Deactivated RFID chips as an innovative approach to enhancing the efficiency of casualty evacuation from combat zones: a scientific review

Chips RFID desactivados como enfoque innovador para mejorar la eficacia de la evacuación de heridos de zonas de combate: una revisión científica

Chip RFID desactivados como uma abordagem inovadora para melhorar a eficiência da evacuação de vítimas de zonas de combate: uma revisão científica

- Date of receipt: 2025/05/01
- Evaluation date: 2025/07/30
- Date of approval: 2025/08/22

To reference this article / Para citar este artículo / Para citar este artigo: Askarov, A. A., Begaliyev, Y. N., Mediyev, R. A. & Orakbayev, A. B. (2025). Deactivated RFID chips as an innovative approach to enhancing the efficiency of casualty evacuation from combat zones: a scientific review. *Revista Criminalidad, 67*(3), 99-114. https://doi.org/10.47741/17943108.701

Aslan A. Askarov
Doctoral student under the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
Republic of Kazakhstan
aslan.askarov1515@gmail.com
https://orcid.org/0009-0003-2351-7395

Yernar N. Begaliyev
Doctor of Legal Sciences
Law Enforcement Academy under the Prosecutor General's office of the Republic of Kazakhstan
Republic of Kazakhstan
ernar-begaliev@mail.ru
https://orcid.org/0000-0001-6659-8576

Renat A. Mediyev
University of Illinois Urbana-Champaign
Doctor of Legal Sciences
Republic of Kazakhstan
rinkevith@gmail.com
https://orcid.org/0009-0004-7765-7315

Esta obra está bajo licencia CC BY-NC-ND 4.0© por Policía Nacional de Colombia

Abstract

This article explores the potential use of deactivated RFID chips as an innovative solution aimed at enhancing the efficiency of casualty evacuation from combat zones. These chips address the critical need for ensuring the security and confidentiality of soldiers' locations on the battlefield. In their default state, the chips remain inactive, preventing unauthorised data access while allowing for the monitoring of physiological indicators during emergencies. In the event of severe injury or death, the chip automatically activates, transmitting real-time data on the soldier's condition and precise location. This enables a faster medical response and more accurate decision-making in evacuation planning. The objective of this study is to develop a tool that supports in-the-field medical evacuation and simplifies the identification of deceased military personnel. **Materials and Methods:** the research analyses the feasibility of replacing traditional military dog tags with deactivated RFID chips to improve field medicine and evacuation processes. A SWOT analysis was conducted to assess the strengths, weaknesses, opportunities, and threats associated with this technology. **Results:** the findings propose extending chip functionality by transforming them into battery-free adaptive systems that detect heartbeats using body heat as an energy source. This approach offers autonomous operation and enhanced monitoring capabilities, particularly in environments with limited access to power. **Conclusion:** deactivated RFID chips could significantly improve casualty evacuation, enhance location confidentiality, and reduce identification risks in cases where dog tags are destroyed. Their use supports compliance with humanitarian law and facilitates the identification of missing soldiers, bringing closure to their families.

Keywords

Deactivated; humanitarian law; medical evacuation; soldier identification; soldier safety

Resumen

Este artículo explora el posible uso de chips RFID desactivados como solución innovadora destinada a mejorar la eficacia de la evacuación de heridos de las zonas de combate. Estos chips responden a la necesidad crítica de garantizar la seguridad y confidencialidad de la ubicación de los soldados en el campo de batalla. En su estado por defecto, los chips permanecen inactivos, impidiendo el acceso no

Askhat B. Orakbayev
Doctor of Philosophy (PhD)
Alikhan Bokeikhan University
Republic of Kazakhstan
askhat333orakbaev@gmail.com
https://orcid.org 0000-0001-7363-3835

autorizado a los datos y permitiendo al mismo tiempo el control de los indicadores fisiológicos durante las emergencias. En caso de herida grave o muerte, el chip se activa automáticamente, transmitiendo datos en tiempo real sobre el estado del soldado y su localización exacta. Esto permite una respuesta médica más rápida y una toma de decisiones más precisa en la planificación de la evacuación. El objetivo de este estudio es desarrollar una herramienta que apoye la evacuación médica sobre el terreno y simplifique la identificación del personal militar fallecido. **Materiales y métodos:** la investigación analiza la viabilidad de sustituir las tradicionales placas caninas militares por chips RFID desactivados para mejorar la medicina de campo y los procesos de evacuación. Se realizó un análisis DAFO para evaluar los puntos fuertes, débiles, oportunidades y amenazas asociados a esta tecnología. **Resultados:** los hallazgos proponen ampliar la funcionalidad de los chips transformándolos en sistemas adaptativos sin pilas que detectan los latidos del corazón utilizando el calor corporal como fuente de energía. Este enfoque ofrece un funcionamiento autónomo y una mayor capacidad de monitorización, sobre todo en entornos con acceso limitado a la energía. **Conclusión:** los chips RFID desactivados podrían mejorar significativamente la evacuación de heridos, aumentar la confidencialidad de la localización y reducir los riesgos de identificación en los casos en que se destruyan las placas. Su uso favorece el cumplimiento del derecho humanitario y facilita la identificación de los soldados desaparecidos, aportando un consuelo a sus familias.

Palabras clave

Desactivado; derecho humanitario; evacuación médica; identificación de soldados; seguridad de los soldados

Resumo

Este artigo explora o uso potencial de chips RFID desativados como uma solução inovadora para melhorar a eficiência da evacuação de vítimas de zonas de combate. Esse chip atende à necessidade crítica de garantir a segurança e a confidencialidade da localização dos soldados no campo de batalha. Em seu estado-padrão, o chip permanece inativo, impedindo o acesso não autorizado aos dados e permitindo o monitoramento de indicadores fisiológicos durante emergências. Em caso de lesão grave ou morte, o chip é ativado automaticamente, transmitindo dados em tempo real sobre a condição e a localização exata do soldado. Isso permite uma resposta médica mais rápida e uma tomada de decisão mais precisa no planejamento da evacuação. O objetivo deste estudo é desenvolver uma ferramenta que dê suporte à evacuação médica em campo e simplifique a identificação de militares falecidos. **Materiais e métodos:** a pesquisa analisa a viabilidade de substituir as tradicionais plaquetas de identificação militar por chip RFID desativado para melhorar a medicina de campo e os processos de evacuação. Foi realizada uma análise SWOT para avaliar os pontos fortes, os pontos fracos, as oportunidades e as ameaças associadas a essa tecnologia. **Resultados:** as descobertas propõem ampliar a funcionalidade do chip, transformando-os em sistemas adaptativos sem bateria que detectam batimentos cardíacos usando o calor do corpo como fonte de energia. Essa abordagem oferece operação autônoma e recursos de monitoramento aprimorados, especialmente

em ambientes com acesso limitado à energia. **Conclusão:** os chips RFID desativados podem melhorar significativamente a evacuação de vítimas, aumentar a confidencialidade da localização e reduzir os riscos de identificação nos casos em que as etiquetas são destruídas. Seu uso apoia a conformidade com o direito humanitário e facilita a identificação de soldados desaparecidos, trazendo consolo para suas famílias.

