Passive Defense as a Deterrence Strategy: A Review of Its Roles and Functions in Preventing Military Surprise in the Health and Non-Health Sectors

Abstract

Aims: This paper presents a review of the functions and roles of Passive Defense in strengthening non-offensive deterrence and reducing vulnerability.

Method: This systematic review was conducted to comprehensively gather related literature, spanning from the conceptual evolution of Passive Defense (2005) up to the year 2025. No geographical or document type restrictions were imposed. Electronic searches were performed across three specialized databases (Web of Science, Scopus, PubMed), two general search engines (Google Scholar, Google), and Persian databases (SID, 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 literature review revealed that the role of Passive Defense in preventing and countering military surprise can be delineated across fifteen key axes. The most critical application areas identified in the scientific documents fall into four main categories that form the foundation of defense strategies. Moreover, the dimensions of Passive Defense in these studies are categorized into nine key sections, and the fundamental elements and components of Passive Defense, which specify the executive requirements, collectively comprise seven vital components.

Conclusion: it functions as an active, multi-layered strategy that ensures national resilience against military surprise. This approach prevents a limited attack from escalating into a strategic catastrophe by reducing physical and cyber vulnerabilities and disrupting the enemy's timing. also guarantees national survival and the continuity of sovereignty under novel threat conditions.

Keywords: Passive Defense, Military Surprise, Defense Strategy, Review Study

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 (4). 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.(٦)

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

In Press

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.(۸)

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 damages, 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).

Passive defense has consistently been regarded as one of the most effective and sustainable means of protection against various threats. Its ultimate goal is to ensure the continuity of essential infrastructures, meet vital needs, maintain public services, and enable delivery of assistance with minimal damage and disruption.(۱۰)

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 seeks to conduct a comprehensive review to identify the dimensions, components, functional domains, and implications of passive defense in preventing military surprise.

Materials and Methods

Literature Search and Search Strategy

The search strategy for this study encompassed both electronic database searching and manual searching. This combined approach included: (a) electronic searches across three major bibliographic databases and two search engines, and (b) forward/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 grey literature sources. The keywords utilized in this search are detailed as follows:

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

In Press

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 concerning geographical region or document type. In addition to the core database searches, a structured search for grey 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

For a visual representation of the search and screening process, please refer to Figure 1. 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.

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:

Must be a peer-reviewed scientific article.

Must be published in either English or Persian.

The full text of the article must be accessible.

Articles must examine Passive Defense in Warfare.

The study must evaluate interventions pertaining to the health research system.

Exclusion Criteria:

Studies published as letters to the editor, editorials, or books.

Retracted articles.

Duplicate information.

Editorials, unless they provided novel information not covered elsewhere.

In Press

Articles for which full-text access was not possible.
Studies that discussed defense mechanisms in a general manner without specifying a particular country or type of passive defense strategy.

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.

As illustrated in the PRISMA flowchart, a total of 668 articles were initially identified in the primary search. Subsequently, 379 duplicate records were identified and removed using EndNote software. 234 references were eliminated following the title and abstract screening. 57 references were retrieved after deduplication. The full text of 55 articles was successfully retrieved and assessed. This review ultimately included 32 studies after the screening process (Figure 1).

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 the third reviewer until consensus was achieved.

