Beware the unfriendly skies: how drones are being used as the latest weapon in cybercrime.

Martin S. Bressler
Southeastern Oklahoma State University

Linda Bressler
Southeastern Oklahoma State University

ABSTRACT

Practically every time an individual reads the paper/internet news, etc., computer crime of one sort or another can be found. Examples of cybercrime methods include ransomware, click-jacking, doxxing, phishing, pharming, and even drones; (Ikseu & Yongyun, 2015). Could this situation be as some authors indicate, our fault (Gerirtz, 2014) or as Heaven (2015) believes, could it be because companies may be in such a rush to utilize new systems, these companies may not take the time to ensure their devices will be properly secured first (Heaven, 2015)? Since computer crime or cybercrime comes in many forms, small and large businesses can be attacked and not always by hackers. Some of the threats to individuals can involve computer and Internet issues. But new threats can be outside our computer screens. Leopold (2014) suggests that the next major security breach issue will be in the form of drones. In this paper the authors will examine legitimate drone use, but will concentrate on one of the cybercrime methods for which growth can be considered exponential: drones.

Key words: drones, cybercrime, drone detection, drone defense

INTRODUCTION

Terminology

Click-jacking: Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending personal information to a website. Numerous click-jacking scams have been deployed via "Like" and "Share" buttons on social networking websites. Researchers indicated there can be other ways to use your browser options to maximize security (Rydstedt, et.al, 2010).

Cyber-crime: criminal activity or a crime that involves the Internet, a computer system, or computer technology: identity theft, phishing, and other kinds of cybercrime. (http://dictionary.reference.com/browse/cybercrime)

Doxxing: Publicly releasing a person's identifying information online without authorization. Caution should be exercised by users when sharing or posting information about themselves, their family, and their friends (http://www.thestar.com/news/insight/2015/08/16/whats-up-with-dox-the-troubling-history-of-an-online-scare-tactic.html).

Ethics-neutral: technology is unable to make decisions based on ethics; therefore technology can be used for good or evil at the discretion of the user. (Author).

Mini-drone/UAV: is a powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload (Unmanned Aerial Vehicle Wikipedia definition Retrieved 12/07/2015 from https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle#Definition_and_terminology).

Phishing: trying to obtain financial or other confidential information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organization, usually a financial institution. It also typically contains a link to a fake website that closely resembles the real one (http://www.ask.com/web?qsrc=1&o=0&l=dir&q=phishing).

Pharming: a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure" (http://searchsecurity.techtarget.com/definition/pharming).

Ransomware: a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. (http://www.trendmicro.com/vinfo/us/security/definition/ransomware)

UUV/unmanned underwater vehicle: used for scientific or military purposes. (Center for the Study of the Drone at Bard College, Retrieved 12/20/2016 from http://dronecenter.bard.edu/underwater-drones/.

DISCUSSION

The use of drones generates heavy deliberation and debate over important considerations dealing with the use of drones. Yeonmin (2014) believes that the most major issue dealt with Obama's increased use of drones in counterterrorism strategies in Pakistan and Yemen. The

author noted the increased discussion on the legality of "targeted killings and military strikes conducted …without a formal declaration of war." In spite of this controversy, more U.S. government agencies and private companies sought applications in order to purchase and utilize drones for their own use.

Drones have also become the high-tech weapon of choice for cyber-criminals, who steal proprietary company information, financial records and customer data. Drones are even capable of hovering outside your office window and stealing faxes that come through the airwaves and waiting to be printed from your printer. Drones have also been used to smuggle contraband into prisons, including cell phones and drugs. Drones can also hack into the solar panels on your roof to take down an entire power grid or hack into your car to cause it to crash (Weise, 2016). Using ransomware, the hackers can then demand payment by threatening to sell your information or destroy your products.

Because drone use has many different applications, for both good and malicious purposes, drone use is growing rapidly around the world. Due to the potential for nefarious use, experts believe drones will be used in order to not only carry cameras, but also to carry weapons, explosives, and toxic chemicals. This makes drones an ideal weapon for terrorism, espionage, and smuggling. Chess Dynamics managing director Graham Beall states: "Countering drones is now a global issue and an increasing concern for the military, government and homeland security forces across every continent" (Drones anti-drone defense system, 2015).

