Introduction:

This report discusses the issues behind the imminent new type of warfare that will soon be fought, this war will not be fought with guns and bullets; they will instead be fought with computers and computer code. The battleground will not be on Earth, but on the plane of information known as cyberspace. We can already see this happening, and in fact, it has already emerged in the form of a computer worm named Stuxnet, which is one of, if not the first cyberweapon. This paper will explain the origin of this cyberweapon, the spreading and infection methods, and the attack algorithm. Some ethical issues that emerged when stopping this virus will be explained along with the moral and ethical implications of the different choices that were made. And finally, with the emergence of this virus, new ethical questions are now starting to be asked. Some have explained what they believe is the ethical response to certain situations, so those responses will be examined. Before these are explained though, one must fully understand certain terms in this paper to understand the power of this virus and the people behind the construction of it.

A Zero-Day Exploit is a previously unknown programming error that one can use to break into a computer system for personal gain. These are unknown to the manufacturer until either they find it themselves, or they are notified by someone else. These exploits can be sold for as much as $250,000 on the black market. Being able to find and use just one of these exploits is impressive and will make any virus stand out among the rest. Stuxnet managed to use four of these to complete its goal, each of which is soon to be discussed in this paper.

A Supervisory Control and Data Acquisition (SCADA) system is a computer system used to gather and analyze real time data. They are used to monitor and control a plant or equipment in many different industries. They can be relatively simple, such as a system used to monitor the environment of a small building to incredibly complex, such as a system used to monitor the activity of a water treatment system, or possibly more importantly, a nuclear power plant.

A Programmable Logic Controller (PLC) is a device used to control the automation of physical manufacturing systems. These are used in everything from water treatment plants, to automotive manufacturing to nuclear processing. They are programmed to do everything from turning on heaters and coolers, to starting conveyor belts, to shutting a plant down at the end of the day.

Siemens Step7 is a piece of software owned by the German company Siemens. Siemens says Step 7 is used to create a single easy to use user interface for companies to easily and properly program their PLCs.

A nuclear centrifuge is a crucial piece of equipment used for the enriching of Uranium. These centrifuges spin at a set amount of hertz, or cycles per second.

The Mossad is the headquarters of Israel's foreign intelligence agency. One can imagine it like a top secret version of the United States CIA. It is (usually) strictly off limits to everyone, including reporters and politicians.

RealTek and JMicron are two well known and trusted companies located in the same business park in Taiwan. RealTek is a hardware manufacturer and JMicron is a circuit manufacturer.

President Mahmoud Ahmadinejad surrounded by IR-1 centrifuges located at the Natanz Uranium Enrichment Facility
Background:

In January of 2010, the Uranium enriching facility located in Natanz started experiencing strange problems with their centrifuges. One by one, the centrifuges were breaking with very little explanation other than claiming they received faulty equipment. They also noticed something strange happening with their computers. They were constantly starting up and shutting down. They were to soon find out that these two problems were related.

An Iranian firm got a hold of Sergey Ulasen of VirusBlokAda, a small company in Minsk, Belarus, complaining about their computers constantly rebooting. Upon looking into the problem, Sergey Ulasen discovered what was soon to be named Stuxnet, a virus that was found out to be much more complicated and sophisticated than any other piece of malware known as of yet. Soon after the discovery, Ulasen notified other anti-virus companies, including Symantec, one of the largest anti-virus software companies today.

Symantec's Liam O'Murchu and Eric Chien, and Ralph Langner, owner of Langner Communications, were three people who studied the virus in an attempt to stop it. O'Murchu immediately gained an interest when he saw that the malware inside of Stuxnet was over 500kB of pure computer code. To put this in perspective, the average amount of code in a piece of malware is about 10 to 15 KB, about 50 times smaller than Stuxnet. This realization drove him to better understand the malware's intention.

When Ralph Langner and his team got a hold of the virus, they infected their own systems in an attempt to get the virus to attack so they could better understand its intent. Langner's team soon found out that Stuxnet would not take the bait and attack as they expected. This made them realize that this must be a directed attack. Upon further investigating, they found that what Stuxnet was looking for were certain PLCs with a specific configuration.