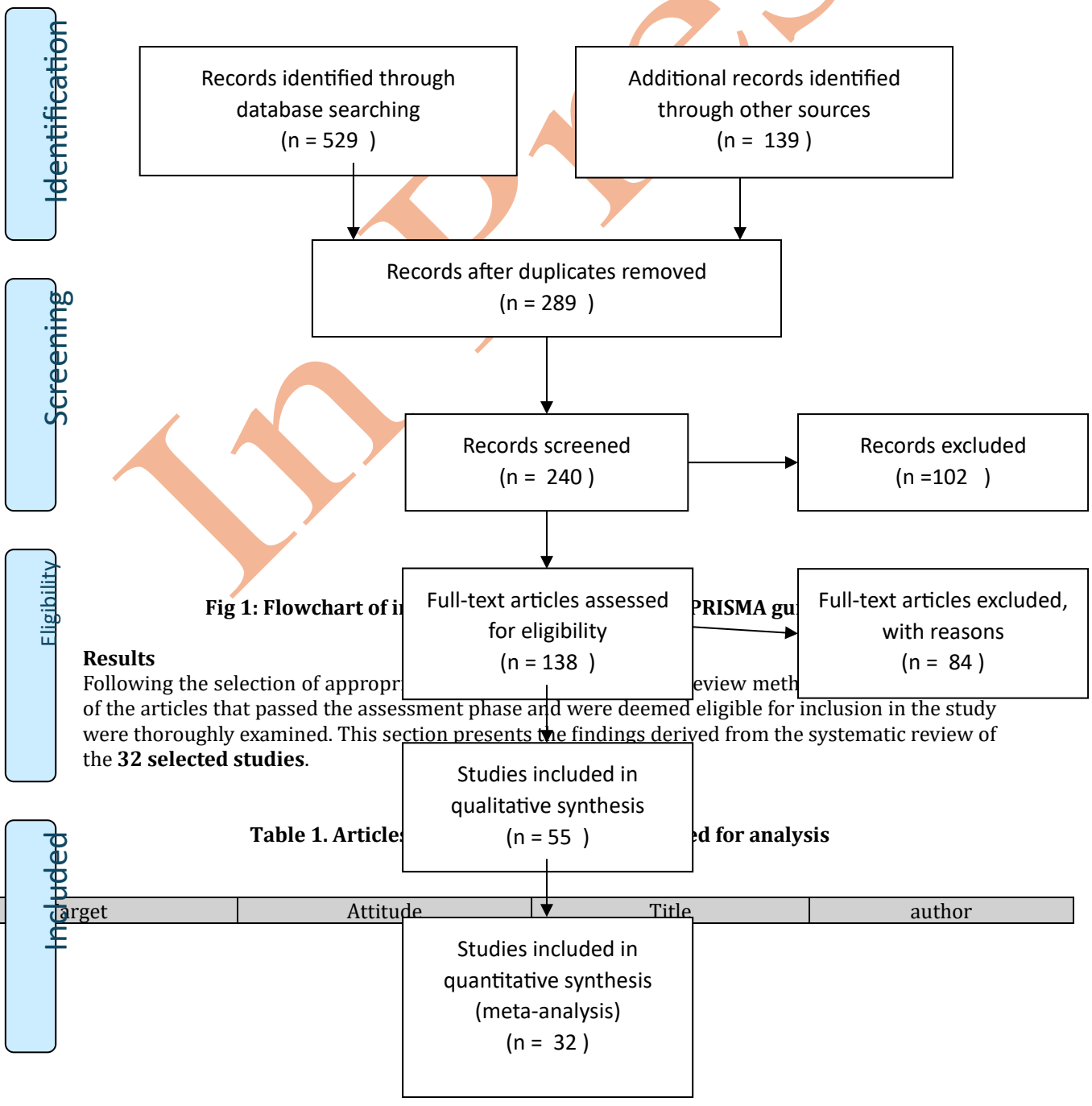

Fig 1: Flowchart of i PRISMA gu

Results

Following the selection of appropr eview meth of the articles that passed the assessment phase and were deemed eligible for inclusion in the study were thoroughly examined. This section presents the findings derived from the systematic review of the **32 selected studies**.

