Shiraz University
RICeST
ISC
ISSN: 2008-7926

Journal of
Legal Studies
Scientific

Vol. 17, Issue 4, Winter 2026

JLS

Journal of Legal Studies
Journal Homepage: https://jls.shirazu.ac.ir/
doi: https://10.22099/JLS.2026.54478.5391

Research Article

# The Doctrine of Asymmetric and Combined Response: An Analysis of Iran's Legal-Political Strategy in the Twelve-Day War

**Seyed Ali Mirlohi***

PhD graduate in Jurisprudence and Private Law, Shahid Motahari University and Graduate School, Tehran, Iran

*Article history:* Received: 08-10-2025 Accepted: 04-01-2026

## Abstract

Technological developments in the sphere of international security have transformed the nature, scope, and speed of conflicts, confronting the classical paradigms of law and strategy with fundamental challenges. While the twentieth century was the era of symmetric warfare, the twenty-first century is characterized by asymmetric and hybrid threats operating in the "gray zone" between peace and war. The Twelve-Day War of Summer 1404 (2025), initiated by the Zionist regime's direct attacks on Iran's military and nuclear facilities, served as a turning point in modern conflicts. This event highlighted those legal concepts derived from the Westphalian order, such as the prohibition on the use of force (Article 2(4) of the UN Charter) and self-defense (Article 51), require redefinition to address the realities of the digital age. The core problem of this research stems from the tension between traditional law and modern technology. The primary objective is to analyze Iran's legal-strategic response to this aggression and to answer the question: What strategy did Iran adopt to legitimize its defensive actions against a technological and asymmetric threat?

*Please cite this article as:*
Mirlohi, S.A (2026). The Doctrine of Asymmetric and Combined Response: An Analysis of Iran's Legal-Political Strategy in the Twelve-Day War. *Journal of Legal Studies*, *17*(4), 41-70. https://doi: 10.22099/JLS.2026.54478.5391

* Corresponding author:
E-mail address: mirlohi@motahari.ac.ir

**Methods**

This research employs an analytical-descriptive approach, relying on a "documented case study" method. The study first examines the theoretical foundations of the "right to self-defense" and the legal challenges posed by emerging technologies, utilizing sources such as the "Tallinn Manual" to interpret cyber operations within the framework of armed attacks. Subsequently, the article conducts a detailed analysis of the Twelve-Day War's timeline, evaluating the military and cyber actions of both parties. The methodology involves scrutinizing the legal arguments presented by both sides—specifically Israel's invocation of the "preemptive defense" doctrine versus Iran's reliance on "self-defense" and "countermeasures"—against customary international law criteria such as necessity, proportionality, and immediacy. The focus is on extracting Iran's strategic behavioral pattern from operational data and official political stances.

**Results and Discussion**

The findings indicate that Israel's initial military strike on June 13, 2025, justified under the rejected doctrine of "preemptive defense," lacked the prerequisite of an "imminent threat" and thus constituted a clear violation of international law and an act of aggression. In response, the analysis reveals that Iran, rather than engaging in a symmetric response (e.g., air-to-air combat), implemented an innovative doctrine termed the "Asymmetric and Hybrid Response Doctrine." This doctrine comprised three simultaneous components:

- **Asymmetric Kinetic Response:** Iran shifted the battlefield from air superiority (the enemy's advantage) to missile and drone warfare. "Operation True Promise 3," involving hundreds of ballistic missiles targeting strategic Israeli infrastructure, was designed to impose direct costs and psychological shock, justified legally under Article 51.
- **Offensive Cyber Warfare:** Complementing the kinetic strikes, Iran launched extensive cyberattacks against Israel's critical infrastructure (banking, media, services). The strategic goal was the "functional paralysis" of the enemy's society, framed as legitimate countermeasures against prior Israeli sabotage.
- **Expansion of the Front (Gray Zone):** The activation of proxy actors, such as the Houthis, to launch attacks from different fronts served to exhaust Israel's air defense resources and create "legal ambiguity" regarding state attribution.

The discussion highlights that this "legal-military" conflict exposed the inefficacy of collective security institutions like the UN Security Council and demonstrated how both parties utilized international law as a tool.

**Conclusions**
The research concludes that Iran successfully combined classical deterrence with modern asymmetric warfare tools to execute a unique "legal-operational strategy." This approach not only responded to the immediate threat but also aimed to shape future legal norms in cyberspace. However, the conflict underscored significant gaps in international humanitarian law, particularly regarding the protection of dual-use infrastructure in hybrid wars. The article suggests that adapting to these new realities requires the formulation of a "Digital Additional Protocol" to the Geneva Conventions and the establishment of an independent international body for the technical attribution of cyberattacks to prevent miscalculations and the escalation of future conflicts.

**Keywords**: Asymmetric response, hybrid warfare, Iran-Israel war, self-defense, jus ad bellum.

.

مجله مطالعات حقوقی
علمی
شاپا: ۷۹۲۶-۲۰۰۸

دوره هفدهم، شماره چهارم، زمستان 1404

مجله مطالعات حقوقی
Journal Homepage: https://jls.shirazu.ac.ir/
doi: https://10.22099/JLS.2026.54478.5391

JLS

مقاله پژوهشی

# دکترین پاسخ نامتقارن و ترکیبی: تحلیل راهبرد حقوقی - سیاسی ایران در جنگ دوازده‌روزه با رژیم صهیونیستی

**سیدعلی میرلوحی***

**دانش‌آموخته فقه و حقوق، مدرسه عالی و دانشگاه شهید مطهری (ره)، تهران، ایران**

اطلاعات مقاله | تاریخ دریافت: 1404/07/16 | تاریخ پذیرش: 1404/10/14

## چکیده

**مقدمه:** تحولات فناورانه در سپهر امنیت بین‌الملل، ماهیت و دامنه مخاصمات را دگرگون کرده و پارادایم‌های کلاسیک حقوق بین‌الملل را با چالش‌های بنیادین مواجه ساخته است. قرن بیست و یکم، عصر ظهور تهدیدات نامتقارن و ترکیبی است که در «منطقه خاکستری» میان صلح و جنگ عمل می‌کنند. جنگ دوازده روزه تابستان ۱۴۰۴ که با حملات مستقیم رژیم صهیونیستی به مراکز نظامی و هسته‌ای ایران آغاز شد، نقطه عطفی در این دگرگونی بود. این رویداد نشان داد که مفاهیم سنتی مانند «توسل به زور» و «دفاع مشروع» (ماده ۵۱ منشور ملل متحد) در برابر واقعیت‌های جنگ‌های سایبری و هیبریدی نیازمند بازتعریف هستند. مسئله اصلی این پژوهش، بررسی تنش میان حقوق سنتی و فناوری مدرن در بستر این جنگ خاص است. هدف اصلی این مطالعه، پاسخ به این پرسش محوری است که استراتژی حقوقی-راهبردی ایران در توجیه و اجرای پاسخ نظامی به این تجاوز چه بود و چگونه از ابزارهای حقوقی برای مشروعیت‌بخشی به اقدامات خود در برابر یک تهدید فناورانه استفاده کرد؟ این تحقیق می‌کوشد تا با تحلیل این موردکاوی، خلاء پژوهشی موجود در زمینه کاربرد عملی حقوق بین‌الملل در جنگ‌های ترکیبی را پر کند.

**استناد به این مقاله:**

**میرلوحی، سیدعلی** (1404). **دکترین پاسخ نامتقارن و ترکیبی: تحلیل راهبرد حقوقی - سیاسی ایران**

**در جنگ دوازده‌روزه با رژیم صهیونیستی. *مجله مطالعات حقوقی*. شماره** 17. (4). 70-41.

*** نویسنده مسئول:** E-mail address: mirlohi@motahari.ac.ir

**روش‌ها:** این پژوهش با رویکردی تحلیلی-توصیفی و با اتکا به روش «موردکاوی مستند» انجام شده است. برای تبیین دقیق موضوع، ابتدا چارچوب نظری «حق دفاع مشروع» و چالش‌های ناشی از فناوری‌های نوظهور و جنگ‌های سایبری با استفاده از منابع کتابخانه‌ای و اسناد حقوقی بین‌المللی (مانند راهنمای تالین) واکاوی شده است. سپس، با تمرکز بر وقایع جنگ دوازده روزه، اقدامات نظامی و سایبری طرفین به صورت روزشمار و تطبیقی مورد تحلیل قرار گرفت. در این راستا، استدلال‌های حقوقی طرفین در مجامع بین‌المللی، از جمله استناد اسرائیل به دکترین «دفاع پیش‌دستانه» و استناد ایران به «دفاع مشروع» و «اقدامات متقابل»، با اصول حقوق بین‌الملل عرفی (ضرورت، تناسب و فوریت) سنجیده شد. تمرکز اصلی روش‌شناسی بر استخراج الگوی رفتاری ایران از میان داده‌های عملیاتی و مواضع سیاسی اعلامی بوده است.

