

Artificial Intelligence Warfare and Public Health: A Governance Framework for Evaluating Population Health Implications

Dr. David Bull

PhD., DBA, MBA, MSc, BCMHC, PMP
American InterContinental University System, School of Business

DOI: <https://doi.org/10.5281/zenodo.19592338>

Published Date: 15-April-2026

Abstract: The rapid integration of artificial intelligence (AI) into military operations has transformed the conduct of warfare, raising significant ethical, legal, and public health concerns. However, existing scholarship has largely examined AI warfare and public health in isolation, with limited attention to the governance mechanisms linking these domains. The purpose of this study was to examine how ethical governance and regulatory frameworks shape the public health implications of AI-enabled warfare and to develop a governance-centered conceptual framework connecting AI capabilities to population health outcomes. This study employed a qualitative policy analysis and structured narrative review of international legal instruments, policy documents, and peer-reviewed literature. Data were analyzed using thematic coding and comparative policy analysis, guided by the AI Warfare–Public Health Impact (AIW–PHI) framework. Findings indicate that current governance structures are fragmented, lack enforceable mechanisms, and remain insufficiently adapted to the complexities of AI-enabled warfare. Ethical governance mechanisms—such as human oversight, accountability, and transparency—are inconsistently implemented, while public health considerations are largely absent from existing regulatory frameworks. These gaps contribute to increased health system vulnerability and heightened risks to civilian populations. This study introduces the AIW–PHI framework as a novel, governance-centered model that conceptualizes AI-enabled warfare as a structural determinant of population health mediated by governance processes. The findings underscore the need to integrate public health into AI governance and to strengthen regulatory approaches to mitigate systemic harm. This study contributes to emerging scholarship at the intersection of AI, governance, and public health and provides a foundation for future empirical research and policy development.

Keywords: Artificial intelligence; AI-enabled warfare; ethical governance; international humanitarian law; public health; health system vulnerability; population health; autonomous weapons; military AI; governance frameworks; civilian protection; AI regulation.

I. INTRODUCTION

The rapid integration of artificial intelligence (AI) into modern warfare has fundamentally transformed the conduct of military operations, particularly in intelligence processing, target identification, and operational coordination. AI-enabled systems now analyze vast datasets derived from satellite imagery, surveillance feeds, and signals intelligence to enhance decision-making speed and precision (NATO, 2021). For instance, initiatives such as Project Maven illustrate how machine learning algorithms are embedded within military command-and-control systems to support real-time targeting and operational efficiency (U.S. Department of Defense, 2020). While these advancements improve tactical effectiveness, they simultaneously introduce complex ethical and governance challenges, particularly when algorithmic outputs influence life-and-death decisions (Boulain & Verbruggen, 2017; Scharre, 2018).

The expansion of AI in warfare has intensified concerns regarding compliance with international humanitarian law (IHL), particularly the principles of distinction, proportionality, and accountability. IHL, as codified in the Geneva Conventions, requires that parties to a conflict distinguish between combatants and civilians and minimize harm to noncombatants (International Committee of the Red Cross [ICRC], 2021). However, emerging research suggests that AI-assisted decision-support systems may face limitations in reliably interpreting complex, context-dependent environments, thereby increasing the risk of misidentification and unlawful targeting (Human Rights Watch, 2020). Furthermore, over-reliance on automated systems may erode meaningful human control, weakening moral accountability and potentially increasing civilian harm due to diminished human judgment in high-stakes contexts (Scharre, 2018; Sparrow, 2016). These concerns underscore the growing tension between technological capability and legal accountability in contemporary conflict environments.

Beyond legal and ethical considerations, the public health consequences of warfare, now increasingly mediated by advanced technologies, remain substantial and far-reaching. Armed conflict continues to produce both direct and indirect health effects, including mortality, injury, displacement, and the degradation of health systems (World Health Organization [WHO], 2022). Importantly, indirect effects, such as damage to infrastructure, disruption of sanitation systems, and interruption of healthcare delivery, often exceed direct battlefield injuries in both scale and duration (Ghobarah et al., 2003; Levy & Sidel, 2016). The integration of AI into warfare does not eliminate these outcomes; rather, it may reshape their distribution and intensity, particularly in highly interconnected and fragile health systems where disruptions can cascade across populations.

Despite the accelerating deployment of AI in military contexts, global governance frameworks remain fragmented and insufficiently developed. Emerging international initiatives, including the Framework Convention on Artificial Intelligence and the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, signal growing recognition of the need for AI governance. However, these frameworks often lack binding authority or fail to comprehensively address military applications (United Nations, 2023). Efforts to regulate autonomous weapons systems through multilateral negotiations have progressed slowly, hindered by geopolitical divergence and the absence of enforceable mechanisms (Boulainin, 2023). Consequently, significant regulatory gaps persist, creating uncertainty regarding how AI-enabled warfare should be governed to ensure the protection of civilian populations and public health systems.

The problem, therefore, is that although AI-enabled warfare technologies are rapidly advancing and increasingly deployed, there is a lack of coherent and effective governance frameworks to guide their use in ways that protect public health. Existing international legal structures were primarily designed for human-directed warfare and do not adequately account for algorithm-assisted decision-making, technological asymmetries, or the systemic health consequences of modern conflict (ICRC, 2021; WHO, 2022). This gap limits the capacity of policymakers, military institutions, and international organizations to evaluate, regulate, and mitigate the public health risks associated with AI-mediated warfare.

The purpose of this study is to examine how ethical governance and regulatory frameworks shape the public health implications of AI-enabled warfare and to develop a governance framework linking AI warfare capabilities to population health protection. To achieve this purpose, the study is guided by the following research questions: (RQ1) How are AI warfare technologies currently governed under international humanitarian law and related regulatory frameworks? (RQ2) What governance gaps exist in mitigating public health risks associated with AI-enabled warfare? and (RQ3) What governance mechanisms can be developed to better protect population health in AI-mediated conflict environments? The study achieved its purpose by (a) examining how ethical governance and regulatory frameworks shape the public health implications of AI-enabled warfare through qualitative policy analysis and literature synthesis, and (b) developing the AIW–PHI framework as a governance-centered, theory-building model linking AI warfare capabilities to population health outcomes. While the framework provides a robust conceptual foundation, future research is needed to empirically test and validate its proposed relationships.

II. CONCEPTUAL FRAMEWORK

This study is guided by the AI Warfare–Public Health Impact (AIW–PHI) framework, which conceptualizes AI-enabled warfare as a structural determinant of population health, mediated and moderated by ethical governance and regulatory mechanisms. The framework provides a parsimonious and governance-centered structure appropriate for examining policy environments and identifying regulatory gaps. The AIW–PHI framework is advanced as a novel, integrative mid-range theory that explains how AI-enabled warfare functions as a structural determinant of population health through governance-mediated pathways. See Figure 1.

AI Warfare—Public Health Impact Framework (AIW-PHI)

