David R. Shedd and Ivana Stradner examine how Russia, China, and Iran conduct sophisticated disinformation campaigns. These operations are designed to destabilize the United States by exploiting its open information environment using state-affiliated media, proxy organizations, and social media manipulation. Much of the groundwork is built into the system by relying heavily on digital platforms leveraging algorithms to amplify divisive content. Adversaries exploit America's open society and free speech protections as vulnerabilities. For example, Russian operatives have used media outlets and shell companies to launder Kremlin-approved narratives into mainstream American discourse. These outlets often disguise their affiliations through neutral branding and plausible deniability. The article also points to the evolution of these campaigns from simple bots and troll farms to AI-generated content and deep fakes, increasing both believability and scalability. Efforts are often timed to coincide with key political events, such as elections, judicial rulings, or civil unrest, to maximize their disruptive impact. Furthermore, the article calls attention to how these campaigns are often successful not because of foreign ingenuity but due to American complacency. Additionally, the authors stress how these operations are coordinated across domains, making them a part of a holistic foreign policy strategy to weaken U.S. global influence and internal cohesion. The U.S. has failed to develop a credible deterrence policy for countering peacetime information warfare. The authors call for a national strategy integrating intelligence, law enforcement, tech companies, and civil society to build cognitive resilience against these non-kinetic forms of aggression. In this case analysis, I will argue that Kantian Deontology shows us that these nations did engage in information warfare against the U.S. by influencing national rhetoric and seeking manipulation and control through media operations.

Jarred Prier introduces the concept of ‘command the trend’ as a central mechanism of modern information warfare. He argues that controlling narratives on social platforms in present conflicts is as strategically important as controlling physical territory. Hostile actors seek to generate, amplify, and manipulate online trends to shape public opinion. Rather than persuading the public toward a specific viewpoint, the goal is often to sow confusion, distrust, and polarization, undermining faith in democratic institutions. Prier highlights that this tactic leverages the design of media platforms, which reward emotional, divisive content through algorithms that amplify engagement. He also explains that adversaries create and spread disinformation to trigger viral reactions, making the population itself a force multiplier. In this sense, information warfare is low-cost, highly scalable, deniable, and extremely difficult to counter within an open society that values free expression. Commanding the trend blurs the line between foreign aggression and domestic unrest, making it a valuable tool in the arsenal of malicious actors.

Applying Prier’s concept to the case of election interference by Russia, China, and Iran shows that these actions constitute information warfare. According to Sheed and Stradner, these states exploited digital platforms to infiltrate and manipulate American discourse, laundering state-sponsored narratives through seemingly neutral media outlets and proxies. Russia, in particular, demonstrated adeptness in commanding the trend by promoting extremist political views on both sides of the spectrum to deepen existing societal divisions. In these situations, Americans are the proverbial gun and ammo for this type of attack. All the attackers need to do is find a medium. These actors transformed America’s information environment into a battlefield by promoting extreme political narratives on both sides. Their use of bots, shell organizations, and AI-generated content mirrors Prier’s techniques. China and Iran similarly targeted U.S.

audiences by amplifying discontent around societal issues and the timing of significant events to maximize disruption. The coordination across media, cyber, and diplomatic domains reflects the broader strategic objective of eroding national unity and global credibility. These operations were not isolated incidents but parts of a sustained campaign, consistent with Prier's framework of exploiting trends to undermine societal cohesion without resorting to traditional military force. A sustained campaign aimed at destabilizing societal trust and a nation's internal political legitimacy without physical force fits the definition of information warfare by treating the environment as a battlefield.

Under Kantian Deontology, the disinformation campaigns launched by Russia, China, and Iran are ethically unjustifiable. Kant's categorical imperative demands that entities operate according to principles that respect the inherent dignity and rationality of all people. Deception, manipulation, and exploitation of public discourse treat individuals not as autonomous agents but as tools for achieving political ends. Foreign election interference via disinformation fails the universality test: if each nation attempted to manipulate another's population, trust and democratic self-determination would collapse globally. The act itself is morally wrong according to deontological ethics. Similarly, if the United States conducted comparable interference in Russia, China, or Iran, it would equally be unethical and constitute information warfare. Deontology holds that right actions adhere to duty and respect for autonomy, not by outcomes; therefore, all instances of election interference are morally impermissible, regardless of the actor's intentions or the political context.