**یافته‌ها:** یافته‌های تحقیق نشان می‌دهد که اقدام اولیه اسرائیل در ۲۳ خرداد ۱۴۰۴، مبتنی بر دکترین مردود «دفاع پیش‌دستانه» بوده که به دلیل فقدان شرط «قریب‌الوقوع بودن تهدید»، نقض آشکار ماده ۲ (۴) منشور ملل متحد و یک فعل تجاوزکارانه محسوب می‌شود. در مقابل، تحلیل اقدامات ایران نشان می‌دهد که تهران به جای درگیری در یک پاسخ متقارن (نبرد هوایی کلاسیک)، یک دکترین نوآورانه تحت عنوان «آموزه پاسخ نامتقارن و ترکیبی» را اجرا کرد. این دکترین دارای سه مؤلفه اصلی بود که به صورت همزمان عملیاتی شدند: ۱. پاسخ کینتیک نامتقارن: ایران با پرهیز از درگیری هوایی (که نقطه قوت دشمن بود)، نبرد را به حوزه موشکی و پهپادی منتقل کرد. عملیات «وعده صادق ۳» با شلیک صدها موشک بالستیک، با هدف ایجاد شوک روانی و تحمیل هزینه مستقیم به زیرساخت‌های استراتژیک اسرائیل انجام شد و ذیل حق ذاتی دفاع مشروع (ماده ۵۱) توجیه شد؛ ۲. جنگ سایبری تهاجمی: همزمان با حملات فیزیکی، ایران جنگ سایبری گسترده‌ای را علیه زیرساخت‌های حیاتی (بانک‌ها، رسانه‌ها و خدمات عمومی) اسرائیل آغاز کرد. هدف این مؤلفه، «فلج‌سازی کارکردی» جامعه دشمن و تکمیل فشار کینتیک بود که به‌عنوان «اقدام متقابل» در برابر خرابکاری‌های پیشین تلقی شد؛ ۳. گسترش جبهه (منطقه خاکستری): فعال‌سازی بازیگران نیابتی و محور مقاومت (مانند حوثی‌ها) برای حمله از جبهه‌های دیگر، با هدف فرسایش سامانه‌های پدافندی اسرائیل و ایجاد «ابهام حقوقی» در زمینه انتساب مسئولیت بین‌المللی صورت گرفت. یافته‌ها همچنین حاکی از آن است که این جنگ «حقوقی-

نظامی»، ناکارآمدی نهادهای امنیت جمعی مانند شورای امنیت را آشکار ساخت و نشان داد که طرفین از حقوق بین‌الملل به عنوان ابزاری برای «جنگ حقوقی» بهره برده‌اند.

**نتیجه‌گیری:** پژوهش نتیجه می‌گیرد که ایران موفق شد با تلفیق بازدارندگی کلاسیک و ابزارهای نوین جنگ نامتقارن، معادله امنیت را به نفع خود تغییر دهد و پاسخی مشروع در چارچوب حقوق بین‌الملل ارائه دهد. با این‌حال، این جنگ نشان‌دهنده خلاءهای جدی در حقوق بشردوستانه، به‌ویژه در حفاظت از زیرساخت‌های دوگانه در برابر حملات سایبری است. مقاله در پایان پیشنهاد می‌دهد که برای انطباق حقوق جنگ با واقعیت‌های نوین، تدوین «پروتکل الحاقی دیجیتال» به کنوانسیون‌های ژنو و ایجاد نهادی مستقل برای انتساب فنی حملات سایبری ضروری است تا از سوءبرداشت‌ها و تشدید ناخواسته مخاصمات جلوگیری شود.

**واژگان کلیدی:** پاسخ نامتقارن، جنگ ترکیبی، جنگ ایران و رژیم صهیونیستی، دفاع مشروع، حقوق توسل به زور.

## سرآغاز

تحولات فناورانه در سپهر امنیت بین‌الملل، ماهیت، دامنه و سرعت مخاصمات را دگرگون کرده و پارادایم‌های کلاسیک حقوق و استراتژی را با چالش‌های بنیادین مواجه ساخته است. اگر قرن بیستم عرصه تثبیت قواعد حقوقی برای جنگ‌های متقارن و عمدتاً فیزیکی بود، قرن بیست و یکم دوران ظهور تهدیدات نامتقارن، ترکیبی و فناورانه‌ای است که در «منطقه خاکستری» میان صلح و جنگ عمل می‌کنند (Hoffman, 2007: 35). جنگ کوتاه اما پردامنه دوازده‌روزه تابستان ۱۴۰۴، تجلی تمام‌عیار این دگرگونی بود؛ درگیری‌ای که نه با غرش توپ‌ها که با کدهای مخرب در فضای سایبری آغاز شد و با فلج ساختن زیرساخت‌های حیاتی یک کشور، نظام حقوق بین‌الملل را در برابر این پرسش حیاتی قرار داد که مرز میان یک خرابکاری دیجیتال و یک «حمله مسلحانه» کجاست؟ این رویداد، نشان داد که مفاهیم حقوقی برآمده از دنیای وستفالیایی، مانند تمامیت ارضی و توسل به زور، نیازمند بازتعریفی متناسب با واقعیت‌های عصر دیجیتال هستند، واقعیتی که در آن یک حمله سایبری می‌تواند خساراتی به‌مراتب بیشتر از یک تهاجم نظامی محدود به بار آورد. مسئله اصلی این پژوهش، از همین نقطه، تنش میان حقوق سنتی و فناوری مدرن نشأت می‌گیرد. ماده ۲ (۴) منشور ملل متحد، دولت‌ها را از «توسل به زور» علیه تمامیت ارضی یا استقلال سیاسی هر کشوری منع می‌کند و ماده ۵۱ نیز حق ذاتی دفاع مشروع فردی یا جمعی را صرفاً در صورت وقوع «حمله مسلحانه» به رسمیت می‌شناسد (United Nations, 1945). این چارچوب حقوقی که برای جلوگیری از تکرار فجایع جنگ‌های جهانی طراحی شده بود، امروز در تفسیر و اعمال بر تهدیدات سایبری با ابهام جدی روبروست. حقوق بین‌الملل کلاسیک، در مورد اینکه آیا یک حمله

سایبری غیر فیزیکی که منجر به مرگ یا تخریب گسترده نمی‌شود؛ اما کارکردهای حیاتی یک دولت را مختل می‌سازد، می‌تواند به‌عنوان «حمله مسلحانه» تلقی شود، سکوت کرده است (Schmitt, 2017: 331). این خلأ حقوقی، یک «معضل بازدارندگی[1]» ایجاد می‌کند؛ از یکسو، پاسخ نظامی به یک حمله سایبری ممکن است به‌عنوان یک اقدام تجاوزکارانه نامتناسب تلقی شود و از سوی دیگر، عدم پاسخ قاطع می‌تواند دشمن را به انجام حملات بیشتر ترغیب کند (Rid, 2013: 160). این وضعیت، به‌ویژه برای کشورهایی که دکترین دفاعی آن‌ها بر بازدارندگی استوار است، یک چالش امنیتی- حقوقی فوری محسوب می‌شود.

پیشینه پژوهش در این حوزه را می‌توان به سه جریان اصلی تقسیم کرد. جریان نخست، به مبانی نظری «حق دفاع مشروع» در حقوق بین‌الملل می‌پردازد. آثاری چون کتاب مرجع یُرام دینشتاین (Dinstein, 2011) و مطالعات یان براونلی (Brownlie, 2008)، به تشریح دقیق معیارهای کلاسیک دفاع مشروع، ازجمله معیار «کارولین» (ضرورت، تناسب و فوریت)، پرداخته‌اند. این جریان، هرچند بنیان‌های نظری را به خوبی تبیین می‌کند، اما به‌طور مستقیم به چالش‌های ناشی از فناوری‌های نوظهور نمی‌پردازد. جریان دوم پژوهش‌ها، مشخصاً بر انطباق حقوق جنگ با فضای سایبری متمرکز است. در این حوزه، پروژه «راهنمای تالین» به سرپرستی مایکل اشمیت، نقطه عطفی محسوب می‌شود که تلاش کرده تا قواعد موجود حقوق بین‌الملل را بر عملیات سایبری اعمال کند (Schmitt, 2017). این راهنما و مقالات مرتبط با آن، به بحث‌های مهمی در مورد آستانه «حمله مسلحانه» در فضای سایبری دامن زده‌اند و معیارهایی چون «مقیاس و آثار» حمله را به‌عنوان شاخصی برای عبور از

1. deterrence dilemma

این آستانه پیشنهاد کرده‌اند (Hathaway et al, 2012: 845). با این حال، راهنمای تالین یک سند غیر الزام‌آور است و اجماع جهانی در مورد مفاد آن وجود ندارد. با این حال، ضعف اصلی جریان دوم در تمرکز بیش‌ازحد آن بر رویکردهای دولت - محور و فنی است. این جریان، اغلب نقش بازیگران غیردولتی و نیروهای نیابتی سایبری[1] را که به ابزار اصلی جنگ‌های ترکیبی در منطقه خاکستری تبدیل شده‌اند، نادیده می‌گیرد (Giles, 2016). پژوهش‌هایی که مشخصاً به مسئولیت بین‌المللی دولت در قبال اقدامات این گروه‌ها می‌پردازند، هنوز در ابتدای راه قرار دارند و نیازمند تحلیل‌های عمیق‌تر بر اساس مورد کاوی‌های واقعی هستند (Bílková, 2020). این در حالی است که ماهیت جنگ دوازده‌روزه نشان داد که انتساب حقوقی اقدامات این گروه‌ها به دولت حامی، پاشنه آشیل هرگونه پاسخ مشروع بین‌المللی است.» جریان سوم، به بررسی دکترین امنیتی و استراتژی دفاعی جمهوری اسلامی ایران اختصاص دارد. پژوهشگرانی مانند حسین سلیمی (۱۳۹۸) و کاظم غریب آبادی (۱۴۰۰) ابعاد مختلف دکترین دفاعی ایران را که مبتنی بر بازدارندگی، عدم تقارن و توسعه قابلیت‌های بومی است، تحلیل کرده‌اند. این مطالعات، به‌درستی به اهمیت فزاینده توانمندی‌های سایبری در استراتژی دفاعی ایران اشاره دارند (تبریزی، 1397). با وجود غنای این سه جریان پژوهشی، خلأ تحقیق در نقطه تلاقی آن‌ها آشکار است. تاکنون پژوهشی جامع و متمرکز که به تحلیل «استراتژی حقوقی - سیاسی» ایران، در توجیه یک پاسخ نظامی به حملات سایبری گسترده در چارچوب دکترین دفاع پیشگیرانه بپردازد، انجام نشده است؛ به عبارت دیگر، این سؤال که

