnerability variables into the picture.

In February 2018, it was announced that the US Navy would purchase 800 InstantEye UAVs for ISR purposes, so as to virtually supply each Marine infantry squad with one. I therefore argued that such a choice, based on the information available at the moment of writing, seemed to be the best solution to prevent most of the previously-mentioned cybersecurity threats. Nevertheless, I would suggest that further research into the InstantEye in-depth specifications, whether and whenever they become official, should be more thorough and complete. Specifically, I would suggest researching the analogue video link that connects the InstantEye UAV to its GCS, as well as the GCS's specifications. ■

2 Command and control.

REFERENCES:

Air Force Technology. (n.d.). *RQ-11B Raven Unmanned Air Vehicle (UAV)*. Retrieved from: https://www.airforce-technology.com/projects/rq11braven/ [Accessed February 2018]

Apple. (n.d.). *App Review*. Retrieved from: https://developer.apple.com/app-store/review/

Arthur, C. (2009). SkyGrabber: the $26 software used by insurgents to hack into US drones. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked

Chamayou, G. (2014). *Teoria del drone. Principi filosofici del diritto di uccidere*. Roma, Derive Approdi.

Corrigan, F. (2018). How Do Drones Work and What Is Drone Technology. *DroneZon*. Retrieved from: https://www.dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/

Cox, M. (2015) Soldiers Embrace Smartphone-Based Kit. *Military.com*. Retrieved from: https://www.military.com/kitup/2015/03/soldiers-embrace-smartphone-based.html

Dalton, W. (2012) RIM's BlackBerry phones may lose public sector monopoly. *ITProPortal*. Retrieved from: https://www.itproportal.com/2012/08/24/rims-blackberry-phones-may-lose-public-sector-monopoly/

Elnaggar, M. et al. (2017). Online Control Adaptation for Safe and Secure Autonomous Vehicle Operations. *NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*. Retrieved from: http://ieeexplore.ieee.org/document/8046365/

Giray, S. M. (2013). Anatomy Of Unmanned Aerial Vehicle Hijacking With Signal Spoofing. *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, Istanbul, 2013, pp. 795-800. Retrieved from: http://ieeexplore.ieee.org/document/6581320/ [Accessed January 2018]

Glaser, A. (2017). DJi is running away with the drone market. *Recode*. Retrieved from: https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast [Accessed December 2017].

Gorman, S., Dreazen, Y. J., Cole, A. (2009). Insurgents Hack US Drones. *The Wall Street Journal*. Retrieved from: https://www.wsj.com/articles/SB126102247889095011 [Accessed November 2017].

Guerin, R., Ahmadi, H. and Naghshineh, M. (1991). Equivalent capacity and its application to bandwidth allocation in high-speed networks. *IEEE Journal on Selected Areas in Communications*, vol. 9, no. 7, pp. 968-981, Sep 1991. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=103545&isnumber=3202 [Accessed February 2018].

Hambling, D. (2016). The US Army Wants Tiny Flying Eyes for Every Footsoldier. *Popular Mechanics*. Retrieved from: https://www.popularmechanics.com/military/research/a20862/the-army-wants-tiny-flying-eyes-for-every-footsoldier/ [Accessed December 2017].

Hartmann, K. & Steup, C. (2013). The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. *2013 5th International Conference on Cyber Conflict*. NATO CCD COE Publications, Tallinn. Retrieved from: http://ieeexplore.ieee.org/document/6568373/ [Accessed January 2018]

Holpuch, A. (2016). Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties [Accessed February 2018]

Hsu, J. (2017). The Military May Soon Buy the Same Drones You Do. *Wired*. Retrieved from: https://www.wired.com/2017/01/military-may-soon-buy-drones-home/ [Accessed December 2017].

InstantEye Robotics (2016). *InstantEye in the News*. Retrieved from: https://instanteyerobotics.com/uncategorized/national-defense-marine-corps-experimenting-with-new-drones/ [Accessed February 2018].

(2018). United States Marine Corps Orders 800 InstantEye Systems. Retrieved from: https://instanteyerobotics.com/uncategorized/united-states-marine-corps-orders-800-instanteye-systems/

(n.d. a) *InstantEye Mk-2 GEN3*. Retrieved from: https://instanteyerobotics.com/products/gen3/

(n.d. b) *InstantEye Mk-2 GEN3-A0 sUAS Specification Sheet*. Retrieved from: https://instanteyerobotics.com/wp-content/uploads/2017/11/InstantEye-Mk-2-GEN3-A0-v2.3-11-20-17.pdf

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., Alam, M. (2012). Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2012, pp. 585-590. Retrieved from: http://ieeexplore.ieee.org/document/6459914/

Javaid, A. Y., Sun, W., Mansoor, A. (2013). UAVSim: A Simulation Testbed for Unmanned Aerial Vehicle Network Cyber Security Analysis. *Globecome 2013 Workshop – Wireless Networking and Control for Unmanned Autonomous Vehicles*. Retrieved from: http://ieeexplore.ieee.org/document/6825196/

Kwon, C., Liu, W., Hwang, I. (2013). Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks. *2013 American Control Conference (ACC)*. Retrieved from: http://ieeexplore.ieee.org/document/6580348/

Lawrence, C. (2011). Virus infects program that controls US drones. *CNN*. Retrieved from: http://edition.cnn.com/2011/10/10/us/drone-program-virus/index.html [Accessed December 2017].

Lichtblau, E. and Benner, C. (2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Retrieved from: https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

Karpowicz, J. (2018). 8 Commercial Drone Predictions for 2018. *Commercial UAV Expo*. Retrieved from: https://www.expouav.com/wp-content/uploads/2017/12/8-Commercial-Drone-Predictions-for-2018.pdf

Kerr, D. (2016). Defense Department drops exclusive contract for BlackBerry. *CNET*. Retrieved from: https://www.cnet.com/news/defense-department-drops-exclusive-contract-for-blackberry/

Kim, A. et al. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. *American Institute of Aeronautics and Astronautics*. Retrieved from: https://arc.

aiaa.org/doi/abs/10.2514/6.2012-2438

Mansfield, K. et al. (2013). Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model. *2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, 2013, pp. 722-728*. Retrieved from: http://ieeexplore.ieee.org/document/6699093/

Mihelic, P. (2007). Jamming systems play secret role in Iraq. *CNN*. Retrieved from: http://edition.cnn.com/2007/TECH/08/13/cied.jamming.tech/

Milian, M. (2012). US government, military to get secure Android phones. *CNN*. Retrieved from: https://edition.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html

Military Aerospace Electronics (2016). Backpack jammers help Marines counter roadside bombs, disrupt enemy communications. *Military Aerospace Electronics*. Retrieved from: https://www.militaryaerospace.com/articles/print/volume-27/issue-1/product-applications/backpack-jammers-help-marines-counter-roadside-bombs-disrupt-enemy-communications.html

Morante, S., Victores, J. G. & Balaguer, C. (2015). Cryptobotics: why robots need cyber safety. Retrieved from: https://www.frontiersin.org/articles/10.3389/frobt.2015.00023/full [Accessed January 2018]

Pullen, J. P. (2015). This Is How Drones Work. *Time*. Retrieved from: http://time.com/3769831/this-is-how-drones-work/

Ribeiro, J. (2012). BlackBerry loses government contract to iPhone. *PCWorld*. Retrieved from: https://www.pcworld.com/article/2012862/blackberry-loses-government-contract-to-iphone.html

Rivera, E., Baykov, R., Gu, G. (2014). A Study On Unmanned Vehicles and Cyber Security. Retrieved from: https://pdfs.semanticscholar.