An Interdisciplinary Examination of Cybersecurity Risks Facing Military Telemedicine in Combat Environments

Sean M. Shreve

Old Dominion University

IDS 300W

Dr. Kat LaFever

December 03, 2025

Introduction

The rapid expansion of telemedicine has transformed healthcare delivery across civilian and military contexts. In recent years, military operations have increasingly relied on telemedicine to support deployed medics, extend specialist reach, and reduce morbidity and mortality in combat environments (Madsen et al., 2023, p. 17). However, these systems introduce significant cybersecurity risks that threaten the confidentiality, integrity, and availability of sensitive medical and operational information. Cyber attacks aimed at military telemedicine platforms can compromise clinical decisions, disrupt medical evacuations, or reveal troop readiness (Kim et al., 2020, pp. 3–4). Because these platforms operate in contested and resource-limited environments, cybersecurity failures pose direct operational and clinical consequences.

For this paper, military telemedicine systems are defined as network enabled technologies that allow healthcare personnel to diagnose, consult, monitor, or treat service members remotely, including video consultations, remote triage, digital imaging transfer, and wearable sensors (Madsen et al., 2023, p. 17). Cybersecurity challenges refer to threats and vulnerabilities that may compromise data confidentiality, integrity, authentication, or system availability (Kim et al., 2020, pp. 3–4). From a Health Science perspective, protected health information (PHI) must remain private, secure, and accurate for safe care delivery, and telehealth introduces risks related to data security and confidentiality (Houser et al., 2023, p. 1). These definitions frame the interdisciplinary analysis across Computer Science, Health Science, and Military Medicine to answer the research question: What are the major cybersecurity challenges to protect military telemedicine systems used in combat zones?

Computer Science

Computer Science provides the technical foundation for understanding cybersecurity risks within military telemedicine systems. Research in this discipline shows that interconnected medical devices, sensors, software platforms, and networks expand the attack surface for adversaries. Kim et al. (2020, pp. 3–5) identify seven major vulnerability areas within telemedicine system architecture, including patient devices, telemedicine hardware, local networks, gateway devices, the public Internet, the system back end, and data storage. Each layer introduces unique weaknesses. For example, patient or field medic devices often lack enterprise level hardening and are highly susceptible to device loss, weak passwords, or malicious applications. Gateway devices that connect tactical networks to broader telemedicine systems are also attractive targets for attacks if not properly secured.

Kim et al. (2020, pp. 3–4) further emphasize that telemedicine frequently relies on public networks during data transmission, a critical issue in combat zones where adversaries monitor and intercept communication channels. Data traveling over unsecured paths may be captured, altered, or blocked. Garg and Brewer (2011, pp. 768–771) add that many telemedicine architectures suffer from outdated encryption standards, weak authentication protocols, and legacy software that fails to address modern cybersecurity threats. Their systematic review found that insufficient reporting, outdated security standards, and poor key management practices remain common across telemedicine platforms.

These vulnerabilities become more severe in combat environments. An oppositional force could manipulate or delay medical data, leading to clinical errors, or analyze telemedicine traffic patterns to acquire tactical intel that could assist in operational strategy. Strong encryption, updated authentication mechanisms, hardened devices, and continuous network monitoring help

prevent military telemedicine systems becoming highly exposed. From the Computer Science perspective, preventing these sophisticated cyber-attacks is paramount. This discipline makes it clear that the security of telemedicine is only as strong as the technical architecture supporting it.

Health Science

Health Science focuses on patient care quality, privacy, safety, and regulatory compliance. From a cybersecurity perspective, concerns relate to protecting protected health information (PHI), safeguarding patient identities, and ensuring the accuracy of clinical data used in treatment. Specific vulnerabilities exist within the telemedicine system because it extends care beyond controlled clinical environments into virtual spaces that rely on varied devices, networks, and software platforms. Andreadis et al. (2024, pp. SP459–SP460) found that both patients and providers experienced significant privacy concerns in telemedicine, including fears of hacked video consultations, unauthorized listeners, and the use of devices or platforms not designed with strong clinical data protections. Although this study focused on civilian telemedicine, these risks are magnified in military environments where PHI and operational information often intersect.

Health Science emphasizes that clinicians rely on accurate and trustworthy information when making medical decisions. Houser et al. (2023, p. 1) found that telehealth introduces risks related to insufficient authentication, device vulnerabilities, and insecure data transmission. Interference with medical data can produce serious clinical consequences through delays, loss, alteration, or spoofing. For example, altered digital imaging or manipulated vital signs from wearable devices may lead to misdiagnosis or inappropriate treatment. Privacy breaches could also expose sensitive medical information that adversaries might exploit to infer a unit's readiness or identify weaknesses.