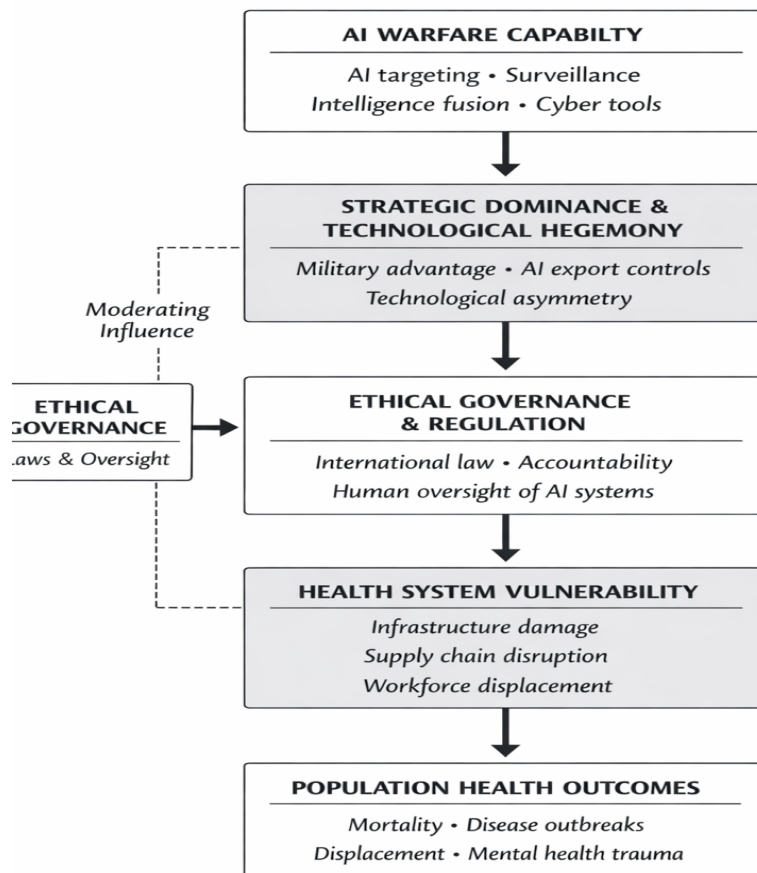


Figure 1

AIW–PHI provides a structured, multilevel model that explains how artificial intelligence–enabled military capabilities translate into downstream population health outcomes through a series of interconnected mechanisms. The framework applies to conflict environments in which AI-enabled or AI-assisted military systems are deployed and where civilian populations are exposed to infrastructure and system-level disruptions. This framework addresses a critical gap in existing literature, where AI warfare has been examined primarily from military or ethical perspectives, and public health impacts have been studied independently, with limited integration of governance mechanisms as a linking construct. The framework is conceptually aligned with systems thinking and public health impact pathways, positioning AI warfare not merely as a technological phenomenon but as a socio-technical system with cascading effects across governance, infrastructure, and human well-being.

AI Warfare Capability

At the foundational level, AI warfare capability represents the primary exogenous construct, encompassing AI targeting, surveillance, intelligence fusion, and cyber operations. These capabilities enhance military efficiency and decision-making speed, consistent with contemporary defense strategies (NATO, 2021). Within the framework, these capabilities do not directly affect health outcomes; instead, they operate through an intermediate structural mechanism, strategic dominance and technological hegemony. This construct captures how AI-enabled advantages create asymmetries in power, including disparities in technological access, export controls, and operational superiority. Such asymmetries shape the conditions under which conflict unfolds, influencing both the intensity and distribution of harm.

The framework introduces ethical governance and regulation as a central mediating construct, reflecting the role of international humanitarian law, accountability structures, and human oversight in shaping how AI systems are deployed in

warfare. This component aligns with principles articulated by the International Committee of the Red Cross (2021), emphasizing the necessity of maintaining meaningful human control and adherence to legal norms such as distinction and proportionality. Ethical governance functions primarily as a mediating mechanism through which AI warfare capabilities influence health system vulnerability, while also conditionally moderating the strength of these relationships depending on the robustness of oversight and regulatory enforcement. In addition, ethical governance provides a point of intervention, determining whether AI capabilities exacerbate or mitigate harm. In this sense, governance quality directly influences the translation of technological power into real-world consequences.

A key innovation of the AIW–PHI framework is the identification of health system vulnerability as the immediate precursor to population health outcomes. This construct captures the structural fragility of healthcare systems in conflict settings, including infrastructure destruction, supply chain disruption, and workforce displacement. Drawing on public health literature (World Health Organization, 2022), the framework recognizes that indirect effects of conflict, such as system breakdown, often produce more sustained health consequences than direct violence. Thus, AI-enabled warfare influences health not only through immediate casualties but through systemic degradation of healthcare capacity.

The final endogenous construct, population health outcomes, captures both the direct and indirect consequences of conflict, including mortality, communicable disease outbreaks, forced displacement, and long-term psychological trauma. Within the proposed framework, these outcomes are conceptualized as the downstream effects of a cascading causal pathway, whereby upstream technological advancements in warfare particularly artificial intelligence (AI) and governance structures shape epidemiological patterns through intermediate system disruptions. Emerging evidence indicates that contemporary warfare increasingly affects population health through indirect mechanisms, such as the degradation of healthcare infrastructure, disruption of supply chains, and breakdown of public health systems, rather than solely through direct battlefield injuries (World Health Organization, 2023; United Nations, 2024). This systems-based perspective reinforces the notion that health outcomes in conflict settings are structurally mediated, with cascading effects across interconnected sectors.

A distinguishing feature of the model is the incorporation of ethical governance as a moderating and mediating construct, represented through dynamic pathways within the framework. Ethical governance encompasses mechanisms such as regulatory oversight, transparency, accountability, and adherence to international humanitarian law, all of which shape how AI-enabled warfare influences health system vulnerability. Recent scholarship highlights that weak or fragmented governance structures exacerbate civilian harm and public health deterioration, whereas robust governance can mitigate these risks by constraining the misuse of emerging technologies (Kania et al., 2023; International Committee of the Red Cross, 2024). From an analytical standpoint, ethical governance functions both as a mediator, explaining how technological capabilities translate into health impacts, and as a moderator, influencing the strength and direction of these relationships. This dual role enhances the explanatory capacity of the framework and provides a strong foundation for empirical testing using multivariate techniques, including structural equation modeling, to examine complex, interdependent pathways within AI-mediated conflict environments.

While the model is presented as a linear pathway for conceptual clarity, it acknowledges that AI warfare capabilities may also exert direct effects on population health outcomes, particularly in high-intensity conflict scenarios. While the AIW–PHI framework provides a parsimonious and governance-centered model, refinements were made to clarify construct relationships, reduce role ambiguity, and improve theoretical precision. Specifically, ethical governance is conceptualized as the primary mediating mechanism, while direct pathways between AI warfare capability and population health outcomes are acknowledged to enhance realism.

Overall, the AIW–PHI framework offers a theoretically grounded and policy-relevant model for understanding the intersection of AI warfare and public health. It integrates technological, legal, and health system perspectives into a unified causal structure, thereby addressing a critical gap in existing literature. The framework is particularly valuable for guiding empirical inquiry aligned with the study's research questions, as it enables the systematic examination of governance gaps (RQ2) and the development of targeted governance mechanisms (RQ3) to mitigate public health risks in AI-mediated conflict environments.

The AIW–PHI framework is intentionally structured as a parsimonious, governance-centered model to provide conceptual clarity and policy relevance. While more complex systems-based models may capture recursive dynamics, the present framework prioritizes explanatory clarity to support governance analysis and framework development.

III. LITERATURE REVIEW

The AI Warfare–Public Health Impact (AIW–PHI) framework provides the theoretical foundation for this study by conceptualizing AI-enabled warfare as a structural determinant of population health mediated by ethical governance mechanisms. While the framework establishes the key constructs and their relationships, it is necessary to situate these elements within the broader body of existing scholarship to assess their empirical and theoretical grounding. Accordingly, the following literature review examines prior research across three interrelated domains: artificial intelligence in warfare, governance and regulatory frameworks under international humanitarian law, and the public health consequences of armed conflict.

Given the study’s focus on conceptual framework development and governance analysis, a structured narrative review informed by a systematic search strategy was employed rather than a formal PRISMA-based systematic review. A comprehensive search was conducted across major academic databases, including Scopus, Web of Science, PubMed, and Google Scholar. Keywords and Boolean combinations were used to capture relevant studies, including “artificial intelligence AND warfare,” “autonomous weapons AND international humanitarian law,” “AI governance AND military,” “conflict AND public health outcomes,” and “health system vulnerability AND war.” Additional searches incorporated terms such as “ethical oversight,” “civilian protection,” and “AI-enabled conflict.” The search was limited to peer-reviewed articles, policy reports, and institutional publications from organizations such as the United Nations, World Health Organization, International Committee of the Red Cross, and NATO. Emphasis was placed on recent literature (primarily 2015–present) to reflect the rapid evolution of AI technologies, while seminal works on war and public health were also included to provide foundational context.

The selection process followed a structured narrative review informed by a systematic search strategy. Titles and abstracts were initially reviewed for relevance to AI warfare, governance mechanisms, and public health impacts. Full-text articles were then assessed based on inclusion criteria, including (a) explicit discussion of AI or emerging military technologies, (b) relevance to governance, ethics, or regulatory frameworks, and (c) implications for civilian populations or health systems. Studies that focused solely on technical AI development without governance or health implications were excluded. This process ensured that the final body of literature directly informed the constructs and relationships specified in the AIW–PHI framework.

Guided by this structure narrative approach, the literature review serves two primary purposes. First, it contextualizes each construct of the AIW–PHI framework by synthesizing relevant empirical and theoretical literature on AI-enabled military capabilities, governance and ethical oversight, and health system impacts in conflict settings. Second, it identifies critical gaps in the literature, particularly the limited integration of governance mechanisms as a linking factor between AI warfare and population health outcomes.

