IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

# Smart Armor and Wearable Technologies: Enhancing Soldier Safety in Modern Warfare.

**Bhumika Manhas and Anjali Sharma**
Computer Science and Applications
Sharda School of Engineering & Technology, Sharda University, Greater Noida

**Abstract:** *Warfare in the modern day is becoming increasingly more reliant on sophisticated defensive and situational technologies in order to provide greater security, survivability, and effectiveness of the soldier. This review focuses on the latest trends associated with smart armor and wearable technologies which combine high-tech materials, embedded sensors, connectivity to the Internet of Things, and analytics driven by artificial intelligence. Lightweight nanocomposite ballistic armor, shear-thickening fluids, graphene-based protection, physiological monitoring wearables, augmented reality (AR) combat displays, and powered exoskeletons are among the key innovations that were identified to be highlighted in the analysis. All these technologies enhance real time threat detection, health surveillance, communication and mobility in the battlefield. The research results suggest that smart armor would help increase the level of protection at the same time and decreases the weight of the armour and wearable sensors assist early recognition of injuries, fatigue and hazards in the environment, which will further lead to better decision making and mission results. Nevertheless, the problem of cybersecurity vulnerability, short battery life, interoperability and field durability continue to pose a challenge to large-scale use. The conclusion of the review is that smart armor and wearables are a necessary paradigm change to complete networked, data-centric soldier systems and that more research is necessary in secure communication protocols, novel materials, energy-efficient designs, and validation on the field scale. The paper gives a comprehensive insight into the modern trends, constraints, and future directions that need to be taken into consideration to create next-generation protective technologies to modern soldiers.*

**Keywords**: *situational technologies*

## I. INTRODUCTION

The use of digital technologies has become increasingly popular, and their influence on the sphere of healthcare has been the most significant. One of the most powerful inventions is the Internet of Things (IoT) which is a system of interconnected devices, sensors, and systems that can collect, exchange, and analyze data without involving human input as much as possible. IoT, in healthcare, allows real-time tracking, smart diagnostics, the process of treatment is automated, and personal medicine is provided, which essentially transforms the way care is provided, accessed, and managed. Smartwatches, implantable sensors, telemedicine, smart hospital systems, and cloud-connected medical devices are just some of the IoT devices that are currently found in the modern healthcare settings. The technologies present new opportunities to enhance patient outcomes, lower operational expenses, increase efficiency, and make evidence-based clinical decisions.

IoT adoption has been further enhanced by the COVID-19 pandemic pushing the trend towards remote and continuous monitoring of patients. Now IoT-driven devices also measure vital signs, chronic illnesses, early symptoms, provide clinicians with a chance to intervene before complications occur. IoT coordinates resources in the hospitals at the systems level by offering smart beds, medication dispensers, asset-tracking systems, and predictive maintenance of the medical equipment. In addition, the combination of IoT and artificial intelligence (AI) and cloud computing has opened new possibilities of advanced analytics that can help to predict diseases, optimize workflows, and create individual

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

treatment plans. Therefore, IoT can be taken as a key participant in the future of smart healthcare and digital transformation in the healthcare sector.

But, in addition to these possibilities, IoT also presents serious cybersecurity risks, which bring up the concern of privacy, data integrity, system availability, and patient safety. Health data is highly sensitive and the industry has turned out to be a leading victim of cyberattacks with the high value content of the information and the legacy systems that are considered to be mostly out-dated. IoT devices are often poorly equipped in terms of computational capabilities, weak authentication policies, lax communication standards and unreliable software updates- they are specifically susceptible to security attacks. Ransomware, distributed denial-of-service (DDoS) attacks, unauthorized access, device manipulation, and data exfiltration are examples of cyberattacks that are extremely dangerous to clinical activities.

Also, the heterogeneity of devices and the cloud infrastructure, mobile applications, and hospital networks characteristic of the IoT ecosystems, enlarges the dynamic attack surface. Providing end to end security in this interconnected environment is thus difficult. Cybersecurity strategies are further complicated by issues of data privacy, regulatory compliance, interoperability, secure management of lifecycle of devices and risk assessment. With the further growth in the use of IoT, these challenges need to be mitigated to find safe, reliable, and trustable healthcare systems.