Health Science highlights the role of human behavior in cybersecurity. Both patients and providers may choose ease of use over strict security, especially under time pressure or stressful conditions. Andreadis et al. (2024, pp. SP459–SP460) found that many patients preferred familiar platforms such as FaceTime because they perceived them as convenient, even if they lacked full compliance with privacy standards. In combat settings, medics and remote providers may similarly prioritize rapid communication over proper safety protocol, increasing risk. This discipline underscores that cybersecurity failures directly translate into clinical harm, making strong cyber protections a core component of patient safety.

Military Medicine

Military Medicine provides the operational context necessary to understand the unique cybersecurity challenges present in combat zones. Function must be reliable across unstable tactical networks, satellite links, and field deployed devices, often under hostile cyber conditions. Unlike civilian healthcare, military medical support occurs in dynamic, limited resourced and even threat intense environments. Madsen et al. (2023, p. 21) found that deployed medical units face bandwidth limitations, intermittent connectivity, and heightened cybersecurity requirements designed to withstand adversarial interference. These constraints often force telemedicine systems to operate with degraded performance, increasing the risk of compromised or incomplete data transmission.

Military research also emphasizes that adversaries may attempt to intercept telemedicine traffic because medical information can reveal troop health, casualty rates, and overall readiness. Mousavi et al. (2022, p. 3) identified cybersecurity concerns, network constraints, and latency issues as major barriers to effective telemedicine deployment in operational settings. Their review demonstrated that systems must not only protect data but also remain functional under

cyber attack. Even short disruptions can delay triage decisions, prolong evacuations, or interfere with remote surgical guidance. This discipline demonstrates that in combat environments, cybersecurity is inseparable from mission success, force protection, and battlefield survival.

Common Ground

Despite their differences, all three disciplines agree that cybersecurity risks in telemedicine systems pose significant threats to the protection of sensitive medical information and to patient safety. Computer Science emphasizes the technical vulnerabilities that enable cyber attacks, Health Science highlights the clinical dangers of compromised data, and Military Medicine stresses the operational implications of system failure during missions. Each discipline recognizes that telemedicine introduces exposure points across devices, networks, and users. Because of these points of exposure, opportunities for adversaries to intercept, manipulate, or disrupt critical medical information are now possible.

Shared concerns include the dangers of unencrypted or weakly encrypted data transmission, inadequate authentication processes and insecure communication platforms. These alone and together create vulnerabilities in both hardware and software components. All three disciplines agree that the consequences of a cyber breach extend beyond data loss. It may impair clinical decision making, compromise patient trust, threaten operational security, or impede treatment that can save lives. There is also agreement that telemedicine systems require stronger safeguards, including secure platforms, encrypted communication channels, and user training to mitigate human error vulnerabilities. This common ground provides a foundation for integrating disciplinary insights into a more holistic understanding of how to secure telemedicine systems in combat environments.

Disciplinary Conflicts

Although there is substantial agreement, the disciplines also differ in several important ways. Consider Computer Science, which tends to prioritize system integrity. Even sometimes favoring highly restrictive security measures that may slow clinical workflows. From the perspective of Computer Science, rigorous multi-layer encryption, multi-factor authentication, and strict access controls are ideal. However, these measures may slow communication or complicate access during emergencies.

Health Science, however, emphasizes usability, patient access, and workflow efficiency. Health care workers often need systems that are simple and that operate at a high tempo. Rigid cybersecurity controls can impede the timely exchange of information or frustrate users to the point of bypassing protocols entirely. For example, if a system requires multiple authentication steps in a high stress environment, a medic may attempt to circumvent it to reach a provider quickly.

Military Medicine introduces yet another set of priorities, focusing on operational readiness and mission timing. While Computer Science may advocate the strictest security and Health Science may emphasize ease of use, Military Medicine must consider the realities of combat. Limited bandwidth, unstable networks, time-critical injuries, and adversarial interference are all in the realm of possibility. A system that is too secure to function quickly may hinder mission success, while one that prioritizes ease of use without adequate protection may expose systems or personnel to cyber attacks.

These disciplinary conflicts reveal the challenge of designing secure military telemedicine systems that are both technically rigorous, clinically efficient, and operationally

viable. Each discipline places emphasis on different tradeoffs, making interdisciplinary integration essential for a balanced solution.

Ch. 12 "Constructing a More Comprehensive Understanding or Theory"?