The review is therefore organized in alignment with the AIW–PHI framework. It begins with an examination of AI warfare capabilities and their implications for strategic dominance and technological asymmetry, followed by an analysis of ethical governance and regulatory approaches. It then explores health system vulnerability in conflict environments and concludes with a synthesis of research on population health outcomes. Through this structured and systematic review process, the study establishes a strong evidentiary foundation for the proposed governance framework and highlights the need for integrative approaches to mitigate public health risks in AI-mediated conflict environments.

AI Warfare Foundations and Theoretical Development

Foundational scholarship on autonomous and artificial intelligence (AI)–enabled weapon systems established the conceptual basis for understanding the transformation of modern warfare. Early work emphasized that increasing autonomy shifts decision-making authority from human operators to algorithmic systems, thereby altering command structures, compressing decision timelines, and introducing risks related to system unpredictability and escalation (Scharre, 2018; Arkin, 2009). Parallel analyses documented the integration of machine learning into surveillance, targeting, and operational coordination, highlighting a trajectory toward increasingly autonomous battlefield ecosystems (Boulain & Verbruggen, 2017).

Ethical and legal scholarship further deepened this foundation by examining the implications of autonomy for accountability, moral agency, and compliance with international humanitarian law. These studies raised concerns regarding the “accountability gap,” wherein responsibility becomes diffused across human–machine interactions, complicating legal attribution and ethical judgment (Crootof, 2015; Sparrow, 2016; Asaro, 2012). Such concerns positioned AI warfare as not merely a technological evolution but a normatively disruptive phenomenon requiring new governance frameworks.

More recent research has expanded this perspective by situating AI-enabled warfare within broader socio-technical and geopolitical systems. Contemporary analyses emphasize that AI is increasingly embedded within interconnected military infrastructures, including cyber warfare, autonomous surveillance systems, and decision-support algorithms, thereby amplifying the scale, speed, and complexity of conflict (Horowitz, 2018; Johnson, 2020; Payne, 2021). These developments introduce systemic risks, including reduced human oversight, algorithmic bias in targeting, and the potential for unintended escalation due to rapid, machine-driven decision cycles.

Emerging interdisciplinary scholarship also highlights the indirect and cascading impacts of AI-enabled warfare on civilian populations, particularly through disruptions to critical infrastructure and essential services. Studies in global health and conflict research demonstrate that modern warfare disproportionately affects population health through system-level breakdowns, including damage to healthcare infrastructure, interruption of supply chains, and forced displacement (Ghobarah et al., 2003; Wise, 2022; Garfield & Neugut, 2023). These findings reinforce the need to conceptualize AI warfare as a determinant of population health, extending beyond immediate combat effects to long-term epidemiological and societal consequences.

Collectively, these diverse sources support the characterization of AI warfare as a complex, adaptive socio-technical system shaped by interactions among technological innovation, institutional governance, and human decision-making. This expanded theoretical foundation provides a robust basis for advancing frameworks such as AIW–PHI and TWD–PH, which integrate technological, ethical, and public health dimensions to explain how AI-enabled warfare produces cascading effects across interconnected systems.

Artificial Intelligence in Warfare and Strategic Transformation

The integration of artificial intelligence (AI) into military operations has significantly transformed modern warfare, particularly in intelligence processing, targeting, and decision-making systems. AI-enabled technologies allow military actors to analyze vast datasets from surveillance, satellite imagery, and signals intelligence, thereby enhancing operational speed, precision, and scalability (Carranza, 2025; Mishra et al., 2025). These developments reflect a broader shift toward data-driven warfare, where algorithmic systems increasingly support or augment human decision-making processes.

Foundational research on autonomous and AI-enabled weapon systems provides important context for understanding these developments. Paul Scharre (2018) argued that increasing autonomy fundamentally reshapes military decision-making structures, introducing both efficiency gains and risks related to control, reliability, and escalation. Similarly, Boulanin and Verbruggen (2017) documented the rapid evolution of autonomy in weapon systems, emphasizing the growing role of machine learning in targeting and operational coordination. These findings are complemented by broader analyses of emerging military technologies, which highlight how AI is reshaping the strategic logic of warfare and contributing to technological competition among state actors (Mishra et al., 2025).

Recent scholarship further underscores the implications of these developments for strategic power dynamics. AI-enabled systems contribute to strategic dominance and technological asymmetry, reinforcing disparities between technologically advanced and less-resourced actors. Empirical evidence from contemporary conflicts demonstrates that AI tools are increasingly used to process real-time data streams for target identification, significantly compressing operational timelines and expanding the scale of engagement (Amaral, 2026). Collectively, these studies establish AI warfare capability as a transformative force that shapes both operational efficiency and structural power relations in modern conflict.

Ethical Governance and Regulation of AI in Warfare

As AI technologies become more deeply embedded in military operations, governance and ethical oversight have emerged as critical concerns. A growing body of literature emphasizes that governance frameworks are essential for ensuring that technological capabilities are translated into responsible and accountable military practices (Hammer, 2025). These frameworks encompass legal, ethical, and institutional mechanisms, including compliance with international humanitarian law, accountability structures, and human oversight in decision-making.

Ethical critiques of AI in warfare highlight significant challenges related to responsibility and accountability. Robert Sparrow (2016) argued that autonomous weapons systems disrupt traditional notions of moral responsibility by diffusing accountability across human and machine actors. Similarly, Crootof (2015) identified legal ambiguities associated with emerging military technologies, particularly regarding attribution of responsibility in cases of harm. More recent analyses suggest that AI decision-support systems may further complicate accountability by reducing transparency and interpretability in decision-making processes (Johnson, 2026).

Policy-oriented research indicates that existing governance mechanisms remain fragmented and insufficient. Boulanin (2023) argued that current regulatory approaches lack the technical specificity required to effectively govern AI-enabled systems, while the United Nations (2023) has acknowledged ongoing challenges in achieving international consensus on autonomous weapons regulation. Similarly, Simmons-Edler et al. (2025) emphasized that governance frameworks often fail to keep pace with technological advancements, creating regulatory gaps that may increase risks to civilian populations.

Collectively, these studies demonstrate that while governance structures are critical, they remain underdeveloped relative to the pace of technological innovation. This reinforces the central role of ethical governance within the AIW–PHI framework as a key mechanism shaping how AI warfare capabilities translate into real-world outcomes.

AI Warfare and Public Health Implications in Contemporary Conflict

Although the literature on AI-enabled warfare has expanded rapidly, comparatively fewer studies have explicitly examined its implications for public health. Nevertheless, emerging interdisciplinary research indicates that AI-enabled warfare is reshaping both the scale and nature of health risks in contemporary conflicts. In ongoing conflicts such as those in Ukraine and Gaza Strip, the integration of AI-driven surveillance, targeting, and decision-support systems has accelerated operational tempo and increased strike precision; however, these same capabilities have also intensified risks to civilian populations due to compressed decision cycles and reduced opportunities for human deliberation (Jecker et al., 2024; Nobles, 2024; Maurer, 2023). As military operations become increasingly data-driven and automated, the potential for rapid escalation and widespread exposure to harm correspondingly increases.

A critical concern emerging from recent scholarship is the risk of algorithmic misidentification and targeting errors, particularly in densely populated urban environments. AI systems trained on incomplete or biased datasets may misclassify individuals or infrastructure, leading to unintended civilian casualties and subsequent cascading public health effects, including trauma, displacement, and disruption of essential services (Amaral, 2026; Sharkey, 2022). These risks are amplified in asymmetric warfare contexts, where combatants and civilians are often spatially intertwined, complicating the reliability of automated targeting systems.

Beyond immediate physical harm, AI-enabled warfare contributes to broader systemic and indirect health impacts. Contemporary conflict analyses highlight how attacks on energy grids, water systems, and healthcare infrastructure—often facilitated or optimized through AI-assisted intelligence—produce cascading failures across public health systems (Devi, 2022; Wise, 2022). For example, disruptions to electricity and water supply chains in conflict zones have been associated with increased incidence of infectious diseases, reduced access to medical care, and heightened mortality among vulnerable populations. These findings reinforce the argument that the most significant health consequences of modern warfare often arise not from direct violence but from infrastructure degradation and system collapse.

Emerging research also underscores the environmental and long-term societal implications of AI-enabled warfare. Military applications of AI, particularly in cyber-physical systems and autonomous operations, have been linked to environmental degradation, including damage to industrial facilities, pollution of water sources, and exacerbation of climate-related health risks (Irfan & Sirvent, 2025; Mach et al., 2023). These environmental disruptions further extend the temporal scope of health impacts, contributing to chronic disease burdens, food insecurity, and population displacement long after active hostilities have ceased.

