Malfunctions in Combat Drones: An Ethical Analysis

Introduction

With the advance of technology, numerous industries have begun to rely on machines and robots to accomplish their goals. The military is no different from any other industry, and in the past years we have seen a move from infantry focused combat to a more advanced technology reliant form of warfare. This shift is especially apparent in the assassination of so called high value targets. The number of US drones strikes increased from 51 under the Bush administration to 373 under the Obama administration, an increase of 631% (Serle & Purkiss, 2017). Previously, the majority of operations would rely on deploying ground troops to the location, or at the very least a manned aircraft strike. However, with the recent introduction of semi-autonomous aircraft, or drones, it is now possible to conduct these operations remotely without ever setting foot in the location of the target.

Of all industries the military sector is commonly a leader in encouraging technological advancements and one of the first adopters of brand new technology (Shu, 2014). While innovative technology may make the battlefield safer (Stone, 2003), the use of new and untested technology is not without inherent risks. New technology can lead to malfunctions in hardware, as well as bugs in software. These malfunctions can be especially deadly in the use of drone strikes, as there is a large capacity for unwanted collateral damage. Estimates differ wildly by source, but it is broadly accepted that between 5-30% of civilian casualties caused by drones are in reality a result of malfunctions (Roggio 2016; Bergen & Tiedemann, 2010).

As drones are unmanned and rely on a significant amount of software to interface between aircraft and op-erator (Axe, 2012), there is a visible disconnect between the person who pushes the button, and the target. Therefore, in the event of a malfunction, it becomes difficult to firmly rest the responsibility for the incident on one single actor.

This paper will focus on two different possible scenarios in which a malfunction has occurred. The first being a software or hardware malfunction, and the second concerning autonomous drones. In scenario number one, we can see that modern drones have a large array of software to assist them in combat, and therefore a malfunction in any of this software could cause a large amount of collateral damage (Whitlock, 2014). Alternatively, a malfunction in the hardware of the drone could cause a misfire, or in the worst case scenario the drone could crash. Such faults could potentially cause a high number of civilian deaths.

On the other hand, scenario number two imagines a time in which drones are fully automated, which is likely to happen in the near future (Guizzo, 2016). This concept has resulted in a considerable amount of fear, causing an open letter to be created to discourage the development of autonomous weapons. This letter garnered the support of thousands of AI and Robotics researchers as well as support from leaders of industry such as Elon Musk and Steve Wozniak.

The argument for autonomous weapons is the same as for combat drones. That is, these machines reduce casualties for the user. Yet, such artificially intelligent weapons have the potential to operate on a much larger scale. Instead of the large missile wielding drones of today, we could potentially have armed quad-copters that could be deployed on mass, able to search for and eliminate targets meeting certain pre-defined criteria (Autonomous Weapons: An Open Letter, 2015). In this scenario the potential for a significant number of unwanted casualties due to a malfunction is incredibly high. However, in this case, questions about where the fault actually lies become very difficult to answer. Say for example a fully autonomous drone misidentifies a target, and kills them, who is accountable for this disaster?

In attempting to get to the bottom of this issue, a number of questions will first need to be asked. Primarily, what actually went wrong? Was this a unique occurrence, or has it happened before? If so, who knew about it? In this paper, we will be exploring the ethical issues surrounding this topic, in an attempt to identify where the responsibility and accountability for such an incident may lie. In particular, we will examine the professional and moral aspects of the issue and how this impacts the various stakeholders and actors involved.

Framework

Throughout this essay, a number of ethical and philosophical theories will be utilized. This will be done in an attempt to analyze and evaluate the situation from multiple different angles and perspectives for both scenarios. Additionally, the most relevant ethical theories will be evaluated.

The scenarios are first examined from the utilitarian perspective. Utilitarianism is an ethical theory that is based on the principle that our policies and laws should be such that they produce the greatest good (happiness) for the greatest number of people (Tavani, 2013, Chapter 1, p. 15). According to this theory, it may follow that although deploying the drones could harm or kill some civilians as a result of a malfunction, eliminating high value targets may be preferential. Conversely, a deontological point of view might lead to a completely different conclusion. Deontological theories are theories in which the notion of duty, or obligation, serves as the foundation for morality (Tavani, 2013, Chapter 2, p.57). The idea of signing off on a technology that may cause innocent deaths is ethically irresponsible and inexcusable under this theory, and therefore the precautionary principle should be enforced until all possible malfunctions are accounted for.