Palavras-chave

Desativado; direito humanitário; evacuação médica; identificação de soldados; segurança de soldados

Introduction

Since the advent of Radio Frequency Identification (hereinafter referred to as RFID), the process of automatic object recognition has become significantly more efficient. RFID systems operate by reading and writing data transmitted via radio signals, which are stored in specialized devices known as transponders or RFID tags (hereinafter —RFID chips). These technologies not only enhance identification accuracy, but also significantly reduce the time and labor costs associated with data collection and processing, making them particularly valuable in situations that require rapid response.

The operation of an RFID system functions as follows: an RFID reader transmits radio waves at a specific frequency, which activates a transponder located within the signal's range. Once activated, the transponder transmits its stored data back to the reader, which then processes the information and relays it to a control system. This process occurs almost instantaneously and enables precise identification of objects without the need for visual contact, barcode scanning, or manual data entry.

RFID systems offer high speed and reliability in data acquisition while minimizing human error in the identification process. In environments where accuracy, speed, and security are of critical importance —such as logistics, healthcare, transportation, or the military— RFID has proven to be a universal and effective solution. It is capable of being seamlessly integrated into a wide range of technological workflows and adapting to the specific demands of various operational contexts (Baevsky, 2015).

Initially, the development and use of RFID devices demonstrated high efficiency in retail and the production of consumer goods. However, over time, the advantages of this technology were identified and successfully adapted for sectors such as services, security, pharmaceuticals, and other industries (Begaliyev, 2020).

In the early 2000s, government and private institutions in the United States actively implemented RFID chips in various areas of daily life, ranging from official documents (passports, identification cards) to millions of bank credit cards (Sterling, 2005). U.S. experts J. A. Garrity and J. Landt, in their researches, emphasize that: "FID technology has become an integral part of modern life, widely used in various areas of trade, and even golfers use RFID chips to find lost balls" (Garrity, January 14, 2016), and that: "Its introduction into everyday processes is explained by its high efficiency, accuracy, and ability to automate object identification" (Landt, 2005).

In Russia and the countries of the Commonwealth of Independent States (CIS), RFID technologies are widely used in various sectors of the economy. In logistics and warehousing, RFID facilitates the automation of inventory management processes, improving the accuracy and speed of operations, especially in large distribution centers (Kulikov et al., 2022). RFID has been applied in retail since the 2000s. However, many large-scale projects planned for the implementation of this technology were not realized for various reasons. Today, the largest retail chains have switched to electronic document management, and retail companies have started to use new digital capabilities, such as bots, big data, online cash registers, and artificial intelligence (AI), which now creates new opportunities for more active use of RFID technology (Barkova, 2021).

Companies such as Reply and Oversight use in-store cameras and RFID technology integrated with AI. By leveraging AI and the company's software, they optimize their product promotion strategies (Barkova, 2021). Additionally, RFID is used in logistics to monitor the movement of goods and automate customs procedures (Grigorieva, 2016). In industry, RFID is implemented in manufacturing plants, where the technology helps track assembly stages, control product quality, and manage raw material inventories (Elistratova & Korshakeevich, 2014).

It should also be noted that, despite the active development of the technology, its implementation in the industrial sector in Russia and the CIS countries is associated with a number of difficulties. The main barrier is the high cost of equipment and implementation systems, as well as the lack of a unified system of standards, which complicates the integration of RFID solutions from different manufacturers (Bobtsov et al., 2007). Inadequate technological infrastructure in remote regions is also an obstacle to the widespread adoption of the technology (Ayandina, 2019).

The next stage in the evolution of RFID technology was its expansion not only to inanimate objects, but also to living organisms — including humans. Currently, RFID chips are actively used for identifying pets (Dove & Martin, April 25, 2023), as well as for monitoring elderly people suffering from Alzheimer's disease (Currid, 2009), and employees in the workplace (Rodríguez, 2019). Additionally, RFID chips are actively applied in medicine. In transplantation, their implementation could significantly speed up the process of determining compatibility between donors and recipients (Amirov et al., 2024).

Considering the experience of integrating AI with RFID technologies, it is worth noting the interesting case described in the work of Sadykov et al. (2024), where it is highlighted that "the possible integration of AI with human chipping opens up wide opportunities for the technological market in the field of forensic medical expertise, enabling the collection of detailed physiological data and processing them using AI-managed systems". This expansion in the use of RFID technology has been driven by the growing need to enhance security, improve control, and optimize management processes across various spheres of public and professional life. The integration of RFID systems into daily operations became a logical step in response to the increasing demand for more efficient and automated methods of identification and monitoring. These systems have become an integral part of modern solutions for managing resources, personnel, logistics, and even maintaining public order.

Initially used exclusively in logistics and business for inventory tracking and warehouse automation, RFID technology has gradually entered the private sphere, significantly broadening its scope of application. Today, RFID chips can be found in transit passes, bank cards, health insurance policies, and even in household pets, facilitating identification and recovery in case of loss. This shift from corporate to personalized use marked a major turning point in the evolution of the technology, raising new societal concerns regarding the balance between technological advancement and the protection of personal data, as well as the ethical and legal implications of surveillance and control. For instance, the U.S. Department of Homeland Security planned to use RFID technology in key immigration documents and state driver's licenses but later abandoned this decision (Weinberg, 2008).

The U.S. Transportation Security Administration proposed the implementation of RFID tags in airline boarding passes. This innovation was aimed at allowing security personnel to track the whereabouts of all passengers in real-time at every airport. It was anticipated that the integration of RFID technology would enhance airport security by providing more efficient passenger flow control and enabling the timely detection of potential threats (Weinberg, 2008).

All the aforementioned initiatives for the implementation of RFID technology led to concerns from advocacy groups, experts, and researchers regarding the privacy and security of individuals' personal information (Smith, 2007). Research in the field of RFID technology implementation has identified three interrelated privacy threats (Smith, 2007):

1. Geographical location tracking: RFID technology allows anyone with access to a reader device to identify the identity of individuals with RFID chips, as RFID accurately determines the subject's location in space, functioning as a Global Positioning System (GPS);

2. Profile creation: An individual collecting data using RFID technology can create a detailed profile of the subject, including observation results and any other information obtained through RFID. In the case of a passport, this may include identification numbers, addresses, and physical characteristics. Moreover, data can be collected by third parties, not just the government authorities that initially created the RFID tag;

3. Implementation risk: By identifying a person through RFID technology, subjects or devices connected to the reader network may take actions based on the collected data. This could include further surveillance, arrest, or targeted advertising, depending on the goals and intentions of the parties involved (Pappu, 2003).

