



State Responsibility in the Era of Information Warfare

Seyed Asghar Jafari¹

1. Associate prof, International Relations and Law Department, Malek Ashtar University of Technology, Tehran, Iran. jafari1647@yahoo.com

Abstract

In recent years, information warfare has become one of the most important tools for states to demonstrate power at the international level. This type of warfare includes cyberattacks, psychological operations, and the dissemination of false information, aiming to disrupt critical infrastructures, destabilize political systems, and influence public opinion. This phenomenon poses significant challenges for international law, including the difficulty of attributing information operations to states, ambiguity in identifying violations of international obligations, weak enforcement mechanisms, and the increasing role of non-state actors. The present study, aiming to clarify the international responsibility of states in the era of information warfare, seeks to answer the central question: What responsibilities do states have in the age of information warfare? Methodologically, the research is applied in purpose, qualitative in nature, and follows a descriptive-analytical approach for data collection and analysis. The findings show that states' responsibility in the realm of information warfare is based on three key principles: first, refraining from any unlawful information interference in the internal affairs of other states; second, adopting preventive measures and engaging in effective cooperation to prevent cyberattacks originating from their territory; and third, in case of violations of international law, the obligation of the offending state to immediately cease the wrongful act and compensate for the damages caused.

Keywords: Information Warfare, State Responsibility, International Law, Cyber attacks, International Security

Volume info

Vol. 3
Series: 9
Spring 2026
P.P: 95-124

Article Type

Research Paper

Article History

Received:
02 November 2025
Revised:
14 July 2026
Accepted:
16 July 2026

ISSN – E-ISSN

ISSN: 3092-6459
E-ISSN: 3092-6424



Cite this article: Jafari, S.A. (2026). State Responsibility in the Era of Information Warfare. Cognitive Research in Political Studies, 3(2),95-124. [10.20241403/CRPS.2511.1097.2.9.4](https://doi.org/10.20241403/CRPS.2511.1097.2.9.4)

Publisher: Political Deputy of
the Ideological-Political
Organization

© The Author(s).



مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی

سیداصغر جعفری^۱

۱. دانشیار، گروه حقوق و روابط بین‌الملل، دانشگاه صنعتی مالک اشتر، تهران، ایران. jafari1647@yahoo.com

چکیده

در سال‌های اخیر، جنگ اطلاعاتی به یکی از ابزارهای مهم دولت‌ها برای نشان دادن قدرت در سطح بین‌المللی تبدیل شده است. این نوع جنگ شامل حملات سایبری، عملیات روانی و انتشار اخبار نادرست است که هدف آن مختل کردن زیرساخت‌های حیاتی، بی‌ثبات‌سازی سیاسی و تأثیرگذاری بر افکار عمومی است. این پدیده برای حقوق بین‌الملل مشکلات زیادی به همراه داشته است؛ از جمله دشواری در انتساب اقدامات اطلاعاتی به دولت‌ها، ابهام در شناسایی نقض تعهدات بین‌المللی، ضعف ضمانت اجراها و نقش فزاینده بازیگران غیردولتی. پژوهش حاضر با هدف، تبیین مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی، به این پرسش اصلی پاسخ خواهد داد که دولت‌ها در عصر جنگ اطلاعات دارای چه مسئولیتی هستند؟ از نظر روش‌شناسی، این تحقیق از نظر هدف کاربردی، از نظر ماهیت کیفی و از نظر جمع‌آوری و تحلیل داده‌ها، رویکردی توصیفی-تحلیلی دارد. یافته‌ها نشان می‌دهد که مسئولیت دولت‌ها در عرصه جنگ اطلاعاتی بر سه اصل کلیدی استوار است: نخست، پرهیز از هرگونه مداخله غیرقانونی اطلاعاتی در امور داخلی سایر کشورها؛ دوم، اتخاذ اقدامات پیشگیرانه و همکاری مؤثر برای جلوگیری از حملات سایبری که از قلمرو آن‌ها آغاز می‌شود؛ و سوم، در صورت نقض حقوق بین‌الملل، تعهد دولت متخلف به توقف فوری اقدام خلاف و جبران خسارت‌های واردشده.

کلیدواژه‌ها: جنگ اطلاعاتی، مسئولیت بین‌المللی دولت‌ها، حقوق بین‌الملل، حملات سایبری، امنیت بین‌المللی.

استناد: جعفری، سیداصغر. (۱۴۰۵). مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی. شناخت پژوهی مطالعات

سیاسی، ۳(۲)، ۹۵-۱۲۴. [10.2024/1403/CRPS.2511.1097.2.9.4](https://doi.org/10.2024/1403/CRPS.2511.1097.2.9.4)

ناشر: معاونت سیاسی سازمان
عقیدتی - سیاسی ودجا
نویسندگان.



سال و شماره

سال ۳، پیاپی: ۹
تأسیسات ۱۴۰۵
صص: ۹۵-۱۲۴

نوع مقاله

مقاله پژوهشی

سابقه مقاله

تاریخ دریافت: ۱۴۰۴/۰۸/۱۱
تاریخ بازنگری: ۱۴۰۵/۰۴/۲۳
تاریخ پذیرش: ۱۴۰۵/۰۵/۲۵

شاپا چاپی و الکترونیکی

شاپا چاپی: 3092-6459
الکترونیکی: 3092-6424



مقدمه

چنان‌که تاریخ حیات نشان می‌دهد، جنگ و درگیری همواره جزئی ثابت از زندگی انسان بوده و هیچ دوره‌ای را نمی‌توان یافت که خالی از خشونت و نبرد باشد. به همان اندازه که نبردها شکل گرفته‌اند، ساخت و گسترش سلاح نیز پدید آمده است. با پیشرفت علم و فناوری و انقلاب اطلاعات^۱ و پیدایش رایانه، ابزارهای نبرد و توانایی جنگ افروزی متحول شده و میدان‌های جنگ چند بعدی گردید. به عبارتی ماهیت جنگ دستخوش تحول اساسی شده و از قالب تهدیدات فیزیکی و متعارف فاصله گرفته است. گرچه هنوز جنگ سنتی از جوامع امروزی حذف نشده، اما جنگ بیشتر در قالب تهدیدهای اجتماعی و فکری از طریق رسانه‌ها و فناوری‌های نوین دیده می‌شود. این شکل نوین از جنگ، هرچند بخشی از ویژگی‌های جنگ‌های پیشین را در بردارد، اما به لحاظ گستره و میزان تأثیرگذاری، تهدیدی بسیار عمیق‌تر و گسترده‌تر از نمونه‌های گذشته به شمار می‌آید. به دیگر سخن، در سال‌های اخیر، مفهوم جنگ از حالت سنتی، یعنی وجود برخورد مسلحانه، تغییر یافته و دیگر مثل گذشته فقط در میدان نبرد و با ابزارهای فیزیکی نیست، بلکه گستره و تأثیر عمیق‌تری دارد و مفاهیم دیگری بر آن مترتب شد. یکی از این مفاهیم جنگ اطلاعاتی است.

در دنیای امروز، اطلاعات به ابزاری مهم برای رسیدن به اهداف سیاسی و نظامی تبدیل شده است و به‌کارگیری آن به‌عنوان سلاح، تهدیدی جدی برای امنیت ملی کشورها به شمار می‌آید. جنگ اطلاعاتی شکل‌های مختلفی دارد؛ مانند انتشار اخبار جعلی، حملات سایبری، تبلیغات، عملیات روانی و دست‌کاری رسانه‌ها. در این زمینه نه تنها دولت‌ها، بلکه گروه‌های غیردولتی و حتی بخش خصوصی نیز می‌توانند نقش داشته باشند. چنین روندی مرز میان جنگ و صلح را مبهم کرده و دولت‌ها را با چالش‌های تازه‌ای در زمینه امنیت و حقوق بین‌الملل روبه‌رو ساخته است.

مسئولیت بین‌المللی دولت‌ها یکی از اصول بنیادین حقوق بین‌الملل است که دولت‌ها را در برابر اعمال خود پاسخگو می‌سازد. مطابق با پیش‌نویس مواد کمیسیون حقوق بین‌الملل (ILC, 2001)، هرگاه یک دولت مرتکب عمل متخلفانه بین‌المللی شود، مسئولیت آن محقق می‌شود. این مسئولیت شامل دو شرط اساسی است: نخست، انتساب عمل به دولت؛ و دوم، نقض یک تعهد بین‌المللی. در عصر جنگ اطلاعاتی، تحقق این شروط با پیچیدگی‌های فراوان مواجه است، زیرا بسیاری از

^۱ Information Revolution

اقدامات اطلاعاتی به صورت پنهان، غیرمستقیم و با مشارکت بازیگران غیردولتی انجام می‌شود. یکی از مهم‌ترین چالش‌ها در این حوزه، انتساب اقدامات اطلاعاتی به دولت‌ها است. حملات سایبری می‌توانند از طریق شبکه‌های پیچیده، سرورهای واسطه و گروه‌های هکری غیردولتی انجام شوند و تعیین نقش مستقیم دولت‌ها در این اقدامات دشوار است (Schmitt, 2017: 99). دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه علیه ایالات متحده معیار «کنترل مؤثر» را برای انتساب اعمال گروه‌های غیردولتی به دولت‌ها مطرح کرده است (ICJ, 1986). با این حال، در حوزه جنگ اطلاعاتی، اثبات چنین کنترل یا هدایت مستقیم عملی پیچیده است و اغلب دولت‌ها از این خلأ بهره‌برداری می‌کنند. چالش دیگر مربوط به ابهام در شناسایی نقض تعهدات بین‌المللی است. اصولی همچون حاکمیت دولت‌ها، عدم مداخله در امور داخلی و منع استفاده از زور، از ستون‌های حقوق بین‌الملل به شمار می‌آیند (UN Charter, 1945: Article 2)؛ اما هنوز اختلاف نظرهای فراوانی درباره این وجود دارد که آیا انتشار اخبار جعلی، عملیات روانی یا حملات سایبری می‌توانند نقض این اصول محسوب شوند یا خیر (Schmitt, 2017: 17-20). این ابهام‌ها، پاسخگویی بین‌المللی دولت‌ها را با محدودیت مواجه ساخته و خطر سوءاستفاده را افزایش می‌دهد. علاوه بر این، رشد فزاینده بازیگران غیردولتی از جمله گروه‌های هکری و شرکت‌های فناوری است که بسیاری از عملیات اطلاعاتی توسط این بازیگران اجرا می‌شوند (Deibert, 2013) و در این راستا دولت‌ها به صورت غیرمستقیم در آن دخیل هستند و یا از آن سود می‌برند. این شرایط موجب شده است که چارچوب‌های سنتی حقوق بین‌الملل نتوانند پاسخگویی مؤثر در برابر جنگ اطلاعاتی را تضمین کنند. با توجه به این چالش‌ها، بررسی مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی از اهمیت حیاتی برخوردار است. چراکه، با وجود رشد اعمال جنگ اطلاعاتی توسط دولت‌ها و بازیگران غیردولتی، حقوق بین‌الملل هنوز در بسیاری از موارد فاقد قواعد کاملاً شفاف و اجرایی برای تعیین مسئولیت بین‌المللی در برابر این نوع تهاجم‌ها است.

