Journal Website

Article history:
Received 27 April 2026
Revised 10 October 2026
Accepted 18 October 2026
Published online 23 October 2026

Journal of Social-Political Studies of Iran's Culture and History

Volume 5, Issue 3, pp 1-21



Analysis and Evaluation of the Vulnerabilities of the Islamic Republic of Iran's Defense-Security Strategy in Confronting Emerging Threats, 2021–2026

Hossein. Behdarvand[1], Mohammad. Torabi[2*], Ali. Shirkhani[2]

[1] PhD Student, Department of International Relations, Qo.C., Islamic Azad University, Qom, Iran
[2] Department of Political Science, Qo.C., Islamic Azad University, Qom, Iran

*** Corresponding author email address**: mohammad.torabi@iau.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Behdarvand, H., Torabi, M., & Shirkhani, A. (2026). Analysis and Evaluation of the Vulnerabilities of the Islamic Republic of Iran's Defense-Security Strategy in Confronting Emerging Threats, 2021–2026. *Journal of Social-Political Studies of Iran's Culture and History*, *5*(3), 1-21.

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

A B S T R A C T

The transformation of contemporary security threats has made traditional defense and security models, which were primarily centered on direct military threats and hard power, insufficient for addressing the complexity of the current strategic environment. Cyber threats, cognitive warfare, economic pressure, technological sanctions, biological threats, military applications of artificial intelligence, and hybrid warfare have created new challenges for the defense-security strategy of the Islamic Republic of Iran during the 2021–2026 period. This study aims to analyze and evaluate the major vulnerabilities of Iran's defense-security strategy in confronting these emerging threats. Using a descriptive-analytical approach, the study examines structural, managerial, technological, human, and operational dimensions of the existing strategy and assesses the extent to which they correspond to the evolving characteristics of contemporary threats. The findings indicate that the primary challenge is not the absolute absence of defense capabilities or deterrence capacity, but rather a growing gap between the rapid transformation of the threat environment and the pace of adaptation in decision-making structures, technology, institutional coordination, and human resources. Weak interinstitutional coordination, the predominance of reactive rather than anticipatory approaches, vulnerabilities in selected cyber infrastructures, dependence on certain strategic technologies, insufficient integration among military, economic, cognitive, and cyber domains, and limited capacity for the integrated utilization of emerging technologies constitute the most significant strategic weaknesses. The study concludes that improving Iran's defense-security strategy requires a transition toward an integrated, anticipatory, multilayered, data-driven, and resilient model capable of coordinating military, cyber, economic, cognitive, biological, and technological capacities within a coherent national security architecture.

Keywords: *Defense-Security Strategy, Emerging Threats, Hybrid Warfare, Cybersecurity, Deterrence, Artificial Intelligence, National Resilience*

EXTENDED ABSTRACT

The contemporary security environment has undergone a profound transformation in which the conventional distinction between military and non-military threats, domestic and external vulnerabilities, and conditions of war and peace has become increasingly blurred. The expansion of digital technologies, artificial intelligence, cyber operations, cognitive warfare, economic coercion, biotechnological risks, unmanned systems, information manipulation, and hybrid forms of confrontation has fundamentally altered the logic of national defense and security planning. In classical security paradigms, national defense was largely associated with military preparedness, territorial protection, weapons capability, force structure, and the capacity to respond to direct aggression. However, emerging threats are often networked, multidimensional, indirect, asymmetric, and capable of producing strategic effects without crossing the threshold of formal armed conflict. This transformation has required states to redefine not only the meaning of threat, but also the conceptual scope of deterrence, resilience, strategic adaptation, and security governance. Earlier studies on emerging threats emphasized that defense-security strategies must be reformulated in response to changing patterns of vulnerability and the growing importance of strategic governance (Ebrahimi, 2010). Within the Iranian context, this issue is particularly significant because the Islamic Republic of Iran operates in a complex geopolitical environment characterized by persistent regional instability, sanctions, technological restrictions, military competition, political confrontation, and recurring cyber and information threats. Deterrence has therefore remained a major pillar of Iran's defense-security posture, particularly through the development of retaliatory capability and the effort to increase the perceived costs of hostile action (Ansarifard & Haji Yousefi, 2017). At the same time, the strategy of "threat against threat" has reflected an effort to prevent adversaries from enjoying one-sided coercive advantages by creating reciprocal costs and countervailing capabilities (Kalantari & Eftekhari, 2014). Yet, as hybrid and emerging threats have become more prominent, the adequacy of a predominantly hard-power-centered deterrence posture has increasingly been questioned. The present study therefore examines the vulnerabilities of the Islamic Republic of Iran's defense-security strategy in confronting emerging threats during the period from 2021 to 2026, with particular attention to the extent to which existing strategic structures, institutions, technologies, and decision-making processes have adapted to a rapidly changing threat environment.

The theoretical and analytical framework of the study is grounded in a structural understanding of international security in which states continue to operate under conditions of uncertainty, competition, and the absence of a fully authoritative supranational security guarantor. In this environment, survival, power, autonomy, and national security remain central concerns of state behavior. The broader realist tradition has long emphasized the centrality of power and security in international politics (Ghavam, 2005), while analyses of international relations have also highlighted the significance of systemic structure, power distribution, and state capabilities in shaping strategic behavior (Seifzadeh, 2003). Nevertheless, the present study applies this logic in an expanded form by recognizing that power in the contemporary security environment can no longer be measured solely through military hardware, troop numbers, or conventional firepower. Cyber capability, technological autonomy, economic resilience, intelligence integration, cognitive influence, data control, artificial intelligence, and institutional coordination have become increasingly important components of national power. This expanded understanding is especially relevant in the context of hybrid threats, which combine military and non-military instruments in coordinated ways and target multiple layers of national security simultaneously. The typology of hybrid threats demonstrates

that such threats may operate across political, military, economic, social, informational, and technological domains, and that pressure in one domain can amplify vulnerabilities in another (Pourshasb & Kalantari, 2021). Recent discussions of Iran's defense-security doctrine likewise emphasize the necessity of moving toward a more integrated response to hybrid threats rather than relying exclusively on conventional forms of deterrence (Piri & Masoumi, 2025). Accordingly, the central analytical proposition of this study is that the most important weakness in Iran's defense-security strategy is not the absolute absence of capability, but rather the existence of a strategic-structural adaptation gap between the speed and complexity of threat evolution and the pace at which institutions, technologies, human resources, and decision-making arrangements are adjusted to those changes.

Cybersecurity represents one of the most visible and consequential areas in which this adaptation gap can be observed. The increasing dependence of government services, financial systems, transportation, communication networks, energy infrastructure, identity databases, and military command systems on digital platforms has transformed cybersecurity from a technical issue into a core national security concern. Cyber threats possess characteristics that differentiate them from many conventional threats: barriers to entry are relatively low, actors are diverse, attribution is difficult, geographical distance is less relevant, and operations can be launched rapidly and anonymously across borders. The national-security implications of cyber threats have been recognized in earlier studies, particularly in relation to the vulnerability of critical infrastructure and strategic information systems (Khalilipour Roknabadi, 2012). Research on emerging cyber threats to the armed forces has likewise demonstrated that network security, information protection, command-system resilience, and cyber preparedness are increasingly inseparable from overall military effectiveness (Mahdavi Haji & Bouzmehrani, 2020). The principal vulnerabilities identified in this study include technological dependence in selected hardware and software components, inadequate institutionalization of security requirements in some technological development processes, weaknesses in data protection and access control, insufficient coordination among responsible agencies, fragmented cyber governance, and the persistence of reactive rather than anticipatory approaches. These problems are particularly serious because cyber vulnerabilities can generate cascading effects across economic, military, administrative, and social systems. The issue is therefore not simply whether domestic technological products exist, but whether Iran possesses sustained control over the security, maintenance, updating, auditing, and recovery mechanisms associated with critical digital systems. In this sense, technological self-reliance must be understood functionally rather than symbolically. A domestically produced system that lacks adequate security standards may remain vulnerable, while a foreign-origin technology that is rigorously evaluated, isolated, monitored, and controlled may present a lower operational risk. The key strategic requirement is therefore the ability to maintain secure and resilient technological ecosystems.

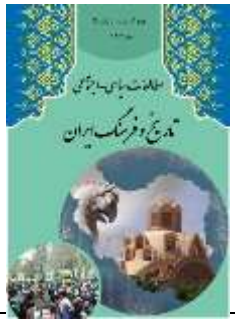
The study further identifies hybrid, cognitive, economic, biological, and technological threats as interconnected dimensions of the same strategic problem. Hybrid warfare creates particular difficulties because it exploits the seams between institutions and sectors. If military, cyber, economic, informational, diplomatic, health, and social institutions operate according to separate threat assessments and disconnected chains of response, adversaries can exploit the resulting gaps. This problem is compounded by hierarchical decision-making structures that may be effective in conventional command environments but less adaptable to fast-moving, cross-domain crises. Hybrid threats require rapid information exchange, common situational awareness, joint scenario analysis, and coordinated strategic action. The growing

significance of cognitive warfare also increases the vulnerability of national security systems that evaluate conflict primarily through physical or military indicators. Cognitive operations seek to influence perception, public trust, strategic judgment, and social cohesion rather than merely destroy material infrastructure. In this environment, information credibility, media literacy, communication speed, and public confidence become strategic assets. Economic pressure represents another major component of the threat environment because sanctions, financial restrictions, supply-chain disruptions, and limitations on access to technology can gradually weaken the material foundations of defense and resilience. Hybrid-threat analysis confirms that economic and informational instruments can reinforce one another and produce cumulative strategic pressure (Pourshasb & Kalantari, 2021). Biological threats present similar cross-sector challenges. Bioterrorism and other emerging biological risks can affect public health, economic continuity, psychological stability, and emergency management simultaneously, meaning that their consequences extend well beyond conventional military planning (Shahraki, 2021). The research therefore argues that Iran's defense-security strategy must treat cyber, economic, cognitive, biological, and conventional military threats as parts of an integrated national-security environment rather than as isolated policy domains.

Artificial intelligence and advanced military technologies constitute another critical dimension of both opportunity and vulnerability. The historical development of military technology has repeatedly altered the nature of strategic competition, as demonstrated by the growing importance of satellite systems for communications, surveillance, reconnaissance, and military operations (Abedini, 1996). The current technological transition is even more complex because artificial intelligence is increasingly embedded in intelligence analysis, autonomous systems, surveillance, cyber defense, predictive modeling, target recognition, data processing, and decision support. The potential defense-security applications of artificial intelligence for Iran have recently received greater analytical attention, particularly because AI can enhance the speed and precision of threat detection and strategic decision-making (Mahdavikia, 2025). At the same time, artificial intelligence creates new vulnerabilities by enabling the automation of cyberattacks, the mass generation of deceptive content, rapid exploitation of discovered weaknesses, and accelerated battlefield decision cycles. The study therefore identifies a major risk in the widening gap between the pace of technological innovation and the capacity of defense-security institutions to absorb, govern, validate, and securely integrate such technologies. Effective use of AI requires more than hardware or software acquisition. It depends on reliable datasets, secure computational infrastructure, skilled human resources, institutional rules for verification, human oversight, and mechanisms for protecting algorithms and data from manipulation. Similar considerations apply to advanced weapons systems, unmanned platforms, missile technologies, sensors, and space-based capabilities. Defense self-reliance remains an important strategic asset, especially under long-term sanctions and restrictions, but self-reliance should not be equated automatically with technological superiority. The key criterion is the capacity for continuous innovation, secure integration, interoperability, maintenance, upgrading, and adaptation to changing operational conditions. Thus, the strategic goal should be the development of a defense innovation ecosystem that links military organizations, universities, research institutions, industry, cyber specialists, data scientists, and strategic decision-makers.

