Ethical Implication of Digital self-defense/hacking back

When thinking about digital self-defense, it is important to look at the whole scope of the action as well as the causes and effects. One thing to think of is that people in society are all different when it comes to decisions. One person could think that the way to defend against an attack is right, while another person thinks that is wrong. Everyone's ethical viewpoints on situations vary. It is the same thing with how people view digital self defense itself. Obviously, there are multiple different techniques that people to use to defend which makes the ethical implication of it a little more tricky as to if it is right or wrong. "It poses and creates some problems related to ethics ,and contains in general three main types of ethical issues: personal privacy, access right, and harmful actions" (Gunarto 2003). In any case, those three issues would help dictate whether or not the practice of digital self defense as a whole is ethically valid. Not everyone has the same knowledge of the cyberspace and how to defend themselves against threats. That would also correlate to how they see digital self defense and if it is right or not. There are not many laws on technology and how people can defend themselves so there is not a specific scope that people can operate their self-defense tactics in. Some people are more equipped with the knowledge to be able to defend off attacks directly aimed at them but some of those tactics could be deemed "overkill" in a way." Ethical reasoning in the form of judgements about good versus harm done, the level of proof required to act, and the matter of when and how to respond to actions in the cognitive domain will all be of critical importance moving forward" (Bjørguln 2023). In a sense, one way to look at this is through a comparison to is like if someone broke into your house with a weapon. There are a lot of ways you can deal with it, but some options are more morally accepted than others. This is the same concept but, in the cyberspace, and there are less laws, so it makes it more of a gray area. Having the policy of digital self-

defense does allow for people to realize that if they have the tools and ability to defend themselves then they can and should. Everyone has the right to privacy so they should be able to defend their right as well. If nothing else is protecting that right, they should be able to standup for themselves and act. “Important here is that if the state is not protecting its citizens or their interests (potentially invested in firms), the state is not fulfilling the terms of the social contract, whereby citizens accept the authority of the state in return for its protection. It follows that individuals (and firms) are permitted to protect their own interests and to use private firms to help them do this” (Pattison 2020). This is what that policy insinuates, it lets them see that they do have that ability to. There are multiple ways that people can defend themselves. They could personally do it with the tools they have, or they can get someone they know or hire someone to do it. It just depends on how they would rather go about it and how comfortable they are with it. If they thought it was wrong to personally, do it then they would hire someone else, but if they think that they are in the right by hacking back then they will do it themselves. Defense can only do so much which is why the policy lets us know that we can go on the offensive as a form of defense.” …Even if defensive measures might work *somewhat*, or be less likely to succeed, offensive force might be justified if it is likely to better protect your legitimate interests. For instance, if barricading your house might mean that only half of it is blown up, spilling the bomb-making material can be justified” (Pattison 2020). In terms of the ethics of what a person does, it is solely based on what each person thinks is morally acceptable to do. In a sense though, they are a victim of a cyber-attack/crime that breached their right to privacy so they have to stand up for their right in whichever way they can.

Works cited.

Gunarto, H. (2003, January). Ethical issues in cyberspace and IT society. In *Symposium on Whither the Age of Uncertainty. Retsumeikan Asia Pacific University*.

Bjørgul, L. K. P. (2023). –LEGAL AND ETHICAL IMPLICATIONS RELATED TO DEFENCE AGAINST COGNITIVE WARFARE. *Mitigating and Responding to Cognitive Warfare*.

Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233-254.