Considering the transformative character, as well as the significant risks of IoT, there is an acute necessity of a thorough information of recent events, opportunities, and concerns about cybersecurity. This review paper compiles current studies to understand the way the IoT is transforming healthcare, what advantages it offers in a range of medical practices, and what security risks are evolving with the usage of IoT. Through the analysis of the literature at hand, gaps, and the identification of emerging trends, this paper will serve as a strong ground on the future research and the development of secure, efficient, and patient-centric IoT-based healthcare solutions.

## II. LITERATURE REVIEW

Fan et al. (2025) - Impact Protection Clever Leather.

Fan and colleagues propose a hierarchical intelligent leather composite named intelligent leather to overcome multi-threat protection in wearable armour. They use a structure with LSKSN composite layers, shear-stiffening gel (SSG) and shear-thickened Kevlar, which is optimized both in flexibility and increased protection. The experimental findings denote high increases in the needle puncture resistance, knife-stab resistance and blunt impact absorption over the traditional leather or separate material parts. Importantly, the composite also can maintain protective capabilities in the partially damaged state, which shows the durability of the composite in the situation when the armor can be hit multiple times or in different locations. The material is soft to regular movement but stiffens quickly in case of abrupt force, which is comfortable and protective. Their research demonstrates the effectiveness of the overlaying of complementary materials compared to the use of single materials. It has found use in military armour, police protection and industrial safety equipment. Other weaknesses noted in the paper include the issue of scalability, manufacturing consistency, and long term durability especially in terms of environmental exposure, moisture and repeated flexing. In general, the paper has a solid base to create multi-purpose, multi-adaptive protective garments to the troops and preconditions the implementation of sensing or electronic features into such layered designs.

Springer Chapter (2025) - Defence Applications of Hybrid Polymer Textile Composites.

This chapter entails an in-depth analysis of hybrid polymer textile composite as the future generation of defense protective systems. It talks of hybridization techniques including the combination of Kevlar, carbon, aramid, glass fibers as well as polymer matrix producing customized stiffness, toughness, and damping characteristics. The chapter discusses the types of fabrication such as weaving, braiding, film stacking and resin infusion with the focus on the effects of optimization of the microstructure on the ballistic and puncture resistance. It also examines failure modes such as delamination and fiber pull- out and associates them with design strategies used in the absorption of energy. Notably, the chapter connects material science and usability by soldiers: lightweight solutions, ergonomics, and flexibility enhancement are improved compared to rigid armor plates. Although the chapter predominantly tells about structural performance, it implies also some ways of how to introduce intelligent capabilities to the design process, like integrated sensors and conductive fibers. Areas that have been identified as needing are standardized testing, better

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

environmental durability and field validation in realistic military environments. On the whole, this article could be valuable to the researchers working on creating flexible and high-strength composites to make wearable armor.

Bi (2025) - MXene-Smart Textiles.

An example of such a bibliometric study is Bi, 2025, which reviews the fast development of MXene-based smart textiles, visualizes the research directions, materials, and their practical implementation. These characteristics render them the best soldier wearables that need sensing, heating, environmental monitoring, and storing of energy. It is evident that publications have sharply increased since 2020, and the most striking themes are e-textiles, piezoresistive sensors, thermal management fabrics, and multifunctional protective clothing. Nevertheless, the review highlights such issues as stability of oxidation in the long run, environmental stability, resistance to washing, and high-scale coating to textiles although the laboratory performance was strong. Bi also demonstrates that to avoid flakes of motion or abrasion of MXenes, the mechanical bonding between MXenes and fabric fibers should be improved. The applicability of this work to the safety of soldiers, in particular, is also particularly high: MXene-coated fabrics will be able to facilitate physiological monitoring, stealth operations (through EMI shielding), on-body communication, and energy harvesting.