پژوهش حاضر، با هدف ارائه تصویری جامع از وضعیت مسئولیت بین‌المللی دولت‌ها در مواجهه با تهدیدات نوین اطلاعاتی و پیشنهاد راهکارهای عملی برای تقویت نظم حقوقی بین‌المللی؛ به این پرسش پاسخ خواهد داد که دولت‌ها در عصر جنگ اطلاعات دارای چه مسئولیتی هستند؟

۱- پیشینه پژوهش

تاکنون پژوهشی با این عنوان انجام نشده است، اما به‌طور جداگانه پژوهش‌هایی در باره واژه‌های بکار برده در موضوع تحقیق انجام یافته که برخی از آن‌ها به شرح زیر آمده است. رشیدزاده (۱۳۸۵)، در مقاله‌ی عصر اطلاعات و جنگ اطلاعاتی به تبیین جنگ اطلاعاتی در عصر اطلاعات به‌عنوان فنی‌ترین شکل جنگ دفاعی پرداخته و اشاره کرد که با بهره‌گیری حرفه‌ای از تجهیزات اطلاعاتی و ارتباطی نوین می‌توان ارتش‌های بزرگ را از پای درآورد. مرادپیری و خضرای (۱۳۹۹)، نقش فناوری‌های نوین اطلاعاتی در جنگ‌های آینده با رویکرد کاربردی، داده‌ها را با اتکاء بر موضوعات نظری و مطالعات تطبیقی، تحلیل نموده و با تبیین نقش فناوری‌های نوین اطلاعاتی در جنگ‌های آینده نشان داده که فناوری‌های نوین به‌صورت یک سلاح جدید موجب شده با اصلاح دکترین، سازمان و استراتژی نظامی، جنگ‌های آینده را دچار تحولات جدی نماید.

ضیایی و خلیل زاده (۱۳۹۲)، در مقاله‌ای با عنوان مسئولیت بین‌المللی دولت ناشی از حملات سایبری بیان کردند حملات سایبری به‌عنوان یکی از جلوه‌های نوین مداخلات سایبری مورد شناسایی قرار گرفته است. حملات سایبری اگر مصداقی از تجاوز یا توسل به زور محسوب نشوند می‌تواند به‌عنوان مداخله در امور داخلی دولت یک تخلف بین‌المللی تلقی شود. در صورت انتساب این تخلف بین‌المللی به دولت طرح مسئولیت بین‌المللی دولت امکان‌پذیر خواهد بود. در این صورت امکان جبران خسارت به روش‌های مختلف اعم از توقف عمل متخلفانه، پرداخت غرامت و جلب رضایت وجود خواهد داشت.

طلائی (۱۴۰۴) در مقاله‌ای با عنوان هوش مصنوعی و جنگ‌های سایبری: ابعاد حقوقی مسئولیت دولت‌ها در حقوق بین‌الملل بیان کرده است با گسترش سریع فناوری‌های نوین و بهره‌گیری از سامانه‌های هوشمند در حملات سایبری، مسئولیت دولت‌ها را از حیث انتساب عمل، منع توسل به زور و اصل عدم مداخله در قبال اقدامات صورت گرفته در فضای مجازی با پرسش‌های جدیدی مواجه کرده است. این مقاله با هدف تحلیل ابعاد حقوقی جنگ‌های سایبری متکی بر هوش مصنوعی، ضمن بررسی چارچوب‌های موجود در حقوق بین‌الملل عمومی و حقوق مخاصمات مسلحانه، به چالش‌های مرتبط با مسئولیت بین‌المللی دولت‌ها می‌پردازد.

ترابی و احمدی (۱۴۰۴)، در مقاله‌ای با عنوان تاب‌آوری شناختی در برابر جنگ شناختی علیه ایران: مؤلفه‌ها، تحلیل و راهکارهای ارتقای بیان کردند جنگ شناختی یکی از ابعاد نوظهور و پیچیده‌ی جنگ‌های نوین است که با بهره‌گیری از فناوری‌های دیجیتال، شبکه‌های اجتماعی و عملیات روانی، ذهن و ادراک افراد را هدف قرار می‌دهد. در سال‌های اخیر، جمهوری اسلامی ایران به‌طور گسترده در معرض این نوع جنگ قرار گرفته است؛ به‌ویژه در رخدادهایی نظیر اغتشاشات پاییز ۱۴۰۱ که طی آن، دشمن با تولید و انتشار محتوای هدفمند، بمباران اطلاعاتی و القای توهم اکثریت، تلاش کرد تا انسجام ذهنی جامعه را دچار اختلال کند. یافته‌ها نشان می‌دهد که ضعف در آموزش سواد رسانه‌ای، نبود پلتفرم‌های بومی و خلأ در نهادهای سازنده‌ی جهاد تبیین، از مهم‌ترین چالش‌های تاب‌آوری شناختی در ایران هستند.

بررسی پیشینه نشان می‌دهد که هر یک از مطالعات پیشین تنها بر بخشی از موضوع تمرکز داشته‌اند؛ برخی بر ابعاد فناورانه جنگ اطلاعاتی، برخی بر حملات سایبری و مسئولیت حقوقی دولت‌ها و برخی دیگر بر جنگ شناختی علیه ایران. مزیت پژوهش حاضر در جامع‌نگری و نگاه تلفیقی آن نهفته است. برخلاف مطالعات گذشته که به‌صورت بخشی یا موضوعی محدود پرداخته‌اند، این پژوهش تلاش دارد «مسئولیت بین‌المللی دولت‌ها» را در کل طیف جنگ اطلاعاتی شامل حملات سایبری، عملیات روانی و استفاده از فناوری‌های نوین بررسی کند. همچنین، این پژوهش به چالش‌های عملی نظیر دشواری انتساب اقدامات، ضعف ضمانت اجراها و نقش بازیگران غیردولتی می‌پردازد؛ موضوعاتی که در منابع فارسی کمتر به شکل نظام‌مند مطرح شده‌اند. بدین ترتیب، این پژوهش گامی نو در پر کردن خلأ موجود و ارائه چارچوبی منسجم برای تقویت پاسخگویی بین‌المللی محسوب می‌شود.

۲- ادبیات مفهومی

۲-۱- جنگ

جنگ به‌طور سنتی معمولاً به درگیری بین دو یا چند کشور گفته می‌شود که در آن ارتش‌ها با هم وارد خشونت و نبرد می‌شوند. در واقع، جنگ یک رویارویی مسلحانه و ادامه‌دار میان دو طرف است (Mosaffa & et al., 1986: 1). به بیان دیگر، جنگ درواقع درگیری بین دولت‌هاست. این

درگیری ممکن است رسمی باشد، یعنی یک دولت رسماً به دولت دیگر اعلان جنگ بدهد، یا غیررسمی، یعنی بدون اعلان رسمی اما با استفاده گسترده از نیروهای نظامی آغاز شود (Dinstein, 2004: 15). آنچه در این تعریف ذکر شد مفهوم سنتی از جنگ یعنی وجود برخورد مسلحانه است؛ اما در عصر حاضر دیگر این مفهوم تغییر یافته و مفاهیم دیگری بر آن مترتب شد که از جمله آن جنگ شناختی، جنگ اطلاعاتی و امثالهم است.

۲-۲- جنگ شناختی

اولین کنفرانس علمی در زمینه جنگ‌های شناختی که با حمایت ناتو و توسط هاب نوآوری در سال ۲۰۲۱ برگزار شد، در باره جنگ شناختی آمده است: جنگ شناختی^۱، نوعی جنگ غیرمعارف است که با استفاده از ابزارهای سایبری، فرآیندهای شناختی دشمن را تغییر می‌دهد، سوگیری‌های ذهنی یا تفکر واکنشی او را بهره‌برداری می‌کند، باعث تحریف افکار، تحت تأثیر قرار دادن تصمیم‌گیری و مختل کردن اقدامات می‌شود که اثرات منفی، هم در سطح فردی و هم در سطح جمعی دارد. این جنگ به‌طور طبیعی با مفهوم جنگ سایبری مرتبط است که از ابزارهای دیجیتال برای کنترل، تغییر یا نابودی اطلاعات استفاده می‌کند؛ اما جنگ شناختی فراتر از اطلاعات می‌رود و بر نحوه واکنش مغز انسان نسبت به اطلاعات تمرکز دارد؛ بنابراین اثر شناختی، محصول جانبی نیست، بلکه هدف اصلی است. اگرچه ابزارهای فناوری وسیله‌ای برای رسیدن به این اثر هستند، هدف جنگ شناختی مستقل از فناوری‌های مورد استفاده است. می‌توان آن را از یک سو «جنگ روانی-اجتماعی-فنی» و از سوی دیگر به‌عنوان نوعی «جنگ نفوذ» با استفاده از ابزارهای سایبری دانست. در زمینه نظامی، این شامل استفاده از استراتژی‌هایی است که هدف‌شان انجام عملیات رزمی، شناسایی و یا امنیتی است (Claverie and du Cluzel, 2023)؛ به عبارت دیگر، جنگ شناختی به معنای هدف قرار دادن قوه شناخت و اثرگذاری بر نگرش‌ها، باورها، عقاید، اهداف و ارزش‌های جامعه هدف از طریق مدیریت ادراک به‌منظور ایجاد تغییر در مخاطبان تا مرز همسو شدن آن‌ها با اهداف تعریف شده و دستیابی به منافع مورد نظر است. در جنگ شناختی به‌جای اینکه مخاطب با تهییج احساسات و عواطف، به یک باره و فوری وادار به واکنش شود، در فرایندی مدیریت شده قرار می‌گیرد تا نگرش وی نسبت به مسائل اساسی نظیر اعتقادات و باورها، خانواده، مناسبات

¹ Cognitive warfare

اجتماعی و سیاسی، الگوی رفتاری، شیوه زندگی و ایده حاکمیت به صورت کاملاً نامحسوس و خزنده تحت تأثیر قرار گیرد (Nikoonahad & Biyouk, 2024: 17-18). تفاوت اصلی میان جنگ اطلاعاتی و جنگ شناختی در این است که جنگ اطلاعاتی، اطلاعات را هدف قرار می‌دهد (کنترل و دستکاری اطلاعات) و جنگ شناختی ذهن و رفتار انسان‌ها را هدف می‌گیرد (کنترل و تأثیرگذاری بر ذهن و رفتار انسان‌ها نسبت به اطلاعات).