In conclusion, the analysis demonstrates that the central challenge facing the Islamic Republic of Iran's defense-security strategy between 2021 and 2026 is the strategic-structural adaptation gap between the rapidly evolving character of emerging threats and the ability of national institutions to respond in an

integrated, anticipatory, and resilient manner. Iran possesses significant defense capabilities, experience in deterrence, important areas of technological self-reliance, and established institutional structures; however, the effectiveness of these assets depends increasingly on their integration within a coherent multidomain security architecture. The most significant vulnerabilities arise from fragmented institutional coordination, reactive decision-making, technological dependence in selected critical areas, insufficient integration of cyber and cognitive security into broader defense planning, limited cross-sector threat assessment, and the uneven incorporation of artificial intelligence and other emerging technologies. The future effectiveness of Iran's defense-security strategy therefore requires a transition from a predominantly sectoral and response-oriented model toward an integrated, anticipatory, data-driven, multilayered, and resilient model. Such a strategy should link military deterrence with cyber resilience, economic security, cognitive defense, biological preparedness, technological innovation, and institutional coordination. It should also strengthen joint threat assessment, cross-organizational information sharing, strategic foresight, scenario-based planning, and rapid recovery capacity. The ultimate objective is not merely to increase the quantity of defense capabilities, but to ensure that existing and emerging capabilities operate as a coherent system capable of detecting threats early, reducing vulnerabilities before crisis, responding proportionately during confrontation, and restoring critical functions rapidly after disruption. In this sense, the future of national defense-security effectiveness depends less on the isolated strength of individual institutions than on the quality of coordination, adaptation, learning, and integration across the entire national security system.



مطالعات سیاسی–اجتماعی تاریخ و فرهنگ ایران

دوره ۵، شماره ۳، صفحه ۲۱-۱

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۷ اردیبهشت ۱۴۰۵
اصلاح شده در تاریخ ۱۸ مهر ۱۴۰۵
پذیرفته شده در تاریخ ۲۶ مهر ۱۴۰۵
منتشر شده در تاریخ ۱ آبان ۱۴۰۵

تحلیل و ارزیابی آسیب‌های راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با تهدیدات نوین از ۱۴۰۰ تا ۱۴۰۵

حسین بهداروند[۱]، محمد ترابی[۲*]، علی شیرخانی[۲]

۱. دانشجوی دکتری، گروه روابط بین‌الملل، واحد قم، دانشگاه آزاد اسلامی، قم، ایران
۲. گروه علوم سیاسی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

[*] **ایمیل نویسنده مسئول:** mohammad.torabi@iau.ac.ir

اطلاعات مقاله

نوع مقاله
پژوهشی اصیل

نحوه استناد به این مقاله:
بهداروند، حسین.، ترابی، محمد.، و شیرخانی، علی. (۱۴۰۵). تحلیل و ارزیابی آسیب‌های راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با تهدیدات نوین از ۱۴۰۰ تا ۱۴۰۵. *مطالعات سیاسی-اجتماعی تاریخ و فرهنگ ایران*، ۵(۳)، ۲۱-۱.

© ۱۴۰۵ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

چکیده

تحول ماهیت تهدیدات امنیتی در سال‌های اخیر موجب شده است که الگوهای سنتی دفاع و امنیت، که عمدتاً بر تهدیدات نظامی مستقیم و قدرت سخت متمرکز بودند، به‌تنهایی پاسخگوی محیط پیچیده و چندلایه کنونی نباشند. تهدیدات سایبری، جنگ شناختی، فشارهای اقتصادی، تحریم‌های فناوری، تهدیدات زیستی، کاربردهای نظامی هوش مصنوعی و جنگ ترکیبی، محیط امنیتی جمهوری اسلامی ایران را در دوره ۱۴۰۰ تا ۱۴۰۵ با الزامات جدیدی مواجه کرده‌اند. پژوهش حاضر با هدف تحلیل و ارزیابی مهم‌ترین آسیب‌های راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با این تهدیدات انجام شده است. روش پژوهش توصیفی ـ تحلیلی بوده و با تمرکز بر ابعاد ساختاری، مدیریتی، فناورانه، انسانی و عملیاتی راهبرد دفاعی ـ امنیتی، میزان انطباق آن با ماهیت متحول تهدیدات نوین بررسی شده است. یافته‌ها نشان می‌دهد که مهم‌ترین مسئله، فقدان مطلق ظرفیت دفاعی یا بازدارندگی نیست، بلکه وجود شکاف میان سرعت تحول محیط تهدید و سرعت انطباق ساختارهای تصمیم‌گیری، فناوری، هماهنگی نهادی و منابع انسانی با این تحولات است. ضعف در هماهنگی میان نهادهای مسئول، غلبه رویکرد واکنشی بر رویکرد پیش‌نگر، آسیب‌پذیری برخی زیرساخت‌های سایبری، وابستگی در برخی فناوری‌های راهبردی، ناکافی بودن پیوند میان حوزه‌های نظامی، اقتصادی، شناختی و سایبری، و محدودیت در بهره‌برداری یکپارچه از فناوری‌های نوظهور از مهم‌ترین آسیب‌های شناسایی‌شده هستند. بر این اساس، ارتقای راهبرد دفاعی ـ امنیتی مستلزم حرکت به سوی الگویی یکپارچه، پیش‌نگر، چندلایه، داده‌محور و تاب‌آور است که بتواند ظرفیت‌های نظامی، سایبری، اقتصادی، شناختی، زیستی و فناورانه را در قالب یک معماری منسجم امنیت ملی هماهنگ سازد.

کلیدواژگان: *راهبرد دفاعی ـ امنیتی، تهدیدات نوین، جنگ ترکیبی، امنیت سایبری، بازدارندگی، هوش مصنوعی، تاب‌آوری ملی*

مقدمه

تحولات محیط امنیتی در دهه‌های اخیر نشان داده است که مفهوم تهدید و در پی آن منطق طراحی راهبردهای دفاعی ـ امنیتی دستخوش دگرگونی بنیادین شده است. در الگوهای سنتی امنیت، تهدید عمدتاً با قابلیت‌های نظامی دولت‌های رقیب، ظرفیت تهاجم سرزمینی، توان تسلیحاتی، آرایش نیروها و احتمال وقوع جنگ مستقیم تعریف می‌شد و ازاین‌رو بخش مهمی از برنامه‌ریزی دفاعی دولت‌ها بر توسعه نیروی نظامی، افزایش توان آتش، تحکیم مرزهای جغرافیایی و ایجاد بازدارندگی در برابر تجاوز مستقیم تمرکز داشت. با این حال، گسترش فناوری‌های اطلاعاتی و ارتباطی، توسعه شبکه‌های فرامرزی، افزایش وابستگی متقابل اقتصادی، ظهور هوش مصنوعی، پیچیده‌تر شدن عملیات سایبری، گسترش جنگ شناختی و استفاده هم‌زمان از ابزارهای نظامی و غیرنظامی سبب شده است که مرز سنتی میان جنگ و صلح و همچنین میان تهدید داخلی و خارجی تضعیف شود. در چنین فضایی، دولت می‌تواند بدون ورود رسمی به جنگ، از طریق فشار اقتصادی، اختلال در زیرساخت‌های دیجیتال، عملیات اطلاعاتی، مهندسی ادراک عمومی، تحریم فناوری، استفاده از بازیگران نیابتی و ایجاد اختلال در زنجیره‌های تأمین تحت فشار راهبردی قرار گیرد. مفهوم تهدید نوین دقیقاً در چنین بستری اهمیت پیدا می‌کند؛ زیرا این مفهوم به تهدیداتی اشاره دارد که ماهیتی شبکه‌ای، چندبعدی، فناورانه، غیرخطی و غالباً ترکیبی دارند و نمی‌توان آن‌ها را صرفاً با ابزارهای کلاسیک دفاع نظامی مدیریت کرد. توجه به تحول مفهوم تهدید از مدت‌ها پیش در ادبیات سیاست دفاعی مطرح بوده و ضرورت بازنگری در فرایند تدوین راهبردهای دفاعی ـ امنیتی در برابر تهدیدات نوظهور مورد تأکید قرار گرفته است (Ebrahimi, 2010). از این منظر، مسئله اصلی امنیت در عصر حاضر نه صرفاً برخورداری از قدرت نظامی بیشتر، بلکه توانایی تبدیل مجموعه ظرفیت‌های نظامی، اقتصادی، سایبری، اطلاعاتی، فناوری، اجتماعی و شناختی به یک منظومه هماهنگ برای پیشگیری، بازدارندگی، پاسخ و بازیابی پس از بحران است.

جمهوری اسلامی ایران به دلیل موقعیت ژئوپلیتیکی، الگوی روابط منطقه‌ای، تعارضات پایدار با برخی قدرت‌های فرامنطقه‌ای و قرار داشتن در معرض طیفی از فشارهای نظامی، سیاسی، اقتصادی، فناوری و اطلاعاتی، با محیط امنیتی ویژه‌ای مواجه است. راهبرد دفاعی ـ امنیتی ایران طی چند دهه گذشته عمدتاً بر بازدارندگی، خوداتکایی دفاعی، توسعه توان موشکی، بهره‌گیری از عمق راهبردی، پدافند غیرعامل و افزایش هزینه اقدام خصمانه برای دشمن استوار بوده است. بازدارندگی در این چارچوب به معنای ایجاد محاسبه‌ای در ذهن رقیب است که بر اساس آن، هزینه یا مخاطرات اقدام علیه کشور از منافع احتمالی آن بیشتر ارزیابی شود. اهمیت این منطق در راهبرد دفاعی ایران در مطالعات پیشین نیز برجسته شده و بازدارندگی به‌عنوان یکی از عناصر اصلی سیاست دفاعی ـ امنیتی کشور تحلیل شده است (Ansarifard & Haji Yousefi, 2017). علاوه بر این، سیاست «تهدید در برابر تهدید» نیز بر این فرض استوار است که مقابله مؤثر با فشار خارجی مستلزم برخورداری از قابلیت متقابل برای افزایش هزینه تهدیدکننده و کاهش آزادی عمل وی است (Kalantari & Eftekhari, 2014). این منطق در حوزه تهدیدات سنتی و نظامی دارای کارکرد قابل توجهی بوده است؛ اما ظهور تهدیدات نوین موجب شده است که پرسش درباره کفایت شکل موجود بازدارندگی و ظرفیت آن برای مواجهه با تهدیدات چندلایه اهمیت بیشتری پیدا کند.

بازه زمانی ۱۴۰۰ تا ۱۴۰۵ از این منظر اهمیت ویژه‌ای دارد که در این دوره محیط امنیتی ایران شاهد تشدید و هم‌زمانی چند نوع تهدید بوده است. گسترش حملات سایبری علیه خدمات عمومی و زیرساخت‌های حیاتی، افزایش نقش فضای مجازی در شکل‌دهی به افکار عمومی، تشدید رقابت اطلاعاتی و شناختی، استمرار فشارهای اقتصادی و تحریمی، توسعه پهپادها و سامانه‌های هوشمند، رشد کاربردهای نظامی هوش مصنوعی و آشکارتر شدن ماهیت جنگ ترکیبی، نظام تصمیم‌گیری دفاعی ـ امنیتی را با الزامات جدیدی مواجه کرده است. تهدیدات ترکیبی از این جهت متمایزند که در آن‌ها ابزارهای مختلف قدرت به‌طور هم‌زمان و هماهنگ مورد استفاده قرار می‌گیرند و هدف

مهاجم الزاماً نابودی نظامی مستقیم نیست، بلکه می‌تواند فرسایش ظرفیت تصمیم‌گیری، کاهش تاب‌آوری ملی، ایجاد شکاف اجتماعی، تضعیف اقتصاد و اختلال در کارکرد نهادهای حیاتی باشد. بررسی گونه‌های مختلف تهدید ترکیبی نشان می‌دهد که این تهدیدات می‌توانند در سطوح گوناگون امنیت ملی عمل کرده و پیامدهای یک حوزه را به حوزه‌ای دیگر منتقل کنند (Pourshasb & Kalantari, 2021). بنابراین، آسیب‌پذیری اقتصادی می‌تواند بستر عملیات شناختی شود، حمله سایبری ممکن است کارکرد اقتصادی و خدمات عمومی را مختل کند و فشار رسانه‌ای می‌تواند پیامدهای یک بحران محدود را به بحرانی در سطح اعتماد و ادراک اجتماعی تبدیل سازد.