Together, these developments support the conceptualization of AI-enabled warfare as a multidimensional determinant of population health, operating through both direct and indirect pathways. Rather than being confined to immediate injury and mortality, the health impacts of AI-mediated conflict are better understood as cascading, system-level phenomena that unfold across interconnected domains, including infrastructure, environment, and social systems. This perspective aligns with a growing body of public health and conflict research emphasizing that contemporary warfare particularly when augmented by advanced technologies produces prolonged and compounding effects on population health outcomes, necessitating integrated frameworks that account for technological, governance, and systemic drivers of harm.

Health System Vulnerability in Conflict Environments

A substantial body of public health and conflict literature demonstrates that armed conflict disproportionately undermines health systems, often resulting in long-term structural degradation. Core mechanisms include the destruction of healthcare infrastructure, displacement and attrition of the health workforce, disruption of pharmaceutical and supply chains, and the erosion of governance and financing structures. While early foundational work established these relationships (e.g., Levy & Sidel, 2016), more recent analyses confirm that contemporary conflicts continue to produce system-wide fragility,

particularly in already resource-constrained settings (World Health Organization, 2023; Kruk et al., 2022). In ongoing conflicts such as those in Ukraine and Gaza Strip, repeated attacks on hospitals, energy systems, and water infrastructure have further demonstrated how modern warfare systematically degrades the operational capacity of health systems, reducing access to essential services and increasing population vulnerability (Devi, 2022; Rubenstein et al., 2023).

Empirical research consistently shows that the indirect effects of conflict on health systems often exceed direct mortality in both magnitude and duration. Classic studies demonstrated that excess mortality persists long after hostilities cease, largely due to weakened health systems and deteriorating living conditions (Ghobarah et al., 2003). This pattern has been reaffirmed in more recent global health research, which highlights how service interruptions, reduced vaccination coverage, and loss of maternal and emergency care contribute to prolonged morbidity and mortality in post-conflict environments (Garfield & Neugut, 2023; Wise, 2022). These findings underscore that health system collapse operates as a central mediating mechanism, translating conflict exposure into long-term epidemiological consequences.

Contemporary scholarship further emphasizes that health systems in conflict settings are not only physically vulnerable but also systemically fragile due to interdependence across critical infrastructures. Disruptions to electricity, transportation, and communication networks—often targeted in modern warfare—produce cascading failures that compromise healthcare delivery at multiple levels (Kruk et al., 2022; Blanchet et al., 2023). This systems perspective aligns with emerging resilience frameworks, which conceptualize health systems as adaptive but highly sensitive to shocks, particularly when compounded by repeated or prolonged disruptions.

Emerging evidence suggests that AI-enabled warfare may intensify existing vulnerabilities while introducing new forms of systemic risk. The integration of AI into targeting, surveillance, and cyber operations has increased the precision and frequency of strikes on critical infrastructure, while also accelerating the pace of conflict in ways that overwhelm already fragile health systems (Maurer, 2023; Nobles, 2024). In addition, the growing reliance on digital health infrastructure—such as electronic health records, telemedicine platforms, and data networks—has expanded the attack surface for cyber operations, creating new vulnerabilities related to health information systems and communication networks (Monzon Baeza et al., 2025; Kott & Linkov, 2021). These developments suggest that AI-enabled warfare not only amplifies traditional pathways of harm but also introduces hybrid threats that blur the boundaries between physical and digital domains.

Taken together, these findings support the positioning of health system vulnerability as a proximal and dynamic mechanism linking warfare to population health outcomes within the AIW–PHI framework. Rather than functioning as a static condition, vulnerability emerges as a cascading, system-level phenomenon, shaped by the interaction of infrastructural damage, governance capacity, technological disruption, and environmental stressors. This conceptualization provides a robust foundation for analyzing how contemporary and AI-mediated conflicts produce both immediate and long-term health consequences across interconnected systems.

Population Health Outcomes in Technological Conflict

A substantial body of conflict and global health literature demonstrates that armed conflict produces multidimensional population health outcomes, including mortality, injury, forced displacement, infectious disease outbreaks, and long-term mental health sequelae. While early foundational research established that war generates both immediate and prolonged health burdens, more recent evidence confirms that indirect effects, mediated through system disruption, often exceed direct battlefield mortality in magnitude and duration (Ghobarah et al., 2003; Garfield & Neugut, 2023). Contemporary conflicts continue to reflect this pattern, as seen in Ukraine and Gaza Strip, where large-scale displacement, disruption of essential services, and constrained access to healthcare have produced cascading health consequences across affected populations (Devi, 2022; Rubenstein et al., 2023).

Recent scholarship suggests that the integration of artificial intelligence (AI) into warfare may reshape both the distribution and intensity of these health outcomes. AI-enabled systems, particularly in surveillance, targeting, and decision-support—compress decision timelines and increase operational tempo, thereby expanding the scale and frequency of population exposure to conflict-related hazards (Horowitz, 2018; Nobles, 2024). Although such systems may enhance precision in some contexts, they also introduce risks associated with algorithmic bias, misidentification, and reduced human oversight, which can contribute to unintended civilian harm and amplify downstream public health effects (Sharkey, 2022; Jecker et al., 2024). In densely populated or asymmetric conflict environments, these risks are further magnified, increasing the likelihood of widespread exposure to injury, trauma, and displacement.

Beyond physical outcomes, AI-enabled warfare raises significant concerns regarding psychological and social health impacts. Persistent exposure to AI-driven surveillance, autonomous systems, and high-intensity conflict environments contributes to chronic stress, anxiety, and trauma among civilian populations. Emerging research highlights the cumulative mental health burden associated with prolonged conflict exposure, including increased prevalence of post-traumatic stress disorder (PTSD), depression, and anxiety disorders, particularly among displaced and vulnerable groups (Charlson et al., 2019; Wise, 2022). These findings suggest that the health impacts of technological warfare extend beyond immediate physical harm to encompass long-term psychosocial consequences that shape population well-being across generations.

Importantly, population health outcomes in technological conflict are not determined solely by the presence or sophistication of AI capabilities but are significantly shaped by structural and governance-related factors. Institutional capacity, regulatory oversight, and adherence to international humanitarian norms influence both the conduct of warfare and its downstream health consequences (Kruk et al., 2022; Payne, 2021). Variations in governance quality can mediate the extent to which technological capabilities translate into population-level harm, reinforcing the role of systemic and institutional conditions as critical determinants of health outcomes in conflict settings.

Taken together, these findings support the conceptualization of population health outcomes as the terminal, yet dynamically influenced, construct within technological conflict frameworks such as AIW–PHI. Health outcomes emerge from interacting pathways involving technological capability, system vulnerability, and governance mechanisms, rather than from isolated battlefield events. This systems-based perspective underscores the need to analyze population health in conflict environments as a cascading, multilevel phenomenon, shaped by both immediate exposures and broader structural conditions over time.

Synthesis and Identified Gap

Across the reviewed literature, several key themes emerge. First, AI is rapidly transforming warfare by enhancing operational efficiency and contributing to strategic dominance and technological asymmetry (Boulanin & Verbruggen, 2017; Mishra et al., 2025; Paul Scharre, 2018). Second, governance and ethical oversight are critical yet underdeveloped components in regulating AI-enabled military systems, with existing frameworks often fragmented and insufficient (Boulanin, 2023; Crootof, 2015; Simmons-Edler et al., 2025; United Nations, 2023). Third, conflict continues to produce profound public health consequences, particularly through the disruption of health systems and the persistence of indirect health effects (Ghobarah et al., 2003; Levy & Sidel, 2016).

Foundational and supporting studies on autonomous weapons, governance frameworks, and conflict-related health outcomes further reinforce these findings, highlighting the ethical, legal, and systemic complexities associated with AI-enabled warfare (Boulanin & Verbruggen, 2017; Crootof, 2015; Scharre, 2018; Sparrow, 2016).

Despite these advances, a significant gap remains. The literature on AI warfare primarily focuses on military and ethical considerations, while public health research examines conflict impacts largely independent of emerging technologies. Few studies explicitly integrate governance as the linking mechanism between AI warfare capabilities and population health outcomes.