۲-۳- جنگ اطلاعاتی

جنگ اطلاعاتی^۱ مفهومی است که در ادبیات روابط بین‌الملل و مطالعات امنیتی از دهه ۱۹۹۰ میلادی به‌طور گسترده مطرح شد. این اصطلاح به مجموعه‌ای از اقدامات هماهنگ و هدفمند برای دستکاری، تخریب یا بهره‌برداری از جریان اطلاعات با هدف تأثیرگذاری بر تصمیم‌گیری، امنیت ملی یا افکار عمومی یک دولت یا جامعه اشاره دارد (Libicki, 2007:16). به عبارت دیگر، «جنگ اطلاعاتی جنگ در فضای اطلاعات با هدف آسیب‌زدن به سامانه‌ها، فرآیندها، منابع اطلاعاتی و ساختارهای حیاتی کشور هدف تعریف می‌شود. هدف این جنگ برخلاف گذشته که عمدتاً پیروزی نظامی در جنگ کلاسیک بود، اثرگذاری بر نظام‌های سیاسی، اقتصادی، فرهنگی و اجتماعی، ایجاد کمپین‌های روانی گسترده جهت تضعیف ثبات جامعه و فشار بر یک دولت به گونه‌ای است که مطابق با منافع عاملان جنگ اطلاعاتی تصمیم‌گیری و عمل کند» (Torabi & Taherizadeh, 2021: 47).

در تعریفی دیگر آمده است: جنگ اطلاعاتی استفاده راهبردی از فناوری‌های اطلاعات و ارتباطات (ICT) برای دستیابی به نتایج مطلوب است. این فرایند شامل گردآوری، تحلیل، انتشار و دست‌کاری اطلاعات به‌منظور شکل‌دهی به دیدگاه‌ها، برداشت‌ها و تصمیم‌های افراد، سازمان‌ها یا دولت‌ها است. جنگ اطلاعاتی می‌تواند اشکال گوناگونی از جمله کمپین‌های انتشار اطلاعات نادرست، حملات سایبری، تبلیغات، عملیات روانی و دست‌کاری رسانه‌ای به خود بگیرد. دامنه کاربردهای آن گسترده است؛ از کسب برتری سیاسی گرفته تا بی‌ثبات کردن دشمن یا حفاظت از منافع خود (Jatmiko, 2023: 134). در این چارچوب، جنگ اطلاعاتی هم‌زمان شامل «عملیات

^۱ Information Warfare

تهاجمی» همچون حملات سایبری و انتشار اخبار جعلی و «عملیات تدافعی» مانند حفاظت از زیرساخت‌های اطلاعاتی و امنیت سایبری است. نکته قابل توجه آنکه جنگ اطلاعاتی فراتر از جنگ سایبری است؛ زیرا شامل ابعاد روانی، فرهنگی، سیاسی و اجتماعی نیز می‌شود.

۲-۴- تمایز جنگ اطلاعاتی و جنگ سایبری

هرچند دو مفهوم جنگ اطلاعاتی و جنگ سایبری ارتباط نزدیکی دارند، اما تمایزهایی نیز میان آن‌ها وجود دارد. جنگ سایبری^۱ بیشتر به حملات فنی علیه زیرساخت‌های دیجیتال نظیر شبکه‌های برق، سیستم‌های بانکی یا پایگاه‌های داده اشاره دارد (Rid, 2012). نمونه‌های شاخص آن ویروس استاکس‌نت علیه سانتریفیوژهای ایران و حملات نات‌پتیا علیه اوکراین بوده است. ویروس استاکس‌نت، توسط ایالات متحده و رژیم صهیونیستی، در سال ۲۰۱۰ سانتریفیوژهای تأسیسات هسته‌ای نطنز ایران را هدف قرار داد. این عملیات با هدف تخریب فیزیکی تجهیزات حیاتی و بدون درگیری مستقیم نظامی انجام شد. بر اساس معیارهای «تالین منوال^۲»، استاکس‌نت به دلیل ایجاد خسارت فیزیکی معادل با حمله نظامی و مصداق «استفاده از زور» تلقی می‌شود (Schmitt, 2017: 342). در سال ۲۰۱۷، بدافزار نات‌پتیا^۳، شبکه‌های اوکراین و چندین شرکت بین‌المللی را مختل کرد. این حمله باعث خسارت مالی میلیاردی شد، اما تلفات انسانی مستقیم نداشت. از نظر حقوقی، نات‌پتیا به‌عنوان «تخریب اقتصادی گسترده» ارزیابی شده و در محدوده «نقض اصل عدم مداخله» قرار می‌گیرد، هرچند هنوز سطح استفاده از زور را احراز نمی‌کند (Schmitte & Biller, 2017). در مقابل، جنگ اطلاعاتی دامنه وسیع‌تری دارد و علاوه بر حملات سایبری، شامل عملیات روانی، تبلیغات، کنترل رسانه‌ها، دستکاری افکار عمومی و استفاده از ابزارهای فرهنگی برای تغییر درک و رفتار جوامع است. به بیان دیگر، جنگ سایبری بخشی از جنگ اطلاعاتی محسوب می‌شود؛ اما جنگ اطلاعاتی حوزه‌ای چندبعدی‌تر است که ابعاد نرم و شناختی را نیز در برمی‌گیرد. این تمایز برای تحلیل مسئولیت بین‌المللی دولت‌ها اهمیت ویژه‌ای دارد، زیرا تعیین مرزهای حقوقی پاسخ به اقدامات سایبری نسبتاً ساده‌تر از پاسخ به اقدامات روانی یا تبلیغاتی است.

^۱ Cyber Warfare

^۲ Tallinn Manual

^۳ NotPetya

۵-۲- اشکال و ابزارهای جنگ اطلاعاتی

جنگ اطلاعاتی اشکال گوناگونی دارد که می‌توان آن‌ها را در سه دسته کلی طبقه‌بندی کرد:

۱. عملیات سایبری^۱: شامل هک، بدافزارها، حملات DDoS و نفوذ به شبکه‌های حیاتی که می‌تواند خسارت‌های اقتصادی و امنیتی گسترده به بار آورد (Shackelford, 2010)؛ به عبارت دیگر، عملیات سایبری به معنای ارسال کدهای رایانه‌ای از یک یا چند سیستم به یک رایانه هدف است. این کار می‌تواند برای نفوذ به سامانه و انجام اقداماتی مانند جمع‌آوری، استخراج، حذف یا رمزگذاری داده‌ها انجام شود. همچنین از عملیات سایبری می‌توان برای تغییر یا دستکاری فرآیندهایی که آن سامانه کنترل می‌کند استفاده کرد (Mousazadeh & Azarpandar, 2024: 191).

۲. عملیات روانی و تبلیغاتی^۲: انتشار اخبار جعلی^۳، دستکاری تصاویر و ویدئوها و بهره‌گیری از رسانه‌های اجتماعی برای تأثیرگذاری بر افکار عمومی و برهم زدن انسجام اجتماعی (Benkler et al., 2018). به دیگر سخن، تبلیغات یعنی تلاشی هدفمند برای اثر گذاشتن بر افکار و رفتار دیگران از طریق ابزارهای ارتباطی، به گونه‌ای که واکنش آن‌ها با خواست و منافع تبلیغ‌کننده هماهنگ شود (Kaviani, 2001: 111)؛ و عملیات روانی یعنی استفاده سازمان‌یافته از تبلیغات، چه به صورت آشکار از راه رسانه‌هایی مثل رادیو، تلویزیون، مطبوعات، اینترنت و شبکه‌های اجتماعی و چه به صورت پنهان از طریق شایعه، جاسوسی یا ترور. هدف از این عملیات تغییر یا تحریف باورها، تضعیف روحیه مردم یا نیروهای دشمن، بی‌اعتبار کردن انگیزه‌ها و کاهش قدرت حکومت مخالف است (Moradi, et al., 2016).

۳. عملیات اطلاعاتی^۴: شامل ایجاد اختلال در جریان ارتباطات دشمن، جاسوسی اطلاعاتی و سرقت داده‌های حساس (Nye, 2014). به بیان دیگر، عملیات اطلاعاتی مجموعه‌ای از اقدامات هماهنگ و برنامه‌ریزی‌شده است که با هدف تأثیرگذاری بر جریان اطلاعات و فرآیندهای تصمیم‌گیری دشمن انجام می‌شود و شامل فعالیت‌هایی چون جاسوسی، اختلال در ارتباطات، سرقت یا دستکاری داده‌ها است.

^۱ Cyber Operations

^۲ Psychological Operations

^۳ Fake News

^۴ Information Operations

در کنار این سه دسته، مفاهیم نوینی چون هوش مصنوعی^۱، دیپ‌فیک^۲ به عنوان یک فناوری قدرتمند در عصر نوظهور هوش مصنوعی (Fakheri, 2024: 260) و الگوریتم‌های تبلیغاتی نیز به سرعت به ابزارهای جدید جنگ اطلاعاتی تبدیل شده‌اند.

۶-۲- مسئولیت بین‌المللی دولت

حقوق بین‌الملل، مجموعه‌ای از حقوق و تعهدات میان بازیگران مختلف نظام بین‌الملل، شامل دولت‌ها، افراد و سازمان‌های بین‌المللی را تعیین می‌کند. دولت‌ها مسئولیت‌های گسترده‌ای بر عهده دارند و هرگونه تخلف یا قصور در انجام این وظایف، مسئولیت قانونی آن‌ها را به دنبال خواهد داشت. این حقوق و تعهدات، ضمن فراهم آوردن چارچوب عملیاتی برای دولت‌ها، محدوده مسئولیت‌های آنان را نیز مشخص می‌سازد. مسئولیت بین‌المللی به عنوان یکی از ارکان بنیادین نظام بین‌المللی، تضمین‌کننده رعایت قواعد و اصول حاکم بر روابط میان کشورها است و نقض آن می‌تواند امنیت و ثبات روابط بین‌المللی را تهدید نماید (Madani, 1998, 2: 77).

