Depending on the society that people are surrounded around, the way that they view technology will differ. In every society though, they all utilize technology all in different complex ways since everyday life is heavily digitized now. “Society is increasingly reliant upon complex and interconnected cyber systems to conduct daily life activities. From personal finance to managing defense capabilities to controlling a vast web of aircraft traffic, digitized information systems and software packages have become integrated at virtually all levels of individual and collective activity” (Linkov 2019). In addition to their views and usage on technology being different from society to society, the way they handle cyber-attacks may be different as well as the repercussion that may happen if they chose to handle it themselves. Cyber attacks can range from different types of attacks, and they can happen to anyone anywhere. Society may know about major ones that happen to major organizations or the government, but most of the citizen are unfamiliar about the everyday cyber attacks that could happen to people like themselves. If the society that people are in does not raise awareness about how to implement cyber tactics to defend against attackers, then that society would be more susceptible to incoming attacks since attackers’ prey on the weak so to say. “These computer intrusions share a common tactic-the use of unknowing intermediaries' computers to hide the true origins of attacks. Sophisticated and unsophisticated attackers alike choose to leverage existing infections in order to hide their own identities” (Huang 2014). In a sense, the citizens who keep their technology systems up to date are the ones who are least likely to get any attacks, but citizens who understand the ways that people can cyber attack would also know how to defend themselves in a more aggressive way. If a person only relied on their anti-virus and anti-intrusion systems and suddenly, they got cyber attacked, by the time they notified someone it happened, the damage will already be too great. But with digital self-defense policies, if a person who had

adequate knowledge on information systems and tactics gets cyber attacked, they have a chance to defend and protect their privileged information. As years go on and technology gets bigger and more advanced, cyberculture grows within the societies as well, normally with the newer and rising generation." we are all at an infantile stage of the development of the web. The outcome of the impact this development will have on us in the future, in the long run, hinges on the importance for our children of their development with the web" (Pereira 2018) They start to learn about all of the wonders that you can do with technology, and they decide that they want to try to learn or master different skills within it. Just like with most hackers, they don't do it for very much gain other than to see if they can really do it without being noticed or caught. There are even jobs out there for people to be bounty hunters in relation to cybersecurity defense. The way that we demonstrate the wide range of cyber utilities, as well as showing the risks of what can happen in an event of an unwanted cyberattack, shows that the policy of using digital self defense is acceptable within a scope. There are no clear guidelines as to how people can utilize it, but depending on the society surround a person and their prior knowledge would show them how to approach various situations in relation to cyber-attacks. A major risk with the allowance of digital self defense is always the chance that people could use it to cause chaos within the society as well. There is no way for an organization to make sure that everyone uses it only for self-defense. But having this policy in place in a way makes it "all or nothing". In addition to that, society would have to make sure that it does not lose itself due to the growing cyberculture and subcultures that would appear as time and technology moves on. What that means is that if innovation progresses and citizens are quickly keeping pace along with it in society but the higherups are not, it could also lead to chaos. The societies in the world and the technology need

to fit together symbiotically so that they can both progress without the worry or risk of corruption or fail.

Works cited.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.

Huang, S. (2014). Proposing a Self-Help Privilege for Victims of Cyber Attacks. *The George Washington Law Review, 82*(4), 1229-1266.

Pereira, L. (2018). Cyberculture, symbiosis, and syncretism. *AI & Society, 33*(3), 447-452.