Another relevant theory is that of communalism. The concept of communalism encompasses the idea that all scientific knowledge should be published and be publicly available (Grooters & Zevenburg, 2017). This idea is often ignored, especially in combat scenarios in an attempt to gain the upper hand by possessing superior technology. Ignoring the idea of communalism brings about its own issues as it may allow for malfunctions. Furthermore, a lack of peer reviews leaves military hardware and software additionally vulnerable to malfunction.

The problem of induction is also relevant in the context of technologies with as great an impact as drones. Is it possible to test all of the possible scenarios that drones will be subjected to? What should happen if an error is to occur in a situation that it has not been prepared for and has not been tested? Additionally, with a weapon as powerful, indiscriminate and disconnected as a drone, the concept of moral protectability arises. This theory encapsulates the idea that people who cannot protect themselves should be protected. Due to the sheer power that a drone possesses, the average person will not be able to protect themselves from these drones.

Finally, we examine the situation from the technology ethics theory. Is it ethical for a company to develop software for drones and should a company care what the technology they are developing is used for? Do organizational structures prevent an individual from being responsible for their own creation? Or should we expect whistleblowers to expose potential injustices being committed for the sake of national security?

Research Question

The key aim in this paper is to investigate the various factors that may lead to a drone malfunction, in an attempt to draw conclusions as to who can be held accountable in each case. As such we pose our research question as follows:

Who is responsible for malfunctions in combat drones, and are those who are responsible, also accountable?

To ask such a question, we will first need to define the difference between responsibility and accountability. Responsibility, specifically moral responsibility, is described in terms of two conditions: causality and intent. A person X is morally responsible for an event Y, then X caused Y. X can also be morally responsible for Y if X intended for Y to happen, even if it did not (Tavani, 2013, Chapter 4, p. 118). Accountability, on the other hand, is a much broader concept than responsibility, in the case of asking who is actually answerable for an event. While responsibility is usually attributed to an individual, accountability can apply to a group of individuals, or even an organization (Tavani, 2013, Chapter 4, p. 118).

To explore this question fully we will be asking it in the context of two different scenarios. To be able to come to a satisfactory conclusion in each of these scenarios, there are some important subquestions that will have to be tackled. In each scenario the primary question will be: what exactly caused the malfunction to

occur? This is the most crucial question when assigning responsibility, however may not be so relevant in terms of accountability. To get an accurate picture of who is accountable we may ask if there were any professional codes of conducts that were violated, or if the quality of the product was properly assured. In these cases, rather than investigating the actual cause of the malfunction, we are trying to find if there was any malpractice that has led to the incident, as accountability often lies with those who were not following the correct procedure.

Another question that needs to be considered is whether limits and conditions placed on the project, such as budget, secrecy and time constraints, could have had a contributing factor towards the malfunction. Again this may not have much an influence on who is responsible, but could certainly influence where accountability lies.

The final subquestion to be considered is whether the incident was at all preventable? While parts of this may have already been answered by previous questions, there are further aspects of this question that we can explore: Were the risks of deploying drones in combat evaluated in the first place? Is it even ethical to deploy drones?

By exploring these subquestions using our framework, we hope to be able to successfully answer our research question and provide thorough analysis of the majority of key aspects involved.

Results and Analysis

To assess the ethical issues in our scenarios, the different actors were examined. An actor is defined as a participant who performs an action or is influenced by some action. Identifying and characterizing the different actors is imperative to objectively analyze the cases. In the following section we will outline several different actors along with their goals and interests. Additionally, the framework will be used to analyze the possible behavior of the different actors. Finally, we will try to answer two main subquestions which encapsulate all of our other subquestions as well.