«مسئولیت بین‌المللی دولت^۳، عبارت از تکلیفی است که به موجب حقوق بین‌الملل به یک دولت تحمیل می‌گردد تا خساراتی را که در اثر نقض قواعد حقوق بین‌الملل [ناشی از عمل یا خودداری از آنان، در انجام تکلیف نسبت] به دولت دیگری وارد کرده است جبران نماید» (Fiyouzi, 2000: 25). به عبارت دیگر، «مسئولیت بین‌المللی یک نهاد حقوقی است که به موجب آن کشوری که عمل برخلاف حقوق (بین‌الملل) به او منتسب است، باید طبق حقوق بین‌الملل خسارت وارده به کشور متضرر از آن عمل را جبران نماید» (Ziaee Bigdeli, 1992: 260). «یعنی اینکه اگر دولتی با انجام عمل مخالف حقوق بین‌الملل و یا نقض و خودداری از انجام تکالیفی که به موجب قواعد بین‌المللی به عهده دارد، به دولت یا اتباع دولت دیگری خسارت مالی و یا روحی و یا جانی وارد آورد، مکلف است خسارات وارده را جبران کند» (Sharifi Taraz Kouhi, 1996: 3).

^۱ Artificial Intelligence

^۲ دیپ فیک یا جعل عمیق (Deep fake) فناوری هوش مصنوعی است که برای تولید محتوای رسانه‌ای دست‌کاری شده به کار می‌رود. این محتوا می‌تواند شامل فیلم، تصویر یا فایل صوتی باشد که در آن افراد به گونه‌ای نشان داده می‌شوند یا سخن می‌گویند که در واقعیت هرگز رخ نداده است (Chesney and Citron, 2019).

^۳ International Responsibility of the State

189). از این رو، می‌توان گفت که این امر به منزله‌ی اختیاری قانونی و صلاحیتی است که بر اساس قواعد حقوق بین‌الملل برای دولت‌ها پیش‌بینی و به رسمیت شناخته شده است.

۲-۷- اهمیت موضوع مسئولیت بین‌المللی دولت

از موضوعات بسیار مهم و اساسی در حوزه حقوق بین‌الملل که تشکیل دهنده سازوکارهای نظم عمومی به شمار می‌آید، موضوع مسئولیت دولت است (Brownlie, 2004: 99). چراکه مسئولیت، سازوکار تنظیم‌کننده اساس حقوق بین‌الملل است. مسئولیت، حاکمیت کشورها را محدود نمی‌کند، بلکه برعکس، نتیجه لازم و ضروری آن می‌باشد. در حقوق بین‌الملل راه‌های چندانی وجود ندارد که بتوان از طریق آن‌ها کشورها را به رعایت مقررات این حقوق وادار نمود، زیرا کشورها خود حاکم هستند؛ ولی حداقل کشورهای دیگر توقع دارند تا در صورت نقض مقررات حقوق بین‌الملل یک راه برای جبران خسارات وارده باز باشد و آن وجود مسئولیت است (Emadzadeh, 1991: 199)؛ بنابراین، مسئولیت بین‌المللی را می‌توان به عنوان ضمانت اجرای صلاحیت در حقوق بین‌الملل دانست. دیوان دائمی بین‌المللی دادگستری^۱ در رأی خود راجع به قضیه کارخانه کوروزف (۱۹۲۷) چنین اظهار نظر کرد: «این یک اصل حقوق بین‌الملل است که نقض یک تعهد متضمن تکلیف به جبران آن به نحو کافی می‌باشد. بنابراین جبران خسارت مکمل لازم قصور در اجرای یک عهدنامه به شمار می‌آید و نیازی به ذکر در آن در خود کنوانسیون نمی‌باشد» (PCIJ, 1927; Series, 21).

این بیان صریح در پذیرش مسئولیت دولت در قبال نقض یک تعهد در رویه قضایی بین‌المللی حکایت از اهمیت موضوع مسئولیت دولت دارد.

توجه به مسئولیت دولت و رعایت قواعد حقوق بین‌الملل، نه تنها به تقویت چارچوب‌های حقوقی بین‌المللی و ارتقای امنیت و ثبات در روابط میان کشورها و شهروندان آن‌ها کمک می‌کند، بلکه الزام دولت‌ها به جبران هرگونه اقدام غیرقانونی نیز به طور مستقیم بر رفتار آن‌ها تأثیرگذار است. این امر، ارتباط مستقیم احترام و حیثیت دولت‌ها در جامعه بین‌المللی با پایبندی به اصول و قواعد بین‌المللی را نشان می‌دهد.

^۱ Permanent Court of International Justice (P.C.I.J)

۸-۲- شرایط تحقق مسئولیت بین‌المللی دولت

در طرح کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت در قبال اعمال نادرست بین‌المللی آمده است:

ماده ۱: هر عمل نادرست بین‌المللی دولت موجب مسئولیت بین‌المللی آن دولت می‌گردد.
ماده ۲: عمل نادرست بین‌المللی یک دولت وقتی به وجود می‌آید که مبتنی بر فعل و یا ترک فعلی باشد که:

الف) قابل انتساب به دولت بر اساس حقوق بین‌الملل باشد؛
ب) موجب نقض تعهد بین‌المللی گردد (ILC, 2001, art. 1 & 2).
بر این مبنا می‌توان گفت: برای تحقق مسئولیت بین‌المللی دولت چهار شرط در حقوق بین‌الملل به این شرح مقرر است:

۱. نقض یک تعهد بین‌المللی و به تعبیر دیگر انجام یک عمل نامشروع؛
 ۲. تحقق ضرر و زیان؛
 ۳. وجود رابطه سببیت بین نقض تعهد و ضرر و زیان وارده؛
 ۴. قابلیت انتساب عمل زیان‌آور به یک ارگان مسئول دولتی (Madani, 1998, 3: 282)؛
- به بیان دیگر، پیش شرط اصلی مسئولیت دولت، ارتکاب یک عمل خلاف است. برای اینکه عمل خلافی صورت گیرد، لازم است عناصر عینی و ذهنی‌ای پدیدار شوند.
- عناصر ذهنی عبارت‌اند از:
- ۱) انتساب یک رفتار خاص (فعل یا ترک فعل) مغایر با تعهدات بین‌المللی به یک دولت؛ و ۲) در برخی موارد، تقصیر دولت در انجام یک عمل خلاف.
- عناصر عینی از این قرارند:
- الف) مغایرت یک رفتار خاص با تعهدات بین‌الملل؛ ب) وارد آمدن زیان مادی یا معنوی به یکی از تابعان بین‌المللی؛ ج) فقدان هرگونه شرایط رافع مسئولیت^۱ (Cassese, 2007: 348).

^۱ در طرح مسئولیت بین‌المللی دولت، ۷ شرط برای شرایط رافع مسئولیت اقدامات خلاف در نظر گرفته شده است که عبارتند از: رضایت دولت لطمه دیده، رعایت نرم‌های آمره، دفاع مشروع، اقدامات متقابل، فورس ماژور یا قوهی قاهره، اضطرار، حالت ضرورت.

۳- چهار چوب نظری

۳-۱- نظریه امنیت شناختی

در قرن بیست و یکم، مفهوم قدرت از حوزه‌های سنتی و فیزیکی به عرصه‌ای جدید و ناملموس منتقل شده است؛ عرصه‌ای که محور آن «ذهن انسان» است. امروزه توجه، ادراک، حافظه و تصمیم‌گیری افراد به هدف اصلی عملیات‌های نفوذ و تأثیرگذاری تبدیل شده‌اند. این تحول، مفهوم «امنیت شناختی»^۱ را به عنوان یکی از محورهای نوین مطالعات امنیتی مطرح کرده است.

با دگرگونی ماهیت تهدیدات امنیتی در عصر دیجیتال، نظریه‌های امنیت سایبری و امنیت شناختی به ابزارهای مهمی برای تحلیل مسئولیت دولت‌ها در مواجهه با جنگ اطلاعاتی تبدیل شده‌اند. در این چارچوب، تهدیدات دیگر محدود به حملات نظامی یا تروریستی نیستند، بلکه در قالب حملات سایبری، عملیات روانی، انتشار اطلاعات نادرست و دستکاری افکار عمومی نیز نمود پیدا می‌کنند. در این میان، امنیت سایبری بر حفاظت از زیرساخت‌ها و داده‌ها تمرکز دارد، در حالی که امنیت شناختی به صیانت از ادراک و رفتار جمعی می‌پردازد. بر این اساس، نظریه پردازان امنیت شناختی معتقدند که دولت‌ها نباید تنها به حفاظت فنی از زیرساخت‌ها بسنده کنند، بلکه لازم است به تقویت سواد رسانه‌ای، آموزش تفکر انتقادی و ایجاد سازوکارهای مؤثر برای اعتبارسنجی اطلاعات نیز توجه جدی داشته باشند (Sheikholeslami & Seddighi, 2025: 35-36).

پیدایش امنیت شناختی به طور مستقیم با تحولات انقلاب صنعتی چهارم، به ویژه گسترش هوش مصنوعی، یادگیری ماشین و فضای دیجیتال، مرتبط است. محیط اطلاعاتی جدید نه تنها حامل اطلاعات، بلکه شکل دهنده ادراک و قضاوت انسان‌هاست. در نتیجه، فرایندهای شناختی به عنوان زیرساختی حیاتی برای امنیت ملی و پایداری جوامع مطرح می‌شوند. در این میان، رویکردهای سنتی مانند امنیت سایبری و مقابله با اطلاعات نادرست، به تنهایی پاسخگوی تهدیدات جدید نیستند؛ زیرا این رویکردها بیشتر بر حفاظت از داده‌ها یا صحت محتوا تمرکز دارند، در حالی که تهدیدات نوین مستقیماً ذهن و ادراک انسان را هدف قرار می‌دهند. فناوری‌هایی مانند هوش مصنوعی مولد، دیپ‌فیک‌ها و الگوریتم‌های شبکه‌های اجتماعی، با ایجاد محتوای بسیار واقعی و تأثیرگذاری احساسی، می‌توانند اعتماد عمومی را تضعیف و تصمیم‌گیری‌ها را منحرف کنند. بر این اساس، نظریه

^۱ Cognitive Security

امنیت شناختی تأکید می‌کند که باید تمرکز از «حفاظت از اطلاعات» به «حفاظت از فرایندهای شناختی» تغییر یابد (Bıçakçı, 2025: 1-2). با افزایش بهره‌گیری مهاجمان از اطلاعات فریبده و دستکاری‌شده به منظور اختلال در فرایندهای شناختی انسان - از جمله ادراک، توجه، حافظه و پردازش‌های ذهنی - افراد به سمت استدلال‌های نادرست هدایت شده و تصمیماتی اتخاذ می‌کنند که تحت تأثیر دستکاری قرار دارد و در مواردی می‌تواند به اختلال یا حتی فروپاشی در سطح کلان سیستم‌ها منجر شود. در چنین شرایطی، امنیت شناختی با هدف حفاظت از انسان‌ها در برابر سوءاستفاده از آسیب‌پذیری‌های شناختی مطرح می‌شود و می‌کوشد زمینه تصمیم‌گیری آگاهانه، مستقل و مصون از نفوذ ناموجه را فراهم سازد. افزون بر این، امنیت شناختی در پی آن است که با کاهش اثرات اولیه این نوع حملات، از تشدید ریسک‌ها در مراحل بعدی زنجیره حمله مهاجم نیز جلوگیری کند (Huang & Zhu, 2023: 13). هدف این رویکرد، تقویت توانایی انسان‌ها در تفکر مستقل، قضاوت آگاهانه و مقاومت در برابر دستکاری است، نه صرفاً کنترل محتوا. در نهایت، تضعیف امنیت شناختی می‌تواند به بحران در اعتماد عمومی، کارآمدی حکمرانی و مشروعیت دموکراتیک منجر شود. از این‌رو، امنیت شناختی به یکی از ارکان اساسی تاب‌آوری ملی در عصر جنگ اطلاعاتی و هوش مصنوعی تبدیل شده است (Bıçakçı, 2025: 3).