تحول حوزه سایبری نمونه‌ای روشن از تغییر محیط امنیتی است. فضای سایبری هزینه ورود به منازعه را برای بسیاری از بازیگران کاهش داده و امکان اثرگذاری را در اختیار دولت‌ها، گروه‌های سازمان‌یافته، شرکت‌ها، شبکه‌های غیردولتی و حتی افراد قرار داده است. ماهیت فرامرزی شبکه‌های ارتباطی، دشواری انتساب قطعی حملات، سرعت بالای عملیات و امکان هدف قرار دادن زیرساخت‌های حساس بدون عبور فیزیکی از مرزها، محاسبات سنتی دفاعی را با چالش مواجه کرده است. در بررسی تهدیدات سایبری و تأثیر آن‌ها بر امنیت ملی، بر این نکته تأکید شده است که وابستگی روزافزون ساختارهای دولتی و اجتماعی به سامانه‌های اطلاعاتی می‌تواند آسیب‌پذیری امنیت ملی را در برابر اختلال، نفوذ و سرقت اطلاعات افزایش دهد (Khalilipour Roknabadi, 2012). در حوزه نیروهای مسلح نیز تحول تهدیدات سایبری سبب شده است که دفاع از شبکه‌ها، سامانه‌های فرماندهی، پایگاه‌های داده و ارتباطات به بخشی از خود مفهوم آمادگی دفاعی تبدیل شود (Mahdavi Haji & Bouzmehrani, 2020). بنابراین، دیگر نمی‌توان امنیت سایبری را حوزه‌ای پشتیبان و فرعی در کنار دفاع نظامی دانست؛ بلکه این حوزه در بسیاری از موارد پیش‌شرط کارکرد مؤثر قابلیت‌های نظامی، اقتصادی و مدیریتی است.

تحول فناوری همچنین مسئله کیفیت و ماهیت قدرت دفاعی را تغییر داده است. در دوره‌های پیشین، دستیابی به فناوری‌های نظامی پیشرفته و سامانه‌های فضایی نقش مهمی در افزایش قدرت شناسایی، ارتباطات و فرماندهی داشت و پیوند تحول فناوری با تغییر الگوهای جنگ از دهه‌های گذشته مورد توجه بوده است (Abedini, 1996). در دوره کنونی، این روند با هوش مصنوعی، یادگیری ماشین، کلان‌داده، سامانه‌های خودکار، پردازش سریع اطلاعات و قابلیت‌های تصمیم‌یار وارد مرحله جدیدی شده است. کاربرد هوش مصنوعی در حوزه دفاعی ـ امنیتی می‌تواند ظرفیت تحلیل داده، تشخیص الگو، شناسایی تهدید و سرعت تصمیم‌گیری را افزایش دهد و به همین دلیل بررسی قابلیت‌های آن برای کاربردهای دفاعی ایران به یکی از موضوعات نوظهور مطالعات امنیتی تبدیل شده است (Mahdavikia, 2025). با وجود این، فناوری پیشرفته در صورتی که با داده معتبر، ساختار فرماندهی مناسب، نیروی انسانی توانمند، امنیت شبکه و سازوکار روشن مسئولیت و تصمیم‌گیری همراه نباشد، الزاماً به افزایش متناسب امنیت منجر نمی‌شود. مسئله اصلی از این منظر تنها دستیابی به فناوری نیست، بلکه توان ادغام فناوری در معماری کلی دفاع و امنیت است.

تهدیدات زیستی نیز نشان می‌دهند که محیط امنیتی جدید محدود به حوزه‌های نظامی و دیجیتال نیست. قابلیت استفاده از عوامل زیستی، آسیب‌پذیری جوامع در برابر شیوع بیماری‌ها، پیچیدگی تشخیص منشأ برخی رخدادهای زیستی و امکان هم‌پوشانی بحران‌های طبیعی و اقدامات عامدانه باعث شده است که زیست‌امنیت به یکی از ابعاد مهم امنیت ملی تبدیل شود. بررسی انواع سلاح‌های بیوتروریستی نشان داده است که تهدیدات زیستی می‌توانند آثار گسترده انسانی، روانی، اجتماعی و اقتصادی ایجاد کنند و به همین دلیل پاسخ به آن‌ها مستلزم همکاری فرابخشی میان ساختارهای بهداشتی، امنیتی، علمی و مدیریتی است (Shahraki, 2021). این ویژگی بار دیگر نشان می‌دهد که الگوی سازمانی مبتنی بر تفکیک کامل حوزه‌ها نمی‌تواند به‌تنهایی پاسخگوی محیط تهدید جدید باشد.

مسئله پژوهش حاضر از همین نقطه شکل می‌گیرد. با وجود برخورداری جمهوری اسلامی ایران از ظرفیت‌های مهم دفاعی، تجربه بازدارندگی، زیرساخت‌های سازمانی گسترده و توان توسعه بخشی از فناوری‌های بومی، این پرسش مطرح است که راهبرد دفاعی ـ امنیتی

کشور در فاصله ۱۴۰۰ تا ۱۴۰۵ تا چه اندازه با ماهیت متحول تهدیدات نوین انطباق یافته و مهم‌ترین آسیب‌های آن در چه سطوحی قرار دارد. هدف اصلی این پژوهش، تحلیل و ارزیابی آسیب‌های راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با تهدیدات نوین و تبیین رابطه میان ماهیت جدید تهدیدها و کاستی‌های ساختاری، مدیریتی، فناوری، انسانی و اجرایی راهبرد موجود است. رویکرد تحقیق توصیفی ـ تحلیلی است و تلاش می‌شود به جای بررسی مستقل و پراکنده هر تهدید، الگوی مشترک آسیب‌پذیری در سطوح مختلف استخراج شود. فرض بنیادی تحلیل این است که مسئله اصلی راهبرد دفاعی ـ امنیتی ایران فقدان مطلق ظرفیت قدرت نیست، بلکه وجود فاصله میان سرعت تحول محیط تهدید و سرعت انطباق مفهومی، سازمانی، فناورانه و مدیریتی با آن است. ازاین‌رو، تحلیل حاضر بر مفهوم «شکاف انطباق راهبردی ـ ساختاری» متمرکز است؛ شکافی که می‌تواند توضیح دهد چرا برخورداری از توانمندی‌های قابل توجه در برخی حوزه‌ها لزوماً به معنای ایجاد پاسخ یکپارچه و پایدار در برابر تهدیدات ترکیبی نیست.

چارچوب مفهومی و تحول محیط تهدیدات نوین علیه جمهوری اسلامی ایران

تحلیل راهبرد دفاعی ـ امنیتی بدون توجه به ماهیت نظام بین‌الملل و رابطه میان قدرت، بقا و امنیت ناقص خواهد بود. در برداشت واقع‌گرایانه از روابط بین‌الملل، دولت همچنان یکی از بازیگران اصلی محیط امنیتی است و حفظ بقا و منافع ملی در شرایط فقدان یک اقتدار عالی تضمین‌کننده امنیت، از مهم‌ترین انگیزه‌های رفتار آن محسوب می‌شود. بررسی مبانی روابط بین‌الملل نشان می‌دهد که مسئله قدرت و چگونگی تأمین امنیت دولت‌ها از عناصر محوری تحلیل سیاست جهانی بوده است (Ghavam, 2005). در این چارچوب، هر دولت ناگزیر است بخشی از امنیت خود را از طریق ایجاد توانایی مستقل برای مقابله با تهدیدها تأمین کند و نمی‌تواند بقای خود را صرفاً بر تضمین‌های بیرونی استوار سازد. اصول روابط بین‌الملل نیز بر اهمیت ساختار نظام جهانی، توزیع قدرت و محاسبات امنیتی دولت‌ها در شکل‌دهی رفتار راهبردی تأکید دارند (Seifzadeh, 2003). با این حال، کاربرد این چارچوب در محیط جدید نیازمند تعریف گسترده‌تری از قدرت است؛ زیرا قدرت دیگر صرفاً با شمار نیروها، تعداد سامانه‌های تسلیحاتی یا ظرفیت آتش نظامی سنجیده نمی‌شود، بلکه کنترل اطلاعات، قدرت فناوری، تاب‌آوری اقتصادی، توان سایبری، انسجام نهادی، قدرت شناختی و قابلیت مدیریت بحران نیز در تعیین موقعیت امنیتی دولت نقش دارند.

از منظر راهبردی، تهدید زمانی شکل می‌گیرد که قابلیت آسیب‌رسانی یک بازیگر با قصد، فرصت یا زمینه مناسب برای اعمال آن ترکیب شود. تهدیدات سنتی معمولاً نسبتاً قابل مشاهده، دارای منشأ مشخص و مبتنی بر ابزارهای فیزیکی بودند؛ در حالی که بسیاری از تهدیدات نوین دارای منشأ مبهم، شکل غیرمستقیم و تأثیر تدریجی هستند. ممکن است حمله‌ای بدون اعلام رسمی خصومت آغاز شود، در چند عرصه به صورت هم‌زمان جریان یابد و حتی بخشی از عملیات آن در قالب فعالیت‌های اقتصادی، رسانه‌ای یا فناوری عادی پنهان شود. همین ویژگی موجب شده است که مفهوم امنیت از تمرکز صرف بر حفاظت سرزمینی به حفاظت از کارکردهای حیاتی، شبکه‌های اطلاعاتی، نظام اقتصادی، فرآیند تصمیم‌گیری و انسجام جامعه گسترش پیدا کند. تحلیل جایگاه تهدیدات نوظهور در تدوین راهبرد دفاعی ـ امنیتی نشان می‌دهد که پاسخ مؤثر به چنین تهدیداتی مستلزم نگاه راهبردی و حکمرانی هماهنگ در سطح ملی است (Ebrahimi, 2010). بنابراین، اگر ساختار دفاعی تنها برای شناسایی و مقابله با تجاوز نظامی آشکار طراحی شده باشد، امکان دارد تهدیدی که از مسیر مالی، اطلاعاتی یا سایبری وارد می‌شود دیر شناسایی شده و پس از گسترش آثار آن به مسئله‌ای امنیتی تبدیل شود.

جنگ ترکیبی بارزترین نمود این تحول است. مفهوم تهدید ترکیبی به استفاده هماهنگ یا متوالی از ابزارهای نظامی، سیاسی، اقتصادی، اطلاعاتی، سایبری، نیابتی، حقوقی و شناختی برای دستیابی به اهداف راهبردی اشاره دارد. اهمیت این الگو در آن است که دشمن می‌تواند به جای تمرکز بر قوی‌ترین بخش نظام دفاعی، ضعیف‌ترین حلقه‌های محیط ملی را هدف قرار دهد و از پیوند میان آن‌ها برای افزایش اثر فشار استفاده کند. مطالعات مربوط به گونه‌شناسی تهدیدات ترکیبی نشان می‌دهد که این تهدیدات می‌توانند در سطوح سیاسی، نظامی،

اقتصادی، اجتماعی و اطلاعاتی امنیت ملی فعال شوند (Pourshasb & Kalantari, 2021). ازاین‌رو، یک کشور ممکن است از بازدارندگی نظامی بالایی برخوردار باشد، اما هم‌زمان از مسیرهایی چون فشار اقتصادی، عملیات شناختی، جنگ رسانه‌ای یا اختلال سایبری با فرسایش امنیتی مواجه شود. دکترین دفاعی جدید در برابر چنین تهدیداتی ناگزیر باید از تمرکز تک‌بعدی فاصله گرفته و میان انواع ظرفیت‌های قدرت ارتباط برقرار کند؛ اهمیت این تحول در بررسی دکترین دفاعی ـ امنیتی ایران در برابر تهدیدات ترکیبی نیز برجسته شده است (Piri & Masoumi, 2025).

تهدید سایبری در این منظومه جایگاهی خاص دارد، زیرا هم به‌عنوان تهدید مستقل و هم به‌عنوان ابزار تقویت دیگر تهدیدها عمل می‌کند. حمله به شبکه برق، سیستم بانکی، ارتباطات، سامانه‌های حمل‌ونقل یا زیرساخت‌های فرماندهی می‌تواند بدون تخریب گسترده فیزیکی، اختلالی ایجاد کند که آثار اقتصادی، امنیتی و اجتماعی آن با حملات سنتی قابل مقایسه باشد. ماهیت فضای سایبری همچنین مسئله تشخیص مهاجم و تصمیم درباره نوع پاسخ را دشوار می‌کند. تهدید سایبری می‌تواند از طریق بازیگران دولتی، گروه‌های وابسته، پیمانکاران خصوصی یا شبکه‌های مجرمانه اجرا شود و همین امر مرز مسئولیت و انتساب را پیچیده می‌سازد. آثار امنیتی این تحول پیش‌تر نیز در تحلیل تهدیدات سایبری مورد تأکید قرار گرفته است (Khalilipour Roknabadi, 2012). علاوه بر این، بررسی تهدیدات نوظهور سایبری در نیروهای مسلح نشان می‌دهد که گسترش وابستگی سامانه‌های نظامی به شبکه‌ها و فناوری اطلاعات، دفاع سایبری را به یکی از عناصر اصلی آمادگی رزمی تبدیل کرده است (Mahdavi Haji & Bouzmehrani, 2020). در چنین شرایطی، آسیب‌پذیری سایبری یک سامانه فرماندهی یا اطلاعاتی می‌تواند کارآمدی تجهیزات پیشرفته فیزیکی را نیز کاهش دهد.

