Foreign Relations Center for Strategic Research
https://frqjournal.csr.ir E-ISSN: 2588-6541
Vol. 17, No. 2, Issue. 66, Summer 2025 Received: 2025/01/28 Accepted: 2025/07/09
Research paper

The Cyber Dimension of Hybrid Warfare and the Conceptual Transformation of International Armed Conflict Law: A Case Study of the Defensive Doctrine of the Islamic Republic of Iran

Abdolhossein Safaee
Corresponding Author, Assistant Professor, Department of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran.
Email: safaee.1385@gmail.com
Farshad Bakhshi Jolfan
PhD Candidate in International Law, Faculty of Security, National Defense University, Tehran, Iran.
Email: bakhshi1357@yahoo.com

Abstract

Introduction: The increasing complexity of modern armed conflicts, driven by advancements in technology and the emergence of hybrid warfare, has profoundly reshaped the normative framework of international humanitarian law. Hybrid warfare a form of conflict that blends conventional military operations with cyber warfare, disinformation, proxy tactics, and economic measures poses unique legal and strategic challenges, particularly in regions marked by protracted geopolitical tension. This article focuses on the Islamic Republic of Iran as a case study, analyzing the country's evolving defensive doctrine in response to the multidimensional threats posed by the United States and its allies. It explores how Iran has restructured its military and legal strategy to address the blurred lines of conflict in hybrid settings, particularly within the cyber domain. Moreover, as warfare increasingly migrates into the digital realm, traditional conceptualizations of battlefield and belligerency are no longer sufficient. The proliferation of non-kinetic operations ranging from coordinated cyber espionage to AI-enabled surveillance and disruption requires an expanded legal lexicon and new operational doctrines. Iran's strategic environment, situated at the crossroads of international cyber conflict, has become a testing ground for such emerging paradigms.

Research Question:What transformations has the defensive doctrine of the Islamic Republic of Iran undergone in response to the hybrid warfare conducted by the United States and its allies, and how do these transformations influence the adaptation of international armed conflict law to the cyber domain?

Research Hypothesis:The central hypothesis of this study is that the Islamic Republic of Iran’s defensive doctrine has undergone a systematic transformation

in response to multidimensional threats, especially in cyberspace. This transformation reflects a strategic shift toward active deterrence, intelligentized cyber defense, and legal countermeasures. It rests on a comprehensive interpretation of deterrent defense aligned with Iran's geopolitical context and legal traditions. As traditional legal instruments often fail to address the sub-threshold nature of hybrid threats, Iran's evolving doctrine reveals the need for conceptual expansion of legal norms to address cyber warfare and asymmetric tactics.

Methodology (and Theoretical Framework if there are):This study employs a descriptive-analytical approach, using both doctrinal and empirical methods. It analyzes primary and secondary legal sources, including international treaties, resolutions, reports from international organizations, national policy documents, and relevant legal doctrines. The research also incorporates a theoretical framework based on jus ad bellum, jus in bello, and the law of state responsibility. It evaluates Iran's defense policy in light of normative legal developments, focusing on how Iran's responses align or diverge from the principles of necessity, proportionality, distinction, and attribution. Emphasis is placed on interpreting Iran's doctrinal evolution within both regional strategic dynamics and the broader context of international legal discourse on cyber conflict.

Results and Discussion:Iran's response to hybrid threats has unfolded along several strategic and normative lines. First, it has institutionalized the concept of intelligentized defense, combining cyber surveillance, artificial intelligence, and automated threat response systems. These innovations allow Iran to identify and neutralize threats proactively, enhancing both tactical readiness and legal justifiability. Second, Iran has embraced strategic deterrence and escalation control through asymmetric tactics such as cyber counterattacks, regional proxy engagement, and targeted disinformation campaigns while framing these actions as lawful under Article 51 of the UN Charter. Third, the doctrinal emphasis on legalism has led Iran to justify its countermeasures by invoking customary international law, including the ILC's Articles on State Responsibility, which support proportionate non-forcible responses to internationally wrongful acts. These countermeasures are carefully framed to fall below the threshold of armed conflict while still sending strong strategic signals to adversaries.
The study further finds that Iran's cyber strategy has evolved to include multi-layered public-private partnerships aimed at building domestic cyber capacity. These partnerships not only enhance operational resilience but also reflect a broader effort to localize cyber technologies and reduce dependence on foreign infrastructures. Additionally, Iran has introduced legal reforms to integrate cyber threats into national security law, recognizing them as potential threats to territorial integrity and sovereign functionality. This institutional embedding of hybrid and cyber dimensions into national law exemplifies a deeper harmonization between strategic doctrine and legal adaptation.

Furthermore, Iran's strategic posture has been deeply shaped by its leadership's political ideology, emphasizing resistance, sovereignty, and independence. The Supreme Leader's discourse reinforces a defense culture grounded in asymmetry and legitimacy, viewing hybrid threats as part of a larger struggle over legal norms and narrative dominance. Within this framework, law becomes both a tool of resistance and a shield against external intervention. Iran's legal counter-

strategy thus reflects both a rejection of Western dominance over the international legal order and an effort to influence that order from within by proposing normative alternatives.
This study also finds that the gaps in existing international humanitarian law frameworks, particularly regarding cyber operations, attribution standards, and thresholds of armed attack, create legal ambiguities that Iran navigates through interpretive innovation. Iran argues that the fragmented nature of hybrid threats necessitates a revised understanding of jus ad bellum, including recognition of hostile cyber acts and disinformation campaigns as forms of aggression. Moreover, it emphasizes that the principle of proportionality must be contextually applied in cyber domains, taking into account the cumulative and often indirect effects of such operations.
Conclusion:Iran's evolving defensive doctrine exemplifies how a state subjected to continuous hybrid aggression can reshape both its strategic behavior and legal interpretations. Its emphasis on legal countermeasures, intelligentized defense, and norm-building in cyberspace illustrates a multifaceted approach to modern conflict that is both defensive and anticipatory. The Iranian case reveals the pressing need for the international community to update the legal architecture governing warfare to include cyber-specific rules, improve attribution standards, and legitimize proportional defensive responses to hybrid threats. As hybrid warfare becomes the defining feature of 21st-century conflict, Iran's experience offers a compelling model for how national defense doctrines and international law can co-evolve in response to unprecedented strategic realities. Finally, the findings suggest that Iran's experience can inform the global conversation on legal innovation in warfare. By foregrounding the principles of legal proportionality, strategic necessity, and cyber sovereignty, Iran contributes to an evolving body of practice that may influence future treaty-making processes. This development underscores the role of regional powers in shaping international norms, particularly in domains where legal consensus remains fragmented or underdeveloped.

Keywords: Hybrid warfare, Cyber Warfare, Defensive Doctrine, Deterrent Defense, Countermeasures, Sovereignty, Intelligentized Defense, International Humanitarian Law, Strategic Adaptation, Iran

E-ISSN: 2588-6541 / Center for Strategic Research / Quarterly of Foreign Relations

10.22034/fr.2025.502931.1632

سال هفدهم، شماره دوم (پیاپی ۶۶)، تابستان ۱۴۰۴، صص. ۱۵۹-۱۹۰
تاریخ دریافت: ۱۴۰۳/۱۱/۰۹ ـ تاریخ پذیرش: ۱۴۰۴/۰۴/۱۸

مقاله پژوهشی

بُعد سایبری جنگ ترکیبی و تحول مفهومی حقوق مخاصمات مسلحانه بین‌المللی: مطالعه موردی دکترین دفاعی جمهوری اسلامی ایران

عبدالحسین صفایی
نویسنده مسئول، استادیار گروه حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
Email: safaee.1385@gmail.com

فرشاد بخشی جلفان
دانشجوی دکتری حقوق بین‌الملل، دانشکده امنیت، دانشگاه عالی دفاع ملی، تهران، ایران.
Email: bakhshi1357@yahoo.com

چکیده

جنگ ترکیبی در عصر جدید به‌عنوان شکلی پیچیده و چندبُعدی از مخاصمات، تحولات عمیقی در ماهیت سنتی جنگ و چهارچوب‌های حقوقی حاکم بر آن به‌وجود آورده است. این پدیده به دلیل گستردگی و پیچیدگی آن و استفاده هم‌زمان نیروهای نامنظم، نیروهای ویژه، حمایت از ناآرامی‌های داخلی، جنگ اطلاعاتی و تبلیغاتی، دیپلماسی، حملات سایبری، جنگ اقتصادی و نیروهای نظامی منظم در میدان جنگ به تحولات حقوق مخاصمات افزوده است. از طرفی توسعه فناوری‌های نوین، به‌ویژه در بُعد سایبری جنگ ترکیبی، علاوه بر ایجاد تغییرات بنیادین در رویکردهای نظامی، چالش‌های حقوقی بی‌سابقه‌ای را در سطح بین‌المللی ایجاد نموده است. جنگ سایبری با توجه به مطرح و گسترده‌تر شده بحث هوش مصنوعی موجب تقویت توانمندی‌های ملی و جنگ‌های آینده در نظام بین‌الملل شده است. جمهوری اسلامی ایران با توجه به تعارضات راهبردی که در منطقه غرب آسیا با آمریکا و اعضای ناتو دارد همواره در قالب جنگ ترکیبی از سوی آمریکا و متحدین آن مورد هجمه واقع شده است. در این چهارچوب دکترین دفاعی ایران با اتخاذ رویکردی پیشگیرانه و بازدارندگی فعال بر هوشمندسازی سامانه‌های دفاعی، تقویت زیرساخت‌های امنیت سایبری و انعطاف‌پذیری راهبردی تأکید داشته است. سؤال پژوهش حاضر این است که در چهارچوب جنگ ترکیبی آمریکا و متحدین آن بر علیه ایران دکترین دفاعی جمهوری اسلامی ایران چه تغییراتی داشته است؟ در پاسخ به سؤال فوق، نگارندگان فرضیه ذیل را مطرح می‌کنند: دکترین دفاعی جمهوری اسلامی ایران با توجه به تنوع تهدیدات پیش‌رو در حال تحول است و بر اساس لحاظ شدن اصل تنوع در دفاع همه‌جانبه تنظیم شده است. روش پژوهش مقاله حاضر توصیفی- تبیینی و روش گردآوری منابع اسنادی است.

