International Journal of Healthcare Sciences ISSN 2348-5728 (Online)
Vol. 14, Issue 1, pp: (86-98), Month: April 2026 - September 2026, Available at: www.researchpublish.com

Technological Warfare Disruption and Public Health (TWD–PH): A Systems-Based Framework for Cascading Health Impacts in AI-Enabled Conflict

Dr. David Bull

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

DOI: https://doi.org/10.5281/zenodo.20119223

Published Date: 11-May-2026

Abstract: **Contemporary warfare is increasingly defined by artificial intelligence (AI), yet its implications for population health remain insufficiently theorized. Existing scholarship is fragmented across security, governance, and public health domains, with limited integration of the mechanisms through which technological warfare produces health outcomes. This study addresses this gap by advancing the Technological Warfare Disruption–Public Health (TWD–PH) framework (Bull, 2026) as a novel mid-range explanatory theory. Grounded in complex adaptive systems theory and the structural determinants of health, the framework conceptualizes AI-enabled warfare as a structural driver of population health outcomes through cascading system disruption. The TWD–PH framework identifies key constructs, including AI warfare capability, technological dominance and strategic asymmetry, health system vulnerability, cascading disruption, and population health outcomes, while incorporating ethical governance and regulatory oversight as moderating and mediating influences. Central to the theory is cascading disruption, defined as the nonlinear and amplifying failure of interconnected systems following an initial technological shock. The framework advances a set of theoretically grounded propositions (P1–P6) that explain how technological inputs propagate through health systems and infrastructure to produce emergent outcomes such as increased morbidity, mortality, displacement, and psychological trauma. By integrating technological, structural, and governance dimensions into a unified explanatory model, the TWD–PH framework extends existing literature beyond descriptive and governance-centered approaches. The theory contributes by introducing cascading disruption as a central mechanism, conceptualizing health system vulnerability as a dynamic mediating construct, and embedding governance within system-level interactions. These contributions provide a coherent foundation for future empirical testing and offer critical insights for policy development aimed at mitigating the public health consequences of AI-enabled conflict.**

Keywords: **Artificial intelligence warfare; theory development; population health; cascading disruption; health system vulnerability; technological asymmetry; complex adaptive systems; governance.**

I. INTRODUCTION

The character of modern warfare is rapidly evolving through the integration of artificial intelligence (AI), cyber capabilities, and data-driven technologies that extend conflict beyond traditional physical domains. AI-enabled warfare now encompasses autonomous systems, algorithmic targeting, and network-centric operations that reshape how conflict is conducted and experienced. While these developments are often examined through strategic and military lenses, their broader societal implications, particularly for population health, remain insufficiently theorized. Increasingly, technological warfare is not confined to battlefield engagements but interacts with civilian infrastructure, thereby embedding health consequences within the structural dynamics of conflict itself.

Recent evidence highlights the growing vulnerability of health systems within technologically mediated conflict environments. Cyberattacks targeting healthcare infrastructure have increased significantly over the past decade, disrupting clinical operations, delaying treatments, and in some cases forcing the shutdown of entire facilities (Li, 2025; World Health Organization [WHO], 2024). In 2024 alone, hundreds of large-scale cyber incidents affected healthcare systems globally, exposing millions of individuals to risks associated with service interruption and compromised care delivery. These disruptions extend beyond digital systems to affect supply chains, diagnostic services, and emergency response capabilities, illustrating how technologically driven attacks can undermine the foundational components of healthcare delivery.

In parallel, conflict settings have witnessed escalating attacks on healthcare infrastructure, including hospitals, medical personnel, and essential services. Reports indicate that thousands of such attacks occur annually, reflecting a growing erosion of protections for health systems in conflict zones. It is worthy to note that, these events do not operate in isolation; rather, they produce interconnected and compounding effects across health systems. For example, disruptions in digital infrastructure may lead to delayed diagnostics, which in turn affect treatment outcomes, workforce strain, and overall system capacity. This interconnectedness underscores the need to move beyond event-based analyses toward a systems-oriented understanding of how technological warfare generates health consequences.

Recent geopolitical discourse has highlighted escalating concerns regarding the global diffusion of advanced artificial intelligence (AI) capabilities, particularly in military applications. Government leaders and policymakers have raised alarms about the potential transfer and proliferation of highly precise and autonomous AI systems across national boundaries, emphasizing their capacity to enhance the lethality, speed, and unpredictability of modern warfare (U.S. Department of Defense, 2023; Congressional Research Service, 2024). These concerns reflect a broader recognition that AI-enabled warfare technologies are not only tools of strategic advantage but also systemic risk factors capable of amplifying conflict intensity and extending disruption into civilian and critical infrastructure domains, including healthcare systems.

Literature Gap and Contribution

Despite increasing scholarly attention to artificial intelligence (AI) in warfare and its ethical and legal implications, the literature remains fragmented across disciplinary domains. Research in security studies and international humanitarian law has largely focused on governance, regulation, and ethical considerations, while public health scholarship has emphasized downstream outcomes such as morbidity, mortality, and displacement. However, these domains are rarely integrated into a unified analytical framework, limiting the ability to systematically explain how technological warfare shapes population health outcomes (World Health Organization [WHO], 2024; Ewoh, 2024). These cascading disruptions ultimately manifest in population health outcomes, including mortality, disease burden, displacement, and long-term psychological trauma. Population health outcomes are conceptualized as a single, unified system-level construct, representing emergent consequences of cumulative system disruption rather than isolated effects of warfare.

A critical limitation in the existing literature is the absence of mechanistic explanations linking technological warfare to public health consequences. Most studies treat conflict as a contextual or exogenous factor rather than a dynamic system characterized by internal processes and interactions. Emerging evidence demonstrates that modern technological threats, particularly cyberattacks, can directly disrupt healthcare delivery, delay treatment, and compromise patient safety, yet these effects are often examined in isolation rather than as part of a broader causal system (WHO, 2024).

