International Journal of Paramedicine

Published by the National EMS Management Association (USA)

EDITORIALS

WHEN HEALTHCARE BECOMES A TARGET: THE IMPACT OF HYBRID WARFARE ON PREHOSPITAL EMERGENCY CARE

Fredrik Granholm, MD*[1,2]; Stephen O´Neill, GDip EMS AP, MSc IC, DipATACC RCS[3]

Author Affiliations: 1. Blizard Institute, Queen Mary University of London, London, UK; 2. Department of Anaesthesia, Sundsvall Regional Hospital, Sundsvall, Sweden; 3. National Ambulance Service, Ireland.

Recommended Citation: Granholm, F., & O'Neill, S. (2026). When healthcare becomes a target: The impact of hybrid warfare on prehospital emergency care. *International Journal of Paramedicine*. (15). 10-15. https://doi.org/10.56068/BTEC9235

Keywords: hybrid warfare, prehospital, cybercrime, resilience, emergency medicine, emergency medical services, EMS, paramedicine

Disclosures: The authors have no conflicts of interest and nothing to disclose.

Funding: External funding was not used to support this work.

Received: March 2, 2026
Revised: April 24, 2026
Accepted: May 4, 2026
Published: July 15, 2026

**Corresponding Author:* fredrik.granholm@rvn.se

ABSTRACT

Hybrid warfare increasingly targets civilian healthcare infrastructure through cyber operations, infrastructure sabotage, disinformation, and energy disruption. Paramedics operate at the frontline of these system-level threats, positioned at the intersection of emergency healthcare delivery, public safety, and societal resilience. This editorial examines how hybrid warfare directly and indirectly affects paramedic practice and prehospital emergency care systems.

Drawing on recent international examples, the paper highlights how secondary system failures, including disrupted communications, loss of digital documentation, impaired rostering, supply chain interruption, and reduced hospital throughput, fundamentally alter paramedic decision-making and operational safety in the field. Growing dependence on integrated digital platforms, combined with reduced analogue redundancy and a workforce trained primarily in technology-enabled environments, increases vulnerability during prolonged disruption.

The editorial argues that recognizing hybrid warfare as a core concern for paramedicine is essential for patient safety, professional preparedness, and resilient prehospital emergency care systems.

INTRODUCTION

Paramedics operate at the intersection of healthcare delivery, public safety, and societal resilience (Williams et al., 2021). In an era increasingly shaped by hybrid warfare, this intersection has become both exposed and vulnerable. Hybrid warfare is commonly understood as the coordinated use of conventional and unconventional means, including cyber operations, infrastructure sabotage, terrorism, disinformation, and criminal activity, designed to exploit societal vulnerabilities while remaining below the threshold of declared armed conflict (Hoffman, 2009). These threats are no longer theoretical. They directly affect prehospital emergency care systems and the ability of paramedics to deliver safe, timely, and effective care, with parallel consequences for hospital emergency medicine systems and overall health system resilience (Granholm et al., 2022).

Although the vulnerability of healthcare systems to cyber and infrastructure disruption is increasingly recognized, the operational implications for prehospital emergency care remain less clearly described. Much of the existing literature focuses on hospital-based systems, while the effects on prehospital decision-making, workflow adaptation, and patient safety have received comparatively limited attention.

HYBRID WARFARE AND HEALTHCARE SYSTEMS

Attacks of this nature have the potential to cripple entire emergency medical and health service systems, with cascading effects across the full spectrum of care, from frontline emergency response to patients receiving ongoing, chronic, or elective treatment. Importantly, hybrid attacks do not require the complete collapse of emergency medical services to cause harm. Even when dispatch centers, ambulance response, or radio systems remain partially functional, secondary system failures may significantly impair service delivery (Goebel et al., 2019). Rostering systems, digital communications, supply chains, patient records, and hospital throughput can all be disrupted, creating a broad operational footprint that directly affects paramedic decision-making in the field. These disruptions may also result in delayed response times, reduced situational awareness, and increased cognitive workload for clinicians operating in dynamic and uncertain environments.

