Adversaries continue to seek non-traditional methods to weaken and undermine a nation's security. While traditional warfare involves using physical force to destroy assets, hybrid warfare combines kinetic and non-kinetic tactics to achieve strategic objectives. Non-kinetic tactics include cyber warfare, particularly attacks on critical infrastructure. Critical infrastructure refers to systems essential to a nation's functionality, such as power grids, water treatment facilities, communication networks, and transportation systems. These are among the most vulnerable targets. The shift toward hybrid warfare represents an evolving threat to national security with immediate and long-term implications. By incapacitating essential services and limiting a nation's ability to respond to emergencies, adversaries aim to create chaos and erode public trust without resorting to direct military engagement. The communications sector is especially critical, as it supports the operation of all other infrastructure sectors. A breakdown in alerting and communication systems during a conflict can significantly hinder the responsiveness of both civilian and military personnel, exacerbating panic and confusion. Delays in restoring control over these systems can jeopardize national security, economic stability, public health, and safety. Furthermore, a secure communication channel breach risks leaking sensitive operational information to adversaries. To mitigate these threats, nations must prioritize the protection of critical infrastructure through robust cybersecurity frameworks, comprehensive vulnerability assessments, simulated attack exercises, and strategic investments in upgrades and system redundancies. While sectors like banking, public services, and general supply chains may not always be classified as "critical," their disruption can demoralize civilian populations and destabilize essential systems. Addressing existing threats is vital, but so is anticipating emerging risks, highlighting the need for strong preventative measures. In this case analysis, I will argue that utilitarianism shows us that these actions could be part of a just war because of the minimization of kinetic damage.

Michael Boylan uses *"Can There Be a Just Cyber War?"* to explore whether cyber warfare can adhere to the principles of just war theory. He emphasizes two key requirements for a just war: jus ad bellum (justice in going to war) and jus in bello (justice in conduct during war). The assumption that cyber warfare is inherently less violent and thus more ethical is challenged. Instead, he highlights the ambiguity of harm in cyber operations. He does this by emphasizing that while physical destruction is limited, the psychological, infrastructural, and long-term consequences may still violate just war principles if they lack accountability and transparency in addition to disproportionately harming the civilian population. There are two important principles to consider: the Principle of Proportionality, which states that the harm must be proportional to the good achieved, and the Principle of Discrimination, which states that combatants must be distinguished from non-combatants. Additionally, he discusses the epistemic uncertainty involved in cyber warfare. Unlike traditional attacks, cyberattacks frequently obscure the attacker's identity, making it challenging to assign moral responsibility or confirm adherence to war principles. This lack of clarity can enable plausible deniability, eroding trust in international norms and undermining accountability. The just war framework assumes a certain level of transparency, which cyber operations lack by design. Boylan's work challenges us to consider whether a war that cannot be clearly attributed or whose effects cannot be accurately measured can ever truly meet the moral clarity demanded by jus in bello or jus ad bellum.

Cyber warfare is increasingly being integrated into hybrid conflict strategies from surveillance systems to psychological operations, as discussed in the article *"Digital Battlegrounds: Evolving Hybrid-Kinetic Warfare"* by Paul Veeneman. When assessed through

Boylan's framework, these actions raise key ethical concerns. If cyber attacks are too broad, in scope they risk violating the Principle of Discrimination by failing to distinguish military and civilian targets. Similarly, if the intended strategic advantage gained is minimal compared to the civilian disruption caused, the Principle of Proportionality may not be met. Boylan would argue that even in the absence of physical violence, the potential for wide-reaching, less visible harm makes cyber warfare ethically complex and demands heightened scrutiny. Therefore, in analyzing the case from his perspective, these operations can only be considered if their intent, methods, and outcomes are narrowly tailored and justified.

Utilitarianism focuses on maximizing the overall good and minimizing harm. Suppose cyber warfare reduces the need for kinetic violence and saves lives on both sides by targeting enemy infrastructure or disrupting hostile plans with minimal civilian impact. In that case, it aligns with utilitarian ideals. Hybrid cyber-kinetic tactics undermine and disrupt an opponent's coordination, morale, communications, and military logistics, while limiting large-scale destruction. From a utilitarian perspective, if these actions significantly reduce battlefield casualties or possibly prevent escalation, they can be ethically permissible. However, utilitarianism also demands scrutiny: if cyber actions indirectly lead to long-term civilian harm, the net utility diminishes, making the actions unjust. The primary goal of utilitarians should be to minimize suffering and preserve life. Using Boylan's just war principles and a utilitarian ethical lens allows us to conclude that cyber warfare can be a just part of the war when meeting standards of discrimination and proportionality, resulting in a net harm reduction.

