ASPI | Afarand Scholarly Publishing Institute; Turkey
ISSN: 2980-969X Iranian Journal of War & Public Health 2026;18(2):189-200. 10.58209/ijwph.18.2.189

The Roles and Functions of Passive Defense as a Deterrence Strategy in Preventing Military Surprise

ARTICLE INFO

Article Type
Systematic Review

Authors
Moradpour Dehnavi A.M.[1] *PhD*
Sadeghi R.[2] *PhD*
Bamir M.*[3] *PhD*

How to cite this article
Moradpour Dehnavi AM, Sadeghi R, Bamir M. The Roles and Functions of Passive Defense as a Deterrence Strategy in Preventing Military Surprise. Iranian Journal of War & Public Health. 2026;18(2):189-200.

[1]Department of Islamic Studies, Sirjan School of Medical Sciences, Sirjan, Iran
[2]Department of Public Health, Sirjan School of Medical Sciences, Sirjan, Iran
[3]Research Center for Social Determinants of Health, Institute for Futures Studies in Health, Kerman University of Medical Sciences, Kerman, Iran

***Correspondence**
Address: Faculty of Medical Sciences, Old Imam Reza Hospital, Ibn Sina Street, Sirjan, Iran. Postal Code: 7614914537
Phone: +98 (34) 31296600
bamirmousa@gmail.com

Article History
Received: December 23, 2025
Accepted: March 17, 2026
ePublished: April 14, 2026

ABSTRACT

Aims This paper presented a review of the functions and roles of passive defense in strengthening non-offensive deterrence and reducing vulnerability.

Information & Methods This systematic review was conducted to comprehensively gather related literature, spanning the conceptual evolution of passive defense from 2005 to 2025. No geographical or document type restrictions were imposed. Electronic searches were performed across three specialized databases (Web of Science, Scopus, and PubMed), two general search engines (Google Scholar and Google), and Persian databases (SID and Magiran). Furthermore, gray literature sources and manual citation tracing (forward and backward tracking) were utilized to ensure complete coverage of the literature. The study selection process followed the PRISMA framework.

Findings The role of passive defense in preventing and countering military surprise was delineated across 15 key axes. The most critical application areas identified in the scientific documents fell into four main categories that formed the foundation of defense strategies. Moreover, the dimensions of passive defense in these studies were categorized into nine key sections, and the fundamental elements and components of passive defense, which specify the executive requirements, collectively comprised seven vital components.

Conclusion Passive defense is a proactive, multi-layered strategy that strengthens national resilience by reducing vulnerabilities and preventing attacks from escalating.

Keywords Military Personnel; Defense Mechanisms; Review

CITATION LINKS

[1] The role of new information ... [2] Introduction of the components and tools of the US hybrid ... [3] HSE management system, passive defence and its ... [4] The role of passive defense in ... [5] The effects of passive ... [6] Bioterrorism and biological warfare, from ... [7] Passive Defense as a Deterrence Strategy: A Review of Its ... [8] Passive defense threats and measures in crisis ... [9] An introduction to passive defense ... [10] Passive defense strategies for critical infrastructure ... [11] Military, political, cultural, and societal implications ... [12] From passive defense to proactive ... [13] The role of passive defense principles on air ... [14] Evaluation of soldiers' knowledge ... [15] Lessons learned from passive ... [16] A comparative study of passive defense policy models of non-governmental industries ... [17] Pathology of health and treatment centers ... [18] The approach of passive defense in the location of essential ... [19] Active and passive defense ... [20] Presenting a model to identify the relationship ... [21] Local government, passive ... [22] Passive defense challenges in hospital ... [23] Explaining the factors influencing the formulation of ... [24] Prospective research of medical passive defense ... [25] Strategic model of public security ... [26] Assessment of hospital preparedness of Tehran ... [27] Risk management in human made ... [28] Investigating the factors related to the ... [29] Passive defense in the ... [30] Passive defense in cyberspace and ... [31] Exploring factors influencing the evolution ... [32] Strategies of passive defense to ... [33] The model of strategic monitoring for ... [34] Obstacles to the implementation ... [35] The role of passive ... [36] Passive defense strategy ... [37] Passive defense ... [38] Passive defense in new ... [39] Anti-Islamic computer ... [40] Adopt passive defense ... [41] Evaluating the level of vulnerability of urban infrastructures ... [42] Presenting a strategic model of people-centered ... [43] The importance of human ... [44] Investigating Iran's economic ... [45] Passive defense strategies ... [46] Identifying and prioritizing culture ... [47] The role of passive defense in ... [48] The role of psychological factors of soft power in the field ... [49] Strategic and efficient factors in securing basic needs (food) from the passive defense ...

Copyright© 2026, the Authors | Publishing Rights, ASPI. This open-access article is published under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License which permits Share (copy and redistribute the material in any medium or format) and Adapt (remix, transform, and build upon the material) under the Attribution-NonCommercial terms.

Introduction

War has always been a persistent element of human existence. With the advancement of technology and the introduction of modern and intelligent weaponry, its nature has become increasingly complex and destructive [1]. The contemporary concept of hybrid warfare refers to a sophisticated military strategy that combines conventional, unconventional, cyber, psychological, and information operations [2]. Surprise, as one of the key methods of executing military tactics, has gained such importance that it has become a fundamental principle of warfare. In modern conflicts—given technological progress and changing patterns of combat—it has evolved into a vital factor capable of determining the outcome of a war [2].

In this context, defense has emerged as one of the most strategic approaches, consisting of two main dimensions: active and passive defense. Since the formation of human society, defense in various forms has existed and evolved alongside technological development [3]. Active defense refers to all military actions and the use of direct war equipment to counter enemy attacks, including fighter aircraft, missile defense systems, tanks, artillery, and other military hardware. In contrast, passive defense encompasses non-military measures aimed at reducing vulnerability to enemy attacks, relying on non-weapon tactics, and is as old as human civilization itself. A review of the history of warfare demonstrates that passive defense has always existed in different forms and has continuously adapted with technological advancements [4]. Today, it stands as an indispensable principle of both contemporary and future warfare [5].

The extensive use of nuclear, biological, and chemical agents in wars and terrorist attacks over the past two decades indicates that threats are not only persistent but also increasing [6]. Implementing diverse forms of passive defense measures to counter military aggression, natural and man-made disasters, as well as non-military threats, such as cyberattacks and psychological warfare, has become a fundamental necessity [7]. The scope and magnitude of such measures encompass all key infrastructures and critical, sensitive, and vital military and non-military facilities [6].