Companies motivated by the success of the military's use of drones in addition to the rapidly growing hobby and security market, recognize the potential for drones in many types of applications, especially company espionage and counter espionage purposes (West, 2015). In 2012, the Federal Aviation Administration (FAA) recorded only 327 active permits given to only law enforcement and universities (Sorcher, 2013). Chordas (2016) noted that by 2020, the FAA estimated about 30,000 drones will be utilized for all types of industries. However, as

One of the issues surrounding the use of interceptor drones will be whether they can be considered legal for use. Is the sky over a personal residence free space? Of course, in addition to cyber-theft there is the potential for voyeurs, paparazzi, etc., but drones also have an enormous commercial potential, as evidenced by the $90 billion estimated value of the drone industry (Smith, 2016).

Drones can be used by companies for deliveries (Sorcher, 2013), border security, or by the military for spying, taking pictures, and eventually stealing the enemy's information. Many organizations utilize mini-drones to deliver packages and some drones can be fitted with expensive cameras (Graves, 2015; Hilaly, 2015- Project) and still other drones can be programmed to steal private information from your GPS location on your phone including usernames and passwords without the owner of the phone being aware of the theft (Knowles, 2015; Williams, 2014).

How many drones are there? Smith (2016) reports that there are currently more than 700,000 drones in use, primarily for hobby or recreational purposes. An estimated 400,000 drones were purchased last year for Christmas and are likely to be one of the hottest gifts again in 2016. At this time, only about 300,000 drones are registered with the FAA and the push is on to increase registration in light of the approximately 300 incidents of close encounters between drones and conventional aircraft (http://expandedramblings.com/index.php/drone-statistics/).

The popularity of mini-drones increases every year. When first conceived, plans for the drones included protecting human life by sending a machine to take pictures in remote or hazardous areas such as oil and gas companies utilizing drones to monitor pipelines, oil rigs, etc.

Drones can be used for deliveries and can also help police to identify criminals abusing Wi-Fi re: downloading child pornography (West, 2015). Drones can also be purchased to perform other tasks, for example, realtors could showcase properties with the use of drone cameras. Farmers could attack fungus or other crop issues by periodically sweeping their fields with drone cameras before infestations spread to their hundreds or thousands of acres. In manufacturing, drones could remove the risk of employees climbing ladders to search for items or other work-related issues. But, drones could also be utilized for cybercrime purposes. Some mini-drones with HD cameras can take excellent videos and pictures from the air (Leopold, 2014). In addition, drones can fly over buildings with intent to steal companies' proprietary information. Ripley (2015) tells about the time he was on an East Coast government aluminum roof when he surprisingly faced a machine built like a metal box with a microphone and attached metal rod. In Ripley's case, in the building below housed the Homeland Security Office and the machine appeared to be listening for a threat of some kind, but apparently Ripley was not considered a threat even though he spoke to the machine and took its picture. The machine, called DroneShield, was placed on top of the roof to deter other drones sent to acquire information or to deliver unwanted packages. In addition, Zhongli, Li, et. al (2015) suggested that drones could locate explosive devices (IED) which could be programmed to detonate upon receiving a certain signal.

Schubarth (2015) noted a recent Singapore study/experiment designed to help companies determine their vulnerability to drone espionage with drones carrying phones. See Figure 2 in the Appendix for a photo of a drone which carried two apps:

1) Detection of open wireless printers which can notify companies they could be vulnerable to hacking.
2) Detection of open wireless printers but also creates a fake access point set up to intercept documents/information.

The purpose of the study/experiment was to fly around the area in question to find open printers vulnerable to drones carrying phones.