تهدید شناختی و رسانه‌ای بعد دیگری از محیط امنیتی جدید است. در این حوزه، هدف اصلی الزاماً تخریب زیرساخت یا از بین بردن نیروی نظامی نیست، بلکه تغییر ادراک، ایجاد تردید، کاهش اعتماد، افزایش شکاف اجتماعی و تأثیرگذاری بر فرآیند تصمیم‌گیری است. فضای مجازی با امکان توزیع بسیار سریع محتوا، شخصی‌سازی پیام، تکثیر شبکه‌ای اطلاعات و تولید محتوای مصنوعی، دامنه و سرعت چنین عملیاتی را افزایش داده است. هوش مصنوعی نیز می‌تواند توان تولید و پردازش محتوای هدفمند را بالا برده و تشخیص مرز میان محتوای واقعی و دستکاری‌شده را دشوار کند. قابلیت‌های هوش مصنوعی برای کاربردهای دفاعی ـ امنیتی تنها به سامانه‌های رزمی محدود نیست و حوزه‌هایی مانند تحلیل اطلاعات، کشف الگو، پیش‌بینی، پردازش زبان، شناسایی تهدید و پشتیبانی تصمیم را نیز شامل می‌شود (Mahdavikia, 2025). همین ظرفیت دوگانه سبب می‌شود هوش مصنوعی هم فرصت افزایش توان دفاعی باشد و هم در صورت عقب‌ماندگی فناورانه یا ضعف حکمرانی داده، منبع جدید آسیب‌پذیری تلقی شود.

تهدید اقتصادی در مورد ایران اهمیت مضاعفی دارد، زیرا فشار اقتصادی می‌تواند بدون درگیری نظامی مستقیم، منابع لازم برای توسعه دفاعی، رفاه عمومی، سرمایه‌گذاری در زیرساخت و حفظ تاب‌آوری جامعه را تحت تأثیر قرار دهد. از منظر جنگ ترکیبی، تحریم، محدودیت دسترسی به فناوری، اختلال در زنجیره تأمین، فشار بر تبادلات مالی و ایجاد بی‌ثباتی در انتظارات اقتصادی می‌توانند مکمل سایر ابزارهای فشار باشند. هنگامی که آسیب اقتصادی با عملیات رسانه‌ای و شناختی همراه شود، آثار آن صرفاً در شاخص‌های اقتصادی باقی نمی‌ماند و می‌تواند به مسئله اعتماد عمومی، ادراک کارآمدی و انسجام اجتماعی تبدیل شود. بنابراین، اقتصاد نه حوزه‌ای جدا از دفاع، بلکه بخشی از زیرساخت قدرت ملی است. در منطق «تهدید در برابر تهدید»، توانایی کاهش آسیب‌پذیری و ایجاد هزینه متقابل برای طرف تهدیدکننده یکی از عناصر مهم راهبرد محسوب می‌شود (Kalantari & Eftekhari, 2014). با این حال، در محیط جدید، ایجاد هزینه متقابل تنها از مسیر قدرت نظامی حاصل نمی‌شود و افزایش تاب‌آوری داخلی نیز به همان اندازه در کاهش اثربخشی تهدید نقش دارد.

تهدیدات زیستی نیز ماهیتی فرابخشی دارند. عوامل زیستی می‌توانند بخش سلامت، اقتصاد، حمل‌ونقل، آموزش، امنیت روانی و مدیریت عمومی را هم‌زمان تحت تأثیر قرار دهند. انواع تهدیدات بیوتروریستی و تأثیر احتمالی آن‌ها بر امنیت ملی نشان می‌دهد که آمادگی در برابر این حوزه باید فراتر از ساختارهای پزشکی روزمره باشد و سازوکارهای شناسایی، هشدار، پاسخ سریع، ارتباط عمومی و تداوم خدمات حیاتی را دربرگیرد (Shahraki, 2021). آسیب مهم در اینجا آن است که اگر تهدید زیستی تنها در قالب حمله نظامی کلاسیک تصور شود، بخشی از سناریوهای نوظهور که در مرز میان بحران سلامت، خرابکاری و عملیات ترکیبی قرار دارند از حوزه برنامه‌ریزی امنیتی خارج می‌شوند.

تحول ابزارهای نظامی نیز ادامه یافته و موجب از بین رفتن اهمیت قدرت سخت نشده است. فناوری‌های ماهواره‌ای از چند دهه قبل قابلیت‌های شناسایی، هدایت، ارتباطات و نظارت نظامی را متحول کرده‌اند (Abedini, 1996) و در دوره کنونی، ترکیب حسگرها، شبکه‌های ارتباطی، پهپادها، موشک‌های دقیق و پردازش هوشمند داده موجب افزایش سرعت چرخه شناسایی تا اقدام شده است. از این منظر، راهبرد امنیتی ایران با مسئله دوگانه‌ای مواجه است: از یک سو باید مزیت‌های بازدارندگی سخت و قابلیت‌های نظامی ایجادشده را حفظ و ارتقا دهد و از سوی دیگر، نباید تصور کند که قدرت سخت به‌تنهایی همه اشکال فشار راهبردی را پوشش می‌دهد. بازدارندگی در محیط ترکیبی باید چندلایه باشد؛ یعنی دشمن نه فقط در برابر هزینه نظامی، بلکه در برابر احتمال شکست سایبری، ناکامی اقتصادی، بی‌اثر شدن عملیات شناختی و مقاومت ساختاری کشور نیز با محاسبه پرهزینه مواجه شود. همین ضرورت، زمینه ارزیابی راهبرد دفاعی ـ امنیتی ایران در دوره ۱۴۰۰ تا ۱۴۰۵ را فراهم می‌کند.

راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با تهدیدات نوین از ۱۴۰۰ تا ۱۴۰۵

راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در دوره مورد بررسی را نمی‌توان به یک سند یا یک ابزار منفرد تقلیل داد، بلکه باید آن را مجموعه‌ای از رویکردهای مکمل دانست که حول مفاهیمی چون بازدارندگی، خوداتکایی دفاعی، حفاظت از زیرساخت‌های حیاتی، افزایش عمق دفاعی، پاسخ متقابل، پدافند غیرعامل و توسعه قابلیت‌های نوین شکل گرفته‌اند. در سطح سنتی‌تر، عنصر بازدارندگی همچنان جایگاه مرکزی خود را حفظ کرده است. بازدارندگی ایران بر این مبنا استوار است که دشمن در محاسبه سود و زیان اقدام نظامی، با هزینه‌هایی مواجه شود که تصمیم به حمله را غیرعقلانی یا بسیار پرمخاطره سازد. تحلیل بازدارندگی به‌عنوان راهبرد دفاعی ـ امنیتی ایران نشان می‌دهد که توان پاسخ، اراده استفاده از قابلیت‌های دفاعی و انتقال معتبر پیام بازدارنده از ارکان این رویکرد هستند (Ansarifard & Haji Yousefi, 2017). توسعه توان موشکی، ارتقای سامانه‌های دفاعی و حفظ ظرفیت پاسخ به حمله در همین چارچوب قابل فهم است. با این حال، محیط امنیتی ۱۴۰۰ تا ۱۴۰۵ نشان داده است که بازدارندگی سخت باید با حوزه‌های جدید قدرت پیوند بخورد، زیرا طرف مقابل ممکن است به جای عبور از آستانه جنگ مستقیم، از ابزارهای زیرآستانه‌ای و ترکیبی استفاده کند.

راهبرد «تهدید در برابر تهدید» نیز بخشی از منطق مقابله‌ای جمهوری اسلامی ایران را تشکیل داده است. این راهبرد بر آن است که تهدید یک‌جانبه نباید بدون هزینه باقی بماند و کشور باید در سطح متناسب از امکان پاسخ برخوردار باشد. تحلیل این راهبرد در سیاست دفاعی ایران نشان داده است که هدف آن ایجاد توازن در محاسبات تهدید و جلوگیری از شکل‌گیری تصور مصونیت برای بازیگر مهاجم است (Kalantari & Eftekhari, 2014). در محیط تهدیدات نوین، این مفهوم نیازمند تفسیر گسترده‌تر است. اگر فشار از مسیر اقتصادی اعمال می‌شود، پاسخ راهبردی الزاماً به معنای اقدام نظامی نیست، بلکه می‌تواند شامل کاهش آسیب‌پذیری اقتصادی، تنوع‌بخشی به مسیرهای مبادله، توسعه ظرفیت‌های داخلی و افزایش هزینه سیاسی تداوم فشار باشد. اگر تهدید سایبری باشد، بازدارندگی باید از ترکیب دفاع فعال، افزایش تاب‌آوری، توان کشف و انتساب و قابلیت پاسخ متناسب شکل گیرد. بنابراین، مفهوم تهدید در برابر تهدید در دوره جدید باید از یک الگوی عمدتاً سخت به الگویی چندحوزه‌ای تبدیل شود.

در حوزه سایبری، جهت‌گیری اصلی راهبرد دفاعی ـ امنیتی ایران بر تقویت حاکمیت سایبری، کاهش وابستگی به زیرساخت‌های خارجی، توسعه قابلیت‌های بومی، حفاظت از پایگاه‌های داده، افزایش تاب‌آوری زیرساخت‌های حیاتی و ارتقای توان دفاع سایبری استوار شده است. اهمیت تهدیدات سایبری برای امنیت ملی پیش از دوره مورد مطالعه نیز شناسایی شده بود (Khalilipour Roknabadi, 2012)، اما رشد استفاده از خدمات دیجیتال و انتقال بخش وسیعی از خدمات عمومی و اقتصادی به سامانه‌های برخط، وزن این حوزه را افزایش داده است. راهبرد مطلوب در این عرصه تنها جلوگیری از نفوذ نیست، بلکه باید تمام چرخه تهدید، شامل پیشگیری، شناسایی، پاسخ، تداوم خدمت و بازیابی را پوشش دهد. بررسی تهدیدات سایبری نوظهور در نیروهای مسلح نیز بر ضرورت توجه سازمان‌یافته به ظرفیت‌های دفاع سایبری و آمادگی در برابر اشکال جدید حمله تأکید کرده است (Mahdavi Haji & Bouzmehrani, 2020). در نتیجه، امنیت شبکه‌های فرماندهی و کنترل، حفاظت از سامانه‌های ارتباطی و ذخایر داده و مدیریت زنجیره تأمین سخت‌افزار و نرم‌افزار به بخش جدایی‌ناپذیر از دفاع ملی تبدیل شده‌اند.

با این حال، بومی‌سازی در این حوزه نباید صرفاً معادل تولید داخلی سخت‌افزار یا نرم‌افزار در نظر گرفته شود. مفهوم راهبردی بومی‌سازی زمانی معنا دارد که کشور بتواند فناوری را ارزیابی، نگهداری، به‌روزرسانی، ایمن‌سازی و در صورت بحران مستقل از تأمین‌کننده خارجی اداره کند. ازاین‌رو، استقلال سایبری نیازمند مجموعه‌ای از توانایی‌های فنی، مدیریتی و انسانی است. وابستگی به سامانه‌ای خارجی زمانی به آسیب‌پذیری تبدیل می‌شود که کنترل بر اجزای حساس آن، به‌روزرسانی امنیتی یا داده‌های حیاتی در اختیار طرفی باشد که امکان اعمال محدودیت یا نفوذ دارد. در مقابل، تولید داخلی نیز اگر فاقد استاندارد امنیتی، به‌روزرسانی مستمر و ارزیابی مستقل باشد، خود می‌تواند آسیب‌پذیر باقی بماند. راهبرد سایبری مؤثر باید از تقابل ساده «داخلی یا خارجی» عبور کرده و معیار اصلی را میزان کنترل، امنیت، تداوم‌پذیری و قابلیت اعتماد قرار دهد.