Passive defense refers to the reduction of vulnerability during crises without resorting to direct military action and solely through civil, technical, and managerial activities. Its goal is to minimize the impact of enemy attacks by reducing susceptibility and creating obstacles against various threats—especially modern and hybrid ones—without engaging in direct combat [7]. Consequently, it plays a vital role in preventing military surprise. The adoption of passive defense strategies helps sustain human resources, which serve as the principal element in crisis management [8].

As one of the most effective and enduring approaches to defense against multifaceted threats, passive defense has consistently attracted the attention of numerous countries worldwide. Even nations with substantial military capabilities, such as the United States and the former Soviet Union, have paid special attention to this field. Likewise, neutral countries like Switzerland—despite not facing direct threats or involvement in the two world wars—have invested remarkably in passive defense [9].

In past wars, passive defense has played a crucial role in reducing casualties and damage, helping to preserve lives, property, and the continuity of essential activities. Experiences derived from major conflicts—including World War II, NATO's eleven-week war against Yugoslavia in 1999, the 2003 U.S.-U.K. invasion of Iraq, Israel's thirty-three-day war against Lebanon in 2006, the Hamas attack against Israel on October 7, and other military and non-military conflicts—all confirm that aggressor nations often attempt to break the opponent's will and political, economic, military, and managerial capacities by employing a center-of-gravity destruction strategy, primarily through bombing and annihilating vital, sensitive, and critical facilities [8].

Evidence from these wars demonstrates that countries employing multifaceted passive defense strategies, including rapid (strike) and non-strike forms of defense, have been significantly less vulnerable to surprise attacks and threats [9]. Likewise, lessons learned from natural disasters such as the 2003 Bam earthquake and the 2001 Golestan flood in Iran confirm that inadequate implementation of passive defense principles led to extremely high financial and human losses [9].

The Islamic Republic of Iran, due to its geographical and geopolitical location in the turbulent region of West Asia, the growth of terrorist groups in recent years, the hegemonic ambitions of major powers, threats posed by NATO and Israel, and extensive media campaigns aimed at altering public ideology toward the ideals of the Islamic Revolution, faces heightened strategic vulnerabilities. Moreover, given the nuclear doctrine and the adversaries' superiority in advanced weapons, technology, and equipment, the necessity of implementing passive defense measures has become even more critical. Failure to adopt these measures would expose the country to far more severe damage and losses. All these factors underscore the need for integrated defense strategies to enhance preparedness against emerging threats and to emphasize passive defense as a complementary component within the national defense chain.

Accordingly, this study sought to conduct a comprehensive review to identify the dimensions,

components, functional domains, and implications of passive defense in preventing military surprise.

Information and Methods

Literature search and search strategy

The search strategy encompassed both electronic database searching and manual searching. This combined approach included electronic searches across three major bibliographic databases and two search engines, and forward and backward citation tracking. For the literature search, we systematically queried the following international databases and search engines: Web of Science, Scopus, PubMed, Google Scholar, and Google. Additionally, Persian-language literature was sought through the SID (Scientific Information Database) and Magiran databases, alongside searches in gray literature sources (Table 1).

Table 1. Search strategy

Web of Science
TS=("Passive defense" OR "Non-operating defense" OR "Inactive defense" OR Unarmed OR "Civilian defense" OR "Non-military Defense" OR "Preventive Measures") AND TS=(War OR battle OR fight OR belligerence OR Threat OR menace OR military)
Scopus
TITLE-ABS-KEY ("Passive defense" OR "Non-operating defense" OR "Inactive defense" OR Unarmed OR "Civilian defense" OR "Non-military Defense" OR "Preventive Measures") AND TITLE-ABS-KEY (War OR battle OR fight OR belligerence OR Threat OR menace OR military)
PubMed
("Passive defense"[Title/Abstract]) OR ("Non-operating defense"[Title/Abstract])) OR ("Inactive defense"[Title/Abstract])) OR (Unarmed[Title/Abstract])) OR ("Civilian defense"[Title/Abstract])) OR ("Non-military Defense"[Title/Abstract])) OR ("Preventive Measures"[Title/Abstract])) AND (War[Title/Abstract])) OR (battle[Title/Abstract])) OR (fight[Title/Abstract])) OR (belligerence[Title/Abstract])) OR (Threat[Title/Abstract])) OR (menace[Title/Abstract])) OR (military[Title/Abstract])
Google, Google Scholar, Grey literature, SID and Magiran
Combining two by two keywords together

The electronic literature search was conducted for studies published from 2005 up to June 2025. The year 2005 was selected as a significant global reference point, marking the beginning of updated passive defense strategies and the conceptual evolution of passive defense in many nations. The search was conducted without restrictions regarding geographical region or document type. In addition to the core database searches, a structured search for gray literature was performed using the advanced Google search engine. This involved targeting reports, technical documents, theses, conference proceedings, policy briefs, and official documents from relevant organizations, such as the WHO, specialized agency reports, governmental records, and NGO publications. The keywords employed for this specific search included terms, such as report, technical report, working paper, policy brief, conference proceedings, dissertation, and thesis. Crucially, no limitations were imposed on the "Title/Abstract" fields, operating under the logic that our intended results might sometimes serve as a secondary objective within broader studies. To enhance the sensitivity and comprehensiveness of the review, manual searching was also performed by examining the reference lists (bibliographies) of all identified relevant studies. Finally, the findings derived from the systematic review process were reported following the PRISMA (preferred reporting items for systematic reviews and meta-analyses) guidelines.

Study selection

Titles and abstracts of the identified studies were initially screened for relevance. Subsequently, full-text retrieval was initiated for articles whose abstracts did not provide sufficient information to definitively determine their eligibility (Figure 1).

The article assessment was conducted independently by two of the authors. Any discrepancies arising between the two reviewers were resolved through discussion or by consulting a third author to reach a consensus. Documents were then reviewed against the defined inclusion and exclusion criteria. During the full-text review, articles whose titles primarily addressed the general research problem but had a comparatively lower focus on the health research system were excluded from the study. Disagreements were resolved through discussion.

Inclusion and exclusion criteria

Inclusion criteria were peer-reviewed scientific articles published in either English or Persian, with accessible full text, examining passive defense in warfare, and evaluating interventions related to the health research system. Letters to the editor, editorials, books, retracted articles, duplicate information, and editorials—unless they provided novel information not covered elsewhere—were excluded. Studies discussing defense mechanisms in a general manner without specifying a particular country or type of passive defense strategy, as well as those without full-text access, were also not included.