Civilian healthcare systems have already been targeted within the framework of hybrid warfare. A prominent example is the attempted cyberattack on Boston Children's Hospital in the United States, attributed by U.S. authorities to state-sponsored actors (Raymond, 2022). Although the attack was disrupted before direct patient harm occurred, it demonstrated that healthcare institutions are considered legitimate targets in modern hybrid conflict.

The WannaCry ransomware attack in 2017 provides a concrete illustration of how cyber operations can disrupt emergency medical systems at scale (Smart, 2018). The attack caused widespread digital system failures across the United Kingdom's National Health Service, forcing hospitals to revert to manual workflows, cancel services, and divert emergency ambulances. For paramedics, this translated into longer transport times, uncertainty regarding hospital capacity, disrupted handovers, and altered destination decisions, all occurring under conditions of increased cognitive and operational stress (National Audit Office, 2017; Moore et al., 2023). Subsequent analyses of the incident highlighted the importance of system redundancy, fallback communication pathways, and the ability to maintain safe clinical practice in the absence of digital support systems (Smart, 2018; National Audit Office, 2017). These indirect effects on prehospital care are rarely captured in traditional outcome measures but represent a significant patient safety risk.

More recent events demonstrate that the impact of cyberattacks on healthcare extends well beyond the immediate loss of clinical systems. The large-scale cyberattack against the Irish Health Service Executive in 2021 resulted in extensive secondary disruption across the health system. Although emergency dispatch and ambulance response technology were not directly disabled, national healthcare email systems were shut down, staff rostering and crewing updates became unavailable, and supply chains for medical equipment were interrupted. Clinicians were forced to rely on telephone communica-

tion and paper-based processes, patient records could not be accessed, and outpatient appointments and elective surgical procedures were cancelled (Moore et al., 2023). The consequences of the attack were prolonged, with operational and clinical effects persisting long after the initial incident. This illustrates how hybrid threats can produce widespread degradation of healthcare delivery even when frontline emergency response appears superficially intact. Similar patterns have been observed in more recent cyber incidents affecting healthcare infrastructure, reinforcing concerns that increasing digital dependence may outpace the development of system resilience. Hybrid threats may originate from both state and non-state actors (Hoffman, 2009). State actors may employ coordinated cyber operations and infrastructure disruption as part of broader strategic objectives, while non-state actors, including criminal networks, may contribute through ransomware or targeted attacks. This convergence complicates attribution and increases the unpredictability of healthcare system disruption.

IMPLICATIONS FOR PREHOSPITAL EMERGENCY CARE

From a paramedic perspective, digital system failures fundamentally alter prehospital practice. Modern ambulance services are increasingly dependent on integrated technological platforms, including mobile data terminal dispatch systems, digital radio networks, satellite navigation and vehicle tracking, electronic patient care reporting, telemetry transmission of electrocardiograms, and real-time communication with receiving facilities. The loss or degradation of these systems increases the risk of error, delay, and cognitive overload, even when immediate mortality effects are not easily measurable (Kahl et al., 2026). These operational consequences remain underexplored in paramedic-focused research. Disruption or manipulation of dispatch systems, including false or spoofed emergency calls, may also lead to misallocation of resources and further strain on emergency response capacity (Goebel et al., 2019). These risks are summarized in Table 1.

Domain	Threat	Operational Consequence	Impact on Prehospital Care	Mitigation
Digital systems	System failure	Loss of patient data	Increased uncertainty in clinical decision-making	Paper documentation, offline systems
Dispatch	False or spoofed calls	Resource misallocation	Delayed Response	Call verification protocols
Energy	Power outage	Equipment failure	Increased demand	Backup power planning
Transport	GPS disruption	Navigation errors	Prolonged transport	Paper maps

Table 1. Hybrid threats and implications for prehospital emergency care.