کلیدواژه‌ها: جنگ ترکیبی، نبرد سایبری، دکترین دفاعی، تهدیدات نامتقارن، امنیت چندلایه، محیط راهبردی

شاپای الکترونیک: ۶۵۴۱-۲۵۸۸/ پژوهشکده تحقیقات راهبردی/ فصلنامه روابط خارجی

doi 10.22034/fr.2025.502931.1632

مقدمه و بیان مسئله

در دهه‌های اخیر، پیشرفت‌های شگرف در فناوری‌های نوین به‌ویژه در عرصه‌های نظامی و امنیتی، چهارچوب‌های حقوقی حاکم بر مخاصمات مسلحانه را با چالش‌های جدی مواجه کرده است. این تحولات عمدتاً شامل ظهور سلاح‌های خودکار، هوش مصنوعی، جنگ سایبری و سلاح‌های دقیق هدایت‌شونده هستند که شیوه‌های جنگی و قواعد حاکم بر رفتار دولت‌ها در مخاصمات مسلحانه را به‌طور اساسی تغییر داده‌اند. جنگ‌های ترکیبی که ترکیبی از ابزارها و روش‌های متعارف و غیرمتعارف را به‌کار می‌گیرند، مرزهای مفهومی و عملیاتی حقوق مخاصمات مسلحانه را دچار تحول کرده و تهدیدات جدید و پیچیده‌ای به‌ویژه در زمینه فضای سایبری به‌وجود آورده است. فضای سایبری به‌عنوان یکی از ابعاد اصلی جنگ‌های ترکیبی، تهدیداتی بی‌سابقه و با قابلیت‌های تخریبی بسیار بالا ایجاد کرده است که در بسیاری از موارد از مخاصمات متعارف و معمول فراتر می‌رود. حملات سایبری می‌توانند زیرساخت‌ها و اماکن حیاتی غیرنظامی را هدف قرار داده و خسارات سنگینی را مشابه با حملات نظامی کلاسیک وارد کنند. این امر چالش‌هایی در زمینه تعریف و شناسایی حملات مسلحانه و تعیین مسئولیت‌های بین‌المللی ایجاد کرده است که باید به‌طور مؤثر و مطابق با قواعد حقوق بشردوستانه پاسخ داده شود. در این زمینه، حقوق مخاصمات مسلحانه که به‌دنبال تنظیم رفتار دولت‌ها در زمان جنگ بر اساس اصولی چون تفکیک، تناسب، احتیاط و ضرورت است، اکنون باید با واقعیت‌های جدید ناشی از جنگ‌های ترکیبی و تهدیدات سایبری انطباق یابد. ویژگی‌های منحصر به‌فرد فضای سایبری، مانند غیرمتمرکز بودن، سرعت بالای انتقال اطلاعات و گستره اثرگذاری، ایجاب می‌کند که قواعد موجود بازنگری شده و شیوه‌های جدیدی برای مواجهه با این تهدیدات تدوین گردد.

یکی از چالش‌های کلیدی در حقوق بین‌الملل، این است که چگونه می‌توان قواعد حقوقی موجود را با واقعیت‌های نوین جنگ‌های ترکیبی که سایبر به‌عنوان بُعدی اساسی از آن‌ها است، تطبیق داد. در این راستا، موضوعاتی مانند تعیین «آستانه حمله» و قواعد پاسخ‌گویی به حملات سایبری، مسائلی هستند که نیازمند بازتعریف و تطبیق در متن حقوق مخاصمات مسلحانه بین‌المللی می‌باشند. این مقاله با هدف تحلیل تحولات مفهومی حقوق مخاصمات مسلحانه در پیِ ظهور جنگ‌های ترکیبی و بُعد سایبری آن، به بررسی چالش‌ها و فرصت‌های حقوقی پاسخ‌گویی به این تهدیدات نوظهور می‌پردازد. پژوهش حاضر با روش توصیفی-تحلیلی، قواعد حاکم بر حقوق بین‌الملل و اسناد مرتبط با امنیت سایبری را مورد تحلیل قرار داده و تلاش دارد تا

چهارچوبی حقوقی برای پاسخ به پرسش‌های کلیدی در این زمینه ارائه دهد. این مطالعه می‌تواند به فهم بهتر تعامل میان حقوق مخاصمات مسلحانه، جنگ‌های ترکیبی و چالش‌های حقوقی آن کمک کند و پیشنهادهایی برای گسترش و تطبیق قواعد حقوق بشردوستانه بین‌المللی در عصر جدید فراهم آورد.

۱. پیشینه پژوهش

در بررسی اجمالی منابع پژوهشی نزدیک به نوشتار حاضر، چندین عنوان مورد اشاره قرار خواهند گرفت از جمله: «مایکل اشمیت»[1](۲۰۱۲) در مقاله‌ای تحت عنوان: «حمله به‌عنوان یک اصطلاح فنی در حقوق بین‌الملل: در زمینه عملیات سایبری»، به دنبال این مسئله است که آیا یک عملیات سایبری در وهله اول به‌عنوان یک حمله شناخته می‌شود یا خیر و به لحاظ حقوقی چگونه قابل ارزیابی است؟ این مقاله اصطلاح «حمله مسلحانه» را در دو حوزه حقوق جنگ بررسی نموده است؛ نخست، در حقوق توسل به زور به‌عنوان شرط لازم برای توسل به دفاع مشروع طبق ماده ۵۱ منشور سازمان ملل و حقوق بین‌الملل عرفی عمل می‌کند؛ دوم، در حقوق در جنگ به نوعی عملیات نظامی اشاره دارد که مشمول محدودیت‌ها و قواعد خاص حقوق بشردوستانه است. در نهایت مقاله به تمایز و تحلیل این کاربردها پرداخته و نتیجه می‌گیرد که یک عملیات سایبری که پیامدهای جدی مانند اثرات اقتصادی شدید یا اختلال قابل‌توجه در کارکردهای اجتماعی ایجاد می‌کند می‌تواند به‌عنوان حمله مسلحانه تلقی شود، حتی اگر منجر به مرگ، جراحت، آسیب یا تخریب نشود.

محمدرضا مرادی (۱۴۰۱) در مقاله‌ای تحت عنوان: «اصول و قواعد دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی» با این سؤال که اصول و قواعد دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی چیست؟ در نظر دارد مبتنی بر مبانی نظری تدوین دکترین سایبری اصول و قواعد دکترین سایبری جمهوری اسلامی ایران را در حوزه دفاعی امنیتی مدون نماید که در نهایت اصول دکترینی سایبری جمهوری اسلامی ایران در قالب سه اصل استقلال، اقتدار و تواصی را تدوین نموده است.

«برنلی رابوین»[2] (۲۰۱۱) نیز در مقاله خود تحت عنوان: «تحول هم‌زمان حقوق بین‌الملل و ظهور جنگ سایبری» در پاسخ به این سؤال که آیا ظهور جنگ سایبری

1. Michael N. Schmitt
2. Bradley Raboin

موجب تحول هم‌زمان در حقوق بین‌الملل گردیده؟ به بررسی نحوه برخورد قواعد حقوق بین‌المللی با جنگ سایبری و میزان اثربخشی این قواعد پرداخته و در نهایت نتیجه‌گیری می‌شود نیاز به تدوین قواعد حقوقی بین‌المللی جدید و معرفی یک رژیم حقوقی جهانی جدید الزامی است تا بتوان به‌طور مؤثر با مسائل جنگ سایبری مقابله گردد.

«کای آمبوس»[1](۲۰۲۱) در مقاله خود با عنوان: «مسئولیت کیفری بین‌المللی در فضای سایبری» با این سؤال که مسئولیت کیفری بین‌المللی فردی در جنگ سایبری چگونه قابل بررسی است؟ حملات سایبری را بر اساس اساسنامه دیوان بین‌المللی کیفری در سه حوزه جنایات جنگی، جنایت تجاوز و جنایت علیه بشریت بررسی می‌کند و در نهایت نتیجه می‌گیرد که مسئولیت کیفری فردی برای حملات سایبری ممکن است بیشتر در ارتباط با جنایات جنگی باشد تا جرم تجاوز. جنگیدن با «جنگ سایبری» تحت نقض «حقوق در جنگ»[2] به ندرت منجر به مسئولیت کیفری برای جنایت تجاوز طبق ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری خواهد شد، چرا که دشوار است تصور شود که یک حمله سایبری به اندازه کافی به یک عمل تجاوز طبق معنای ماده ۸ (۲) اساسنامه دیوان بین‌المللی کیفری برسد، چه برسد به اینکه یک نقض آشکار طبق معنای ماده ۸ (۱) مکرر اساسنامه دیوان بین‌المللی کیفری باشد.

«سورین دومی‌تر»[3] (۲۰۱۶) در مقاله خود تحت عنوان: «بُعد سایبری جنگ ترکیبی مدرن و ارتباط آن با ناتو» در پاسخ به این سؤال که بُعد سایبری جنگ ترکیبی با نگاه به ناتو چگونه قابل بررسی است ضمن تعیین عناصر جنگ ترکیبی و بررسی ابعاد سایبری جنگ ترکیبی، استفاده از فضای سایبر را به‌عنوان ابزاری برای جنگ سایبری می‌داند و در نهایت نتیجه می‌گیرد که حملات سایبری می‌توانند زنجیره تأمین، پشتیبانی استراتژیک ناتو را تحت تأثیر قرار دهند و ممکن است سعی در تضعیف توانایی ناتو در انجام عملیات و تحقق وظایف اصلی آن داشته باشند. بنابراین متحدان باید وارد یک فرایند انطباق با دفاع سایبری شوند که با سرعت فضای سایبری همخوانی داشته باشد.

هفت لنگ و همکاران (۱۴۰۲) در مقاله بررسی تحول دکترین امنیتی آمریکا در غرب آسیا و الزامات راهبردی جمهوری اسلامی ایران ۲۰۰۹-۲۰۲۲ (مطالعه موردی

1. Kai Ambos
2. Ius ad bellum
3. Sorin Dumitru

افغانستان) به بررسی دکترین آمریکا در منطقه غرب آسیا از زاویه مقابله با چالشگران منطقه‌ای پرداخته‌اند.

شهراینی و همکاران (۱۴۰۱) در مقاله تبیین عوامل مؤثر بر تدوین دکترین پدافند غیر عامل جمهوری اسلامی ایران با رویکرد نظامی به نتایج ذیل دست یافته‌اند. نتایج پژوهش منتج به تبیین عوامل مؤثر بر دکترین پدافند غیر عامل با رویکرد نظامی گردید که این عوامل در سه حوزه «جهت‌دهندگان دکترین»، «ساختاردهندگان دکترین» و «شتاب‌دهندگان محیطی دکترین» دسته‌بندی گردیدند. نتایج نشان داد که به‌منظور تدوین دکترین پدافند غیرعامل با رویکرد نظامی باید به سه حوزه کلی یاد شده توجه ویژه نمود.

باقری زاده (۱۴۰۲) در مقاله شهید سلیمانی و جهت‌گیری دکترین دفاعی-امنیتی جمهوری اسلامی ایران با تأکید بر کنشگری فعال و مدل «تصمیم‌گیری بینش فوق‌العاده به نتایج ذیل دست یافته است. دکترین دفاعی-امنیتی جمهوری اسلامی ایران متأثر از تفکر خردمندانه شهید سلیمانی در قالب الگوی ثابت رئالیسم ایرانی، از منظر دولت واقع‌گرایی دارای شیفت درون پارادایمی از رویکرد انعکاسی و واکنشگرایانه به رویکرد کنشگرایانه امنیتی فعال و صراحت راهبردی در مقابله به مثل متناسب با تهدیدات بوده است.

عزیززاده و همکاران (۱۴۰۲) در پژوهشی با عنوان دکترین نظامی جنگ آینده به یافته‌های ذیل دست یافته است. در تدوین دکترین جدید، می‌بایست از پیشرفت‌هایی که در فناوری اطلاعات، الکترونیک نظامی، قابلیت‌های نظارتی و هدایت دقیق اتفاق می‌افتد، به‌طور کامل بهره برد و این واقعیت نیز باید درک شود که سخت‌افزارهای نظامی امروزی مانند هواپیماها، کشتی‌ها و تانک‌ها به جایگاهی برای حمل مهمات هدایت شونده دقیق، حسگرها و موشک‌ها تنزل یافته‌اند؛ طبق نتایج این پژوهش، کلید آینده یکپارچگی است و دکترین نظامی باید طیف وسیعی از نیروهای مختلف را دربرگیرد و در یک مجموعه مؤثر به هم پیوند دهد تا بتواند به‌عنوان یک نیروی ضربتی توانا مورداستفاده قرار گیرد.