در حوزه جنگ ترکیبی، مهم‌ترین تحول در راهبرد دفاعی ایران افزایش توجه به هم‌زمانی ابزارهای مختلف فشار است. گونه‌شناسی تهدیدات ترکیبی نشان می‌دهد که این تهدیدات در سطح امنیت ملی قابلیت انتقال اثر از یک حوزه به حوزه دیگر را دارند (Pourshasb & Kalantari, 2021). پاسخ به چنین تهدیداتی باید بر «هماهنگی میان حوزه‌ها» استوار باشد، نه صرفاً بر تقویت جداگانه هر حوزه. دکترین دفاعی نوین در برابر تهدیدات ترکیبی نیز بر ضرورت سازگاری ساختار دفاعی با محیط چندلایه تهدید تأکید دارد (Piri & Masoumi, 2025). در عمل، این بدان معناست که نهاد نظامی، امنیتی، اقتصادی، رسانه‌ای، سایبری و دیپلماتیک باید تصویر نسبتاً مشترکی از ماهیت بحران داشته باشند و اقدام آن‌ها در مسیر اهداف واحد قرار گیرد. اگر هر بخش صرفاً بر شاخص‌ها و وظایف تخصصی خود متمرکز شود، مهاجم می‌تواند از فاصله میان آن‌ها استفاده کند. بنابراین، جنگ ترکیبی اساساً آزمون کیفیت حکمرانی امنیتی است.

راهبرد دفاعی در حوزه اقتصادی بر افزایش تاب‌آوری در برابر تحریم، کاهش وابستگی‌های آسیب‌زا، حفظ جریان منابع حیاتی و جلوگیری از انتقال کامل فشار خارجی به ساختار اجتماعی و دفاعی استوار است. در اینجا اقتصاد مقاوم در معنای امنیتی، اقتصادی است که بتواند در شرایط فشار خارجی، کارکردهای حیاتی خود را حفظ کند و امکان تأمین نیازهای ضروری، حمایت از زیرساخت‌ها و تداوم فعالیت‌های دفاعی را فراهم سازد. این رویکرد از نظر نظری با فهم گسترده‌تر از قدرت ملی سازگار است؛ زیرا قدرت در روابط بین‌الملل تنها محصول توان نظامی نیست و ظرفیت اقتصادی یکی از پایه‌های استمرار قدرت محسوب می‌شود (Ghavam, 2005). از سوی دیگر، ضعف اقتصادی می‌تواند قابلیت اعمال سایر ابعاد قدرت را محدود کند. در نتیجه، مدیریت تهدید اقتصادی باید هم‌زمان جنبه پیشگیرانه، تاب‌آورساز و جبرانی داشته باشد.

در حوزه زیستی، راهبرد دفاعی ـ امنیتی باید بر پایش مستمر، شناسایی سریع، آمادگی شبکه سلامت، حفاظت از زیرساخت‌های حیاتی و هماهنگی میان دستگاه‌های علمی، درمانی و امنیتی متمرکز باشد. تنوع ابزارها و الگوهای بیوتروریسم نشان می‌دهد که اتکای صرف به ساختار نظامی برای پاسخ کافی نیست (Shahraki, 2021). در این حوزه، سرعت تشخیص و قابلیت مدیریت اطلاعات به اندازه ظرفیت درمانی اهمیت دارد؛ زیرا تأخیر در تشخیص یا ارتباط عمومی نامناسب می‌تواند پیامدهای یک رخداد محدود را گسترش دهد. همچنین، زیست‌امنیت باید با پدافند غیرعامل و مدیریت بحران پیوند بخورد و سناریوهای احتمالی در قالب رزمایش‌های چندنهادی آزموده شوند.

تحول فناوری‌های هوشمند نیز ضرورت بازنگری در نظام تصمیم‌گیری دفاعی را افزایش داده است. هوش مصنوعی می‌تواند در تحلیل تصاویر، کشف الگوهای تهدید، پردازش اطلاعات، شبیه‌سازی سناریوها، پیش‌بینی و پشتیبانی تصمیم به کار گرفته شود. قابلیت‌های این فناوری برای کاربردهای دفاعی ـ امنیتی ایران مورد توجه مطالعات جدید قرار گرفته است (Mahdavikia, 2025). با این حال، راهبرد مؤثر نباید هوش مصنوعی را به خرید یا طراحی یک ابزار تقلیل دهد. داده‌های باکیفیت، زیرساخت پردازشی، امنیت مدل‌ها، نیروی انسانی متخصص، امکان کنترل انسانی و سازوکارهای اعتبارسنجی از پیش‌شرط‌های بهره‌برداری دفاعی از هوش مصنوعی هستند. اگر داده‌ها ناقص یا آلوده باشند، سامانه هوشمند می‌تواند تصمیم نادرست را با سرعت بیشتری بازتولید کند. به همین دلیل، راهبرد فناوری باید به‌طور هم‌زمان «توسعه قابلیت» و «کاهش آسیب‌پذیری» را دنبال کند.

در حوزه قدرت سخت نیز خوداتکایی دفاعی یکی از عناصر اصلی راهبرد ایران باقی مانده است. محدودیت دسترسی به برخی بازارهای تسلیحاتی انگیزه توسعه ظرفیت‌های داخلی را افزایش داده و در حوزه‌هایی مانند موشکی و پهپادی دستاوردهایی ایجاد کرده است. تحول فناوری نظامی و نقش سامانه‌های فضایی در افزایش قابلیت‌های شناسایی و ارتباطی از گذشته در ادبیات دفاعی مورد توجه بوده است (Abedini, 1996). اکنون مسئله اصلی صرفاً تولید یک سامانه نیست، بلکه قرار گرفتن آن در شبکه‌ای از حسگر، ارتباط، اطلاعات، فرماندهی و تصمیم‌گیری است. تجهیزات پیشرفته زمانی ارزش کامل پیدا می‌کنند که داده مناسب دریافت کرده، با سایر سامانه‌ها ارتباط مؤثر داشته باشند و در محیط اختلال الکترونیکی و سایبری نیز قابل استفاده بمانند.

در مجموع، راهبرد دفاعی ـ امنیتی ایران در دوره ۱۴۰۰ تا ۱۴۰۵ نشانه‌هایی از حرکت به سوی درک گسترده‌تر از تهدید و توجه به سایبر، هوش مصنوعی، جنگ ترکیبی، امنیت اقتصادی و زیست‌امنیت را نشان می‌دهد. مسئله اصلی، وجود یا فقدان مطلق این مؤلفه‌ها نیست؛ بلکه میزان یکپارچگی آن‌ها در سطح راهبرد ملی است. راهبردی که در هر حوزه دارای ظرفیت جداگانه باشد اما فاقد معماری هماهنگ تصمیم‌گیری و پاسخ باشد، در برابر تهدیدات چندلایه با مشکل مواجه خواهد شد. ازاین‌رو، ارزیابی راهبرد موجود باید از سنجش جداگانه قابلیت‌های نظامی فراتر رود و به کیفیت پیوند میان قدرت سخت، فناوری، اقتصاد، اطلاعات، سرمایه انسانی و سازوکارهای حکمرانی توجه کند.

تحلیل و ارزیابی آسیب‌های راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در دوره ۱۴۰۰ تا ۱۴۰۵

مهم‌ترین آسیب راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران را می‌توان در فاصله میان ماهیت به‌شدت شبکه‌ای و ترکیبی تهدیدات جدید و ساختار نسبتاً حوزه‌محور پاسخ به آن‌ها مشاهده کرد. در ساختار تخصصی دفاع و امنیت، تقسیم وظایف میان سازمان‌ها امری ضروری است و تمرکز هر نهاد بر حوزه تخصصی خود می‌تواند به افزایش مهارت و کارآمدی منجر شود؛ اما همین تخصص‌گرایی هنگامی که فاقد سازوکارهای پایدار هماهنگی، اشتراک اطلاعات و تصمیم‌گیری مشترک باشد به منشأ آسیب تبدیل می‌شود. جنگ ترکیبی دقیقاً از شکاف میان نهادها و حوزه‌ها بهره می‌گیرد. بررسی گونه‌شناسی تهدیدات ترکیبی نیز نشان می‌دهد که این تهدیدات از یک سطح امنیتی به سطح دیگر قابل انتقال‌اند و نباید آن‌ها را مجموعه‌ای از تهدیدهای مستقل تلقی کرد (Pourshasb & Kalantari, 2021). برای مثال، یک فشار اقتصادی می‌تواند به افزایش نارضایتی کمک کند، عملیات شناختی آن را برجسته سازد و حمله سایبری هم‌زمان نیز اختلال خدماتی ایجاد

کند. در چنین وضعیتی، پاسخ پراکنده هر نهاد ممکن است در سطح تخصصی درست باشد، اما حاصل جمع این پاسخ‌ها الزاماً یک راهبرد ملی منسجم نخواهد بود.

این مسئله با ساختارهای سلسله‌مراتبی و کندی انتقال اطلاعات تشدید می‌شود. محیط تهدید جدید به تصمیم‌گیری سریع، انعطاف عملیاتی، تبادل داده در زمان نزدیک به واقعی و امکان تشکیل تصویر مشترک از وضعیت نیاز دارد. اگر اطلاعات سایبری در یک سامانه، داده اقتصادی در سامانه‌ای دیگر، ارزیابی اجتماعی در مجموعه‌ای جدا و تحلیل نظامی در زنجیره‌ای مستقل باقی بماند، درک تهدید مرکب با تأخیر شکل می‌گیرد. چنین تأخیری ممکن است موجب شود هر سازمان تنها بخشی از پدیده را ببیند. مفهوم حکمرانی راهبردی در مواجهه با تهدیدات نوظهور دقیقاً از این جهت اهمیت دارد که تدوین و اجرای راهبرد دفاعی نیازمند هماهنگی فراتر از مرزهای سازمانی است (Ebrahimi, 2010). بنابراین، یکی از آسیب‌های اصلی راهبرد موجود، فقدان یا ضعف یک سازوکار کاملاً نهادینه برای ادغام مستمر ارزیابی‌های نظامی، امنیتی، سایبری، اقتصادی، شناختی و زیستی است.

در حوزه سایبری، نخستین دسته آسیب‌ها به وابستگی فناورانه و امنیت زنجیره تأمین مربوط می‌شود. وابستگی بخشی از سخت‌افزارها، نرم‌افزارها، تجهیزات شبکه و فناوری‌های پایه به منابع خارجی، در شرایط خصومت و تحریم می‌تواند مخاطراتی ایجاد کند که از توقف پشتیبانی و محدودیت دسترسی تا آسیب‌پذیری‌های پنهان امنیتی را شامل می‌شود. بررسی تأثیر تهدیدات سایبری بر امنیت ملی نشان داده است که وابستگی ساختارهای حیاتی به سامانه‌های اطلاعاتی، امنیت این سامانه‌ها را به مسئله‌ای ملی تبدیل می‌کند (Khalilipour Roknabadi, 2012). با این حال، پاسخ مناسب به این آسیب صرفاً جایگزین کردن همه فناوری‌های خارجی با نمونه‌های داخلی نیست. مسئله بنیادی‌تر، توانایی ارزیابی امنیتی، کنترل دسترسی، مدیریت چرخه عمر، نگهداری، به‌روزرسانی و بازیابی سامانه‌هاست. اگر محصول داخلی فاقد استاندارد امنیتی و پشتیبانی مستمر باشد، صرف داخلی بودن آن آسیب‌پذیری را برطرف نمی‌کند.