A critical but often overlooked vulnerability lies in the erosion of system redundancy. Historically, transitions to new technologies were accompanied by the retention of legacy systems as operational backups. Over time, many of these redundancies have been reduced or removed in pursuit of efficiency, potentially limiting system resilience when digital infrastructure is disrupted. This vulnerability is further compounded by workforce demographics. A growing proportion of the paramedic workforce has trained and practiced exclusively within technology-enabled environments, with limited exposure to analogue navigation, paper-based documentation, or non-digital communication systems. In the context of large-scale or prolonged cyber incidents, this skills gap may significantly impair system adaptability and patient safety.

Hybrid warfare also encompasses attacks on critical energy infrastructure, where large-scale power outages can rapidly cascade into healthcare emergencies (Granholm et al., 2023a). These events may occur in combination with cyber or communication disruptions, further compounding their impact. Paramedics are often the first healthcare professionals to encounter the downstream consequences, including patients dependent on electrically powered home medical devices, failure of oxygen concentrators and ventilators, compromised communication networks, and surges in emergency call volume during prolonged outages. When cyber disruption, power loss, and physical threats occur simultaneously, a defining feature of hybrid warfare, the strain on prehospital emergency care is magnified.

These threats affect paramedic practice across its expanding subspecialties. Community paramedics, who increasingly care for medically fragile patients in homes and long-term care settings, are particularly exposed during cyber incidents and energy disruptions. Loss of power or monitoring systems in the home environment may result in rapid patient deterioration, increasing demand for emergency response services. Loss of power, digital documentation, or remote monitoring systems may directly compromise patients dependent on home ventilators, infusion pumps, or oxygen therapy, placing paramedics in ethically complex situations where clinical decision-making intersects with social vulnerability and infrastructure failure.

Critical care paramedics face a different but equally significant vulnerability. Their practice relies heavily on advanced monitoring, infusion technologies, ventilatory support, and seamless coordination with receiving facilities (Granholm et al., 2023b). Cyberattacks, communication outages, or hospital system failures can disrupt transport decision-making, interfacility coordination, and real-time clinical oversight, increasing risk during high-acuity transfers. In hybrid warfare scenarios, where redundancy cannot be assumed, critical care paramedics must be prepared to deliver advanced life support under conditions of technological degradation and prolonged system uncertainty. These system-level impacts across different prehospital care contexts are summarized in Table 2.

System level	Vulnerability	Consequence	Effect on EMS
Community care	Device dependency	Patient deterioration	Increased EMS demand
Hospital interface	Capacity uncertainty	Delayed handover	Extended transport
Workforce systems	Rostering disruption	Staffing issues	Reduced capacity
Infrastructure	Power/communication loss	System degradation	Reduced resilience

Table 2. System-level vulnerabilities and downstream effects.

PREPAREDNESS AND SYSTEM RESILIENCE

Despite these realities, education and research addressing hybrid warfare, cyber threats, and infrastructure vulnerability remain largely absent from paramedic education and continuing professional development (Labrague et al., 2018). Training rarely includes structured preparation for operating under prolonged system degradation or in the absence of digital support, despite the likelihood that such conditions may occur. Paramedics are routinely trained for trauma, major incidents, and disaster response, yet rarely for intentional, sustained, and system-level attacks on healthcare infrastructure itself

(Alqahtani et al., 2025). Training programs seldom include structured preparation for operating without digital dispatch, electronic documentation, navigation systems, or networked communications, despite the likelihood that such capabilities may be degraded or unavailable during hybrid attacks. Addressing these vulnerabilities requires coordinated efforts across multiple levels of the healthcare system. At an operational level, this includes preparing clinicians to function in low-technology environments and under conditions of degraded communication. At a system level, maintaining redundancy, strengthening cybersecurity, and developing contingency plans for infrastructure failure are essential. At an organizational level, regional coordination and shared planning may improve overall system resilience.