1. Cyber Proxies

ایران چگونه ممکن است از ابزارهای حقوق بین‌الملل برای مشروعیت بخشی به یک اقدام دفاعی در برابر تهدیدی فناورانه و نامتقارن استفاده کند، به‌صورت یک مورد کاوی تحلیلی بررسی نشده است. به‌ویژه، این مقاله تلاش می‌کند تا نشان دهد چگونه یک قدرت منطقه‌ای مانند ایران، با تلفیق دکترین بازدارندگی کلاسیک و ابزارهای نوین جنگ نامتقارن، یک «استراتژی حقوقی - عملیاتی» منحصربه‌فرد را به اجرا می‌گذارد که هدف آن، نه فقط پاسخ به تهدید، بلکه شکل‌دهی به هنجارهای حقوقی آینده در فضای سایبری است. این تحلیل از منظر مطالعات راهبردی حقوقی که به بررسی استفاده از حقوق به‌عنوان ابزار قدرت می‌پردازد، کاملاً بدیع و نوآورانه است (زمانیان، 1401).

ازاین‌رو، اهمیت و ضرورت این پژوهش در ابعاد نظری و عملی نهفته است. در بعد نظری، این مقاله به غنی‌سازی ادبیات حقوق بین‌الملل در حوزه جنگ‌های مدرن و ارائه تحلیلی از تفسیر و عملکرد یک بازیگر مهم منطقه‌ای در برابر تهدیدات نوظهور کمک می‌کند. در بعد عملی و راهبردی، این تحلیل می‌تواند برای سیاستگذاران و استراتژیست‌های نظامی، درکی عمیق‌تر از منطق حقوقی - امنیتی ایران و همچنین پویایی‌های بالقوه تشدید تنش در مخاصمات آینده فراهم آورد. درک این منطق، برای جلوگیری از سوءبرداشت و محاسبات اشتباه که می‌تواند به درگیری‌های گسترده‌تر منجر شود، حیاتی است. بر این اساس، پرسش اصلی پژوهش این است که: استراتژی حقوقی - سیاسی ایران در توجیه اقدامات خود در جنگ دوازده‌روزه، چه تفسیری از حق دفاع پیشگیرانه در برابر تهدیدات فناورانه ارائه داد و این تفسیر چه پیامدهایی برای نظام حقوق بین‌الملل دارد؟ در پاسخ به این پرسش، فرضیه مقاله این است که ایران در جنگ

دوازده‌روزه، با عبور از دکترین کلاسیک «دفاع پیشگیرانه»، یک دکترین نوآورانه «پاسخ ترکیبی و نامتقارن» را به اجرا گذاشت. این رویکرد، ضمن به چالش کشیدن هنجارهای کلاسیک، بر ضرورت گذار از مفاهیم سنتی به سمت یک چارچوب حقوقی جدید برای جنگ‌های ترکیبی تأکید دارد. برای آزمون این ادعا، مقاله در چهار بخش سازمان‌دهی شده است. پس از طرح کلی مسئله، پیشینه و چارچوب مفهومی در بخش دوم، مبانی نظری دفاع مشروع و چالش‌های حقوقی ناشی از فناوری‌های نوظهور را با جزئیات بیشتری واکاوی می‌کند. بخش سوم، به‌عنوان قلب مقاله، به تحلیل مورد کاوی استراتژی حقوقی - سیاسی ایران در طول جنگ دوازده‌روزه می‌پردازد. درنهایت، بخش چهارم به نتیجه‌گیری، جمع‌بندی یافته‌ها و ارائه پیامدهای این رویداد برای نظام حقوقی و امنیتی بین‌المللی اختصاص خواهد یافت.

## ۱. چارچوب نظری: حق توسل به زور در عصر جنگ‌های ترکیبی

شالوده نظام حقوق بین‌الملل معاصر بر اصل بنیادین منع توسل به زور استوار است که در ماده ۲ (۴) منشور ملل متحد، متبلور شده است. این اصل، به‌عنوان یک قاعده آمره، هرگونه تهدید یا استفاده از نیروی نظامی علیه تمامیت ارضی یا استقلال سیاسی دولت‌ها را ممنوع می‌کند. تنها استثنای صریح و مورد اجماع جهانی بر این قاعده، حق ذاتی دفاع مشروع فردی یا جمعی ذیل ماده ۵۱ منشور است. با این حال، اعمال این حق منوط به یک پیش‌شرط اساسی است: وقوع یک «حمله مسلحانه» علیه دولت عضو (United Nations, 1945). دیوان بین‌المللی دادگستری در قضیه تاریخی نیکاراگوئه علیه ایالات‌متحده، به دقت این آستانه را تبیین کرد و تأکید کرد که هرگونه توسل به زوری، لزوماً مصداق «حمله مسلحانه»

نیست. دیوان میان «وخیم‌ترین اشکال توسل به زور» (که حق دفاع مشروع را فعال می‌کنند) و «اشکال خفیف‌تر» (مانند حوادث مرزی جزئی یا کمک تسلیحاتی به شورشیان) تمایز قائل شد (ICJ Reports, 1986: para. 191). علاوه بر این، حقوق بین‌الملل عرفی، مشروعیت اقدام دفاعی را به سه معیار کلاسیک برگرفته از قضیه «کارولین» یعنی ضرورت، تناسب و فوریت مقید ساخته است (Jennings & Watts, 1992: 421). چالش حقوقی که مستقیماً زمینه را برای جنگ دوازده‌روزه فراهم کرد، مربوط به تفسیر زمان‌بندی و آستانه اعمال این حق است. حقوق بین‌الملل عرفی، «دفاع مشروع پیشگیرانه[1]» را صرفاً در شرایطی بسیار مضیق، یعنی مواجهه با یک حمله قطعی و «قریب‌الوقوع» که «هیچ فرصتی برای مشورت و هیچ راه دیگری برای اقدام» باقی نگذارد، مجاز شمرده است (Gray, 2018: 160). با این حال، برخی دولت‌ها کوشیده‌اند این مفهوم را به دکترین بسیار موسع‌تر و فاقد وجاهت حقوقی «دفاع پیش‌دستانه[2]» تسری دهند. این دکترین که به دولت اجازه می‌دهد علیه تهدیداتی که هنوز قریب‌الوقوع نیستند اما «در آینده» می‌توانند به خطری جدی تبدیل شوند، اقدام نظامی کند (Glennon, 2003: 98)، با مخالفت شدید جامعه جهانی مواجه شده است؛ زیرا مرز میان دفاع و تجاوز را عملاً از بین می‌برد (Franck, 2002: 52).

حمله نظامی غافلگیرانه اسرائیل در ۲۳ خرداد ۱۴۰۴ (۱۳ ژوئن ۲۰۲۵) علیه تأسیسات هسته‌ای و نظامی ایران (Nextgov, 2025; Politico, 2025)، دقیقاً بر مبنای همین دکترین مردود «دفاع پیش‌دستانه» توجیه شد (Nextgov, 2025). این اقدام که آشکارا فاقد وصف «قریب‌الوقوع بودن» تهدید بود، از

1. Pre-emptive Self-Defense
2. Preventive Defense

سوی بسیاری از پژوهشگران حقوقی و دولت‌ها به‌عنوان نقض صریح قوانین بین‌المللی و فعل تجاوزکارانه محکوم شد (انجمن ایرانی مطالعات سازمان ملل متحد، ۱۴۰۴، مرکز پژوهش‌های مجلس، ۱۴۰۴). این تجاوز اولیه، مبنای حقوقی لازم را برای پاسخ ایران در چارچوب ماده ۵۱ فراهم آورد. پیچیدگی دوم در تحلیل این جنگ، ماهیت «ترکیبی» آن است. جنگ‌های مدرن دیگر صرفاً نظامی نیستند، بلکه ترکیبی از عملیات نظامی کلاسیک، جنگ اطلاعاتی، حملات سایبری گسترده و بهره‌گیری از عملیات مخفیانه هستند (Hoffman, 2007: 35). اسرائیل در این جنگ، علاوه بر حملات هوایی، از «عملیات خرابکارانه مخفیانه» برای از کار انداختن پرتابگرهای ایران (Nextgov, 2025) و «پایگاه پهپادی موساد» در داخل خاک ایران استفاده کرد (JPost, 2025). این ماهیت ترکیبی، چالش‌های حقوقی جدیدی را در خصوص آستانه «حمله مسلحانه» ایجاد می‌کند. آیا یک حمله سایبری که منجر به مرگ یا تخریب فیزیکی نمی‌شود اما زیرساخت‌های حیاتی (مانند شبکه برق یا نظام بانکی) را فلج می‌کند، می‌تواند «حمله مسلحانه» تلقی شود؟ (Zetter, 2014: 175). جامعه حقوقی در «راهنمای تالین» تلاش کرده است تا با ارائه معیار «مقیاس و آثار» به این پرسش پاسخ دهد؛ بدین معنا که اگر آثار یک حمله سایبری با یک حمله نظامی کلاسیک قابل‌مقایسه باشد، می‌تواند حمله مسلحانه تلقی شود (Schmitt, 2017: 342). با این حال، این معیار همچنان مبهم است (Roscini, 2014: 125) و بازیگران دولتی از همین ابهام در «منطقه خاکستری» برای پیشبرد اهداف خود استفاده می‌کنند.