Data extraction and analysis

The reviewers designed a data extraction template. They pilot-tested this template on a few identified records to ensure consistency and reached an agreement on the results. The required information extracted from all eligible articles included first author, year of publication, country, study title, and objective.

A total of 668 articles were initially identified in the primary search, including 529 records from database searching and 139 additional records from other sources. Subsequently, 379 duplicate records were identified and removed using EndNote software, leaving 289 records after duplicates were removed. Of these, 240 records were screened based on titles and abstracts, resulting in the exclusion of 102 records. One hundred thirty-eight full-text

articles were then assessed for eligibility. Following full-text review, 83 articles were excluded for various reasons. This review ultimately included 55 studies in the qualitative synthesis, with 31 studies included in the quantitative synthesis (meta-analysis).

Two independent reviewers examined the full text of the publications identified through the literature search for potential relevance or screened the titles and abstracts for inclusion in the review. If a disagreement arose, it was resolved in consultation with a third reviewer until consensus was achieved.

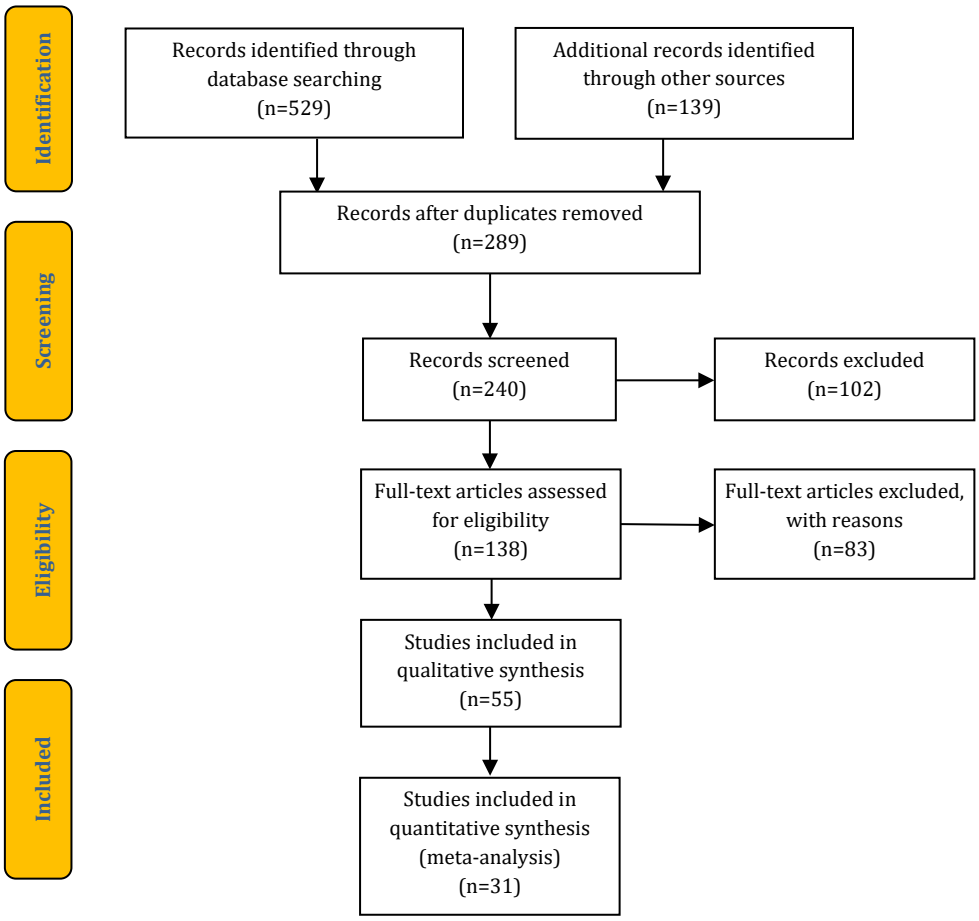

Figure 1. Flowchart of included studies based on the PRISMA guidelines

Findings

Following the selection of appropriate articles via the systematic review methodology, the full texts of the articles that passed the assessment phase and were deemed eligible for inclusion in the study were thoroughly examined (Table 2).

Table 2. Summary of the included studies

Author (year)	Attitude	Target
Darabi (2025) [10]	Futures-oriented and expert survey	Development of passive defense strategies for the country's non-military airports to counter biological threats using the SWOT technique
Pilkington (2024) [11]	Analysis on a case-by-case basis	Why Iran has prioritized passive defense in some areas over others
Shi *et al.* (2023) [12]	Based on pure reasoning	A review of related works from both passive defense and preventive defense perspectives
Ebrahimi Aligar *et al.* (2023) [13]	The research method is survey-based, descriptive, and analytical. According to the type of data used, it is of a mixed-method nature.	This study examines the extent to which passive defense principles influence air operation capability, with particular attention to the principle of training
Zawadzka et al. (2024) [14]	-	Illuminating the inherent challenges in preventing military-economic crimes under martial law in Ukraine
Foruzan (2024) [15]	The study employed a mixed structure and a descriptive-analytical approach.	An analysis of passive defense experiences and measures during the sacred defense period
Frozan (2023) [16]	The research employed a descriptive-exploratory method.	A comparative analysis of passive defense policy-making models for non-governmental industries across seven countries