In the initial discovery of Stuxnet, Symantec found that two servers, one in Malaysia and one in Denmark, were the sources of this attack. The servers were reachable through the websites www.todaysfutbol.com and www.mypremierfutbol.com. They were registered under a false name and a forged credit card. With this new information, they decided to monitor Stuxnet by redirecting the communication from the two servers to their own servers, located in Dublin. By doing this, they were able to see how many computers (around 100,000) were being infected and where the infections were taking place. So when it was found out that 60% of the total infections were located in Iran, it seemed very likely that they were the target of this attack.

Method of Infection and Spreading

During the time spent dissecting Stuxnet, they started to learn what it was doing. They found that the virus used five vulnerabilities, four of which were Zero-Day Exploits. It was found that Stuxnet initially infects machines via USB sticks. It was able to do this easily by using a .LNK Zero-Day Exploit on the machine it was in. This allowed it to install itself on the machine without any user interaction whatsoever. It also contained two certificates, one from RealTek and one from Jmicron, to give the idea that it was a legitimate program. It would use two more
exploits, one from the keyboard file and one from the task scheduler file to increase its own privileges in order to gain full control. It would then spread by using its last Zero-Day Exploit. This one involved using a shared printer's print spooler. By using the exploit in the software for the print spooler, it was able to infect another computer using that same printer, treating it like a Local Area Network.

**Attack Algorithm:**

They found that Stuxnet was looking for computer systems that were running Siemens Step7-300. When it found this system, it notified the servers and would verify the target. When it found the appropriate target, it would then drop the malware into the system in order to infect the PLCs. The infected PLCs would then start to act strangely, the malware would speed up the centrifuges to 1410 hertz for 15 minutes, then return to the normal operating speed of 1064 hertz. It would then wait for 27 days before slowing down to 2 hertz. After waiting another 27 days, it would repeat this process until the centrifuges cracked and/or exploded. This was one of, if not the first time that a virus was used to physically sabotage an object.

With the sophistication of this code, the fraudulent certificates, and the fact that Iran was the source of the attack, Stuxnet started to look like the product of a covert government operation. But they still had to know what they were attacking.

After the revelation that this could be the result of a government operation, some questions started being brought up by Symantec. Should they publish their findings for the world to examine? Should they even stop this attack? What benefits or harms will come from choosing one way or another? And who would benefit or be harmed by our decisions? These are some of the central questions about cyber warfare, specifically for anti-virus companies. By publishing these findings, they could be causing sensitive information about a crucial government operation, meant to prevent a potential disaster, to be leaked, and inadvertently cause an even worse disaster, such as war. If they don't disclose this information, they are doing a disservice to their clients, and in fact not doing what they promise their clients they will do. This is why these issues need to be examined, and they will be according to some of the foremost ethical theories.

**Ethical Theories:**

According to Immanuel Kant in his first formulation of the categorical imperative. If one cannot will a choice to be a universal law, it is ethically wrong. When applied to this situation, Symantec must either believe that they should never disclose information about viruses that they know about, or they must always disclose information about what they find. If they were to never disclose information, clients would never know what is happening on their own systems, and therefore would not know what measures to take to prevent a future attack. The client would likely distrust the company and look elsewhere for protection. This would likely cause the business to quickly collapse. From this, it seems fairly obvious that it is wrong to withhold information about an attack from a client.

Under the second categorical imperative, one should never use another person as a means to an end. The problem is that now, Symantec fears that they maybe giving information about a government attack. If this is true, there would likely be some legal issues, but withholding their information is not in their client's best interest. Symantec can be considered to be using their client as a source of income, and from that, a means to an end. If they do release this information though, it may not be in Symantec's best interest, thereby causing their client to receive information that they want, regardless of what happens to the company or employees, causing Symantec to be used as a means to an end by the client. It is evident that this is a no win scenario and a clear right and wrong cannot be derived here.

