Tony Janus

NET-100

10/13/2024

Stuxnet: The Crossing of the Digital Rubicon

It was 2006, the era of the Bush Administration. September 11th had occurred years prior, and the public had already become aware that the warnings of weapons of mass destruction in Iraq had been unfounded. People were growing weary over the war on terror and had begun to question the US government and President Bush's motives in the Middle East. The Bush administration was in a tough position, because though public distrust was growing, signs were pointing to Iran having begun working on developing nuclear weapons.

The public story was that Iran was utilizing the radioactive material they were obtaining for their sole nuclear power facility, however the US government strongly doubted this due to the sheer volume of material Iran was importing. Iran began enriching uranium at an underground facility at Natanz. This facility became known to the US only three years prior. Mahmoud Ahmadinejad, president of Iran at the time, intended to install 50,000 centrifuges to enrich the uranium they were receiving from Russia, again for the supposed intended use in the country's single nuclear power reactor.

However, because of tensions and ongoing war in the region, a military strike would have provoked too much of a response, which would have cascaded into a likely global conflict. So a plan was created to develop code that would ultimately hamper or even take down Iran's

enrichment operations. Once the US deployed their beacon programs onto the hardware destined for the Natanz facility and later received information from those beacons detailing the electronic directories, blueprints, layouts, and more of the facility's systems, they began to test their malware on the same hardware being used by Iran, which the US had obtained when Qaddafi stopped his nuclear program in 2003.

After weeks and months of testing, the worm worked and caused the self-destruction of the centrifuges. So, now that they knew this bit of code they had developed qualified as a successful cyberweapon, in conjunction with Israel, the US deployed Stuxnet. Through social engineering, essentially using a buffoon with a thumb drive to gain access to air-gapped systems, the Stuxnet worm was installed in the facility and began its work.

Over time, Stuxnet allowed the US to not only hamper the facility's output, at first only causing a few centrifuges to malfunction, but eventually to cause entire sections of the facility to be brought offline and analyzed, employees and experts working at the facility to be fired, and even the Iranian government to question its own competence and overreact to the situation.

Over the years, the Stuxnet worm, called Olympic Games by the US government, stalled Iran's nuclear production and caused both mechanical and cultural chaos within the facility. Then in 2010, when a new variant was deployed in Natanz, catastrophe struck. Reports of a new worm were coming in from around the world. Stuxnet had gotten out, and it was replicating itself on Windows computers everywhere. Security experts could now analyze the code, figure out what it was doing, and try to determine where it came from.

While this was a major concern for the then Obama administration, they continued with the program, soon taking down just under 1,000 centrifuges only a week after Stuxnet's escape had been discovered. However, even given the program's success, Stuxnet was out in the wild. Blame would eventually be placed on the US, and now the worm could be reverse-engineered and used for attacks that it was never intended to be used for by agents it was never intended to be used by.

Would this program qualify as cyber-terrorism? If an attack like this were to have happened against the US, I'm pretty sure it would have been labeled as a cyber-terror attack. And in recent years, we've seen many cyber attacks against the US, which while not given the media fanfare they may have been given in the 2000's, are discussed using the language of terrorism and cyber warfare. I don't think we can say Stuxnet wasn't cyber-terrorism just because it was our own government perpetrating it. Terrorism is terrorism, cyber or otherwise, regardless of who's doing it. So yes, Stuxnet was an example of cyber-terrorism, and it was a historic moment. It was the crossing of the digital Rubicon. Before Stuxnet, cyber-attacks were more about infiltration and information gathering. Stuxnet was the first time a piece of malware resulted in the kind of damage that only military strikes with physical weaponry could have caused before then.

As for whether it was ethical or not, that's a question I'm not so sure can be answered concretely. If Iran was truly trying to build out its nuclear arsenal, the argument can certainly be made that the attack was justified. Iran with a nuclear stockpile means big problems for Israel and its allies, and if an attack were to happen, the consequences would certainly be global conflict. Questions regarding what ramifications the Stuxnet attack would have on US security

have been raised as well. Given that the US has perpetrated cyber-terrorism, would this now embolden hackers and terrorists to become more extreme with their tactics against the US? Does this give them the justification to cause damage to the US and harm to its people? These questions directly impact the conversation on whether the US had the ethical grounds to launch such an attack. While Stuxnet may have prevented Iran from launching nuclear attacks, or at least slowed down their development of their nuclear arsenal, it placed a giant target on the US and its infrastructure. Was the US government in the right to bring that potential upon its citizens?

A part of me says no, that a nation's leaders should do all they can to protect its population and prevent anything that may bring even the potential of harm. However, I do not live in the land of fairy tales and copium. I fully understand the nature of war and conflict, and sometimes sacrifices must be made to prevent an even greater tragedy. If Iran had gained nuclear capabilities and launched missiles at Israel, the US would have been dragged into a nuclear world war, the death toll of which would have been catastrophic, and the damage done to vast areas of land, making them uninhabitable, would have been nearly impossible to recover from. So, I think that while it is always ideal to avoid conflict and those things which would lead to it, the US took the most ethical route it could. We are certainly still dealing with the fallout that resulted from that decision, as is most of the Western world. But considering the potential scenario we avoided, I have to say that it was worth the cost.

Of course, it would have been ideal to avoid those consequences, some of which we may not even be aware of yet even so many years afterwards. I must wonder how much malicious code is out there on the internet, causing problems with national infrastructure and affecting

the personal and private lives of our citizens, was written using techniques learned by studying the Stuxnet code. The fact it escaped what was meant to be containment within the Natanz facility and infected computers around the world not only damaged the US's relations with allies and neutral nations, but essentially acted to serve our enemies technology, which they otherwise could not develop on their own, on a silver platter with a note saying "You're welcome to use this against us" delivered with it.

So as with most of the topics we've covered this semester, there is no well-defined right or wrong in this instance. There are valid arguments for the ethicality of the attack, and against the ethicality of the attack, though at least this time I have a clearer and less ambiguous position than I have on previous topics. However, I recognize the arguments against deploying Stuxnet and find my position a difficult one to hold, though I suppose either position is a difficult one to hold. I find it most interesting how these events are portrayed in a certain way by the media, but then when I study them and get deeper into the facts, it seems that time and time again, there is no clearly defined right or wrong answer.

I find this extremely troubling given my firmly held belief in an objective morality given to us through divine revelation. And I would say that one of the key takeaways I'm getting from this class is the ability to separate my principled positions from my intellectual ones. It's been a roller coaster, emotionally and intellectually, to have my morality put into question through these conversations. Ultimately, though, I think I'm learning that while I can engage in these conversations from an intellectual purview, I must also begin to analyze these topics through the worldview of my Christian faith, applying my morality and my understanding of divine command to these conversations. Perhaps then, I will struggle less in finding my ethical position

on difficult topics. I think that's a more valuable thing to take from an ethics class than just a collection of facts and data, and for that, I'm grateful.

Sources:

- **Obama Order Sped Up Wave of Cyberattacks Against Iran** – New York Times, https://www.removepaywall.com/search?url=https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
- Stuxnet: Computer Worm Opens New Era of Warfare – CBS News, https://www.youtube.com/watch?v=6WmaZYJwJng
- Alex Gibney on What He Discovered Making 'Zero Days' – Engadget, https://www.youtube.com/watch?v=nmCCeD6Pj2o&t=27s
- Zero Days Cyber Security - https://ihavenotv.com/zero-days-cyber-security
- Data and Goliath: The Hidden Battles To Control Your World – Bruce Schneier