Israel and Iran have been engaged in a cyberwar for more than a decade. Israeli attacks include an attack on Iran's largest port, potentially attacks on Iranian computer systems, and potentially an attack on nationwide gas stations. Iran's attacks include things like an attack on an Israeli hospital. The Iranian attacks reduced the hospital's ability to operate and forced the workers to work manually. The supposed Israeli attacks caused thousands of trains to be canceled and thus made Iranians unable to get gas for some time. Israel has also frequently worked alongside, or in tandem with, the U.S. to wage the cyberwar. This is part of the reason why sometimes it is difficult to identify some of the perpetrators of the attacks. Often, though, like in the case of Stuxnet, Israel and/or the U.S. are likely the culprits. Israel has been defined as having "superiority" in the war. In this case analysis, I will argue that Ubuntu shows us that the cyberwar between Israel and Iran is not just because it violates the principles of what could be considered a just cyberwar.

Michael Boylan's, "Can there be a just cyberwar", is a powerful text that can be used to better understand cyberwarfare. One concept explained by Boylan, is the difference between cyberwar and cyberespionage. Boylan explains that, really, cyber espionage is simply a lesser form of cyberwar. Boylan leads this into an explanation of traditional war, briefly explaining ad bellum, in bello, the idea of "might makes right", and the belligerent kraterist agenda. These concepts allow Boylan to explain the traditional view of what a just war is. Traditionally, there are two judgments to make to decide whether a war is just or not. Judgment A is about the origin of the war. Judgment B is about how the actual actions are carried out. These judgments mirror the concepts of ad bellum and in bello as well. Boylan uses this understanding of traditional war to introduce how cyberwar concepts challenge the traditional perceptions and judgments made relating to war. One such difference is that while in traditional warfare, the act of killing is a common and integral part, it's not quite the same in cyberwar. Death and killing do still occur and could even occur in large numbers, but they're more indirect and occur in mostly reduced numbers. This suggests that simply measuring a cyberwar's ethics by the direct losses of agents and civilians is not particularly effective. Another important concept to imagine is that the attribution of attacks and operations is completely changed by the nature of cyberwar. Already discussed were the attacks on Iran, for instance, that technically were not claimed and were not 100% attributable to a specific entity. Despite this, many different cyberattacks were eventually identified. For instance, the Stuxnet attack was seemingly carried out by Israel and the United States. Neither entity has admitted to it, and they have not been accused or charged formally by any supranational entity. Despite this, analysts and experts are relatively certain they are the perpetrators. In other cases, the attacker is clear, but in others, we can only rely on speculation and inference. To add on to this, territoriality in cyberspace has completely changed. The ideas of territory, operational range, neutrality, neutral ground, and similar concepts are all fundamentally different in cyberwar. As an example, the Stuxnet attack was aimed at one nuclear facility in Iran. Despite the intended target, the changes in territoriality and interconnection caused numerous systems worldwide to be directly affected. In cyberspace, all systems are connected in some way, and there is no clear border or designation between one "territory" and another. This, combined with the various anonymizing abilities of cyberspace, makes neutrality seem like an impossibility. Boylan explains that he is not attempting to reject the traditional theories of warfare and just war. Instead, Boylan recommends an expansion and updating of the current theories to better reflect the reality of cyberwarfare. Boylan's primary recommendations are based on finding international consensus. These include a fifth Geneva Convention, international standards for compensation related to cyberwar, and a change in the rules of liability as they relate to cyberwar. Boylan's analysis has significant relevance for an ethical analysis using Ubuntu. Just as warfare in the modern age has changed, so too has our communities and relationships with them. One parallel is how cyberwar has expanded and warped our preconceptions of territoriality. The interconnected information age of today has also expanded and changed how our communities function as well. Just as the boundaries between one nation and another muddle in cyberspace, so too, do the boundaries between and inside of communities become blurrier, and harder to map out. Relationships now are more global than ever, and changes and movements in them can impact other relationships across the globe. With Ubuntu in mind, it suggests that as our relationship networks both broaden and deepen, we should be more mindful about the impacts our actions have towards harming and changing them on a global scale. Applying these principles does not bode very well for an ethical analysis of Israel's actions. Israel's actions seem to have a wider impact, affecting more members of the communities they are both a part of and adjacent to. This broader approach is seemingly less empathetic, as it casts more and more groups affected by the results as targets, or hostile actors, whose existences and communities are secondary to the efforts of a cyberwar. One could imagine a more empathetic approach would be to not wage war at all, instead realizing the shared humanity, and the web of communities between them, and instead attempting a more diplomatic approach. At the very least, crimes could be owned up to, discussed among those affected in the community and a solution could be discussed. Instead, in some cases, the crime is not even admitted to, and those affected are told, although indirectly, that they will have no say in the actions that affect their livelihood and community so long as the conflict rages.