Table 1. Article ed for analysis

arget	Attitude	Title	author

In Press

			(سال)
Development of passive defense strategies for the country's non-military airports to counter biological threats using the SWOT technique.	Futures-oriented and expert survey	passive defense strategies for critical infrastructures to counter biological threats using the SWOT technique (Case study: non-military airports)	Darabi (2025)
Why Iran Has Prioritized Passive Defense in Some Areas Over Others	Analysis on a case-by-case basis	Military, Political, Cultural, and Social Implications of the Passive Defense Strategy of the Islamic Republic of Iran:	Aaron R. Pilkington (2024)
A Review of Related Works from Both Passive Defense and Preventive Defense Perspectives	Based on Pure Reasoning	From Passive Defense to Preventive Defense: Strategies and Technologies	Chung Xi (2024)
This study examines the extent to which passive defense principles influence air operation capability, with particular attention to the principle of training.	The research method is survey-based, descriptive, and analytical. According to the type of data used, it is of a mixed-method nature. Data and information were collected through library and field methods, utilizing questionnaires, note-taking forms, and library records.	The Role of Passive Defense Principles in Air Operation Capability with Emphasis on the Principle of Training	Ebrahimi (2024)
Illuminating the Inherent Challenges in Preventing Military-Economic Crimes under Martial Law in Ukraine	-	Prevention of War and Economic Crimes under Martial Law in Ukraine	Zawadzka. (2024)
Awareness of the Level of Threats	Survey	Assessment of Soldiers' Knowledge and Perception of Threat Regarding Exposure to Biological Risk Factors in the Workplace	Marsalkowska (2024)
An Analysis of Passive Defense Experiences and Measures during the Sacred Defense Period	The study employed a mixed structure and a descriptive-analytical approach. To collect theoretical findings, document analysis and expert interviews were used	Lessons Learned from Passive Defense in the Field of Vulnerability Reduction during the Sacred Defense Period	Forouzan (2024)

In Press

A Comparative Analysis of Passive Defense Policy-Making Models for Non-Governmental Industries across Seven Countries	The research employed a descriptive-exploratory method, including library and documentary studies, as well as expert opinions collected through a structured closed-ended questionnaire	A Comparative Study of Passive Defense Policy-Making Models in Non-Governmental Industries of Selected Countries	Forouzan (2023)
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	Review Study	Pathology of Health and Medical Centers from a Passive Defense Perspective: A Review Study	Narimani (2022)
Selected indicators influencing the location selection of essential goods warehouses	Analytic Hierarchy Process (AHP)	Passive Defense Approach in the Location Selection of Essential Goods Warehouses Using AHP	Poursamsam (2022)
Identifying a defense framework with combined active and passive defense strategies	Case study	Active and passive defense strategies of cyber-physical power system against cyber attacks considering node vulnerability	Zhengwei Kuo (2022)
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	descriptive-correlational in which exploratory structural equations are used.	Identifying the relationship between effective factors in the construction and establishment of field hospitals with a passive defense approach	Abbasian (2022)
Lessons learned from war and passive defense.	Based on purely analytical reasoning	Local Government, Passive Defense, and Aerial Bombing in Barcelona During the Spanish Civil War, 1936–1939	Messenger (2021)

In Press

Identify the challenges of passive defense in hospital environments and wartime conditions.	The research method is descriptive-survey. The statistical population of the study consists of experts in the field of passive defense and crisis management in military hospitals.	Challenges of Passive Defense in Hospital Settings and Combat Conditions	Mirzadeh (2021)
Explaining the effective factors on the passive defense doctrine of the Islamic Republic of Iran with a military approach.	The research is qualitative, and data collection was conducted through library studies by reviewing documents and records. Finally, their validation was performed using a three-stage Delphi method approved by experts	Explaining the effective factors in the formulation of the passive defense doctrine of the Islamic Republic of Iran with a military approach	Shahraini (2021)
Medical passive defense in biological attacks	This research has been conducted with a descriptive-analytical approach using documentary methods referring to library and online sources	Future Studies of Medical Passive Defense in Biological Attacks with an Emphasis on the Bioterrorism Hypothesis of Coronavirus	Mousavi Fard (2021)
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?	The type of research was applied-developmental with a mixed approach, which was conducted using a survey method and an expert panel. To achieve the goals of this research, it was first conducted by reviewing the research literature, upstream documents, and conducting interviews with elites.	The strategic management model of the country's public security with an emphasis on passive defense	Rostami (2020)
The aim of this study was to assess the readiness of hospitals in Tehran regarding passive defense in the year 1397 (2018-2019)	This study is a cross-sectional descriptive study conducted on 15 hospital managers in Tehran. The sampling method was a census, and the data collection tool was a four-part researcher-made questionnaire. Data analysis was performed using SPSS23 software and descriptive and analytical statistical tests, including Spearman correlation, univariate regression, and t-test.	Assessing the readiness of the hospitals affiliated with Tehran University of Medical Sciences for implementing passive defense strategies from the perspective of managers	Agha Babai (2020)
It is the design of the crisis management building of Rafsanjan city with a passive defense approach.	Qualitative and of content analysis type	Designing a crisis management building with a passive defense approach	
It examines the role of factors related to the acceptance and	Survey study	Investigating factors related to the acceptance	Manteghi Tabar (2020)