نظریه امنیت شناختی بُعد جدیدی به مسئولیت بین‌المللی دولت‌ها می‌افزاید و نشان می‌دهد که در عصر جنگ اطلاعاتی، تعهدات دولت‌ها دیگر صرفاً ناظر بر قلمرو فیزیکی یا سایبری نیست، بلکه شامل حفاظت از فضای شناختی انسان‌ها نیز می‌شود. از این‌رو، دولت‌ها هم در مقام «فاعل» یعنی پرهیز از مداخله شناختی و هم در مقام «ضامن» یعنی پیشگیری و حمایت، دارای مسئولیت هستند و این امر ضرورت توسعه قواعد حقوق بین‌الملل متناسب با این تحولات را برجسته می‌سازد.

۴- روش‌شناسی پژوهش

این پژوهش با هدف بررسی مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی، از نظر هدف کاربردی، از نظر ماهیت کیفی و از نظر جمع‌آوری و تحلیل داده‌ها، رویکردی توصیفی-تحلیلی دارد.

در گام نخست، مطالعه کتابخانه‌ای و مستندات انجام شد. منابع مورد استفاده شامل اسناد حقوق بین‌الملل مانند منشور ملل متحد و پیش‌نویس مواد کمیسیون حقوق بین‌الملل، گزارش‌های نهادهای بین‌المللی، مقالات علمی، کتاب‌های تخصصی در حوزه جنگ اطلاعاتی و امنیت سایبری و مطالعات موردی معتبر بود. این مرور مستندات امکان شناسایی مبانی نظری، چارچوب‌های حقوقی و چالش‌های اصلی مسئولیت بین‌المللی دولت‌ها را فراهم کرد. در گام دوم، تحلیل تطبیقی و استخراج حقوقی انجام شد تا خلأها و چالش‌های موجود در حقوق بین‌الملل و مسئولیت دولت‌ها در عصر اطلاعات شناسایی شود. این تحلیل به تدوین پیشنهادهایی برای بهبود چارچوب‌های حقوقی، تقویت سازوکارهای پاسخگویی و افزایش شفافیت در مواجهه با جنگ اطلاعاتی منجر شد.

۵- یافته‌های پژوهش

۵-۱- معیارهای حقوقی مسئولیت و جنگ اطلاعاتی

مسئولیت بین‌المللی دولت‌ها یکی از اصول بنیادین حقوق بین‌الملل است که بر اساس آن، هر دولت موظف است در صورت ارتکاب یک عمل متخلفانه بین‌المللی پاسخگو باشد. کمیسیون حقوق بین‌الملل سازمان ملل متحد در سال ۲۰۰۱ «پیش‌نویس مواد مسئولیت دولت‌ها در قبال اعمال متخلفانه بین‌المللی» را تصویب کرد که به‌عنوان سند مرجع در این حوزه شناخته می‌شود (ILC, 2001). بر اساس این مواد، تحقق مسئولیت بین‌المللی نیازمند دو شرط اصلی است: ۱) انتساب عمل به دولت؛ ۲) نقض یک تعهد بین‌المللی. به بیان دیگر، اصل مسئولیت بین‌المللی دولت‌ها زمانی فعال می‌شود که یک عمل متخلفانه به یک دولت قابل انتساب باشد و آن عمل ناقض تعهدات بین‌المللی باشد. در حوزه جنگ اطلاعاتی، دو مؤلفه کلیدی مطرح است (Schmitt, 2017: 80 & 100):

۱. انتساب^۱: یعنی اثبات اینکه یک دولت مستقیماً یا از طریق عوامل وابسته اقدام به عملیات اطلاعاتی کرده است.
۲. نقض تعهد بین‌المللی^۲: مثلاً نقض اصل عدم مداخله و نقض حاکمیت دولت‌ها.

^۱ Attribution

^۲ Violation of international obligations

۱- معیار انتساب

انتساب یکی از دشوارترین مباحث در حوزه مسئولیت دولت‌ها در جنگ اطلاعاتی است. به دلیل ماهیت نامرئی و پیچیده عملیات اطلاعاتی، اثبات ارتباط میان اقدام و دولت بسیار دشوار است. این امر موجب می‌شود دولت‌ها اغلب از مسئولیت‌پذیری طفره برونند و جامعه بین‌المللی نیز ابزار کافی برای پاسخگو کردن آن‌ها نداشته باشد. به عنوان مثال، حملات سایبری می‌توانند از سوی گروه‌های غیردولتی انجام شوند، اما با حمایت، هدایت یا حتی چشم‌پوشی دولت‌ها صورت گیرند (Schmitt, 2017: 137). بر اساس پیش‌نویس مواد کمیسیون حقوق بین‌الملل، اعمال ارگان‌های رسمی دولت یا افرادی که تحت دستور، هدایت یا کنترل مؤثر دولت عمل می‌کنند، به دولت منتسب می‌شود (ILC, 2001, arts. 4-8).

طبق ماده ۸ پیش‌نویس کمیسیون حقوق بین‌الملل، اگر یک گروه غیردولتی تحت «دستور» یا «کنترل مؤثر»^۱ یک دولت عمل کند، اقداماتش به دولت منتسب خواهد بود. با این حال، تعیین سطح «کنترل مؤثر» در عملیات اطلاعاتی به دلیل ماهیت پنهان و پیچیده این اقدامات بسیار دشوار است. پرونده‌هایی مانند حملات سایبری به استونی (۲۰۰۷) یا اوکراین (۲۰۱۵) نشان داده‌اند که حتی در صورت وجود شواهد قوی فنی، اثبات کنترل مستقیم یک دولت به سادگی ممکن نیست (Schmitt, 2017: 376).

در زمینه عملیات اطلاعاتی، معیار «کنترل مؤثر» که دیوان بین‌المللی دادگستری (ICJ) در قضیه نیکاراگوئه علیه ایالات متحده (۱۹۸۶) مطرح کرد، اهمیت دارد. بر این اساس، برای انتساب عمل به دولت باید اثبات شود که دولت به طور مستقیم دستور انجام عملیات را داده یا کنترل مؤثر بر آن داشته است (ICJ, 1986)؛ اما در فضای جنگ اطلاعاتی، تعیین این سطح از کنترل اغلب دشوار است. به همین دلیل برخی نظریه‌پردازان معیار «کنترل کلی»^۲ را پیشنهاد کرده‌اند که انعطاف بیشتری در انتساب اعمال گروه‌های غیردولتی به دولت‌ها فراهم می‌کند (Cassese, 2007)، چنانکه به صراحت در رأی شعبه تجدیدنظر دیوان بین‌المللی کیفری برای یوگسلاوی سابق در پرونده تادیچ معیار «کنترل کلی» بیان شد (Tadić, Appeals Chamber judgment, paras, 131-140, 145).

^۱ Effective Control

^۲ Overall Control

۲- معیار نقض تعهدات

دومین عنصر در حوزه جنگ اطلاعاتی، نقض تعهدات است. به فرض اینکه انتساب ثابت شود، پرسش دیگر این است که کدام تعهدات بین‌المللی نقض شده‌اند. از این رو، عمل متخلفانه بین‌المللی در صورتی تحقق می‌یابد که تعهدی بین‌المللی نقض شود. در زمینه جنگ اطلاعاتی، تعهدات زیر بیشترین ارتباط را دارند:

الف) نقض اصل حاکمیت دولتها

حاکمیت یک مفهوم اساسی در حقوق بین‌الملل به معنی اختیار یا قدرت عالیه و تجزیه‌ناپذیر دولت جهت وضع و اعمال قوانین خود در خصوص کلیه اشخاص، اموال و وقایع داخل مرزهای آن است (Bledsoe & Boczek, 1987: 75). ورود غیرمجاز به شبکه‌های دیجیتال و حملات سایبری به زیرساخت‌های حیاتی یک دولت می‌تواند به‌عنوان نقض حاکمیت آن دولت تلقی شود (Schmitt, 2017: 17).

زیرساخت حیاتی عبارت است از سیستم‌ها و دارایی‌هایی، اعم از فیزیکی یا مجازی که تضعیف یا نابودی آن‌ها موجب اثرات منفی بر امنیت ملی، امنیت اقتصاد ملی، سلامت عمومی ملی یا ایمنی یا ترکیبی از این موارد شود (Rinaldi et al, 2001: 12). بی‌شک زیرساخت‌ها در هر کشوری بنیان اساسی جامعه آن کشور محسوب می‌شوند و آسیب به آن‌ها می‌تواند پیامدهای جبران‌ناپذیری را در کشورها ایجاد نماید و از آنجایی که زیرساخت‌ها به یکدیگر وابسته هستند و ارکان جامعه نیز به زیرساخت‌ها وابستگی دارند، آسیب در یک بخش می‌تواند بخش‌های دیگر را نیز تحت تأثیر جدی قرار دهد. زیرساخت به ساختار اولیه فیزیکی و سازمان‌یافته‌ای گفته می‌شود که برای اجرای مأموریت و اهداف یک سازمان یا یک جامعه مورد نیاز است و در حالت کلی به عناصر ساختاری مرتبط و به هم پیوسته‌ای گفته می‌شود که چارچوبی را برای توسعه کل ساختارهای دیگر فراهم می‌کند و می‌تواند به‌عنوان یکی از عناصر توسعه‌یافتگی یک کشور مطرح گردد. زیرساخت‌های حیاتی کشور، نه تنها شالوده‌های امنیت ملی، حکومت و حیات اقتصادی را پایه‌ریزی می‌کنند، بلکه تداوم استحکام، قدرت و قابلیت اعتماد آن‌ها همراه با حفظ حس اعتماد در مردم، بخشی از هویت ملی ما را تشکیل می‌دهد (Jafari, 2023: 16).