حتی اگر یک حمله سایبری به آستانه «حمله مسلحانه» نرسد، همچنان می‌تواند یک «فعل متخلفانه بین‌المللی» باشد. بر اساس اصل حاکمیت، هرگونه نفوذ سایبری به زیرساخت‌های

حیاتی یک دولت دیگر یا مداخله در کارکردهای ذاتی دولتی آن، مصداق بارز «نقض حاکمیت[1]» و «اصل عدم‌مداخله» تلقی می‌شود (Schmitt, 2017: 19؛ رستمی، ۱۴۰۱: ۱۶۲). این امر به دولت قربانی اجازه می‌دهد تا به «اقدامات متقابل[2]» دست بزند. درنهایت، یکی از پیچیده‌ترین ابعاد جنگ‌های ترکیبی، استفاده از بازیگران غیردولتی و نیروهای نیابتی است. تحلیل‌های پس از جنگ دوازده‌روزه نشان داد که پاسخ سایبری ایران، شامل «سه لایه مجزا از بازیگران» بود که شامل گروه‌های هکتیویست مانند «سایبر فتاح» می‌شد که مسئولیت حملات سایبری و انتشار اطلاعات علیه اسرائیل را بر عهده گرفتند (Nextgov, 2025; Security Scorecard, 2025). این امر مسئله «انتساب[3]» را مطرح می‌کند. بر اساس اصل «مراقبت بایسته»، هر دولتی موظف است آگاهانه اجازه ندهد قلمروش برای ارتکاب اعمالی که حقوق دیگر دولت‌ها را نقض می‌کند، مورد استفاده قرار گیرد (ICJ Reports, 1949: 22). اگر دولتی از فعالیت‌های یک گروه هکری در قلمرو خودآگاه باشد و اقدامات معقولی برای توقف آن انجام ندهد، به دلیل «قصور» مسئول است (Tikk & Kaska, 2017: 59). اثبات «حمایت فعالانه» یا «کنترل مؤثر» یک دولت بر گروه‌های نیابتی (Lieber West Point, 2025)، می‌تواند آن حمله را مستقیماً به دولت حامی منتسب کرده و آستانه پاسخ نظامی را فعال سازد (جمشیدی، ۱۴۰۲: ۱۱۲)؛ بنابراین چارچوب نظری این مقاله بر این پایه استوار است که جنگ دوازده‌روزه، تبلور یک تجاوز آشکار نظامی بود که با ابزارهای جنگ ترکیبی (سایبری و مخفیانه) تکمیل شد و پاسخ

1. Violation of Sovereignty
2. Countermeasures
3. Attribution

ایران نیز باید در همین چارچوب ترکیبی و در قالب حق دفاع مشروع تحلیل شود.

## ۲. تبیین مؤلفه‌های «آموزه پاسخ نامتقارن و ترکیبی»

همان‌طور که در بخش پیشین اشاره شد، اقدام نظامی مستقیم اسرائیل در ۲۳ خرداد ۱۴۰۴، یک «فعل تجاوزکارانه» و نقض آشکار ماده ۲ (۴) منشور ملل متحد بود (مرکز پژوهش‌های مجلس، ۱۴۰۴) که حق دفاع مشروع ایران ذیل ماده ۵۱ را فعال ساخت. با این حال، یافته اصلی این پژوهش آن است که ایران در پاسخ به این تجاوز، از یک الگوی دفاعی متقارن (مثلاً حمله هوایی متقابل) استفاده نکرد، بلکه از یک دکترین دفاعی پیچیده‌تر، یعنی «آموزه پاسخ نامتقارن و ترکیبی» بهره جست. اندیشه مذکور، دکترین دفاعی چندوجهی است که در مواجهه با یک تهاجم نظامی از سوی یک دشمن برتر (از نظر هوایی)، به‌جای درگیری در میدان نبرد انتخابی دشمن، آگاهانه عرصه نبرد را به حوزه‌هایی منتقل می‌کند که در آن دارای مزیت نسبی است (سلیمی، ۱۳۹۸: 60). هدف این آموزه، نه پیروزی در یک جنگ کلاسیک، بلکه «تحمیل هزینه غیرقابل تحمل» بر دشمن و «فلج سازی کارکردی» جامعه آن از طریق سه مؤلفه هم‌زمان است:

**جدول ۱: چارچوب تحلیلی آموزه پاسخ نامتقارن و ترکیبی ایران**

| مؤلفه آموزه | ابزار اعمالی اصلی | هدف راهبردی | توصیف حقوقی (از منظر ایران) |
|---|---|---|---|
| ۱. پاسخ کینتیک نامتقارن | صدها موشک بالستیک و پهپادهای انتحاری (مانند سجیل، | واردکردن شوک مستقیم، عبور از سامانه‌های دفاعی، ایجاد بازدارندگی | حق دفاع مشروع مستقیم (ماده ۵۱) در پاسخ به تجاوز اولیه اسرائیل (انجمن ایرانی |

| مؤلفه آموزه | ابزار اعمالی اصلی | هدف راهبردی | توصیف حقوقی (از منظر ایران) |
|---|---|---|---|
| | شهاب و شاهد) | سخت، تحمیل هزینه روانی و فیزیکی | مطالعات سازمان ملل، ۱۴۰۴) |
| 2. جنگ سایبری تهاجمی | حملات سایبری علیه زیرساخت‌ها (مانند بانک‌ها، رسانه‌ها، بیمارستان‌ها و بورس) | فلج سازی کارکردی اقتصاد و خدمات اجتماعی، ایجاد وحشت عمومی، تکمیل فشار (Nextgov, 2025) | اقدام متقابل (Countermeasure) در برابر حملات سایبری و خرابکاری‌های پیشین اسرائیل (Security Scorecard, 2025) |
| ۳. گسترش جبهه (منطقه خاکستری) | فعال‌سازی بازیگران نیابتی (مانند حوثی‌ها) برای شلیک موشک و پهپاد | فرسایش منابع دفاعی دشمن (مانند موشک‌های پدافندی)، پراکنده کردن تمرکز نظامی، ایجاد ابهام راهبردی | اقدام مستقل توسط یک بازیگر ثالث در چارچوب «محور مقاومت» (Lieber West Point, 2025) |

## 2-1. مؤلفه اول: پاسخ کینتیک نامتقارن (دکترین موشکی)

مؤلفه اصلی و آشکارترین وجه این آموزه، عدم پاسخ متقارن بود. اسرائیل جنگ را با حملات هوایی پیشرفته (با استفاده از بیش از ۲۰۰ هواپیما)، عملیات مخفیانه کماندویی و خرابکاری پهپادی از داخل خاک ایران آغاز کرد (Politico, 2025; JPost, 2025). پاسخ متقارن به این اقدام، اعزام نیروی هوایی ایران برای مقابله با جنگنده‌های اسرائیلی بود. دکترین ایران، با آگاهی از عدم برتری هوایی کلاسیک، این عرصه نبرد را به‌طور کامل نادیده گرفت و در عوض، بر نقطه قوت استراتژیک خود یعنی توان موشکی بالستیک و پهپادی تمرکز کرد (USMCU, 2025). این یک انتخاب کاملاً نامتقارن است: تغییر میدان نبرد از «جنگ بر سر آسمان» (که اسرائیل در آن

برتر است) به «جنگ از زمین علیه اهداف» (که ایران در آن دست برتر را دارد). هدف از شلیک صدها موشک (ازجمله موشک‌های ویژه و ارتقا یافته) و پهپادها در قالب عملیات «وعده صادق ۳»، نه یک پیروزی نظامی تاکتیکی، بلکه «تحمیل هزینه مستقیم و دردناک» به عمق خاک اسرائیل بود (دیپلماسی ایرانی، ۱۴۰۴). حملات ایران مستقیماً شهرها و زیرساخت‌های کلیدی مانند تل‌آویو، حیفا، فرودگاه بن گوریون، مراکز نظامی (مانند مقر نظامی کریا) و حتی مراکز حساس اقتصادی و علمی (مانند مؤسسه علوم وایزمن و پالایشگاه حیفا) را هدف قرار داد. این اقدام، بُعد «کینتیک» (فیزیکی) این آموزه ترکیبی بود که هدف آن ایجاد شوک روانی بر جمعیت و فشار مستقیم بر تصمیم گیران اسرائیلی بود (IDSA, 2025).