In Press

implementation of passive defense in ICT by the traffic police of South Khorasan province.		and implementation of passive defense in ICT (a case study of traffic police employees in the border areas of South Khorasan)	
Explaining the role and position of passive defense in the defense strategy of the Islamic Republic of Iran.	This study uses a mixed method; data were collected through both library and field methods and analyzed using the Likert scale.	The role and position of passive defense in the defense strategy of the Islamic Republic of Iran	Goodarztafteh (2018)
Explanation of passive defense in soft warfare, capacities of cyberspace in the field of religious education.	Based solely on reasoning	Passive defense in cyberspace and explaining the role of governments and religious institutions	Abazari (2018)
Identification of factors affecting the command and control system of passive defense	Using a descriptive method with a statistical population of 15 experts, and utilizing library resources, questionnaires, and interviews with experts	Explanation of the factors influencing the command and control system of the passive defense organization	Jalali Farahani (2018)
Systematizing strategic thinking of passive defense in the prevention of NAJA's ICT insecurities."	The research method used in this study is practical and, in terms of execution, descriptive-analytical. The statistical population consists of professors and experts in the field of passive defense, selected using Morgan's table through stratified probabilistic sampling. The data collection tool is a researcher-made questionnaire.	Passive defense strategies in preventing vulnerability of NAJA's ICT."	Dabagiyan (2017)
What is the strategic model for implementing the general policies of passive defense in government organizations in the country?"	This qualitative study uses grounded theory and deep interviews	A Strategic Model for Implementing General Policies of Passive Defense in Governmental Organizations	Anwari (2016)
This study presents measures and strategies of passive defense to protect the critical infrastructures of the Islamic Republic of Iran.	The research method in the present study adopts a mixed approach (quantitative and qualitative) and uses documentary and survey methods. Data collection was conducted through library studies and field research.	Measures and Strategies of Passive Defense in Protecting the Critical Infrastructures of the Islamic Republic of Iran	Nazarinejad (2016)
What is the strategic model for implementing the general policies of passive defense in government organizations of the country?	In-depth Interview	Strategic Model for Implementing General Policies of Passive Defense in Government Organizations	Mohammadi Nia (2016)
Explaining the role of passive defense in deterring war	Expertise	The role of passive defense in deterring war	Jamali (2015)

In Press

Data collection and processing that combines passive defense and technology, aiming to provide strategies for protecting national technology infrastructure at the strategic level	Descriptive and Case Study	Passive Defense Strategies in the Field of Technology	Shah Mohammadi (2015)
How can adherence to Passive Defense principles and regulations provide a suitable ground for improving and strengthening political management during crises?	Qualitative Study	Passive Defense and Political Management	Rad Goudarzi (2014)
Identifying the use of new technologies in various stages of incident crisis management in modern warfare.	Review of experiences gained nationally and globally	Passive Defense in Modern Warfare, The Role of New Technologies	Karami (2013)
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?	Purely based on Argumentation/Deduction	Soft War, Anti-Islamic Computer Games, and Passive Defense	Barzegar (2011)

In Press

Components (Elements) of Passive Defense

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 **7 items**, which are:

Table 2: Components and elements of passive defense

Description	Component (Element)	Row
The apparent concealment of facilities, equipment, and personnel from the sight of the enemy or threatening factors.	Camouflage	1
Hiding equipment by utilizing natural terrain features, vegetation cover, or artificial barriers.	Concealment	2
Misleading the enemy regarding the actual target, including the creation of decoys, false information, and temporary relocations.	Deception	3
Appropriate spatial distribution of centers, facilities, and equipment to prevent their simultaneous destruction or vulnerability from a single attack.	Dispersion	4
Increasing the physical and structural resistance of facilities against the effects of threats (such as explosions).	Hardening/Resilience	5
Ensuring the safety of staff and the population through the construction of shelters and safe havens, and the creation of secure spaces.	Safety and Sheltering	6

Planning for the temporary or permanent relocation of vital centers to predetermined locations under emergency conditions.	Backup/Contingency	7

Dimensions of Passive Defense

The dimensions of passive defense generally refer to the domains and levels where protective measures must be implemented. These dimensions reflect 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 are categorized into 9 key sectors:

Table 3: Dimensions of passive defense

Description	Domain	Row
Protecting vital information and communication infrastructures (such as banking networks, air traffic control systems, energy, and communication networks) against cyber-attacks.	Cyber	1
Countering and managing biological and biosecurity threats such as outbreaks of infectious diseases, bioterrorism attacks, or widespread environmental and hospital contaminations.	Biological	2
Adopting necessary measures to reduce vulnerability to nuclear accidents, unintentional radiation exposure, and potential threats from nuclear weapons.	Nuclear and Radiation	3
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.	Physical/Structural	4
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.	Economic	5
Including programs for maintaining public morale, managing public opinion, preventing rumors, and fostering social cohesion when facing crises and threats.	Social and Cultural	6
Public education and community preparedness.	Behavioral	7
Evaluating and controlling the legal requirements for the implementation of declared policies.	Process	8
To increase the dependency and connections of human resources and other organizations.	Structural	9

Applications of Passive Defense

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 extend beyond military issues to cover all vital arteries of the nation. The most important areas of its application in scientific documents include the following 4 items:

Table 4: Applications of passive defense in times of crisis and war

Objective	Specific Sub-Domain	General Domain	Row
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	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	Critical Infrastructure	1

In Press

against various destructive energies (thermal, explosive, electromagnetic, and cyber).	treatment plants, dams, and main water supply networks)		
Creating multiple layers of defense.	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	Facilities and Population Centers	2
Utilization of anti-explosion engineering principles and backup mechanisms.	1. Data Centers (Servers and vital information) 2. Telecommunication Networks 3. Broadcasting (IRIB)	Information and Communications Technology (ICT) Sector	3
Decentralized storage; establishing continuity capability and post-disaster industrial management.	1. Strategic Factories (Defense, pharmaceutical, food, and petrochemical industries)	Production and Industry Sector	4

Passive defense roles

Key roles of passive defense: The key role of passive defense is to focus on reducing the country's vulnerability to any military or non-military threat. The key role of passive defense, which is directly related to preventing and neutralizing military surprise, is mentioned in this table along with the description of the roles of passive defense in preventing military surprise."

Table 5: Key roles of passive defense in times of war and crisis

Row	Role Title	Description of Function in Preventing Military Surprise
1	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.
2	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.
3	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.
4	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.
5	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.

In Press

		Also, designing early warning systems shifts the reaction time in favor of friendly forces.
6	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.
7	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.
8	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.
9	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.
10	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.
11	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.
12	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.
13	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.
14	Protecting Civilian Lives (Citizen Protection)	Protecting the public against direct attacks, and chemical, biological, radiological, and nuclear attacks.
15	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

In Press

In a surprise attack scenario, where the reaction time of combat forces is limited, the successful performance of civil defense turns into a decisive factor in converting a strategic defeat into a manageable situation. This article examines and explains 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 fifteen key axes.