The first actor that is present in our scenarios is the government. The government deploys the drones and chose to utilize them for some purpose. In addition, there is the manufacturer. The manufacturer is an actor that is only present in the scenario of a hardware failure. Because the drone's hardware is a product produced by this actor, the manufacturer's actions are likely to influence the frequency of such an error. Furthermore, we identify the operator as the actor who operates the drone at the moment it malfunctions. This operator is not present in our future scenario, where the operator is no longer necessary as he can be replaced by an autonomous system. In the case of a software malfunction, the programming company plays a major role in the incident, and is, therefore, a key actor as well. The programming company is in charge of creating the software and ensuring the quality of the code. A more passive actor in our scenarios is the general public. The general public can do little to affect the drones' deployment, but they suffer from its usage. Finally, the press can be viewed as an actor, as they may have a significant impact on society.

Quality assurance

The first question we will examine is whether the quality of the product was properly assured. In the case that the quality was assured, then there is really no blame to assign. If the quality was not properly assured, then the government, software company and the manufacturer are all relevant actors. Certain limits are associated with development of drones, such as time and money. The first drones (that are still in use today, such as the MQ-1 Predator) were rushed to war, and were not designed to last. The money that was spend on research and development did not focus on safety and today these drones fly with persistent mechanical defects (Whitlock, 2014). This a very unethical practice to deploy detective drones. However, the military claim that the drones function way beyond expectation and that in 2018 they will replace all Predator drones with the more effective and safer successor, the MQ-9 Reaper drone. The US Government at the time was focused on national security which is a feasible argument for the lack of safety features at the time. Now that drones are most likely going to be part of everyone's future, safety should be a major concern.

Since the government regulates the drones, they oversee all the different processes interacting with the deployment and usage of the drones. Therefore, the government has a significant influence on all other actors and they should assess the quality of both the manufacturer and the programming company.

The manufacturer's goals are to maximize their profits and to satisfy their customers. Maximizing their profits is directly in conflict with the interests of other actors. Therefore, the manufacturer needs an ethical inclination

if they want to minimize the chances of errors in the hardware. Manufacturers usually take a deontological point of view, whereby they will instill a professional code of conduct for their workers to follow. A part of this code of conduct may also include a form of a precautionary principle.

The software company is quite similar to the manufacturer as it has the same goals. By paying a significant amount of attention to safety and correctness of their software, the programming company can minimize the chances of such a malfunction. Assuring their product is bug free is a challenging and onerous task, which can never be completely guaranteed.

Because the software development cycle is so prone to bugs, it will cost a lot of resources to prevent these bugs. However, in the case of drones, the bugs can have devastating effects. Minimizing the bugs in the software would be a core responsibility for the software company from the consequentialist perspective because these bugs could result in undesired consequences. In reality, it is impossible to have no bugs at all (Greenberg & Stokes, 1995). Another situation that could be present in the software company is that an employee discovers a bug in the software. The employee should then report this to his supervisor if he wants to act ethically correct. If his supervisor choose to ignore this warning, then the situation changes. From the deontological perspective, the employee has already acted justly and therefore he can leave the issue alone. On the other hand, the consequentialist approach would argue that the employee should 'whistle blow' the issue to the public because it can have very severe consequences.

Ethical correctness

The second notion we will discuss, is whether the actions surrounding the incident where ethically justified. For this purpose, we identify the relevant actors to be the government, the general public, the press and the operator.

Generally, the government's desire to operate drones originates from their inclination towards protecting civilians. The usage of drones allows for the exclusion of human soldiers, up to some extent, as well as better performance and less casualties in war zones. Clearly the government is acting with a utilitarian point of view: They are taking preventative action against targets to ensure these targets cannot harm a greater number of people. They have concluded that any collateral damage must be less than the potential damage that the targets can cause. It could also be said that governments have a sense of moral protectability toward their own citizens, and may not extend this to citizens of other countries. Additionally it is apparent that the government have taken an anti-communalistic stance towards drone technology, as the majority of governments keep their military technologies secret.

The operator navigated the drone to the location where other civilians were present and he chose to execute some attack nonetheless. Although the operator cannot take a malfunction into account, he did create a dangerous situation which could possibly have been avoided. The goals of the operator are to successfully perform his assignments and achieve this with a minimal amount of collateral damage. Operators of drones are most likely subject to a very strict code of conduct with very harsh repercussions if not followed. It is also noteworthy that due to the way the military works, you could say that drone operators do not have their own ethics and morals, as they must follow their orders.