Under Act Utilitarianism, an action is right if the overall benefit outweighs the overall costs. A couple benefits to letting others know more about the virus are that it saves Iran the cost
of replacing all future damaged centrifuges and the cost to learn how to remove the virus completely on the client's own. It likely keeps Iran's facilities as Symantec's client, and provides valuable information that others can use to better understand what Stuxnet is, does, and how to stop it and other similar attacks.

A couple costs of letting them know are explained as follows: A European intelligence agency did an analysis of Stuxnet and decided that it would have taken a programmer three years and tens of millions of dollars to develop, showing that not only was this backed up by several skilled programmers, but also that they were significantly financially backed. As has been stated, it seemed likely that a nation state was behind the virus, so if Symantec were to disclose their information, all that work and expenditure would be wasted, and possibly worse, would allow for copycats to use the information about the virus to create viruses of their own, this may even cause the release of what one may call Stuxnet 2.0, or son of Stuxnet, as Sean McGurk, head of cyber defense for the Department of Homeland Security called it. 'You can download the actual source code of Stuxnet now and you can re-purpose it and repackage it and then, you know, point it back towards wherever it came from ... They [creators] opened up the box. They demonstrated the capability. They showed the ability and the desire to do so. And it's not something that can be put back.' From this, one would likely think that disclosing this information would be the wrong action to take.

Under Rule Utilitarianism, we need to assume the proposed rule, “If I believe there's a possible danger by giving my client information, I shouldn't do so.” Some benefits from this are that any possible dangers would now be avoided, and from this avoidance, there is a possible local or global improvement.

Some harms from this are that the client now lacks information to prevent future attacks, and really, there is no certainty that any danger was truly avoided. And lastly, this may slow down progress for the affected parties. Based on these costs vs. harms, it should be believed that the rule is good. This is because any business that remains in good standing would likely take this decision very seriously because of the possible frustrations of the client or even the loss of the client to another company should the company choose non-disclosure.

The last ethical theory to look at is the Social Contract Theory. Under this theory we need to first assume some universal rights for all parties. Other than the obvious rights, such as life, we need to first decide who has what rights. Symantec has done the work to understand Stuxnet and what and who it is attacking. It is generally believed that you own your work, therefore you can do as you wish with it. But, since their customers are paying them for protection, one must ask, does the customer have rights to information about an attack that they are the victim of? If so, are these rights limited or absolute rights? When one can answer these questions, the ethical choice will be known.

Next, should Symantec stop Stuxnet? We will first assumed that Symantec chooses to let these attacks take place. According to Kantianism's first categorical imperative, the proposed rule that is derived from this decision is that it is okay for anti-virus companies to let computer attacks take place. The problems with this rule is that this inherently defeats the entire goal of anti-virus companies to protect systems, and therefore is bad for business. So because of this, it would be wrong to let attacks take place.

Under the second formulation, we assume Symantec chooses to let these attacks take place, in this case, we already know that Symantec is not keeping their client's best interest in mind. But now, since no information is leaked, there is likely less, if any issues with stopping this attack. So now, Symantec is using their client as a source of effortless income, and therefore, they are the only ones using someone as a means to an end. Because of this, it would be wrong to let such attacks take place.

Under Act Utilitarianism, we once again assume that Symantec chooses to stop the attack. The benefits from this are that the client saves the cost of buying the many new centrifuges that
would have been destroyed in the future. And now, the nuclear program is no longer delayed.

The costs of preventing such an attack once again are that the attackers time, money and energy is now wasted. It seems that the money saved by Iran seems greater than the attackers losses and because of this, it would be right to stop the attack.

Under Rule Utilitarianism, the proposed rule assumed is, “If I feel that a client's systems are being attacked to protect others, I should allow said attack to take place.”

If anti-virus companies were to follow this rule, they would no longer be trusted to protect clients' systems. A paradoxical point is that allowing this practice would require an incredible amount of trust in a company's decisions.