Mariarosaria Taddeo's "An Analysis for a Just Cyber Warfare," offers more recommendations for what a just cyberwar is and the characteristics of cyberwar today. One reason this is so important is because, as Taddeo says, traditional Just War Theory (JWT) is "necessary but not sufficient" for the analysis of cyberwar. One such issue with using JWT is that it does not fall in line with JWT's doctrine of "war as a last resort". The example given here is: what if a cyberattack is able to delay or outright stop a conflict from turning into a traditional war before it's even able to begin? According to JWT, this would likely be a preemptive strike and thus violate JWT's doctrine of "war as a last resort". Another issue with JWT and cyberwar is the principle of "more good than harm". Traditionally, this principle is used to help determine what could be considered a just war. An entity would need to prove there is more universal good in the war than universal harm. Taddeo points out that, due to the nature of cyberwar, these principles become extremely hard to quantify and/or apply when considered in cyberwar. The last issue Taddeo cites is that cyberwar fundamentally changes the distinction between combatants and non-combatants. In traditional war, the line between combatant and non-combatant is relatively distinct. Taddeo attributes this to the strict distinction between civil and military societies. In cyberwar, those lines are incredibly blurred. Individuals cannot be identified by their uniforms. Anonymity reigns supreme, and adversaries can much more easily hide within civilian society. Taddeo uses these concepts and others to posit three principles for a just cyberwar. The first tenet is that an entity that endangers the infosphere as a whole could be reasonably conceived of as a target. One justification for this is the aforementioned fact that attacks against such an entity could lower the risk of a traditional war. The two other tenets provide regulations for said cyberwars. These are that cyberwars should be waged in order to preserve the infosphere, but also that they should not be waged simply to promote the wellbeing of the infosphere. The second principle ensures a more accurate "war as a last resort" measure for cyberwar. The third principle, however, ensures that proactive wars to simply promote wellbeing should be forbidden. Taddeo clarifies that cyberwars should still aim to do more good than harm and ensure principles of proportionality are adhered to. These principles work well in tandem with Ubuntu. Just as it's just to wage war to protect the infosphere for Taddeo, so too would it be just to wage war to protect the community we share and restore a greater peace. The need for such a war becomes even greater if it is waged out of empathy for others as opposed to hate. It's no secret that, in Iran's case, a large part of why the Iranian-Israeli relationship is so strained is because of Israel's attacks on Palestine and the Palestinian people. From Iran's point of view, the need for a just war could stem from empathy towards what it sees as members of its community, and to protect them, it must unfortunately attack. Importantly, though, I think when we apply both Ubuntu and Taddeo's recommendations for a just cyberwar, we see no room for Israel's actions within the recommendations. Iran has attacked through cyber means, but it is noted that Israel is more advanced, more deadly, and will often attack alongside its ally, the U.S., the most "well-armed" attacker within cyberspace. Iran, the much more diplomatically isolated and technologically inferior nation, attacks seemingly for the sake of protecting the Palestinian community (or at the very least out of retaliation for Israel's treatment of the Palestinian people). Ubuntu would recommend that Israel remember the shared humanity and community between them and come to some sort of diplomatic and empathetic solution. To see a technologically inferior foe, lash out in any way they can, should be seen as a tragic sight. Proportionality seems to be ignored, however. While it seems Israel has waged cyberattacks that are not designed to directly kill (delayed trains, gas station hacking, nuclear facility sabotage), it's also notable that in tandem with these attacks, they have also assassinated numerous Iranian officials as well. Meanwhile, Iran can only wage small scale attacks, like a hack of one hospital. If we use Taddeo's tenets, I would posit that Israel violates the third tenet. To me, Iran seems to pose no real threat to the infosphere of Israel, and the war waged against them is merely a war to promote the wellbeing of the infosphere, not protect it. Ubuntu concurs with the unjust nature of the war. Israel is not acting with empathy, understanding, or a sense of shared community.

In conclusion, the cyberwar between Israel and Iran is not a just war. Cyberwar itself is fundamentally different from traditional war, as it changes many of the aspects of war in fundamental ways. Territoriality, neutrality, and the landscape of war are altered by cyberspace. While the nature of casualties changes, real harm is still good, and proportionality and the principle of more good than harm should still be adhered to, even if they are changed by the nature of cyberspace. These changes have led to the need for altered rules of war and a new definition of what a just war means. The authors aforementioned have expanded upon those definitions and provided a way for the rules of war to be properly updated to meet the realities of cyberspace. The Israel-Iran cyberwar does not seem to meet the criteria of a just war according to those definitions. The principles of Ubuntu further provide context, as it seems Israel has undoubtedly not acted in an ethical way according to them. This example of cyberwar has huge ramifications for nations around the globe. As cyberwar becomes more common, it becomes more important to adhere to the principles of just war. Likewise, the need to act ethically according to the principles of Ubuntu, through empathy and a recognition of our shared humanity, remains a central responsibility for the world.