Moreover, while complex systems approaches have been applied to health systems and disaster response, they have not been systematically extended to technologically mediated conflict. Contemporary reports indicate that healthcare is now one of the most targeted critical infrastructure sectors, with hundreds of cyber incidents and large-scale data breaches affecting millions of individuals annually, highlighting the growing interdependence between digital systems and health outcomes (American Hospital Association, 2025; HIPAA Journal, 2026). However, existing frameworks rarely account for nonlinear propagation of disruption, infrastructure interdependence, or feedback loops, which are essential for understanding the broader impacts of technological warfare.

In addition, health system vulnerability is frequently described in static terms, without being conceptualized as a dynamic and mediating construct shaped by technological and structural forces. Recent research highlights that healthcare systems are increasingly susceptible to cyber and hybrid threats due to digitalization, legacy infrastructure, and insufficient security integration, yet these vulnerabilities are not fully theorized within broader conflict-health models (Ewoh, 2024). Similarly, ethical governance and regulatory mechanisms are often examined independently, rather than being embedded within causal pathways that explain variations in health outcomes across conflict settings.

Furthermore, empirical evidence from conflict zones demonstrates a sharp increase in direct attacks on healthcare infrastructure, including thousands of documented incidents involving hospitals and healthcare workers, underscoring the severity and systemic nature of disruption in modern warfare contexts (Safeguarding Health in Conflict Coalition, 2025). Yet, these findings remain largely descriptive and lack integration into a comprehensive theoretical model.

To address these gaps, this study advances the Technological Warfare Disruption–Public Health (TWD–PH) framework as a novel, theory-driven, systems-based model. The framework conceptualizes AI-enabled warfare as a structural determinant of population health and introduces cascading disruption as the central explanatory mechanism linking technological inputs to health outcomes. By integrating technological capability, strategic asymmetry, health system vulnerability, and governance dynamics into a unified structure, the framework provides a comprehensive and mechanistic account of how modern warfare produces complex and emergent public health consequences. Furthermore, the model advances a set of

theoretically grounded propositions (P1–P6), establishing a foundation for future empirical testing, policy analysis, and intervention design.

This study adopts a systems-based perspective grounded in complex adaptive systems theory and the concept of structural determinants of health. From this perspective, health systems are conceptualized as interdependent networks in which infrastructure, workforce, supply chains, and digital systems interact dynamically to produce health outcomes. AI-enabled warfare is positioned as an exogenous shock that disrupts these systems, triggering cascading effects that propagate across interconnected components. Central to this perspective is the recognition that disruption is not merely a direct consequence of technological attack, but a process of cascading system failure, wherein initial disturbances amplify through feedback loops and interdependencies.

Building on this foundation, the present study introduces the Technological Warfare Disruption and Public Health (TWD–PH) model, a systems-based explanatory framework that theorizes the pathways through which AI-enabled warfare shapes population health outcomes. The model identifies key constructs, including AI warfare capability, technological dominance and asymmetry, health system vulnerability, and population health outcomes, and integrates them through a central mechanism of cascading disruption. The purpose of this study is to develop and articulate the TWD–PH framework as a mid-range explanatory theory. The study addresses the following research questions: (1) How do AI-enabled warfare capabilities generate cascading disruptions across health system components? (2) What are the direct and indirect pathways linking technological disruption to population health outcomes? and (3) How do feedback dynamics within disrupted systems amplify or attenuate health impacts in conflict settings? By shifting the analytical focus from governance to system disruption, this study provides a novel theoretical lens for understanding the public health consequences of technologically mediated conflict and establishes a foundation for future empirical investigation.

Technological Warfare Determinants of Population Health

Figure 1, Technological Warfare Determinants of Population Health, visually operationalizes Technological Warfare Disruption–Public Health (TWD–PH) framework by depicting warfare technologies as upstream structural determinants that propagate through interconnected systems to shape downstream population health outcomes. At the center of the image is a gas mask–covered skull, symbolizing the core construct of population health under threat. The cracked skull and protective mask reflect both biological vulnerability and adaptive responses to toxic, conflict-driven environments. This central positioning aligns with your article's premise that population health is not an isolated outcome but the convergent endpoint of multiple technological warfare inputs.

Figure 1: Technological Warfare Determinants of Population Health

Note: *This conceptual model illustrates how technological warfare domains, including drones and airstrikes, cyber warfare, chemical and biological threats, and autonomous robotics, function as upstream determinants of population health. These inputs influence health outcomes through mediating mechanisms, including mental health impacts and healthcare system disruption. Bidirectional relationships indicate feedback dynamics between mediators. The model culminates in population-level outcomes, including morbidity and mortality.*

Source*: Author-generated using AI image generation tools.*

Radiating outward are four primary technological warfare domains, each representing systemic shock inputs within the TWD–PH framework: 1) Drones & Airstrikes (top-left): Depicted through aerial drones and explosions, this domain captures kinetic warfare mechanisms leading to bombardment, collateral damage, and forced displacement. These elements correspond to direct physical destruction and immediate injury pathways in your model. 2) Cyber Warfare (top-right): Illustrated by a hooded figure operating a computer, this section represents non-kinetic disruption, including cyberattacks, infrastructure failure, and misinformation. This aligns with your framework's emphasis on invisible yet systemic disruptions affecting healthcare delivery and public trust. 3) Chemical & Biological Weapons (bottom-left): Shown through laboratory vials and biohazard symbols, this domain reflects toxicological and epidemiological threats, including environmental contamination and pathogen exposure. This directly corresponds to biological hazard pathways within your model. 4) Autonomous Robotics (bottom-right): Represented by a robotic soldier, this section highlights AI-enabled warfare systems, including lethal autonomous weapons. This reinforces your conceptualization of technological escalation and reduced human oversight as amplifiers of systemic risk.