شمولی و همکاران (۱۴۰۲) در مقاله تبیین الگوی جنگ نامتقارن در دکترین امنیتی جمهوری اسلامی ایران در خلیج فارس به این نتیجه دست یافته‌اند که ایران به دلیل محدودیت‌ها و الزامات، این شیوه جنگ را انتخاب نموده و بهره‌گیری از آن باعث تولید بازدارندگی، خودکفایی، خوداتکایی، تغییر ساختار و نهایتاً تغییر در استراتژی دشمن شده است. در مقاله حاضر، نگارنده با توجه به تحولات حاضر در

جنگ ترکیبی جدید و رویکردهای بین‌المللی به آن به تبیین دکترین دفاعی جمهوری اسلامی ایران در محیط پرتخاصم جدید خواهد پرداخت.

۲. مفهوم پژوهی جنگ ترکیبی و تحول در اشکال جنگ

در عصر حاضر، جنگ‌ها به شکل پیچیده‌ای از ترکیب عملیاتی نظامی متعارف، نامتقارن، سایبری، روانی، اقتصادی و حقوقی ظهور یافته‌اند؛ پدیده‌ای که در ادبیات نوین به «جنگ ترکیبی» شناخته می‌شود. این شیوه نوین از جنگ، مرز میان ابزارهای نظامی و غیرنظامی را تضعیف کرده و به‌کارگیری هم‌زمان طیف وسیعی از ابزارهای قدرت را در دستور کار بازیگران دولتی و غیردولتی قرار داده است (Leonard, 2021). جنگ ترکیبی، به‌ویژه با بهره‌گیری از فناوری‌های نوین و نقش فزاینده گروه‌های غیردولتی، موجب تحول در فهم سنتی از «درگیری مسلحانه» و چالش در طبقه‌بندی آن در چهارچوب حقوق بین‌الملل بشردوستانه شده است.

واژه «جنگ ترکیبی» نخستین بار به‌طور رسمی توسط ژنرال جیمز ماتیس و فرانک هافمن در سال ۲۰۰۵ مطرح شد. آنان تأکید کردند که درگیری‌های آتی، ترکیبی از تهدیدات سنتی، غیرمتعارف، مخرب و فاجعه‌آمیز خواهند بود و این هم‌پوشانی مفهومی، مستلزم بازتعریف مفاهیم نظامی و حقوقی در مواجهه با تهدیدات نوین است (Mattis & Hoffman, 2005: 18–19). اهمیت این مفهوم پس از بحران اوکراین و الحاق کریمه توسط روسیه در سال ۲۰۱۴ افزایش یافت و در ادبیات نظامی و حقوقی به‌عنوان نمونه‌ای از جنگ‌های نوین مورد توجه قرار گرفت(Galeotti, 2016: 283). جنگ ترکیبی، از ابزارهایی چون تحریم اقتصادی، حملات سایبری، عملیات روانی، فریب اطلاعاتی و تحریک نیروهای نیابتی بهره می‌برد (Giegerich, 2016: 65). اگرچه این ابزارها در تاریخ نیز سابقه دارند، اما ویژگی بارز جنگ ترکیبی معاصر، هماهنگی هم‌زمان این ابزارها و هدف‌گذاری غیرمستقیم برای تحقق اهداف سیاسی و استراتژیک بدون ورود به جنگ متعارف است (Thiele, 2015: 10). این وضعیت موجب دشواری در اعمال قواعد حقوق بشردوستانه و شناسایی وضعیت حقوقی منازعات شده است (Cantwell, 2017; Reichborn-Kjennerud & Cullen, 2022).

ابهام در تمایز میان وضعیت جنگ و صلح، بازیگران دولتی و غیردولتی و میان مبارز و غیر مبارز، از جمله چالش‌هایی است که جنگ ترکیبی بر حقوق بین‌الملل تحمیل کرده است (Korhonen, 2015). این وضعیت «خاکستری» با بهره‌گیری از خلأهای حقوقی، اجرای اقدامات غیررسمی و کاهش شفافیت، هزینه‌ها و مسئولیت مهاجمان

را کاهش داده و آن را به استراتژی مطلوبی برای قدرت‌های نوظهور تبدیل کرده است (Nyemann & Sorensen, 2019). در پاسخ به این چالش‌ها، پیشنهادهایی برای تدوین قواعد نوین حقوقی در حال شکل‌گیری است. ماده ۳۶ پروتکل اول الحاقی ۱۹۷۷ به کنوانسیون‌های ژنو ۱۹۴۹[1] و «شرط مارتنس»[2] می‌توانند به‌عنوان زیرساخت حقوقی برای تطبیق قواعد جدید در مواجهه با جنگ‌های ترکیبی و سایبری مورد استناد قرار گیرند (Rekotov, 2022). به‌ویژه، لازم است که نظام دفاعی کشورها بر پایه درک عمیق‌تری از تهدیدات نوظهور، دکترین‌هایی طراحی کنند که نه‌تنها ابعاد سخت‌افزاری، بلکه ابعاد نرم‌افزاری، اطلاعاتی و سایبری نبرد را نیز دربرگیرد. استفاده هم‌زمان از قدرت نظامی، اقتصادی، سایبری و رسانه‌ای، ویژگی بارز دفاع در عصر جنگ‌های ترکیبی است(Treverton et al., 2018).

۳. رویکردهای مختلف نسبت به جنگ ترکیبی و نبردهای سایبری در روابط بین‌الملل

در ارتباط با شکل‌گیری نوع جدیدی از جنگ دیدگاه‌های مختلفی وجود دارد که در ابعاد مختلف حقوقی و سیاسی به بحث ورود کرده‌اند. وجود دیدگاه‌های مختلف بیانگر وجود رویکردهای حقوقی و سیاسی- نظامی متنوع نسب به پدیده نوظهوری است که واکنش‌های مختلف بازیگران دولتی را سبب شده است.

۳-۱. مجوز شورای امنیت

شورای امنیت این اختیار را دارد که به اعضای سازمان ملل اجازه دهد که هم در استفاده از زور و هم استفاده از اقدامات دیگر علیه کشور دیگری که در حال تهدید صلح، نقض صلح یا تجاوز است شرکت کنند.[3] با این حال، شورای امنیت تنها در

---

۱. این ماده به‌طور خاص از دولت‌ها می‌خواهد که قبل از استفاده از سلاح‌ها یا روش‌های جدید جنگی، تطابق آن‌ها با قواعد حقوق بشردوستانه را ارزیابی کنند تا اطمینان حاصل شود که این ابزارها و روش‌های نوین با اصول و قواعد حقوق بشردوستانه به‌ویژه اصول تمایز، تناسب و احتیاط سازگار هستند.

۲. این شرط برای نخستین بار و به پیشنهاد «فئودور فئودورویچ مارتنس» نماینده دولت روسیه، در مقدمه کنوانسیون ۱۸۹۹ لاهه در کنفرانس صلح لاهه گنجانده شد. که می‌گوید: حتی در مواردی که قواعد یا معاهدات مشخصی برای یک وضعیت خاص وجود ندارد، غیرنظامیان و مبارزان همچنان تحت حمایت اصول انسانی، عرف‌های حقوق بشردوستانه، و الزامات وجدان عمومی قرار دارند.

۳. منشور ملل متحد، مواد ۴۱، ۴۲

۴. منشور ملل متحد، ماده ۲۷

صورتی می‌تواند این کار را انجام دهد که در ماده ۳۹ تصمیم بگیرد که اقدامات یک دولت «تهدید صلح، نقض صلح یا اقدام تجاوزکارانه» است. تجربه گسترده نشان داده است که دستیابی به موارد ماده ۳۹ و توصیه‌های استفاده از زور به‌طور استثنایی دشوار است (Graham, 2010:29). اکثر چنین تصمیماتی تنها پس از بررسی‌های گسترده و وقت‌گیر حاصل می‌گردد و حتی در آن زمان نیز چنین تصمیماتی می‌تواند مشمول حق وتوی هر عضو دائم شورای امنیت گردد. بر این اساس، با توجه به ماهیت مبهم حملات سایبری و عدم اطمینان در مورد اینکه آیا شورای امنیت به چنین حملاتی به‌موقع پاسخ خواهد داد، به نظر می‌رسد این فرض درست باشد که یک کشور استفاده از حق دفاع مشروع برای مقابله با حملات سایبری که به حدی شدید باشد که تهدیدی معادل حمله مسلحانه به شمار آید را دارد.

۲-۳. حق دفاع مشروع فردی یا جمعی

حق یک دولت برای انجام اقدامات دفاعی، حقی نیست که توسط ماده ۵۱ منشور ملل متحد ایجاد شده باشد. همچنین منشور صرفاً بر این حق ذاتی حقوق بین‌الملل عرفی برای بقای دولت‌ها در جامعه بین‌المللی تأکید کرد (ماده ۳۸ اساسنامه دیوان بین‌المللی دادگستری). اجماع بین‌المللی محکمی وجود دارد که برای تجزیه‌وتحلیل حق دفاع از خود باید علاوه بر مفاد ماده ۵۱ به حقوق بین‌الملل عرفی نیز توجه شود، اگرچه چندین تئوری همیشه در مورد انواع اقدامات دولتی که «حملات مسلحانه» را تشکیل می‌دهند وجود داشته است و یک دولت بی‌تردید دارای حق ذاتی برای شرکت در یک پاسخ دفاعی «مناسب» به چنین حمله‌ای است (Graham, 2010:34). سؤال اینجاست که دفاع مشروع مناسب چیست؟ پاسخ در صورتی قانونی است که با دو اصل اصلی حقوق بین‌الملل عرفی «ضرورت» و «تناسب» مطابقت داشته باشد (Wingfield, 2000:74). زمانی که مشخص شود که در شرایط حاکم، دولت نمی‌تواند از طریق راه‌های مسالمت‌آمیز به حل‌وفصل معقول اختلاف دست یابد، یک کشور شرط ضرورت را محقق می‌کند. تناسب مستلزم آن است که دولت اقدامات دفاعی از خود را به میزان نیروی مورد نیاز برای شکست دادن یک حمله در حال انجام یا جلوگیری از حمله آینده محدود کند. رعایت این اصل بدیهی است که بستگی به وضعیت واقعی خاص دارد.

آیا حق دفاع مشروع پیشگیرانه یا پیش‌دستانه در چهارچوب حملات سایبری وجود دارد؟ یک اصل طولانی‌مدت از حقوق بین‌الملل عرفی که به پرونده کارولین ۱۸۳۶ باز می‌گردد که در آن یک دولت در معرض تهدید ممکن است به‌طور قانونی به اقدامات

دفاعی متوسل شود، زمانی که «ضرورت آن دفاع از خود فوری، طاقت‌فرسا است و هیچ راهی باقی نمی‌گذارد و هیچ لحظه‌ای برای مشورت نیست». (Shaw, 2010:21) برای اعمال قانونی این حق، یک دولت باید نشان دهد که حمله مورد انتظار قریب‌الوقوع بوده است. در مورد حملات سایبری، برآوردن چنین الزامی اگر غیرممکن نباشد، دشوار خواهد بود (Graham, 2010:37). به‌عنوان‌مثال، حملات سایبری پیچیده به‌گونه‌ای طراحی شده‌اند که سیستم‌های رایانه‌ای یک کشور هدف را به‌طور آنی تحت تأثیر قرار دهند. البته حملات سایبری وجود دارد که یک دولت ممکن است پیش‌بینی کند و با آن‌ها مقابله کند. یک دولت ممکن است شواهدی از تلاش مهاجمان سایبری به شبکه به دست آورد، ممیزی سیستم‌های رایانه‌ای ممکن است بدافزارهای غیرمجاز را نشان دهد یا دولت‌های هدف ممکن است قبل از حمله هماهنگ یک کمپین آنلاین را که به‌عنوان محل تجمع هکرها برای تجارت اطلاعات و ابزارها کشف کنند، در چنین مواردی دولت هدف با توجه به اینکه قبلاً از یک حمله سایبری برنامه‌ریزی‌شده آگاه بوده ممکن است در صورت تحقق معیارهای پرونده کارولین، از حق خود برای پاسخ‌گویی در دفاع شخصی پیش‌بینی‌شده استفاده کند.