Using Repko and Szostak's integrative method, a more comprehensive understanding emerges by combining the strengths of each discipline while resolving their conflicts. From Computer Science, the paper incorporates rigorous risk assessment, threat modeling, and secure system architecture. Which emphasizes the importance of encryption, authentication, and vulnerability management. From Health Science, it incorporates the need for patient centered design, privacy protections, and clinically reliable data handling to ensure that cybersecurity enhancements do not impede care. From Military Medicine, it incorporates operational constraints, battlefield realities, and the demand for rapid, stable communication. According to Repko and Szostak (2020, p. 328), integration involves synthesizing the most relevant disciplinary insights to create a more comprehensive understanding of complex problems.

Integrating these insights shows that cybersecurity challenges in military telemedicine systems cannot be solved through technical defenses or clinical procedures alone. Instead, the integrated understanding suggests that the most effective protection requires military grade cybersecurity frameworks. To remain adaptable to combat conditions, safeguard both patient data and clinical accuracy, and balance usability with resilience would be paramount. Such a comprehensive approach recognizes that telemedicine systems must be secure enough to withstand adversarial threats while still flexible enough to support medics in extreme environments. This holistic perspective is only achievable by synthesizing the insights of all three disciplines.

Ch. 13 "Reflecting On, Testing, and Communicating the Understanding or Theory"?

Repko and Szostak's Chapter 13 emphasizes evaluating how well the integrated understanding works in practice (2020, p. 357). This new understanding can be tested by applying it to real military telemedicine scenarios. This may include remote trauma care, telephone intensive care operations, and battlefield triage. Systems built on this integrated model would need to demonstrate resilience under cyber attack, high pressure events, and adaptability to unstable bandwidth conditions. Simulated combat environments could also help ensure that cybersecurity measures do not hinder the speed or accuracy of clinical decision making.

Communicating this integrated understanding requires framing cybersecurity not only as a technical problem but as a medical and operational imperative. Policymakers, system designers, and military medical leaders are fundamental. They must keep in mind that cyber resilient telemedicine supports not just data protection but also patient survival and mission outcomes. Training programs for medics, clinicians, and support personnel should incorporate cybersecurity awareness for daily operations. Future research could also draw on perspectives from network engineering, human psychology, or international security studies to refine the integrated model. This reflection process demonstrates that this integrated understanding is adaptable and capable of guiding future improvements to military telemedicine systems.

Conclusion

Military telemedicine systems are essential tools that enhance medical readiness, expand access to specialists, and improve outcomes for service members in combat zones. However, these systems face serious cybersecurity challenges that threaten patient safety, operational security, and the reliability of clinical care. Cybersecurity threats to military telemedicine systems are revealed through insights from Computer Science, Health Science, and Military

Medicine. This interdisciplinary analysis demonstrates that these threats emerge from technical vulnerabilities, clinical risks, and operational constraints. They are also intensified in combat environments where bandwidth limitations, unstable networks, and adversarial cyber activity intersect with urgent medical needs.

By integrating these disciplinary insights, a more comprehensive understanding reveals that protecting military telemedicine requires secure system architectures, patient centered safeguards, and operationally realistic protections that balance security with usability. Ensuring secure telemedicine in combat zones is not only a technological concern but a critical component of military medical readiness and mission success. Strengthening cybersecurity is essential to protecting both the health of service members and the effectiveness of future military missions.

References

Andreadis, K., Muellers, K. A., Lin, J. J., Mkuu, R., Horowitz, C. R., Kaushal, R., & Ancker, J. S. (2024). Navigating privacy and security in telemedicine for primary care. *The American Journal of Managed Care, 30*(Special Issue 6), SP459–SP463. https://doi.org/10.37765/ajmc.2024.89553

Garg, V., & Brewer, J. (2011). Telemedicine security: A systematic review. *Journal of Diabetes Science and Technology, 5*(3), 768–777. https://doi.org/10.1177/193229681100500324

Houser, S. H., Flite, C. A., & Foster, S. L. (2023). Privacy and security risk factors related to telehealth services: A systematic review. *Perspectives in Health Information Management, 20*(Spring), 1–15.

Kim, D., Choi, J., & Han, K. (2020). Risk management–based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making, 20*(1), 106. https://doi.org/10.1186/s12911-020-01145-7

Madsen, C., Poropatich, R., & Pérez Koehlmoos, T. (2023). Telehealth in the Military Health System: Impact, obstacles, and opportunities. *Military Medicine, 188*(Supplement 1), 15–23. https://doi.org/10.1093/milmed/usad048

Mousavi Baigi, S. F., Kimiafar, K., Sarbaz, M., Abbaszadeh, A., & Mousavi, A. S. (2022). Effect of telemedicine in military medicine: A literature review. *Paramedical Sciences and Military Health, 17*(2), 1–12.

Repko, A. F., Szostak, R., & Buchholtz, L. W. (2020). *Introduction to interdisciplinary studies* (4th ed.). SAGE Publications.