The AIW–PHI framework addresses this gap by providing a unified, governance-centered model that connects AI-enabled warfare, regulatory structures, and public health consequences. By integrating technological, legal, and health system perspectives into a single analytical framework, the study advances a novel contribution to both AI governance and conflict-health scholarship and provides a foundation for developing policy-relevant interventions in AI-mediated conflict environments.

IV. METHODOLOGY

Research Design

This study employs a qualitative policy analysis combined with conceptual framework development to examine how ethical governance and regulatory structures shape the public health implications of artificial intelligence (AI)–enabled warfare. The design is interpretive and theory-guided, using the AI Warfare–Public Health Impact (AIW–PHI) framework to structure analysis and synthesis. This approach is appropriate for studies focused on governance environments, regulatory gaps, and framework development rather than causal inference (Bowen, 2009; Walt et al., 2008).

The methodological approach integrates document analysis, comparative policy analysis, and thematic synthesis. Document analysis serves as the primary method for examining governance frameworks, while comparative policy analysis enables cross-context evaluation of regulatory approaches. Thematic synthesis is used to organize findings into analytically meaningful categories aligned with the AIW–PHI constructs. This approach is consistent with recent scholarship emphasizing the importance of governance, ethics, and systems-level perspectives in AI and public health research (Gao et al., 2026; Wagner, 2024).

Data Sources and Sampling Strategy

Data were drawn from both primary and secondary sources. Primary sources included international legal and policy documents relevant to AI and warfare, such as international humanitarian law instruments (e.g., the Geneva Conventions), reports from the United Nations, publications from the World Health Organization, guidance from the International Committee of the Red Cross, and strategic documents from the NATO. National AI defense strategies from major geopolitical actors were also included where available.

Secondary sources consisted of peer-reviewed journal articles, policy briefs, and think tank reports addressing AI in warfare, governance, and public health implications. A purposive sampling strategy was employed to select documents based on their relevance to three criteria: (a) explicit discussion of AI-enabled or emerging military technologies, (b) inclusion of governance, ethical, or regulatory considerations, and (c) implications for civilian protection or health systems (Patton, 2015). This strategy ensured alignment between selected materials and the constructs of the AIW–PHI framework, while also reflecting recent calls for integrating governance and public health perspectives in AI research (Panteli et al., 2025; Bharel et al., 2024).

Search Strategy

A structured search strategy was employed to identify relevant literature and policy documents. Searches were conducted across Scopus, Web of Science, PubMed, and Google Scholar using combinations of keywords such as “artificial intelligence AND warfare,” “autonomous weapons AND international humanitarian law,” “AI governance AND military,” and “conflict AND public health.” Additional terms included “ethical oversight,” “civilian protection,” and “health system vulnerability.”

The search focused primarily on publications from 2015 to 2026 to capture the rapid evolution of AI-enabled warfare, while seminal works were included to provide theoretical grounding. Titles and abstracts were screened for relevance, followed by full-text review based on inclusion criteria. Sources focused exclusively on technical AI development without governance or public health implications were excluded. This approach reflects best practices for structured narrative reviews that prioritize transparency and rigor without requiring formal systematic review protocols (Snyder, 2019) and is consistent with recent methodological applications in AI and public health research (Gao et al., 2026).

Data Collection and Coding Procedures

Selected documents were systematically organized and analyzed using a structured coding protocol. Data extraction focused on identifying policy language and thematic content related to governance mechanisms, ethical principles, regulatory provisions, and public health considerations. Key elements included accountability, human oversight, civilian protection, infrastructure safeguards, and AI-specific regulatory measures.

The analysis followed a three-stage coding process. First, open coding was used to identify recurring themes related to governance and public health. Second, axial coding grouped these themes into higher-order categories, including accountability structures, oversight mechanisms, technological regulation, and health system protections. Third, a gap analysis compared existing governance frameworks with identified public health risks to highlight areas of insufficiency. This analytical approach is consistent with qualitative document analysis methods used in policy research (Bowen, 2009).

Analytical Framework

The AIW–PHI framework guided the interpretation and organization of findings. Specifically, the analysis examined how AI warfare capabilities are addressed within governance structures, how governance mechanisms influence health system vulnerability, and how gaps in regulation contribute to adverse population health outcomes. This aligns with emerging scholarship emphasizing governance as a central mechanism linking technological systems to health outcomes (Wagner, 2024; Onderco, 2026).

Trustworthiness and Rigor

Several strategies were employed to ensure rigor and credibility. Triangulation was achieved through the use of diverse data sources, including policy documents, academic literature, and institutional reports (Creswell & Poth, 2018). Dependability was supported through a consistent coding protocol and documentation of analytical decisions. Confirmability was ensured by grounding interpretations in explicit policy language, while transferability was addressed through the inclusion of multiple global governance contexts. These practices align with established qualitative research standards and recent applications in policy and health systems research.

Ethical Considerations

This study relied exclusively on publicly available documents and secondary sources and therefore did not require institutional review board approval. All sources were accurately represented, and care was taken to maintain analytical neutrality.

V. FINDINGS & RESULTS

Collectively, these findings provide a structured understanding of both the strengths and limitations of current governance approaches to AI-enabled warfare. While existing frameworks demonstrate progress in establishing ethical and regulatory foundations, the identified gaps and public health blind spots reveal critical areas of vulnerability. Building on these results, the next section interprets these themes through the lens of the TWD–PH framework, examining how governance deficiencies contribute to cascading disruptions and shape population health outcomes in technologically mediated conflict environments.

Governance Structures and Gaps in AI-Enabled Warfare

The analysis of international policy documents, institutional reports, and scholarly literature revealed four major thematic areas: (1) existing governance structures, (2) ethical governance mechanisms, (3) governance gaps and limitations, and (4) public health blind spots. These themes reflect how AI-enabled warfare is currently regulated and where critical deficiencies exist in protecting population health.

Existing Governance Structures for AI-Enabled Warfare

Findings indicate that governance of AI-enabled warfare is primarily anchored in existing international humanitarian law (IHL) frameworks rather than AI-specific regulations. Core principles derived from the Geneva Conventions—including distinction, proportionality, and necessity, remain the dominant regulatory foundation guiding the use of emerging military technologies. These principles are reinforced in guidance from the International Committee of the Red Cross (2021), which emphasizes the continued applicability of IHL to AI-assisted systems.

At the international level, governance efforts are further reflected in discussions led by the United Nations (2023) on lethal autonomous weapons systems, as well as strategic frameworks such as the NATO (2021) artificial intelligence strategy. These documents highlight the importance of human oversight, accountability, and compliance with legal norms. However, they largely operate as guiding principles rather than enforceable regulations, indicating that governance remains normative rather than binding.

National-level strategies similarly emphasize ethical AI use, but vary significantly in scope, specificity, and enforcement mechanisms. Overall, governance structures are fragmented and uneven, reflecting differences in political priorities, technological capabilities, and regulatory approaches across jurisdictions.

Ethical Governance Mechanisms and Oversight

Across the analyzed documents, several recurring ethical governance mechanisms were identified. These include meaningful human control, accountability frameworks, transparency requirements, and operational constraints designed to protect civilians. Human oversight is consistently emphasized as a critical safeguard, particularly in decision-making processes involving lethal force. Policy documents frequently refer to the need for human-in-the-loop or human-on-the-loop systems to maintain accountability and ethical responsibility.

Accountability mechanisms, including legal responsibility and post-action review processes, are also present but often lack operational clarity. While institutions acknowledge the importance of accountability, few frameworks specify how

responsibility is assigned in cases involving AI-assisted decision-making. Similarly, transparency is promoted as a principle, but practical mechanisms for ensuring explainability and auditability of AI systems remain underdeveloped.

These findings suggest that ethical governance is widely recognized as essential but is implemented inconsistently and often lacks enforceable mechanisms, limiting its effectiveness in mitigating risks associated with AI-enabled warfare.

Governance Gaps and Regulatory Limitations

A central finding of the analysis is the presence of significant governance gaps in addressing AI-enabled warfare. First, there is a lack of AI-specific regulatory frameworks, with most policies relying on pre-existing legal structures that were not designed to account for algorithmic decision-making or autonomous systems. This creates ambiguity in how traditional legal principles should be applied to emerging technologies.

Second, enforcement mechanisms are weak or absent. Many governance frameworks operate as voluntary guidelines or non-binding agreements, limiting their capacity to regulate state and non-state actors effectively. This is particularly evident in international efforts to regulate autonomous weapons, where consensus remains limited and enforcement mechanisms are unclear.