همچنین برابر قاعده ۱۱ راهنمای تالین ۲,۰ هر عملیات سایبری که ممکن است به‌عنوان توسل به زور تحت ماده ۲ (۴) منشور ملل متحد در نظر گرفته شود، لزوماً به‌عنوان یک «حمله مسلحانه» که حق دفاع مشروع تحت ماده ۵۱ را ایجاد می‌کند، واجد شرایط نخواهد بود. تعیین اینکه آیا یک عملیات سایبری یک حمله مسلحانه را تشکیل می‌دهد یا خیر، به عوامل مختلفی از جمله شدت و فوریت اثرات آن بستگی دارد (Fevre, V,2017). این عبارات و تحلیل‌های مشابه در سایر بخش‌های راهنمای تالین، به‌وضوح نشان می‌دهند که صرفاً برخی از عملیاتی سایبری، آن‌هایی که دارای شدت، مقیاس و اثرات قابل توجه هستند، می‌توانند به آستانه «حمله مسلحانه» به معنای ماده ۵۱ منشور برسند.

۳-۳. جنایت تجاوز در جنگ‌های ترکیبی

جنایت تجاوز، یکی از مهم‌ترین جرائم بین‌المللی است که در ماده ۸ مکرر اساسنامه رم تعریف شده و شامل «توسل به زور علیه حاکمیت، تمامیت ارضی، یا استقلال سیاسی یک دولت» می‌شود. جنگ ترکیبی، با ترکیب ابزارهای نظامی، اقتصادی، سایبری، اطلاعاتی و روانی، تعریف سنتی از توسل به زور را با چالش‌های جدید مواجه کرده است. در جنگ ترکیبی، اعمالی مانند حمایت از گروه‌های شورشی، عملیات

اطلاعاتی برای بی‌ثبات کردن دولت‌ها، یا حملات سایبری به زیرساخت‌های حیاتی، می‌توانند به سطح توسل به زور برسند. با این حال، شناسایی و انتساب این اقدامات به دولت‌ها یا سایر بازیگران بین‌المللی چالش‌برانگیز است. ابهام در معیارهای شدت و تأثیر این اقدامات باعث شده است که تفکیک میان جنایت تجاوز و سایر تخلفات بین‌المللی دشوار باشد (Re, D,2018:180).

یکی از مباحث کلیدی، نقش عوامل غیر دولتی در جنگ ترکیبی است. این عوامل اغلب به‌عنوان واسطه عمل می‌کنند و امکان انکارپذیری دولت‌ها را فراهم می‌آورند. این امر اجرای حقوق بین‌الملل و پاسخ‌گویی را پیچیده‌تر می‌کند؛ زیرا اساسنامه رم برای اثبات جنایت تجاوز، نیازمند ارتباط روشن و قابل اثبات بین اقدام تجاوزکارانه و یک دولت مشخص است. از سوی دیگر، توسعه قواعد حقوق بین‌الملل برای شناسایی عناصر جنگ ترکیبی به‌عنوان جنایت تجاوز ضروری است. اگرچه اساسنامه رم تأکید زیادی بر حملات نظامی فیزیکی دارد، اما جنگ ترکیبی نشان داده است که توسل به زور می‌تواند اشکال غیرسنتی نیز به خود بگیرد. برای نمونه، حملات سایبری که منجر به تخریب زیرساخت‌های حیاتی یک کشور شود، در صورتی که به سطح شدت و اثرات مشابه با حملات نظامی برسد، می‌تواند جنایت تجاوز تلقی شود. در نتیجه، تطبیق حقوق بین‌الملل با پدیده جنگ ترکیبی نیازمند بازتعریف معیارها و ابزارهای حقوقی است تا بتواند جنبه‌های متنوع و پیچیده این نوع جنگ را دربرگیرد (Palyvoda, V,2022)

حملات سایبری در جنگ‌های ترکیبی نیز می‌توانند در مواردی به نقض «حقوق توسل به زور» منجر شوند و حتی مسئولیت کیفری جنایت تجاوز طبق ماده ۸ (۱) مکرر اساسنامه دیوان کیفری بین‌المللی را در پی داشته باشند (Ophardt, J. A,2010). این دیدگاه، مشروط به این است که حمله سایبری توسط یک دولت انجام شود، زیرا ماده ۸ مکرر شامل رفتار بازیگران غیردولتی نمی‌شود. با این حال، تصور حمله سایبری که به «نقض آشکار» منشور ملل متحد طبق ماده ۸(۱) مکرر برسد، دشوار است. همچنین، مسئولیت کیفری تنها متوجه افرادی است که در موقعیت کنترل مؤثر یا هدایت سیاسی یا نظامی یک دولت قرار دارند، نه افرادی که مستقیماً حمله را اجرا می‌کنند. ماده ۸ (۲) مکرر اساسنامه دیوان کیفری بین‌المللی، فهرستی از «اعمال تجاوز» ارائه می‌دهد که بر استفاده از نیروی مسلح متمرکز است. طبق تفسیرهای موجود، نیروی مسلح معمولاً به معنای نیروی جنبشی از طریق سلاح‌های سنتی است (Gillett, M,2013). با این وجود، تفسیر معاصر از «نیروی مسلح» می‌تواند در برخی شرایط استفاده از شبکه‌های کامپیوتری به‌عنوان سلاح را شامل شود.

۴-۳. جنگ ترکیبی تحت عنوان جنایات جنگی

پیشرفت‌های فناورانه در عرصه درگیری‌های معاصر، مفهوم جنگ ترکیبی را به پدیده‌ای پیچیده و چالش‌برانگیز در حقوق بین‌الملل تبدیل کرده است. این شکل از جنگ، که با تلفیق روش‌های سنتی و ابزارهای نوینی چون حملات سایبری عمل می‌کند، مرز میان جنگ و صلح را مبهم ساخته و اجرای حقوق بشردوستانه بین‌المللی را با چالش‌های جدی مواجه کرده است(Mazaraki & Goncharova, 2022).

از منظر جنایات جنگی، بهره‌گیری از ابزارهای سایبری برای هدف قرار دادن زیرساخت‌های حیاتی یا خدمات ضروری غیرنظامیان می‌تواند مصداق تخلفات جنگی باشد، به‌ویژه زمانی که این اقدامات به‌طور عمدی، غیرنظامیان یا اموال آن‌ها را هدف گیرد. ماده ۸ اساسنامه دیوان کیفری بین‌المللی (ICC) جنایات جنگی را در بیش از ۵۰ مورد احصا کرده که همگی بر مبنای حقوق لاهه و ژنو شکل گرفته‌اند. این جرائم را می‌توان در سه دسته کلی تقسیم‌بندی کرد: نقض حقوق افراد و اموال تحت حمایت، حملات غیرقانونی علیه جمعیت غیرنظامی و استفاده از روش‌های غیرمجاز در جنگ (Ambos, 2022).

تطبیق حملات سایبری با این دسته‌بندی‌ها نیازمند تحقق شرایط عینی و ذهنی خاص هر مورد است. اعمال حقوق بشردوستانه بین‌المللی بر جنگ‌های ترکیبی و حملات سایبری، مشروط به وجود درگیری مسلحانه، استفاده از نیروی مسلح و انتساب اقدامات به یکی از طرف‌های درگیر است (Ambos, 2022:123). در این میان، دو رویکرد برای تشخیص «درگیری مسلحانه» در فضای سایبری وجود دارد: رویکرد ابزار و رویکرد آثار. رویکرد دوم بر پیامدهای حملات سایبری همچون تخریب زیرساخت‌های حیاتی تمرکز دارد و در صورتی که شدت حمله به سطح استفاده از زور برسد، آن را مصداق درگیری مسلحانه می‌داند(Schmitt, 2017:350).

مسئله انتساب حمله نیز اهمیت بنیادینی دارد. بر اساس حقوق بین‌الملل، وجود ارتباط سازمان‌یافته میان گروه‌های مسلح و یکی از طرف‌های درگیری برای احراز مسئولیت ضروری است (Ambos, 2021:543). اجرای حمله سایبری از قلمروِ یک کشور به‌تنهایی کفایت نمی‌کند، بلکه باید انتساب واقعی و مؤثر آن به یک بازیگر مشخص اثبات شود. پیچیدگی بیشتر زمانی پدیدار می‌شود که این حملات از قلمروهای مختلف سرچشمه می‌گیرند و مرزهای جغرافیایی سنتی را درمی‌نوردند(Schmitt, 2012:252).

افزون بر این، در فضای سایبری، غیرنظامیان نیز ممکن است در انجام عملیاتی خصمانه مشارکت داشته باشند، که خود چالش جدی برای تمایز میان مبارزان و

غیرمبارزان محسوب می‌شود. راهنمای تالین ۲,۰ در این زمینه به شناسایی مسئولیت کیفری افراد، از جمله فرماندهان و عاملان حملات، پرداخته و شاخص‌هایی نظیر «آستانه آسیب» و «ارتباط با مخاصمه» را برای تعیین مشارکت مستقیم غیرنظامیان پیشنهاد کرده است(Ambos, 2021:155). در مجموع، چالش‌های فنی، انتسابی و مفهومی حملات سایبری در قالب جنگ ترکیبی، نشان می‌دهد که چهارچوب‌های فعلی حقوق بشردوستانه نیازمند تفسیر توسعه‌یافته و شاید تدوین قواعد جدید برای مقابله با اشکال نوظهور جنایات جنگی هستند.

۵-۳. حملات سایبری و جنایات علیه بشریت

مطابق ماده ۷ (۱) اساسنامه دیوان بین‌المللی کیفری، جنایات علیه بشریت نیازمند رفتارهایی مانند قتل یا شکنجه است که به‌عنوان بخشی از یک حمله گسترده یا سیستماتیک علیه جمعیت غیرنظامی انجام شود. این حمله باید با یک سیاست مشخص هم‌سو باشد «ماده ۷(۲)(الف)» و ویژگی «گسترده» یا «سیستماتیک» آن به‌صورت کیفی ارزیابی شود. در حملات سایبری، این بدان معناست که چنین حملاتی باید توسط یک دولت یا سازمان برنامه‌ریزی یا حداقل تحمل شوند. گروه‌های مسلح سازمان‌یافته که از روش‌های جنگ سایبری استفاده می‌کنند، می‌توانند این معیارها را برآورده کنند. اگر این حملات خسارات شدید و گسترده‌ای ایجاد کنند، ممکن است به‌عنوان «گسترده» نیز طبقه‌بندی شوند. چنین حملات گسترده یا سیستماتیک سایبری می‌توانند به اعمالی مانند قتل یا دیگر جرائم ماده ۷ منجر شوند؛ اما تحقق جنایات علیه بشریت، در نهایت به ارزیابی شرایط خاص هر مورد بستگی دارد (Assidiq, H., Safira, A., & Lubis, S. N,2020).