Continue of Table 2 from the previous page

Narimani *et al.* (2023) [17]	Review study	The purpose of this study was to identify key factors related to the location, architecture, and vulnerability assessment of health and medical centers during crisis situations, as well as to reduce their susceptibility to various natural and man-made hazards and threats. It also aimed to determine critical issues associated with the passive defense approach
Poursamsam *et al.* (2023) [18]	Analytic Hierarchy Process (AHP)	Selected indicators influencing the location selection of essential goods warehouses
Qu *et al.* (2022) [19]	Case study	Identifying a defense framework with combined active and passive defense strategies
Abbasian & Shapoorian (2023) [20]	A descriptive-correlational using exploratory structural equations are used	Identifying the relationship between these factors to facilitate the management and provision of services to the wounded during war and potential crises with a passive defense approach
Messenger (2021) [21]	Based on purely analytical reasoning	Lessons learned from war and passive defense
Mirzadeh & Asgharzadeh (2021) [22]	A descriptive-survey in experts of passive defense and crisis management in military hospitals	Identify the challenges of passive defense in hospital environments and wartime conditions
Shahr Aieni *et al.* (2022) [23]	The research is qualitative using a three-stage Delphi method approved by experts	Explaining the effective factors on the passive defense doctrine of the Islamic Republic of Iran with a military approach
Mousavifard *et al.* (2022) [24]	A descriptive-analytical approach using documentary methods	Medical passive defense in biological attacks
Moradi & Firoozabadi (2021) [25]	Applied-developmental with a mixed approach, using a survey method and an expert panel.	This research aimed to identify the dimensions, components, and indicators of public security with passive defense considerations and to present a codified model in order to find the answer to the question, what is the strategic management model of public security with passive defense considerations?
Aghababaei *et al.* (2020) [26]	A cross-sectional descriptive study conducted on 15 hospital managers in Tehran.	The aim of this study was to assess the readiness of hospitals in Tehran regarding passive defense in the year 1397 (2018-2019)
Modiri et al. [27]	Qualitative and of content analysis type	It is the design of the crisis management building of Rafsanjan city with a passive defense approach
Monazami Tabar (2021) [28]	Survey study	It examines the role of factors related to the acceptance and implementation of passive defense in ICT by the traffic police of South Khorasan province
Tafteh & Kalantari (2019) [29]	A mixed method through both library and field methods and analyzed using the Likert scale	Explaining the role and position of passive defense in the defense strategy of the Islamic Republic of Iran
Abazari & Izadi Fard (2018) [30]	Based solely on reasoning	Explanation of passive defense in soft warfare, capacities of cyberspace in the field of religious education
Shaheen (2017) [31]	Using a descriptive method with a statistical population of 15 experts.	Identification of factors affecting the command and control system of passive defense
Doagooyan (2017) [32]	A practical descriptive-analytical in experts of passive defense, selected.	Systematizing strategic thinking of passive defense in the prevention of NAJA's ICT insecurities
Farzin (2022) [33]	This qualitative study uses grounded theory and deep interviews	What is the strategic model for implementing the general policies of passive defense in government organizations in the country?
Anvari (2019) [34]	In-depth interview	What is the strategic model for implementing the general policies of passive defense in government organizations of the country?
Jamali & Madani (2015) [35]	Expertise	Explaining the role of passive defense in deterring war
Shamohammadi & Mohammadinia (2015) [36]	Descriptive and case study	Data collection and processing that combines passive defense and technology, aiming to provide strategies for protecting national technology infrastructure at the strategic level
Akhbari (2015) [37]	Qualitative study	How can adherence to passive defense principles and regulations provide a suitable ground for improving and strengthening political management during crises?
Karami (2013) [38]	Review of experiences gained nationally and globally	Identifying the use of new technologies in various stages of incident crisis management in modern warfare
Barzegar & Lalalizadeh (2011) [39]	Purely based on argumentation/deduction	What negative role have Western computer games, as a soft war tool, played in the religious attitudes and beliefs of individuals, especially teenagers and young adults?
Nazarinejad & Pourshaseb 2020) [40]	A mixed quantitative and qualitative approach.	This study presents measures and strategies of passive defense to protect the critical infrastructures of the Islamic Republic of Iran

The components of passive defense refer to the main principles and elements that must be observed in the design and execution of defense projects and plans. The key principles and elements of passive defense are a set of engineering, managerial, and technical measures whose ultimate goal is to create resilience against threats. These components and elements of passive defense include seven items (Table 3).

Table 3. Components and elements of passive defense

Parameter	Description
Camouflage	The apparent concealment of facilities, equipment, and personnel from the sight of the enemy or threatening factors
Concealment	Hiding equipment by utilizing natural terrain features, vegetation cover, or artificial barriers
Deception	Misleading the enemy regarding the actual target, including the creation of decoys, false information, and temporary relocations
Dispersion	Appropriate spatial distribution of centers, facilities, and equipment to prevent their simultaneous destruction or vulnerability from a single attack
Hardening/resilience	Increasing the physical and structural resistance of facilities against the effects of threats (such as explosions)
Safety and sheltering	Ensuring the safety of staff and the population through the construction of shelters and safe havens and the creation of secure spaces
Backup/contingency	Planning for the temporary or permanent relocation of vital centers to predetermined locations under emergency conditions

The dimensions of passive defense generally referred to the domains and levels where protective measures must be implemented. These dimensions reflected the breadth of measures, ranging from the technical and structural design phase of infrastructure to the managerial layers, as well as the manner of training and culture-building within society and organizations, ensuring the entire country is immunized against threats. Based on scientific documents, the dimensions of the application scope of passive defense were categorized into nine key sectors (Table 4).

Table 4. Dimensions of passive defense

Parameter	Description
Cyber	Protecting vital information and communication infrastructures (such as banking networks, air traffic control systems, energy, and communication networks) against cyber-attacks
Biological	Countering and managing biological and biosecurity threats such as outbreaks of infectious diseases, bioterrorism attacks, or widespread environmental and hospital contaminations
Nuclear and radiation	Adopting necessary measures to reduce vulnerability to nuclear accidents, unintentional radiation exposure, and potential threats from nuclear weapons
Physical/structural	Engineering and structural measures in the design, site selection, and execution of development projects to increase the resistance of structures against physical attacks, explosions, and natural disasters
Economic	Reducing vulnerability in key economic areas such as financial systems, foreign exchange provision, production and distribution of essential goods, and maintaining economic stability during crises
Social and cultural	Including programs for maintaining public morale, managing public opinion, preventing rumors, and fostering social cohesion when facing crises and threats
Behavioral	Public education and community preparedness
Process	Evaluating and controlling the legal requirements for the implementation of declared policies
Structural	To increase the dependency and connections of human resources and other organizations

Passive defense is not merely a military matter but rather a managerial and technical approach that has applications in all infrastructural and service sectors of the country. The application domains of passive defense extended beyond military issues to cover all vital arteries of the nation. The most important areas of its application in scientific documents included four items (Table 5).

Table 5. Applications of passive defense in times of crisis and war

Domain	Specific sub-domain	Objective
Critical infrastructure	1. Energy (refineries, power plants, oil/gas transmission lines, and electricity distribution networks), 2. Transportation (airports, ports, railway stations, and main road networks), 3. Water (water treatment plants, dams, and main water supply networks)	Hardening, reducing vulnerability, and ensuring the survival of key centers. This is an engineering process aimed at increasing the resistance of vital structures and systems against various destructive energies (thermal, explosive, electromagnetic, and cyber)
Facilities and population centers	1. Treatment and health centers (hospitals and health crisis management centers, especially concerning biological defense), 2. Educational and cultural centers (schools, universities, and gathering places), 3. Government centers	Creating multiple layers of defense
Information and communications technology (ICT) sector	1. Data centers (servers and vital information), 2. Telecommunication networks, 3. Broadcasting (IRIB)	Utilization of anti-explosion engineering principles and backup mechanisms
Production and industry sector	1. Strategic factories (defense, pharmaceutical, food, and petrochemical industries)	Decentralized storage; Establishing continuity capability and post-disaster industrial management

The primary role of passive defense was to reduce the country's vulnerability to any military or non-military threat. Its key function, which directly involves preventing and neutralizing military surprise, was outlined along with a description of the roles passive defense plays (Table 6).