دسته دوم آسیب‌های سایبری به حفاظت از داده‌ها و تمرکز گسترده اطلاعات مربوط است. توسعه دولت الکترونیک، خدمات بانکی دیجیتال، سامانه‌های هویتی و شبکه‌های سازمانی حجم بزرگی از داده‌های حساس را در زیرساخت‌های متصل متمرکز کرده است. این تمرکز از یک سو کارآمدی مدیریتی ایجاد می‌کند و از سوی دیگر ارزش اهداف سایبری را افزایش می‌دهد. در صورتی که طبقه‌بندی داده، کنترل دسترسی، پشتیبان‌گیری، تفکیک شبکه‌ها و پایش رخدادها به اندازه کافی توسعه نیافته باشد، نفوذ به یک نقطه می‌تواند پیامدهای گسترده‌ای ایجاد کند. تهدیدات سایبری نیروهای مسلح نیز از همین منطق تبعیت می‌کنند و حفاظت از ارتباطات و اطلاعات عملیاتی جزئی اساسی از امنیت دفاعی است (Mahdavi Haji & Bouzmehrani, 2020). آسیب راهبردی زمانی شدیدتر می‌شود که دفاع سایبری عمدتاً پس از رخداد فعال شود و سرمایه‌گذاری در شناسایی زودهنگام، شبیه‌سازی حمله و ارزیابی مستمر آسیب‌پذیری کمتر از نیاز واقعی باشد.

غلبه رویکرد واکنشی یکی از آسیب‌های مشترک در چند حوزه است. در مدل واکنشی، ساختار دفاعی پس از مشاهده آثار تهدید اقدام می‌کند؛ در حالی که بسیاری از تهدیدات جدید در مرحله ظهور قابل کنترل‌تر هستند. پیش‌نگری راهبردی به معنای پیش‌بینی قطعی آینده نیست، بلکه ایجاد سازوکاری برای رصد روندها، طراحی سناریوها، تشخیص نشانه‌های هشدار و آزمودن گزینه‌های پاسخ پیش از وقوع بحران است. اهمیت تهدیدات نوظهور در تدوین سیاست‌های دفاعی نشان می‌دهد که برنامه‌ریزی باید به‌طور مستمر با تغییر محیط تهدید به‌روزرسانی شود (Ebrahimi, 2010). در حوزه سایبری، زیستی، هوش مصنوعی و جنگ شناختی سرعت تحول به اندازه‌ای بالاست که چرخه‌های کند سیاست‌گذاری می‌توانند خود به منبع آسیب‌پذیری تبدیل شوند.

در حوزه هوش مصنوعی، خطر اصلی شکاف میان سرعت تحول فناوری و ظرفیت نهادی برای جذب و حکمرانی آن است. قابلیت‌های هوش مصنوعی در حوزه دفاعی می‌توانند قدرت تحلیل، شناسایی و تصمیم‌گیری را افزایش دهند (Mahdavikia, 2025)، اما همین فناوری

امکان خودکارسازی حملات سایبری، تولید انبوه محتوای گمراه‌کننده، تحلیل آسیب‌پذیری‌های دشمن و افزایش سرعت عملیات را نیز فراهم می‌کند. اگر توسعه زیرساخت داده، قدرت پردازشی، منابع انسانی و نظام ارزیابی مدل با سرعت تحول فناوری هماهنگ نباشد، شکاف فناورانه شکل می‌گیرد. افزون بر این، اتکای بیش از حد به سامانه‌های هوشمند بدون سازوکار کنترل انسانی ممکن است خطاهای الگوریتمی را وارد فرآیندهای حساس کند. بنابراین، آسیب هوش مصنوعی تنها عقب‌ماندگی در تولید فناوری نیست، بلکه ضعف در معماری استفاده مسئولانه و امن از آن نیز هست.

در حوزه جنگ شناختی و رسانه‌ای، یکی از چالش‌های اصلی آن است که ساختار دفاعی ممکن است همچنان موفقیت را عمدتاً با شاخص‌های فیزیکی و نظامی بسنجد، در حالی که هدف عملیات شناختی تغییر ادراک و رفتار است. دشمن می‌تواند بدون تغییر موازنه تسلیحاتی، بر برداشت جامعه از امنیت، آینده، اعتماد به نهادها و کارآمدی نظام تصمیم‌گیری اثر بگذارد. رشد فناوری‌های ارتباطی و رسانه‌های شبکه‌ای دامنه این تهدید را افزایش داده است. مفهوم تهدید ترکیبی نیز عملیات اطلاعاتی و شناختی را در کنار ابزارهای سخت به‌عنوان بخشی از فشار چندلایه در نظر می‌گیرد (Piri & Masoumi, 2025). در چنین شرایطی، پاسخ صرفاً رسانه‌ای و پسینی کافی نیست. آسیب زمانی شکل می‌گیرد که ارتباطات عمومی در بحران با تأخیر، چندصدایی نامنسجم یا فقدان روایت معتبر مواجه شود، زیرا خلأ اطلاعاتی می‌تواند توسط روایت‌های رقیب پر شود.

در حوزه اقتصادی، آسیب اصلی در پیوند میان وابستگی‌های ساختاری و امکان تبدیل آن‌ها به اهرم فشار امنیتی قرار دارد. وابستگی شدید برخی درآمدها، محدودیت کانال‌های مالی، آسیب‌پذیری زنجیره تأمین فناوری و اثرگذاری تحریم بر سرمایه‌گذاری و نوسازی زیرساخت‌ها می‌تواند ظرفیت دفاع ملی را در بلندمدت محدود کند. از منظر روابط بین‌الملل، قدرت اقتصادی یکی از اجزای بنیادین قدرت ملی است و توان دولت برای تعقیب اهداف خارجی و امنیتی را تحت تأثیر قرار می‌دهد (Ghavam, 2005). بنابراین، افزایش تورم، کاهش قدرت سرمایه‌گذاری و دشواری دسترسی به فناوری تنها مسائل اقتصادی نیستند، بلکه می‌توانند آثار امنیتی غیرمستقیم داشته باشند. آسیب راهبردی زمانی افزایش می‌یابد که مدیریت فشار اقتصادی از معماری امنیت ملی جدا شود و هماهنگی میان سیاست اقتصادی، سیاست خارجی، حوزه فناوری و نیازهای دفاعی ضعیف باشد.

تحریم‌های فناوری و تسلیحاتی نیز هم‌زمان دو پیامد متفاوت ایجاد کرده‌اند. از یک سو، محدودیت دسترسی به بازارهای خارجی انگیزه خودکفایی و توسعه برخی توانمندی‌های بومی را افزایش داده است و این امر در بعضی حوزه‌ها به کاهش وابستگی منجر شده است. از سوی دیگر، خودکفایی لزوماً مترادف با برتری فناورانه نیست. تحول فناوری نظامی بسیار سریع است و حفظ فاصله کم با مرز فناوری نیازمند دسترسی به دانش، سرمایه انسانی، تحقیق و توسعه و شبکه‌های پیچیده تولید است. بررسی تاریخی تحول فناوری‌های نظامی و نقش سامانه‌های ماهواره‌ای نشان می‌دهد که فناوری همواره یکی از عوامل تغییر کیفیت قدرت نظامی بوده است (Abedini, 1996). بنابراین، مسئله تنها تولید داخلی تجهیزات نیست، بلکه توانایی ارتقای پیوسته آن‌ها و ادغامشان با سامانه‌های اطلاعاتی، فضایی، سایبری و هوشمند است.

در حوزه بازدارندگی نیز یکی از آسیب‌های احتمالی تمرکز بیش از اندازه بر بعد نظامی مفهوم بازدارندگی است. بازدارندگی نظامی برای جلوگیری از جنگ مستقیم ضروری است و مطالعات مربوط به سیاست دفاعی ایران اهمیت آن را تأیید کرده‌اند (Ansarifard & Haji Yousefi, 2017). با این حال، بازیگری که از هزینه حمله نظامی آگاه است ممکن است به استفاده از ابزارهای زیرآستانه‌ای روی آورد. اگر بازدارندگی تنها بر توان پاسخ نظامی تعریف شود، تهدیدکننده می‌تواند در حوزه‌هایی فعالیت کند که آستانه پاسخ نظامی را فعال نمی‌کنند. به همین دلیل، بازدارندگی در برابر جنگ ترکیبی باید شامل قدرت مقاومت، بازیابی و خنثی‌سازی نیز باشد. هدف باید آن باشد که دشمن به این نتیجه برسد نه تنها حمله مستقیم، بلکه فشار سایبری، اقتصادی یا شناختی نیز قادر به دستیابی کم‌هزینه به اهداف راهبردی نیست.

سیاست تهدید در برابر تهدید نیز در صورت تفسیر صرفاً متقارن می‌تواند با محدودیت مواجه شود. منطق اصلی این سیاست افزایش هزینه اقدام خصمانه است (Kalantari & Eftekhari, 2014)، اما در محیط نوین پاسخ مؤثر لزوماً هم‌جنس تهدید نیست. حمله سایبری ممکن است با ترکیبی از دفاع فنی، اقدام حقوقی، افشای انتساب، فشار سیاسی و تقویت تاب‌آوری پاسخ داده شود. فشار اقتصادی ممکن است با تنوع‌بخشی، اصلاح داخلی و دیپلماسی اقتصادی خنثی شود. بنابراین، یکی از الزامات اصلاحی آن است که مفهوم پاسخ متقابل از تقارن ابزاری فاصله گرفته و بر تناسب راهبردی متمرکز شود.

در زیست‌امنیت، آسیب مهم تقلیل تهدید زیستی به سناریوی حمله نظامی آشکار است. سلاح‌ها و عوامل بیولوژیک می‌توانند به اشکال متنوع مورد استفاده قرار گیرند و آثار آن‌ها بر امنیت ملی فراتر از حوزه سلامت باشد (Shahraki, 2021). اگر سازوکارهای دفاع زیستی عمدتاً برای شرایط رسمی جنگ طراحی شده باشند، آمادگی در برابر رخدادهای مبهم یا ترکیبی کاهش می‌یابد. همچنین، نبود سامانه یکپارچه پایش داده‌های زیستی، ضعف ارتباط میان مراکز تخصصی و فقدان رزمایش‌های مشترک می‌تواند زمان تشخیص و پاسخ را افزایش دهد.

سرمایه انسانی نیز در تمام این حوزه‌ها نقش تعیین‌کننده دارد. فناوری‌های پیشرفته بدون متخصصان توانمند و ساختارهای آموزشی پویا قابل بهره‌برداری نیستند. در سایبر، هوش مصنوعی، جنگ شناختی و زیست‌امنیت، دانش تخصصی با سرعت بالا تغییر می‌کند و آموزش‌های ثابت و دوره‌ای نمی‌توانند به‌تنهایی پاسخگو باشند. ازاین‌رو، جذب، نگهداشت و شبکه‌سازی میان نخبگان دانشگاهی، فنی، نظامی و مدیریتی باید بخشی از راهبرد امنیتی باشد. فقدان این پیوند می‌تواند موجب شود فناوری خریداری یا تولید شود ولی بهره‌برداری عملیاتی از آن با کیفیت مطلوب انجام نشود.

در جمع‌بندی این بخش، آسیب محوری راهبرد دفاعی ـ امنیتی ایران را می‌توان «شکاف انطباق راهبردی ـ ساختاری» نامید. این شکاف از تفاوت میان سرعت تحول تهدید و سرعت تحول ساختار پاسخ ناشی می‌شود. نمودهای آن در ضعف هماهنگی نهادی، واکنش‌محوری، وابستگی فناورانه، محدودیت در پیش‌بینی تهدید، جزیره‌ای بودن داده‌ها، ضعف پیوند قدرت سخت با قدرت اقتصادی و شناختی و تأخیر در جذب فناوری‌های نوظهور قابل مشاهده است. دکترین دفاعی جدید در مواجهه با تهدیدات ترکیبی زمانی اثربخش خواهد بود که این شکاف را کاهش دهد و ظرفیت‌های موجود را در یک معماری واحد قرار دهد (Piri & Masoumi, 2025). بنابراین، مسئله اصلی نه کمبود مطلق ابزار، بلکه چگونگی ترکیب ابزارها، کیفیت حکمرانی آن‌ها و سرعت سازگاری با محیط تهدید است.