ب) نقض اصل عدم‌مداخله در امور داخلی

اقدامات اطلاعاتی مانند انتشار اخبار جعلی با هدف تأثیرگذاری بر انتخابات یک دولت انجام شود و یا بی‌ثبات‌سازی سیاسی، مداخله غیرقانونی تلقی می‌شود و منجر به نقض این اصل خواهد شد. منشور ملل متحد اصل برابری حاکمیت^۱ و عدم مداخله^۲ در امور داخلی دولت‌ها را به‌عنوان یکی از ستون‌های اصلی نظم بین‌المللی معرفی می‌کند (UN Charter, 1945: 2). اصل احترام به حاکمیت سرزمینی کشورها یک قاعده شناخته‌شده در حقوق بین‌الملل است. دیوان لاهه در دو پرونده لوتوس (۱۹۲۷) و تنگه کورفو (۱۹۴۹) این اصل را تأیید کرده است. طبق این اصل، هر کشور فقط خودش حق اعمال حاکمیت در سرزمینش را دارد و هیچ کشور دیگری نمی‌تواند در قلمرو آن دخالت کند (Namdar, 2019: 114).

هرگونه اقدامی که به‌طور مستقیم یا غیرمستقیم بر استقلال سیاسی یا تمامیت ارضی دولت دیگر تأثیر گذارد، می‌تواند نقض این اصل باشد. بر اساس اصل حاکمیت و تمامیت ارضی، دولت‌ها حق دارند در موضوعات داخلی خود آزادانه تصمیم‌گیری کنند و هیچ دولتی نباید در این امور دخالت کند. مداخله یعنی ورود یک کشور به امور داخلی کشور دیگر، چه با زور و نیروی نظامی برای وادار کردن آن کشور به کاری مانند تغییر حکومت، امضای معاهده یا واگذاری بخشی از سرزمین و چه با هر اقدام دیگری در داخل سرزمین آن کشور (Namdar, 2019: 116). در چارچوب جنگ اطلاعاتی، مداخله در انتخابات، تحریک افکار عمومی علیه دولت، یا ایجاد بی‌ثباتی سیاسی از طریق اطلاعات نادرست نمونه‌هایی از نقض اصل عدم مداخله هستند. در نتیجه، چنین اقداماتی در صورت انتساب به یک دولت می‌توانند موجب مسئولیت بین‌المللی شوند.

ج) نقض تعهدات ناشی از منشور ملل متحد

در صورتی که عملیات اطلاعاتی منجر به تهدید صلح و امنیت بین‌المللی شود، می‌تواند نقض بند ۴ ماده ۲ منشور تلقی شود (UN Charter, 1945). بند ۴ ماده ۲ منشور اشعار می‌دارد: «کلیه اعضاء در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مبادت داشته باشد خودداری خواهند نمود».

^۱ Principle of Sovereignty equality of states

^۲ Principle of Non-intervention

مسئله مهم در این باره این است که آیا عملیات اطلاعاتی می‌تواند مصداق استفاده از زور باشد؟ دیدگاه‌ها در این زمینه متفاوت است؛ برخی تنها خسارات فیزیکی را کافی می‌دانند (Dinstein, 2017)، در حالی که برخی دیگر آثار شدید اقتصادی و سیاسی را نیز در این دسته قرار می‌دهند (Schmitt, 2017: 337).

۲-۵- ضمانت اجراها و پیامدهای حقوقی

اگرچه اسناد بین‌المللی مانند منشور ملل متحد بر اصل عدم مداخله و احترام به حاکمیت دولت‌ها تأکید دارند، اما هنوز سند الزام‌آور مشخصی درباره جنگ اطلاعاتی وجود ندارد. «دستورالعمل تالین ۲»^۱ تلاشی غیرالزام‌آور برای تبیین قواعد حقوق بین‌الملل در حوزه عملیات سایبری بود (Schmitt, 2017: 1-3)، اما درباره ابعاد غیرسایبری جنگ اطلاعاتی همچنان خلأ جدی وجود دارد. از منظر اجرایی نیز، حتی در صورت شناسایی یک عملیات اطلاعاتی به عنوان اقدام متخلفانه، ابزارهای حقوقی و سیاسی برای اعمال مسئولیت بین‌المللی علیه دولت‌ها بسیار محدود است. این امر نشان‌دهنده نیاز به بازاندیشی در قواعد حقوق بین‌الملل و توسعه چارچوب‌های نوین برای پاسخگویی به تهدیدات اطلاعاتی است.

جنگ اطلاعاتی پدیده‌ای چندوجهی و پیچیده است که مرزهای سنتی جنگ و صلح را دگرگون کرده و دولت‌ها را با چالش‌های جدیدی در عرصه حقوق بین‌الملل مواجه ساخته است. فهم دقیق ابعاد مفهومی آن، تمایز میان جنگ اطلاعاتی و جنگ سایبری، شناسایی ابزارها و اشکال مختلف آن و بررسی چارچوب‌های مسئولیت بین‌المللی دولت‌ها برای تحلیل پیامدهای حقوقی و سیاسی این پدیده ضروری است. بدون توسعه قواعد حقوقی شفاف و سازوکارهای اجرایی کارآمد، خطر آن

^۱ دستورالعمل تالین که توسط مرکز همکاری ناتو در حوزه دفاع سایبری تدوین شده، یکی از مهم‌ترین منابع در زمینه حقوق بین‌الملل سایبری به شمار می‌رود. دستورالعمل تالین ۱ (۲۰۱۳) به بررسی قواعد حاکم بر جنگ سایبری می‌پردازد و بیشتر از دو حوزه حقوق توسل به زور و حقوق بشردوستانه تشکیل شده است. دستورالعمل تالین ۲ (۲۰۱۷)، بر خلاف نسخه نخست آن که تنها به عملیات سایبری در چارچوب درگیری‌های مسلحانه می‌پرداخت، دامنه گسترده‌تری دارد و عملیات سایبری خارج از این شرایط را نیز بررسی می‌کند. این دستورالعمل در قالب ۴ بخش و ۲۰ فصل، شامل ۱۵۴ قاعده کلی است که مهم‌ترین مباحث حقوق بین‌الملل مرتبط با عملیات سایبری را مطرح کرده و قواعد حاکم بر این‌گونه عملیات و حملات را در زمینه‌های مربوطه مورد تحلیل قرار می‌دهد (کرمی، ۱۴۰۲).

وجود دارد که دولت‌ها با سوء استفاده از مناطق خاکستری^۱ حقوقی برای اقدامات خصمانه بهره‌برداری کنند و نظم بین‌المللی بیش از پیش دچار بی‌ثباتی شود. در حقوق بین‌الملل نیز مانند حقوق داخلی هنگامی یک شخص تعهدی حقوقی را نقض می‌کند که رفتار آن با خواست تعهد مزبور منطبق نباشد؛ بنابراین زمانی نقض تعهد محرز می‌شود که شخص ملزم به اجرای تعهد بین‌المللی، رفتاری مغایر با آنچه اجرای تعهد لازم است در پیش گیرد (مستقیمی و طارم سری، ۱۳۷۷: ۸۱). این مفهوم از نقض تعهد مورد تأیید کمیسیون حقوق بین‌الملل نیز قرار گرفته که در ماده ۱۲ آن بیان شده است.

ماده ۱۲: وجود نقض یک تعهد بین‌المللی

«وقتی تعهد توسط یک کشور نقض می‌گردد که عمل آن دولت با خواست تعهد مبنی بر نظم حقوقی بین‌المللی مطابقت نداشته باشد».

وقتی دولتی نقض تعهدی را صورت داده است در قبال آن مسئولیت بین‌المللی دارد، در این صورت بایستی به استناد ماده ۳۰ و ۳۱ طرح کمیسیون حقوق بین‌الملل، تکالیفی را صورت دهد که درواقع ضمانت اجرای مؤثری محسوب می‌شود.

۱- خودداری از تخلف و عدم تکرار آن

ماده ۳۰: قطع تخلف و عدم تکرار:

^۱ مفهوم «مناطق خاکستری» یا Gray Zones به حوزه‌هایی از روابط بین‌الملل اطلاق می‌شود که در آن اقدامات دولت‌ها یا بازیگران غیردولتی نه کاملاً صلح‌آمیز هستند و نه آشکارا جنگی یا تجاوز نظامی محسوب می‌شوند. این فضاها غالباً با تاکتیک‌های فراتر از جنگ سنتی و پایین‌تر از سطح درگیری نظامی مستقیم مشخص می‌شوند و شامل فعالیت‌هایی مانند حملات سایبری، عملیات روانی، جنگ شناختی و تبلیغات هدفمند می‌شوند (Mazarr, 2015). ویژگی اصلی مناطق خاکستری این است که شناسایی مسئولیت و انتساب اقدامات دشوار است. به عنوان مثال، یک حمله سایبری می‌تواند توسط گروه‌های غیردولتی انجام شود اما با حمایت یا هدایت غیرمستقیم دولت‌ها همراه باشد. این شرایط موجب می‌شود که دولت‌ها از پاسخگویی مستقیم فرار کنند و همچنین، جامعه بین‌المللی در اعمال مجازات یا واکنش قانونی دچار ابهام شود (Schmitt, 2017). مناطق خاکستری در عصر جنگ اطلاعاتی اهمیت ویژه‌ای دارند، زیرا بسیاری از عملیات سایبری و روانی دقیقاً در همین فضای مبهم انجام می‌شوند. بازیگران از این فضا بهره می‌برند تا اهداف خود را دنبال کنند بدون اینکه به صورت رسمی قوانین بین‌الملل یا معیارهای سنتی جنگ و صلح نقض شود.

«دولتی که مسئول تخلف بین‌المللی است باید به تکالیف زیر عمل کند: الف: توقف تخلف، اگر ادامه‌دار باشد؛ ب: دادن اطمینان و تضمین مناسب جهت عدم تکرار آن».