**۲-۲. مؤلفه دوم: جنگ سایبری تهاجمی (فلج سازی کارکردی)**

هم‌زمان با حملات موشکی، مؤلفه دوم آموزه یعنی جنگ سایبری، فعال شد. این بخش، تکمیل‌کننده فشار کینتیک بود. اگر موشک‌ها «جسم» دشمن (زیرساخت‌ها و پایگاه‌ها) را هدف می‌گرفتند، حملات سایبری «سیستم عصبی» آن (اقتصاد و خدمات) را هدف قرار می‌دادند. گزارش‌های متعددی از حملات سایبری تهاجمی توسط گروه‌های هکری همسو با ایران علیه نهادهای صهیونیستی حکایت دارد (Atlantic Council, 2025). برای مثال، هم‌زمان با حملات، گروه هکری «گنجشک درنده» مسئولیت حمله سایبری به بانک سپه در ایران را بر عهده گرفت که نشان‌دهنده تبادل آتش دیجیتال بود (Security Scorecard, 2025)؛ اما در بُعد تهاجمی ایران، هدف‌گیری «برای تضعیف روحیه» (Nextgov, 2025) و همچنین ایجاد اختلال در بورس و خدمات دولتی بود. این حملات همچنین شامل هک و قطع موقت پخش شبکه‌های تلویزیونی اسرائیل و انتشار پیام‌های اعتراضی و

جنگ روانی می‌شد. هدف در اینجا «فلج سازی کارکردی» جامعه و تضعیف روحیه عمومی از طریق اختلال در خدمات روزمره بود (Rid, 2013: 160).

### 2-3. مؤلفه سوم: گسترش جبهه (بهره‌گیری از منطقه خاکستری)

مؤلفه نهایی این آموزه، فعال‌سازی بازیگران ثالث و متحدان منطقه‌ای، به‌ویژه حوثی‌ها در یمن، بود. هم‌زمان با شلیک موشک‌ها از ایران، حوثی‌ها نیز اقدام به شلیک موشک‌های بالستیک و پهپاد به سمت اسرائیل کردند. این اقدام، سه هدف استراتژیک کلیدی را دنبال می‌کرد:

1) فرسایش دفاعی: وادار کردن اسرائیل به مصرف موشک‌های گران‌قیمت پدافندی خود (مانند سامانه ارو) علیه تهدیداتی که از جبهه‌ای کاملاً متفاوت می‌آیند. این امر، به‌ویژه با توجه به گزارش‌هایی مبنی بر اتمام ذخایر موشک‌های رهگیر اسرائیل (Wall Street Journal, 2025) اهمیت می‌یابد.
2) پراکندگی تمرکز: ایجاد یک تهدید چند جبهه‌ای که توان محاسباتی و نظامی اسرائیل را تحلیل می‌برد و آن را مجبور به دفاع هم‌زمان در دو جبهه متفاوت می‌کند.
3) ابهام حقوقی (منطقه خاکستری): اگرچه در سطح راهبردی، این حملات کاملاً هماهنگ بودند؛ اما در سطح حقوقی، ایران می‌توانست ادعا کند که این اقدامات تصمیم مستقل متحدانش در «محور مقاومت» بوده و مسئولیت مستقیم بین‌المللی متوجه تهران نیست. این دقیقاً مصداق بهره‌برداری از «منطقه خاکستری» در حقوق بین‌الملل برای فرار از انتساب مستقیم است (Lieber West Point, 2025).

این سه مؤلفه در کنار یکدیگر، «آموزه پاسخ نامتقارن و ترکیبی» را تشکیل می‌دهند.

## ۳. تحلیل انطباقی موردکاوی: آموزه و عمل در جنگ دوازده‌روزه

بخش پیشین، چارچوب نظری «آموزه پاسخ نامتقارن و ترکیبی» را تبیین کرد. این بخش اکنون به‌صورت مستند به تحلیل وقایع جنگ دوازده‌روزه می‌پردازد تا نشان دهد که چگونه اقدامات ایران در میدان عمل، انطباق کامل با سه مؤلفه این آموزه داشته است.

### 3-1. جرقه جنگ: تجاوز نظامی اسرائیل و دکترین مردود پیش‌دستانه

جرقه جنگ دوازده‌روزه تهاجم نظامی مستقیم، غافلگیرکننده و کینتیک از سوی اسرائیل در بامداد ۲۳ خرداد ۱۴۰۴ (۱۳ ژوئن ۲۰۲۵) بود (Politico, 2025). این حمله که با پشتیبانی اطلاعاتی و فنی ایالات‌متحده صورت گرفت، عملیاتی «ترکیبی» و پیچیده بود که شامل ترور فرماندهان ارشد نظامی، حملات هوایی گسترده (با بیش از ۲۰۰ هواپیما) علیه تأسیسات هسته‌ای (نطنز، اصفهان)، پایگاه‌های نظامی و زیرساخت‌های موشکی ایران و هم‌زمان، عملیات خرابکارانه مخفیانه موساد از داخل خاک ایران برای از کار انداختن سامانه‌های پدافندی و پرتابگرها بود (JPost, 2025; Nextgov, 2025). این تهاجم، همچنین منجر به ترور هدفمند فرماندهان ارشد نظامی و دانشمندان هسته‌ای ایران شد. اسرائیل این اقدام را ذیل دکترین «دفاع پیش‌دستانه ضروری» برای مقابله با «تهدید وجودی» هسته‌ای ایران توجیه کرد (Nextgov, 2025). همان‌طور که در بخش مبانی نظری اشاره شد، این دکترین فاقد هرگونه وجاهت در حقوق بین‌الملل بوده و از سوی اکثریت قاطع دولت‌ها و حقوق‌دانان، مصداق بارز «فعل تجاوزکارانه» و نقض آشکار ماده ۲ (۴) منشور ملل متحد تلقی می‌شود (مرکز پژوهش‌های مجلس، ۱۴۰۴). این تجاوز نظامی آشکار، مبنای

حقوقی لازم را برای فعال شدن حق ذاتی دفاع مشروع ایران ذیل ماده ۵۱ منشور فراهم آورد.

### 2-3. پاسخ ایران: اجرای گام‌به‌گام آموزه پاسخ نامتقارن و ترکیبی

در مواجهه با این تجاوز، ایران از پاسخ متقارن (مانند درگیری هوایی) پرهیز کرد و دقیقاً «آموزه پاسخ نامتقارن و ترکیبی» را در سه فاز عملیاتی موازی فعال کرد:

الف) اجرای مؤلفه اول: پاسخ کینتیک نامتقارن (عملیات وعده صادق ۳): این مؤلفه، آشکارترین بخش پاسخ ایران بود. تنها چند ساعت پس از حملات اسرائیل، ایران با شلیک صدها موشک بالستیک (ازجمله سجیل و شهاب) و پهپادهای انتحاری (شاهد)، عملیات «وعده صادق ۳» را آغاز کرد (Atlantic Council, 2025) و مصداق اجرای مؤلفه اول (پاسخ کینتیک نامتقارن) بود. ایران به‌جای درگیری هوایی، عرصه نبرد را به حوزه موشکی (نقطه قوت خود) منتقل کرد. هدفگیری ایران نیز صرفاً نظامی نبود، بلکه با هدف «فلج سازی کارکردی» و ایجاد شوک روانی صورت گرفت. اهداف کلیدی شامل: مراکز فرماندهی و نظامی (مانند مقر نظامی کریا در تل‌آویو)، زیرساخت‌های استراتژیک (مانند فرودگاه بن گوریون، پالایشگاه نفت حیفا و موسسه علوم وایزمن و زیرساخت‌های مخفی نظامی حیاتی در تل‌آویو، بت یام و ریشون لتسیون شد و ده‌ها کشته و زخمی بر جای گذاشت) (IDSA, 2025). این پاسخ مستقیم، سنگین و کینتیک، هسته اصلی دفاع مشروع ایران در برابر تجاوز اسرائیل بود.

ب) اجرای مؤلفه دوم: جنگ سایبری تهاجمی: هم‌زمان با شلیک موشک‌ها، مؤلفه دوم آموزه نیز فعال شد. تحلیل‌های پس از جنگ نشان داد که «پاسخ سایبری ایران شامل سه لایه مجزا از بازیگران» بود (Nextgov, 2025). این حملات که شامل هک شبکه‌های تلویزیونی اسرائیل، انتشار اطلاعات

نادرست و حملات مختل‌کننده علیه زیرساخت‌های مالی و خدماتی بود، دقیقاً با هدف «ارعاب غیرنظامیان و تضعیف روحیه» و تکمیل فشار ناشی از حملات موشکی صورت گرفت (Nextgov, 2025). این تبادل آتش دیجیتال، بُعد دوم جنگ ترکیبی را تشکیل می‌داد (Atlantic Council, 2025).

ج) اجرای مؤلفه سوم: گسترش جبهه (منطقه خاکستری): درنهایت، مؤلفه سوم آموزه با ورود حوثی‌های یمن به درگیری فعال شد. حوثی‌ها هم‌زمان با ایران، اقدام به شلیک چندین موشک بالستیک به سمت اسرائیل کردند. این اقدام دقیقاً اهداف استراتژیک مؤلفه سوم را محقق ساخت؛ فرسایش دفاعی (وادار کردن اسرائیل به مصرف رهگیرهای گران‌قیمت پدافندی علیه جبهه دوم) و پراکندگی تمرکز نظامی اسرائیل (Lieber West Point, 2025). این اقدام، ضمن هماهنگی راهبردی، به ایران امکان می‌داد تا در سطح حقوقی از مسئولیت مستقیم آن شانه خالی کند.