الزامات ارتقای راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در برابر تهدیدات نوین

ارتقای راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در برابر تهدیدات نوین مستلزم تغییر در منطق سازمان‌دهی قدرت ملی است. نخستین ضرورت، گذار از نگاه حوزه‌ای به حکمرانی یکپارچه امنیتی است. این امر به معنای حذف تخصص یا ادغام سازمان‌ها نیست، بلکه به معنای ایجاد سازوکارهایی است که نهادهای نظامی، امنیتی، سایبری، اقتصادی، رسانه‌ای، علمی و مدیریتی بتوانند در شرایط عادی و بحران بر پایه ارزیابی مشترک از تهدید تصمیم‌گیری کنند. تهدیدات ترکیبی به دلیل ماهیت چندسطحی خود، پاسخ‌های جزیره‌ای را کم‌اثر می‌کنند (Pourshasb & Kalantari, 2021). ازاین‌رو، معماری دفاعی باید امکان تبادل سریع اطلاعات، تعریف مسئولیت روشن، هماهنگی بین‌سازمانی و تمرین سناریوهای مشترک را فراهم سازد. چنین ساختاری می‌تواند مانع از آن شود که هر نهاد تنها بخشی از پدیده را مشاهده کند و اهمیت روابط متقابل میان بحران‌های اقتصادی، سایبری، اجتماعی و نظامی نادیده گرفته شود.

دومین ضرورت، گذار از غلبه رویکرد واکنشی به رویکرد پیش‌نگر است. حکمرانی راهبردی در حوزه دفاعی باید دارای سازوکار دائمی آینده‌پژوهی و پایش روندهای فناوری، امنیتی و ژئوپلیتیکی باشد. جایگاه تهدیدات نوظهور در تدوین راهبردهای دفاعی نشان می‌دهد که تنظیم سیاست دفاعی نمی‌تواند مبتنی بر الگوی ثابت و به‌روزرسانی‌های بلندمدت باشد (Ebrahimi, 2010). لازم است چرخه شناسایی تهدید،

ارزیابی آسیب‌پذیری و بازنگری راهبرد کوتاه‌تر شود و سناریوهای احتمالی به طور مستمر مورد آزمون قرار گیرند. هدف از آینده‌پژوهی نیز پیش‌بینی قطعی آینده نیست، بلکه کاهش غافلگیری راهبردی و افزایش آمادگی برای طیفی از احتمالات است.

در حوزه سایبری، ارتقا باید هم‌زمان بر سه محور امنیت زیرساخت، سرمایه انسانی و حکمرانی متمرکز شود. تهدید سایبری به دلیل گستردگی و پیوند مستقیم با امنیت ملی نیازمند رویکردی فراتر از حفاظت فنی محدود است (Khalilipour Roknabadi, 2012). توسعه مراکز عملیات امنیت، پایش مستمر شبکه‌های حیاتی، نظام یکپارچه گزارش رخداد، پشتیبان‌گیری امن، معماری مقاوم و استانداردهای مشترک امنیتی می‌تواند تاب‌آوری را افزایش دهد. در کنار آن، کاهش وابستگی به اجزای پرخطر زنجیره تأمین و افزایش قابلیت ارزیابی امنیتی تجهیزات ضروری است. در نیروهای مسلح نیز تحول تهدیدات سایبری اقتضا می‌کند دفاع سایبری بخشی از آموزش، رزمایش و طراحی عملیات باشد (Mahdavi Haji & Bouzmehrani, 2020). به بیان دیگر، امنیت سایبری نباید وظیفه واحدی جداگانه تلقی شود، بلکه باید در طراحی همه سامانه‌ها از ابتدا لحاظ گردد.

ایمن‌سازی داده‌ها نیز نیازمند نگاه ویژه است. داده به یکی از منابع اصلی قدرت در محیط امنیتی جدید تبدیل شده و کیفیت تصمیم‌گیری به قابلیت جمع‌آوری، تحلیل و حفاظت از آن وابسته است. استفاده از هوش مصنوعی بدون داده کافی و معتبر ممکن نیست و به همین دلیل توسعه این فناوری باید با حکمرانی داده همراه باشد. قابلیت‌های هوش مصنوعی در کاربردهای دفاعی ـ امنیتی می‌تواند دامنه بزرگی از تحلیل اطلاعات تا پشتیبانی تصمیم را پوشش دهد (Mahdavikia, 2025). برای بهره‌گیری مؤثر از این ظرفیت لازم است استانداردهای مشترک داده، زیرساخت پردازشی امن، مراکز پژوهشی تخصصی و سازوکارهای آزمایش و اعتبارسنجی توسعه یابد. همچنین، کنترل انسانی بر تصمیم‌های حساس باید حفظ شود تا هوش مصنوعی به ابزار افزایش دقت تصمیم تبدیل شود، نه جایگزین کامل مسئولیت انسانی.

در حوزه جنگ شناختی، راهبرد دفاعی باید از الگوی پاسخ رسانه‌ای پسینی فراتر رود و بر افزایش تاب‌آوری شناختی جامعه تمرکز کند. مقابله با اطلاعات نادرست تنها با حذف یا رد پیام رقیب امکان‌پذیر نیست. اعتماد عمومی، شفافیت ارتباطی، سرعت ارائه اطلاعات معتبر و ارتقای سواد رسانه‌ای از عناصر دفاع شناختی هستند. جنگ ترکیبی از شکاف‌های اجتماعی و اطلاعاتی به‌عنوان ضریب تقویت‌کننده سایر فشارها استفاده می‌کند (Piri & Masoumi, 2025). بنابراین، کاهش این شکاف‌ها خود بخشی از بازدارندگی است. ساختاری که در شرایط بحران بتواند اطلاعات دقیق و هماهنگ ارائه دهد و از چندصدایی متناقض جلوگیری کند، فضای عملیات شناختی مهاجم را محدود می‌کند.

در حوزه اقتصادی، راهبرد امنیتی باید بر مفهوم تاب‌آوری تمرکز بیشتری داشته باشد. تاب‌آوری به معنای مصونیت کامل از فشار نیست، بلکه توان حفظ کارکردهای حیاتی، سازگاری با بحران و بازگشت سریع به شرایط پایدار است. ظرفیت اقتصادی یکی از پایه‌های قدرت دولت محسوب می‌شود (Ghavam, 2005) و ازاین‌رو مدیریت تحریم و فشار خارجی باید با برنامه‌ریزی دفاعی مرتبط باشد. تنوع‌بخشی به درآمدها، کاهش نقاط تک‌آسیب‌پذیر، حفاظت از زیرساخت‌های انرژی و مالی و تقویت زنجیره تأمین کالاهای راهبردی می‌تواند امکان اثرگذاری جنگ اقتصادی را کاهش دهد. از منظر امنیتی، سیاست اقتصادی باید تنها بر شاخص‌های رشد کوتاه‌مدت متمرکز نباشد، بلکه اثر تصمیم‌ها بر تاب‌آوری در شرایط بحران را نیز در نظر گیرد.

بازدارندگی نیز نیازمند بازتعریف چندلایه است. بازدارندگی سنتی همچنان برای جلوگیری از تجاوز نظامی مستقیم ضروری است (Ansarifard & Haji Yousefi, 2017)، اما باید با بازدارندگی سایبری، اقتصادی، شناختی و اجتماعی تکمیل شود. بازدارندگی چندلایه زمانی شکل می‌گیرد که دشمن در هر حوزه با دو نوع هزینه مواجه باشد: هزینه‌ای که امکان تحمیل متقابل دارد و هزینه‌ای که از ناکامی در دستیابی به هدف ناشی می‌شود. اگر یک حمله سایبری به دلیل تاب‌آوری شبکه‌ها اثر محدودی داشته باشد، ارزش راهبردی حمله کاهش

می‌یابد؛ اگر عملیات شناختی نتواند اعتماد عمومی را به شکل مورد نظر تغییر دهد، هزینه سرمایه‌گذاری در آن برای مهاجم افزایش می‌یابد. بنابراین، مقاومت و بازیابی بخشی از بازدارندگی هستند.

سیاست تهدید در برابر تهدید نیز باید با همین منطق توسعه یابد. هدف اصلی آن افزایش هزینه تهدیدکننده است (Kalantari & Eftekhari, 2014)، اما در محیط نوین پاسخ می‌تواند نامتقارن و چندابزاری باشد. مهم آن است که پاسخ، رفتار رقیب را تحت تأثیر قرار دهد و نه اینکه الزاماً از همان ابزار استفاده کند. چنین رویکردی امکان انعطاف بیشتری در مدیریت بحران فراهم می‌سازد و از گرفتار شدن سیاست دفاعی در منطق واکنش ثابت جلوگیری می‌کند.

در حوزه زیست‌امنیت، توسعه شبکه هشدار سریع، ظرفیت آزمایشگاهی، ذخایر راهبردی، آموزش نیروهای تخصصی و رزمایش‌های مشترک ضروری است. تنوع سلاح‌ها و شیوه‌های بیوتروریستی نشان می‌دهد که پاسخ به تهدید زیستی نیازمند ترکیب دانش پزشکی، اطلاعاتی و امنیتی است (Shahraki, 2021). همچنین، ارتباطات عمومی در رخداد زیستی اهمیت ویژه دارد، زیرا شایعات و اطلاعات نادرست می‌توانند آثار روانی بحران را تشدید کنند. ازاین‌رو، دفاع زیستی باید به عنوان بخشی از دفاع ترکیبی دیده شود، نه حوزه‌ای منفصل.

در حوزه قدرت سخت، حفظ و توسعه مزیت‌های موجود باید با توجه به تحول سریع فناوری ادامه یابد. تجربه تاریخی نشان داده است که فناوری‌های جدید از جمله سامانه‌های فضایی می‌توانند ماهیت عملیات نظامی را تغییر دهند (Abedini, 1996). امروز این تحول در قالب ادغام فضا، سایبر، پهپاد، حسگر، ارتباطات امن و هوش مصنوعی ادامه یافته است. بنابراین، سیاست خودکفایی دفاعی باید از مفهوم تولید محصول به مفهوم توسعه اکوسیستم فناوری ارتقا یابد. اکوسیستم فناوری شامل پژوهشگاه، دانشگاه، صنعت، نیروی انسانی، داده، استاندارد، آزمایش و زنجیره تأمین است. این تغییر سبب می‌شود توان دفاعی نه به چند سامانه خاص، بلکه به ظرفیت دائمی نوآوری متکی باشد.

سرمایه انسانی نیز باید در مرکز اصلاحات قرار گیرد. تهدیدات نوین نیازمند نیروهایی هستند که توان فهم میان‌رشته‌ای داشته باشند. کارشناس سایبری باید از منطق عملیاتی اطلاع داشته باشد، مدیر امنیتی باید پیامد اقتصادی تصمیم خود را بشناسد و تحلیلگر نظامی باید اثر جنگ شناختی و داده را در محاسبه قدرت لحاظ کند. آموزش‌های مشترک میان نهادها می‌تواند زبان مفهومی واحدی ایجاد کند و هماهنگی را افزایش دهد. جذب نخبگان حوزه هوش مصنوعی، امنیت سایبری، علوم شناختی، زیست‌فناوری و تحلیل داده نیز باید در قالب مسیرهای حرفه‌ای پایدار انجام شود. ظرفیت فناوری زمانی به قدرت ملی تبدیل می‌شود که سرمایه انسانی قادر به توسعه و استفاده راهبردی از آن باشد.

در نهایت، ارتقای راهبرد دفاعی ـ امنیتی مستلزم ایجاد نظام ارزیابی مستمر است. راهبرد نباید صرفاً مجموعه‌ای از اهداف کلی باشد؛ بلکه باید شاخص‌هایی برای سنجش آمادگی، سرعت پاسخ، تداوم خدمات، هماهنگی سازمانی، امنیت زیرساخت و توان بازیابی داشته باشد. رزمایش‌های ترکیبی باید نه فقط توان نظامی، بلکه واکنش هم‌زمان شبکه‌های انرژی، ارتباطات، سلامت، رسانه و مدیریت اقتصادی را آزمایش کنند. نتیجه چنین ارزیابی‌هایی باید مستقیماً به اصلاح برنامه‌ها منجر شود. هدف نهایی حرکت به سوی الگویی است که در آن قدرت نظامی با قدرت سایبری، فناوری، اقتصادی، شناختی، اجتماعی و دیپلماتیک پیوند برقرار کند و پاسخ به تهدید نوین بر پایه یک تصویر واحد از امنیت ملی شکل گیرد.