These four domains are connected to two intermediate disruption pathways, which function as mediating mechanisms in this framework: 1) Mental Health Impacts: Positioned on the lower left, this includes trauma, anxiety, and PTSD. It reflects psychosocial disruption, consistent with your argument that warfare produces long-term, non-visible health burdens. 2) Healthcare Disruption: Positioned on the lower right, this includes destruction of facilities and lack of access to care. This represents system-level breakdown, a key component of health system vulnerability in your model.

A bidirectional arrow between these two mediators suggests feedback loops, reinforcing your TWD–PH assertion that disruptions are nonlinear and mutually reinforcing (e.g., healthcare collapse exacerbates mental health crises, and vice versa). At the bottom, the infographic culminates in "Morbidity & Mortality," which serves as the ultimate outcome variable. This reflects the emergent consequence of cascading failures, consistent with your framework's emphasis on nonlinear propagation and system-wide collapse rather than isolated cause-effect relationships.

The background imagery of a war-torn urban environment, with soldiers, drones, and armored vehicles, contextualizes these processes within real-world conflict ecosystems, reinforcing the ecological validity of your framework. Overall, the image effectively mirrors your article's central thesis: Technological warfare acts as a multi-domain structural determinant of population health, operating through interdependent, cascading pathways that disrupt physical, psychological, environmental, and healthcare systems, ultimately producing complex, emergent health outcomes.

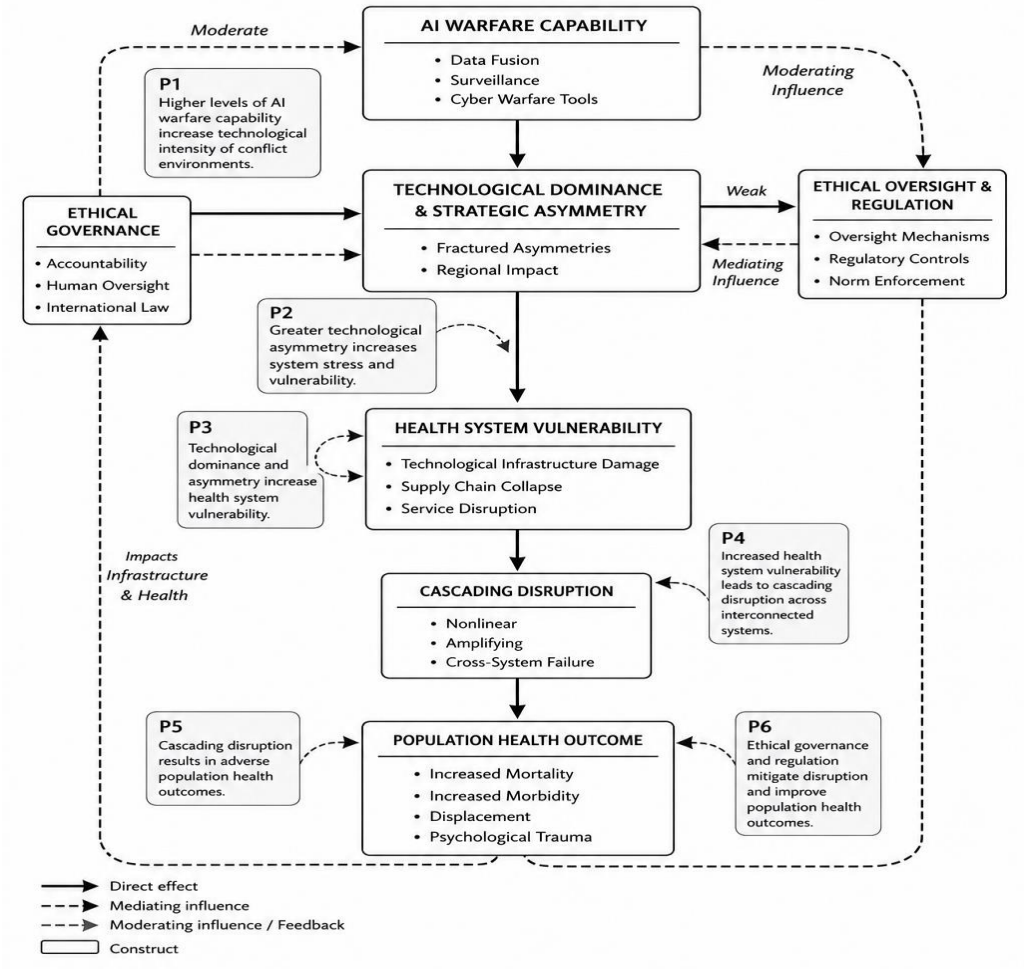
II. CONCEPTUAL FRAMEWORK

The theoretical framework advanced here is the Technological Warfare Disruption–Public Health (TWD–PH). The framework conceptualizes technological warfare as a structural determinant of population health operating through cascading system disruption (Bull, 2026). As illustrated in Figure 2, the model specifies relationships among key constructs through a series of propositions (P1–P6). The TWD–PH) framework is advanced as a novel mid-range explanatory theory that conceptualizes AI-enabled warfare as a structural determinant of population health through cascading system disruption. Grounded in complex adaptive systems theory and the structural determinants of health, the framework shifts the analytical focus from governance-centered perspectives to the underlying mechanisms through which technological warfare destabilizes health systems and produces emergent health outcomes (Peters, 2014; World Health Organization [WHO], 2024). Within this framework, population health outcomes are treated as a unified system-level construct emerging from dynamic interactions among technological, infrastructural, and social systems.