Drone technology is not foolproof, however. There can be several ways to deflect or disarm mini-drones hovering over homes or businesses. One company created a counter-drone system similar to the one noted earlier in this paper but this system could not only detect a drone but fuse the sensor data and jam the other drone's system which would in turn, interrupt its navigation system. Knowles (2015) noted that a European company, Plath GmBh created an electromagnetic fence which would surround the area a business would like to protect and prevent drone cyber-spying.

DRONE CYBER-SPIES GO BENEATH THE SURFACE

Rogers (2015) noted that the U.S. Navy and Coast Guard worked on the Defense Advanced Research Program (DARPA) created to find a cost-effective way to monitor enemy submarine activity without sacrificing human lives. Apparently, anything with embedded software can be exposed and susceptible to cyber-attacks. Vulnerabilities such as weak external interfaces will usually be the first place hackers will attack. In addition, hackers many times exploit software bugs which then create vulnerabilities.

The use of UUV's (unmanned underwater vehicles), or drones by the U.S. Navy goes back to the late 1950's, used primarily for deep underwater research. Even the early drones could dive as deep as 10,000 feet and remain submerged for up to four hours (Center for the Study of the Drone, 2016). Underwater drones are commonly used for various underwater explorations,

including finding the wreckage of the *Titanic* in 1985, and the World War II battleship, the *Bismarck*, in 1989 (Center for the Study of the Drone, 2016).

Of course, underwater drones are also used by the Navy for defense and spying purposes, especially to track submarines from foreign navies. The *New York Times* recently reported that China seized a U.S. underwater done in international waters in the South China Sea and held the drone for several days (Perlez and Rosenberg, 2016). China argued that the regulations regarding underwater drones are vague and therefore within their rights to seize the drone. The United States stated that the drone was for research purposes and that China was not within their rights to seize the drone. After several days, China agreed to return the drone, thereby smoothing over relations between the two countries (Perlez and Rosenberg, 2016).

Keller (2016) indicated that cybersecurity experts at Rockwell Collins in Iowa continue to work with government agencies to fend off hackers even over unprotected data links. The Rockwell team's testing indicated the possibility of repelling cyber-attacks by enabling a drone to operate safely despite onboard and off-board cyber-attacks on their drone's software. Underwater drones that can also fly are already being developed for both military and civilian use. Developed by researchers and students at Rutgers University, and in conjunction with the Office of Naval Research, the *Naviator* is a drone prototype that eventually will be able to carry a sufficient payload for a variety of uses (Reich, 2015). The drone industry also has a number of hobby drones on the market.

SOME DRONES USE THEIR POWERS FOR GOOD!

Selyukh (2016) reports that currently some 20,000 drones are registered with the Federal Aviation Administration (FAA) for commercial use. However, with new rules just released the FAA expects as many as 600,000 drones will be in use commercially within the next year. Instead of requiring a commercial pilot's license, new rules allow anyone over the age of 16 to become a drone pilot after first passing a certification test. The FAA reports that on the first day of the new rules more than 3,000 people signed up to take the certification test. Selyukh (2016) further reports that previous drone rules will continue to apply: "No flights beyond line-of-sight, over people, at night, above 400 feet in the air or faster than 100 miles an hour. Drones also can't be heavier than 55 pounds, and all unmanned aircraft have to be registered. (Some locations, such as Washington, D.C., prohibit drones altogether.)

Drone technology has tremendous commercial potential. Already, real estate companies are using drones to photograph property. For example, in the field of agriculture, DJI markets drones to perform key agricultural activities such as crop inspection, irrigation management, crop consulting, and spraying (http://enterprise.dji.com/agriculture?gclid=CI3Dz6zv09ACFQkyaQod9ukJ4Q). Using drones for crop inspection eliminates the need for farmers to walk the fields and manually inspect crops for plant stress and disease. Drones can also be fitted with thermal imaging, which is especially effective in monitoring greenhouses. Agronomists also consider thermal imaging very effective in irrigation management.