In this context, it is advisable to consider several case studies illustrating the privacy and security issues arising from the use of RFID technology. These examples will allow for a detailed analysis of the impact of RFID chips on personal data protection and security assurance.

Case study: Integration of Nike Plus iPod in consumer gadgets

In August 2006, Nike and Apple introduced the Nike Plus iPod Sport Kit, a fitness package that enables runners to track distance, calories burned, and speed using an RFID chip embedded in Nike shoes and a receiver connected to an iPod Nano. Apple marketed this device as a convenient way to monitor workouts in real time. However, researchers from the Department of Computer Science at the University of Washington in the United States found that the Nike Plus iPod device not only assists with workouts, but can also be used for surveillance. Scientists and experts identified several issues (Newitz, December 1, 2006).

First, the RFID sensor in the shoe, which has its own power source, turns the shoe into a radio transmitter capable of sending signals up to 20 meters, far enough to be picked up by a passing car. Second, the sensor broadcasts a unique identifier to any Nike Plus iPod receiver. The researchers also discovered that the device is easy to hack, allowing, for instance, a malicious actor to track a user's running routes and times by compromising their Nike Plus iPod system (Saponas et al., 2007).

Case: RFID-Embedded T-Shirts for preschoolers

In early 2010, local authorities in Contra Costa county, California, USA, implemented measures to enhance the safety of preschool children. As part of this initiative, they decided to use RFID tags embedded in children's T-shirts (Mutigwe & Aghdasi, 2007). Officials argued that employing RFID technology to track children's real-time location increases their safety and reduces the risk of them going missing. However, the American Civil Liberties Union (ACLU) advocated for limiting the use of RFID technology due to concerns over privacy and security.

Nicole Ozer (November 1, 2008), Director of Technology and Civil Liberties at the ACLU of California, emphasized that "one of the potential risks of using RFID tags in preschool T-shirts is that malicious actors could easily copy the information from an RFID tag and create a duplicate. This would make it possible to remove a child from the school campus while the cloned RFID chip continues to signal that the child is still on school grounds".

All the aforementioned cases and examples concerning privacy have led to a slower adoption of RFID technology than initially anticipated. Nevertheless, scientific research in this field continues, focusing on overcoming challenges related to data privacy and security. In this regard, in 2012, the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense announced the launch of a project aimed at developing implantable sensory RFID microchips for use in the U.S. military (Newman, May 8, 2012).

DARPA emphasized that the new RFID microchips would allow for real-time monitoring of any potential medical issues among soldiers, giving the U.S. Armed Forces a strategic advantage over adversaries. At the time, it was noted that RFID implant technology represented a truly groundbreaking innovation, as nanotechnology had the potential to revolutionize modern warfare. It was also highlighted that the primary goal of introducing RFID microchips was to enhance medical evacuation procedures, which are more frequently necessitated by illnesses and diseases rather than combat-related injuries or wounds (Newman, May 8, 2012).

In 2016, DARPA launched another innovative project aimed at implanting RFID chips into soldiers' brains, enabling them to interface directly with supercomputers (Smith, 2007). The new initiative, titled the Neural Engineering System Design (NESD) program, seeks to utilize electrochemical communication between neurons to convert neural signals into digital commands capable of controlling computer software, robotics, or prosthetic devices. Program developers stated that "the goal is to develop an interface that can be implanted into the human skull to provide unprecedented signal resolution and data transmission bandwidth".

In 2021, the Ministry of National Defense of the People's Republic of China (People's Liberation Army — hereinafter referred to as 'the PLA') announced the issuance of the first batch of identification tags containing QR codes and RFID microchips to a training unit of the PLA under the Xinjiang Military Command for testing purposes (Charlie, 2021). It was noted that this innovation would enhance the efficiency of field medicine and logistical operations by providing each soldier with a device for storing personal data (see Figure 1).

Figure 1.| A metal identification tag with a QR code and a green plastic tag embedded with an RFID microchip

Specialists from the (PLA) noted that:

> […] metal identification tags with QR codes provide more detailed information about the soldier and are highly resistant to heat exposure and explosions […] The green plastic tag with an embedded RFID microchip contains additional information about the soldier, including fingerprints, allergy history, and past injuries. This information is intended to be used for granting access to medical facilities. (Science and Space, 26 July 2023)

American military experts, studying the use of RFID microchips for soldiers, highlighted their advantage in high-speed data reading even in unfavorable conditions. At the same time, they emphasized the vulnerability of RFID technology due to the risk of remote data access over significant distances (Singh, April 9, 2021). The experience of the U.S. military in using RFID microchips in 2019 revealed vulnerabilities in wearable tracking devices, which, by creating location maps, unintentionally disclosed the locations of secret bases abroad (Singh, April 9, 2021). This incident underscores the need for strict control over the use of RFID technologies to prevent their exploitation by adversaries.

However, at the 2024 meeting of the Microelectronics Council, U.S. Deputy Secretary of Defense Kathleen Hicks emphasized the key role of microchips in modern military technology, which is used in nearly all systems: ships, aircraft, tanks, ammunition, radars, communication systems, and satellites. According to Kathleen Hicks: "The U.S. Department of Defense is committed to fostering collaboration between the government, industry, and academia to remain a leader in research, design, production, and scaling of microchips" (Vergun, October 29, 2024).

Thus, after analyzing the practices of various countries, it is reasonable to proceed to a comparative analysis of the cases of the United States, China, and Russia, which reveals significant divergence in approaches to the implementation of RFID technologies. These differences are driven by both political-economic and sociocultural factors.

In the United States, RFID has been integrated into everyday life since the early 2000s — through passports, bank cards, logistics, and even the sports industry. Among the most ambitious initiatives were those led by the Transportation Security Administration, which sought to incorporate RFID into airline boarding passes, as well as the military's experiments with implantable microchips to monitor soldiers' health conditions. These projects illustrate a high level of technological maturity and an ambition to create a "smart soldier". However, criticism from the ACLU and a number of public scandals — such as the case involving the Nike Plus iPod system — have demonstrated RFID's high vulnerability to unauthorized tracking and privacy violations. As a result, while RFID technologies in the U.S. are developing rapidly, they are subject to strict public and legal oversight.

In China, RFID implementation is characterized by a centralized and disciplinary approach. One example is the equipping of the PLA soldiers with identifiers that combine QR codes and RFID chips. The emphasis is placed on functionality, durability, and integration with biometric systems, which enhances the effectiveness of military medicine and logistics. However, as noted by Western analysts, the large-scale deployment of RFID in the Chinese military poses significant risks of sensitive data leakage, including geolocation data. China demonstrates an extremely high degree of technical centralization, while issues of human rights and privacy remain largely unaddressed.