At the foundation of the framework is AI Warfare Capability, conceptualized as an exogenous system shock comprising data fusion, surveillance technologies, and cyber warfare tools. These capabilities extend the operational scope of conflict into civilian, digital, and healthcare domains, increasing exposure of critical infrastructure to disruption. The strategic concern surrounding the proliferation of advanced AI capabilities has been reflected in contemporary policy discourse, where governments have emphasized the risks associated with the diffusion of highly precise and potentially autonomous systems across geopolitical boundaries (Congressional Research Service, 2024). Such concerns underscore that AI warfare capability extends beyond technological advancement to represent a critical driver of systemic disruption. This perspective reinforces Proposition 1 (P1), which posits that increased AI warfare capability intensifies the technological nature of conflict environments and amplifies the scale and scope of disruption.

Figure 2

Technological Warfare Determinants of Population Health (TWD–PH)



Note. P1–P6 denote theoretical propositions in the TWD–PH framework.

Description. The figure presents a systems model explaining how technological characteristics of modern warfare involving artificial intelligence (AI) and cyber capabilities shape population health outcomes. AI warfare capability enhances technological dominance and strategic asymmetry (P1), which increases system stress and health system vulnerability (P2–P3). Heightened vulnerability contributes to cascading disruption across interconnected systems (P4), which produces adverse population health outcomes (P5). Ethical oversight and regulation exert moderating and mediating influences throughout the pathway and can mitigate disruptions, thereby improving population health outcomes (P6).

Source: Conceptual model developed by the author (Bull, 2026).

Contemporary evidence indicates that healthcare systems are increasingly targeted through cyber and hybrid warfare tactics, leading to service interruptions, delayed care, and compromised patient safety (Ewoh, 2024; WHO, 2024). In line with this, P1 posits that higher levels of AI warfare capability increase the technological intensity of conflict environments, thereby amplifying systemic disruption conditions.

AI warfare capability gives rise to Technological Dominance and Strategic Asymmetry, wherein disparities in technological resources and capabilities produce uneven power distributions between conflict actors. These asymmetries result in fractured operational environments and regionally differentiated impacts, where less technologically equipped populations experience disproportionate exposure to harm. This structural imbalance is particularly pronounced in fragile and resource-constrained health systems (UNOCHA, 2024). Accordingly, P2 proposes that greater technological asymmetry increases instability and unequal exposure to risk among affected populations.

These upstream conditions contribute directly to Health System Vulnerability, a central construct within the TWD–PH framework. Health system vulnerability is conceptualized as a dual-layered mediating condition encompassing both immediate infrastructure damage and cumulative system degradation. Healthcare systems are treated as interdependent networks in which infrastructure, workforce capacity, supply chains, and digital systems are tightly coupled. Disruptions to one component propagate across the system, producing compounding effects. Empirical evidence documents increasing

attacks on healthcare infrastructure in conflict settings, including facility destruction, service disruption, and depletion of essential medical resources (Safeguarding Health in Conflict Coalition, 2024; International Committee of the Red Cross [ICRC], 2023). Consistent with this, P3 posits that higher levels of AI warfare capability and technological asymmetry are positively associated with increased health system vulnerability.

The defining contribution of the TWD–PH theory is the introduction of cascading disruption as the central mechanism linking technological warfare to population health outcomes. Cascading disruption refers to the sequential and amplifying failure of interconnected system components, whereby an initial technological shock triggers a chain reaction across healthcare delivery systems and related infrastructures. Research on infrastructure interdependencies demonstrates that disruptions in one sector can propagate across others, amplifying system-wide instability (Rinaldi et al., 2001). Within this framework, cascading disruption operates through both direct and indirect pathways, reinforcing the nonlinear nature of system failure. Accordingly, P4 proposes that greater health system vulnerability amplifies cascading disruptions across interconnected systems.

These cascading disruptions ultimately manifest in Population Health Outcomes, including mortality, disease burden, displacement, and long-term psychological trauma. These outcomes are conceptualized as system-level consequences of accumulated disruption rather than isolated or immediate effects of warfare. Humanitarian data indicate that indirect effects, such as disrupted healthcare access, breakdown of preventive services, and supply shortages, account for a substantial proportion of morbidity and mortality in conflict-affected populations (UNOCHA, 2024; WHO, 2024). In alignment with this perspective, P5 posits that increased cascading disruption is positively associated with adverse population health outcomes.

Importantly, the TWD–PH framework incorporates a recursive feedback dynamic, reflecting the principles of complex adaptive systems. Adverse population health outcomes, including widespread morbidity, displacement, and trauma, place additional strain on already fragile health systems, further weakening infrastructure and service capacity. This creates a self-reinforcing cycle of instability, where system outputs re-enter as inputs. Thus, P6 posits that adverse population health outcomes reinforce health system vulnerability, sustaining and amplifying systemic disruption over time.

Complementing these core relationships, the framework integrates Ethical Governance and Ethical Oversight and Regulation as critical system-level controls. Ethical governance, defined by accountability, human oversight, and adherence to international humanitarian law, functions as a stabilizing force that can mitigate the destructive potential of technological warfare. In contrast, ethical oversight and regulation are conceptualized as comparatively weaker mechanisms, reflecting current limitations in enforcement and global coordination in AI-enabled warfare contexts (ICRC, 2023; WHO, 2024). Ethical governance primarily functions as a moderating influence, while ethical oversight and regulation operate as weaker mediating mechanisms within the pathway. As moderators, they shape the strength of the relationship between AI warfare capability and technological asymmetry (P1–P2). As mediators, they influence how asymmetry translates into health system vulnerability (P3), particularly in contexts where regulatory capacity is limited. These dynamics are consistent with resilience theory, which emphasizes the role of institutional capacity in buffering system shocks and reducing vulnerability (Kruk et al., 2015).