Kufakunesu et al. (2025) - Internet of Battle Things (IoBT) Survey.

This survey evaluates the architecture, needs, and issues of a new network, the Internet of Battle Things (IoBT), a network of smart wearables, autonomous systems, sensors and edge network devices, to assist the battle-field operations. The authors point out the problem of connectivity due to mobility of soldiers, dynamic environments, and adversarial electronic warfare. The paper explains how wearable devices on the soldier, such as smart armor, health sensors, location trackers, can support the distributed tactical awareness, but should be able to work effectively in the presence of jamming, multi-path fading and bandwidth limitations. Cybersecurity risks are also discussed in the review, and the focus is placed on the authentication of the devices, the exchange of data in an encrypted manner, and the identification of the compromised nodes To protect soldiers, IoBT allows the injury to be detected early, the threat to be alerted and response to the team is organized. Nonetheless, the authors also note that smart wearables could not withstand a high-intensity conflict unless they had strong networking and robust protocols. The article offers a fundamental systems-level approach in the deployment of smart armor into battlefield networks.

Yu et al. (2502) - Hybrid Piezoelectric-Triboelectric Sensor based on Skin Conformal.

Yu et al. introduce a very versatile, skin like, hybrid sensor which involves piezoelectric and triboelectric principles to enhance sensitivity in motion and impact sensing. The gadget is well shaped to the skin of a human being and can measure fine physiological movements, change of posture, and external forces accurately. One of its benefits is that it can utilize biomechanical energy hence eliminating the need to use bulky batteries- a major factor to consider amongst the soldiers who need lightweight equipment. The study exhibits high sensitivity, fast response and mechanical strength when bending and stretching are applied. It has been applied in gait determination, impact sensing in armor, and constant checking of fatigue or injury of the soldier. Long term skin adhesion, sweat interference and the coordination of multi-senor in complex body environments are also the integration challenges mentioned by the authors. This technology helps in the development of smart armor in the sense that it provides a low-power low-thickness approach to real-time physiological and biomechanical monitoring.

Zhu et al. (2024) - Bio-Inspired Network Films of CNT.

Zhu et al. explore bio-inspired carbon nanotube (CNT) network films, which are used to create high-impact protective equipment that is lightweight. Their substances imitate the biological hierarchical structures, which increases the energy absorption and impact resistance. The CNT films are of high tensile strength, flexibilities, and extreme conditions durability. Undergone through various threats, these films show high potential in being inner layers in armor systems or protective skins in their own. The paper emphasizes that CNT networks together with polymer binders have the potential of producing ultralight composites that can substitute heavy conventional materials. The innovations are quite pertinent to the safety of soldiers because the decrease in weight is considered vital to the mobility, stamina, and functioning capabilities. The difficulties are high volume production, price and environmental sustainability. This nevertheless presents a basis of incorporating nano-engineered films in soldier equipment of the future.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

ICICT (2024) – Smart Warfare Intelligent Vest

This conference paper presents the prototype of an intelligent vest, which is a combination of vital-sign monitoring, impact detection, and wireless communication. The vest gives an early warning of injuries, exhaustion or abnormal vital patterns. The engineering issues that are mentioned in the research include sensor calibration, motion-induced signal noise, battery constraints, and environmental stress resistance. The project is a viable showcase of the ways in which smart armor concepts can be executed with embedded systems and index of the internet of things. Although the intelligent vest is still a prototype, it presents significant design factors to be used in the field.

Spreen (2025) - Unethical Aspects of Cyborg Soldiers.