Third, there is a disconnect between technological development and regulatory adaptation. AI capabilities are advancing rapidly, while governance structures evolve more slowly, resulting in a widening gap between what technology can do and what regulatory frameworks can effectively control. Recent analyses also highlight growing public resistance and ethical concerns regarding military AI deployment, further complicating governance efforts (Trends Research & Advisory, 2025).

Finally, governance frameworks often fail to address system-level risks, focusing instead on individual decision points rather than broader structural impacts of AI-enabled warfare. This limits their ability to mitigate cascading effects on infrastructure and civilian populations.

Public Health Blind Spots in Governance Frameworks

A critical finding of this study is the limited integration of public health considerations within AI warfare governance frameworks. While existing policies emphasize civilian protection in general terms, they rarely incorporate explicit public health metrics or frameworks for assessing health-related impacts.

Few documents address issues such as 1) Health system disruption 2) Infrastructure damage affecting healthcare delivery 3) Indirect mortality and morbidity 4) Long-term population health consequences

Although organizations such as the World Health Organization (2022) highlight the significant health impacts of conflict, these considerations are largely absent from AI governance discussions. This represents a major gap, as health outcomes are often shaped by systemic disruptions rather than direct violence alone.

Additionally, there is limited attention to health system resilience or the protection of critical infrastructure such as hospitals, water systems, and supply chains in the context of AI-enabled warfare. This omission suggests that governance frameworks are not fully aligned with the broader determinants of population health.

Overall, the findings indicate that while governance structures for AI-enabled warfare exist, they are fragmented, insufficiently adapted to emerging technologies, and largely disconnected from public health considerations. Ethical governance mechanisms are widely recognized but inconsistently implemented, and significant gaps remain in regulatory specificity, enforcement, and integration of health-related outcomes.

These findings provide the empirical foundation for examining how governance functions within the AIW–PHI framework and highlight the need for a more integrated, governance-centered approach to protecting population health in AI-mediated conflict environments.

VI. DISCUSSION

This study examined how ethical governance and regulatory frameworks shape the public health implications of artificial intelligence (AI)–enabled warfare. The findings indicate that although governance structures exist, they remain fragmented, insufficiently adapted to emerging technologies, and largely disconnected from public health considerations. These results are consistent with interdisciplinary scholarship demonstrating that regulatory frameworks continue to lag behind rapid technological advancements in autonomous and AI-enabled systems (Horowitz, 2018; Payne, 2021). Interpreted through the AI Warfare–Public Health Impact (AIW–PHI) framework, the findings reinforce the conceptualization of AI-enabled

warfare as a structural determinant of population health, mediated through governance mechanisms and system-level dynamics.

Governance as the Central Mediating Mechanism

A central contribution of this study is the empirical and conceptual reinforcement of ethical governance as the primary mediating mechanism within the AIW–PHI framework. The findings demonstrate that AI warfare capabilities do not directly translate into population health outcomes; rather, their effects are filtered through governance structures that shape how technologies are developed, deployed, and constrained.

Existing frameworks grounded in international humanitarian law, particularly the principles of distinction and proportionality, provide a normative foundation for regulating conflict. However, these frameworks were not designed to address algorithmic decision-making systems and therefore exhibit limitations when applied to AI-enabled warfare. This observation aligns with prior legal and ethical scholarship emphasizing that the implications of autonomous systems depend on the presence of human oversight, accountability, and enforceable governance structures (Crootof, 2015; Sharkey, 2022; Asaro, 2012; Sparrow, 2016).

The findings extend this literature by demonstrating that governance functions not only as a normative constraint but as a causal pathway, mediating the relationship between AI warfare capability and health system vulnerability. Where governance mechanisms are robust, characterized by enforceable oversight, clear accountability, and meaningful human control, the risks associated with AI-enabled warfare may be mitigated. Conversely, weak or fragmented governance allows technological capabilities to operate with fewer constraints, increasing the likelihood of systemic disruption and adverse population health outcomes.

Fragmentation and the Governance–Technology Gap

The findings further highlight a persistent governance–technology gap, wherein the pace of AI development exceeds the capacity of regulatory frameworks to adapt. While international efforts emphasize ethical principles and human oversight, they often lack binding enforcement mechanisms, resulting in governance systems that remain largely normative rather than operational.

This observation is consistent with existing research demonstrating that global governance mechanisms for AI in warfare are fragmented and unevenly implemented (Johnson, 2020; Maurer, 2023). From the perspective of the AIW–PHI framework, this gap weakens the mediating role of governance, allowing AI-enabled systems to exert greater influence on downstream outcomes. The absence of enforceable standards, combined with variability in national policies, contributes to regulatory inconsistency and uneven implementation.

This fragmentation is particularly consequential in conflict environments, where asymmetries in both technological capability and governance capacity amplify risks to civilian populations. As supported by prior research, such inconsistencies contribute to unequal exposure to harm and reinforce patterns of systemic vulnerability (Rubenstein et al., 2023).

Ethical Governance as a Conditional Moderator of Harm

In addition to its mediating role, the findings support the conceptualization of ethical governance as a conditional moderator within the AIW–PHI framework. Governance mechanisms influence not only whether AI capabilities translate into harm but also the magnitude and distribution of that harm.

This dual role is consistent with broader literature on technological risk and system resilience, which highlights the importance of institutional capacity and regulatory quality in shaping the societal impacts of advanced technologies (Kruk et al., 2022; Kott & Linkov, 2021). For instance, the presence of human-in-the-loop systems and accountability processes may reduce the likelihood of unintended targeting or escalation, whereas their absence increases risks associated with automation and algorithmic error (Jecker et al., 2024; Nobles, 2024).

This moderating function becomes particularly significant in contexts of strategic dominance and technological asymmetry. As AI-enabled warfare enhances the operational capabilities of certain actors, governance structures become essential for constraining these capabilities in ways that protect civilian populations. Where governance is weak, technological advantages may translate into disproportionate impacts on vulnerable populations, reinforcing inequality and systemic harm.

Health System Vulnerability as the Critical Pathway

A key insight from this study is the identification of health system vulnerability as the primary pathway through which AI-enabled warfare affects population health outcomes. The findings indicate that governance frameworks rarely address the systemic impacts of conflict on healthcare infrastructure, workforce capacity, and service delivery, instead focusing primarily on immediate targeting decisions.

This aligns with extensive conflict-health literature demonstrating that indirect effects of conflict, particularly those mediated through health system disruption, often exceed direct mortality in magnitude and duration (Ghobarah et al., 2003; Garfield & Neugut, 2023). Recent evidence from contemporary conflicts further supports this, showing that attacks on infrastructure produce cascading failures that disrupt healthcare delivery and compromise population health (Devi, 2022; Wise, 2022).

Within the AIW–PHI framework, health system vulnerability functions as the proximal mechanism linking governance failures to population health outcomes. The absence of governance provisions addressing system resilience, infrastructure protection, and continuity of care therefore represents a critical gap in current regulatory approaches.

Public Health as a Missing Dimension of AI Governance

One of the most significant findings of this study is the absence of public health integration within AI warfare governance frameworks. While existing policies emphasize civilian protection in general terms, they rarely incorporate explicit public health metrics, health system considerations, or mechanisms for assessing long-term health impacts. This reflects a broader disconnect between security-focused and public health-oriented policy domains (Wise, 2022; Blanchet et al., 2023).

The AIW–PHI framework addresses this gap by explicitly linking governance mechanisms to population health outcomes, thereby expanding the scope of AI governance beyond ethical and legal considerations to include health system resilience and epidemiological impacts. This represents a critical shift from viewing AI warfare solely as a military or technological issue to understanding it as a public health concern with systemic implications.

Theoretical Contribution of the AIW–PHI Framework

The findings provide strong empirical and conceptual support for the AIW–PHI framework as a novel, governance-centered model for understanding the intersection of AI warfare and public health. Specifically, the study contributes to theory in three keyways.

First, it reframes AI-enabled warfare as a structural determinant of population health, extending existing conflict-health literature to incorporate emerging technological dynamics. Second, it positions ethical governance as a central causal mechanism, rather than a peripheral or normative consideration. Third, it integrates technological, legal, and public health perspectives into a unified analytical framework, addressing a critical gap in existing scholarship.

Although the framework is presented as linear for conceptual clarity, the findings suggest that future research should explore dynamic and recursive relationships, particularly how governance failures and health system disruptions reinforce one another over time.

