

Caleb Judy

Professor Nicol

11/19/23

Case Analysis on Cyberconflict

The articles “Iran says sweeping cyberattack took down gas stations across country” by Chantal Da Silva, Kevin Collier and Reuters; and “The Cyberwar Between Israel and Iran is Heating Up” by Dr Abnan Abu Amer dive into the rising conflict between Israel and Iran, more specifically the cyber conflict between the two nations. Silva et al specifically dives into an instance where Iran was hit with a cyberattack that affected gas stations in the country. It affected motorists using government issued credit cards, and when used at the pumps, a cryptic message would be played that resulted in long queues. Amer discusses more broader instances of cyberattacks targeting Israel, specifically those that target things like critical infrastructure, civilian sites, and essential services. He highlights more specific instances, like those that target hospitals or railway systems. In both articles it seems that governments and the economies of those governments are the targets of these cyberattacks, but unfortunately the citizens of these countries are also affected by them. In this Case Analysis, I will argue that virtue ethics shows us that the cyberwar between Israel and Iran is not just because even though it does not harm civilians, it still impacts their lives in a negative way.

First, I want to explore an article written by Michael Boylan, “Can There Be a Just Cyber War?” Boylan discusses the necessity of updating international law, as well as conflict resolution mechanisms to address the challenges presented by cyber warfare. He argues that traditional war theories were designed around conventional warfare between states, and that they focus solely on physical aggression and territorial disputes, which is why international law needs to be updated. Cyber warfare has blurred the lines between traditional military actions and covert cyberattacks, which is why change to international law is needed. He suggests integrating new rules and protocols into international law that will define cyber warfare, determine responsibility

for cyberattacks, and establish compensation mechanisms for affected parties. This adaptation of international law would aim to fill in the gaps in traditional legal frameworks, enabling effective identification, attribution, and response to cyber aggression while also ensuring accountability and reparation.

Boylan also emphasizes the need for conflict resolution mechanisms to evolve in this new age of warfare. He highlights the limitations of traditional responses, like conventional military retaliation, in dealing with cyberattacks. Instead, he proposes that we move away from the traditional mindset of fault-based liability in just war theory to one of strict liability, emphasizing civil law, as well as compensation for damages caused by cyber aggression. Boylan recommends establishing internationally recognized categories for compensating loss of property and life, which is similar to standards that are set by international insurance policies. This evolution of conflict mechanisms ultimately aims to integrate cyberwarfare into a revised canon of just war theory, emphasizing the legal resolutions and reducing the reliance on conventional military responses for cyber conflicts.

In addition, the moral philosophy of virtue ethics can be used to assess the situation between Iran and Israel. Virtue ethics is defined as a moral and ethical theory that focuses on the character and virtues of an individual as the primary factors in determining what is right or wrong. It places emphasis on the virtuous traits of a person, like courage, kindness, honesty, etc. Virtue ethics highlights the importance of responsibility and accountability. In the context of cyber conflicts, individuals and organizations who are responsible for developing or deploying cyber weapons should exhibit virtues like accountability or honesty. They should consider the potential consequences of their actions on civilians or infrastructures. In Silva's article, Iran's gas stations suffered a cyberattack, as mentioned. But there was never a group that claimed to have done it, nor was anyone held responsible for it. This anonymous group targeted Iranian gas stations, which resulted in people waiting in long lines for gas, and some people may not have been able to get gas at all. While this isn't physically harmful to people, it can still harm

their livelihood. For example, if someone can't get gas into their vehicle, how will they get to work? An event such as this could cause someone to lose their job. So even though no one was physically harmed, this anonymous group affected the lives of millions, without claiming responsibility for their actions, which was morally wrong.

Boylan's article is also similar to virtue ethics and can be used to assess the situation between Iran and Israel. When adapting international law to address cyber warfare, virtue ethics can be used by lawmakers and policymakers to prioritize fairness when attributing responsibility for cyberattacks. Additionally, Virtue ethics can encourage the development of conflict resolution mechanisms that prioritize ethical considerations, seeking solutions that promote fairness, minimize harm to non-combatants, and encourage the virtuous conduct of the parties involved. I think that both ideas presented by Boylan, as well as the concept of virtue ethics could be employed to create a more regulated, and balanced cyber war, but I still believe that the current cyber war between Israel and Iran is not just because of the effect it is having on civilians, as mentioned.