The TWD–PH framework advances a theory-driven, systems-based explanation of how technological warfare shapes population health through cascading disruption mechanisms. By integrating technological inputs, structural asymmetries, system vulnerabilities, and governance controls into a unified model, the theory captures both direct and indirect pathways, as well as nonlinear and recursive dynamics. The propositions (P1–P6) provide a coherent theoretical structure that strengthens explanatory power while establishing a clear foundation for future empirical testing, policy analysis, and intervention design.

III. LITERATURE REVIEW

To support the development of the Technological Warfare Disruption and Public Health (TWD–PH) framework, this study employed a targeted integrative literature approach to synthesize recent scholarship across artificial intelligence (AI)–enabled warfare, cyber conflict, health system vulnerability, and population health outcomes. As Whetten (1989) emphasized, theory-building research prioritizes conceptual relevance and explanatory power over exhaustive coverage. Accordingly, this study focused on identifying literature that explains mechanisms of disruption, rather than merely describing governance or isolated outcomes.

Recent empirical evidence demonstrates that AI-enabled and cyber-mediated warfare increasingly targets healthcare systems as critical infrastructure, thereby introducing new forms of systemic vulnerability. For example, Li (2025) reported that cyberattacks on hospital systems have increased substantially, with disruptions directly affecting clinical operations and emergency response capacity. Similarly, the World Economic Forum (2026) identified healthcare as one of the most targeted sectors globally, noting that cyber incidents increasingly compromise patient safety and continuity of care. These findings support the TWD–PH proposition that AI warfare capability functions as a systemic shock input, destabilizing health systems through both digital and physical pathways.

The literature further indicates that AI-enabled warfare contributes to technological dominance and strategic asymmetry, creating uneven distributions of risk across health systems. According to Trellix (2026), the rapid digitalization of healthcare, through cloud systems, remote access, and AI-driven processes, has expanded the attack surface, making less-resilient systems disproportionately vulnerable. This aligns with broader conflict research suggesting that technologically advanced actors can exploit these asymmetries to disrupt weaker infrastructures, thereby reinforcing systemic inequalities in conflict environments.

A consistent theme across recent studies is the characterization of health systems as complex, interdependent networks. Ewoh (2024) argued that healthcare systems rely on tightly coupled infrastructures, including information systems, supply chains, and clinical operations, making them highly susceptible to cascading failure. Supporting this, Aldosari (2025) found that cyberattacks not only compromise data integrity but also disrupt clinical workflows, delay treatment, and increase risks to patient safety. These findings reinforce the TWD–PH assumption that health system vulnerability emerges from interdependence, rather than isolated component failure.

Recent conflict-based evidence further demonstrates the direct targeting of healthcare infrastructure, reinforcing the role of technological warfare in producing systemic disruption. The World Health Organization (2024) reported over 1,400 verified attacks on healthcare facilities in a single year, resulting in deaths, injuries, and widespread service interruptions. Similarly, the Safeguarding Health in Conflict Coalition (2024) documented persistent attacks on medical personnel and facilities, highlighting the erosion of protections for health systems in conflict zones. These findings demonstrate that technological warfare extends beyond cyber domains into physical infrastructure disruption, further compounding system vulnerability.

The concept of cascading disruption, central to the TWD–PH framework, is increasingly supported by empirical evidence. HIPAA Journal (2026) reported that large-scale cyberattacks on healthcare systems have produced widespread downstream effects, including delays in surgeries, disruptions in pharmacy services, and national-level healthcare instability. These cascading effects illustrate how localized disruptions propagate across interconnected systems, amplifying their impact over time. This aligns with foundational work by Rinaldi et al. (2001), who demonstrated that disruptions in interdependent infrastructures can trigger multi-sector system failures. Within the TWD–PH framework, such cascading processes represent the primary mechanism through which technological warfare translates into large-scale health system degradation.

Finally, the literature consistently highlights the population health consequences of systemic disruption, particularly in conflict settings. The United Nations Office for the Coordination of Humanitarian Affairs (2024) emphasized that disruptions to healthcare systems contribute to increased mortality, disease outbreaks, displacement, and long-term psychological trauma. Similarly, the WHO (2024) highlighted that indirect effects, such as reduced access to preventive services and chronic disease management, often exceed the direct health impacts of conflict. These findings support the TWD–PH proposition that population health outcomes are emergent consequences of accumulated system disruption, rather than direct effects of warfare alone.

IV. METHODOLOGY

This study employed a qualitative, theory-building research design to develop the Technological Warfare Disruption and Public Health (TWD–PH) framework. The design is grounded in principles of conceptual and explanatory theory development, which emphasize construct identification, relationship specification, and mechanism articulation (Whetten, 1989). The primary aim is to explain how AI-enabled warfare produces population health outcomes through cascading system disruption, rather than to test statistical relationships.

Consistent with this objective, the study adopts an integrative qualitative approach, synthesizing interdisciplinary literature to construct a systems-based explanatory model. This approach is appropriate for emerging areas of research where theoretical development precedes empirical testing.

Methodological Approach

The study utilized qualitative document analysis as the primary methodological approach. As Bowen (2009) explained, document analysis provides a systematic procedure for reviewing and interpreting textual data to identify patterns, themes, and meanings. This method is particularly suitable for policy-oriented and interdisciplinary research, where insights must be derived from diverse sources.

In addition, the study draws on thematic analysis principles to organize and interpret findings. Tracy (2020) emphasized that qualitative analysis involves identifying recurring patterns and organizing them into meaningful categories that support theoretical interpretation. This approach enabled the identification of system interactions, disruption pathways, and emergent mechanisms central to the TWD–PH framework.

Data Sources and Search Strategy

Data were derived from a targeted set of scholarly and institutional documents, including peer-reviewed journal articles and reports from organizations such as the World Health Organization, International Committee of the Red Cross, and United Nations Office for the Coordination of Humanitarian Affairs. These sources were selected to capture both empirical evidence and policy-relevant insights on AI-enabled warfare, cyber disruption, and health system impacts.