Another interesting result of this rule comes to light, but first, a little background is needed. Currently, the United States and interestingly, the Czech Republic, currently have the largest market share of anti-virus protection. It is generally safe to assume that anti-virus companies are likely to have the same or similar values as the country they're from. Because of this, there is greater leverage for residents of these countries and the countries themselves to push their interests onto the rest of the world. This would give an unfair advantage to the residents of these countries and the countries themselves, and would give far too much power to anti-virus companies. Therefore it is wrong to let anti-virus companies choose who can be attacked and when they can.

Lastly, under Social Contract Theory, we once again look at the rights of the company and the client. It is already known that clients pay anti-virus companies to protect their systems. It is therefore reasonable to believe that the clients company will fulfill their duties, and that anti-virus companies don't generally have the right to choose to not fulfill duties that they were paid to do. So under Social Contract Theory, it is wrong for companies to choose when and when not to protect a paying client's systems.

Based on these ethical theories, it is fairly difficult to determine whether or not an anti-virus company should disclose information about an attack because each of the ethical theories either give conflicting answers or answers that cannot be uncovered until more information is known. But it seems fairly safe to say that the ethical theories are in consensus that antivirus companies must stop computer attacks, no matter who the client is.

In the end, Symantec chose to disclose all information they ever uncovered. But this wasn't always a guarantee. As O'Murchu said, “If it had got to the point where we had found 100 percent attribution who was behind it, I think we would have had some really serious conversations about publishing that.” They also believed it was right to always protect client's systems, no matter what. As Eric Chien stated, “It's a threat, it's affecting people, we gotta look at it. I think that's the bottom line for us, no matter what it is … we're not beholden to a nation … we're a multinational, private company protecting customers.”

These are not the only ethical issues that anti-virus companies have to face. Ones that needs to be talked about are anti-virus companies’ responsibilities when war arises; for countries to properly determine what is and is not considered an act of war; and to determine what should and should not be done when attacked. These issues need to be discussed and guidelines for these decisions need to be set before more or worse incidents happen. According to former U.S
intelligence chief, Mike McConnell at an RSA conference, the U.S is likely to do nothing until an attack occurs, then overreact, rather than plan ahead. Some guidelines he believes should be set are that espionage and information theft should not be considered acts of war, but that destruction of data and systems are, and even then, the scale must be large enough and the origin of the attack must be known. Some problems that already arise are that the origin of the attack itself would be the most difficult to determine. And that even if the origin is known, it would still be difficult to determine if an attack was really an act of war based on the scale. After all, it could very well be an act of espionage that went wrong and accidentally caused the destruction of data and systems.

James Lewis, the moderator of the RSA conference said viruses such as Stuxnet needs to be viewed in the same light as we would view Israel’s evident bombing of a suspected nuclear facility in Syria in 2007. “If one is war, the other one is, if one isn’t, the other one isn’t.” This is an interesting idea, and is worth examining. The ethics behind war is out of the scope of this paper. So this needs to assume that war is neither ethical or unethical.

Under Kantianism’s first categorical imperative, the rule is assumed that if data and systems are destroyed, it should be considered an act of war. If this rule were to be followed, it would mean even small attacks, such as the destruction of a small business’ database, if done by another country, should be considered an act of war. This is the reason why McConnell also stated that the size of the attack must be large enough. But another problem arises. In the case where two countries are at war, acts of hacktivism that are part of a protest of the war would have to be considered an act of treason, which is generally not the intention of hacktivists. Therefore, it would be wrong to consider the destruction of data and systems acts of war.

Under Kantianism’s second categorical imperative, an experimental situation is examined involving two countries. In this situation, one country has destroyed the entire database for a well known American news company, such as CNN. For fear of more attacks, the U.S is responding by declaring the attack an act of war. In this case, the information about the attack is being used to determine whether the attack was an act of war, but the company itself is not being used as a means for determination. So it must be considered that under the second categorical imperative, declaring the destruction of data and systems an act of war is ethical in the sense that no one is being used as a means to an end. Because the first and second categorical imperatives conflict each other, Kantianism is too unreliable to determine the ethics of declaring an attack an act of war.