Overall, the findings indicate that AI-enabled warfare operates through governance-mediated pathways that shape health system vulnerability and, ultimately, population health outcomes. The effectiveness of governance mechanisms determines whether technological capabilities are constrained or amplified, thereby influencing the scale and distribution of harm.

However, current governance frameworks remain fragmented, weakly enforced, and largely disconnected from public health considerations. These insights underscore the need for a more integrated and health-informed approach to AI governance, one that explicitly incorporates public health as a core dimension of regulatory frameworks and addresses the systemic impacts of emerging military technologies.

Synthesis of Findings, Literature, and Theoretical Contributions

To strengthen the interpretive rigor of this study and situate the findings within the broader body of scholarship, a structured synthesis was conducted linking key empirical insights to supporting literature and their corresponding theoretical implications within the AI Warfare–Public Health Impact (AIW–PHI) framework. This approach enables a systematic integration of results with existing evidence, ensuring that the study's conclusions are not only internally consistent but also externally validated through alignment with prior research.

The synthesis presented in Table 1 maps the study’s core findings to relevant scholarly literature and identifies how each finding contributes to the development and refinement of the AIW–PHI framework. Specifically, the table highlights how governance functions as both a mediating and moderating mechanism, how health system vulnerability operates as a proximal pathway linking technological capability to population health outcomes, and how the absence of public health integration represents a critical gap in current AI governance frameworks.

By explicitly connecting findings to established research and theoretical constructs, this synthesis reinforces the study’s contribution to emerging scholarship at the intersection of artificial intelligence, governance, and public health. It also provides a foundation for future empirical testing by clarifying the relationships among key variables and identifying pathways that can be operationalized in subsequent quantitative or mixed-methods research.

Table 1: Findings and Theory Synthesis

Key Finding	Supporting Literature	Theoretical Contribution (AIW–PHI)
Governance mediates AI warfare impacts	Crootof (2015); Sharkey (2022)	Governance as primary mediating mechanism
Governance–technology gap exists	Johnson (2020); Maurer (2023)	Weak mediation → increased system disruption
Governance moderates harm	Jecker et al. (2024); Nobles (2024)	Governance as conditional moderator
Health system vulnerability is key pathway	Ghobarah et al. (2003); Garfield & Neugut (2023)	Vulnerability as proximal mechanism
Indirect effects exceed direct mortality	Wise (2022); Devi (2022)	Supports cascading systems logic (TWD–PH)
Public health missing in governance	Blanchet et al. (2023)	Identifies critical theoretical gap
AI accelerates and amplifies harm	Horowitz (2018); Payne (2021)	AI as structural determinant amplifier

Implications for Policy, Practice, and Theory

The findings of this study have important implications for policy development, military practice, and theoretical advancement. By demonstrating that governance mechanisms mediate the relationship between AI-enabled warfare and population health outcomes, this study highlights the need for a more integrated, governance-centered approach to regulating emerging military technologies.

Policy Implications

The results underscore the urgent need to strengthen and modernize governance frameworks for AI-enabled warfare. Existing regulatory structures, largely grounded in the Geneva Conventions, provide a normative foundation but are insufficient to address the complexities of algorithmic decision-making and autonomous systems. Policymakers should prioritize the development of AI-specific regulatory standards that explicitly address issues such as algorithmic accountability, system transparency, and the preservation of meaningful human control.

A key policy implication is the need to integrate public health considerations into AI governance frameworks. Current approaches emphasize civilian protection in general terms but fail to incorporate explicit mechanisms for assessing and mitigating health system impacts. Governance frameworks should therefore include provisions for 1) Health impact assessments prior to deployment 2) Protection of critical health infrastructure 3) Monitoring of population health outcomes during and after conflict.

International coordination is also essential. Efforts led by the United Nations and strategic initiatives from the NATO should move beyond voluntary guidelines toward more coherent and enforceable international standards. Without stronger coordination, fragmented governance will continue to create regulatory gaps and uneven protection for civilian populations.

Practice Implications

For military and operational stakeholders, the findings highlight the importance of embedding ethical governance mechanisms into the design and deployment of AI systems. This includes ensuring meaningful human oversight in decision-making processes, particularly in high-risk contexts involving lethal force. Operational protocols should incorporate safeguards that account for uncertainty, bias, and system limitations inherent in AI technologies.

In addition, military planning should incorporate health system resilience as a strategic consideration. The protection of healthcare infrastructure, supply chains, and workforce capacity should be treated as integral to operational planning rather than as secondary concerns. This requires coordination between defense institutions, humanitarian organizations, and public health agencies.

The findings also suggest the need for real-time monitoring and accountability systems. AI-enabled operations should include mechanisms for auditing decision processes, tracking outcomes, and identifying unintended consequences. Such systems would enhance transparency and support post-action evaluation, thereby strengthening both operational effectiveness and ethical accountability.

Theoretical Implications

This study contributes to theory by advancing the AI Warfare–Public Health Impact (AIW–PHI) framework as a novel, governance-centered model that links technological capability to population health outcomes. The findings provide support for conceptualizing AI-enabled warfare as a structural determinant of health, extending existing conflict and public health literature to incorporate emerging technologies.

A key theoretical implication is the positioning of ethical governance as a central causal mechanism, rather than a peripheral or normative consideration. By demonstrating how governance mediates and conditions the effects of AI warfare capabilities, the study highlights the importance of integrating legal, ethical, and institutional dimensions into analyses of technological impact.

The findings also suggest avenues for future theoretical development. While the AIW–PHI framework is presented as a linear model for conceptual clarity, the observed governance gaps and systemic vulnerabilities indicate the potential for dynamic and recursive relationships. Future research could extend the framework to incorporate feedback loops, cumulative effects, and interactions between governance failure and health system collapse. Such extensions would align with more complex systems-based approaches and provide a deeper understanding of how technological conflict evolves over time.

Implications for Future Research

The study identifies several directions for future research. First, empirical studies are needed to test the relationships proposed in the AIW–PHI framework, particularly the mediating and moderating roles of governance. Quantitative approaches, including regression analysis or structural equation modeling, could be used to examine these relationships across different conflict contexts.

Second, future research should explore the measurement of health system vulnerability and population health outcomes in AI-mediated conflict environments. Developing reliable indicators and data collection methods will be essential for assessing the real-world impact of governance interventions.

Third, comparative studies examining differences in national governance approaches could provide insights into best practices and policy effectiveness. Such research would be particularly valuable in identifying how variations in regulatory frameworks influence outcomes across contexts.

Finally, interdisciplinary research integrating perspectives from public health, international law, and artificial intelligence will be critical for advancing both theory and practice in this emerging field.

Collectively, these implications underscore the need for a governance-centered approach to AI-enabled warfare—one that integrates technological innovation with ethical oversight and public health protection to ensure that emerging military capabilities do not produce unintended and disproportionate harm to civilian populations.

Limitations

This study has several limitations. First, it relies on qualitative policy analysis and publicly available documents, limiting insight into real-world implementation and effectiveness. Second, the purposive sampling strategy may introduce selection bias, and some relevant perspectives may not have been captured. Third, the study is conceptual and theory-building, and the AIW–PHI framework was not empirically tested, requiring future validation through quantitative or mixed-methods research. Fourth, the rapidly evolving nature of AI and military technologies may render some findings time-sensitive. Finally, the analysis focuses primarily on international and national governance, with limited attention to subnational, operational, or non-state actor dynamics.

VII. CONCLUSION

This study examined how ethical governance frameworks shape the public health implications of AI-enabled warfare and found that current approaches are fragmented, slow to adapt to technological advances, and insufficiently integrated with public health considerations. In response, the AI Warfare–Public Health Impact (AIW–PHI) framework is introduced as a novel, governance-centered model that conceptualizes AI-enabled warfare as a structural determinant of population health, operating through governance mechanisms and health system vulnerability.

This study contributes by integrating technological, legal, and public health perspectives into a unified framework and by positioning governance as a central causal mechanism in shaping outcomes. The findings highlight a critical gap in existing frameworks, the lack of explicit public health integration, and underscore the need to reconceptualize AI warfare as both a security and public health issue.

Strengthening governance through accountability, transparency, and health-focused safeguards is essential to mitigate systemic harm and ensure that advancements in military AI align with ethical standards and the protection of human well-being. By offering both explanatory clarity and practical guidance, the AIW–PHI framework provides a foundation for policymakers and researchers seeking to address the health risks associated with emerging military technologies.