The literature search focused on publications between 2015 and 2026, with particular emphasis on recent studies (2023–2026) to ensure relevance to rapidly evolving technological threats. A structured Boolean search strategy was employed using keywords aligned with the core constructs of the TWD–PH framework, including *AI warfare, cyber warfare, health system vulnerability, infrastructure disruption, and population health outcomes.*

Inclusion and Exclusion Criteria

Inclusion criteria were established to ensure alignment with the study's theoretical focus. Documents were included if they: (a) examined AI-enabled warfare or cyber conflict, (b) addressed health system vulnerability or infrastructure disruption, (c) linked technological disruption to health or population outcomes, and (d) were published in English. Documents were excluded if they lacked empirical or theoretical grounding, were purely opinion-based, or were not relevant to health systems or conflict contexts.

Analytical Procedure

The analysis followed a three-stage qualitative coding process. First, open coding was used to identify recurring themes related to technological disruption, system vulnerability, and health outcomes. This initial stage allowed for the emergence of patterns across diverse sources.

Second, axial coding was applied to organize these themes into higher-order categories corresponding to the core constructs of the TWD–PH framework. As Tracy (2020) noted, axial coding enables the identification of relationships among categories, facilitating the development of conceptual structure.

Third, a comparative gap analysis was conducted to examine inconsistencies between existing literature and observed patterns of disruption in conflict settings. As O'Cathain et al. (2020) emphasized, comparative analysis strengthens qualitative rigor by identifying gaps and underlying mechanisms. This process led to the identification of cascading disruption as the central explanatory mechanism within the TWD–PH framework.

Model Development

Insights from the coding and synthesis process were integrated to develop the TWD–PH conceptual model, which specifies relationships among key constructs, including AI warfare capability, technological asymmetry, health system vulnerability, cascading disruption, and population health outcomes. The model reflects principles of complex adaptive systems, emphasizing interdependence, nonlinearity, and feedback dynamics.

Data Collection and Coding Procedures

Selected documents were systematically organized and analyzed using a structured coding protocol. As Bowen (2009) explained, document analysis provides a systematic procedure for reviewing and evaluating documents to extract meaningful themes and patterns. Consistent with this approach, data extraction in the present study focused on identifying policy language and thematic content related to governance mechanisms, ethical principles, regulatory provisions, and public health considerations. Key elements examined included accountability, human oversight, civilian protection,

infrastructure safeguards, and AI-specific regulatory measures, which are commonly emphasized in policy and governance analyses.

The analysis followed a three-stage coding process grounded in established qualitative methodologies. First, open coding was used to identify recurring themes related to governance and public health. Second, axial coding, as described by Tracy (2020), was applied to organize these themes into higher-order categories, including accountability structures, oversight mechanisms, technological regulation, and health system protections. Third, a gap analysis was conducted to compare existing governance frameworks with identified public health risks, allowing for the identification of areas of insufficiency and misalignment. Furthermore, O'Cathain et al. (2020) emphasized the importance of integrating and comparing data sources to strengthen analytical rigor, which informed the comparative aspect of this study. Collectively, this multi-stage analytical approach reflects established qualitative and policy analysis practices that prioritize systematic coding, thematic synthesis, and evaluative comparison.

Analytical Framework

The analytical framework is grounded in a systems-based qualitative approach, integrating complex adaptive systems principles to examine how AI-enabled warfare generates cascading disruptions across health systems. Consistent with theory-building methodologies, the analysis prioritized mechanism identification and relational pathways rather than quantification (Whetten, 1989).

AI warfare capability was conceptualized as an exogenous shock producing technological asymmetry, which increases health system vulnerability and enables cascading disruption, the sequential failure of interdependent system components. Findings were organized into thematic domains aligned with the TWD–PH constructs, allowing for identification of patterns, system interactions, and feedback dynamics consistent with systems thinking (Peters, 2014).

To ensure methodological rigor, the study adhered to established qualitative research standards, including credibility, dependability, confirmability, and transparency (Bowen, 2009; Tracy, 2020). Credibility was achieved through triangulation of multiple data sources, including peer-reviewed and institutional documents. Dependability was supported by a systematic and structured analytical process, incorporating open and axial coding procedures. Confirmability was maintained by grounding interpretations in recurring patterns across the literature rather than researcher bias. Transparency was ensured through clear documentation of the search strategy, data selection, and analytical procedures. Collectively, these strategies align with best practices in qualitative research and document analysis.

Although no human subjects were involved, the study adhered to principles of academic integrity, objectivity, and responsible scholarship. Sources were selected based on relevance and credibility, and findings were presented with sensitivity to conflict-affected populations. The study also recognizes its ethical responsibility to contribute knowledge that supports the protection of health systems and mitigates harm in technologically mediated conflict environments.

V. SYNTHESIS OF FINDINGS & RESULTS

The synthesis of findings across recent literature provides strong empirical support for the Technological Warfare Disruption and Public Health (TWD–PH) framework, demonstrating that AI-enabled and cyber-mediated warfare functions as a systemic shock that propagates through interdependent health systems, producing cascading disruption and adverse population health outcomes. Across sources, a consistent pattern emerges linking technological warfare capability → system vulnerability → cascading disruption → population health impact, reinforcing the framework's mechanistic logic.

First, the literature confirms that healthcare systems have become primary targets of technologically mediated conflict, particularly through cyber operations. The World Health Organization (WHO, 2024) reported that healthcare is among the most frequently targeted critical sectors, with cyber incidents capable of delaying treatment and compromising patient safety. Similarly, industry-wide analyses indicate that a substantial proportion of healthcare organizations experience cyberattacks annually, many of which directly disrupt care delivery (HIPAA Journal, 2026). These findings substantiate the TWD–PH proposition that AI warfare capability operates as an exogenous system shock, extending conflict into digital infrastructures essential to health systems.