"An Analysis for a Just Cyber Warfare" by Mariarosaria Taddeo explores ideas similar to Boylan's and discusses three key principles: necessity, proportionality, and discrimination. Taddeo argues that cyber warfare must still be assessed by how well it respects these moral

boundaries and principles. She emphasizes that the unique attributes of cyberware do not automatically make it more ethical. Alternatively, she warns of a “moral buffer” where the absence of kinetic force may cause decision-makers to overlook or underestimate the ethical implications. For a cyber operation to be just, it must be targeted, necessary to achieve a legitimate military objective, and not produce excessive harm compared to its achievements. These criteria directly imitate traditional just war concepts while accounting for cyber operations’ unique attributes. There is concern regarding the asymmetry of access to cyber tools and capabilities. In many cases, powerful state actors possess disproportionate cyber resources, which could create exploitative scenarios that undermine fair engagement. This imbalance can introduce the potential for a nation to exacerbate inequality and destabilize weaker nations. Furthermore, she highlights the difficulty of post-attack assessment and accountability when evaluating non-visible damage.

Applying Taddeo’s framework to cyber operations described in Veeneman’s article, we see a range of tactics aimed at disrupting adversary communications, surveillance, and infrastructure. These operations, while non-kinetic, are not automatically just and must meet the requirements of Taddeo’s three principles. If attacks on infrastructure or a nation’s capabilities spill over into civilian sectors, they risk violating proportionality or discrimination by inflicting harm on non-combatants. She would stress the importance of intentionality and precision in such operations. The moral legitimacy of cyber tools depends not just on what is targeted, but how clearly the targets are defined to avoid collateral harm.

When evaluated with utilitarian principles, these cyber operations are ethically permissible when they significantly reduce the expected harm compared to kinetic warfare. If targeting military systems prevents the need for large-scale, high-casualty engagements, then the net outcome may favor using cyber tools. Utilitarianism evaluates actions based on the balance of outcomes: reducing overall suffering and preserving life. However, utilitarian ethics also demand a full accounting of long-term consequences. The net benefit becomes questionable if the destabilization caused by cyber tactics leads to broader insecurity or future retaliation. The ethical imperative under utilitarianism is not just to reduce immediate casualties, but to promote lasting stability and minimize suffering across all affected populations. A utilitarian concern with cyber warfare is the dangerous precedent it sets by normalizing conflict through low-cost, low-risk means. This can lower the threshold for engaging in war, increasing the risk of overuse and global instability. Even if cyber operations reduce immediate harm, their ethical permissibility depends on long-term impacts, including restoration and future conflict behavior. Combining Taddeo's criteria with a utilitarian lens leads to the conclusion that cyber warfare can be part of a just war, but only when it is tightly constrained in scope, avoids harm to civilians, and demonstrably leads to a net reduction in suffering over both the short and long term.

In conclusion, this analysis has shown that cyber warfare can, under certain conditions, be ethically justified within the framework of just war theory and utilitarianism by applying the principles outlined by both Boylan and Taddeo: necessity, proportionality, and discrimination. It becomes clear that non-kinetic cyber operations must be held to the same moral standards as traditional warfare. Utilitarianism further supports cyber tactics when they demonstrably reduce suffering, prevent escalation, and minimize civilian harm compared to kinetic alternatives. One primary concern is the difficulty of accurately assessing long-term consequences. The lack of transparency and adversary identification complicates moral accountability, potentially allowing unethical actions to go unpunished. Additionally, the normalization of low-cost cyber conflict could erode the threshold for engaging in war, leading to more frequent and less justified uses of force. Minimizing kinetic damage alone is not sufficient for moral justification. These objections underscore the need for ongoing scrutiny, restraint, and international regulation of cyber capabilities. Each action must be carefully evaluated for its intent, impact, and potential to contribute to a more stable and secure global order. For cyber warfare to truly align with utilitarian ethics, its outcomes must be shown to reduce suffering sustainably, not shift the burden from one form to another.