An Ethical Analysis of the Actions of the Developers of the Stuxnet Computer Virus using Just War Theory

STS Research Paper
Presented to the Faculty of the
School of Engineering and Applied Science
University of Virginia

By

Michael Wood

Spring 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: ____

Approved: ______________________________________ Date ________________________
Benjamin J. Laugelli, Assistant Professor, Department of Engineering and Society

Introduction

The Stuxnet virus is a cyber worm most notably deployed in June 2010 against the programmable logic controllers (PLCs) of the uranium enrichment centrifuges at a nuclear facility in Natanz, Iran. When all was said and done, Stuxnet had destroyed approximately 1000 of the 5000 purifying centrifuges that Iran was using at the time (Sanger, 2012). It was developed by a nation-state (inferred later to be the United States) or coalition of nation-states with incredible espionage capabilities, because its implementation targeted a very specific set of machines, and was successful in destroying them.

The current ethical discourse around Stuxnet is mostly concerned with applying laws (both U.S. and international) to its physical effects on the Iranian centrifuges. Take this quote from David Fidler in his article “Was Stuxnet an Act of War? Decoding a Cyberattack?”: “Reviewing Stuxnet’s features, many international lawyers would see a deliberate, offensive, and sustained act undertaken through unprecedented means or methods, intended to cause physical damage or destruction, and perpetrated in all likelihood by a state or states against a perceived national security threat from a rival power,” (Fidler, 2011). This is a good assessment of the timeline of Stuxnet’s deployment as well as its characteristics, but it does little to morally assess the actions of the developers, especially in the context of being an act of war. The danger in going down this path is that we might forget that there are in fact *human* actors behind all that code and all those destroyed centrifuges.

In this paper, I will argue that the developers of Stuxnet were acting morally in creating and releasing Stuxnet because they were acting with support from the authority of the sovereign, because they were acting in line with a just cause, and because they were acting with rightful intention. In order to complete this moral analysis, I will be making use of just war theory.

Background

Stuxnet was unique among cyberattacks in that its main goal was to "physically destroy a military target," rather than simply perform espionage or alter information (Langner, 2011a) and in that it took advantage of 4 "zero-day exploits," meaning exploits that took advantage of previously unknown system vulnerabilities in the Natanz PLCs (Singer, 2015). It is unparalleled in its size and complexity, which allows it to evade detection even while dropping its payload corrupting controller logic.

Literature Review

A great deal of research has been done into the origins, virus timeline, and even the ethics of Stuxnet's implementation and deployment. However, most scholars focus on the facts of what occurred rather than making a statement on the morality of the development team. Even when the area of ethics is ventured into, the focus is on a broad concept of "good" and "bad," rather than utilizing specific frameworks and methodologies to formulate arguments. In addition, most articles that touch on the ethical aspects of Stuxnet make use of ethical points that are not strong enough in themselves to tell the whole story of morality with respect to the situation.

In his article titled "Stuxnet: Dissecting a Cyberwarfare Weapon," computer specialist Ralph Langner offers an in-depth breakdown of the nature of the Stuxnet code itself. For example, he describes the way in which the virus was able to cause actual damage. First, he explains that while Windows SCADA (supervisory control and data acquisition) systems were crucial to the spread of the virus, the real attack was "aimed at industrial [uranium centrifuge] controllers that might or might not be attached to a SCADA system," (Langner, 2011a). These controllers would determine the movements of physical devices such as "pumps, valves, drives, thermometers, and tachometers," (Langner, 2011a). Once Stuxnet had attained access to the controllers via physical USB sticks and local networks, it was able to cause the aforementioned devices to perform in such a way that would render them inoperable and the uranium unusable.