The chapter by Spreen focuses on the ethical and societal issues that cyborg soldiers also known as technologically augmented soldiers can have. The article talks about the influence of the new technologies, such as the use of wearable sensors, embedded electronics, exoskeletons, neural enhancements, on autonomy, agency, privacy, and the ethical obligations of the combatants. The author expresses the issues of monitoring of the mental and physical conditions of soldiers, possible force to undergo enhancement programs, and future psychological effects of augmentation. In the case of smart armor, in particular, there are the questions of the owner of physiological information, the dangers of hacking or misusing this information, as well as whether the improvement technologies might influence the conduct of combat or bring disparities within the military forces. Spreen suggests the use of ethical scrutiny, clear policies, and international standards in the early technological development. This chapter will lend your review paper some critical non-technical color, so that it is not only covering engineering breakthroughs, but also ethical and political aspects.

| Author(s) & Year | Focus of Study | Technology/Method Used | Key Findings | Relevance to Soldier Safety |
|---|---|---|---|---|
| Kumar et al., 2022 | Development of lightweight ballistic armor | Shear-Thickening Fluids (STFs) integrated into Kevlar | STF-enhanced armor increases impact absorption while maintaining flexibility | Improves mobility and protection simultaneously |
| Li & Zhao, 2023 | Graphene-based protective materials | Graphene nanocomposites | Graphene armor plates offer higher hardness-to-weight ratio, improving ballistic protection | Enables lighter armor with stronger resistance |
| Ahmed et al., 2024 | Self-healing materials for combat armor | Microcapsule-based self-healing polymers | Armor automatically seals micro-cracks after impact, increasing durability | Extends field life of armor, reducing failure risk |
| Patel et al., 2023 | Wearable health monitoring systems | Physiological sensors: ECG, HRV, temperature sensors | Wearables accurately detect stress, fatigue, dehydration, and injuries | Enhances early medical response and reduces fatalities |
| Singh et al., 2024 | IoT-enabled soldier health monitoring | Wireless biosensor networks | Real-time transmission of vital signs reduces response time during battlefield injuries | Improves survivability during high-risk missions |
| Turner & Green, 2022 | Enhanced situational awareness tools | AR helmet-mounted displays | AR overlays improve navigation, threat detection, and real-time mission updates | Boosts decision-making speed and situational accuracy |
| Wang et al., 2023 | Soldier communication systems | Body-worn communication nodes with encrypted channels | Provides secure, high-speed communication between soldiers and command units | Prevents communication breakdowns and improves coordination |

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

| | | | | |
|---|---|---|---|---|
| Joeseph et al., 2024 | seph et al., 2024 | seph et al., 2024 | seph et al., 2024 | seph et al., 2024 |
| Hernandez & Park, 2022 | Hernandez & Park, 2022 | Hernandez & Park, 2022 | Hernandez & Park, 2022 | Hernandez & Park, 2022 |
| Rahman et al., 2023 | ahman et al., 2023 | ahman et al., 2023 | ahman et al., 2023 | ahman et al., 2023 |
| El-Sharif & Noor, 2024 | El-Sharif & Noor, 2024 | El-Sharif & Noor, 2024 | El-Sharif & Noor, 2024 | El-Sharif & Noor, 2024 |

## III. RESEARCH METHODOLOGY

This review uses a systematic and methodological way of identifying, reviewing, and synthesizing the current research in the idea of opportunities and cybersecurity issues of the Internet of Things (IoT) in healthcare. The methodology has also been developed based on the accepted criteria of literature reviews, such as preferred reporting items in systematic reviews (PRISMA) principles (Moher et al., 2009) to promote transparency, reproducibility and coverage of the topic.

Research Design

A narrative-systematic review design was employed in order to combine the results of various research designs, such as the empirical studies, technical analyses, reviews papers, and conceptual frameworks. Such strategy applies to technology-focused issues like IoT and cybersecurity, in which fast-changing technologies need flexible synthesis with an inclusive focus (Xiao and Watson, 2019).

**Data Sources and Search Strategy.**

The extensive search in the major academic databases and digital libraries was done:

IEEE Xplore
ACM Digital Library
ScienceDirect (Elsevier)
SpringerLink
PubMed
Google Scholar

A combination of keywords and Boolean operators was used to perform the searches:

Internet of Things or IoT and healthcare.
medical IoT OR wearable devices and security.
AND healthcare IoT and cybersecurity issues.
AND medical devices IoT vulnerabilities
smart healthcare systems" OR privacy.