۴. دکترین دفاعی جنگ ترکیبی جمهوری اسلامی ایران

دکترین دفاعی، مجموعه‌ای از اصول و راهبردهای نظامی است که برای مقابله با تهدیدات و حفاظت از حاکمیت ملی تدوین می‌شود. این دکترین با تحلیل شرایط داخلی و بین‌المللی، تهدیدات نوظهور و ظرفیت‌های ملی، چهارچوبی برای اقدام‌های دفاعی فراهم می‌سازد. از منظر حقوق بین‌الملل، این چهارچوب باید با تعهدات بین‌المللی، به‌ویژه ماده ۵۱ منشور ملل متحد درباره دفاع مشروع، منطبق باشد و قابلیت پاسخ‌گویی به تهدیدات غیر سنتی نظیر جنگ ترکیبی و سایبری را داشته باشد

(Ohlin, 2015). جمهوری اسلامی ایران، با توجه به پیچیدگی محیط امنیتی منطقه‌ای، دکترین جنگ ترکیبی خود را به‌عنوان یک راهبرد جامع برای مقابله با تهدیدات متعارف و نامتقارن تدوین کرده است. این دکترین با ادغام ابزارهای نظامی، سایبری، اقتصادی، دیپلماتیک و اطلاعاتی، به‌دنبال تحقق بازدارندگی فعال و چندوجهی در برابر تهدیدات است (رحمانی، ۱۴۰۱: ۲۹۹). از منظر حقوقی، پایبندی به منشور سازمان ملل و اصول حقوق بین‌الملل بشردوستانه نظیر تناسب، تفکیک و احتیاط در حملات نظامی در این دکترین مورد توجه قرار گرفته است (Bachmann & Munoz Mosquera, 2018).

در بُعد نظامی، ایران با تکیه بر ظرفیت‌های داخلی و نیروهای بسیج مردمی به‌عنوان ابزار جنگ نامتقارن، تلاش دارد از منابع خود بهره‌برداری مؤثری داشته باشد (افشردی و همکاران، ۱۴۰۳: ۹۰). همچنین، عملیات سایبری و جنگ روانی بخشی از راهبرد بازدارندگی فعال ایران محسوب می‌شود که باید در قالب حقوق بین‌الملل و با رعایت حقوق غیرنظامیان به کار گرفته شود (دانش آشتیانی، ۱۳۹۱: ۱۳۰). تغییرات سریع در حوزه فناوری و امنیت جهانی، جمهوری اسلامی را وادار به بازنگری و به‌روزرسانی دکترین خود کرده است تا هم‌راستا با تحولات حقوقی و تکنولوژیک، کارآمدی دفاعی خود را ارتقا دهد (دانش آشتیانی، ۱۳۹۱: ۱۲۰). در مجموع، دکترین جنگ ترکیبی ایران با تلفیق ابعاد حقوقی، نظامی و امنیتی، پاسخی بومی و مؤثر به تهدیدات چندوجهی محسوب می‌شود که تلاش دارد ضمن رعایت موازین بین‌المللی، از امنیت ملی و تمامیت ارضی کشور صیانت کند (خالقی، ۱۳۸۵).

۱-۴. دکترین دفاعی جنگ ترکیبی ایران از نگاه رهبر معظم انقلاب اسلامی

پیروزی انقلاب اسلامی ایران در سال ۱۳۵۷ با واکنش شدید نظام سلطه به‌ویژه ایالات‌متحده آمریکا همراه شد. حمایت همه‌جانبه آمریکا از رژیم بعثی عراق در تجهیز تسلیحاتی و اطلاعاتی، به جنگی هشت‌ساله انجامید که در نهایت با حملات مستقیم آمریکا به تأسیسات دریایی ایران در خلیج فارس همراه شد (Smith, 2015). پس از پایان جنگ، راهبردهای آمریکا از مقابله نظامی به ابزارهای غیرنظامی مانند تهاجم فرهنگی و تحریم‌های اقتصادی تغییر یافت؛ این تحریم‌ها در دهه ۱۳۹۰ خورشیدی به اوج خود رسید و به‌طور خاص بر پایه ادعای فعالیت‌های هسته‌ای ایران توجیه شد (Torbat, 2005). از دیدگاه آیت‌الله خامنه‌ای، دفاع ترکیبی که شامل استفاده از تمامی ظرفیت‌های موجود نظامی، سیاسی و فرهنگی است، تنها راه مقابله با جنگ ترکیبی دشمن است.

بر اساس این راهبرد، جمهوری اسلامی ایران با تقویت توان بازدارندگی نظامی و سرزمینی خود، توانسته است از وقوع حملات گسترده نظامی جلوگیری کند.

برای بررسی دیدگاه‌های آیت‌الله خامنه‌ای در ارتباط با «جنگ ترکیبی» دشمن، لازم است ابتدا شناختی عمیق از هستی‌شناسی سیاسی و نگاه ایشان به نظام جهانی و محیط راهبردی جمهوری اسلامی ایران داشته باشیم. مفاهیم کلیدی به کار گرفته شده توسط آیت‌الله خامنه‌ای در تحلیل نظام ناعادلانه بین‌المللی، ریشه در رویکردهای رهایی‌بخش و انتقادی ایشان به وضعیت موجود دارد. به اعتقاد ایشان، «جنگ ترکیبی» ابزاری است که نظام سلطه جهانی برای مقابله با نیروی رهایی‌بخش انقلاب اسلامی ایران به کار گرفته است تا انقلاب را در نظم جهانی موجود مستحیل کند. به گفته آیت‌الله خامنه‌ای، نظام سلطه یک نظام جهانی است که بر زندگی بشر تسلط یافته و به دو طرف تقسیم می‌شود: یک طرف ابرقدرت‌هایی که سلطه‌گرند و طرف دیگر دولت‌هایی که سلطه‌پذیرند و دخالت‌های گستاخانه ابرقدرت‌ها را می‌پذیرند. در این میان، ملت‌هایی که آگاهی یا توان مقاومت ندارند، پایمال می‌شوند؛ اما ملت ایران، که در مقابل این زورگویی‌ها ایستاده است، با اعتماد به نفس و اتکا به اراده خود، به سلطه‌گران «نه» گفته و به مقاومت می‌پردازد (خامنه‌ای، مکتوبات، ۱۳۶۸).

در سال‌های ابتدایی رهبری، آیت‌الله خامنه‌ای ویژگی‌های نظام سلطه را با استفاده از مفاهیم قرآنی و دینی تحلیل کردند. از دید ایشان، استکبار جهانی مشابه حالت فرعونیت و دیکتاتوری در سطح بین‌المللی است. ملت‌ها ممکن است در داخل کشور خود با دیکتاتوری مبارزه کنند، اما در سطح بین‌المللی، با یک دیکتاتور جهانی مواجه هستند که در سرنوشت آن‌ها دخالت می‌کند (خامنه‌ای، مکتوبات، ۱۳۷۶). در دهه ۱۳۷۰، تحلیل‌های آیت‌الله خامنه‌ای از نظام سلطه، با تمرکز بیشتری بر نقش آمریکا در این نظام دنبال شد. ایشان رفتارهای استکباری آمریکا را اصلی‌ترین تجلی نظام سلطه معرفی کردند و بر این باور بودند که ایالات‌متحده به‌عنوان رأس نظام سلطه، به دنبال تسلط بر جهان است (خامنه‌ای، مکتوبات، ۱۳۷۰). این رویکرد باعث شد که آیت‌الله خامنه‌ای آمریکا را مظهر اصلی نظام سلطه معرفی کنند.

در نهایت، آیت‌الله خامنه‌ای تأکید دارند که نظام سلطه به هیچ معاهده بین‌المللی یا اصول اخلاقی پایبند نیست. هر جا که آمریکا منافع خود را در خطر ببیند، به خود اجازه می‌دهد که از ابزارهای نظامی و قهری استفاده کند، حتی اگر این منافع در تضاد با حقوق بین‌الملل باشد (خامنه‌ای، مکتوبات، ۱۳۷۴). همچنین آیت‌الله خامنه‌ای رویکرد اخیر خود را در مواجهه با جنگ ترکیبی دشمن تبیین کرده و فرمودند نمی‌توان

همیشه در موضع دفاعی بمانیم و باید جمهوری اسلامی ایران نیز در جنگ ترکیبی اقدام متقابل نماید، ایشان در بیانات خود فرمودند: «دشمنان ما امروز دست زده‌اند به یک تهاجم ترکیبی؛ تهاجم دشمن یک تهاجم ترکیبی است؛ یعنی جنبه اقتصادی در آن هست؛ جنبه سیاسی در آن هست؛ جنبه امنیتی در آن هست؛ جنبه رسانه‌ای در آن هست؛ جنبه دیپلماسی در آن هست و از همه جهت یک حمله ترکیبیِ دسته‌جمعی را شروع کرده‌اند؛ ما هم در مقابل بایستی حرکتمان حرکت ترکیبی باشد؛ از همه جهت بایستی تلاش کنیم. البته دفاع باید بکنیم؛ اما همیشه در موضع دفاعی نمی‌توانیم بمانیم؛ این را باید توجه داشت. این که من می‌گویم باید دفاع کنیم، خب دفاع یک کار لازم است؛ اما همیشه نمی‌شود در موضع دفاعی ماند؛ دشمن تهاجم می‌کند، ما هم باید تهاجم داشته باشیم ...» (خامنه‌ای، بیانات، ۱۳۹۹).

جنگ ترکیبی در دیدگاه آیت‌الله خامنه‌ای به‌عنوان راهبردی پیچیده و چندوجهی مطرح شده است که همواره به‌عنوان هشداری برای تصمیم‌سازان سیاست خارجی جمهوری اسلامی ایران ارائه می‌شود. جنگ ترکیبی به‌عنوان راهبردی نظام‌مند، طراحی شده توسط نظام سلطه به رهبری ایالات‌متحده به‌منظور مقابله با انقلاب اسلامی و سیاست‌های رهایی‌بخش آن است (خامنه‌ای، مکتوبات، ۱۴۰۲). در این رویکرد، ابزارهای نرم‌افزاری و جنگ نرم در دستیابی به اهداف دشمن نقشی کلیدی ایفا می‌کنند. آیت‌الله خامنه‌ای در چندین نوبت با تأکید بر لزوم تقویت قدرت بازدارندگی جمهوری اسلامی، نفوذ نرم دشمن را به‌عنوان سازوکاری خطرناک تلقی کرده‌اند که با تهدیدات جدید مواجه است (خامنه‌ای، بیانات، ۱۴۰۲). در جنگ ترکیبی، پیچیدگی سازوکارهای اعمال شده علیه جمهوری اسلامی ایران ناشی از رویکرد چندسطحی و شبکه‌ای است که دشمن برای مقابله با جمهوری اسلامی به کار می‌گیرد. این جنگ، نه‌تنها بر جنبه‌های نظامی، بلکه بر ابزارهای غیرنظامی نظیر رسانه‌ها، فرهنگ، امنیت، نفوذ اقتصادی و حتی فناوری‌های ارتباطی متمرکز است. هدف این نوع جنگ، ایجاد یأس و ناامیدی در میان ملت، قطع ارتباط آنان با منابع اطلاعاتی صحیح و تحریف واقعیت‌ها است. دشمنان سعی می‌کنند با استفاده از همه این ابزارها، ملت ایران را تحت محاصره قرار دهند و آنان را از توانایی‌های خود غافل کنند(خامنه‌ای، بیانات، ۱۴۰۰).