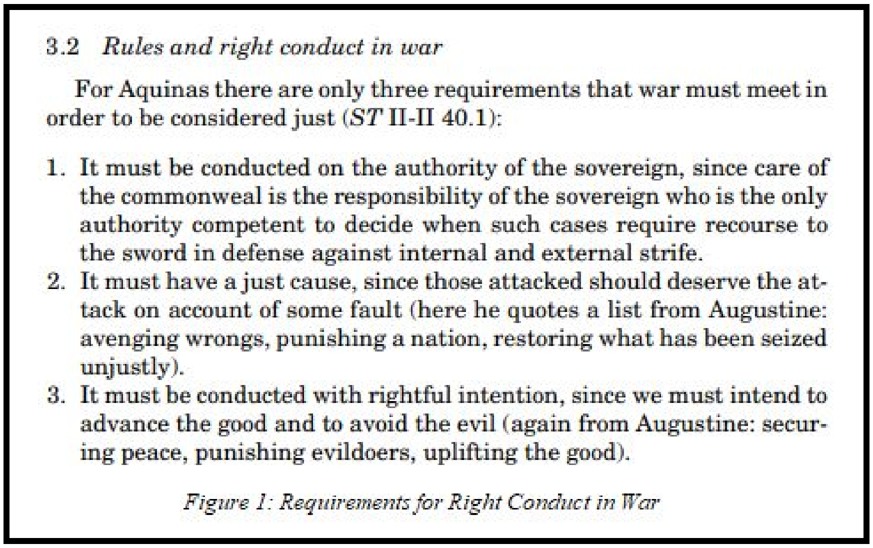
Langner fails to adequately include the human element in his analysis, treating the virus as standalone and mentioning only cursorily its developers. While Langner's discussion is mainly a technical one, the analysis provided allows for the reader to far better understand the nature of Stuxnet as a virus. This is, however, not to discount the importance of a thorough technical understanding of the virus when discussing Stuxnet, as they are critical to understanding the intentions of the developers.

P.W. Singer aims to analyze an ethical dimension of Stuxnet in his article "Stuxnet and its Hidden lessons on the Ethics of Cyberweapons." He cites the *jus in bello*, or "law in wartime," developed by legal thinker Hugo Grotius in the 1600s in order to make his point (Singer, 2015). Singer identifies the two most important elements of *jus in bello*: proportionality and discrimination (2015). Proportionality means that the effects of actions that are taken in the context of war by one side cannot outweigh that which provoked the conflict (Singer, 2015). Discrimination refers to the concept that "all belligerent sides must distinguish between non-legitimate targets (e.g. civilians or wounded persons), and do their utmost to only cause harm to the intended, legitimate targets," (Singer, 2015). Because Iran had previously obtained the nuclear centrifuges illegally, putting code in place that took the aforementioned centrifuges out of commission (with no physical injury) satisfies the proportionality element. Although it is true that Stuxnet infected many tens of thousands of computers around the world, it was inherently designed to only cause damage when the Natanz centrifuge configuration was detected (Singer, 2015), thereby satisfying (somewhat arguably) the discrimination criterion.

While there is value in both articles reviewed above, two deficiencies stand out. The Langner article, while useful for a low-level understanding of the Stuxnet virus, does not dive deep into the human factors of its development and is thus limited in its scope. The Singer article, while it puts forth an ethical analysis of Stuxnet's deployment, does not go in-depth enough with respect to its analysis. The *jus in bello* criteria of proportionality and discrimination are valid in themselves, but I do not believe their existence or non-existence are sufficient to declare morality or a lack thereof. In contrast, I believe that the use of just war theory, posited by St. Thomas Aquinas and expounded upon by Darrell Cole in his article "Thomas Aquinas on Virtuous Warfare," will be invaluable in forming a judgment of the morality of Stuxnet's development and deployment.

Conceptual Framework

The implementation and deployment of the Stuxnet virus can be morally analyzed using the framework of just war theory, as posited by philosopher St. Thomas Aquinas. Just war theory focuses on the criteria needed for acts of war to be considered morally acceptable (Cole, 1999). When dealing with moral acts, performed either by an individual or a collective, the relevant parameters at play are the actor(s), the intention that the actor(s) has/have in mind when performing the act, the object of the act itself, and (to a degree) the circumstances surrounding the act. In his article, Cole reproduces the three requirements that Aquinas deemed necessary for a war to be considered just. They can be seen in the figure below.



3.2 *Rules and right conduct in war*

For Aquinas there are only three requirements that war must meet in order to be considered just (*ST* II-II 40.1):

1. It must be conducted on the authority of the sovereign, since care of the commonweal is the responsibility of the sovereign who is the only authority competent to decide when such cases require recourse to the sword in defense against internal and external strife.
2. It must have a just cause, since those attacked should deserve the attack on account of some fault (here he quotes a list from Augustine: avenging wrongs, punishing a nation, restoring what has been seized unjustly).
3. It must be conducted with rightful intention, since we must intend to advance the good and to avoid the evil (again from Augustine: securing peace, punishing evildoers, uplifting the good).

Figure 1: Requirements for Right Conduct in War

Despite the fact that Aquinas's original intention was to have these criteria be applied to wars on a macro level, I will apply them to Stuxnet, which can be thought of individually as an act of war. These criteria can be applied for a couple of reasons. The evidence overwhelmingly supports the notion that Stuxnet was developed with the support of at least one nation-state, namely the United States (Sanger, 2012), which means that Stuxnet was an attack on one sovereign nation perpetrated by at least one other. In addition, these criteria encompass all of the aforementioned aspects of a moral act, or more specifically acts of war: the actor, the object, the intention, and the circumstances. Because of these reasons, Aquinas's just war framework is best suited to determine the moral character of the Stuxnet virus's development and subsequent deployment.