The general public will almost always want to strive for safety. This safety concern is a paradox in itself when it comes to drones. The drones can provide more safety for the civilians, but at the same time they can harm innocent bystanders. Society is likely to view the drones as more harmful than good, therefore they might protest against the usage of these drones. From a deontological point of view the usage of drones is quite amiss from the perspective of the citizens. The actions in which innocent citizens could be victim to a drone attack are in that case not ethically correct because they have not done anything wrong and are not involved in the situation. From a consequentialist perspective, the usage of drones is accepted as long as the advantages outweigh the disadvantages. Therefore, if the drones result in a smaller number of casualties overall, even though there is a quite significant amount of collateral, then the drones will be ethically accepted. Lastly, it could be argued that the concept of moral protectability applies to the citizens, as they are incapable of protecting themselves from both the drones and the terrorists.

Following an incident, the press is likely to publish an article concerning the events surrounding the accident. Therefore, the press also directly influences the government, the programming company and the manufacturer. By publishing an article regarding a drone incident, there might be severe consequences for a company that was involved in the production of these drones. These consequences could include the declining of the company's stock value as well as specific employees having to leave the company. Another plausible outcome would be that the media ignites a shift in citizens, causing them to protest against the usage of drones. We will define the

goals of the press to be informing the public as well as gaining public attention. Providing correct and factual information is an action which is very pure in nature. Therefore, the objective of the press to inform the public is a perfectly valid approach from the deontological perspective.

Discussion and Conclusion

Looking at the first scenario (software and hardware malfunction), when a malfunction occurs, we can investigate the cause, who is responsible and who should be held accountable. Firstly, we will examine the possible examples of malfunction. In terms of hardware, we can have a defective unit caused by human or machine error. Even in fully automated industrial production lines, there is always a small chance of producing a defective unit. These defective units are sifted out by testing all units according to a checklist and only after passing all tests can a unit be shipped out for use. Consider the occurrence of a hardware malfunction, such as a defective part or a broken propeller, in a drone which results into the drone crashing into a civilian's home, killing the occupants. Initially it may not seem that anyone specific is responsible, but in the end someone should be accountable for the incident.

The first person that should be investigated is the pilot. Did he do all in his powers to prevent the accident? If possible he should self-destruct the drone or steer the drone to intentionally crash into an unpopulated area as soon as the malfunction is detected, as this is standard military procedure while operating a drone (Whitlock, 2014). If the pilot did not use all measures to prevent this, he should be held accountable and placed under investigation for suspected dereliction of duty and possibly charged under military law for being willfully negligent. If he did all that he could, then the manufacturer should be investigated, for instance checking whether all parts used in the drone were sourced from reliable sources or even if the sourced parts were intended for application in aerial vehicles. If the drone manufacturer is deemed responsible, they should put in measures so that a recurrence of the event is avoided.

In the case of a software malfunction, it is possible that an operating drone malfunctions due to an error caused by bad coding. Such a malfunction can cause the drone to crash into innocent civilians or a misfire causing collateral damage. In this case, one would naturally hold the programmer who wrote the code that caused the bug, responsible for the incident. However, humans are prone to error, one may come up with an algorithm and seems very logical and clear, but they may not factor in an extreme case that the algorithm produces the wrong output. Since most of standard software development focuses on maintenance and fixing bugs, there is almost always a person or team peer reviewing code. However, one or more members of this team may not have detected a bug. We also have to consider the case in which a system that failed had contributions from many different individuals and it is not clear which of these individuals contributed the faulty code. From this we can see we have run into the problem of "Many Hands" where it is impossible to hold one specific individual responsible. However, accountability - unlike responsibility - is not limited to individuals, and can apply to several actors, and even entire organizations. Therefore in this case we can hold everyone who has been found to have contributed to causing the bug accountable, especially if they are found to have broken their code of conduct.

The accountability does not have to stop here either. The software company themselves can also be accountable for the incident. It is their responsibility to enforce a good code of conduct for their employees to follow, as well as assuring suitable standards of quality control and peer review are in place. They also have to ensure that their employees have good working conditions, and are not putting too much pressure on them to deliver their work, as this can lead to shortcuts. In most cases the company that provided the software which malfunctioned will take on some of the accountability for the incident, as they were ultimately responsible for delivering a good product.