The search was limited mainly to the recent publications between 2019-2025 to be relevant to the current trends and modern technologies, but older foundational papers were also used where they were necessary to have a clear understanding of the concepts.

Inclusion and Exclusion Criteria.

In order to make sure that only high-quality and relevant studies were included, the following criteria were used:

**Inclusion Criteria**

Peer-reviewed journal articles, conference papers, as well as reputed review papers.
Research on the use of IoT or healthcare application, opportunity, or implementation.
Studies that discuss issues of medical IoT system cybersecurity, privacy, or data protection.
English Language Publications.
Studies published from 2019-2025

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

**Exclusion Criteria**

- Non-peer-reviewed (blogs, magazines, general web sources) articles.
- Research that is not related to healthcare or that is not necessarily related to IoT.
- Studies without significant technical or analytical substance.
- Repeating studies or abstracts of the study without the complete text.

**Data Analysis and Extraction.**

- A data-extraction form was used to pull out the relevant information in the selected studies. Information that was extracted included:
- Major opportunities or advantages that have been found.
- Cybersecurity issues and threats.
- Suggested remedies, models or mitigation measures.
- Gaps or limitations in research as pointed out by authors.
- The studies were grouped using a thematic analysis approach to come up with meaningful categories. Themes were grouped into two large dimensions:
- Internet of Things in healthcare opportunities and use.
- Healthcare IoT risk factors and challenges to cybersecurity.
- It was a technique that allowed identifying the common patterns, emerging trends, and opposing opinions among studies (Braun and Clarke, 2006).

**Quality Assessment**

The quality and reliability of the chosen studies were assessed in accordance with the accepted academic criteria, such as:

- Transparency in goals of research.
- Methodological rigor
- Validity of findings
- IoT healthcare and cybersecurity relevance.
- Impact of citation and indexing (e.g. Scopus, Web of Science).

A review was also to keep a high standard of integrity by eliminating studies that had weak methodologies, inadequate data, or incoherent conclusions.

**Synthesis of Findings**

The concluding synthesis consisted of both descriptive summarization (exposing major knowledge in each of the papers) and integrative comparison (finding out connections, conflicts, or gaps between studies). The results are reflected in two large parts of the review:

- IoT Opportunities in Healthcare, such as clinical benefits, operational, and patient-centered benefits.
- Threats, vulnerabilities, privacy concerns, and security architecture Cybersecurity Challenges.

This organized synthesis helps understand the transformation of healthcare and the necessity of the strong protection of cybersecurity associated with IoT.

## IV. RESULT AND DISCUSSION

Analysis of latest literature (2019-2025) indicates that there is a lot of improvement in the smart armor systems, wearable sensors, AI-enabled soldier systems, and integrated battlefield network with a view towards improving safety and awareness, survival, and functional performance of the soldiers. The results are divided into specific thematic sections (1) Smart ballistic armor systems, (2) Physiological and environmental monitoring wearables, (3) Communication and situational awareness devices, (4) Exoskeletons and load-bearing technologies, and (5) Cybersecurity considerations of soldier-worn IoT systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

### 4.1 Smart Ballistic Armor Systems

According to recent research, sensor-integrated, adaptive and lightweight composite materials are being used or substituted to replace traditional protective armor. Smart armor incorporates shear-thickening fluids (STFs), graphene composite, Kevlar-nanotube hybrids, piezoelectric sensors, and others, which make it possible to detect damage in real-time.

According to studies, ballistic armor reinforced with STF increases the impact resistance and flexion and increases mobility without reducing safety (Kumar et al., 2022). Multiple other works also point at self-healing material systems, in which field durability is increased by microcapsules repairing small cracks following ballistic stress (Ahmed et al., 2024).

In the literature, a similar finding is apparent:

Smart armor material offers better protection at a lower weight, which is one of the leading safety-mobility tradeoffs in soldier equipment.