Russia and the CIS countries are currently in a transitional phase. Despite early initiatives in logistics and transportation, the full-scale integration of RFID into the medical or military sectors faces several challenges, including high equipment costs, a fragmented regulatory framework, and underdeveloped infrastructure. At the same time, the growing interest in digitalization and the adoption of AI creates prerequisites for more active implementation of RFID technologies in the coming years. Summarizing the comparison, one can highlight the key characteristics of each country's approach (see Table 1).

Table 1. | Characteristics of RFID system implementation in different countries

Country	Drivers of implementation	Key cases	Challenges and risks
USA	Technological leadership, military and commercial interests	Military, logistics, and consumer sector	Privacy violations, non-consensual tracking
China	Centralized control, military logistics	RFID tags for soldiers, biometrics	High efficiency, but weak protection of individual rights
Russia and CIS	Digitalization of the economy, AI, and logistics	Retail, industry, healthcare (limited)	Financial and infrastructural constraints

Thus, international experience shows that the effectiveness of RFID implementation in a given sector depends not only on the technical specifications of the system, but also on the level of public trust, the maturity of the legal and regulatory framework, and the adherence to ethical standards. For the successful adaptation of such technologies in the medical and military domains, it is essential to consider not only their technological aspects but also their implications for civil rights, logistics, and strategic security.

Analyzing the advantages and risks of using RFID technology in the armed forces of developed countries, it is necessary to reconsider the approach to the application of RFID chips for soldiers. An optimal solution could be the use of "deactivated" or "sleeping" RFID chips, which are activated only in the event of a soldier's serious injury or death, minimizing security and privacy risks. This article explores the possibility of using deactivated RFID chips as a replacement for traditional military dog tags, proposing this as an innovative approach to enhancing the effectiveness of field medicine.

Materials and methods

This study examines the use of deactivated RFID chips as an effective alternative to traditional military dog tags, aiming to enhance field medicine capabilities, including medical evacuation, and identification of soldiers in combat conditions. The study evaluates not only the technological aspects of implementing RFID systems, but also their humanitarian dimensions, such as the protection of human rights, data privacy, and the enhancement of medical service efficiency.

The analysis is based on the application of the SWOT method, which systematically evaluates the strengths and weaknesses of the proposed technology, as well as identifies potential opportunities and threats associated with its implementation. The SWOT analysis provides a comprehensive view of all aspects of using deactivated RFID chips in military and medical operations. This approach makes it possible not only to assess the internal advantages and risks of the technology, but also to consider its impact on the effectiveness of medical evacuation, and its compliance with international humanitarian standards.

The methodological framework of the study is based on a modified SWOT analysis, aimed at identifying the strengths, weaknesses, opportunities, and threats associated with the implementation of RFID technologies under conditions of elevated risk and unstable infrastructure. This analysis was supplemented by documentary research and a comparative case study review of countries where such technologies have been applied in military, crisis, and medical settings.

The information base was formed through targeted searches in international academic databases (Scopus, Web of Science, IEEE Xplore, PubMed), as well as official sources, including reports from government agencies, international organizations (WHO, ITU), defense institutions, and technological consortia. The selection criteria for literature and case studies included the following parameters:

- Availability of documented use of RFID/NFC technologies under conditions of limited internet access, medical evacuation, combat operations, or large-scale emergencies;
- Presence of technical detail and outcome-related data;
- Relevance and practical or regulatory significance of the information provided.

Materials with only superficial mentions or outdated technological solutions were excluded. The collected data were systematized into a summary analytical table structured around several parameters, such as: level of technological maturity, method of implementation, application context, legal constraints, vulnerabilities, and outcomes.

It is worth noting that, as part of this research, the author developed a technical solution that has been granted legal protection in the form of a utility model patent in the Republic of Kazakhstan. According to a notification from the Republican State Enterprise "National Institute of Intellectual Property" under the Ministry of Justice of the Republic of Kazakhstan, and in accordance with Paragraph 1 of Article 25 of the Patent Law of the Republic of Kazakhstan, a protection document has been issued for utility model application No. 2025/0415.2 titled "Device for the Identification and Monitoring of Servicemen's Condition".

To obtain expert feedback and assess the practical significance of the proposed device, an online survey incorporating elements of structured interviews was conducted. The study was carried out from March to May 2025 using an anonymous questionnaire containing both closed and open-ended questions. More than 70 respondents participated in the survey, including military medical officers, specialists in military logistics and communications, IT experts in defense technologies, as well as instructors and cadets from relevant military and technical educational institutions.

Respondents were asked to evaluate the relevance, technical feasibility, and potential risks associated with the deployment of the device. The results demonstrated a high level of interest and support for the concept:

- 91% of participants recognized the relevance of such technologies in modern military operations and emergency scenarios;
- 84% supported the integration of RFID systems into the individual equipment of military personnel to facilitate identification and status monitoring in the field;
- 77% indicated that the device could significantly enhance the effectiveness of first aid and evacuation during mass casualty events;
- 68% expressed concerns regarding cybersecurity risks, particularly the possibility of signal interception and unauthorized data access;
- 94% favored the use of passive RFID tags, which do not require autonomous power sources and are known for their high reliability.

In addition, 73% of the respondents confirmed their willingness to participate in further testing and the implementation of a prototype of the device once developed.

Open-ended responses collected during the interviews provided valuable feedback regarding the design characteristics of the device. Key suggestions included: compactness and ergonomic design, resistance to mechanical damage and environmental conditions, ease of integration into standard military gear, and the inclusion of an alert function in the event of a critical deterioration in a serviceman's condition. These inputs were taken into account when formulating the design requirements and refining the technical specifications of the device.

Regarding validation, testing, and the potential implementation of a pilot project, it should be noted that due to the sensitive nature of the topic, the development and prospective deployment scenarios of the device fall under restricted-access information and may be classified as "for official use only". The device is being considered within the context of defense and specialized medical infrastructure, which necessitates a non-public approach to certain stages of testing, approval, and simulation.

Nevertheless, the granted utility model patent in the Republic of Kazakhstan confirms both the technical novelty and legal protection of the developed solution. The device has attracted interest among experts, and the conducted survey demonstrated a high level of professional recognition of the concept. This supports the conclusion that the project holds significant applied potential and represents a promising direction in the development of technologies aimed at enhancing medical support and identification capabilities during military operations and emergency situations.

In conducting the empirical analysis, various data sources have been used, including results from existing scientific studies, reports, and publications in the field of RFID technology application in military and medical practice. The experience of already implemented RFID systems in military operations has been analyzed, and current research and developments aimed at improving identification and medical evacuation in field conditions have been reviewed.