Analysis

The developers of the Stuxnet virus were justified in their actions of creating and releasing it to accomplish its given task of laying siege to Iran's uranium enrichment centrifuges. In order to show this, I will demonstrate how the aforementioned actions comply with Aquinas's three requirements for a just war (or in this case, act of war). These three requirements are laid out in Figure 1 above, but I will reproduce each here. First, for an act of war to be considered just, it must be carried out "on the authority of the sovereign," (Cole, 1999), meaning that the act of war must have been carried out by or with the support of the collective currently in power of the acting nation. Second, the act of war must have some "just cause, since those attacked should deserve the attack on account of some fault," (Cole, 1999). Third, the act of war "must be conducted with rightful intention," (Cole, 1999) which means that the actor must intend for only good results to come from it. In showing that all three of these criteria are met, I will conclude that the use of Stuxnet in context of a cyberattack was indeed justified.

Sovereignty

There is a multitude of evidence which supports the notion that Stuxnet was developed with the support of and under the direction of at least one national government, namely those of the United States and/or Israel (Sanger, 2012). David Sanger of the New York Times reported in 2012, "...President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities." Sanger goes on to mention that his information was coming from both American and Israeli officials with inside knowledge of the program, none of whom were willing to give their names due to the classified nature of the project (2012). Sanger notes that the goal of Stuxnet was to "[slow] Iran's progress toward developing the ability to build nuclear weapons," (2012). Accomplishing this, of course, would be in the best interest of the United States, especially considering that rocky relations between the two nations date back to the early 1950s (Ekmanis,2020).

Given the concerns outlined above, especially those related to Iran's pursuit of nuclear weapons, I am sure that the Stuxnet virus was developed with the support of the United States' sovereign/government. It appears that the US government, acting within its authority to "decide when such cases require recourse to the sword in defense against internal and external strife" (Cole, 1999), set the Stuxnet project in motion with the end goal of pursuing the common good of United States citizens (insofar as protecting citizens from an international nuclear threat is pursuing the common good). Taking all of these factors into account, it is clear that Stuxnet has met this first requirement, because the evidence suggests that it was set forth from the highest levels (Sanger mentions that Obama had significant input) of the US government to promote the common good and protect from external strife.

Just Cause

Similarly, there is a great deal of evidence to show that the United States had just cause to develop the Stuxnet virus and utilize it to wreak havoc on Iran's uranium refinement centrifuges at Natanz. Ralph Langner put it very well in his viral TED Talk from 2011 about Stuxnet entitled "Cracking Stuxnet, a 21st-Century Cyber Weapon,": "The idea behind the Stuxnet computer worm is actually quite simple. We don't want Iran to get the bomb. Their major asset for developing nuclear weapons is the Natanz uranium enrichment facility," (Langner, 2011b). However blunt, this quote gets right to the heart of the issue. The United States did not want Iran, a country with whom the United States did not get along with very well, to hold any sort of capability to construct nuclear weapons. In 2007, Iranian leadership stated that "its goal in developing a nuclear program is to generate electricity without dipping into the oil supply it prefers to sell abroad, and to provide fuel for medical reactors," (Richardson, 2011).

As noted above, Singer reported that Iran had *illegally* obtained centrifuges to conduct illicit nuclear research at its Natanz site (2015). Up until this point, it was a bit difficult to map what Iran was doing to some "fault" for which the United States would have been justified in attacking them. However, the fact that the centrifuges were obtained illicitly adds some intrigue to the case. One can assume that because Iran was trying to hide its activities, it knew that some or all of what it was doing was wrong. Minimally, it knew that it should not have been conducting research into nuclear weapons. Treating this illegal obtaining and use of centrifuges as the "fault" within the just cause requirement allows me to say that Stuxnet meets the just cause requirement for a just act of war.

For what it is worth, the case for just cause is helped by the United States' preemptive efforts to achieve a "real (just) peace," (Cole, 1999) for the world, since it is highly unpredictable what Iran would do with nuclear weapons if it were to produce them.