Table 6. Key roles of passive defense in times of war and crisis

Parameter	Description of function in preventing military surprise
Reducing infrastructure vulnerability	Designing key structures and facilities (such as bridges, power grids, and communication networks) with resistant materials and specific engineering to withstand the severity of impact and explosions. The goal is to prevent total destruction in the event of a surprise attack, allowing operational sections to remain functional
Delaying enemy operations	Using camouflage, concealment, and network redundancy to prevent the enemy from achieving its main objectives within the anticipated time frame. This disrupts the enemy's attack schedule and provides time for reaction
Protection of critical and sensitive centers	Creating fortified shelters, mobile or underground command rooms, and transferring sensitive equipment to secure locations. This ensures that decision-making and command centers remain active after a surprise attack
Maintaining readiness of support forces	Storing strategic reserves (fuel, consumables) in secure and dispersed locations, as well as training service personnel for the immediate commencement of reconstruction and relief operations. This prevents the complete collapse of operational support following an attack
Increasing reaction time	Public education and civil preparedness ensure that the community's initial response to chemical, radiological, or explosive attacks is faster than the time required for the enemy to fully deploy their effects. Also, designing early warning systems shifts the reaction time in favor of friendly forces
Mitigating the destructive effects of modern weapons	Focusing on countering modern threats such as electronic warfare, cyber-attacks, and precision-guided weapons. This includes protecting signals, strengthening shielding walls against electromagnetic pulses (EMP), and securing computer networks
Creating cover against advanced reconnaissance	Active use of decoys and active concealment systems to divert the enemy's attention and reconnaissance resources from real targets, especially in the initial hours of a crisis or before the main attack
Maintaining social order and ensuring continuity of public services	Designing water, gas, and energy networks with the ability to quickly isolate damaged sections and immediately connect to alternative resources (mobile or backup lines). This ensures that society and the military do not quickly face disruption in basic services
Engineering of command and backup communications	Establishing communication networks independent of conventional infrastructure (such as radio communications on different frequencies, backup fiber optics, or satellite) to prevent the paralysis of the command center if main communications are cut off via cyber or electromagnetic attacks
Limiting environmental and radiation effects	Preparing covered areas (shelters) with advanced air filtration systems to fully protect vital personnel and commanders against chemical, biological, and radiological agents. These measures prevent the enemy's unconventional attacks from causing widespread poisoning or contamination that would remove human resources from the scene
Psychological preparedness and public education	Military surprise is not just about a physical attack; It also includes psychological surprise of the community. Continuous public education on the correct way to take shelter, use protective equipment, and emergency protocols significantly reduces the effect of the psychological shock from an attack, enabling the community to respond effectively instead of being paralyzed
Protection of resources and supply chain	The vital role of passive defense is the strategic storage of necessary materials for the continuity of life and war (such as fuel, ammunition, medicine, and food) in protected, underground warehouses. These reserves ensure that the country can continue its operations for a determined period if supply routes are cut off during a surprise
Countering enemy soft war	Managing the virtual space, ensuring security, preserving social capital, establishing justice and responding to needs, and protecting the cohesion between the people and the government
Protecting civilian lives (citizen protection)	Protecting the public against direct attacks and chemical, biological, radiological, and nuclear attacks
Reducing overall damage and facilitating reconstruction and increasing resilience	Rapid return of society to normal conditions after the crisis ends or its intensity is reduced

Discussion

This article examined and explained the key roles and functions of civil defense in preventing and neutralizing military surprise based on a literature review. The role of civil defense in preventing and countering military surprise can be examined across 15 key axes.

The first vital role of civil defense is reducing the vulnerability of infrastructure. This strategy focused on the "hard" physical and engineering design to guarantee the inherent resistance of key facilities (power plants, telecommunication centers, and dams) against the enemy's initial strikes. The use of energy-absorbing materials, the installation of secondary structures, and placing sensitive equipment in protected environments prevent the complete destruction of infrastructure in a surprise attack, thus providing the necessary time for recovery. This strategy refers to hard physical design, and the goal is to create inherent resistance against all types of incoming attacks. In the design of critical infrastructure (such as power plants, main telecommunication centers, and dams), anti-explosion engineering principles are applied. The use of energy-absorbing materials, the installation of secondary structures to protect main components, and placing sensitive control equipment deep underground or inside heavily reinforced concrete enclosures ensure that the enemy's first blow does not completely take the facility offline and provides the necessary time to activate repair and recovery plans. Nazarinejad and Pourshaseb showed in a

study that taking civil defense measures in today's asymmetric wars to counter hostile incursions and reduce damage from the enemy's air, ground, and sea attacks is a fundamental issue whose scope covers all critical and sensitive military and non-military infrastructure, political, communication, command and control centers, and the civilian population [7]. Salahshur *et al.* showed in a study that employing civil defense principles is one of the most important measures for reducing the vulnerability of cities against enemy threats and military actions in urban areas [41].

The second role was delaying enemy operations by complicating targets. This is achieved through the extensive use of physical decoys (mock-ups of sensitive equipment), advanced radar camouflage, and active and passive concealment. The goal is for the enemy's detection systems to be confronted with a large volume of conflicting data, causing them to waste time and munitions on false targets, thereby delaying the main wave of the attack. This role disrupts the enemy's overall operation timeline by complicating their targeting process. As a result, precision munitions are expended, false targets are engaged, and ultimately, the main attack wave is delayed from reaching the primary strategic targets, creating an opportunity for a counter-response. Ahmadi Moghadam *et al.* identified five dimensions—cyber domain management, ensuring security, preserving social capital, establishing justice, and responding to needs—as useful for the civil defense model in this area [42].

The third role, protecting vital and sensitive centers, focuses on ensuring the continuity of the operation's brain. Command, control, and communication centers, as well as national data centers, must be made resilient against physical destruction through the construction of underground command fortresses, the use of mobile command systems, and the transfer of decision-making backups to remote, secure locations. These actions ensure that the backbone of the country's crisis management remains active even after severe strikes. The main objective is that even if the enemy succeeds in destroying surface centers, the backbone of the country's crisis management remains operational. Ahmadi Moghadam *et al.* stated that protecting critical infrastructure and key assets is among the most important duties and missions of the government, because their destruction or damage can easily jeopardize the continuation of a country's life and seriously endanger its political, economic, and defense security; civil defense is very useful in this regard [42].