Under Act Utilitarianism, we assume the same experimental situation. Some benefits that are derived from this are that other similar attacks would be less likely because of the quick military response of the United States, and the benefit that weapons manufacturers would likely gain a large profit, these would likely be the only benefits. The costs of this are the time and money that would be spent at war with the attackers, which could be years and millions or billions of dollars. Another cost is the lives lost while at war. The same losses would also be felt from the attacking country. So, for this reason, declaring the destruction of data and systems an act of war would likely gain much less benefits than it would costs and therefore, should be considered an unethical response to an attack such as this.

Under Rule Utilitarianism, the rule assumed is that the destruction of data and systems should be considered an act of war. Some benefits that come from this are that attacks would be far less common, since the first fear that the attackers would realize would be that this attack may end up causing the country to go to war. This assumption should be considered true because in general, a country attacking another via computer likely does not want physical confrontation. Because of this, much data, and likely millions of dollars is saved from unimplemented attacks. Some costs to this are lives, millions of dollars on both sides, and the time spent at war with the opposing country. From this, it would be safe to say the costs
outweigh the benefits, therefore it is wrong to declare destruction of data and systems an act of war.

Under Social Contract Theory we examine the rights of the attackers and the attacked. We know that both sides have the absolute right to life and the positive right to have property that's free from destruction, which means some negative rights that would be assumed are the negative right to attack or kill someone and the negative right of the destruction of property. These are all rights that are already being violated by both parties at this point, so the best course of action would be to determine the value of each of these rights, and determining which rights are being violated the most. By determining these, one can determine the greatest violation, and therefore, what should not be done.

Most people would likely agree that the right to life is greater than the right to property, since most people would give up their own property before their own life, and that the destruction of a large corporation's data would likely be of far less valuable than the destruction of life and property that would come with war. It is for these reasons that under Social Contract Theory, declaring the destruction of data and systems an act of war would be highly unethical.

Based on these four ethical theories, it can be safely determined that declaring the destruction of systems and data an act of war is an unethical response to an attack. Therefore, the U.S needs a new and better strategy for handling cyber attacks.

Conclusion and Current Events:
As was discussed, information and virus control is a major ethical issue for anti-virus companies, and there are also issues in determining whether an attack should be considered an act of war. These are only the first types of questions that need to be discussed in the coming decades. There are still many other issues at hand, such as how much can be sacrificed to stop another cyber attack, or the cost of choosing cyber attacks vs. militarized attacks. Although questions such as these haven't been answered yet, the emergence of Stuxnet has got many researchers actively searching for a solution that will both be ethical, and of the highest benefit to all.

After the investigation, Israel's Mossad and the United States have taken credit as the ones who created and launched Stuxnet. This was done because of the fear that if Iran would have nuclear resources, they would use it to make nuclear weapons that could be used in an attack on another country. Meir Dagan, Head of the Mossad, spoke about Stuxnet. He spoke about the risks of a military strike against Iran, he spoke about how this method of attack would cause an eventual war with Hezbollah and Hamas, and Syria. He also explained that any physical attack would at best slow down the nuclear program. This is why they decided that the use of bombs were out of the question. Currently, it has been found that Stuxnet has at least four other cousins. The most known of these is a virus known as Duqu. The recently known goal of these viruses is to search for their cousins by searching a computer's registry for specific keys linked to Stuxnet and Duqu. Iran has obtained new centrifuges. These new centrifuges are designed to be able to spin up to and above 1410 hertz and should be able to withstand attacks similar to Stuxnet. Even though the U.S and Israel fears that Iran is going to use nuclear technology to create nuclear weapons, there 118 nations that believe otherwise. They believe that Iran has the right to nuclear technology for the purpose of pursuing peaceful endeavors such as using clean and cheap energy. This is why on August 31, 2012, these 118 nations declared their support for the continuation of Iran's nuclear program at the Non Aligned Movement conference. Whether this is a good idea is something that will not be able to be determined until either Iran attacks, or proves that nuclear bombs are not of interest to them. So now the final question is, was the use of Stuxnet to destroy Iran's centrifuges a justifiable attack?

Only time will tell.