Second, the evidence demonstrates that technological warfare generates persistent and systemic vulnerability across health systems. Reports indicate that healthcare data breaches and cyber incidents affect millions of individuals annually, disrupting operational continuity and exposing structural weaknesses in healthcare infrastructure (HIPAA Journal, 2026).

This growing exposure reflects the increasing interdependence of digital health systems, supporting the TWD–PH argument that vulnerability is structural rather than episodic.

Third, the literature provides strong evidence for technological asymmetry and uneven system resilience. Cybersecurity analyses show that healthcare organizations often struggle to remediate vulnerabilities in a timely manner, leaving critical systems exposed to exploitation (American Hospital Association [AHA], 2025). At the same time, the sophistication of cyber threats continues to evolve, enabling more advanced actors to exploit weaker systems more effectively (World Economic Forum [WEF], 2026). These findings support the TWD–PH assertion that technological dominance produces disproportionate disruption capacity, particularly in resource-constrained or highly networked environments.

Fourth, the most critical finding supporting the TWD–PH framework is the clear evidence of cascading disruption across health systems. Real-world incidents demonstrate that localized cyberattacks can trigger system-wide failures, affecting multiple components of healthcare delivery. For example, the 2024 Change Healthcare cyberattack disrupted pharmacy services, insurance processing, and provider operations across the United States, significantly limiting patient access to care (AHA, 2025). Similarly, ransomware attacks have been shown to delay surgeries and interrupt clinical workflows, illustrating how disruptions propagate across interconnected systems (HIPAA Journal, 2026). These findings align with research on infrastructure interdependencies, which shows that failures in one domain can trigger cascading effects across others (Rinaldi et al., 2001).

Fifth, the literature highlights that population health outcomes are largely indirect and system-mediated, rather than direct consequences of conflict alone. Disruptions to healthcare delivery, such as delays in treatment, reduced access to medications, and interruptions in preventive services, contribute to increased morbidity and mortality (WHO, 2024; United Nations Office for the Coordination of Humanitarian Affairs [UNOCHA], 2024). These findings reinforce the TWD–PH framework's central claim that health outcomes emerge from accumulated system disruption, rather than isolated events.

Finally, the synthesis reveals the presence of feedback loops that amplify system instability over time. Repeated cyber incidents, unresolved vulnerabilities, and infrastructure dependencies contribute to cumulative system degradation, reducing resilience and increasing susceptibility to future disruptions (WEF, 2026). The increasing frequency and scale of cyberattacks suggest that health systems are entering a state of chronic vulnerability, where disruption becomes systemic rather than exceptional.

Overall, the evidence converges on a systems-based, mechanistic explanation of how AI-enabled warfare shapes population health. The literature consistently demonstrates that AI and cyber warfare function as systemic shock inputs, disrupting critical infrastructures that underpin healthcare delivery. These disruptions expose the structural vulnerability of health systems, which arises from their interdependence across digital networks, supply chains, and clinical operations.

The findings show that disruptions do not occur in isolation but propagate through cascading, nonlinear pathways, whereby failures in one component trigger subsequent failures across the system. As a result, population health outcomes, including increased morbidity, mortality, and reduced access to care, emerge not as direct effects of conflict alone, but as system-level consequences of accumulated disruption.

Furthermore, the presence of feedback loops reinforces these dynamics, creating self-amplifying cycles of instability that further degrade system resilience over time. Together, this synthesis provides strong empirical grounding for the TWD–PH framework and confirms that cascading disruption is the central mechanism linking technological warfare to population health outcomes.

VI. DISCUSSION

The findings provide compelling support for the Technological Warfare Disruption and Public Health (TWD–PH) framework, advancing a systems-based, mechanistic explanation of how AI-enabled warfare shapes population health. Across literature, technological warfare, particularly cyber-enabled operations, emerges as an exogenous system shock that extends conflict into civilian and digital infrastructures, fundamentally altering the pathways through which harm is produced. This reframes conflict-related health impacts from being primarily direct and kinetic to indirect, systemic, and technologically mediated, thereby expanding the scope of public health analysis in modern warfare contexts.

A central insight of this study is that health system vulnerability is structural and emergent, arising from the interdependence of critical components such as digital infrastructure, supply chains, workforce capacity, and service delivery systems. Consistent with systems theory, these tightly coupled systems are highly susceptible to disruption, as failures in one domain

rapidly propagate across others. Within this context, the study validates cascading disruption as the core explanatory mechanism, demonstrating that localized technological shocks, such as cyberattacks or infrastructure damage trigger sequential and compounding failures that degrade system functionality at scale. These cascading processes produce outcomes that exceed the magnitude of the initial disruption, reinforcing the need to shift analytical focus from isolated events to dynamic processes of system failure.

Importantly, the findings show that population health outcomes are predominantly indirect and system-mediated, emerging from sustained disruption rather than immediate exposure to conflict. Increased morbidity, mortality, and reduced access to care are driven by breakdowns in healthcare delivery systems, including delayed treatments, supply chain interruptions, and diminished service capacity. These outcomes are further intensified by feedback loops, where repeated disruptions and unresolved vulnerabilities create self-reinforcing cycles of instability. As health systems become increasingly digitized, these dynamics contribute to conditions of chronic vulnerability, in which disruption is no longer episodic but persistent.

While governance and regulatory frameworks remain relevant, the findings indicate that their role is primarily moderating rather than determinative. Existing governance mechanisms often lack the capacity to fully prevent or mitigate cascading disruption, particularly given the speed, scale, and complexity of AI-enabled threats. This underscores a critical theoretical and practical shift: protecting population health in technologically mediated conflict requires not only governance, but system resilience.