The first vital role of civil defense is reducing the vulnerability of infrastructure. This strategy focuses 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 prevents 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 used. The use of energy-absorbing materials, the installation of secondary structures against the destruction of main components, and placing sensitive control equipment deep underground or inside heavily reinforced concrete enclosures ensures that the enemy's first blow does not completely take the facility offline and provides the necessary time to activate repair and recovery plans. Nazari Nezhad and Abdolalipour (1399) 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 (10). Alizadeh et al. (1401) 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 (11).

The second role is 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 faced with a large volume of conflicting data, leading them to waste their 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 targets for them. This results in the expenditure of precision munitions, engagement with false targets, and ultimately, a delay in the main attack wave reaching the primary strategic targets, creating an opportunity for a counter-response. Ahmadi Moghaddam et al. (1402) considered five dimensions (cyber domain management, ensuring security, preserving social capital, establishing justice, and responding to needs) useful for the civil defense model in this area (12).

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. Zarqani et al. (1390) 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 (13).

The fourth role emphasizes maintaining the readiness of support forces. This is achieved through the strategic stockpiling of vital items (fuel, spare parts, 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 part guarantees the continuation of operations after the attack. Furthermore, organizing rapid response teams for infrastructure maintenance and extensive training of relief and support forces to work in contaminated or destroyed environments ensure that the country retains the ability to move to the second phase of defense and reconstruction after the initial attack ends. Minaei (1390) 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 means severe vulnerability (15).

In Press

The fifth role is increasing community reaction time. This is achieved through extensive public education on how to properly act against various types of attacks, using shelters, and home preparedness. The development of advanced early warning networks also allows the public and defense systems to gain critical seconds or minutes in their favor, preventing confusion and casualties caused by panic. This dimension elevates the response force from an organizational level to a citizen and individual level. Continuous public education on how to act correctly against 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) immediately upon threat detection allow defense systems and the public to gain critical seconds or minutes in their favor. Mansouri and Afqah (1396) showed in a study that civil defense can be resilient against external risks and shocks and possess the ability to withstand and pass through these shocks with minimal cost (16).

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 is a direct response to 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 paralyzed in the face of military surprise through digital or jamming attacks. Karami et al. (1392) showed in a study that if crisis management is summarized in four stages—prevention, preparedness, response, and reconstruction—then with a better understanding of the effects of biological weapons and the necessary preparedness in the civil defense sector, not only will the resulting damages be minimized, but the speed of reconstruction and return to the initial state will increase significantly (17).

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 area 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 done 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 (1394) 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 the organization being threatened; in this case, civil defense strategies can be very important and helpful (18).

The eighth role, Ensuring Continuity of Public Services, requires the establishment of a "Resilient" Service Network. Water and electricity networks must be designed so that damaged sections can be quickly supplied via backup lines or emergency sources, preventing a limited attack from turning into social collapse. This goes beyond mere repairs and involves creating a "resilient" service network. For example, water and electricity networks must be designed so that damaged sections can be supplied without cutting off the entire network, using backup lines or emergency power generation sources (such as centralized or distributed generators). This prevents a limited strike from escalating into a social collapse due to the interruption of water and energy, which can itself lead to internal instability. Ghahramani et al. (1396) showed in their research that the goal of passive defense and its application is the continuity of underlying activities, securing vital needs, the continuation of public services, and facilitating the governance of the country under threat conditions, etc. (19).

Role 9: Engineering Command and Backup Communications, The ninth axis, 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 is possible even if the main networks are completely cut off. This task 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 a terrestrial infrastructure). This

In Press

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. Pourshasab and Nazari Nejad (1399) showed in their research that the role of passive defense in communication and information infrastructure and main networks is ranked second among Iran's infrastructures (20).