The fourth role emphasizes maintaining the readiness of support forces. This is achieved through the strategic stockpiling of vital items (fuel, spare parts, and medical equipment) in multiple, inaccessible locations, as well as organizing rapid response maintenance teams, ensuring the country does not lose the ability to move to the second phase of defense and reconstruction. This role guarantees the continuation of operations after the attack. Furthermore, organizing rapid response teams for infrastructure maintenance and extensively training relief and support forces to operate in contaminated or destroyed environments ensure that the country retains the ability to transition to the second phase of defense and reconstruction after the initial attack ends. Minaei showed in a study that civil defense plays two very important roles in preserving, maintaining, and preparing personnel; civil defense plays the primary and essential role, and ignoring it results in severe vulnerability [43].

The fifth role is increasing community reaction time. This is achieved through extensive public education on how to properly respond to various types of attacks, use shelters, and prepare homes. The development of advanced early warning networks also allows the public and defense systems to gain critical seconds or minutes, preventing confusion and casualties caused by panic. This dimension elevates the response force from an organizational level to the citizen and individual level. Continuous public education on how to act correctly during various types of attacks (such as immediate notification, use of public shelters, and home preparedness) drastically reduces the time lost due to public confusion and panic. Moreover, the development and deployment of advanced early warning networks (auditory, visual, and cyber) that activate immediately upon threat detection allow defense systems and the public to gain critical seconds or minutes in their favor. Mansouri and Afqah showed in a study that civil defense can be resilient against external risks and shocks and possesses the ability to withstand and recover from these shocks with minimal cost [44].

The sixth dimension, reducing the destructive effects of modern weapons, is a direct response to cyber and electromagnetic threats. This involves installing physical shielding for sensitive electronic equipment and implementing distributed cyber architectures so that the nation's guidance, communication, and financial systems are not paralyzed by digital attacks. This role addresses the technological threats of the twenty-first century: cyber and electromagnetic attacks. The goal is to prevent the country's missile guidance, communication, and financial systems from being disabled by digital or jamming attacks during a military surprise.

The seventh role, creating cover against advanced detection, is carried out through strategic deception. By intentionally leaking false information into enemy channels and installing deceptive thermal and radar equipment, the enemy is forced to focus its valuable detection resources on fictitious targets, and the data collected by the enemy are strategically distorted. This role operates using "strategic deception" techniques. The goal is to compel the

enemy to focus its valuable detection assets (such as spy satellites and advanced drones) on unreal targets. This is achieved by intentionally leaking false information into enemy communication channels, installing deceptive thermal and radar equipment, and creating false optical and thermal networks in sensitive areas to strategically distort the data collected by the enemy. Kafi showed in his research that any organization possessing valuable information is vulnerable to advanced persistent threat techniques. Conversely, the more valuable the organization's information, the higher the probability of being targeted; in this case, civil defense strategies can be very important and helpful [45].

The eighth role, ensuring continuity of public services, requires the establishment of a "resilient" service network. Water and electricity systems must be designed so that damaged sections can be quickly supplied via backup lines or emergency sources, preventing a limited attack from escalating into social collapse. This goes beyond mere repairs and involves creating a truly resilient service network. For example, water and electricity networks must be designed so that damaged sections can be supplied without cutting off the entire system, using backup lines or emergency power generation sources (such as centralized or distributed generators). This prevents a limited strike from escalating into social collapse due to interruptions in water and energy, which can, in turn, lead to internal instability. Sheikhi and Ghahramani showed in their research that the goal of passive defense and its application is the continuity of underlying activities, securing vital needs, maintaining public services, and facilitating governance under threat conditions [46].

The ninth role, engineering command and backup communications, guarantees multi-layered communications independent of the main network. Communications must include fiber-optic layers, jamming-resistant radio, and emergency satellite communications so that command coordination remains possible even if the main networks are completely cut off. This role focuses on ensuring multi-layered communications independent of the main network. Communications must have various layers: Layer One (main fiber-optic network), Layer Two (jamming-resistant radio communications), and Layer Three (emergency satellite or encrypted messenger communications that do not require terrestrial infrastructure). This multiplicity ensures that even if the enemy succeeds in completely cutting off the main communication networks, senior commanders will still be able to coordinate forces.

The tenth role, limiting environmental and radiation effects, directly addresses unconventional threats (chemical and radiological). This includes deploying critical personnel in locations equipped with strong positive-pressure ventilation and filtration systems, as well as extensively training forces in anti-contamination protocols to prevent the rapid attrition of efficient human resources. This defensive measure counters unconventional threats. To respond effectively to chemical or radiological surprises, it is necessary for critical personnel to be stationed in locations offering the highest level of protection. Furthermore, training forces in anti-contamination protocols and fully equipping them with masks and protective suits prevents the rapid loss of skilled manpower. Pourian and Pourramazan showed in their research that overarching policies must be prepared by the country's Environmental Protection Organization in cooperation with the Passive Defense Organization to ensure the continuity of biological cycles, taking passive defense into account [47].

The eleventh role, psychological preparedness, defends against the psychological impact of surprise attacks. Regular training, periodic drills, and general public awareness of protocols encourage the community to respond by rapidly executing predetermined instructions rather than succumbing to panic, thereby neutralizing the enemy's psychological leverage. This aspect of passive defense targets the psychological dimension of surprise. A well-trained society does not suffer psychological paralysis under sudden attacks. Training should include periodic drills, awareness of danger signals, and instruction in first-response actions; this helps the community's initial reaction lean toward executing predetermined protocols instead of panic and chaos, neutralizing the enemy's psychological influence. Asghar Zade and Hasani showed in their research that by understanding the methods and techniques that affect people's minds and raising awareness in this field, the psychological factors of soft power can be managed within the domain of passive defense [48].

The twelfth role, protection of resources and supply chain, focuses on the continuity of national life. This is achieved by creating separate, infiltration-resistant strategic depots with temporary self-sufficiency capabilities so that the country can remain self-sufficient for an extended period if supply routes are completely cut off. Stockpiling strategic reserves does not merely mean storing materials; it means creating separate, infiltration-resistant storage points with temporary self-sufficiency. These protected depots (very deep or hidden) ensure that if supply routes are completely cut off and surface depots are destroyed by a surprise attack, the country can remain self-sufficient in terms of food, medicine, and ammunition for months and have the necessary resources for a counter-response. Khoshchehreh and Kaini showed in their research that passive defense can be very instrumental in food security, securing essential goods, and maintaining the supply chain [49].