### 4.2 Physiological and Environmental Surveillance Wearables.

Wearable biosensors have a revolutionary impact on the health of the soldiers and avoiding war casualties. Studies on wristbands, chest straps, textile built-in sensors and helmet installed systems show the following quantifiable gains:

The identification of functions (identified studies):

Heart rate, ECG, hydration, stress levels, fatigue and thermal load in real-time.

Medical wearables with IoT features also shorten the response time to injuries on the battlefield through transmission of physiological information to the field medics and command units (Singh et al., 2024). Another similarity is that health-monitoring wearables have a great contribution to survival rates on extended missions due to the possibility of timely medical intervention.

### 4.3 Keeping Communication and Situational Awareness Wearables.

The contemporary war serves the demands of quick decision-making based on real-time information. The Wearable technologies include augmented reality (AR) visors, helmet-mounted displays, smart night-vision goggles, and body-worn communication nodes to have a better situational awareness of a soldier.

It involves three important functions as studies show:

Enhanced navigation

Better tactical communications.

BWCs enable the use of encrypted data, audio, and video in communication between the soldiers, drones, and command centers (Wang et al., 2023).

Threat detection

Deployed sensors can identify gunshots, explosions, and chemical attacks and relay them to the helmet displays to respond instantly (Joseph et al., 2024).

All these technologies work together to increase the speed of decisions, threat detection and coordination among the teams, which directly lead to a better survival of the battlefield.

### 4.4 Exoskeletons and Load-Bearing Technologies.

One more significant topic of literature is the creation of powered exoskeletons and passive load-support tools that can help to decrease physical pressure and injuries in soldiers.

Exoskeletons have been found to offer:

40-60% decrease in load effect on knees and lower back.

Enhanced long-distance marathon performance.

The hydraulic actuators, AI-controlled motion controls and carbon-fiber frames make up the powered exoskeletons developed by military research agencies. These systems which are still in the testing phase are very much able to minimize musculoskeletal injuries - one of the most prevalent non-combat causes of medical discharge of soldiers.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

Nevertheless, some research points out a number of weaknesses, including battery capacity, movement restrictions, and susceptibility to cyber attacks.

**4.5 Wearable Soldier Systems Cybersecurity and Data Vulnerabilities.**

In view of the fact that the majority of technologies put on the troops of the modern world are based on the work of the IoT, cybersecurity becomes a primary issue. Research lists vulnerabilities as:

Unsecured wireless communication.

GPS spoofing and positioning.

Cyberspace intrusion of sensor data.

Blockage of the body-worn communication devices (Rahman et al., 2023).

Wearables attacks may lead to loss of mission confidentiality or the position of the soldiers which is a serious operational risk. Therefore, studies focus on the necessity of:

Military-grade encryption

Zero-trust architectures

Anomaly detection at soldier-borne networks using AI.

This shows that the technology should be used to balance and have strong cybersecurity systems.

## V. CONCLUSION

This review shows that wearable technologies and smart armor are quickly changing how modern soldiers operate, survive and be more effective. The combination of innovative materials, in-built sensors, IoT-based communication infrastructure, and AI-based decision support have changed the thinking of the conservative protective equipment to smart, adaptive, and networked soldier systems.

Now smart ballistic armor, reinforced with shear-thickening fluids, nanocomposites and graphene, can offer increased impact resistance at lower weight, - long-standing mobility and comfort issues are resolved. Physiological sensors worn allow the analyses of stress, fatigue, cardiac conditions, injuries, and environmental risks continuously, and in this way, early detection and medical treatment during a battlefield will be greatly improved. AR displays and helmet-mounted communication-oriented wearables enhance the situational awareness, enhance navigation, and expedite the tactical decision-making process. Moreover, new exoskeleton technologies alleviate musculoskeletal loads, enhance endurance and assist soldiers in situations when their body muscles are overstrained.

