Over the past couple of decades, the United States has become increasingly interested and involved in the use of cyber warfare in cyberspace. Advances in the use of the internet, as well as other cyber technology has prompted a new frontier in the way conflicts are handled between opposing countries. Cyber weapons have also seen dramatic advances by both our government and by military for defense and offensive uses, strengthening the United States' military capabilities. The technological advantages that the United States has over a majority of the countries in the world has allowed them to The United States is not the only country that has access to cyber weapons, though.

Initially, the United States' use of cyberspace was not meant to be launched as a means of attacking other countries. Security and defense of the government in the world's accent into the digital era justified the need for more spending into the cyber sector. The initial response by the US government was to create programs that would help to defend themselves from potential cyber threats and hackers that would try to steal top secret information. Tom Gjelten, a reporter for National Public Radio, and the lead pentagon correspondent during the 9/11 attacks and the Iraq and Afghanistan invasions, reported the Pentagon created the "Strategy for Operations in Cyberspace" in July of 2011, in order to defend their own computer networks, not for the purpose of attacking others (Gjelten). It would have appeared that the government's intentions were merely to protect their own computer systems. In 2013, the Washington Post had reported that the Pentagon made the decision to significantly expand their cybersecurity programs across all of the branches of the government and Army, who also decided to create a new branch of forces, the first created since 1987. While all these branches rely heavily on the use of computer networks in order to maintain their functions, rapid expansion of these cyber programs seemed a bit more complex than just cyber security. The United States was clearly getting into other cyberspace areas outside the scope of just cyber security.

But why would a country such as the United States engage in the use of cyber warfare, when the US has one of the largest and most powerful militaries in the world? For starters, the use of cyber attacks does not require the use of soldiers and military force in order to execute. Cyber attacks also enable the aggressor to attack from anywhere in the world at any time, and while it may not cause any physical harm to the enemy, the attack has the ability to do vast amounts of damage to an economy, infrastructure or computer systems. Danny Vinik, an assistant editor of The Agenda at Politico News, writes of how the internet has made the physical distance between enemies basically irrelevant which makes attacks easier to carry out and harder for governments to monitor. Being able to carry out an attack without a government or defense agency tracking the attacker has made the use of cyber warfare much more lucrative than inflicting physical damage on an enemy. Another reason the US would use carry out sober attacks over the use of the military presence is that cyber attacks are typically a one-time deal. Because cyber security is a constant battle to fix and patch flaws in a security network, attacks are usually only used once before they are detected and unable to used again. Vinik goes on to state that, “If the government has a piece of malicious software and uses it to exploit a flaw in an enemy’s code, it could render future uses of that capability ineffective, since the adversary could just patch it” (Vinik). Using malware more than once is essentially ineffective, justifying the use of it only once.

As the United States continue to build their cyber security forces in order to secure their own networks, the government found that they could also use cyberspace as a mechanism for undermining their own enemies. While the average citizen went about their day streaming the internet for clothes, shoes, and on Facebook, the US government was using the internet in order to carry out attacks on their enemies without anyone knowing. The most prominent example of this is the discovery of the Stuxnet worm, a secret military cyber virus created jointly by both the United States and Israel, as part of a larger operation called the “Olympic Games”.

The operation was first created under the Bush administration in 2006, as a last-ditch effort of the administration to try to deal with Iran and their growing nuclear research. With Iran increasing the number of centrifuges to an upwards of 50,000, the fear of stockpiling uranium that could later be turned into bomb-material, crossed the mind of the US government. Unwilling to use sanctions for fear of the effects that doing so would have on other countries’ economies, the United States believed that an alternative course of action would be needed. The idea was to create a cyber virus that could successfully infiltrate the Iranian computer systems without being detected and affect the centrifuges, as well as the computer systems, without the engineers or technicians knowing why these anomalies were occurring. Ultimately, their goal was to make the Iranians believe that the malfunctions were a product of their own doing, rather than an attack on the facility itself. And while the attack was successful, the aftermath led to much more than just stopping the centrifuges.

Although the initial damage to the plant was successful, the repercussions of using the virus was not anticipated. The Stuxnet virus eventually made its way to the mainstream internet after a technician working at the plant had taking his infected computer home and synced up to the internet. The virus quickly spread around the globe and prompted action in order to stop the spread of the virus. Discovery of the use of the Stuxnet virus was concealed until 2011 when David Sanger, author and Washington correspondent for the Washington Post, wrote about it in his book Confront and Conceal. The Stuxnet virus was just one of the first known major cyber attacks that have been reported on, and although neither the United States nor Israel have admitted to be the creators of the Stuxnet virus, the use of the virus on an Iranian nuclear plant has shown the capabilities and damage of cyber warfare on a government.

The use of the Stuxnet virus was successful in the way it was able to infiltrate the Iranian nuclear plant and shut down the facility with such ease. Even though this was the case, ultimately, the discovery of virus and headline news stories have opened Pandora's box. The secret blueprint to creating a virus that can has the capabilities of doing the same damage to the United States, or any western country for that matter, as was done to the Iranian nuclear plant. German cyber expert, Ralph Langer, who was one of the first experts to analyze the Stuxnet virus after its discovery. In an with the Washington Post's Jason Ukman, Langer commented, "The bigger problem that we have with Stuxnet is not the virus itself – it is that various exploits used in Stuxnet can be copied and can be used against targets .... These systems remain vulnerable. These systems cannot only be found somewhere in Iran – they can also be found, for example, in U.S. power plants, chemical facilities, in production facilities for food and beverages, et cetera." (Langer) While the virus was only good for a single attack on a flawed system, replication of the same attack on another country with the same virus is not a serious threat. Langer foresees that variations of the virus can be used to attack much larger targets and do more catastrophic damage. Stuxnet may have caused calamitous damage to the nuclear plant as a means to slow down the progress of the Iranian nuclear program, but the repercussions of the discovery of the virus has caused great concern for many counties whose infrastructure and daily ways of life are dependent on computer systems.