The thirteenth and most extensive role is countering the enemy's soft war. This includes active defense in the informational space by monitoring and neutralizing disinformation campaigns, strengthening national cohesion, and implementing swift and transparent responses to rumors. The goal is to preserve social integrity and completely contain the enemy's surprise in the psychological and social dimensions. This broad dimension involves defense against informational and social disruption and consists of five axes, including cybersecurity: monitoring and neutralizing disinformation campaigns; ensuring social security: countering attempts to undermine public trust; preserving social capital: strengthening national cohesion against divisive efforts; establishing justice and accountability: swift transparency in responding to rumors to reduce discontent; and protecting cohesion: containing any attempt by the enemy to incite internal divisions. These measures neutralize the enemy's surprise in the psychological and social dimensions, allowing society to respond with unity. Countering the enemy's soft war, as one of the main pillars of passive defense, focuses on maintaining the mental, psychological, and social health of society against the enemy's psychological operations, destructive propaganda, cultural infiltration, and cyber operations. This area includes measures to strengthen national cohesion, teach media literacy, produce convincing content, and rapidly identify and neutralize false or divisive narratives so that national will and public trust in the country's core structures and values are not undermined during a crisis. Ahmadi Moghadam *et al.* demonstrated in their research that one of the novel methods of passive defense is a people-centered passive defense, whose primary mission is to protect the cohesion between the people and the government in the soft war [42].

The fourteenth role, protection of civilian lives, is considered the most primary and urgent duty of passive defense. Its goal is to minimize human casualties against all direct and indirect threats—military, chemical, biological, and cyber. This is ensured through establishing public preparedness mechanisms, timely danger detection and signaling, emergency evacuation management, creating and equipping safe shelters, and providing immediate essential needs such as food, water, and medical services in safe areas, thereby preserving citizen survival under wartime conditions.

Finally, the fifteenth role, damage reduction and restoration of resilience, has a long-term and strategic nature, focusing on safeguarding the country's vital infrastructure, such as power grids, water, communications, transportation, and key industries. This is achieved by implementing passive defense designs, such as reinforcing structures, camouflage, and concealment of critical facilities, as well as developing operational plans for the rapid return of damaged sectors to the production and service cycle after the threat ends or successful attacks. Ultimately, this strengthens the country's overall capacity to withstand and quickly recover from the consequences of war.

Conclusion

Passive defense is a proactive, multi-layered strategy that strengthens national resilience by reducing vulnerabilities and preventing attacks from escalating.

Acknowledgments: The authors thank Kerman University of Medical Sciences.

Ethical Permissions: This article was reviewed at Kerman University of Medical Sciences and approved with the ethics code IR.kmu.REC.1403.109.

Conflicts of Interest: The authors declared no conflicts of interest.

Authors' Contribution: Moradpour AM (First Author), Introduction Writer/Methodologist/ Assistant Researcher/ Discussion Writer/Statistical Analyst (35%); Sadeghi R (Second Author), Introduction Writer/Methodologist/ Assistant Researcher/Discussion Writer/Statistical Analyst (30%); Bamir M (Third Author), Introduction Writer/Methodologist/Main Researcher/Discussion Writer/Statistical Analyst (35%)

Funding/Support: This study did not receive funding from any organization or individual, and the applicant will be exempt if the article is accepted.

References

1- Morad Pirii H, Khazraei H. The role of new information technologies in future wars. Soft Power Stud. 2021;10(2):159-77. [Persian]

2- Riyazi V, Akbari A, Bajlani S, Akbari HR. Introduction of the components and tools of the US hybrid war against the IR of Iran. Sci Q J Def Strategy. 2021;19(1):37-67. [Persian]

3- Khaleghi Nejad A, Ruhollahi M, Bahador R. HSE management system, passive defence and its role in sustainable development. Proceedings of the National Conference on Passive Defence and Sustainable Development. Tehran: Ministry of Interior; 2016. [Persian]

4- Mahdavizadeh M, Khalafzadeh R. The role of passive defense in countering bioterrorism attacks in the armed forces. J Sci Promot. 2021;8(29):27-50. [Persian]

5- Minaie M, Hossein Zadeh M, Begheri Pour M. The effects of passive defense in modern NBC warfare. Passiv Def Q. 2011;2(3):37-51. [Persian]

6- Mojoodi M, Alizadeh Q, Ebrahimian M. Bioterrorism and biological warfare, from the past to the present: A classic review. War Stud. 2019;1(3):107-30. [Persian]

7- Moradpour AH, Sadeghi R, Bamir M. Passive Defense as a Deterrence Strategy: A Review of Its Roles and Functions in Preventing Military Surprise in the Health and Non-Health Sectors. Iran J War Public Health. 2026;18(2):1001-9.

8- Atash Panjeh H, Parbin Z, Dastdadeh F. Passive defense threats and measures in crisis management. Proceedings of the National Conference on Passive Defense and Sustainable Development. Tehran: Ministry of Interior; 2016. [Persian]

9- Kohkan A, Jadidi Narges. An introduction to passive defense and its place in foreign policy: Background to