Drones equipped with visual and/or thermal cameras provide agronomists a powerful view of crop production that cannot be seen by the naked eye. Drones can record information every week, every day, or every hour. Agronomists then have a time lapse view of the crop which can then highlight troubles with the crop as well as opportunities for better crop management. Finally, drones provide an efficient and effective means for crop spraying as they

can spray fertilizer, herbicides, or insecticide over ten acres per flight. Studies find drones to be 60 times faster than manual spraying (http://enterprise.dji.com/agriculture?gclid=CI3Dz6zv09ACFQkyaQod9ukJ4Q).

Airware also markets drones for commercial use including applications for mining, quarrying, and construction. Essentially, drones can cover a large range of property and provide detailed information useful to companies that utilize drones for these purposes. Drones have also revolutionized the manner in which insurers manage business as drone use enables swift collection of data on customer property used by underwriters, in addition to loss prevention and claims inspection (http://www.airware.com/industries/insurance?gclid=CNX_2_rz09ACFYJ8fgodgV8G2Q).

Drone use is regulated by the Federal Aviation Administration (FAA) and new rules for commercial use were put into place in June, 2016. According to the FAA, commercial drones could provide an influx of $82 billion to the economy, while creating an estimated 100,000 new jobs over the next 10 years. The agency developed the regulations to prevent damage to aircraft, property, and people. In addition, the regulations require that drone pilots keep the drone aircraft within visual range. (https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515). Finally, the new regulations provide height and speed limits on drone use and will be required to have lights for twilight use.

This could prove problematic for companies such as Amazon, which has already been testing the use of drones to deliver packages (Bishop, 2016). This also explains why drone testing has taken place in the United Kingdom, where the regulatory environment is friendlier to companies like Amazon seeking to utilize drones for commercial purposes. Amazon's goal is be able to utilize a fleet of drones that will be able to deliver packages within 30 minutes or less. Amazon reports successful recent testing in delivering a customer order in only 13 minutes from the time the order was places (Bishop, 2016).

Flying drones can be disastrous as they may be adversely affected by weather because of rain, snow, and changing airflows. Smith (2016) reports there have been 300 incidents of "close encounters between drones and manned aircraft". These flying mechanisms could hit people, buildings, or damage someone's property, not to mention the annoyance of being "spied on" (Graves, 2015). And of course, could be a danger to both wildlife and aircraft that could be in the air. In addition, (Froomkin, 2015) mentions there may be owner liability for such damages and perhaps it might be prudent to require drones built with lights, and to also consider these drones as *ultra-hazardous* (such as use of dynamite or owners possessing dangerous wild animals). There can also be a simple privacy issue and Gregory, et.al (2015) spoke about the concept of an Opt-out program that could cover sensitive area governmental buildings, airports, and owners' private property. Drone Deploy, a third-party organization, developed a database for individuals to register their property as a no-fly zone and with the proper software uploaded; the drones could automatically avoid such areas. But all is not lost as with deterring hackers, researchers indicate that there can be counter-measures for drone incidents as well (Knowles, 2015; Liu, et. al., 2015; Williams, 2015).

DRONE DETECTION AND DEFENSE SYSTEMS

DroneWatcher utilizes three different technologies, which together, can easily detect drones from 1-2 miles away (www.detect-inc.com/drone.html). DroneWatcher APP is based on advanced signals intelligence technology which allows the user of an Android phone or tablet to

record data which includes the type of drone, the ID number, and other information used to document incursions and provides support to law enforcement agencies in prosecuting offenders. The APP system has a limited range of ¼ to ½ mile.

DroneWatcher RF uses a compact electric box installed around the perimeter of the facility. This system has a longer range of 1-2 miles. The Harrier DSR (drone surveillance radar) with a range of 2+ miles can detect uncontrolled, programmed drones which fly on autopilot and are typically not detected by other systems.

Other companies deploy drones that attack and disable the spying drone. The Rapere (brand) drone attacks other drones by dropping string into the drone rotors which tangle and thereby disable the opposing drone (http://www.popsci.com/rapere-anti-drone-interceptor). However, the potential for damage to property and persons on the ground exists anytime a drone crashes.