Policy Recommendations

Drawing on the TWD–PH framework, several policy implications emerge for strengthening health system resilience in the context of technological warfare. The growing concern among policymakers regarding the international spread of advanced AI capabilities further underscores the urgency of strengthening governance frameworks. Without coordinated regulatory mechanisms, the diffusion of highly precise and autonomous systems may exacerbate technological asymmetries and intensify cascading disruptions, particularly in vulnerable health systems. These dynamics highlight the need for global governance structures capable of mitigating the public health risks associated with AI-enabled warfare.

First, policymakers should prioritize health system resilience as a core national security objective, recognizing healthcare infrastructure as critical to societal stability. This includes integrating health system protection into cybersecurity and defense strategies, with particular emphasis on safeguarding digital health infrastructure.

Second, there is a need to develop and implement cyber resilience frameworks tailored to healthcare systems. These frameworks should include proactive threat detection, redundancy mechanisms, rapid response protocols, and recovery planning to minimize cascading disruption. Investment in cybersecurity infrastructure and workforce capacity is essential to reduce system vulnerability.

Third, health systems should adopt redundancy and decentralization strategies to mitigate the effects of disruption. Diversifying supply chains, decentralizing critical services, and establishing backup systems can reduce dependence on single points of failure and limit the propagation of disruption across the system.

Fourth, international organizations and policymakers should strengthen global coordination and accountability mechanisms to protect healthcare systems in conflict settings. While governance alone is insufficient, coordinated efforts can enhance information sharing, establish norms for the protection of health infrastructure, and support capacity-building in vulnerable regions.

Finally, there is a need to incorporate systems-based risk assessment into health policy and planning, recognizing that disruptions are interconnected and nonlinear. This requires moving beyond traditional risk models toward approaches that account for interdependencies, feedback loops, and cascading effects. This study advances a novel, systems-based theoretical framework that reconceptualizes AI-enabled warfare as a driver of population health outcomes through cascading disruption. By identifying technological warfare as a systemic shock, health system vulnerability as a structural condition, and cascading disruption as the central mechanism, the TWD–PH framework provides a comprehensive explanation of how modern conflict produces complex and amplified health impacts.

The findings highlight a critical shift in understanding: the most significant health consequences of technological warfare are not immediate but emerge through the breakdown of interconnected systems over time. This underscores the importance of moving beyond event-based and governance-centered approaches toward resilience-oriented, systems-level strategies.

Ultimately, the TWD–PH framework offers both theoretical and practical contributions. It provides a foundation for future research examining system dynamics in conflict environments and offers actionable insights for policymakers seeking to protect health systems in an era of rapidly evolving technological threats. As warfare continues to transform, so too, the frameworks used to understand and mitigate its impact on population health.

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] Aldosari, B. (2025). Cybersecurity in healthcare: Emerging threats to patient safety. *Journal of Medical Systems.* Advance online publication.

[2] Benatar, S. R., Gill, S., & Bakker, I. (2011). Global health and the global economic crisis. *American Journal of Public Health, 101*(4), 646–653.

[3] Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

[4] Bull, D. (2026). *Technological warfare disruption–public health (TWD–PH): A systems-based explanatory theory.* Manuscript in preparation.

[5] Congressional Research Service. (2024). *Artificial intelligence and national security: Policy considerations.* U.S. Congress.

[6] Dennis, C. R. (2025). Cybersecurity incidents and healthcare disruption: Implications for patient safety. *Journal of Medical Systems.* Advance online publication.

[7] Ewoh, P. (2024). Vulnerability to cyberattacks and sociotechnical solutions in health care systems: A systematic review. *Journal of Medical Internet Research, 26*(1), e46904. https://doi.org/10.2196/46904

[8] 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.

[9] Guha-Sapir, D., & D'Aoust, O. (2011). Demographic and health consequences of civil conflict. In *World development report background papers.* World Bank.

[10] Health and Human Services Office for Civil Rights. (2024). *Healthcare data breach statistics and cyber incidents report.* U.S. Department of Health and Human Services.

[11] HIPAA Journal. (2026). *Healthcare data breach statistics and trends.*

[12] Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts.* Ashgate.

[13] International Committee of the Red Cross. (2023). *Health care in danger report.*

[14] Kello, L. (2017). *The virtual weapon and international order.* Yale University Press.

[15] Kruk, M. E., Myers, M., Varpilah, S. T., & Dahn, B. T. (2015). What is a resilient health system? Lessons from Ebola. *The Lancet, 385*(9980), 1910–1912.

[16] Li, S. (2025). Cyber-attacks on hospital systems: A narrative review. *Journal of Healthcare Security and Infrastructure.* Advance online publication.

[17] Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847

[18] O'Cathain, A., Murphy, E., & Nicholl, J. (2010). Three techniques for integrating data in mixed methods studies. *BMJ, 341*, c4587. https://doi.org/10.1136/bmj.c4587

[19] Peters, D. H. (2014). The application of systems thinking in health: Why use systems thinking? *Health Research Policy and Systems, 12*, 51. https://doi.org/10.1186/1478-4505-12-51

[20] Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

[21] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

[22] Safeguarding Health in Conflict Coalition. (2024). *Epidemic of violence report.*

[23] Safeguarding Health in Conflict Coalition. (2025). *Attacks on healthcare in conflict zones: Annual report.*

[24] Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world.* McGraw-Hill.

[25] Tracy, S. J. (2020). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (2nd ed.). Wiley.

[26] Trellix. (2026). *Healthcare cybersecurity threat intelligence report.*

[27] U.S. Department of Defense. (2023). *Data, analytics, and artificial intelligence adoption strategy.*

[28] United Nations Office for the Coordination of Humanitarian Affairs. (2024). *Global humanitarian overview.*

[29] World Economic Forum. (2026). *Cyber resilience in healthcare systems.*

[30] World Health Organization. (2024). *Cyber-attacks on critical health infrastructure.* https://www.who.int