sustainable development. Proceedings of the National Conference on Passive Defense and Sustainable Development. Tehran: Ministry of Interior; 2016. [Persian]
10- Darabi M, Ataee Kachoee MH, Arefnia MH, Farhadinia A. Passive defense strategies for critical infrastructure against biological threats by SWOT method (case study: Civilian airports). Mil Manag. 2025;25(97):194-233. [Persian]
11- Pilkington AR. Military, political, cultural, and societal implications of the Islamic Republic of Iran's passive defense strategy [dissertation]. Denver: University of Denver; 2024.
12- Shi C, Peng J, Zhu S, Ren X. From passive defense to proactive defence: Strategies and technologies. In: Artificial intelligence security and privacy. Singapore: Springer; 2023. p. 190-205.
13- Ebrahimi Aligar M, Sharifan E, Zarvandi J. The role of passive defense principles on air operations capability with emphasis on the principle of training. Mod Aviat Technol. 2023;2(1):17-26. [Persian]
14- Zawadzka M, Lis A, Marszałkowska-Jakubik J, Szymański P, Peng Jr. Evaluation of soldiers' knowledge and sense of threats regarding exposure to biological risk factors at the place of service. Healthcare. 2024;12(17):1777.
15- Foruzan H. Lessons learned from passive defense in the field of vulnerability reduction the time frame of holy defense. Holy Def Stud. 2024;10(3):9-35. [Persian]
16- Frozan H, Ataee Kachoee MH, Araghizadeh M, Rezaei M, Eghdam E. A comparative study of passive defense policy models of non-governmental industries in chosen countries. Strateg Def Stud. 2023;21(94):77-102. [Persian]
17- Narimani K, Ghadrpouran S, Ganji M. Pathology of health and treatment centers in terms of passive defense: A review study. J Combat Med. 2023;6(2):86-92. [Persian]
18- Poursamsam H, Akbari E, Momeni K. The approach of passive defense in the location of essential items storage with the help of AHP. Passiv Def Q. 2023;14(4):101-10. [Persian]
19- Qu Z, Shi H, Wang Y, Yin G, Abu-Siada A. Active and passive defense strategies of cyber-physical power system against cyber attacks considering node vulnerability. Processes. 2022;10(7):1351.
20- Abbasian M, Shapoorian S. Presenting a model to identify the relationship between effective factors in the construction and establishment of field hospitals with a passive defense approach. Sci J Passiv Def. 2023;14(4)-75-83. [Persian]
21- Messenger DA. Local government, passive defense and aerial bombardment in Barcelona during the Spanish Civil War, 1936-9. J Contemp Hist. 2021;56(4):1084-101.
22- Mirzadeh S, Asgharzadeh A. Passive defense challenges in hospital space and combat conditions. Nurse Physician War. 2021;9(30):13-9. [Persian]
23- Shahr Aieni SS, Sepehri Rad A, Riyazi V, Hemmat H. Explaining the factors influencing the formulation of the passive defense doctrine of the Islamic Republic of Iran based a military approach. Mil Sci Tactics. 2022;18(60):223-43. [Persian]
24- Mousavifard SMR, Khodayar H, Bijani M, Romanan F. Prospective research of medical passive defense in biological attacks emphasizing the hypothesis of corona bioterrorism. Med Law J. 2022;16(57):1001-16. [Persian]
25- Moradi R, Firoozabadi SH. Strategic model of public security of the country with emphasis on passive defense. Strateg Def Stud. 2021;19(85):177-200. [Persian]
26- Aghababaei M, Hosseini SM, Maher A. Assessment of hospital preparedness of Tehran University of Medical Sciences for implementation of non-operational defense strategies from the viewpoint of managers. Passiv Def Q. 2020;11(1):37-50. [Persian]
27- Modiri M, Ahadnejad M, Hosseini A. Risk management in human made crises with passive defense approach (case study: Tehran). Res Urban Plan. 2017;7(27):163-82. [Persian]
28- Monazami Tabar J. Investigating the factors related to the acceptance and application of passive defense in ICT: A case study of highway patrol and traffic control (known as RAHVAR) police officers in the border areas of south Khorasan. Passiv Def Q. 2021;11(4):47-58. [Persian]
29- Tafteh G, Kalantari F. Passive defense in the IRI's defensive strategy: Role and position. Strateg Def Stud. 2019;16(74):99-116. [Persian]
30- Abazari MH, Izadi Fard AA. Passive defense in cyberspace and explaining the role of governments and religious institutions. Int Multidiscip J Pure Life. 2018;5(15):149-77. [Persian]
31- Shaheen S. Exploring factors influencing the evolution and stability of command control systems in small nuclear weapon states [dissertation]. London: King's College London; 2017.
32- Doagooyan D. Strategies of passive defense to prevent vulnerability of FAVA NAJA (Cyber Police). J NAJA Strateg Stud. 2017;2(4):87-108. [Persian]
33- Farzin M, Vahidi A, Bagheri A. The model of strategic monitoring for the implementation of general policies. Q J Macro Strateg Policies. 2022;10(37):2-40. [Persian]
34- Anvari G. Obstacles to the implementation of overall policies of passive defense in govermental organizations. Strateg Def Stud. 2019;17(76):233-58. [Persian]
35- Jamali A, Madani SM. The role of passive defense in the deterrence of war. Sci Q J Def Strateg. 2015;13(3):171-206. [Persian]
36- Shamohammadi M, Mohammadinia R. Passive defense strategy in technology. Strateg Def Stud. 2015;13(59):121-43. [Persian]
37- Akhbari M, Ahmadi Moghaddam M. Passive defense in urban management. Int Q Geopolit. 2015;10(34):36-69. [Persian]
38- Karami A. Passive defense in new warfare, impact of novel technologies. Nurse Physician War. 2013;(21-22):37-42. [Persian]
39- Barzegar E, Lalalizadeh M. Anti-Islamic computer games and passive defense. Soft Power Stud. 2011;1(1):93-117. [Persian]
40- Nazarinejad AA, Pourshaseb AA. Adopt passive defense strategies to protect the critical infrastructure of the Islamic Republic of Iran. Strateg Def Stud. 2020;18(82):313-36. [Persian]
41- Salahshur Z, Ahmadian M, Alizadeh K. Evaluating the level of vulnerability of urban infrastructures with a passive defense perspective (case study: Shirvan). Geography. 2022;20(72):137-53. [Persian]
42- Ahmadi Moghadam I, Hosseini H, Forouzan H, Tahmasebi P. Presenting a strategic model of people-centered passive defense in confronting the enemy's soft war. Strateg Def Stud. 2023;21(93):147-68. [Persian]
43- Minaei H. The importance of human resources in passive defense. Mil Sci Technol. 2010;7(18):77-96.
44- Mansouri SA, Afghah SM. Investigating Iran's economic and social resilience with a passive defense approach. Def Econ Sustain Dev. 2018;2(6):73-98. [Persian]

45- Kafi S. Passive defense strategies against advanced persistent threats in the cyber environment. J Def Policy. 2016;23(1):51-71. [Persian]

46- Sheikhi A, Ghahramani A. Identifying and prioritizing culture producing strategies in passive defense. Superv Insp. 2017;11(41):97-120. [Persian]

47- Pourian MT, Pourramazan E. The role of passive defense in environmental security. Passiv Def Secur. 2012;1(1):7-28. [Persian]

48- Asghar Zade M, Hasani H. The role of psychological factors of soft power in the field of passive defense. J Sci Promot. 2014;3(10):53-78. [Persian]

49- Khoshchehreh M, Kaini MR. Strategic and efficient factors in securing basic needs (food) from the passive defense standpoint with the focus on the resistive economy. Strateg Def Stud J. 2017;15(69):251-74. [Persian]