Special attention has been given to the scientific and technical aspects of using personalized identification devices, such as microchips, which can store critically

important medical data, including information about blood type, allergies, chronic illnesses, and other health features that may be essential in emergency medical situations. An additional method of analysis has involved data on the current use of similar technologies in other countries, including comparisons with practices and standards from NATO and other military alliances, to identify potential areas for improvement and implementation of these technologies.

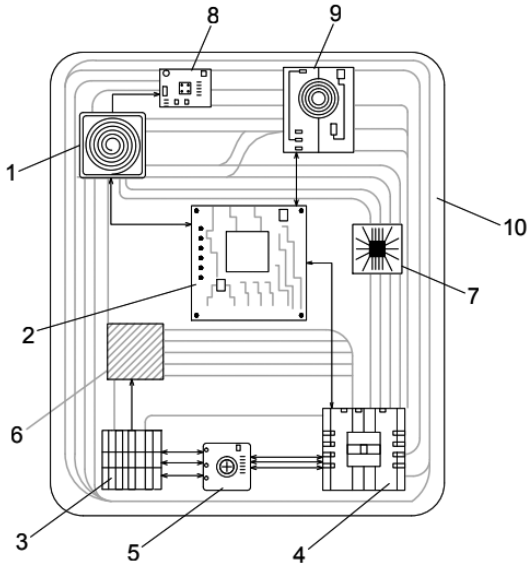
Additionally, to ensure the reliability of the results, it is advisable to conduct testing of the proposed RFID solutions in real field conditions with the participation of military personnel. This experimental approach will provide empirical data necessary for a comprehensive analysis of the effectiveness of deactivated RFID chips in military settings.

Results

As part of the research findings, it is proposed to expand the functionality of deactivated RFID chips by transforming them into a battery-free adaptive system capable of detecting human heartbeat (Bose et al., 2020a). From a theoretical perspective, it seems feasible to develop RFID chips that use human body heat as an energy source while simultaneously responding to temperature changes. This technology could provide autonomous operation of the devices and enhance their effectiveness in monitoring physiological states, especially in environments where access to external power sources is limited. In our view, the implementation of this technology would enable continuous monitoring of human physiological parameters, significantly increasing its practical value, particularly in the field of surgery. Using human body heat as an energy source minimizes the need for external resources, ensuring the autonomy and reliability of the system in challenging operational conditions.

In their research, scientists Bose, Shen, and Johnston (2020b) proposed an innovative battery-free system for detecting heartbeat, based on the "crystal on chip" technology (SoC-System on Chip). The uniqueness of this development lies in the use of human body heat as the primary energy source, enabling the system to operate completely autonomously, without the need for traditional power sources such as batteries or accumulators (see Figure 2).

Figure 2.| Innovative implantable tag



Where:

1 – Antenna;

2 – Microcontroller (RFID chip);

3 – Thermoelectric generator;

4 – Heart rate sensor;

5 – Temperature sensor;

6 – Energy accumulator;

7 – Energy-dependent memory (EEPROM/FRAM);

8 – Communication module (NFC/RFID);

9 – Signal transmission module;

10 – Protective biocompatible casing.

This approach opens up vast prospects for the application of the technology in various fields, including not only civilian medicine, but also military operations and emergency rescue activities in remote or extreme conditions. This technology is particularly significant in the context of ensuring the health and safety of military personnel in combat situations. In field conditions, where access to medical facilities is limited and power supply is unstable or completely absent, autonomous systems for monitoring vital signs can play a crucial role in the timely detection of critical conditions, such as heart failure or cardiac arrest. This helps significantly reduce the time between the onset of a life-threatening situation and its detection, thereby increasing the chances of successful first aid and subsequent evacuation.

Additionally, it should be noted that the integration of this technology with miniaturized RFID chips contributes to the creation of more compact, reliable, and resilient devices that are resistant to external impacts. Unlike traditional systems, which are sensitive to temperature fluctuations, vibrations, or mechanical damage, such battery-free solutions ensure long-term operational stability. This is particularly important when carrying out prolonged missions in high-risk environments or isolated regions, such as deserts, mountains, or disaster-stricken areas.

The integration of heartbeat detection technology with automatic activation functions in the event of cardiac arrest, along with the ability to transmit the exact coordinates of the soldier's location in real-time, creates the potential for a fundamentally new level of medical support system. Such a system can be programmed to automatically notify not only medical units, but also command structures, facilitating quick coordination of actions and decision-making. At the same time, the principles of confidentiality and security are upheld, as deactivated RFID chips do not transmit signals until activation, preventing their interception by the enemy and enhancing stealth on the battlefield.

Under real combat conditions, the effectiveness of the device largely depends on its ability to operate during critical physiological states of a serviceman, such as Grade III-IV traumatic shock. The most common causes of death in the first minutes following injury are massive hemorrhage (hypovolemic shock) and tension pneumothorax (obstructive shock), as confirmed by data from Tactical Combat Casualty Care[1].

According to clinical observations, in cases of blood loss exceeding 40 % (classified as Grade IV shock), skin temperature can rapidly drop to 30-32 °C within 2-3 minutes after injury. This phenomenon complicates the use of certain types of sensors that rely on body heat. Under such conditions, it is vital that the device remains operational even in the presence of pronounced peripheral hypothermia.

The proposed thermosensitive activation mechanism of the device is based on the temperature contrast between the human body and the surrounding environment. However, in a state of shock —especially in cold climates— the temperature differential may be insufficient. Therefore, it is advisable to implement a multichannel activation approach, incorporating redundant sensors based on heart rate, pulse variability, SpO_2, or changes in blood pressure. In other words, the design should account for the sensitivity threshold of sensors aimed at detecting temperature fluctuations.

One potential solution is the use of infrared or hybrid biosensors capable of detecting not only temperature, but also other vital biomarkers such as heart rate or galvanic skin response. This would increase the likelihood of device activation even under conditions of reduced body temperature.

The work of Romanov et al. (2023) confirms that multisensor monitoring can reliably track blood loss dynamics and shock severity, even in field conditions. The authors emphasize the effectiveness of using combined algorithms that incorporate skin temperature, pulse rate, oxygen saturation, and behavioral parameters —an approach particularly critical when a soldier's condition deteriorates rapidly in combat scenarios.

Moreover, given the high mortality rate associated with tension pneumothorax —the second leading cause of death on the battlefield— it is essential to incorporate the ability to detect signs of sudden respiratory decompensation or a sharp decline in oxygen saturation. These indicators could be integrated into future versions of the device as potential triggers for emergency alerts (Kotwal et al., 2016). Indeed, accounting for physiological changes resulting from severe combat injuries enables the adaptation of the technology for more effective use, ensuring activation within the so-called "golden hour" —the critical time window during which emergency medical intervention is most vital for survival.