The second scenario concerning the autonomous drones is quite similar to the previous scenario. In general, the autonomous drones concept could provide many advantages over regular drones. These advantages include the reduction of human errors and crashes which are currently the largest cause of accidents regarding drones. The crashes have been a result of either aggressive turns in strong winds causing the drone to crash, pilots not realizing that the drone armed with a hellfire missile that they are piloting is upside down resulting in it plummeting into the ground, or pilots not noticing warnings built into the drone's software (Whitlock, 2014). Additionally, the autonomous drones could reduce the amount of collateral damage, as drones are free from human emotion and have no sense of self preservation, allowing them to make logical, intelligent decisions based on all the available information.

There are, however, some issues with the usage of drones. From the deontological point of view it is not ethically correct to let a machine decide who gets to live and who does not. The programmers could not possi-

bly let a drone properly evaluate every situation and make an ethically correct choice. From a consequentialist perspective the user of autonomous drones is debatable, as the outcome could have a lot of advantages but could also result in tremendous disasters. Viewing this issue from the precautionary principle, we would have to argue that there is not enough certainty that autonomous drones will be without danger, therefore we should not utilize them in the near future.

In conclusion, it is apparent that where the responsibility, and also the accountability lies depends vastly on the circumstances of the incident. Regarding the two scenarios considered, in the first it is clear that responsibility would lie with whomever is found to have made the mistake that directly lead to the incident, be it the pilot, the programmer or the manufacturer. However this does not necessarily mean that they are also accountable for the incident. For example in the case of a software malfunction, while a programmer may have made the mistake that caused the malfunction, the company he worked for could have put him under unreasonable conditions, or pressured him to break the code of conduct. In this case the company would have accountability for the malfunctions.

In the case of our second scenario, most of the same applies. However potential risks of deploying fully autonomous drones are much greater than piloted drones, as in the case of a malfunction there is no human safeguard to try and prevent the incident. Therefore we could argue that most of the responsibility and accountability for such an incident would rest with whomever made the decision to deploy the drones in the first place, namely, the government.

Information sources

References:

Serle, J., & Purkiss, J. (January 1 2017). *Drone Wars: The Full Data.* Retrieved from https://www.thebureauinvestigates.com/stories/2017-01-01/drone-wars-the-full-data

Autonomous Weapons: *an Open Letter from AI & Robotics Researchers.* (July 28 2015). Retrieved from https://futureoflife.org/open-letter-autonomous-weapons/

Axe, D. (November 30 2012). *Navy Preps Killer Drone for First Carrier Launch.* Retrieved from https://www.wired.com/2012/11/navy-killer-drone/

Shu, L. (May 26 2014). *Gps, Drones, Microwaves and other everyday Technologies born of the battlefield.* Retrieved from http://www.digitaltrends.com/cool-tech/modern-civilian-tech-made-possible-wartime-research-development/

Roggio, B. (June 16 2016). *Charting the data for US airstrikes in Pakistan, 2004 – 2017.* Retrieved from http://www.longwarjournal.org/pakistan-strikes

Guizzo, E. (April 14 2016). *Autonomous Weapons "Could Be Developed for Use Within Years," Says Arms-Control Group.* Retrieved from http://spectrum.ieee.org/automaton/robotics/military-robots/autonomous-weapons-could-be-developed-for-use-within-years

Stone, P. (December 17 2003). *New Technologies Make Life Easier, Safer for Troops on the Battlefield.* Retrieved from http://archive.defense.gov/news/newsarticle.aspx?id=27613

Bergen, P., & Tiedemann, K. (February 24 2010). *The Year of the Drone.* Retrieved from https://web.archive.org/web/20110315175041/http://counterterrorism.newamerica.net/sites/newamerica.net/files/policydocs/bergentiedemann2.pdf

Whitlock, C. (June 20 2014) *When drones fall from the sky.* Retrieved from http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/

Tavani, H. (2013). *Ethics and technology: Controversies, questions, and strategies for ethical computing.* Hoboken, NJ: John Wiley & Sons, Inc.

Grooters, S., & Zevenberg, J. (2017). *Computing Science: Ethical and Professional Issues* [Syllabus]. Groningen: Faculty of Science and Engineering, University of Groningen.

Greenberg, B., & Stokes, S. (1995). *Repetitive Testing in the Presence of Inspection Errors.* Technometrics, 37(1), 102-111.