Information Warfare Through Utilitarian Reasoning

Shedd and Stradner discuss the idea of an ongoing information war between the U.S. and other countries, such as Iran, China, and Russia. In their article, they discuss multiple startling revelations of this information war; primarily, the U.S. is losing. Russia has constructed information networks across multiple platforms such as YouTube that push Russia friendly, right-wing agendas. China used its own narratives to attack the banning of its platform Tiktok, using the argument of free speech to encourage Americans to protest this move. Iran encouraged Americans to sit out of the 2024 election, likely impacting the final results. Shedd and Stradner discuss all of this, but there remains the unsatisfying conclusion that the U.S. simply is not doing enough. They make the argument that the U.S. should be using similar information tactics to fight back against misinformation propagated by our enemies, just as it did during the cold war. Under this line of thinking, I will argue that there is an ongoing information war and discuss the U.S.' justifications for using similar tactics to our enemies to fight in it through a utilitarian perspective.

One of the concepts discussed by Prier is *Commanding the Trend*. This is made up of three categories: trend distribution, trend hijacking, and trend creation. All three of these methods are used in varying ways by American adversaries. Trend distribution is simply wherein a particular message is just attached to a current trend so that when users look at the trend, they also see the message. Trend hijacking is a bit more complex and involves bot networks changing the underlying trend without changing the name of it, leading to an inundation of their target message for users. Trend creation is the most difficult in which humans and bots work together to create a trend that is favorable to their message. The reason why all of these methods are done is so that their target message can spread. The more their target message is spread, particularly by people, the more likely it is that users will become favorable to their cause.

In this context, it is evident how foreign adversaries disrupt American democracy as discussed by Shedd and Stradner. The ultimate target message is that of distrust in democracy and in larger American institutions through the conduit of social media, which the vast majority of Americans trust implicitly for their daily news and entertainment. This degradation of trust has vast reaching consequences, such as a difference in election outcomes and thereby U.S. policy, a breakdown of the judicial system which cannot function without that trust, and a distrust of other Americans, leading to a breakdown of culture and cultural relations. In this, no outright violent act was committed, but it remains antithetical to the core of America's functions, making these acts of information warfare. On the issue of policy, it seems evident that our adversaries are winning this cyberbattle. Russia has demonstratably interfered with three American elections, two being arguably successful, with the election of Trump being favorable to Russian interests.

This leads to what should be done next. Shedd and Stradner argue that the American response has been weak and underwhelming. Under the utilitarian model, one must weigh their options on the basis of least harm committed and the greatest good for the greatest number. Cyberwar and information war are both moral wrongdoings of their own accord, both unduly influencing the populace towards actions they would otherwise not take and charting courses for entire nations that may not end positively. However, if American adversaries continue to be the only ones to engage in this type of war, then Americans and our institutions will continue to be terribly harmed. On the other hand, if the U.S. engages with information war, we would be undermining Russian and other countries' institutions and their populaces. This might constitute as doubling the amount of harm to some, however it must also be taken into consideration what institutions even are moral in the first place. To keep this short, as this is not the primary focus of this essay, it can be argued that Russia's authoritarian institutions are causing more harm than

good for their people, and therefore undermining them may be morally neutral or morally good. As such, under the utilitarian model, the U.S. using similar trend hijacking tactics to protect its own population and undermine Russia's institutions can be seen as causing the least amount of harm possible in this scenario, making it the most morally correct choice.

Morkevičius presents another angle for which information warfare must be considered. In their argument, they discuss the principles of *jus ad vim*. These principles describe the full scope of justifications and actions during war. They emphasize the idea that war should not be done for avengeance, but for public good. War must be a response to a grievous harm and must have proper cause. Also discussed is the principle of distinction, in which the proportionality of acts committed informs what tactics are available or should be taken. Lastly, there is the principle of proportionality, in which the harms must not outweigh the benefits of a given action, mirroring the principles of utilitarianism.

Under these principles, the ongoing information war can be evaluated. Given the evidence that entities like Russia have struck first in this war, it can be argued that they do not have the just cause for their actions. However, the U.S. as the defensive party does have just cause, and can retaliate accordingly. As the aggressor, there is no argument for Russia to be committing information war for its own public good. On the contrary, there is the argument that Russia is inviting harm to their public by opening up the opportunity for retaliation. Where the water becomes muddier however is the idea of the U.S. properly responding to this under the principle of grievous harm. Where does one draw the line in an information war that has hard to measure effects? Is election interference grievous harm? Or is that only reserved for hardline economic and physical damage? As such, the proportionality and distinction are hard to

calculate. How does one weigh the potential harms of information war when they remain this difficult to calculate for ourselves, let alone the impacts on our intended targets?

This leads to the utilitarian perspective where harms must be calculated and weighed against the greater good. This is one area where the utilitarian model can be considered to fail, as not all actions are clear cut. On the surface, it would seem that the harms are very minimal and that the U.S. should obviously join the information war for the greater good. However, we do not truly understand how our actions will play out across the next decade or even century. We do not know if we are opening a Pandora's box, wherein if we join the information war if it will escalate to conventional or even nuclear war in a butterfly effect. Obviously, this is an extreme example, but there is little room for error in the global arena.

The information war is a complex topic, but nonetheless is a very real and prevalent one. Seeing the shortcomings of the utilitarian model, I conclude that it needs to be evaluated under multiple moral frameworks so as to create a more comprehensive conclusion. While the utilitarian model does lean towards justifying the information war when viewed through a certain lens, due to the high risk nature of this topic I do not feel confident in agreeing with this justification. Alternatively, there is clearly the issue that what is currently being done is insufficient for addressing the ills of this war. As such, I remain tentatively neutral towards this topic and encourage further research into the history of war, the moral arguments of war, and the mechanisms of information war.