Role 10: Limiting Environmental and Radiation Effects, The tenth role, Limiting Environmental and Radiation Effects, directly addresses unconventional threats (chemical/radiological). This includes deploying critical personnel in locations with strong positive-pressure ventilation and filtration systems, as well as extensive training of forces in anti-contamination protocols to prevent the rapid attrition of efficient human resources. This defensive measure is against unconventional threats. To counter chemical or radiological surprises, it is necessary for critical personnel to be stationed in locations with the highest level of protection. Furthermore, training forces on anti-contamination protocols and fully equipping them with masks and protective suits prevents the rapid loss of efficient manpower. Pourian and PourRamezan (1390) showed in their research that overarching policies must be prepared by the country's Environmental Protection Organization in interaction with the Passive Defense Organization to ensure the continuity of biological cycles, considering passive defense (21).

Role 11: Psychological Preparedness

The eleventh section, Psychological Preparedness, is a defense against the psychological aspect of surprise. Regular training, periodic drills, and general public awareness of protocols cause the community's reaction to lean toward the rapid execution of pre-determined instructions rather than panic, neutralizing the enemy's psychological leverage. This part of passive defense is a defense against the psychological dimension of surprise. A fully trained society does not suffer from psychological paralysis under sudden attacks. Training should include periodic drills, awareness of danger signals, and teaching the first response; this causes the initial reaction of the community to lean towards executing pre-determined protocols instead of panic and chaos, neutralizing the enemy's psychological force. Asgharzadeh and Hassani (1393) showed in their research that by being aware of the methods and techniques affecting people's minds and raising awareness in this field, the psychological factors of soft power can be managed within the domain of passive defense (22).

Role 12: Protection of Resources and Supply Chain

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 capability so that the country can remain self-sufficient for an extended period if supply routes are completely cut off. This role focuses on the continuity of national life. 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 Ka'ini (1396) showed in their research that passive defense can be very instrumental in food security, securing essential goods, and the supply chain (23).

Role 13: Countering the Enemy's Soft War, 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. This defense consists of five axes: 1. Cybersecurity: Monitoring and neutralizing disinformation campaigns; 2. Ensuring Social Security: Countering attempts to undermine public trust; 3. Preserving Social Capital: Strengthening national cohesion against divisive efforts; 4. Establishing Justice and Accountability: Swift transparency in responding to rumors to reduce discontent; and 5. Protecting Cohesion: Containing any attempt by the enemy to incite internal divisions. These measures neutralize the enemy's surprise in the psychological and social dimension, 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 Moghaddam et al. (1402) demonstrated in their research that one of the novel methods of passive defense is a people-centered passive defense, whose primary mission in the first instance is to protect the cohesion between the people and the government in the soft war (24).

Role 14: Protection of Civilian Lives, 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 guaranteed 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. Do'agooyan (1396) showed in their research that protecting civilians against surprise attacks can be a fundamental role for passive defense today (25).

Role 15: Damage Reduction and Restoration of Resilience, And 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 strengthening the country's overall capacity to withstand and quickly recover from the consequences of war.

Conclusion

Passive defense is a proactive strategy that strengthens national resilience by reducing vulnerabilities and ensuring continuity during attacks. It hardens infrastructure and disperses key assets to limit damage and maintain deterrence. Ultimately, it safeguards lives, essential services, and national sovereignty in times of crisis.

Acknowledgements

The authors thank Kerman University of Medical Sciences..

Author contributions

All authors contributed to the design of the study. Mousa Bamir 25 %, Marym okhovati 25 % ., Atousa pourshikhali 20 % , , Ali Talbian 10 % ., Ali Akbar Haghdoost 20 %.

Funding

This study does not charge any fees from any organization or individual, and the applicant will be exempt if the article is accepted.

Ethics approval and consent to participate

study did not fall under the scope, since the participants were not subject to medical procedures nor required to follow rules of behaviour Therefore, This article was reviewed at Kerman University of Medical Sciences and approved with the ethics code IR.kmu.REC.1403.109. All participants signed an informed consent form before the start of the Matrix completion and received an Matrix summary for member checking afterwards.

Competing interests

The authors declare that there are no competitive conflicts.

In Press