Further research informed by prehospital and emergency medical services expertise is needed to examine how hybrid threats affect workflows, patient outcomes, ethical decision-making, and workforce well-being. Equally important is the integration of this knowledge into education and simulation-based training, with an emphasis on low-technology care, degraded communications, prolonged system failure, and interagency collaboration (Kahl et al., 2026).

Preparing prehospital emergency care systems for hybrid warfare is not an abstract geopolitical concern; it is a patient safety imperative. As emergency medical services become increasingly dependent on digital systems, energy infrastructure, and networked coordination, their vulnerability grows. Paramedics must be equipped not only to respond to clinical emergencies, but also to function effectively when the systems that underpin modern emergency care fail. Recognizing hybrid warfare as a core concern for paramedic practice is a necessary step toward resilient, safe, and sustainable prehospital emergency care.

REFERENCES

Alqahtani, M. A., Sav, A., & Toloo, G. S. (2025). Disaster management education and training for paramedics: A scoping review. *Disaster Medicine and Public Health Preparedness, 19*, e207. https://doi.org/10.1017/dmp.2025.10137

Goebel, M., Dameff, C., & Tully, J. (2019). Hacking 9-1-1: Infrastructure vulnerabilities and attack vectors. *Journal of Medical Internet Research, 21*(7), e14383. https://doi.org/10.2196/14383

Granholm, F., Tin, D., & Ciottone, G. R. (2022). Not war, not terrorism, the impact of hybrid warfare on emergency medicine. *The American Journal of Emergency Medicine, 62*, 96–100. https://doi.org/10.1016/j.ajem.2022.10.021

Granholm, F., Tin, D., & Ciottone, G. R. (2023). Critical energy infrastructure and health: How loss of power may kill. *Prehospital and Disaster Medicine, 38*(2), 279–280. https://doi.org/10.1017/S1049023X23000274

Granholm, F., Tin, D., Doyle, L., & Ciottone, G. (2023). A gray future: The role of the anesthesiologist in hybrid warfare. *Anesthesiology, 139*(5), 563–567. https://doi.org/10.1097/ALN.0000000000004706

Hoffman, F. G. (2009). Hybrid warfare and challenges. *Joint Force Quarterly, 52*, 34–39. https://apps.dtic.mil/sti/pdfs/ADA516871.pdf

Kahl, N. M., Frieden, M. J., Killeen, J. P., Chan, T. C., Longhurst, C. A., Tully, J. L., & Dameff, C. J. (2026). Cybersecurity and emergency medicine: A literary review. *The Journal of Emergency Medicine, 86*, 52–65. https://doi.org/10.1016/j.jemermed.2026.04.004

Labrague, L. J., Hammad, K., Gloe, D. S., McEnroe-Petitte, D. M., Fronda, D. C., Obeidat, A. A., Leocadio, M. C., Cayaban, A. R., & Mirafuentes, E. C. (2018). Disaster preparedness among nurses: A systematic review of literature. *International nursing review, 65*(1), 41–53. https://doi.org/10.1111/inr.12369

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. *BMC health services research, 23*(1), 1112. https://doi.org/10.1186/s12913-023-10076-8

National Audit Office. (2017). *Investigation: WannaCry cyber attack and the NHS* (HC 414, Session 2017–2019). https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Raymond, N. (2022, June 1). *Iranian-backed hackers targeted Boston Children's Hospital, FBI chief says.* Reuters. https://www.reuters.com/world/us/iranian-backedhackers-targeted-boston-childrens-hospital-fbi-chief-says-2022-06-01

Smart, W. (2018). *Lessons learned review of the WannaCry ransomware cyber attack*. Department of Health and Social Care. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Williams, B., Beovich, B., & Olaussen, A. (2021). The definition of paramedicine: An international Delphi study. *Journal of Multidisciplinary Healthcare, 14*, 3561–3570. https://doi.org/10.2147/JMDH.S347811