Varlie Morkevicius explores how traditional just war theories, such as jus ad Bellum and jus in Bello, also apply to information warfare. She argues that information operations are not exempt from ethical scrutiny because they are non-kinetic. These operations must still meet just

cause, proportionality, and discrimination standards. Morkevicius highlights that manipulating civilian populations with falsehoods undermines individuals' autonomy and rational decision-making. Notably, she stresses that the fact that information warfare often operates in a "grey zone" with open declarations of war does not remove ethical obligations. Information campaigns that target civilian trust undermine legitimate political processes or cause psychological and societal harm, which can be as morally damaging as physical violence. Morevicius states that ethical evaluation must adapt to information conflicts while upholding core principles prioritizing human dignity and political sovereignty. She raises the concern of long-term cumulative harm: even with no immediate, visible damage occurring, repeated offenses can degrade political and social fabrics of a nation.

By applying Morkevicius' extension of just war thinking to the interference by Russia, China, and Iran in U.S. elections, it is made clear that these actions violate just war principles and constitute information warfare. Their operations deliberately targeted the American Civilian population with disinformation to distort the public's ability to make informed democratic decisions. This violates the principle of discrimination by targeting civilians' cognitive integrity rather than their physical safety. Furthermore, these campaigns lacked a just cause; undermining another nation's political process for strategic gain does not satisfy the threshold of a legitimate cause to engage in hostile actions. The proportionality of harm caused, creating civil unrest and distrust in democratic institutions, far outweighs any plausible political grievances these states might claim. Finally, by operating covertly and denying responsibility, these nations violated the spirit of right authority and transparency that just war thinking emphasizes. The covert nature additionally breaches the requirement of right authority, which demands that the use of force or

influence be subject to legitimate public political oversight. Therefore, under Morkevicius' adapted framework, the actions constitute unethical information warfare.

Applying a Kantian deontological perspective, the election interference conducted by adversary nations is categorically impermissible. Information warfare that manipulates the public's perception treats people as mere pawns rather than rational agents capable of self-government. Kantian ethics requires that actions respect the rational agency of individuals; manipulating public opinion through lies and distortions treats civilians not as ends in themselves but as mere means to achieve foreign policy goals. This instrumentalization of individuals' cognitive capacities for strategic advantage directly violates one's clear and rational thinking. Furthermore, if such behavior were universalized, the fabric of international cooperation, mutual respect, and self-governance would unravel, failing Kant's universality test. Just as Morkevicius highlights that information warfare erodes the foundations of legitimate political authority, this violates Kantian ethics that require truthfulness and respect for persons. Likewise, if the United States engaged in similar acts, it would also be committing an unethical act, regardless of motives or outcomes. Consistent with Kantian deontology, the correct course of action would have been for all nations to refrain entirely from disinformation campaigns and respect foreign civilian populations' sovereignty and rational capacities. Even seemingly "low-intensity" information operations can produce morally unacceptable outcomes because they threaten the long-term viability of democratic communities and processes.

In this case analysis, it is evident that the election interference conducted by Russia, China, and Iran constitutes unethical information warfare. Using the insights of David Shedd, Ivana Stradner, and Jarred Prier, we see that these adversaries exploited America's open information environment through coordinated disinformation campaigns. This was done to

manipulate public discourse and sow internal division. Their actions align with Prier's concept of "command the trend," weaponizing social media algorithms to amplify polarization and destabilize democratic cohesion. Applying Valerie Mrokevicius' adaptation of just war theory further confirms that these operations violate principles of just cause, proportionality, and discrimination, targeting civilians' cognitive autonomy in ways as morally damaging as physical violence. From a Kantian deontological perspective, these actions are categorically impermissible, as they treat individuals as means to an end rather than respecting their dignity as rational agents. The universalization of such behavior would erode international foundations of trust and self-governance. Anyone committing such acts, information warfare through election interference is inherently unethical. Ultimately, a synthesis of these analyses shows that the correct moral course is the complete rejection of disinformation campaigns, upholding principles of accountability and transparency, respect for sovereignty, and the intrinsic worth of individuals in both domestic and foreign affairs.