Ethics Situation Analysis: Is Digital-Self Defense Ethical

In this modern age of the wide spread of the internet, where crimes such as hacking can happen to anyone, is there a good case to be made for digital self-defense? Hacking in all its forms are illegal under U.S law, but should retaliatory actions be illegal? Certainly, retaliatory action can be a good thing. Shawn Carpenter was interviewed by Nicholas Schmidle, and that discussion covered this topic. Carpenter was a security analyst for a Nevada company called Sandia National Laboratories, and it was part of his job to deal with a hacking that took place in Florida which was most likely done by Chinese hackers (Schmidle, 2018). Legally, Carpenter could not do anything to get back at the hackers. They had stolen the data and that was that. This did not deter Carpenter, and in his own free time he managed to counter the actions of this group; tracing them back to China, he even eventually got the U.S government involved (Schmidle,2018). Legally speaking, everything that Carpenter did was illegal under U.S law. However, his findings were that these Chinese hackers had important documents that they had stolen from the United States and his actions were clearly in the interest of national security. So, we the public should consider, should that really be illegal? Reinicke, Cummings, and Kleinberg (2017) discuss the matter in their work and compare it to international relations. To summarize their point, nations used to be the only actors capable of vying for power. This has changed, in the modern age every individual is can pose a threat to one's agency, thus just as a nation has right to defend its borders so do individuals have a right to defend themselves (Reinicke et al., 2017). They then delve into the counterpoints against the idea of the right to digital self-defense, which are more substantive than the simple issue of illegality. Hacking organizations like the IEEE have affirmatively banned anything malicious. One issue is collateral damage, it is mentioned that hackers may use compromised systems to do their hacking, meaning retaliation would be against a victim (Reinicke et al., 2017). Thus, they claim that retaliation should be handled by professionals and not armatures.

With all of that as the established situation, is digital-self defense ethical? The popular perception of a hacker is certainly not a positive one, but it is hard to look at Carpenter and see someone motivated by anything more than a desire for justice. The fact that what he did was illegal is rather inconsequential to the ethics. Simply put the law can be wrong, it is an imperfect reflection of societal expectation and it is not the source of all moral consideration. That being said, it is a guideline set in place so that individuals have an incentive to not interfere with each other and to punish those who disregard the law. In that respect, the law is effective, hacking is a crime, and one will be punished if they are caught doing it. The only issue with that is implementation, it fails to consider the nature of the internet, and the relative anonymity one can achieve via technologies like virtual private networks, encryption, and much more. Retaliatory action then provides the hacked with a method of tracing down the individuals who hacked them, as Carpenter did when he traced the hackers back to China (Schmidle, 2018). Of course, much more could be done, more damage than simple tracking down of the perpetrator. Thus, as mentioned by Reinicke, collateral damage is a major concern. Ethically speaking it serves the hacked no use to damage the integrity of a fellow victim. That is something which should be deeply considered before taking an action, any chance of further damage to the innocent brings only more problems.

Reinicke, Cummings, and Kleinberg (2017) discuss the ethics of the matter in more detail and

consider the ethics of digital self defense in the context of utilitarian approaches. Specifically, they mention a utilitarian ethical, and a fairness utilitarian approach. The theory behind utilitarianism is that whatever actions bring about the most happiness are the best actions (Quinn, 2020). So, what action brings about the most happiness? Reinicke (2017) claims that ultimately, from these utilitarian perspectives, retaliatory action is both fair, and will bring about less cyber-attacks, thus bringing about the most good. This explanation of the ethical reasoning behind digital self defense feels inadequate however, simply bringing about good fails to satisfy the critique that the action is merely vengeance. From this place, it is an emotional response saying that it is better that some vigilantism occur for the betterment of all. A more complete approach would be to justify the act via the enforcement of the social contract. Quinn (2020) defines Social Contract Theory based on the work of Hobbes. That is, all living in society have agreed to a set of moral rules and the government can enforce these. Hacking is clearly a violation of moral rules, very few would dispute that idea. The issue is the difficulty the government has in enforcing the law. It is difficult to discern the specific method by which this problem may be remedied. From the example of Carpenter, the best method may be to take the route of informing proper authorities of perpetrators; while also giving detail of the specifics of the hack such as what systems were compromised, and what information was stolen. This fits best within the Social Contract theory as it maintains the authority of the government to enforce the law, while also allowing victims to take an active role in going after those who attacked their systems.

This solution is good, but it comes with issues, for instance there is still the potential for accusations of wrongdoing to be levied against other victims of hacking. Moreover, without proper precaution there may be methods by which an actual hacker may falsely claim to be a victim. Another concern could be false accusations. Perhaps a perpetrating hacker could compromise the systems of an innocent party, use their systems for nefarious purposes, and then accuse the victim of committing a crime. While cases like this could potentially be easy to solve, there is the potential to bog a victim down in legal concerns which require that they invest in legal advice before proceeding forward. It is for reasons like this that any policy passed should be of a careful nature. For concerns such as these, digital self-defense is not an area of policy for political disputes and battle as any error in the text could lead to the consequence of victims being prosecuted which is a fear that should not exist.

Of course, there are more considerations that one should make beyond the social contract. As mentioned before, one can think of the place of the individual as an independent entity facing threats as a nation state would (Reinicke et al., 2017). This perspective is not so much a Utilitarian approach but is much closer the approach of Ethical Egoism. Ethical Egoism is a philosophy based on the total self interest of the individual (Quinn, 2020). From this perspective one should ask, what is in the best interest of the individual when they are hacked? That is simple, recover anything stolen, and prevent further attacks. An egoist then could easily justify going further than simply finding the perpetrator and informing the authorities. An egoist may retaliate by embedding a virus into their data to destroy the machine of a hacker, which would certainly stop further hacking from that machine until it is rebuilt. This is most definitely too far, and a risky decision.

Independent of these ethical concerns, is the legal one, simply put the law is not properly providing a workable framework for an individual to take after being hacked. It feels as if the law is behind the technology, not yet fully grasping it. Thus, any changes in policy should provide more for the victims of hacking. As for whether counter efforts should be allowed to be carried

out, it would certainly be consistent with constitutional considerations of self-defense. The right to self defense in general is over a thousand years old and is a right enshrined by the United Nations (Reinicke et al., 2017). If there is no issue with legitimate self defense in the regular world, why then should the digital world be any different? The defense of a system will always be imperfect, sometimes a criminal will break into a home just as a cyber-criminal would break into a network. In both cases the passive defense has failed, why should an active defense be out of the question? It is reasonable to say that the matter should be at least considered by policy makers, even if they do not conclude it should be a legal form of self-defense.

Digital self-defense, all things considered, is a relatively new concept. It is not really any wonder why the law is not yet at a point where such a thing is considered legal. Law is not necessarily a perfect reflection of morality, and there are multiple perspectives from which it be a reasonable and legitimate option. From the point of view of a Utilitarian any action to stop subsequent acts of hacking are ultimately valuable and the just option. The Social Contract would agree, save for the fact that the betterment is for the society and not just for the victim of the hacking. Even an Egoist would agree that retaliation is a valid option, though to what extent an egoist would go is not necessarily clear. Here is a good example of why the law is not always the best place from which to derive moral guidelines, or at least a place where multiple perspectives would disagree with the law. In the future, with public motivation and awareness, the law may be changed to better protect digital rights.