Some consider lasers to be the best way to disable an unfriendly drone. At the Defense Advanced Research Projects Agency (DARPA), the future projects section of the Pentagon is seeking proposals for a system to not only detect drones, but also "address rocket, artillery, mortar, and other conventional threats". In addition, the system must be able to be mounted on both surface ships and ground vehicles.

Neutralizing drones requires a comprehensive strategy as depicted in Figure 1, beginning with drone detection. Drone detection can be considered the easiest step in the process as there are many systems capable of detecting drone incursions. The second step, tracking, is necessary to determine exactly where the drone is heading. With radar systems effective for as much as two miles or more, commercial areas where businesses are clustered need a good sense as to which facilities might be under attack.

Table 1 Drone capabilities

	Advantages	Disadvantages
Registration	identification of owner, transparency, reduced pilot failure	does not deter criminals and/or terrorists
DroneWatcher APP	drone detection and identification	limited range, does not stop drone
DroneWatcher RF	somewhat longer range detection and jamming	identifies drone but drone may return
DroneWatcher Harrier DSR	somewhat longer range detection and identification	identifies but does not stop drone
Drone vs. Drone (Drone Interceptors)	drone is stopped	crash poses risks
Lasers	drone is destroyed	limited range, crash poses risks
Net Cannons	drone is stopped	limited range, limited success
EMP (Electro Magnetic Pulse)	drone is destroyed	limited range, crash poses risks

A good drone defense system will also be able to classify drones that enter commercial airspace. In some instances, drones might enter the airspace by accident. This is especially true for hobby drones that persons, especially kids use for entertainment. In addition, other commercial drones might just be "passing by" on their way to other locations where they could be delivering packages, photographing real estate, or monitoring construction sites.

Drone defense systems can be designed to disrupt intruder drones. This is often safer than methods used to neutralize intruder drones, as neutralizing usually results in a drone crash which can harm persons or damage property. Disruption can occur from jamming signals or using optical disruptors which in effect, blinds the drone and makes it impossible for the drone pilot to control the craft. Electronic fence systems around buildings or facilities also fall into this category. Finally, some drones must be neutralized. In instances where attack drones are found to be stealing or attempting to steal proprietary or classified data, or are being used by smugglers, terrorists, and other violent criminals.

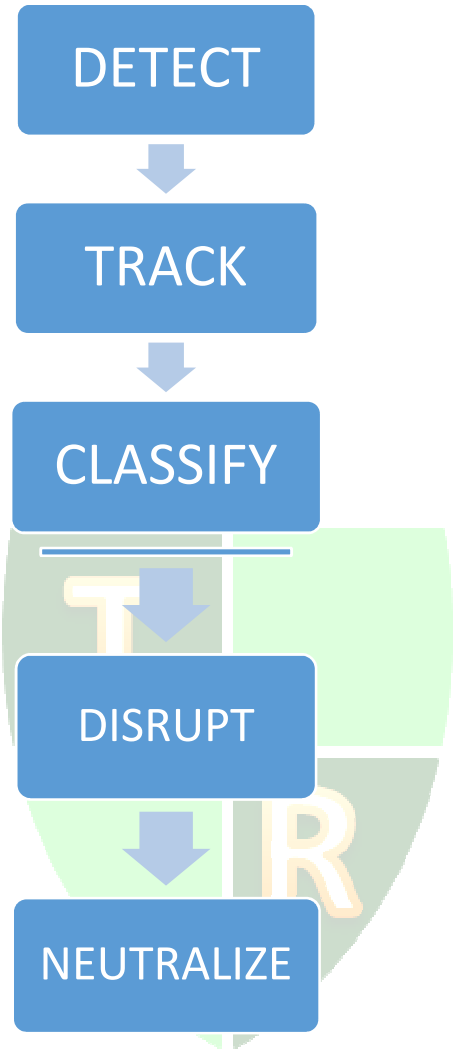
CONCLUSION

One of the most significant challenges with technological advancement is that technology is "ethics-neutral", that is, the technology can be used for either beneficial or harmful purposes. For those who would use drone technology for criminal activity or for espionage, it is important to note that anti-drone technology exists and is getting better every day.