آیت‌الله خامنه‌ای تأکید دارند که برای مقابله با این جنگ، جمهوری اسلامی باید راهبردی چندسطحی اتخاذ کند و از ابزارهای مختلف سخت و نرم در جهت دفاع و حمله استفاده کند. ایشان با اشاره به استمرار قدرت جمهوری اسلامی در بیش از چهار دهه اخیر، آینده‌ای روشن و محکم را برای کشور پیش‌بینی کرده‌اند، مشروط بر اینکه

تمامی مسئولان و مردم وظایف خود را به‌درستی انجام دهند (خامنه‌ای، بیانات، ۱۴۰۰). در نهایت، راهبرد دفاعی جمهوری اسلامی باید به‌گونه‌ای باشد که نه‌تنها به تهدیدات پاسخ دهد، بلکه در برابر تهاجمات دشمن نیز به‌صورت پیش‌دستانه عمل کند. این راهبرد دفاعی شامل تقویت آگاهی عمومی و افزایش هوشیاری ملت در برابر جنگ نرم دشمن است. آیت‌الله خامنه‌ای همواره بر لزوم آگاهی‌بخشی به توده‌های مردمی از طریق اطلاع‌رسانی دقیق و صحیح تأکید کرده‌اند و معتقدند که این اقدام از وظایف اصلی نخبگان در حوزه «جهاد تبیین» است (خامنه‌ای، بیانات، ۱۴۰۲).

۲-۴. تحلیل دکترین دفاعی رهبر معظم انقلاب اسلامی در استفاده از دکترین دفاعی اقدام متقابل برای مقابله با جنگ ترکیبی

از دیدگاه حقوق بین‌الملل اقدام متقابل در عصر حاضر موضوعی پیچیده و بحث‌برانگیز است، به‌ویژه در منطقه‌ای مانند غرب آسیا که تحت تأثیر تحولات ژئوپلیتیک و تهدیدات ترکیبی قرار دارد. جنگ ترکیبی، شامل ترکیب تهدیدات نظامی، اقتصادی، سایبری، رسانه‌ای و دیپلماتیک است که در سطوح مختلف، با هدف بی‌ثبات‌سازی و تضعیف ساختارهای حاکمیتی و اجتماعی یک کشور به‌کار گرفته می‌شود. این نوع جنگ‌ها می‌توانند بدون نقض آشکار مرزهای ملی یک کشور یا استفاده از ابزارهای متعارف نظامی انجام شوند و به همین دلیل، چالش‌هایی را در تعیین پاسخ‌های قانونی و مشروع، به‌ویژه در چهارچوب عمل متقابل، ایجاد می‌کنند. یک کشور می‌تواند این حق را داشته باشد که اقدام‌های متقابلی را در پاسخ به نقض حقوق بین‌المللی انجام دهد که توسط دولت دیگری انجام شده است. این اقدام‌های متقابل به معنای انتقام‌جویی نیست و موجب اعمال «استفاده از زور» نمی‌شود، به شرطی که عمل انجام شده به‌عنوان اقدام متقابل صحیح شناخته شود و اقدام ممنوع شده به‌درستی مورد توجه قرار گیرد.[1](Schmitt, M. N. (Ed.),2017:329). هدف اصلی اقدام‌های متقابل این است که دولت مسئول عمل غیرحقوقی را به توقف آن اعمال یا اقدام‌های وادار کند و در صورت امکان تضمین عدم تکرار و جبران خسارت را ارائه دهد. اقدام‌های متقابل به‌عنوان راه‌حلی طراحی شده‌اند که نتیجه مطلوب برای دولت‌های درگیر باید بازگشت به روابط حقوقی میان آن‌ها باشد[2](Schmitt, M. N. (Ed.),2017:329) .

1. Schmitt, Rule 20
2. Schmitt Rule 21

برابر ماده ۴۹ پیش‌نویس مسئولیت بین‌المللی دولت‌ها ۲۰۰۱ اقدام متقابل[1] وادار کردن دولت نقض‌کننده به رعایت مجدد تعهدات بین‌المللی است، نه تنبیه یا آسیب‌رسانی. اقدام متقابل باید به‌عنوان ابزاری موقت و متناسب با نقض تعهدات باشد. این اقدام باید متناسب با نقض تعهد و با رعایت اصول کلی حقوق بین‌الملل انجام شود. طبق ماده ۵۲ پیش‌نویس مسئولیت بین‌المللی دولت‌ها نسبت به اعمال بین‌المللی غیرحقوقی، شرایطی برای زمانی که یک دولت می‌تواند به اقدام‌های متقابل روی آورد، وجود دارد:

۱. قبل از اتخاذ اقدام‌های متقابل، دولت آسیب‌دیده باید:

- از دولت مسئول، طبق ماده ۴۳، بخواهد که تعهدات خود تحت بخش دوم را انجام دهد؛
- دولت مسئول را از هر تصمیم به اتخاذ اقدام‌های متقابل مطلع کند و پیشنهاد مذاکره با آن دولت را ارائه دهد.

۲. با وجود بند ۱ (ب) فوق، دولت آسیب‌دیده می‌تواند اقدام‌های متقابل فوری را که برای حفظ حقوق خود ضروری است، اتخاذ کند.

اقدام‌های متقابل نباید به حقوقی که برای حفاظت از ارزش‌های بنیادین جامعه بین‌المللی شناخته شده‌اند (مانند حقوق بشری یا حقوق بشردوستانه)، آسیب بزند. ماده ۴۹ همچنین مقدمه‌ای برای مواد بعدی است که به شرایط و محدودیت‌های خاصی که بر اقدام‌های متقابل اعمال می‌شود، از جمله اصل تناسب و رعایت تعهدات غیرقابل نقض در حقوق بین‌الملل، پرداخته است. بااین‌حال، در جنگ‌های ترکیبی که از ابزارهای مختلف و غیرمتعارف استفاده می‌شود، تعیین مرزهای عمل متقابل و مشروعیت آن دشوار است (Hoffman, 2009). حقوق بین‌الملل به‌طور معمول تنها اقدام‌های نظامی مستقیم را در چهارچوب دفاع مشروع و ماده ۵۱ منشور ملل متحد در نظر می‌گیرد؛ اما در جنگ ترکیبی، حملات می‌توانند به‌صورت غیرمستقیم و از طریق ابزارهای سایبری، اقتصادی یا حتی نفوذهای فرهنگی صورت گیرند که پاسخ متقابل به آن‌ها می‌تواند پیچیده‌تر و حتی نامشهودتر باشد. در واقع، اصل تناسب در حقوق بین‌الملل که بیان می‌کند پاسخ باید هم از نظر دامنه و هم شدت متناسب با حمله باشد، در شرایط جنگ ترکیبی به‌سختی قابل اعمال است؛ زیرا آسیب‌های

1. Countermeasure

اقتصادی یا سایبری گاهی غیر قابل اندازه‌گیری و پیش‌بینی هستند (Kofman & Rojansky, 2015).

در بسیاری از موارد جنگ ترکیبی، ابزارهای سایبری و اقتصادی به‌عنوان اهرم‌هایی برای آسیب‌رسانی به زیرساخت‌های کلیدی استفاده می‌شوند. بر اساس قوانین حقوق بین‌الملل، اقدام‌های متقابل در این حوزه‌ها می‌تواند به شرطی مشروع شناخته شود که به هدف رفع تهدید صورت گیرد و آسیب‌های جانبی به‌ویژه برای شهروندان بی‌گناه به حداقل برسد. پاسخ‌های سایبری باید بر اساس قوانین عرفی بین‌الملل کنترل شود و از ایجاد بی‌ثباتی بین‌المللی یا آسیب به ساختارهای ضروری انسانی و اقتصادی کشورهای دیگر جلوگیری نماید. اصل تناسب در پاسخ به اقدام‌های ترکیبی و عمل متقابل، یکی از چالش‌های اصلی حقوق بین‌الملل در این حوزه است. درحالی‌که منشور سازمان ملل متحد، دفاع مشروع را تنها در برابر حملات مسلحانه قانونی می‌داند؛ اما برخی از حقوقدانان این دیدگاه را به اقدام‌های سایبری و اقتصادی نیز گسترش می‌دهند (Hathaway et al., 2012). بنابراین، اقدام‌های تلافی‌جویانه در چهارچوب حقوق بین‌الملل باید به‌گونه‌ای باشد که هم‌زمان با رفع تهدید، از تشدید تنش‌های غیرضروری و آسیب‌های اضافی به شهروندان غیرنظامی جلوگیری کند.

حقوق بین‌الملل عرفی نیز در زمینه جنگ ترکیبی اهمیت پیدا می‌کند. با وجود اینکه قوانین تدوین‌شده بین‌المللی ممکن است پاسخ واضحی به تهدیدات ترکیبی ندهد، حقوق عرفی بین‌الملل می‌تواند به‌عنوان مبنایی برای تعیین اقدام‌های متقابل قابل‌قبول در پاسخ به جنگ ترکیبی عمل کند. در این حوزه، دولت‌ها معمولاً به اصل «مداخله نکردن» استناد می‌کنند، که مطابق آن هیچ کشوری نباید در امور داخلی کشور دیگری مداخله کند؛ به‌ویژه در مواردی که تهدیدات ترکیبی شامل حمایت از نیروهای نیابتی در داخل یک کشور می‌شود. از دیدگاه حقوق بین‌الملل، جنگ ترکیبی با ویژگی تهدیدات زیر آستانه تجاوز و توسل به زور، به‌ویژه در حوزه‌هایی مانند اقتصاد، سایبری، دیپلماسی و عملیات روانی، چهارچوب جدیدی برای مفهوم اقدام متقابل ایجاد می‌کند. چون این اقدام‌های اغلب از سطح تجاوز مسلحانه عبور نمی‌کنند، قواعد حقوق بشردوستانه بین‌المللی که برای درگیری‌های مسلحانه تدوین شده‌اند، الزاماً بر این اقدام‌های قابل اعمال نیستند. بنابراین، اقدام متقابل در این وضعیت می‌تواند در حوزه حقوق بین‌الملل عمومی، به‌ویژه حقوق بین‌الملل عرفی و حقوق مسئولیت دولت‌ها قرار گیرد، به شرط آنکه این اقدام‌های متناسب، محدود به رفع تهدید، و در تطابق با اصول ضروری و تناسب باشند (Hathaway et al, 2012).

در چهارچوب عمل متقابل، اگر تهدیدات ترکیبی شامل حملات سایبری یا تحریم‌های اقتصادی باشد، دولتی که مورد تهدید قرار گرفته می‌تواند با اقدام‌هایی متناسب و در چهارچوب حقوق بین‌الملل به آن پاسخ دهد. این اقدام‌ها باید به‌گونه‌ای باشند که فقط به رفع تهدید بپردازند و از تبدیل وضعیت به درگیری مسلحانه تمام‌عیار جلوگیری کنند. به‌عنوان مثال، در حوزه سایبری، استفاده از اقدام‌های تلافی‌جویانه سایبری به شرطی مجاز است که آسیب به زیرساخت‌های حیاتی غیرنظامی به حداقل برسد و از تأثیرات جانبی غیرقابل توجیه پرهیز شود. به‌طورکلی، راهبرد دفاعی مد نظر رهبری مبنی بر عمل متقابل در جنگ ترکیبی باید همواره با رعایت الزامات حقوقی و در چهارچوب قوانین عرفی و معاهدات بین‌المللی مرتبط، به‌ویژه اصول تناسب و ضرورت، صورت گیرد. از آنجا که بسیاری از اقدام‌های جنگ ترکیبی ممکن است به‌طور مستقیم منجر به نقض حقوق بشردوستانه نشود، ولی اثراتی منفی بر امنیت و ثبات بین‌المللی داشته باشد، پاسخ‌های متقابل در این وضعیت مستلزم رعایت اصولی هستند که بتوانند به حفظ تعادل و جلوگیری از تشدید تنش‌ها کمک کنند.