این ماده دو موضوع مهم و مرتبط با هم در باره دولتی که مرتکب تخلف بین‌المللی می‌شود را بیان می‌کند: یکی پایان دادن تخلف و دیگری اطمینان و تضمین‌های لازم را برای جلوگیری از تکرار آن ارائه نماید.

این قاعده نشان می‌دهد که مسئولیت دولت تنها محدود به پاسخگویی در برابر یک عمل خلاف قانون نیست، بلکه بر عهده آن است که از تداوم نقض جلوگیری کرده و اقدامات پیشگیرانه برای آینده اتخاذ کند. چنین تکلیفی هم به جبران خسارت وارده کمک می‌کند و هم اعتماد جامعه بین‌المللی را در بازگشت دولت متخلف به رعایت حقوق بین‌الملل تقویت می‌سازد.

۲- جبران خسارت

دومین عامل در ضمانت اجرا، جبران خسارت است. در ماده ۳۱ طرح کمیسیون حقوق بین‌الملل در باره جبران خسارت آمده است:

۱. دولت مسئول مکلف است که خسارت وارده ناشی از تخلف بین‌المللی خود را به نحوی کامل جبران کند؛
۲. خسارت شامل هر گونه زیان اعم از مادی یا معنوی است که ناشی از تخلف بین‌المللی توسط دولت صورت گرفته باشد.

«خسارت وسیله‌ای است برای جبران تجاوز و تعدی که باعث مسئولیت شده و با آن حتی المقدور وضع خلاف حقوق بین‌الملل پیش آمده جبران می‌گردد» (Madani, 1998, 3: 293). بر این اساس، هر گونه نقض حقوق بین‌الملل موجب مسئولیت دولت و مستلزم جبران خسارت است.

اصل جبران خسارت در حقوق بین‌الملل بیانگر آن است که هر دولتی که مرتکب نقض تعهدات بین‌المللی شود، موظف به ترمیم و جبران آثار ناشی از عمل متخلفانه خود است. خسارت نه تنها به عنوان یک وسیله جبرانی، بلکه به عنوان سازوکاری برای بازگرداندن تعادل در نظم حقوقی بین‌المللی عمل می‌کند.

بر اساس طرح کمیسیون حقوق بین‌الملل در مورد مسئولیت دولت، روش‌های جبران خسارت عبارت‌اند از: بازگرداندن وضعیت به حالت پیشین، پرداخت غرامت مالی و جلب رضایت زیان دیده (ILC, 2001: 34-37).

گرچه در جنگ اطلاعاتی، دولت مسئول باید خسارات ناشی از اقدامات اطلاعاتی را جبران کند. اما در اجرای این ضمانت اجراها با مشکلاتی روبه‌روست؛ زیرا اولاً محاسبه و اثبات میزان خسارت‌های ناشی از جنگ اطلاعاتی (مانند تضعیف اعتماد عمومی یا آسیب به داده‌های حساس) کار دشواری است. ثانیاً ابزارهای سنتی جبران خسارت برای چنین مواردی کمتر کارآمدند. از این‌رو، نهادهای بین‌المللی و حقوق‌دانان بایستی در جستجوی سازوکارهایی برای تعیین و جبران خسارات ناشی از جنگ اطلاعاتی باشند.

۳- اقدامات متقابل قانونی

به استناد مواد ۴۹ تا ۵۴ طرح کمیسیون حقوق بین‌الملل در مورد مسئولیت دولت (ILC, 2001)، دولت زیان‌دیده یا جامعه بین‌المللی می‌تواند اقدامات متقابل متناسب و مشروع اتخاذ کند؛ زیرا اقدام متقابل^۱ عنصری کلیدی برای اجرای حقوق بین‌المللی و ابزاری برای دولت آسیب دیده به‌منظور اطمینان از توقف تخلف و جبران خسارت توسط دولت مسئول است (Moser, 2012: 811). به دیگر سخن، دولت قربانی می‌تواند اقداماتی متقابل، اما متناسب برای وادار کردن دولت متخلف به رعایت تعهداتش انجام دهد. به‌عنوان مثال، پاسخ سایبری یا تحریم‌های اقتصادی. اصل اقدام متقابل متناسب در جنگ اطلاعاتی به دولت‌ها امکان می‌دهد بدون توسل به زور، از ابزارهای حقوقی و فناورانه برای بازدارندگی استفاده کنند. با این حال، چالش اصلی در اثبات مسئولیت دولت متخلف و تعیین تناسب اقدام متقابل نهفته است (Schmitt, 2017: 127).

۴- اقدامات شورای امنیت

در مواردی که اقدامات اطلاعاتی تهدیدی علیه صلح و امنیت بین‌المللی باشند، شورای امنیت می‌تواند اقدامات الزام‌آور اعمال کند. شورای امنیت سازمان ملل متحد در مواردی مانند حملات سایبری که تهدیدی برای صلح و امنیت بین‌المللی محسوب شوند، اختیار دارد اقدامات جمعی اتخاذ کند (UN Charter, 1945, Chapter VII).

¹ Countermeasures

۵- مسئولیت کیفری افراد

در صورت ارتکاب جنایات بین‌المللی از طریق ابزارهای اطلاعاتی، امکان پیگرد فردی نیز وجود دارد. بر اساس حقوق بین‌الملل کیفری، افراد می‌توانند مسئول جنایات بین‌المللی از طریق ابزارهای اطلاعاتی باشند، به‌ویژه وقتی رسانه‌ها برای تحریک مستقیم و عمومی به نسل‌کشی به کار روند. نمونه بارز آن پرونده رسانه‌ای رواندا (ICTR, 2003) است که در آن مدیران و خبرنگاران رسانه‌ها به جرم تحریک به نسل‌کشی محکوم شدند. این اصل نشان می‌دهد که مسئولیت فردی فراتر از اقدامات فیزیکی بوده و استفاده از ابزارهای ارتباطی و رسانه‌ای نیز قابل پیگرد کیفری است. چارچوب حقوقی مسئولیت بین‌المللی دولت‌ها در عصر جنگ اطلاعاتی بر اصول کلی حقوق بین‌الملل مانند حاکمیت و عدم مداخله استوار است. با این حال، چالش‌های اساسی در زمینه انتساب و تعیین حدود نقض تعهدات همچنان باقی است. خلأهای موجود نشان می‌دهد که نظام حقوقی بین‌الملل نیازمند اصلاح و توسعه است تا بتواند به‌طور مؤثر به تهدیدات ناشی از جنگ اطلاعاتی پاسخ دهد.

۵-۳- جنگ اطلاعاتی و چالش‌های نوین حقوق بین‌الملل

ظهور جنگ اطلاعاتی در دهه‌های اخیر نه تنها مفهوم سنتی جنگ و صلح را تغییر داده بلکه نظام حقوق بین‌الملل را با چالش‌های جدیدی مواجه ساخته است. ابزارهایی همچون شبکه‌های اجتماعی، رسانه‌های دیجیتال و فناوری‌های هوش مصنوعی زمینه‌ای را فراهم کرده‌اند که در آن دولت‌ها می‌توانند بدون عبور از آستانه سنتی استفاده از زور، به شکل گسترده بر امنیت، ثبات سیاسی و افکار عمومی دیگر کشورها تأثیر بگذارند (Rid, 2012). این تحولات موجب شده است که پرسش‌های جدی درباره کفایت اصول سنتی حقوق بین‌الملل در پاسخ به تهدیدات نوظهور مطرح شود.

۱- دشواری انتساب در عملیات اطلاعاتی

یکی از بزرگ‌ترین چالش‌ها در حقوق بین‌الملل، مسئله انتساب^۱ اقدامات اطلاعاتی به دولت‌ها است. در حالی که عملیات نظامی سنتی غالباً منبع و عامل مشخصی دارد، جنگ اطلاعاتی به دلیل ماهیت غیرمادی و قابلیت پنهان‌سازی عاملان، شناسایی منشأ اقدام را بسیار دشوار می‌سازد (Schmitt, 2017: 99). به‌عنوان مثال، حملات سایبری می‌توانند از طریق سرورهای واسطه در

^۱ Attribution

کشورهای مختلف اجرا شوند و انتشار اخبار جعلی ممکن است توسط حساب‌های کاربری ناشناس یا «بات‌های اینترنتی» سازمان‌دهی شود (Benkler et al., 2018). این شرایط باعث می‌شود اثبات مسئولیت دولت‌ها در مجامع بین‌المللی با موانع حقوقی و فنی فراوان روبه‌رو گردد.

۲- ابهام در مفهوم «استفاده از زور»

ماده ۲(۴) منشور ملل متحد استفاده از زور را علیه تمامیت ارضی یا استقلال سیاسی دولت‌ها ممنوع کرده است (UN Charter, 1945)؛ اما پرسش این است که آیا اقدامات اطلاعاتی مانند حملات سایبری یا عملیات روانی می‌توانند مصداق «استفاده از زور» باشند. دیدگاه‌های مختلفی در این خصوص وجود دارد: برخی حقوقدانان معتقدند تنها اقداماتی که خسارت فیزیکی یا تلفات انسانی به همراه داشته باشند، می‌توانند به‌عنوان استفاده از زور تلقی شوند (Dinstein, 2017). گروهی دیگر بر این باورند که حتی در صورت عدم خسارت فیزیکی، اگر عملیات اطلاعاتی آثار شدید اقتصادی یا سیاسی بر دولت قربانی بگذارد، باید به‌عنوان استفاده از زور در نظر گرفته شود (Schmitt, 2017: 337). این اختلاف نظر نشان می‌دهد که نظام حقوق بین‌الملل هنوز نتوانسته مرز روشنی میان اقدامات مجاز و غیرمجاز در جنگ اطلاعاتی ترسیم کند.

۳- خالهای حقوقی موجود

بررسی اسناد بین‌المللی نشان می‌دهد که چارچوب الزام‌آور مشخصی در خصوص جنگ اطلاعاتی وجود ندارد. «دستورالعمل تالین ۲» تلاش کرده است تا قواعد موجود حقوق بین‌الملل را بر حوزه عملیات سایبری منطبق کند (Schmitt, 2017: 1-3)، اما این سند ماهیت الزام‌آور ندارد و بسیاری از کشورها نیز تفسیرهای آن را نپذیرفته‌اند. علاوه بر این، حقوق بین‌الملل سنتی بیشتر بر اعمال فیزیکی تمرکز داشته و در مواجهه با اقدامات غیرمادی مانند دستکاری افکار عمومی یا انتشار اخبار جعلی فاقد قواعد صریح است. این خلا موجب شده است که دولت‌ها در «مناطق خاکستری» حقوقی فعالیت کنند.