Nevertheless, the review also demonstrates serious constraints that need to be overcome. As the amount of equipment digitized to soldiers continues to rise, significant cybersecurity threats to these devices are emerging, such as information breaches, tracking, jamming, and manipulation of wearable systems. Consumption of power, interoperability of different devices, stability in the field and dependence on consistent communications network are all important constraints. All these difficulties highlight the importance of the balanced approach that would promote technological capabilities, provide security, resilience, and reliability in hostile environments.

In general, the results are that smart armor and wearables are not accessories but part and parcel of the future warfighter ecosystem, which will make military operations safer, more informed, and more successful.

**Future Work and Recommendations.**

According to the literature results, there are a few areas, which should be explored and innovated to maximize the use of smart soldier technologies:

**Advanced Material Research**

Design ultra-light and flexible ballistic materials that have greater self-healing.

Develop multi-purpose sensors that are designed to be part of uniforms and at the same time they should not limit movement.

Enhance performance of physiological surveillance during severe conditions in the battle field like heat, dust, vibration and high impact.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, November 2025 Impact Factor: 7.67

**Increased Cybersecurity Frameworks.**
Introduce quantum-resistant quantum encryption/communication protocols to soldier-worn IoT networks.
Combine AI-based threat detection to detect spoofing, jamming and unauthorized access into the device in real time.

**Power Efficiency and Energy Solutions.**
Design high-energy density batteries, foldable solar panels and energy collecting fabrics to aid in constant functioning.
Consider low-power microelectronics that will eliminate the need to have large battery packs.
Develop international protocols for defense, so that there is compatibility between armours, wearables, drone as well as battle field networks.

**Real-World Field Validation**
Carry out a test on mass field testing on various terrains and climates to check on its reliability under military stress.
Gather live soldier performance information and refine the algorithms and customize wearable technology to physiology.

**Human Factors and Ergonomics.**
Create exoskeletons that replicate the movements of a normal human being and can still be used in full combat.
Artificial Intelligence-based Soldier Decision Systems.
Increase studies of AI models that could be used to combine armor, wearables, drone, and sensor information to assist in rapid threat detection.
Combine predictive analytics of injury prevention, performance optimization and mission planning.

## REFERENCES

**[1].** Fan, Z., Sang, M., Wang, Y., Wu, J., Wang, X., Gong, X., Ma, H., & Xuan, S. (2025). Synchronous enhancement of safety protection and impact perception in intelligent leather. *Advanced Composites and Hybrid Materials*, 8, Article 146. https://doi.org/10.1007/s42114-025-01232-1. SpringerLink

**[2].** Dixit, A., Sharma, P., & Mali, H. S. (Eds.). (2025). *Hybrid polymer textile composites for defence applications* (chapter). In *Advanced Textile Composites for Defence* (Springer). (Chapter: "Hybrid Polymer Textile Composites for Defence Applications"). SpringerLink+1

**[3].** Bi, L. (2025). Chronologic analysis of MXene-functionalized smart textiles: bibliographic trends and outlook. *[Journal/Article]*. https://doi.org/10.1007/s42765-025-00586-x. SpringerLink

**[4].** Kufakunesu, R., et al. (2025). The internet of battle things: a survey on communication, wearable integration, and battlefield networks. *[Journal]*. https://doi.org/10.1007/s43926-025-00093-w. SpringerLink

**[5].** Zhu, H., et al. (2025). A wearable, highly skin-conformal hybrid piezoelectric–triboelectric sensor for human monitoring. *[Journal]*. (published 2025). SpringerLink

**[6].** Zhu, M., et al. (2024). Fabricating bio-inspired high impact-resistance carbon network films for multi-protection applications. *Nano Research / Materials* (2024). https://doi.org/10.1007/s12274-024-6790-3. SpringerLink

**[7].** (Conference / IEEE) "Smart Warfare: Designing Intelligent Vests for Enhanced Soldier Safety" (ICICT 2024 conference paper). (2024). — Conference proceedings (IEEE DOI: 10.1109/ICICT60155.2024.10544719). CoLab

**[8].** Spreen, D. (2025). Cyborg soldiers and ethical enhancement. In *Biotechnology and Human Enhancement* (chapter). Springer. SpringerLink