The commercial potential for drones is enormous and the business potential cuts across many industries ranging from agriculture, to real estate, to delivery services, and more. With billions of dollars in commercial potential, the need to protect financial, technological, and customer data is critically important. The fact that drones can be used for criminal activity should not deter those who would use drones for legitimate commercial activity. Rather, anti-drone technology can be used to protect government, commercial, and personal interests from cyber-criminals.

Of course, the military, government agencies, and commercial enterprises alike have a vested interest in anti-drone technology. We are also seeing increased use of drones by law enforcement agencies. Currently, each technology provides different benefits and with varying degrees of success. As emerging anti-drone technologies continue to develop, government, commercial, and consumer data will be protected from cyber-criminals. Until that time, the authors recommend the five-step strategy to defend against malicious drone incursions.

Figure 1: A five-step model to protect against drones



REFERENCES

Airware Commercial Drone Solutions for Insurance http://www.airware.com/industries/insurance?gclid=CNX_2_rz09ACFYJ8fgodgV8G2Q

Atherton, K. (2015, January 16) Forget falcons; fight drones with drones. http://www.popsci.com/rapere-anti-drone-interceptor

Atherton, K. (2016, August 18). Lasers might be the best bet. (http://www.popsci.com/darpa-wants-new-anti-drone-weapon-by-2020

Autonomous commercial drones are going to change the way http://www.airware.com/industries/insurance?gclid=CNX_2_rz09ACFYJ8fgodgV8G2Q

Bishop, T. (2016). Retrieved 12/20/2016 from www.geekwire.com/2016/video-amazon-makes-first-Prime-Air-drone-package-delivery-offers-glimpse-of-new-aircraft-design.

Center for the Study of the Drone at Bard College, *What you need to know about underwater drones*, November 16, 2015. Retrieved 12/20/2016 from http://dronecenter.bard.edu/underwater-drones/.

Chordas, L. (2016). Eye in the Sky. Best's Review, (11), 96.

Dedrone. Definition retrieved 12/07/2016 from http://www.dedrone.com/en/dronetracker/counter-drone-measures

DJI http://enterprise.dji.com/agriculture?gclid=CI3Dz6zv09ACFQkyaQod9ukJ4Q Retrieved 12/01/2016.

Doxxing. Definition retrieved 12/07/2016 from (http://www.thestar.com/news/insight/2015/08/16/whats-up-with-dox-the-troubling-history-of-an-online-scare-tactic.html).

DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems, June 21, 2016 (https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515).

DroneWatcher Drone Detection and Defense Systems www.detect-inc.com/drone.html).

Froomkin, A. M. (November 1, 2015). Self-Defense Against Robots and Drones. Connecticut Law Review, 48(1), 1-69.

Gerirtz, E. (2014). We are losing the cyberwar and it's mostly our fault. Journal of Counterterrorism & Homeland Security international, 20(2), 8-9.

Graves, B (2015). Company has B2B target for sensing technology for drones. *San Diego Business Journal, 36*(37), 4.

Gregory, T. S., Tse, Z. T. H., & Lewis, D. (2015). Drones: Balancing risk and potential. *Science*, *347*(6228), 1323.

Heaven, D. (2015). Your world will be hacked to pieces. *New Scientist,* 226(3016), 1.

Heerkens, H. (2015). Delivery drones: coming to the sky near you? Congressional research service-Legal sidebar, May 6, 2016. *ADIT, the bulletin*.

Hilaly, A. (2015). Project Wing Demo. http://www.businessinsider.com/drone-delivery-could-be-reality-withinmonths-if-government-gets-out-of-way-2015-11.

Hilary, A. (2015). Drone delivery could be a reality within months—If government gets out of the way. Linkedlin.com, 1-28.

Ikseu, K, & Yongyun, C. (2015). Hash-Based Password Authentication Protocol Against Phishing and Pharming Attacks. Journal of Information Science & Engineering, *31*(1), 343-355.