هر چند که از نگاه حقوق بین‌الملل، اصل عدم تقابل در حقوق بشردوستانه حتی در صورت نقض از سوی طرف مقابل همچنان پابرجا و غیرقابل تعلیق هستند. به عبارت دیگر، در حقوق بشردوستانه بین‌المللی، توسل به عمل متقابل برای پاسخ‌گویی به نقض تعهدات بشردوستانه از سوی طرف مقابل نه‌تنها بی‌معنا، بلکه مغایر با اهداف و اصول بنیادین این نظام حقوقی است. هدف حقوق بشردوستانه، حمایت از غیرنظامیان و افرادی است که در جریان درگیری‌ها دیگر نقشی ندارند، و تعهد به رعایت آن برای همه طرفین الزام‌آور است. این رویکرد به صراحت در کنوانسیون‌های ژنو و پروتکل‌های الحاقی ذکر شده است. به‌عنوان مثال، ماده ۱ مشترک بین کنوانسیون‌های ژنو تأکید می‌کند که دولت‌ها باید همواره به تعهدات بشردوستانه خود عمل کنند و از تعلیق آن‌ها به‌عنوان ابزار متقابل استفاده نکنند (ICRC, 2016). همچنین، ماده ۶۰ کنوانسیون وین درباره حقوق معاهدات بیان می‌کند که در صورت نقض یک معاهده بشردوستانه، طرف دیگر نمی‌تواند تعهدات خود را نادیده بگیرد، زیرا این تعهدات از نوع قواعد آمره[1] و برای حمایت از حقوق بنیادین بشر در همه شرایط است. بنابراین، حقوق بشردوستانه یک نظام حقوقی مستقل و الزام‌آور برای همه طرفین درگیر است و تضعیف یا تعلیق

1. Jus Cogens

آن‌ها به بهانه نقض توسط طرف مقابل مغایر با اصول حقوق بین‌الملل و هدف کلی حمایت از بشریت است (Dinstein, 2022).

در نتیجه دکترین جمهوری اسلامی ایران بر «دفاع بازدارنده» و «مقاومت همه‌جانبه» تمرکز دارد و متأثر از عوامل ایدئولوژیک، تاریخی و محیط نظامی-سیاسی بین‌المللی است. اسلام به‌عنوان ایدئولوژی نظام، تأثیری بنیادین بر نهادهای اجتماعی و نظامی داشته و اصول بازدارندگی و دفاع مشروع را بر اساس آیات قرآن مانند سوره انفال (آیه ۶۰) و سوره حج (آیه ۳۹) تقویت می‌کند. این اصول دفاعی در قرآن به‌وضوح بر ضرورت آمادگی نظامی، مقابله با تجاوز، و دفاع از مظلومان تأکید دارد. (یداللهی،۱۳۹۹: ۳۱۵) جنگ هشت‌ساله با عراق نیز تأثیر عمیقی بر شکل‌گیری این دکترین داشته و بر اهمیت بازدارندگی تأکید کرده است. قانون اساسی ایران، به‌ویژه اصل ۱۵۲، سیاست خارجی کشور را بر حفظ استقلال، تمامیت ارضی و رد سلطه‌پذیری استوار می‌داند. مقام معظم رهبری نیز دفاع را بخشی از هویت ملی زنده دانسته و دفاع مشروع را ضرورتی عقلانی برای حفظ کشور و نظام اسلامی معرفی کرده‌اند (خامنه‌ای، مکتوبات، ۱۳۶۸). این ترکیب از آموزه‌های دینی و حقوقی، چهارچوبی جامع برای دکترین دفاعی ایران ایجاد کرده که بر حفظ تمامیت ارضی و مقابله با تهدیدات خارجی، با رعایت حقوق دیگر ملت‌ها، استوار است.

نتیجه‌گیری

جنگ ترکیبی تحولات عمده‌ای در مفهوم و چهارچوب‌های حقوقی حاکم بر مخاصمات مسلحانه ایجاد کرده است. این نوع جنگ، با بهره‌گیری از فناوری‌های نوین به‌ویژه در حوزه سایبری، پیچیدگی‌های جدیدی را در تعریف و ارزیابی تهدیدات نظامی به‌وجود آورده است. از جمله این پیچیدگی‌ها می‌توان به حملات سایبری به زیرساخت‌های حیاتی و چالش‌های مربوط به اثبات منشأ این حملات اشاره کرد. این تحولات نه‌تنها رویکردهای نظامی را به‌طور بنیادین تغییر داده‌اند، بلکه قواعد حقوق بین‌الملل موجود را نیز به‌طور جدی تحت تأثیر قرار داده‌اند. بسیاری از قواعد حقوقی کنونی با ابعاد مختلف جنگ‌های ترکیبی، به‌ویژه جنبه تهدیدات سایبری آن، هماهنگ نیستند و این ناهماهنگی چالش‌های حقوقی و عملیاتی متعددی را ایجاد کرده است. یکی از مهم‌ترین چالش‌های حقوقی ناشی از جنگ‌های ترکیبی، به‌ویژه در حوزه سایبری، مربوط به قواعد دفاع مشروع و آستانه توسل به زور تحت منشور ملل متحد است. استفاده از جنگ سایبری به‌عنوان یک بُعد اساسی از جنگ‌های ترکیبی، مرزهای سنتی

دفاع مشروع را تحت تأثیر قرار داده و نیازمند بازتعریف مفاهیم حقوقی مرتبط است. در این زمینه، مطالعه دکترین دفاعی جمهوری اسلامی ایران نشان می‌دهد که رویکردهای ملی می‌توانند الهام‌بخش تحولات بین‌المللی در حوزه جنگ‌های ترکیبی باشند. دکترین دفاعی ایران در این حوزه با تمرکز بر بازدارندگی فعال و هوشمندسازی سامانه‌های دفاعی و تأکید بر اقدامات متقابل الگویی راهبردی برای مدیریت تهدیدات سایبری ارائه می‌دهد که می‌تواند به‌عنوان یک مدل برای سایر کشورها نیز مورد توجه قرار گیرد.

با توجه به پیچیدگی‌های ناشی از جنگ‌های ترکیبی، تدوین هنجارهای بین‌المللی جدیدی که با اصول و موازین حقوق مخاصمات مسلحانه بین‌المللی هم‌خوانی داشته باشد، ضروری به نظر می‌رسد. طراحی این قواعد مستلزم وجود مبانی مستحکم در حقوق بین‌الملل بشردوستانه است. قواعدی همچون ماده ۳۶ پروتکل اول الحاقی به کنوانسیون‌های ژنو ۱۹۴۹ و شرط مارتنس می‌توانند به‌عنوان زیرساختی برای تنظیم این قواعد جدید عمل کنند. این قواعد می‌توانند چهارچوبی جامع برای رعایت اصول انسانی و پاسخ به نیازهای مخاصمات مدرن فراهم آورند. در عین حال، اصول بنیادین حقوق بشردوستانه بین‌المللی در جنگ ترکیبی از ظرفیت لازم برای انطباق با چالش‌های جدید برخوردار هستند؛ اما نیازمند قواعد مناسبی هستند تا این اصول به‌طور مؤثر اجرایی شوند. در این راستا، همکاری‌های بین‌المللی برای تدوین قواعد جدید و ایجاد سازوکارهای نظارتی مؤثر، بیش از پیش اهمیت یافته است. این همکاری‌ها نه‌تنها به تقویت و تبیین حقوق بین‌الملل در بُعد سایبری جنگ ترکیبی کمک می‌کنند، بلکه می‌توانند زمینه‌ساز ایجاد یک چهارچوب حقوقی جامع و منسجم برای مقابله با تهدیدات نوین باشند. در نهایت، تحولات ناشی از جنگ‌های ترکیبی نشان می‌دهد که حقوق بین‌الملل باید به‌طور مستمر با پیشرفت‌های فناوری و تغییرات در عرصه نظامی همگام شود تا بتواند به‌طور مؤثر به نیازهای جهان معاصر پاسخ دهد.

فهرست منابع

- آیت‌الله خامنه‌ای، سید علی (۱۳۶۸/۰۴/۲۵). بیانات در دیدار اقشار مختلف مردم، رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/speech-content?id=2144
- آیت‌الله خامنه‌ای، سید علی (۱۳۶۸/۰۸/۲۹). بیانات و رهنمودهای ایشان پس از بازدید از ستاد کل سپاه پاسداران انقلاب اسلامی. رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/speech-content?id=11062
- آیت‌الله خامنه‌ای، سید علی (۱۳۷۶/۰۸/۱۴) بیانات در دیدار جمعی از دانش آموزان و دانشجویان رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/speech-content?id=9945
- آیت‌الله خامنه‌ای، سید علی (۱۳۷۰/۰۸/۱۵) بیانات در دیدار اقشار مختلف مردم رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/search-result?q=%D9%81%DA%
- آیت‌الله خامنه‌ای، سید علی (۱۳۷۴/۰۸/۱۴) بیانات در دیدار جمعی از دانش آموزان و دانشجویان رجوع شود به تارنمای الکترونیکی: https content?id=2772h/ir.khamenei.farsi
- آیت‌الله خامنه‌ای، سید علی (۱۳۹۹/۱۱/۱۹) بیانات در دیدار فرماندهان و کارکنان نیروی هوایی و پدافند هوایی ارتش. رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/speech-content?id=49572
- آیت‌الله خامنه‌ای، سید علی (۱۴۰۲/۰۱/۰۱). بیانات در اجتماع زائران و مجاوران حرم مطهر رضوی. رجوع شود به تارنمای الکترونیکی: https://farsi.khamenei.ir/speech-content?id=52275
- اعلائی فرد، سپیده (۱۴۰۳). ***اصل تناسب در پرتو استفاده از هوش مصنوعی در مخاصمات مسلحانه***. مطالعات حقوقی فضای مجازی، شماره نهم،۴۴-۳۵
- بخشی، فرشاد؛ محمودی، هادی (۱۴۰۲). ***بررسی تأثیر ابعاد سایبری جنگ ترکیبی بر حقوق مخاصمات مسلحانه***، چهارمین کنفرانس ملی پدافند سایبری، مراغه، ۲۸۰
- دانش آشتیانی، محمدباقر (۱۳۸۸). ***اصول و روش تدوین دکترین نظامی***، فصلنامه نظم و امنیت انتظامی، شماره سوم سال دوم.
- رحمانی، ساعد؛ شفیعی، جمال (۱۴۰۱). ***مفهوم و مؤلفه‌های امنیت فرهنگی در گفتمان ایرانی اسلامی***، فصلنامه امنیت ملی، ۱۲(۴۴)، ۲۹۹-۳۳۲
- شریفی طراز کوهی، حسین (۱۳۹۵). ***حقوق بشردوستانه بین‌المللی***،چاپ دوم، تهران: انتشارات بنیاد حقوقی میزان.
- صادقی زهره؛ عربیان محمدجواد (۱۴۰۱). ***چالش‌های کاربرد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری چالش‌های تطبیق اصول حاکم بر مخاصمات مسلحانه بر حملات سایبری بررسی موردی: رعایت اصل ممنوعیت توسل به زور و اصل تفکیک در حملات سایبری***، مطالعات حقوقی فضای مجازی، شماره دوم،۷۳-۸۶

- فلک، دیتر (۱۳۹۵). ***حقوق بشردوستانه در مخاصمات مسلحانه***،ترجمه حسین شریفی طراز کوهی و همکاران، چاپ چهارم، تهران: انتشارات شهر دانش
- قاسمی، فرهاد؛ اسماعیلی فرزین، ایرج (۱۳۹۶). ***جنگ ترکیبی در سیستم بین‌المللی پیچیده آشوبی، فصلنامه مدیریت نظامی***، سال هفدهم، شماره ۲،۶۹-۸۵
- موثقی، حسن (۱۴۰۱). ***چالش‌های کاربرد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری***، مطالعات حقوقی فضای مجازی، شماره دوم،۱۷-۲
- نامدار مظفر، ضمیریان محمدحسین (۱۳۹۰). مقام معظم رهبری و نظریه ساختاری روابط بین‌الملل در سیاست‌گذاری خارجی جمهوری اسلامی ایران.
- یداللهی، رضا (۱۳۹۹). ***مبانی و اصول دفاعی جمهوری اسلامی ایران از منظر قرآن کریم***. مطالعات دفاعی استراتژیک، سال هجدهم، شماره ۷۹، ۳۱۱-۳۳۰.

