Unmanned Aerial Vehicles (UAVs) in Warfare

By Amanda Savage, ECE '16

As technology in warfare advances, more drones are used to autonomously fire or spy on specific targets, however many innocent civilians are killed or injured in these missions. Through improvements in drone technology and handling, many of these casualties can be prevented and further damage from autonomous armed machinery can be minimized.

Introduction

The idea of a UAV has been around for centuries, with one of the first recorded UAVs invented in 1849, when Austria launched nearly 200 unpiloted hot air balloons filled with explosives to be flown into Venice, Italy (Shaw, 2014). Many decades later, the United States military would use a kite fitted with a camera during the Spanish-American War in 1898 to produce the first aerial reconnaissance photos. However, the more modern idea of a remotely controlled pilotless aerial vehicle wasn't successfully implemented until World War II, when both allied and axis powers would launch remotely controlled flying bombs that could hit their targets more accurately. From its very origins, drones have been developed for warfare, both as weapons and reconnaissance vehicles, and much of UAV advancement and evolution has been made for the purpose of progressing in modern combat. Through investigation of the effectiveness and reliability of modern military drones, questions are raised over safety and privacy, as well as other ethical concerns.

Background

The increasing use of unmanned aerial vehicles in current armed combat is due to many factors, like the efforts to reach more remote targets, and the desire to not spare the lives of human soldiers. In doing so, the controversy of the danger surrounding the insertion of ground forces can be avoided, providing an advantage both militarily and politically. However, controversy still remains in the safety and privacy of civilians abroad, and those who remain innocent in armed combat. Some major threats to the protection of private citizens include the illusion of accuracy in drone navigation, technology that can be hijacked easily, and unreliable communication links between drones and satellites.

The illusion of accuracy of UAVs is one of the most dangerous perceptions in their usage and this inaccuracy may persist in grainy imaging, imprecise navigation, flawed software, and human error. When GPS navigation is incorrect or not exact, this imprecision can create a ripple effect of errors in imaging and targeting. When the exact location is incorrect, the image may be delayed or inaccurate, creating a completely unreliable target. When an error lies in the technology of drone strikes, no matter how slight, the consequence could be as severe as civilian casualties. GPS data may become unreliable in extreme weather, or when obstructed by large obstacles, like concrete buildings. Such vulnerabilities also exist in software that uses algorithms to create specific and precise positions and images from the UAV. The consequences of inaccurate software are similar to that of faulty navigation or flawed cameras or radar, because the software processes these images and positions and this data is what the user interprets.

One of the major challenges that drone technology faces is in its vulnerability to hijacking attacks. These methods of drone hijacking include techniques like spoofing and jamming. *Spoofing* occurs when a signal disguises itself as another, thus making the fake signal become a substitute for the real one. When spoofing

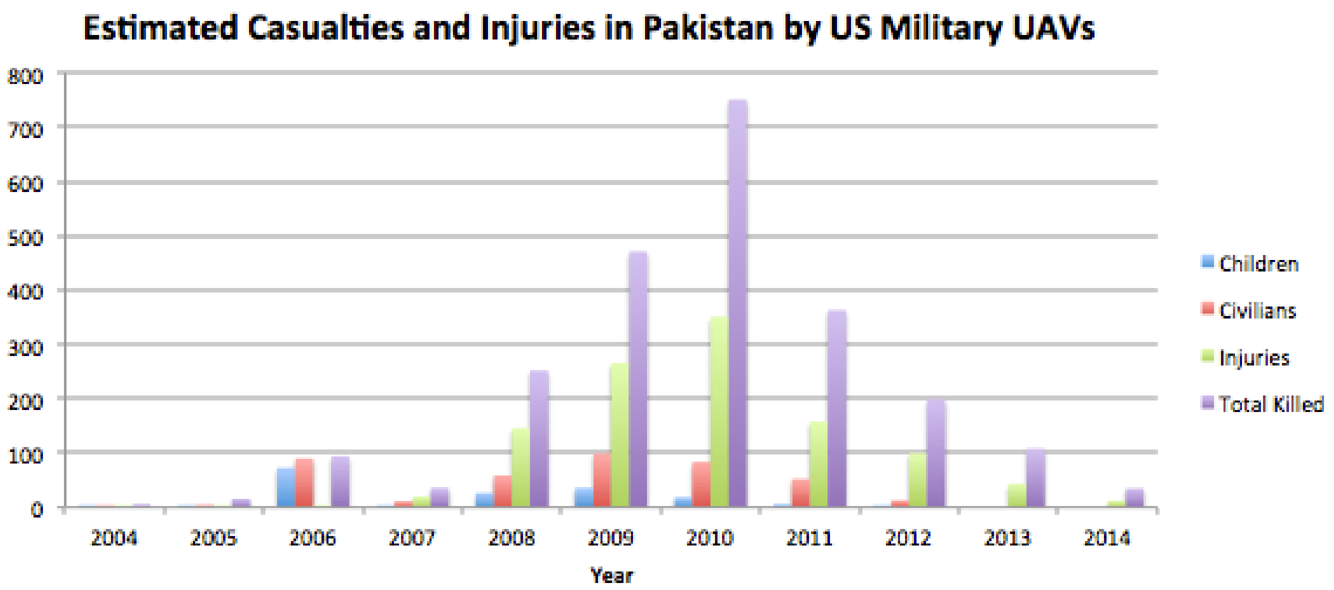

Figure 1. Estimated Casualties and Injuries in Pakistan by United States Military UAVs by Year. Data source: Get the data: Drone wars, 2014.