Therefore, one promising direction for further development is the transition toward a hybrid activation system architecture, in which the thermosensitive module is complemented by other types of biosignal inputs. This approach would provide reliable identification and monitoring of a serviceman's condition even under severe pathophysiological states and unstable environmental conditions.

1 Available at: https://jts.health.mil/index.cfm/CPGs/cpgs

The technology in question can be viewed not only as a tool for health monitoring, but also as a component of a broader system aimed at enhancing the survivability of personnel. The implementation of such solutions permanently within the armed forces requires further applied research, field testing, and interdisciplinary collaboration involving specialists in engineering, medicine, military science, and law. Nevertheless, it is already clear that this technology has the potential to significantly transform both the principles of conducting military operations and the emergency response system.

Discussion

H. Wayne Elliott, of the University of Virginia School of Law, emphasizes in his research that "many of the practical challenges associated with handling deceased soldiers on the battlefield remain unresolved". Despite existing legal norms[2] that mandate honorable treatment of the fallen, "combat conditions often make timely and dignified burial impossible" (Department of the Army Pamphlet 27-50-284). Armed conflicts are inherently risky, and in situations with limited time and resources, decision-making related to burial can become particularly difficult. The importance of prompt and respectful interment of soldiers becomes especially apparent in the context of human rights protection and the preservation of humanitarian principles during military engagements.

An example of the challenges associated with handling the deceased can be found in the 1983 conflict in Grenada, where, due to the hot climate and limited conditions, soldiers were forced to find rapid burial solutions. However, many of the fallen lacked proper identification tags, which complicated their identification and the subsequent repatriation of their bodies. As a result, some of the deceased were not returned to Cuba, despite the assumption that most of them were Cuban nationals. This situation highlights the critical importance of implementing reliable identification systems to prevent such issues in the future (Department of the Army Pamphlet 27-50-284).

Technological advancements over the past decade have opened new opportunities for addressing these challenges. In 1991, during Operation Desert Storm, U.S. fighter pilot Scott Speicher went missing, marking the first combat casualty of the conflict. However, in 2001, after an analysis of intelligence data, his status was changed from "killed in action" to "missing in action". This case became a vivid example of how technology can play a crucial role in altering the status of missing service members and facilitating their search, enabling timely access to information about their situation and location, even if they are wounded or held captive (Sanders, 2004).

One of the technologies capable of enhancing the identification of military personnel is RFID. Despite potential constitutional objections and privacy concerns, the use of RFID chips instead of traditional military dog tags could significantly streamline the process of locating and identifying soldiers. These chips enable rapid access to accurate information about service members, which is crucial both for their rescue and for expediting medical evacuation. RFID technology also holds promise in other areas, such as monitoring soldiers' health status, allowing for real-time updates on their medical conditions and potential injuries (Tukenova et al., 2021).

One of the key requirements for the development of devices intended for use in combat or evacuation conditions is ensuring autonomous and uninterrupted operation of RFID systems in the absence of fixed power sources and under unstable network infrastructure. In this regard, the use of energy-efficient architectures becomes essential, including passive and battery-assisted RFID tags, as well as well-designed wake-up and data exchange mechanisms.

Scientific literature highlights that passive RFID chips exhibit high reliability during short-term contact with a radio frequency source and do not require an internal power supply (Dobkin, 2012). However, to enable extended functionality —such as real-time monitoring of physiological parameters— Battery-Assisted Passive or Active RFID technologies become increasingly relevant. These solutions utilize compact power sources and low-power sleep modes to maintain energy efficiency (Finkenzeller, 2010).

The study by Zatout et al. (2011) demonstrates the capabilities of RFID sensors for long-term monitoring of biomechanical parameters without constant connection to a server, which is particularly relevant for military medical applications. Moreover, modern approaches involve adaptive wake-up mechanisms for RFID circuits, based on physiological triggers or external stimuli, further enhancing autonomy and reducing energy consumption.

From a future-oriented perspective, deactivated RFID chips implanted in a soldier's body could store critical data such as identification information, blood type, medical records, and other vital details. These chips could be utilized to objectively track changes in a soldier's health condition, for example, in cases of unconsciousness or cardiac arrest, by transmitting real-time location data.

2 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field. July 27, 1929. Available at: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.30_GC-I-EN.pdf

This capability is especially relevant in the context of modern military conflicts, where traditional search and identification methods often prove ineffective.

As for the advantages of deactivated RFID microchips, they do not require a constant power source and do not emit signals, making them less susceptible to enemy detection. Unlike active chips, these devices produce no continuous emissions and can be removed through a relatively simple surgical procedure if necessary. This reversible technology represents a significant step toward establishing a comprehensive tracking and monitoring system for military personnel —one that could not only enhance the efficiency of medical evacuation, but also improve the process of locating missing soldiers, providing families with more complete information about the fate of their loved ones (Mukanov & Begaliyev, 2020).

It is important to note that one of the key challenges in implementing digital identification systems under aeromedical evacuation conditions is the limited or entirely absent Internet access in remote and hard-to-reach regions. Areas such as Chocó, Guainía, Guaviare, Amazonas, Vichada, and others are characterized by weak telecommunications infrastructure, lacking stable cellular coverage or satellite relay. This situation creates significant difficulties when attempting to read data from devices that rely on cloud services or online verification —such as QR codes, which often require Internet access for decryption or matching with a centralized database.

To ensure uninterrupted access to medical and identification data in such environments, the integration of alternative autonomous reading technologies is proposed. One of the most effective solutions involves the implementation of wireless modules based on near-field radio communication technologies —such as NFC and/or passive RFID. These technologies enable direct data retrieval from a microchip embedded in a tag without the need for Internet connectivity. In practice, such solutions have already been implemented and described, for example, in patent US10580521B1, which provides for the use of RFID readers integrated into medical equipment, transport stretchers, or helicopter medical modules[3].

When the injured individual is placed on a stretcher, the identifier and relevant medical data are automatically transmitted to the receiving device of the medical crew or physician, without the need for cloud services or network connections. It is worth noting that these technologies enable direct data retrieval from the chip embedded in the tag without requiring Internet connectivity, using a mobile terminal (e.g., a portable medical tablet or a wearable crew device) that has been pre-synchronized with a secure local database prior to deployment.

In addition, the potential use of low Earth orbit satellite communication systems —such as Starlink, OneWeb, and similar platforms— has been considered, as they provide broadband connectivity in remote regions. Despite their high operational cost, such solutions may prove cost-effective in the context of prioritizing the evacuation of severely wounded military personnel, particularly under combat conditions or during natural disasters. However, the full utilization of satellite communication channels requires the prior integration of appropriate modules and antennas into on-board medical and navigation equipment, which must be the subject of a separate technical and economic feasibility study.