**جدول ۲: گاه‌شمار تحلیلی انطباق وقایع جنگ با آموزه پاسخ ترکیبی**

| روزشمار جنگ | اقدام اصلی (اسرائیل / ایران) | مؤلفه آموزه در حال اجرا | هدف حقوقی-راهبردی |
|---|---|---|---|
| روز اول (۲۳ خرداد) | حمله نظامی مستقیم اسرائیل به تأسیسات هسته‌ای و نظامی ایران | تجاوز اولیه (اسرائیل) | اجرای دکترین مردود «دفاع پیش‌دستانه» |
| روز اول (۲۳ خرداد) | پاسخ فوری موشکی و پهپادی ایران (وعده صادق ۳) به تل‌آویو و حیفا | مؤلفه ۱ (پاسخ کینتیک نامتقارن) | اعمال حق دفاع مشروع (ماده ۵۱) و ایجاد بازدارندگی سخت |
| روز اول (۲۳ خرداد) | حمله موشکی حوثی‌ها از یمن به سمت اسرائیل | مؤلفه ۳ (گسترش جبهه) | فرسایش دفاعی اسرائیل و ایجاد ابهام در منطقه خاکستری |
| روز دوم تا دهم | حملات سایبری متقابل؛ هک بانک‌ها و | مؤلفه ۲ (جنگ سایبری) | فلج سازی کارکردی و تکمیل فشار کینتیک |

| | | | |
|---|---|---|---|
| | رسانه‌های اسرائیل (توسط گروه‌های نیابتی). | | (Nextgov, 2025) |
| روز نهم (۲ تیر) | حمله نظامی مستقیم آمریکا به سایت‌های هسته‌ای ایران. | تشدید تنش (بازیگر ثالث) | حمایت مستقیم از اسرائیل و ارسال پیام راهبردی به ایران |
| روز دهم تا دوازدهم | تبادل آتش سنگین موشکی و پهپادی میان ایران و اسرائیل | تداوم مؤلفه ۱ | تحمیل هزینه نهایی پیش از پذیرش آتش‌بس |

## ۳-۳. بازتاب حقوقی: جنگ روایت‌ها و ناکارآمدی نهادهای بین‌المللی

تحلیل وقایع جنگ دوازده‌روزه، بیش از هر چیز نشان‌دهنده استفاده از حقوق بین‌الملل به‌عنوان «ابزار جنگی» یا «جنگ حقوقی» توسط طرفین بود. جدول (۳) این تقابل روایت‌ها را به خوبی نشان می‌دهد.

**جدول ۳: تحلیل تطبیقی مواضع حقوقی طرفین در جنگ دوازده‌روزه**

| موضوع حقوقی | موضع حقوقی اسرائیل و متحدان | موضع حقوقی ایران و حامیان | تحلیل شکاف حقوقی (ابهام در ح ب) |
|---|---|---|---|
| حمله اولیه (۲۳ خرداد) | دفاع پیش‌دستانه ضروری در برابر یک تهدید وجودی هسته‌ای؛ اقدامی مشروع برای جلوگیری از دستیابی ایران به سلاح | فعل تجاوزکارانه و نقض آشکار ماده ۲ (۴) منشور و حاکمیت ملی ایران؛ هیچ حمله مسلحانه‌ای از سوی ایران صورت نگرفته بود | وضعیت حقوقی «دفاع پیش‌دستانه» در حقوق بین‌الملل بسیار مبهم و مورد اختلاف است و اجماع جهانی در مورد آن وجود ندارد |
| پاسخ موشکی ایران (وعده صادق ۳) | حمله مسلحانه نامتناسب علیه اهداف غیرنظامی و نقض حقوق بشردوستانه؛ مصداق تروریسم دولتی برای ایجاد وحشت در میان شهروندان | دفاع مشروع متناسب ذیل ماده ۵۱ در پاسخ به تجاوز اولیه؛ زیرساخت‌های هدف، دارای کاربری دوگانه و در خدمت ماشین جنگی دشمن بوده‌اند | عدم وجود تعریف دقیق و مورد اجماع از «حمله مسلحانه» در فضای سایبری؛ ابهام در مورد وضعیت حقوقی زیرساخت‌های دوگانه |

| | | | |
|---|---|---|---|
| حملات حوثی‌ها از یمن | مسئولیت مستقیم دولت ایران؛ این گروه‌ها تحت «کنترل مؤثر» سپاه پاسداران عمل کرده و اقداماتشان مستقیماً به ایران قابل انتساب است | اقدامات بازیگران غیردولتی مستقل؛ ایران هیچ کنترل مستقیمی بر این گروه‌ها نداشته و صرفاً از مقاومت مشروع آن‌ها حمایت معنوی می‌کند | آستانه بالای اثبات «کنترل مؤثر» برای انتساب اقدامات یک گروه نیابتی به یک دولت که اثبات آن در عمل بسیار دشوار است |

جدول فوق تقابل روایت‌های حقوقی را به تصویر می‌کشد؛ اما بررسی دقیق‌تر، چالش‌های بنیادین در موضع حقوقی اسرائیل را آشکارتر می‌سازد. استناد اسرائیل به دکترین «دفاع پیش‌دستانه» برای توجیه حمله اولیه، بر تفسیری موسع و بسیار بحث‌برانگیز از ماده ۵۱ منشور استوار است که فاقد اجماع در جامعه بین‌المللی است. اکثریت دولت‌ها و حقوق‌دانان برجسته، چنین تفسیری را که مرز میان دفاع و تجاوز را کمرنگ می‌سازد، مغایر با هدف و مقصود منشور ملل متحد در محدود کردن توسل به زور می‌دانند (مرکز پژوهش‌های مجلس، ۱۴۰۴). در مقابل، پاسخ ایران هرچند از منظر انطباق با اصول حقوق بشردوستانه قابل نقد است (که در بخش بعد به آن پرداخته می‌شود) اما در چارچوب کلی دفاع مشروع (به‌عنوان واکنشی به یک حمله مسلحانه پیشین) از مبنای حقوقی قابل دفاع‌تری برخوردار است؛ بنابراین، اقدام اولیه اسرائیل به‌عنوان فعل متخلفانه آغازگر مخاصمه، چالش اصلی را برای نظام حقوقی بین‌المللی ایجاد کرد. درنهایت، این جنگ ناکارآمدی نهادهای امنیت جمعی را به نمایش گذاشت. شورای امنیت سازمان ملل به دلیل وتوی قدرت‌های بزرگ، عملاً فلج شد و نتوانست هیچ اقدام مؤثری برای مهار بحران انجام دهد (انجمن ایرانی مطالعات سازمان ملل متحد، ۱۴۰۴). این ناکارآمدی نشان داد که

ابزارهای سنتی حقوق بین‌الملل برای مدیریت مخاصمات ترکیبی مدرن، کارایی لازم را ندارند.

## ۴. پیامدهای انسانی و چالش‌های حقوق بشردوستانه

در حالی که اقدام اولیه اسرائیل آغاز جنگ را متوجه آن رژیم می‌کند، اقدامات طرفین در طول مخاصمه نیز باید با اصول بنیادین حقوق بشردوستانه، یعنی اصل تمایز و اصل تناسب سنجیده شود (ICRC, 2005, Rules 7 & 14). گزارش‌های مستند جنگ دوازده‌روزه، نقض گسترده این اصول را توسط طرف صهیونیستی نشان می‌دهد؛ گزارش‌ها بیانگر آن بود که حملات اولیه اسرائیل صرفاً به اهداف نظامی محدود نماند. ترور هدفمند ده‌ها دانشمند هسته‌ای (JPost, 2025) و فرماندهان نظامی، حمله به ساختمان صداوسیما (که یک هدف غیرنظامی با کاربری دوگانه مورد اختلاف است) و به‌ویژه، حمله به زندان اوین که بر اساس گزارش‌های رسمی داخلی منجر به کشته شدن ده‌ها نفر شد، همگی نقض آشکار اصل تمایز هستند. همچنین حملات به زیرساخت‌های برق (که منجر به قطع برق در شهران شد) و حملات سایبری که منجر به قطع گسترده اینترنت در شهرهای بزرگ ایران شد (The Record, 2025)، مصداق بارز آسیب جانبی «بیش‌ازحد» (Excessive) به شهروندان و نقض اصل تناسب است. در مقابل نیز رسانه‌های اسرائیلی ادعا کردند، در اجرای مؤلفه اول (پاسخ کینتیک)، حملات موشکی ایران نیز در مواردی منجر به آسیب به اهداف غیرنظامی شده است؛ مهم‌ترین نمونه، اصابت مستقیم موشک به مرکز پزشکی سوروکا در بئرشبع (که خسارات گسترده‌ای به بخش جراحی وارد کرد) و همچنین آسیب مستقیم به مناطقی در بت یام، ریشون لتسیون و تل‌آویو بود که منجر به کشته و زخمی شدن ده‌ها غیرنظامی شد (IDSA, 2025). ادعایی که با توجه به

مخفی بودن زیرساخت‌های نظامی در پوشش غیرنظامی موجه به نظر نمی‌رسد. چنانچه برای ایران هدفگیری زیرساخت‌های دوگانه مشروع بوده و اطلاعاتی مبنی بر اختفای سران نظامی صهیونیستی در این نوع مکان‌ها در اختیار دارد (دیپلماسی ایرانی، ۱۴۰۴)؛ این جنگ نشان داد که در نبردهای ترکیبی، غیرنظامیان به «قربانیان نامرئی» تبدیل می‌شوند و زیرساخت‌های حیاتی (آب، برق، بهداشت، خدمات بانکی) به اولین اهداف جنگی بدل می‌شوند.