Another article I want to explore is "An Analysis for a Just Cyber War" written by Mariarosia Taddeo. It is an ethical analysis on cyber warfare that focuses on two main ethical frameworks: Just War Theory (JWT) and information ethics. To start, Just War Theory is an ethical framework that provides guidelines for evaluating the morality of engaging in warfare. It is rooted in both moral and philosophical principles that assess whether going to war and conducting warfare is justified. JWT includes the two main branches of *jus ad bellum*, or the right to go to war, and *jus in bello*, or the right conduct within war. *Jus ad bellum* focuses on the right to engage in war, considering principles such as just cause (valid reasons for war) or legitimate authority (war declared by proper authority). *Jus ad bello* focuses on ethical conduct during war, emphasizing principles like proportionality (prevents excessive force or attack) and discrimination (distinguishing between combatants and non-combatants). Taddeo explains that In the context of cyber warfare, JWT faces challenges when applying its traditional principles

because of the unique nature of cyber warfare, which includes non-physical elements, various levels of violence, and blurs the lines between combatants and non-combatants.

Another key concept from Taddeo is information ethics. According to Taddeo, Information ethics is a “macro-ethical framework” that essentially addresses ethical issues that arise from the use, creation, and dissemination of information. It considers information as a vital aspect of moral decision making and includes multiple approaches, the main ones being ontocentric, patient-oriented, and ecological. The ontocentric approach treats all entities (which includes digital entities) as having fundamental rights, advocating for the existence of all entities and flourishing within the “Infosphere”, defined by Taddeo as “The totality of what exists”. A Patient Oriented perspective assesses the morality of actions based on their effects on interacting “patients” (entities), focusing on the overall impact of the well-being of the infosphere. The ecological perspective views the well-being of the infosphere as the ultimate good, identifying entropy, defined as “negative impact” or “disruption”, as a moral evil that should be minimized and removed. Taddeo explains that information ethics becomes relevant to cyber warfare by emphasizing the need to consider non-physical damages caused in the infosphere and providing criteria for ethical considerations of cyber warfare’s implications, integrating with JWT to develop ethical guidelines specific to cyberwarfare.

Similar to JWT and information ethics, virtue ethics takes human rights and just conduct into consideration, which can help explain why a cyber war between Iran and Israel is not just. Virtue ethics could help encourage cyber warfare practitioners to consider virtues such as justice, fairness, and respect for human rights. Ethical actors in this field should aim to adhere to internationally accepted laws of armed conflict and ethical norms, ensuring that cyber operations are conducted ethically and proportionately. Let’s consider Amer’s article, where he discusses the situation with the hospital. After Israel targeted computer facilities at an Iranian port, Iran responded to this by targeting the Hillel Yaffe Hospital in Hadera, Israel. The hospital staff had to work manually, putting patients’ lives at risk. While Iran was in the right to launch a

counterattack, it was morally wrong because it was disproportionate and it jeopardized the lives of innocent civilians. If a framework such as JWT, information ethics, or virtue ethics, were to be employed in a cyber war, it could prevent tragedies such as this from happening.

After reading over the articles presented by Boylan and Taddeo, I believe that a just cyber war could be possible. However, when considering the current situation involving Iran and Israel, I believe that the cyber war between the two is not just, for several reasons. Boylan shows us through adoption of international law and the emphasis of conflict resolution mechanisms to evolve how a cyber war can be justified. We can use this as a framework to assess why the gas station attack, discussed by Silva, was morally wrong, as mentioned previously. Additionally, concepts discussed by Taddeo, specifically Just War Theory and information ethics, also show us how a cyber war can be justified. We can use these concepts to assess the several cyberattacks, discussed by Amer, to explain why the Iran-Israel cyber war is not justified, as mentioned previously. Virtue ethics supports the articles written by Boylan and Taddeo, supporting specifically the importance of adapting international law, conflict resolution mechanisms, Just War Theory, and information ethics. These provide a framework that could result in a just cyber war between Israel and Iran, if employed.