Accordingly, the device's technical architecture should be designed to support a hybrid data access model: autonomous —enabling rapid use in offline mode—, and networked —for extended access when an Internet connection is available. This will ensure the system's reliability, resilience to external communication risks, and increase the justification for its implementation in real-world operational conditions.

It is important to emphasize that from a human rights and privacy standpoint, the use of such technologies must be accompanied by specific safeguards. Transparency in matters related to RFID usage becomes a crucial factor in maintaining public trust, particularly with respect to protecting the privacy of soldiers. Ultimately, the implementation of these technologies aims to enhance the humanitarian dimension of military operations, not only by improving the system for locating missing personnel but also by increasing the overall effectiveness of both military and medical services.

As part of our analysis on the integration of deactivated RFID chips into military practice, we employed a SWOT analysis methodology. The results demonstrated that the strengths of using such technologies significantly outweigh the weaknesses, indicating a high potential for further development and implementation of RFID in both military and medical contexts (see Table 2).

3 US Patent US10580521B1. Available at: https://patents.google.com/patent/US10580521B1/en

Table 2. | SWOT analysis deactivated soldiers' RFID chips

Strengths	Weaknesses
1. Deactivated RFID chips ensure confidentiality by preventing unauthorized access and minimizing the risk of data leakage on the battlefield. 2. The immediate determination of the location and condition of the wounded or deceased soldiers' using a deactivated RFID chip significantly accelerates medical evacuation and assistance. 3. Deactivated RFID chips powered by body heat ensure autonomy and reliability in field conditions. 4. Deactivated RFID chips enable quick and accurate identification of the remains of the deceased, ensuring compliance with humanitarian law standards. 5. Deactivated RFID tagging could be mandatory only if the recruit is assigned to serve in combat conditions. 6. Deactivated RFID chips are capable of automatically activating in critical situations, such as severe injury or absence of heartbeat. 7. RFID chips can store and transmit personal data, including identification information, blood type, medical history, and the soldiers' status.	1. The use of chips may raise concerns regarding the control over personal freedom and potential human rights violations. 2. In the event of weapons of mass destruction or terrorist attacks, RFID chips could fail or be damaged, which would prevent the transmission of information about the soldiers' condition and pose a threat to evacuation and assistance efforts.
Opportunities	**Threats**
1. Quick and accurate soldier identification simplifies personnel management and enhances record-keeping efficiency. 2. RFID chips can transmit soldiers' health data to medical or command centers, facilitating prompt decision-making.	1. Identification falsification could create false data, allowing one soldier to be replaced with another, undermining the accuracy of personnel tracking and operations. 2. Cyberattacks on data processing systems could threaten the security of databases and servers storing RFID chip information, potentially disrupting system functionality or resulting in lost critical data.

Conclusion

The conducted study confirms that the use of deactivated RFID chips can represent a significant step forward in transforming medical support and evacuation systems within the military sphere. The results obtained highlight the potential of this technology not only from a technical and organizational perspective, but also in terms of its humanitarian impact. Most notably, the implementation of deactivated RFID chips ensures reliable identification of military personnel even under the most extreme combat conditions, where traditional identification methods such as dog tags may be lost, damaged, or intentionally removed. This significantly reduces the risk of unidentifiable casualties and contributes to more accurate personnel accounting.

Second, the technology significantly improves the speed and accuracy of medical evacuation. By storing critical medical information and precise geolocation data, the system enables the quick identification of the wounded, their condition, and location, while simultaneously transmitting this information to medical units and command centers in real time. This, in turn, reduces response time, improves coordination, and increases the chances of saving the soldier's life.

Third, the protection of confidentiality and human rights in the application of this technology is achieved through the use of an activation mechanism that is only

triggered in critical situations. Deactivated chips do not transmit signals until activated, which eliminates the possibility of surveillance or data interception by the enemy, ensuring a high level of stealth and compliance with international humanitarian law standards.

Fourth, this solution positively impacts the moral and psychological state of both the soldiers themselves and their families. The ability to quickly obtain reliable information about the fate of a loved one —whether they are wounded, evacuated, or, unfortunately, deceased— helps reduce uncertainty, lessen stress, and ensure more reliable communication between the military and society.

Fifth, the legal aspects of implementing this technology should be considered. From an ethical and constitutional standpoint, the mandatory use of RFID chips is permissible only when the soldier is directly engaged in combat operations. This requires legislative measures to establish activation and deactivation mechanisms for the system, as well as the creation of secure protocols for protecting personal data.

The use of deactivated RFID chips to enhance the effectiveness of field medicine and evacuation could become an integral part of modernizing the armed forces. However, realizing this potential requires a systematic approach involving scientific and practical work: conducting large-scale field tests, interdepartmental cooperation, and developing a regulatory framework with the participation of experts in law, medicine, military science, and technology. Only through a comprehensive approach can this innovative technology be integrated into the practical operations of military missions.

Author contributions

All authors confirm that their authorship complies with the ICMJE international criteria (all authors contributed substantially to the conceptualization, search, analysis, and preparation of the article, read and approved the final version before publication). The greatest contribution is distributed as follows: A. A. Askarov —concept and design of the work, collection and processing of material, writing of the manuscript text, scientific editing of the manuscript; E. N. Begaliyev —concept and design of the work, collection and processing of material, manuscript writing, scientific editing of the manuscript, review and approval of the final manuscript; R. A. Mediyev— concept and design of the work, collection and processing of material, writing of the manuscript text, scientific editing of the manuscript, review and approval of the final version of the manuscript; A. B. Orakbayev —conducted the theoretical analysis and structured the article, interpreted the obtained results, and prepared the final text in accordance with academic standards.

Funding source

This research has been funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP25795721).

Conflict of interests

There was no conflict of interest among the authors of this academic research. We declare that we have no financial or personal relationships that could influence the interpretation and publication of the results obtained. We also ensure that we always comply with ethical standards and scientific integrity at all times, following the guidelines established by the academic community and those dictated by this journal.

References

Amirov, A. M., Begaliyev, Y. N., Baimakhanov, A. A. & Bakhteev, D. V. (2024). On the issue of ensuring the protection of personal data by chipping: A review. *Russian Journal of Forensic Medicine. 10*(1), 56-67. https://doi.org/10.17816/fm16096

Ayandina, A. S. (2019). Prospects of using radio frequency tags for spatial identification. *Young Scientist, 248*(10), 5-6.

Baevsky, A. A. (2015). RFID technology and its prospects in Russia. *Proceedings of the Nizhny Novgorod State Technical University No. 3*, pp. 98-103.

Barkova, N. Y. (2021). Radio frequency identification of data in retail: New business opportunities. *Bulletin of the University*, (1), 28-35. https://doi.org/10.26425/1816-4277-2021-1-28-35

Begaliyev, E. N. (2020). On the Introduction of Radio Frequency Identification (RFID) technology as a means of countering the commission of certain types (groups) of crimes. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, 110*(2), 191-195. https://doi.org/10.24411/2073-0454-2020-10095

Bobtsov, A. A., Kamnev, D. A., Kremlev, A. S. & Topilin, S. A. (2007). Radio Frequency Identification Technology (RFID): Prospects of use and emerging problems. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, 242-248.