References

- Alston, P. (2010). Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Addendum, Study on Targeted Killings. United Nations, General Assembly.
- Ambos, K. (2013). Treatise on International Criminal Law: Volume 1: Foundations and General Part. OUP Oxford.
- Ambos, K. (2022). Treatise on International Criminal Law: Volume II: The Crimes and Sentencing. Oxford University Press.
- Amsellem, D. (2020). Le cyberespace israélien, un enjeu de puissance. Hérodote, (2-3), 281-296.
- Asada, M. (2012). The Concept of "Armed Conflict" in International Armed Conflict. In What Is War? (pp. 51-67).
- Assidiq, H., Safira, A., & Lubis, S. N. (2020, December). Cyber Attack-The Burden of International Crime Proof: Obstacles and Challenges. In The 2nd International Conference of Law, Government and Social Justice (ICOLGAS 2020) (pp. 67-74). Atlantis Press.
- Bachmann & Munoz Mosquera (2018). Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach.
- Bange, O. (2009). NATO as a Framework for Nuclear Nonproliferation: The West German Case, 1954–2008. International Journal.
- Barno, D. (2014). Unconventional warfare and modern conflicts. Foreign Affairs.
- Bellal, A. (2020). What Are 'Armed Non-State Actors'? A Legal and Semantic Approach. International Humanitarian Law and Non-State Actors: Debates, Law and Practice, 21-46.
- Blank, L. R. (2020). Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict. Notre Dame L. Rev., 96, 249.
- Bokil, R. (2023). Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law. International Journal for Multidisciplinary Research, 5(1), 1-12.
- Bordin, F. L. (2018). The Nicaragua v. United States Case: An Overview of the Epochal Judgments. Nicaragua Before the International Court of Justice: Impacts on International Law, 59-83.
- Bothe, M., Partsch, K. J., & Solf, W. A. (Eds.). (1982). New rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949. Martinus Nijhoff Publishers.
- Cantwell, D. (2017). Hybrid Warfare: Aggression and Coercion in the Gray Zone. American Society of International Law.
- Dinstein, Y. (2022). The conduct of hostilities under the law of international armed conflict. Cambridge university press
- Dooley, J. F. (2024). Cyber Weapons and Cyber Warfare. In History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms (pp. 241-268). Cham: Springer International Publishing.
- Ducaru, S. D. (2016). The cyber dimension of modern hybrid warfare and its relevance for NATO. Europolity-Continuity and Change in European Governance, 10(1), 7-23.

- Fèvre, V. (2017). TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, Cambridge, Cambridge University Press, 2017, 640 pages. Politique étrangère, (4).
- Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? Small Wars & Insurgencies, 27(2), 282-301.
- Gerasimov, V. (2016). The evolution of modern warfare. Military Review, 23(1)
- Gervais, M. (2012). Cyber-Attacks and the Laws of War. Berkeley Journal of International Law, 30, 525-531.
- Gervais, M. (2012). Cyber-Attacks and the Laws of War. Berkeley Journal of International Law, 30, 525-531.
- Giegerich, B. (2016). Hybrid warfare and the changing character of conflict. Connections, 15(2), 65-72.
- Gillett, M. (2013). The Anatomy of an International Crime: Aggression at the International Criminal Court. International Criminal Law Review, 13(4), 829-864.
- Graham, D. E. (2010). Cyber Threats and the Law of War. Journal of National Security Law and Policy, 4, 89.
- Graham, D. E. (2010). Cyber Threats and the Law of War. Journal of National Security Law and Policy, 4, 89.
- Hadji-Janev, M. (2016). International Legal Aspects of Protecting Civilians and Their Property in the Future Cyber Conflict. In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare (pp. 423-449). IGI Global.
- Hoffman, F. G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict (Vol. 220). Washington, DC: Institute for National Strategic Studies, National Defense University.
- Hannigan, R. (2014). The web is a terrorist's command-and-control network of choice. Financial Times, 3, 2014.
- Hansel, M. (2011). Stuxnet und die Sabotage des iranischen Atomprogramms: Ein neuer Kriegsschauplatz im Cyberspace? (pp. 564-576). VS Verlag für Sozialwissenschaften.
- Hathaway, O. A., & Crootof, R. (2012). The Law of Cyber Attack. Faculty Scholarship Series, Paper 3852.
- International Committee of the Red Cross (ICRC). (2016). Commentary on the First Geneva Convention. Cambridge University Press.
- International Court of Justice. (1986). Nicaragua v. United States of America: Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). ICJ Reports 1986, p. 14. https://www.icj-cij.org/en/case/70
- Kabiri, F. V., Rajaipour, M., & Razmi, S. M. (2021). Una investigación de los delitos cibernéticos desde el punto de vista de la jurisprudencia de Imamieh (Irán). Apuntes Universitarios, 11(1), 352-363.
- Kofman, M., & Rojansky, M. (2015). A closer look at Russia's' hybrid war'. Woodrow Wilson International Center for Scholars
- Korhonen, O. (2015). Deconstructing the conflict in Ukraine: The relevance of international law to hybrid states and wars. German Law Journal, 16(3), 452-478.

- Leonard, M. (2021). The age of unpeace: How connectivity causes conflict. Random House.
- Lin, H. (2012). Cyber conflict and international humanitarian law. International Review of the Red Cross, 94(886), 515-531.
- Lin, H. S. (2010). Offensive cyber operations and the use of force. J. Nat'l Sec. L. & Pol'y, 4, 63.
- Mattis, J. N., & Hoffman, F. (2005). Future warfare: The rise of hybrid wars. Proceedings-United States Naval Institute, 131(11), 18.
- Mazaraki, N., & Goncharova, Y. (2022). CYBER DIMENSION OF HYBRID WARS: ESCAPING A'GREY ZONE'OF INTERNATIONAL LAW TO ADRESS ECONOMIC DAMAGES. Baltic Journal of Economic Studies, 8(2), 115-120.
- Melzer, N. (2009). Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. International Committee of the Red Cross.
- Moore, J. N. (2005). Development of International Law of Conflict Management. In National Security Law (2nd ed.). Durham, NC: Carolina Academic Press.
- Nyemann, D. B., & Sørensen, H. (2019). Deterrence by Punishment as a way of Countering Hybrid Threats-Why we need to go" beyond resilience" in the gray zone.
- Ohlin, J. D. (2015). The Doctrine of Legitimate Defense (Cornell Law School Research Paper No. 15-12).
- Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. Duke L. & Tech. Rev., 9, 1.
- Palyvoda, V. (2022). ON HYBRID WARFARE, WITHOUT MYSTIFICATION OR CONSPIRACY. Strategic Panorama, (1), 66-69.
- Parker, S. K., Winslow, C. J., & Tetrick, L. E. (2016). Designing meaningful, healthy, and effective cyber security work. In Psychosocial dynamics of cyber security (pp. 240-266). Routledge.
- Re, D. (2018). International Crimes: A Hybrid Future?. Nigerian Yearbook of International Law 2017, 173-190.
- Reichborn-Kjennerud, E., & Cullen, P. (2022). What is hybrid warfare?. Norwegian Institute for International Affairs (NUPI)
- Rekotov, P., Nikitenko, V., Korshykova, T., Zherebko, O., & Samoilenko, I. (2022). Protection of the rights and legitimate interests of the individual in a hybrid war. Cuestiones Políticas, 40(73).
- Remus, T. (2013). Cyber-attacks and international law of armed conflicts; a jus ad bellum perspective. J. Int't Com. L. & Tech., 8, 179.
- Schmitt, M. (2012). Classification of cyber conflict. Journal of Conflict and Security Law, 17(2), 245-260.
- Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 37, 885-937.
- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- Schmitt, M., & Biller, J. (2019). Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare.

- Schulze, S. H. (2015). Cyber-" War"-Testfall der Staatenverantwortlichkeit (Vol. 107). Mohr Siebeck.
- Shaw, M. (2010). International Law (6th ed.). Cambridge: Cambridge University Press.
- Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyber-Attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent. Military Law Review, 201, 1-85.
- Smith, Michael. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- Smith, W. (2015). “Our Defense is a Holy Defense!”-The Iran-Iraq War and its Legacy in Contemporary Iranian Factional Politics. Journal of Georgetown University-Qatar Middle Eastern Studies Student Association, 2015(1), 3.
- Sokolov, S., Nyrkov, A., Knysh, T., & Demakov, Y. (2020, September). Cybernetic attacks as a component of information operations during the hybrid warfare. In International Scientific Conference on Architecture and Construction (pp. 67-83). Singapore: Springer Nature Singapore.
- Thiele, R. D. (2015). Crisis in Ukraine–the emergence of hybrid warfare. ISPSW Strategy Series: Focus on Defense and International Security, 347, 1-13.
- Torbat, A. E. (2005). Impacts of the US trade and financial sanctions on Iran. World Economy, 28(3),
- 407-434.
- Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats.
- UN-Human Rights (Office of the High Commissioner). (2016). International Legal Protection of Human Rights in Armed Conflict. United Nations Publication.
- Upeniece, V. (2019). Conditions for the legal commencement of an armed attack. In SHS Web of Conferences (Vol. 68, p. 01022). EDP Sciences.
- van der Wilt, H. (2021). Towards a Better Understanding of the Concept of ‘Indiscriminate Attack’—How International Criminal Law Can Be of Assistance. Yearbook of International Humanitarian Law, Volume 22 (2019), 29-42.
- Vasilovsky, A. (2002). The changing face of war. Journal of Conflict Studies, 23(1)
- Villaruel, A. J. R. (2007). Kombattantbegrepet: Taliban-og Al Qaeda-inns
- Watney, M. (2022).Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective. In European conference on cyber warfare and security (Vol. 21, No. 1, pp. 319-327).
- Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015, October). A theory of cyber attacks: A step towards analyzing MTD systems. In Proceedings of the second ACM workshop on moving target defense (pp. 11-20).

سال هفدهم، شماره دوم (پیاپی ۶۶)، تابستان ۱۴۰۴، صص. ۱۵۹-۱۹۰
تاریخ دریافت: ۱۴۰۳/۱۱/۰۹ ـ تاریخ پذیرش: ۱۴۰۴/۰۴/۱۸