نتیجه‌گیری

تحلیل راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران در مواجهه با تهدیدات نوین در فاصله ۱۴۰۰ تا ۱۴۰۵ نشان می‌دهد که محیط امنیتی کشور وارد مرحله‌ای شده است که در آن تمایز سنتی میان تهدید نظامی و غیرنظامی، داخلی و خارجی، سخت و نرم و حتی جنگ و صلح به میزان قابل توجهی کاهش یافته است. تهدیدات نوین به صورت شبکه‌ای عمل می‌کنند و اغلب به جای هدف قرار دادن مستقیم یک عنصر از قدرت ملی، رابطه میان عناصر مختلف را مورد فشار قرار می‌دهند. حمله سایبری می‌تواند آثار اقتصادی ایجاد کند، فشار اقتصادی

می‌تواند زمینه عملیات شناختی را افزایش دهد، جنگ رسانه‌ای می‌تواند پیامدهای یک بحران محدود را تشدید کند و عقب‌ماندگی فناورانه نیز امکان اثرگذاری سایر تهدیدها را افزایش دهد. ازاین‌رو، امنیت ملی در این دوره بیش از هر زمان دیگر به ظرفیت هماهنگی میان حوزه‌های مختلف وابسته شده است.

یافته اصلی پژوهش آن است که مسئله بنیادین راهبرد دفاعی ـ امنیتی ایران را نمی‌توان فقدان مطلق قدرت، ضعف کامل بازدارندگی یا نبود ظرفیت‌های دفاعی دانست. جمهوری اسلامی ایران در برخی حوزه‌ها از قابلیت‌های مهم و تجربه قابل توجه برخوردار است و در طول چند دهه توانسته است بخشی از محدودیت‌های خارجی را از طریق توسعه ظرفیت‌های داخلی جبران کند. مسئله اصلی در سطحی عمیق‌تر، فاصله میان سرعت تحول محیط تهدید و سرعت سازگاری نظام راهبردی با این تحول است. این فاصله را می‌توان «شکاف انطباق راهبردی ـ ساختاری» نامید. هر اندازه محیط تهدید شبکه‌ای‌تر، فناورانه‌تر و سریع‌تر می‌شود، ساختار دفاعی نیز باید از نظر شیوه تصمیم‌گیری، تبادل اطلاعات، هماهنگی بین‌نهادی، فناوری و سرمایه انسانی با همان سرعت تحول یابد.

یکی از مهم‌ترین نمودهای این شکاف، جزیره‌ای بودن نسبی حوزه‌های تخصصی است. وجود سازمان‌های تخصصی برای دفاع نظامی، امنیت سایبری، مدیریت اقتصادی، رسانه، سلامت و اطلاعات ضروری است، اما هنگامی که سازوکارهای ارتباطی و تصمیم‌گیری مشترک میان آن‌ها ضعیف باشد، مزیت تخصص به محدودیت راهبردی تبدیل می‌شود. تهدید ترکیبی دقیقاً در فاصله میان این حوزه‌ها عمل می‌کند. ممکن است هر نهاد در وظیفه تخصصی خود توانمند باشد، ولی نبود تصویر مشترک از بحران سبب شود که مجموعه قدرت ملی نتواند در زمان مناسب و با جهت واحد عمل کند. بنابراین، معیار اصلی کارآمدی در محیط امنیتی جدید نه تعداد سازمان‌ها یا حجم ظرفیت‌های پراکنده، بلکه توان تبدیل این ظرفیت‌ها به اقدام هماهنگ است.

حوزه سایبری روشن‌ترین نمونه این مسئله است. وابستگی گسترده خدمات حیاتی به زیرساخت‌های دیجیتال سبب شده است که امنیت سایبری از یک موضوع فنی به مسئله‌ای مرتبط با کل امنیت ملی تبدیل شود. ضعف در حفاظت از داده‌ها، وابستگی برخی اجزای فناوری، نبود ارزیابی مستمر آسیب‌پذیری، ناهماهنگی میان متولیان و غلبه واکنش پس از رخداد می‌تواند میزان اثرگذاری حملات را افزایش دهد. در این حوزه، بومی‌سازی باید به معنای کنترل واقعی بر فناوری و توان نگهداری، ارزیابی و ایمن‌سازی آن باشد و نه صرفاً تولید داخلی محصول. همچنین، حفاظت از شبکه‌های حیاتی باید از مرحله طراحی آغاز شود و امنیت به‌عنوان جزء ذاتی توسعه فناوری در نظر گرفته شود.

هوش مصنوعی نیز در سال‌های آینده اهمیت بیشتری خواهد یافت. این فناوری قادر است سرعت تحلیل اطلاعات، کشف الگو، شناسایی تهدید و تصمیم‌سازی را افزایش دهد، اما هم‌زمان ظرفیت دشمن برای خودکارسازی حملات، تولید محتوای جعلی، تحلیل ضعف‌ها و افزایش سرعت عملیات را نیز توسعه می‌دهد. ازاین‌رو، مسئله راهبردی صرفاً دستیابی به ابزار هوش مصنوعی نیست، بلکه شکل‌دهی اکوسیستم داده، نیروی انسانی، قدرت پردازشی، امنیت و کنترل انسانی است. هر گونه عقب‌ماندگی در این اکوسیستم می‌تواند به افزایش فاصله میان تهدید و پاسخ منجر شود.

در حوزه اقتصادی، تحلیل نشان می‌دهد که قدرت دفاعی را نمی‌توان مستقل از توان اقتصادی در نظر گرفت. فشار اقتصادی می‌تواند منابع توسعه فناوری و نوسازی دفاعی را محدود کند و در عین حال آثار اجتماعی و شناختی ایجاد کند. بنابراین، تاب‌آوری اقتصادی بخشی از دفاع ملی است. راهبرد اقتصادی در شرایط فشار باید بر کاهش نقاط آسیب‌پذیر، تنوع‌بخشی، تداوم زنجیره‌های حیاتی و ایجاد امکان بازیابی سریع متمرکز شود. هدف، حذف کامل آثار فشار نیست، بلکه جلوگیری از تبدیل فشار اقتصادی به اختلال راهبردی در سایر حوزه‌های قدرت است.

در حوزه شناختی، اعتماد عمومی و کیفیت ارتباطات به دارایی امنیتی تبدیل شده‌اند. جامعه‌ای که به اطلاعات معتبر دسترسی دارد و میان نهادهای آن ارتباط مؤثر وجود دارد، در برابر عملیات ادراکی و شایعه مقاوم‌تر است. در مقابل، خلأ اطلاعاتی، تأخیر در اطلاع‌رسانی و روایت‌های متناقض می‌توانند فرصت اثرگذاری بیشتری برای عملیات شناختی ایجاد کنند. بنابراین، دفاع شناختی را نباید به تولید پیام تبلیغاتی محدود کرد؛ بلکه باید آن را در ارتباط با سرمایه اجتماعی، شفافیت، سواد رسانه‌ای و کارآمدی مدیریتی فهمید.

در حوزه زیستی نیز ضرورت نگاه میان‌بخشی آشکار است. رخداد زیستی می‌تواند به سرعت از حوزه سلامت به اقتصاد، نظم عمومی، آموزش و امنیت روانی منتقل شود. ازاین‌رو، آمادگی واقعی در این حوزه نیازمند شبکه پایش، هشدار سریع، ظرفیت تخصصی، ذخایر راهبردی، ارتباط عمومی و رزمایش‌های مشترک است. قرار دادن تهدید زیستی صرفاً در چارچوب جنگ نظامی آشکار، بخشی از سناریوهای محتمل را خارج از برنامه‌ریزی قرار می‌دهد.

قدرت سخت و بازدارندگی نظامی همچنان عنصر ضروری امنیت جمهوری اسلامی ایران باقی می‌ماند، اما محیط جدید نشان می‌دهد که بازدارندگی باید گسترده‌تر تعریف شود. جلوگیری از اقدام دشمن تنها با تهدید به پاسخ نظامی حاصل نمی‌شود. اگر کشور بتواند حمله سایبری را خنثی کند، فشار اقتصادی را تحمل و مدیریت کند، عملیات شناختی را کم‌اثر سازد و خدمات حیاتی را پس از بحران به سرعت بازیابی کند، مهاجم با کاهش احتمال موفقیت مواجه خواهد شد. این قابلیت خود نوعی بازدارندگی ایجاد می‌کند. در نتیجه، بازدارندگی آینده باید ترکیبی از توان پاسخ و توان مقاومت باشد.

بر این اساس، راهبرد دفاعی ـ امنیتی مطلوب برای دوره پیش رو باید یکپارچه، پیش‌نگر، چندلایه، داده‌محور و تاب‌آور باشد. یکپارچگی به معنای ایجاد ارتباط مؤثر میان ظرفیت‌های مختلف قدرت ملی است؛ پیش‌نگری به معنای رصد روندها و طراحی سناریو پیش از بحران است؛ چندلایه بودن به معنای ترکیب دفاع نظامی، سایبری، اقتصادی، شناختی و زیستی است؛ داده‌محوری به معنای استفاده از اطلاعات معتبر برای تصمیم سریع و دقیق است؛ و تاب‌آوری به معنای حفظ و بازیابی کارکردهای حیاتی حتی در صورت عبور تهدید از لایه‌های اولیه دفاع است.

نتیجه نهایی آن است که ارتقای راهبرد دفاعی ـ امنیتی جمهوری اسلامی ایران بیش از آنکه به افزودن یک ابزار یا تأسیس یک نهاد جدید وابسته باشد، به اصلاح رابطه میان راهبرد، ساختار، فناوری و سرمایه انسانی نیاز دارد. ظرفیت‌های موجود هنگامی به قدرت مؤثر تبدیل می‌شوند که بر اساس تصویر مشترکی از تهدید هدایت شوند، اطلاعات میان آن‌ها جریان داشته باشد، مسئولیت‌ها روشن باشد و نظام تصمیم‌گیری بتواند متناسب با سرعت بحران عمل کند. کاهش شکاف انطباق راهبردی ـ ساختاری باید در مرکز اصلاحات قرار گیرد، زیرا بسیاری از آسیب‌های شناسایی‌شده، از ضعف هماهنگی تا واکنش‌محوری و وابستگی فناورانه، در نهایت به همین شکاف بازمی‌گردند. آینده امنیت ملی در گرو توانایی تبدیل ساختار دفاعی از مجموعه‌ای از ظرفیت‌های تخصصی به منظومه‌ای هماهنگ، انعطاف‌پذیر و یادگیرنده است که بتواند پیش از تبدیل تهدید به بحران، آن را شناسایی کند، در زمان بحران پاسخ متناسب ارائه دهد و پس از آن با سرعت کارکردهای حیاتی خود را بازسازی کند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Abedini, M. (1996). The Evolution of Military Technologies and the Role of Satellites. *Foreign Policy Quarterly*(14), 68-93.

Ansarifard, M., & Haji Yousefi, A. M. (2017). Deterrence as Iran's Defense-Security Strategy. *Quarterly Journal of International Relations Studies*(55), 7-31.

Ebrahimi, N. (2010). An Analysis of the Position of Emerging Threats in the Formulation of Defense-Security Strategies with Emphasis on Strategic Governance. *Defense Policy*, *18*(71), 9-26.

Ghavam, A. (2005). *International Relations* (2nd ed.). SAMT.

Kalantari, F., & Eftekhari, A. (2014). Examining and Explaining the Strategy of Threat against Threat in Iran's Defense Policy. *Defense Policy*, *22*(88), 63-90.

Khalilipour Roknabadi, K. (2012). *Cyber Threats and Their Impact on National Security*.

Mahdavi Haji, M., & Bouzmehrani, A. A. (2020). An Analysis of Emerging Cyber Threats in the Armed Forces. *Quarterly Journal of War Studies*(6), 100-126.

Mahdavikia, M. (2025). *Examining Artificial Intelligence Capabilities for Defense-Security Applications of the Islamic Republic of Iran* National Conference on the Application of Artificial Intelligence in the Modern Era,

Piri, H. M., & Masoumi, J. (2025). The New Defense-Security Doctrine of the Islamic Republic of Iran in Confronting Hybrid Threats. *Scientific Quarterly of Sacred Defense Studies*, *11*(1), 25-51.

Pourshasb, A., & Kalantari, F. (2021). Typology of Hybrid Threats and Their Application to the Levels of Iran's National Security. *Quarterly Journal of War Studies*(10), 63-97.

Seifzadeh, S. H. (2003). *Principles of International Relations* (3rd ed.). Mizan Publications.

Shahraki, S. (2021). An Examination of Types of Bioterrorism Weapons and Their Impact on National Security. *Quarterly Journal of National Interests Studies*, *6*(22).