Bose, S., Shen, B. & Johnston, M. L. (2020a). *A 20-µW heartbeat detection system-on-chip powered by*

human body heat for self-sustained healthcare [paper]. IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, USA, 19-20 February 2020. https://doi.org/10.1109/ISSCC19947.2020.9062971

Bose, S., Shen, B. & Johnston, M. L. (2020b). A batteryless motion-adaptive heartbeat detection system-on-chip powered by human body heat. *IEEE Journal of Solid-State Circuits*, *55*(11), 2902-2913. https://doi.org/10.1109/JSSC.2020.3013789

Currid, E. G. (2009). More bite than bark: the legal and social consequences of microchipping individuals with Alzheimer's disease. *Indiana Health Law Review, 6*(2), 357-378. https://doi.org/10.18060/16553

Charlie, G. (2021, February 09). *PLA issues first batch of dog tags with QR codes and RFID microchips*. Overt Defense [online]. https://www.overtdefense.com/2021/02/09/pla-issues-first-batch-of-dogtags-with-qr-codes-and-rfid-microchips/

Dobkin, D. M. (2012). *The RF in RFID: Passive UHF RFID in Practice* (2nd ed.). Elsevier.

Dove, D. & Martin, D. (2023, April 25). *The best pet trackers for your furry friends*. Digital Trends [online]. http://bit.ly/487eV5a

Elistratova, A. A. & Korshakeevich, A. S. (2014). Technology of radio frequency identification in the Russian market. *Actual Problems of Aviation and Cosmonautics*, 365-366.

Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near field communication* (3rd ed.). Wiley.

Garrity, J. A. (2016, January 14). *A smart golf ball that tracks my strokes? Tell me more!* [online]. http://bit.ly/3IiLpyT

Grigorieva, A. (2016). Trends in the development of RFID technology: An overview of the global and Russian market. *Electronics, 154*(4), 44-49.

Kotwal, R. S., Howard, J. T., Orman, J. A. Tarpey, B. W., Bailey, J. A., Champion, H. R., Mabry, R. L., Holcomb, J. B. & Gross, K. R. (2016). The effect of a golden hour policy on the morbidity and mortality of combat casualties. *JAMA Surgery, 151*(1), 15-24. https://www.doi.org/10.1001/jamasurg.2015.3104

Kulikov, M. M., Komissarova, M. A. & Nazarova, I. A. (2022). Prospects of using RFID technologies in Russia. *Bulletin of the Rostov State University of Economics (RINH), 4*(80), 191-196. https://doi.org/10.54220/v.rsue.1991-0533.2023.80.4.026

Landt, J. (2005). The history of RFID. *IEEE Potentials, 24*(4), 8-11. https://doi.org/10.1109/MP.2005.1549751

Mukanov, M. R. & Begaliyev, Y. N. (2024). Chipping pedophiles as an alternative to chemical castration. *Russian Journal of Forensic Medicine, 10*(1). https://doi.org/10.17816/fm15175

Mutigwe, C. & Aghdasi, F. (2007). Research trends in RFID technology [online]. *Interim: Interdisciplinary Journal, 6*(1), 68-82. http://bit.ly/46gOszB

Newitz, A. (2006, December 1). *Nike + Ipod = Surveillance*. Wired News [online]. http://bit.ly/46gSMyK

Newman, A. (2012, May 08). *US military seeking implantable microchips in soldiers. The New American* [online]. http://bit.ly/4nKOY03

Ozer, N. A. (2008, November 1). *Rights «Chipped» Away: RFID and identification documents* [online]. https://dx.doi.org/10.2139/ssrn.5015677

Pappu, R. (2003). *Privacy and security in the EPC network* [online]. http://bit.ly/4gmfvy7

Rodríguez, D. A. (2019). Chipping in at work: Privacy concerns related to the use of body microchip (RFID) implants in the employer-employee context. *Iowa Law Review, 104*(3), 1581-1605. http://bit.ly/3JTHYPL

Romanov, V., Galelyuka, I., Mintser, O. & Brondz, I. (2023). Wearable smart sensor system for medical monitoring with an assessment of the level of blood loss and pain shock because of trauma or injury. *International Journal of Analytical Mass Spectrometry and Chromatography, 11*(2), 11-21. https://www.doi.org/10.4236/ijamsc.2023.112002

Sadykov, M. B., Begaliyev, Y. N., Bakhteev, D. V., Kaziyeva, A. N. & Khussainov, O. B. (2024). The use of artificial intelligence and human chipping in forensic medicine: A review. *Russian Journal of Forensic Medicine,10*(1), 88-98. https://doi.org/10.17816/fm16093

Sanders, M. (2004). Chipping: Could a high-tech dog tag find future american MIAS? *Journal of High Technology Law, 4*(209). http://bit.ly/3HVVXnA

Saponas, T. S., Lester, J., Hartung, C., Agarwal, S. & Kohno, T. (2007). Devices that tell on you: Privacy trends in consumer ubiquitous computing. 16th USENIX Security Symposium [online]. http://bit.ly/41Pssul

Science and Space. (2023, July 26). *What's in the high-tech military card of Chinese soldiers?* [online]. http://bit.ly/46gID54

Singh, A. (2021, April 9). *PLA issues dog tags and medical wrist bands to wandering soldiers.* The Daily Guardian [online]. http://bit.ly/47EfhQy

Smith, J. E. (2007). You can run, but you can't hide: Protecting privacy from radio frequency identification technology. *North Carolina Journal of Law & Technology, 8*(249).

Sterling, B. (2005). *Shaping things.* The MIT Press.

Tukenova, Z. S., Alikperov, K. D., Begaliyev, Y. N., Seraliyeva, A. M. & Shayakhmetova, Z. B. (2021). Biochipping in forensic medicine as a technology for determining readiness to cause harm: A review. *Russian Journal of Forensic Medicine, 10*(1), 47-55. https://doi.org/10.17816/fm16092/

Vergun, D. (2024, October 29). *With industry help, DOD strives to be leader in microchip research, production.* DOD News [online]. http://bit.ly/3VGCRVx

Weinberg, J. (2008). Tracking RFID. *Journal of Law and Policy for the Information Society, 3*, 777-805. http://bit.ly/4gi2VzT

Zatout, Y, Kacimi, R., Llibre, J.-F. & Campo, E. (2011). *Mobility-Aware protocol for wireless sensor networks in health-care monitoring* [paper]. IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, 09-12 January 2011. https://doi.org/10.1109/CCNC.2011.5766319