Rightful Intention

Finally, there is a myriad of evidence to show that, as an act of war, Stuxnet was executed with rightful intention. The majority of this evidence lies in the design of the virus itself. When the Stuxnet infected a windows machine, it began a comprehensive process of target matching to see if the current system was the one that it was programmed to attack (Langner, 2011a). Langner argues: "it is even possible to infer… that Natanz must have been Stuxnet's one and only target, because this is the only installation globally where controller infections have been reported" (2011a). This speaks to the specificity of the target matching process. That is to say, the developers of Stuxnet were careful to implement it such that the only affected controllers would be those located in the Natanz nuclear enrichment facility. According to Singer, the virus only targeted a "cascade of centrifuges of a certain size and number (984)... the exact setup at the Natanz nuclear facility," (2015). Stuxnet is an example of how the use of cyberweapons can minimize collateral damage (Jenkins, 2013), and having its destruction be as precise as it was surely supports that assertion.

In short, the design decisions made by Stuxnet's creators to make its target as specific as possible display clearly that they were acting with rightful intention. Now, some might argue that to develop a virus in the first place is to necessarily stray from the intention to avoid evil. They might argue that because many tens of thousands of computers were infected with Stuxnet, that in itself has become an evil act and cannot meet the requirements needed to be considered a just act of war. The breach of privacy on the parts of these computers' owners, they might say, is not worth the possible marginal benefit gained from the virus's payload. I do concede that having Stuxnet spread as it does (it is a worm, or virus that utilizes a network to spread from computer to computer, after all) is not the ideal case. However, in addition to remaining inert if the host computer system does not match the target configuration, Stuxnet only allows itself to spread at most three other computers (Singer, 2015). On top of this, as a sort of catch-all, Stuxnet was programmed to completely destroy itself in 2012 (Singer, 2015), so that it would be guaranteed to not have any adverse effects.

In this situation, the good was intended in that the avoidance of a nuclear weapons race was achieved, at least temporarily. Evil was avoided (or at least put off) in that Iran's nuclear program was delayed by approximately 18 months to 2 years (Sanger, 2012). Considering all of the preventative design choices made by the developers of Stuxnet, and given that the only adverse effects (i.e. controller infiltration) of the virus occurred where they were intended, I can reasonably conclude that the aforementioned developers acted with rightful intention and that the third requirement for a just act of war is satisfied.

Conclusion

I have argued here, using tenets of just war theory, that it is possible to judge the actions of the Stuxnet developers as morally good first because they acted under the authority of the sovereign, which means that they were charged with their task by those whose responsibility it is to uphold the common good (the sovereign/government). Secondly, their actions can be judged as morally good because they had just cause to deploy the virus as they did. In short, it would not be in the United States' best interest for Iran to either be conducting illicit nuclear research or stockpiling nuclear weapons. Both are made possible by having functioning refinement centrifuges. Finally, the Stuxnet developers' actions can be deemed morally good because they acted with rightful intention. The virus was designed to pack a punch, but it will only cause harm to the very specific targets it is geared towards (Iranian programmable logic controllers).

As humanity moves into an increasingly more technological age, the appearance of cyberweapons will no doubt increase in frequency. Just as Stuxnet was a paradigm shift from previous generations of viruses, so too will Stuxnet be overtaken by other viruses many magnitudes more complex than it. Denning notes that Stuxnet will likely even "inspire, accelerate, and serve as a building block for the development of new cyber-weapons that target [industrial control systems] devices" (2012). As this happens, it will become more and more important to continue to evaluate them in terms of their morality, and the just war theory is a great place to start.

Word Count: 2962 (figure included has 133 words)

References

Cole, D. (1999). Thomas Aquinas on virtuous warfare. Journal of Religious Ethics, 27(1), 57-80.

Denning, D. E. (2012). Stuxnet: What has changed?. Future Internet, 4(3), 672-687.

Ekmanis, Indra. “The History of US-Iran Relations: A Timeline.” pri.org, Public Radio International, 3 Jan. 2020

Fidler, David P. "Was Stuxnet an Act of War? Decoding a Cyberattack," in IEEE Security & Privacy, vol. 9, no. 4, pp. 56-59, July-Aug. 2011.

Jenkins (2013) IS STUXNET PHYSICAL? DOES IT MATTER?, Journal of Military Ethics, 12:1, 68-79, DOI: 10.1080/15027570.2013.782640

Sanger, David E. “Obama Ordered Wave of Cyberattacks Against Iran.” New York Times, 1 June 2012.

Singer, P. P. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case Western Reserve Journal of International Law, 47(1), 79-86.

Langner, R. (2011a). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

Langner, R. (2011b). *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon* [Video file]. Retrieved from www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyber_weapon

Richardson, J. (2011). Stuxnet as cyberwarfare: Applying the law of war to the virtual battlefield. John Marshall Journal of Computer and Information Law, 29(1), 1-28.