devices overpower the signals coming from GPS satellites or aircraft transmissions, this causes the drone to veer off course. Spoofing can be prevented if a drone requires that signals must be encrypted with a digital signature in order to be recognized by the UAV, but this technology is still years away from being deployed. *Jamming* a drone can occur when noise transmissions are used to block GPS satellite navigation or control signals, which are critical in piloting the drone. Thus when jamming occurs, the obstruction of signals causes the drone to continue without critical information, thus forcing it to deviate from its path and possibly crash.

Unreliable communication has been cited as one of the prevalent causes of catastrophic failure in the majority of military drones crashes (Cuadra, Whitlock, 2014). When a drone first takes off, it is controlled through a direct data link from a control station on the ground until it leaves the line of sight. Once the drone leaves this line of sight, satellite communication takes over to control the UAV, using GPS to broadcast the drone's position. When any of these communication links are lost, the drone’s programmed response is to fly in circles or to return to its base until the signal is regained. However if contact is not recovered after a certain period of time, the drone could use up all of its fuel trying to reestablish this connection, thus causing it to crash.

Discussion

As drone usage has been expanding in armed combat, these challenges to the protection of innocent civilians in warfare become more urgent, and the result of not addressing these problems can be tragic. The claim that drones are effective at targeting only the primary destination or combatant has been under scrutiny as more information over civilian casualties comes to light. In Pakistan alone (Figure 1), there have been 421 drone strikes by the United States’ Predator drone from 2004 to 2014, resulting in 2,489-3,989 total casualties, 423-965 civilians killed, 172-207 children killed, and 1,158-1,738 total injuries (Get the data: Drone wars, 2014).

This information only solidifies the concerns towards the protection of private, innocent citizens. While the U.S. Military’s Predator drone camera provides exceptionally clear images, drone operators still have difficulty in identifying individuals from above. Without a presence on the ground, the drone’s intelligence is incomplete, and this contributes to that death of about one civilian for every three combative targets killed in Pakistan in the past decade (Callam,

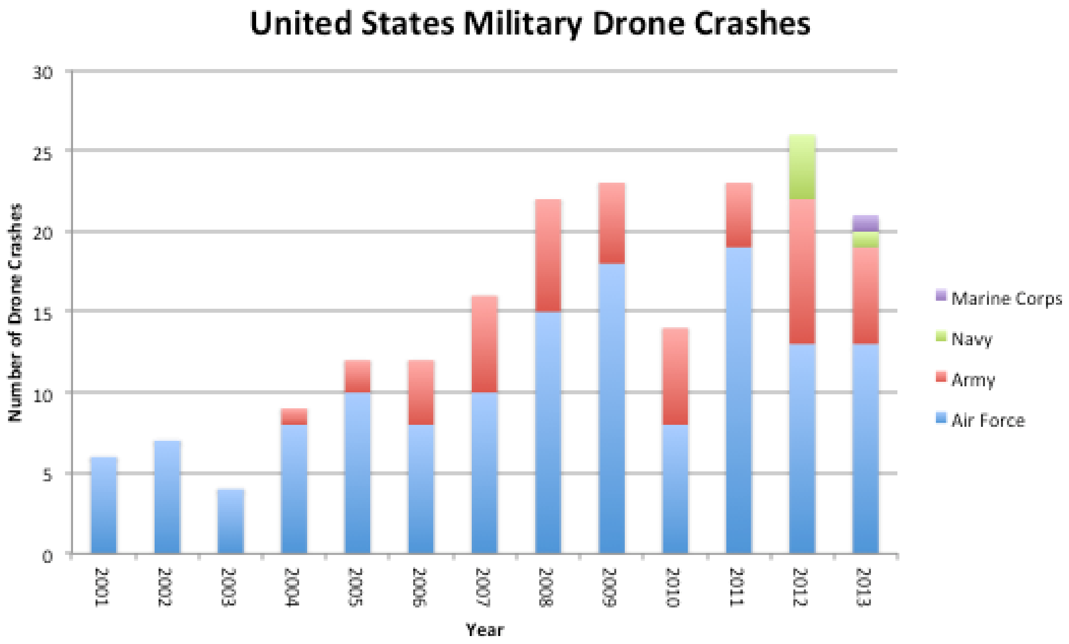

Figure 2. United States Military Drone Crashes. Date source: Chow et al, 2014.