## فرجام سخن

پژوهش حاضر با هدف واکاوی استراتژی حقوقی-راهبردی ایران در جنگ دوازده‌روزه تابستان ۱۴۰۴ آغاز شد. پرسش محوری این بود که ایران در مواجهه با تهاجم نظامی مستقیم و غافلگیرانه اسرائیل در ۲۳ خرداد، چه دکترین دفاعی را اتخاذ کرد و این اقدام چه پیامدهایی برای حقوق بین‌الملل داشت؟ یافته اصلی این مقاله، شناسایی و تبیین دکترین نوآورانه با عنوان «آموزه پاسخ نامتقارن و ترکیبی» است. این پژوهش نشان داد که استراتژی ایران، نه یک دفاع پیشگیرانه کلاسیک و نه یک پاسخ متقارن، بلکه دکترین چندوجهی و پیچیده‌ای بود که آگاهانه عرصه نبرد را از حوزه برتری دشمن (نبرد هوایی) به حوزه‌های مزیت نسبی ایران منتقل کرد. فرضیه مقاله مبنی بر وجود این آموزه، از طریق تحلیل انطباقی در بخش‌های مقاله اثبات شد. بخش اول، با تحلیل اقدام اولیه اسرائیل، ثابت کرد که این حمله (مبتنی بر دکترین مردود پیش‌دستانه) مصداق بارز «فعل تجاوزکارانه» بوده و مبنای حقوقی لازم برای «دفاع مشروع» ایران ذیل ماده ۵۱ منشور را فراهم آورده است. بخش دوم، به تبیین نظری مؤلفه‌های سه‌گانه این آموزه پرداخت. بخش سوم

نیز نشان داد که پاسخ ایران در عمل، انطباق کامل با این آموزه داشته است: اجرای مؤلفه اول (پاسخ کینتیک نامتقارن) از طریق عملیات «وعده صادق ۳» و شلیک صدها موشک بالستیک و پهپاد به عمق خاک اسرائیل که بازدارندگی سخت و شوک روانی را محقق ساخت. اجرای مؤلفه دوم (جنگ سایبری) از طریق حملات هم‌زمان سایبری برای فلج سازی کارکردی اقتصاد و خدمات دشمن. اجرای مؤلفه سوم (گسترش جبهه) از طریق فعال‌سازی هم‌زمان جبهه یمن (حوثی‌ها) برای فرسایش توان پدافندی و پراکندگی تمرکز اسرائیل. نوآوری این پژوهش در کدگذاری و ارائه این مدل سه وجهی، به‌عنوان دکترین دفاعی منسجم است. این جنگ همچنین نشان داد که آستانه توسل به اقدامات خصمانه در حال کاهش است و مهم‌تر از آن، ناکارآمدی نهادهای امنیت جمعی (شورای امنیت) را در مدیریت جنگ‌های ترکیبی مدرن آشکار ساخت. در این میان، ورود مستقیم ایالات‌متحده به جنگ و بمباران تأسیسات هسته‌ای ایران، نه‌تنها نقض مجدد حاکمیت ایران بود، بلکه نشان داد که در منازعات آینده، مرز میان «درگیری منطقه‌ای» و «مداخله جهانی» به شدت باریک شده است. با این حال، این پژوهش صرفاً به توصیف بحران اکتفا نمی‌کند و بر اساس یافته‌های خود، سه پیشنهاد ارائه می‌دهد:

1) نخست، تدوین یک «پروتکل الحاقی دیجیتال» به کنوانسیون‌های ژنو. همان‌طور که پروتکل‌های الحاقی ۱۹۷۷ قواعد حقوق بشردوستانه را برای جنگ‌های چریکی مدرن‌سازی کردند، امروز نیز نیاز به یک سند حقوقی جدید وجود دارد که به صراحت وضعیت زیرساخت‌های حیاتی غیرنظامی (مانند شبکه‌های برق، آب، بهداشت و داده‌های غیرنظامی) را در زمان مخاصمات سایبری و ترکیبی مشخص کرده و برای آن‌ها حمایت ویژه‌ای در نظر بگیرد.

2) دوم، ایجاد یک «سازمان بین‌المللی برای انتساب فنی حملات سایبری[1]». این نهاد فنی - حقوقی مستقل، مشابه آژانس بین‌المللی انرژی اتمی، می‌تواند با ارائه تحلیل‌های فنی بی‌طرفانه در مورد منشأ و ماهیت حملات سایبری بزرگ، به حل معضل «انتساب» کمک کرده و از تصمیم‌گیری‌های شتاب‌زده مبتنی بر اطلاعات ناقص که می‌تواند به تشدید تنش منجر شود، جلوگیری کند.
3) سوم، ترویج «اقدامات اعتماد ساز سایبری[2]» در سطح منطقه‌ای. ایجاد خطوط ارتباطی امن[3] میان مراکز ملی امنیت سایبری کشورها و برگزاری رزمایش‌های مشترک برای مقابله با تهدیدات بازیگران غیردولتی، می‌تواند به کاهش سوءتفاهم‌ها و جلوگیری از محاسبات اشتباه در زمان بحران کمک کند.

## منابع

رستمی، سینا (۱۴۰۱). اصل عدم‌مداخله و آستانه حاکمیت در فضای سایبری. *مجله مطالعات حقوقی*، ۱۴(۲)، ۱۵۵-۱۷۸.
زمانی، سید قاسم (۱۴۰۱). *حقوق بین‌الملل و امنیت سایبری*. تهران: موسسه مطالعات و پژوهش‌های حقوقی شهر دانش.
زمانیان، مهدی (۱۴۰۱). *مطالعات راهبردی حقوقی: کاربرد حقوق بین‌الملل به‌مثابه ابزار سیاست خارجی*. تهران: نشر میزان.
سلیمی، حسین (۱۳۹۸). *ابعاد نظری و عملی دکترین امنیت ملی جمهوری اسلامی ایران*. تهران: انتشارات دانشگاه علامه طباطبائی.
شریفی، محسن (۱۴۰۲). نقدی بر رویکرد قانون‌گذار ایران در قبال بزه‌کاری سبز. *مجله مطالعات حقوقی*، ۱۵(۱)، ۶۴-۹۲.

---

1. OATAC
2 CBMs
3 hotlines

ظفری، محمد و همکاران (۱۴۰۲). مبانی حقوقی دفاع مشروع پیشدستانه در حقوق بین‌الملل. *فصلنامه روابط خارجی*، ۱۵(۳)، ۱۹۹-۲۲۰.

غریب آبادی، کاظم (۱۴۰۰). *دیپلماسی هسته‌ای و دکترین بازدارندگی ایران*. تهران: انتشارات سروش.

فضائلی، مصطفی (۱۴۰۳). حاکمیت سایبری در پرتو حقوق بین‌الملل. *فصلنامه مطالعات راهبردی*، ۲۶(۱)، ۷-۳۰.

کاسسه، آنتونیو (۱۳۹۸). *حقوق بین‌الملل*. ترجمه مرتضی کلانتریان، تهران: شهر دانش.

کمیته بین‌المللی صلیب سرخ (ICRC) (۲۰۰۵). *حقوق بین‌الملل بشردوستانه عرفی، جلد اول: قواعد*. ترجمه دفتر امور بین‌الملل قوه قضائیه، تهران: نشر مجد.

انجمن ایرانی مطالعات سازمان ملل متحد (۱۴۰۴). *تحلیل حقوقی حمله اسرائیل به ایران: پاسخ به چند پرسش*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://unstudies.ir/iauns-forum/تحلیل-حقوقی-حمله-اسرائیل-به-ایران:-پاسخ-به-چند-پرسش/

جمشیدی، محسن (۱۴۰۲). مسئولیت بین‌المللی دولت در قبال حملات سایبری بازیگران غیردولتی. *مجله مطالعات حقوقی*، ۱۵(۳)، ۹۳-۱۱۸.

خبرگزاری تسنیم (۱۴۰۴). *بررسی ابعاد فقهی-حقوقی جنگ ۱۲ روزه رژیم صهیونیستی علیه ایران*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://www.tasnimnews.com/fa/news/1404/05/09/3366369/

خبرگزاری فارس (۱۴۰۴). *افشای شبکه عملیات سایبری اسرائیل در ایران + سند*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://farsnews.ir/aa_mir78/1759645499439499512/

دیپلماسی ایرانی (۱۴۰۴). *ارزیابی تأثیرات جنگ ۱۲ روزه بر دکترین نظامی ایران و اسرائیل*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: http://www.irdiplomacy.ir/fa/news/2035015/

مرکز پژوهش‌های مجلس شورای اسلامی (۱۴۰۴). *ابعاد حقوقی حمله تجاوزکارانه رژیم صهیونیستی به جمهوری اسلامی ایران*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://rc.majlis.ir/fa/news/show/1843363

مشرق نیوز (۱۴۰۴). *از دکترین شلیک اول تا نقض حقوق بشر در جنگ ۱۲ روزه*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://www.mashreghnews.ir/news/1737257/

موسسه بین‌المللی مطالعات استراتژیک (IISS) (۱۴۰۴). *تحلیل تأثیرات راهبردی جنگ ایران و اسرائیل*. (تاریخ

مشاهده ۱۶ مهر ۱۴۰۴) در: https://iranthinktanks.com/analyzing-the-strategic-impacts-of-the-israel-iran-war

موسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران (۱۴۰۴). *ابعاد پیدا و پنهان ناکارآمدی حقوق بین‌الملل در جنگ ۱۲ روزه*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: http://iict.ac.ir/1404/04/

نظام مسائل (۱۴۰۴). *تحلیل راهبردی جنگ ۱۲ روزه: حال و آینده*. (تاریخ مشاهده ۱۶ مهر ۱۴۰۴) در: https://nezammasael.com/?p=2147

## References

ABC7NY (2025). Iranian hackers may conduct malicious cyber activity, US agencies warn. (Viewed on October 8, 2025) at: https://abc7ny.com/post/iran-news-today-iranian-hackers-may-conduct-malicious-cyber-activity-us-agencies-warn/16888067/

Andress, J., & Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier.