REFERENCES

- [1] Amaral, J. (2026). Artificial intelligence and the evolution of modern warfare: Implications for global security and civilian protection. *International Affairs*, 102(2), 215–232.
- [2] Arkin, R. C. (2009). *Governing lethal behavior in autonomous robots*. CRC Press.
- [3] Asaro, P. (2012). On banning autonomous weapon systems: Human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 94(886), 687–709.
- [4] Bharel, M., Auerbach, J., Nguyen, V., & DeSalvo, K. B. (2024). Transforming public health practice with generative AI. *Health Affairs*, 43(6), 776–782.
- [5] Boulanin, V. (2023). *Governing artificial intelligence in military applications*. Stockholm International Peace Research Institute.
- [6] Boulanin, V., & Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems*. Stockholm International Peace Research Institute.
- [7] Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- [8] Carranza, L. (2025). Artificial intelligence and future warfare: Operational transformation and strategic implications. *NCO Journal*. U.S. Army University Press.
- [9] Charlson, F., van Ommeren, M., Flaxman, A., Cornett, J., Whiteford, H., & Saxena, S. (2019). New WHO prevalence estimates of mental disorders in conflict settings: A systematic review and meta-analysis. *The Lancet*, 394(10194), 240–248.
- [10] Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage.
- [11] Crootof, R. (2015). The killer robots are here: Legal and policy implications. *Cardozo Law Review*, 36(5), 1837–1915.
- [12] Devi, S. (2022). Ukraine conflict: Health system under attack. *The Lancet*, 399(10333), 1171–1172. [https://doi.org/10.1016/S0140-6736\(22\)00550-8](https://doi.org/10.1016/S0140-6736(22)00550-8)
- [13] Gao, Q., et al. (2026). Opportunities and challenges of artificial intelligence in public health: A systematic review. *Frontiers in Public Health*.
- [14] Garfield, R., & Neugut, A. I. (1991). Epidemiologic analysis of warfare: A historical review. *JAMA*, 266(5), 688–692.
- [15] Garfield, R., & Neugut, A. I. (2023). The health impact of war. *Annual Review of Public Health*, 44, 1–17.

- [16] Ghobarah, H. A., Huth, P., & Russett, B. (2003). Civil wars kill and maim people long after the shooting stops. *American Political Science Review*, 97(2), 189–202. <https://doi.org/10.1017/S0003055403000603>
- [17] Ghobarah, H. A., Huth, P., & Russett, B. (2003). Civil wars kill and maim people long after the shooting stops. *American Political Science Review*, 97(2), 189–202.
- [18] Hammer, M. D. (2025). Governing artificial intelligence in military contexts: Ethical frameworks and policy challenges. *Journal of Military Ethics*, 24(1), 45–62.
- [19] Heymann, D. L., & Chen, L. (2020). Public health and international security: The intersection of war and health systems. *The Lancet*, 395(10228), 181–182.
- [20] Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 36–57.
- [21] Human Rights Watch. (2020). *Stopping killer robots: Country positions on banning fully autonomous weapons and retaining human control*.
- [22] International Committee of the Red Cross. (2021). *Artificial intelligence and machine learning in armed conflict: A human-centered approach*.
- [23] International Committee of the Red Cross. (2024). *Artificial intelligence and war: Humanitarian perspectives*. <https://www.icrc.org>
- [24] Irfan, M., & Sirvent, D. (2025). Artificial intelligence in military operations: Environmental and public health implications. *Global Public Health*, 20(3), 401–415.
- [25] Jecker, N. S., Atuire, C., & Afolabi, O. (2024). Autonomous weapons systems and global justice: Implications for health equity. *BMJ Global Health*, 9(1), e013456.
- [26] Jecker, N. S., Atuire, C., & Bull, S. (2024). Autonomous weapons and the future of war: Public health risks and ethical considerations. *The Lancet Global Health*, 12(8), e1234–e1236.
- [27] Johnson, A. M. (2026). Moral responsibility and artificial intelligence in warfare: Preserving human control in automated decision-making. *International Affairs*, 102(1), 63–81.
- [28] Johnson, J. (2020). Artificial intelligence and the future of warfare: A critical analysis. *Defense Studies*, 20(3), 1–18.
- [29] Kania, E. B., Costello, K., & Vasan, A. (2023). *AI and the future of warfare: Ethical and governance challenges*. Center for a New American Security.
- [30] Kruk, M. E., Myers, M., Varpilah, S. T., & Dahn, B. T. (2022). What is a resilient health system? Lessons from Ebola and COVID-19. *The Lancet*, 385(9980), 1910–1912.
- [31] Levy, B. S., & Sidel, V. W. (2016). *War and public health* (2nd ed.). Oxford University Press.
- [32] Mishra, P., Singh, R., & Verma, A. (2025). Code, command, and conflict: The strategic implications of artificial intelligence in military competition. *Journal of Strategic Studies*, 48(2), 310–329.
- [33] Monzon Baeza, M., Patel, R., & Nguyen, T. (2025). Digital vulnerabilities in healthcare systems during conflict: The role of AI and cyber infrastructure. *Health Policy and Technology*, 14(1), 100745.
- [34] NATO. (2021). *NATO artificial intelligence strategy*.
- [35] Nobles, A. (2024). AI, targeting, and civilian protection in contemporary warfare. *Defense & Security Analysis*, 40(2), 145–162.
- [36] Nobles, J. (2024). Autonomous war and human consequences: Public health risks of AI-enabled combat systems. *BMJ Global Health*, 9(5), e012345.
- [37] Onderco, M. (2026). Understanding military AI governance through the advocacy coalition framework. *Journal of Peace Research*.

- [38] Panteli, D., Adib, K., Buttigieg, S., Goiana-da-Silva, F., Ladewig, K., & Azzopardi-Muscat, N. (2025). Artificial intelligence in public health: Promises, challenges, and an agenda for policymakers. *The Lancet Public Health*, 10(5), e428–e432. [https://doi.org/10.1016/S2468-2667\(25\)00036-2](https://doi.org/10.1016/S2468-2667(25)00036-2)
- [39] Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage.
- [40] Payne, K. (2021). Artificial intelligence: A revolution in strategic affairs? *Survival*, 63(5), 7–32.
- [41] Rubenstein, L. S., et al. (2023). Attacks on healthcare in conflict: Trends and implications. *Health and Human Rights Journal*, 25(1), 1–12.
- [42] Rustad, S. A., & Binningsbø, H. M. (2012). A price worth fighting for? Natural resources and conflict recurrence. *Journal of Peace Research*, 49(4), 531–546.
- [43] Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- [44] Sharkey, N. (2022). The automation of warfare and the erosion of human control. *Ethics and Information Technology*, 24(2), 1–12.
- [45] Simmons-Edler, R., Kallenborn, Z., & Patel, S. (2025). Governing lethal autonomous weapons: Risks, regulation, and technological complexity. *Journal of Conflict and Security Law*, 30(1), 89–112.
- [46] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
- [47] Sparrow, R. (2016). Robots and respect: Assessing the case against autonomous weapon systems. *Ethics & International Affairs*, 30(1), 93–116. <https://doi.org/10.1017/S0892679415000647>
- [48] Trends Research & Advisory. (2025). *The backlash against military AI: Public sentiment, ethical tensions, and governance challenges*.
- [49] U.S. Department of Defense. (2020). *Summary of the 2018 Department of Defense artificial intelligence strategy*.
- [50] United Nations. (2023). *Developments in the field of lethal autonomous weapons systems*.
- [51] United Nations. (2024). *Protection of civilians in armed conflict: Report of the Secretary-General*. <https://www.un.org>
- [52] Wagner, J. K. (2024). AI governance: A challenge for public health. *JMIR Public Health and Surveillance*, 10, e58358. <https://doi.org/10.2196/58358>
- [53] Walt, G., Shiffman, J., Schneider, H., Murray, S. F., Brugha, R., & Gilson, L. (2008). Doing health policy analysis: Methodological and conceptual reflections and challenges. *Health Policy and Planning*, 23(5), 308–317. <https://doi.org/10.1093/heapol/czn024>
- [54] Wise, P. H. (2022). The epidemiologic challenge to the conduct of war. *The Lancet*, 400(10363), 1603–1605. [https://doi.org/10.1016/S0140-6736\(22\)02185-3](https://doi.org/10.1016/S0140-6736(22)02185-3)
- [55] World Health Organization. (2022). *Health and armed conflict*.
- [56] World Health Organization. (2023). *Health in conflict settings: Protecting health systems and populations*. <https://www.who.int>