2010). In many of these cases, the error doesn't lie in the technology but in human response, but there are many cases where collateral damage has resulted from flaws in the aircraft itself.

The need for safeguarding armed UAVs also becomes more urgent as hijacking techniques have been implemented successfully on expensive drones. In June 2012, a research team from University of Texas was able to successfully spoof an $80,000 drone in the White Sand Missile Range in New Mexico by using a spoofing device to take command of the drone's position. When the spoofing device generated a nearly perfect forged signal, the drone picked up on the stronger signal sent by the spoofing device that was around 0.5 kilometers away, allowing the drone's positioning to be taken over by the spoofing device. Since the device attempted to change the drone's location on erroneous information, the drone veered directly to the ground, and was only saved from crashing by an operator poised to override the spoofing device (Humphreys, Wesson, 2013). In September 2011, In September 2011, *Chosun Ilbo*, a South Korean newspaper, reported that North Korea successfully hijacked a United States spy plane through jamming the planes communication signals (Franceschi-Bicchierai, 2012), making such a major vulnerability a very real hindrance in combat. This susceptibility calls for advancements in drone safeguarding in order to prevent crashes or an unknown host taking control of an aircraft.

Drone crashes caused by mechanical error is also no longer just a hypothetical event, as the United States' Predator drone has crashed numerous times in its missions (Figure 2). It's been found that "the Predator crashes due to mechanical error 43 times per 100,000 flying hours, whereas typical manned aircraft crash 2 per 100,000 hours," (Callam, 2010) which illustrates that not only have crashes been numerous, but unmanned aerial vehicles crash 21 times more than manned aircraft within the same amount of flying hours due to mechanical error, and not by enemy fire. This mechanical error is caused largely due to a loss in communication links, and as the drones are used more frequently and in more remote areas, the number of accidents per year has been steadily increasing over the years.

Conclusion

In a society where self-interest and justice can be carried out through unmanned aerial vehicles in combat, there's a responsibility to ethics in engineering, and in creating safe technology. While the purpose of these complex autonomous vehicles is to be used as weapons, making armed UAVs inherently dangerous, their purpose is to be used for specific targets. Despite the controversy surrounding this, there are few who would argue that it is paramount to, at the very least, spare the lives of those innocent civilians. In order to accomplish this, engineers, including members of the Blue Team, have the responsibility to fix faulty software, further safeguard drones from potential hijacking, create more reliable communication links, and to increase accuracy of navigation, among other developments. Specifically, the Blue Team has worked to incorporate a more accurate differential GPS, precise up to a few centimeters, in order to provide more exact positioning data, and an efficient autofocus algorithm has been generated and implemented in order to produce highly detailed images.

Many expect that drone strikes would be less likely to result in collateral damage in comparison to attacks by human forces, but the results show that this ideal is still in the distant future. As this technology evolves and expands, these challenges preventing the percentage of civilian casualties from decreasing should be met with greater advancements, allowing for a greater balance between law and order, and goodwill.

References

Callam, A. (2010, Winter). Drone Wars: Armed Unmanned Aerial Vehicles. *International Affairs Review* Vol. XVIII (3). Retrieved from http://www.iar-gwu.org/node/144

Chow, E., Cuadra, A., Whitlock, C. (2014, June 20). Fallen From the Skies. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-srv/special/national/drone-crashes/database/

Cuadra, A., Whitlock, C. (2014, June 20). Hazard Above: How Drones Are Controlled. *The Washington Post.* Retrieved from http://www.washingtonpost.com/wp-srv/special/national/drone-crashes/how-drones-work/

Enemark, C. (2013). *War, Conflict and Ethics: Armed Drones and the Ethics of War: Military virtue in a post-heroic age.* Oxon: Routledge. doi: 10.4324/9780203107218

Franceschi-Bicchierai, L. (2012, July 6). Drone Hijacking? That's Just the Start of GPS Troubles. *Wired.* Retrieved from http://www.wired.com/2012/07/drone-hijacking/

Get the data: Drone wars (2014, July 7). *The Bureau of Investigative Journalism.* Retrieved from https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/

Humphreys, T., Wesson, K. (2015, October 15) Hacking Drones. *Scientific American, 309,* 54–59. doi: 10.1038/scientificamerican1113-54

Shaw, I. G. R. (2014). The Rise of the Predator Empire: Tracing the History of U.S. Drones. *Understanding Empire.* Retrieved from https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/

Tencer, D. (2010, September 24). CIA used pirated, inaccurate software to target drone attacks: lawsuit. *Raw Story.* Retrieved from http://www.rawstory.com/2010/09/cia-inaccurate-software-drone-attacks/