Keller, John (August, 2016). Cybersecurity and encryption for the masses. Military & Aerospace Electronics, 27(8) 18-22.

http://dictionary.reference.com/browse/cybercrime
Knowles, J. (2015). Going small: Jamming the mini-drones. *Journal of Electronic Defense, 3*810), 26-30.
Leopold, G. (2014). New hacking scenario emerges: WiFi signal-sniffing drones, Defense Systems, 1-5.
Liu, Zhongli, Li, Zupei, Liu, Benyuan, Fu, Xinwen, Raptis, Ioannis, & Ren, Kui (2015). *Rise of Mini-Drones: Applications and Issues.* PAMCO '15 Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing. Hangzhou, China (June 22-25, 2015).
Perlez, J. & Rosenberg, M. (2016). *The New York Times*, December 17, 2016, China agrees to Return Seized Drone, Ending Standoff, Pentagon Says. Retrieved 12/17/2016 from (www.nytimes.com/2016/12/17/world/asia/china/us/drone.html).
Pharming Wikipedia definition Retrieved 12/07/2015 from https://en.wikipedia.org/wiki/Pharming.
Phishing definition Retrieved 12/06/2015 from http://www.ask.com/web?qsrc=1&o=0&l=dir&q=phishing
Presidential debates. Retrieved 12/07/2016 from http://www.dedrone.com/en/newsroom/press-detail/presidential-debate-secured-against-rogue-drones.
Ransomware definition. Retrieved 1/14/2017 from *Trend Micro*, http://www.trendmicro.com/vinfo/us/security/definition/ransomware.
Ripley, A. (2015). Atlantic, 316(4), 66-74.
Reich, J.E., (2015, December 23). The Naviator Drone Can Fly In The Air And Swim Underwater. *Tech Times*, retrieved 12/07/2016 from www.techtimes.com.articles.the-naviator-drone
Rogers, W.J. (October, 2015). U.S. Naval Institute Proceedings, 141(10), 24-28.
Rydstedt, G., Bursztein, E., Boneh, D., & Jackson, C. (2010). Busting frame busting: a study of clickjacking vulnerabilities at popular sites. *IEEE Oakland Web*, *2*, 1-13.
Schubarth, C. (September 7, 2016) Mercedes teams with Silicon Valley startup on delivery drone-deploying vans Retrieved 11/20/2016 from http://www.bizjournals.com/sanjose/bio/3681/cromwell%20schubarth?page=75
Selyukh, A. (August 29, 2016). FAA Expects 600,000 Commercial Drones In The Air Within A Year. Retrieved 12/08/2016 from http://www.npr.org/sections/thetwo-way/2016/08/29/491818988/faa-expects-600-000-commercial-drones-in-the-air-within-a-year.
Sorcher, Sara. What Drones Can Do for You. *National Journal* 11 Apr. 2013. *Opposing Viewpoints in Context*. Web. 22 Sept. 2016.
Smith, C. (October 9, 2016) 10 Interesting Drone Statistics. http://expandedramblings.com/index.php/drone-statistics/
Unmanned Aerial Vehicle Wikipedia definition Retrieved 12/07/2015 from https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle#Definition_and_terminology
Weise, E. (2016, August 2). As computer security community gathers in Vegas, cutting-edge researchers see more danger lurking. *USA Today*, B1.
West, G. (2015). Drone On: The Sky's the Limit--If the FAA Will Get Out of the Way. *Foreign Affairs*, *94*(3), 90-97.

Williams, L. C., New drone can hack into your smartphone to steal usernames and passwords, March 20, 2015, Think Progress, Retrieved 12/05/2016 from http://thinkprogress.org/home/2014/03/20/3416961/drones-hack/

Yeonmin, C. (2014). Lost in Debate: The Safety of Domestic Unmanned Aircraft Systems. Journal of Strategic Security, 7(4), 36-56. doi:10.5038/1944-0472.7.4.4

Figure 2 Demonstration of a drone incursion on commercial businesses

Researchers in Singapore showed how drones carrying phones can steal documents from wireless printers (Schubarth, 2015). Photo Courtesy of John West.