Ansar Security Consultants (2025). *From the First Shot Doctrine to Human Rights Violations in the 12-Day War*. (Viewed on October 8, 2025) at: https://www.mashreghnews.ir/news/1737257/ [In Persian]

Atlantic Council (2025). *What the Israel-Iran conflict revealed about wartime cyber operations*. (Viewed on October 8, 2025) at: https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/

Bílková, V. (2020). State Responsibility for Cyber Operations by Non-State Actors. *Czech Yearbook of Public and Private International Law*, 11, 127-145.

Binding Hook (2025). How Israel and Iran Brought Cyber Conflict to Centre Stage. (Viewed on October 8, 2025) at: https://bindinghook.com/how-israel-and-iran-brought-cyber-conflict-to-centre-stage/

Brownlie, I. (2008). *Principles of Public International Law*. Oxford: Oxford University Press.

Cassese, A. (2019). International Law. Translated by Morteza Kalantarian, Tehran: Shahr Danesh. [In Persian]

Cybersecurity and Infrastructure Security Agency (CISA) (2023). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. (Viewed on October 8, 2025) at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Dinstein, Y. (2011). *War, Aggression and Self-Defence*. Cambridge: Cambridge University Press.

EU Council (2025). Statement by the High Representative on behalf of the European Union on the malicious cyber activity in the Middle East. Brussels.

Fars News Agency (2025). Disclosure of Israel's Cyber Operations Network in Iran + Document. (Viewed on October 8, 2025) at: https://farsnews.ir/aa_mir78/1759645499439499512/ [In Persian]

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival,* 53(1), 23–40.

Fazaeli, M. (2024). Cyber Sovereignty in Light of International Law. *Strategic Studies Quarterly*, 26(1), 7-30. [In Persian]

Franck, T. M. (2002). *Recourse to Force: State Action Against Threats and Armed Attacks*. Cambridge: Cambridge University Press.

Gerke, M. (2019). Ahead of the Curve: Due Diligence in International Cybersecurity Law. *Global Affairs*, 5(4-5), 419-431.

Gharibabadi, K. (2021). *Nuclear Diplomacy and Iran's Deterrence Doctrine*. Tehran: Soroush Publications. [In Persian]

Giles, K. (2016). *Handbook of Russian Information Warfare*. NATO Defense College.

Glennon, M. J. (2003). The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter. *Harvard Journal of Law & Public Policy*, 25(2), 539-558.

Gray, C. (2018). *International Law and the Use of Force*. Oxford: Oxford University Press.

Hathaway, O. A., et al. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817–886.

Hoffman, F. G. (2007*). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington*, VA: Potomac Institute for Policy Studies.

Institute for Defence Studies and Analyses (IDSA) (2025). *The 12-Day War: Cyber Frontlines Between Israel and Iran*. (Viewed on October 8, 2025) at: https://www.idsa.in/publisher/comments/the-12-day-war-cyber-frontlines-between-israel-and-iran

International Committee of the Red Cross (ICRC) (2005). *Customary International Humanitarian Law*, Volume I: Rules. Cambridge: Cambridge University Press.

International Court of Justice (ICJ) (1949). Corfu Channel Case (United Kingdom v. Albania), Merits, Judgment. ICJ Reports 1949.

International Court of Justice (ICJ) (1986). *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment. ICJ Reports 1986.

International Institute for Iranian Studies (Rasanah) (2025). Analyzing the Strategic Impacts of the Israel-Iran War. (Viewed on October 8, 2025) at:

https://iranthinktanks.com/analyzing-the-strategic-impacts-of-the-israel-iran-war

International Law Commission (ILC) (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts.

Iranian Association for UN Studies (IAUNS) (2025). Legal Analysis of the Israeli Attack on Iran: Answering a Few Questions. (Viewed on October 8, 2025) at: https://unstudies.ir/iauns-forum/تحلیل-حقوقی-حمله-اسرائیل-به-ایران:-پاسخ-به-چند-پرسش/ [In Persian]

Iranian Diplomacy (2025). Assessing the Impacts of the 12-Day War on the Military Doctrines of Iran and Israel. (Viewed on October 8, 2025) at: http://www.irdiplomacy.ir/fa/news/2035015/ [In Persian]

Islamic Parliament Research Center (IPRC) (2025). Legal Dimensions of the Aggressive Attack by the Zionist Regime on the Islamic Republic of Iran. (Viewed on October 8, 2025) at: https://rc.majlis.ir/fa/news/show/1843363 [In Persian]

Jamshidi, M. (2023). International Responsibility of the State for Cyber Attacks by Non-State Actors. *Journal of Legal Studies*, 15(3), 93-118. [In Persian]

Jennings, R., & Watts, A. (Eds.). (1992). Oppenheim's International Law (9th ed., Vol. 1). London: Longman.

Jensen, E. T. (2018). The Tallinn Manual 2.0: Highlights and Insights. Georgetown *Journal of International Law*, 49(3), 775-799.

Jerusalem Post (JPost) (2025). *How IDF, Mossad neutralized Iran's air defenses in 12-day war*. (Viewed on October 8, 2025) at: https://www.jpost.com/middle-east/article-863827

Lieber Institute at West Point (2025). *Non-State Cyber Actors, the 12-Day War, and the Gray Zone of LOAC, Part I*. (Viewed on October 8, 2025) at: https://lieber.westpoint.edu/non-state-cyber-actors-12-day-war-gray-zone-loac-part-i/

Lin, H. (2012). *Cyber Conflict and National Security*. New York: The National Academies Press.

Nextgov (2025). *New research shows Iran's expansive cyber offensive during 12-Day War with Israel*. (Viewed on October 8, 2025) at: https://www.nextgov.com/cybersecurity/2025/08/new-research-shows-irans-expansive-cyber-offensive-during-12-day-war-israel/407207/

Nezam Masael (2025). A Strategic Analysis of the 12-Day War: Present and Future. (Viewed on October 8, 2025) at: https://nezammasael.com/?p=2147 [In Persian]

Politico (2025). *U.S. gave tacit support to Israeli strikes that triggered war with Iran*. (Viewed on October 8, 2025) at:

https://www.politico.com/news/2025/06/22/us-israel-iran-war-cyber-attacks-00417782

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Rostami, S. (2022). The Principle of Non-Intervention and the Threshold of Sovereignty in Cyberspace. *Journal of Legal Studies*, 14(2), 155-178. [In Persian]

Salimi, H. (2019). *Theoretical and Practical Dimensions of the National Security Doctrine of the Islamic Republic of Iran*. Tehran: Allameh Tabataba'i University Press. [In Persian]

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge*: Cambridge University Press.

Security Scorecard (2025). *From the Depths of the Shadows: IRGC and Hacker Collectives of the 12-Day War*. (Viewed on October 8, 2025) at: https://securityscorecard.com/blog/from-the-depths-of-the-shadows-irgc-and-hacker-collectives-of-the-12-day-war/ Access-Date) at: [Link to WSJ article, e.g., https://www.wsj.com/...]

Sharifi, M. (2023). A Critique on the Approach of the Iranian Legislator towards Green Criminality. *Journal of Legal Studies*, 15(1), 64-92. [In Persian]

Sofaer, A. D. (2003). On the Necessity of Pre-emption. European *Journal of International Law*, 14(2), 209-226.

Tabrizi, B. (2018). Iran's Cyber Power: A Study of its Strategic Dimensions. *Middle East Policy*, 25(1), 89-103.

Tasnim News Agency (2025). *A Review of the Fiqhi-Legal Dimensions of the 12-Day War of the Zionist Regime against Iran*. (Viewed on October 8, 2025) at: https://www.tasnimnews.com/fa/news/1404/05/09/3366369/ [In Persian]

Tehran International Studies & Research Institute (2025). *The Visible and Hidden Dimensions of the Inefficiency of International Law in the 12-Day War*. (Viewed on October 8, 2025) at: http://iict.ac.ir/1404/04/ [In Persian]

The Record (2025). Widespread internet outages reported in Iran amid conflict with Israel. (Viewed on October 8, 2025) at: https://therecord.media/iran-internet-outages-israel-conflict

Tikk, E., & Kaska, K. (2017). *Due Diligence in Cyberspace*. Tallinn: NATO CCDCOE Publications.

United Nations (1945). *Charter of the United Nations*. 1 UNTS XVI.

United States Marine Corps University (USMCU) (2025). *Forecasting Iranian Government Responses to Cyberattacks*. (Viewed on October 8, 2025) at: https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-13-no-1/Forecasting-Iranian-Government-Responses-to-Cyberattacks/

Wall Street Journal (2025). *Israel is running low on Arrow interceptor missiles, U.S. official says*. (Viewed on October 8, 2025) at: [Note: Full URL needed if available, e.g., https://www.wsj.com/...]

Waxman, M. C. (2011). Cyber-Attacks and the Use of Force: A Primer. *Yale Journal of International Law*, 36(2), 421-450.

Zafari, M. et al. (2023). The Legal Basis of Preemptive Self-Defense in International Law. *Foreign Relations Quarterly*, 15(3), 199-220. [In Persian]

Zamani, S. Q. (2022). *International Law and Cyber Security*. Tehran: Shahr Danesh Institute for Legal Studies and Research. [In Persian]

Zamanian, M. (2022). *Strategic Legal Studies: The Application of International Law as a Foreign Policy Tool*. Tehran: Mizan Publishing. [In Persian]

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishing Group.