۴- نقش بازیگران غیردولتی

یکی دیگر از چالش‌های اساسی، نقش‌آفرینی بازیگران غیردولتی مانند شرکت‌های فناوری، گروه‌های هکری و سازمان‌های فراملی در جنگ اطلاعاتی است. حقوق بین‌الملل سنتی عمدتاً دولت‌ها را مخاطب قرار می‌دهد، اما در عرصه اطلاعاتی، بخش بزرگی از تهدیدات از سوی این

بازیگران شکل می‌گیرد (Nye, 2014). پرسش اصلی این است که مسئولیت دولت‌ها در قبال اقدامات این بازیگران تا چه اندازه است و آیا باید قواعد جدیدی برای تنظیم رفتار آن‌ها تدوین شود یا خیر.

نتیجه‌گیری و پیشنهادها

پدیده جنگ اطلاعاتی در دهه‌های اخیر نشان داده است که مرزهای سنتی میان جنگ سخت و ابزارهای نرم قدرت به شدت کمرنگ شده و دولت‌ها در عرصه‌ای نوین از رقابت و تعارض قرار گرفته‌اند. در این عرصه، ابزارهای فناورانه و روانی جایگزین یا مکمل سلاح‌های کلاسیک شده و به دولت‌ها این امکان را داده‌اند که بدون ورود مستقیم به درگیری‌های نظامی، به اهداف سیاسی، امنیتی و اقتصادی خود دست یابند. این تحول موجب شده است که نظام حقوق بین‌الملل با چالش‌های جدیدی مواجه گردد؛ چالش‌هایی که عمدتاً از ماهیت غیرملموس، غیرقابل مشاهده و پیچیده جنگ اطلاعاتی ناشی می‌شوند. دشواری انتساب، ابهام در مفهوم استفاده از زور، تهدید علیه صلح و امنیت بین‌المللی، خلأهای حقوقی و نقش بازیگران غیردولتی همگی نشان‌دهنده محدودیت‌های چارچوب‌های موجود حقوقی هستند. بدون بازنگری و توسعه قواعد حقوق بین‌الملل، خطر آن وجود دارد که دولت‌ها از مناطق خاکستری حقوقی سوءاستفاده کرده و نظم بین‌المللی بیش از پیش شکننده شود. از این‌رو، نیاز به گفت‌وگوهای چندجانبه و تدوین قواعد جدید بیش از هر زمان دیگری احساس می‌شود؛ بنابراین، چند مانع اساسی مانع اجرای مؤثر مسئولیت بین‌المللی در عصر جنگ اطلاعاتی هستند:

- ۱) ابهام حقوقی: هنوز اجماعی درباره اینکه کدام اقدامات اطلاعاتی مصداق استفاده از زور یا نقض حاکمیت‌اند وجود ندارد.
- ۲) مشکل فنی انتساب: فناوری‌های پیچیده پنهان‌سازی عاملان، اثبات نقش دولت‌ها را دشوار می‌سازد.
- ۳) ضعف ضمانت اجرا: در بسیاری موارد واکنش‌ها سیاسی یا اقتصادی هستند و ضمانت اجرای حقوقی الزام‌آور وجود ندارد.

۴) نقش بازیگران غیردولتی: بخش بزرگی از عملیات اطلاعاتی توسط گروه‌های هکری یا شرکت‌های فناوری انجام می‌شود و چارچوب مشخصی برای مسئولیت آن‌ها در نظام حقوق بین‌الملل وجود ندارد.

با وجود این چالش‌ها و خلاءهای حقوقی در باره جنگ اطلاعاتی، یافته‌های پژوهش نشان می‌دهد که دولت‌ها در عصر جنگ اطلاعاتی دارای مسئولیت‌هایی بشرح زیر هستند:

نخست، مسئولیت منفی: اصل خودداری از مداخله اطلاعاتی غیرقانونی در امور سایر کشورها است. این اصل مبتنی بر احترام به حاکمیت ملی و استقلال سیاسی کشورهاست و هرگونه تلاش برای نفوذ سایبری، دستکاری اطلاعات یا هدایت افکار عمومی کشور دیگر را در تعارض با اصول بنیادین حقوق بین‌الملل قرار می‌دهد؛ بنابراین، دولت‌ها ملزم‌اند از استفاده ابزاری از فناوری‌های نوین برای برهم زدن ثبات سایر کشورها پرهیز کنند.

دوم، مسئولیت مثبت: اصل پیشگیری و همکاری در مقابله با حملات سایبری از قلمرو خود اهمیت بسزایی دارد. چنانکه دیوان دادگستری بین‌المللی در قضیه کانال کورفو تصریح کرد که دولت‌ها باید مراقب باشند قلمرو آن‌ها برای اعمال خصمانه علیه دیگر دولت‌ها مورد استفاده قرار نگیرد. در دنیای متصل امروز، مرزهای فیزیکی دیگر مانع حملات سایبری نیستند و حملات می‌توانند از طریق زیرساخت‌های دیجیتال هر کشوری به سایر نقاط جهان تسری یابند. در چنین شرایطی، دولت‌ها مسئولیت دارند نه تنها مانع سوءاستفاده از قلمرو خود برای انجام این‌گونه حملات شوند، بلکه با سایر دولت‌ها برای شناسایی و مهار تهدیدات مشترک همکاری مؤثر داشته باشند. این اصل به تقویت اعتماد متقابل بین‌المللی و کاهش بی‌ثباتی جهانی کمک می‌کند.

سوم، مسئولیت جبرانی: اصل جبران خسارت و توقف فوری عمل متخلفانه به عنوان رکن پایانی مسئولیت دولت‌ها در عرصه جنگ اطلاعاتی مطرح است. هر دولتی که در نتیجه اقدامات اطلاعاتی غیرقانونی موجب ورود خسارت به کشور دیگر شود، موظف است ضمن توقف فوری عمل، خسارات وارد شده را جبران نماید. این امر نه تنها تضمینی برای احقاق حقوق متضرر است، بلکه به تقویت نظم حقوقی بین‌المللی و ایجاد بازدارندگی در برابر تکرار تخلفات مشابه کمک می‌کند.

با توجه به نوظهور بودن جنگ اطلاعاتی در عرصه روابط بین‌الملل، پیشنهادهایی بشرح زیر مطرح می‌شود:

- (۱) تدوین معاهدات جدید برای تنظیم جنگ اطلاعاتی و عملیات سایبری؛
- (۲) تعریف روشن تر از مفاهیم «استفاده از زور» و «مداخله» در بستر اطلاعات؛ (برای مثال: انتشار اخبار جعلی و عملیات روانی که منجر به تضعیف ساختارهای سیاسی کشورها می شود باید به عنوان مصادیق نقض اصل عدم مداخله شناسایی شوند).
- (۳) ایجاد سازوکارهای بین المللی برای شفاف سازی و اشتراک اطلاعات درباره حملات سایبری؛ (همانند مدل «مرکز عالی دفاع مشترک سایبری ناتو»^۱، لازم است ساختارهای بین المللی بی طرف برای بررسی و اعلام منشأ حملات اطلاعاتی ایجاد شوند؛ و همچنین دولت ها باید سازوکارهایی برای تبادل اطلاعات درباره حملات اطلاعاتی و تهدیدات نوظهور ایجاد کنند تا روند انتساب و پاسخ سریع تر انجام شود).

تعارض منافع

بنا بر اظهار نویسندگان، مقاله پیش رو فاقد هر گونه تعارض منافع بوده است.

¹ The NATO Cooperative Cyber Defense Centre of Excellence

Translated References to English

- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
- Bıçakçı, Salih (2025), *Cognitive Security in the Age of AI: Building National Resilience Against Synthetic Influence*, Policy Paper No 4, Istanbul Bilgi University and the European Commission Jean Monnet Centers of Excellence.
- Bledsoe, Robert L. and Boczek, Boleslaw A(1987), *The International Law Dictionary*, ABC-CLIO, Santa Barbara California, Oxford, England.
- Brownlie, Ian (2004). *International Law in the Last Years of the Twentieth Century*. Translated by Saleh Rezaei Pish Robat. Tehran: Center for International Political Studies. [in Persian]
- Cassese, A. (2007). *International Law*. Oxford University Press.
- Cassese, Antonio (2006). *International Law*. Translated by Hossein Sharifi Taraz Kouhi. Tehran: Mizan. [in Persian]
- Chesney B. & Citron, D(2019), *Deep fakes: A looming challenge for privacy, democracy and national security*, *California Law Review*, Volume 107, 1753- 1819.
- Claverie, Bernard and du Cluzel, François(2023), *The Cognitive Warfare Concept*, <https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article>.
- Deibert, R. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Signal.
- Dinstein, Yoram(2004), *the Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge university press.
- Dinstein, Yoram. (2017). *War, Aggression and Self-Defence* (6th ed.). Cambridge University Press.
- Emadzadeh, Mohammad Kazem (1991). *Public International Law*. Tehran: Ata Publications. [in Persian]
- Fakheri, S., Nourbakhsh, A., & Yamaghani, M. R. (2024). *Deepfake detection models and methods in artificial intelligence and insights from media and social culture perspective*. *Innovation management and operational strategies*, 5(3), 259-287. [in Persian]
- Fiyouzi, Reza (2000). *International Responsibility and the Doctrine of Diplomatic Protection of Nationals* (Vol. 1). Tehran: University of Tehran Press. [in Persian]
- Huang, Linan & Zhu, Quanyan (2023), *Cognitive Security: A System-Scientific Approach*, Springer Nature Switzerland AG, <https://doi.org/10.1007/978-3-031-30709-6>.
- International Court of Justice (ICJ). (1986). *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America). ICJ Reports.
- International Criminal Tribunal for Rwanda. (2003). *The Media Case: Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze. Judgment and Sentence*. <https://casebook.icrc.org/case-study/ictr-media-case>.
- International Law Commission (ILC). (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. United Nations.
- Jafari, Seyed Asghar (2023), *Identifying and analyzing the key drivers of strengthening the country against threats based on the view of Imam Khamenei*, *CSocial crisis management*, 15(4), 11–38. [in Persian]
- Jatmiko, Bagus(2023), *What are information warfare and its significance for Indonesian defense and security?* *Maritime Nusantara*,3(2). 133-148.
- Kaviani, Mohammad (2001). *Propaganda and Psychological Warfare*. *Methodology of Human Sciences*, 7(29), 110–133. [in Persian]
- Kermani, Mousa (2023). *A Brief Look at the Tallinn Manual on International Law Applicable to Cyber Space*. Retrieved from the Forum of the Iranian Association for United Nations Studies, Publication Date:09/03/2024 [in Persian]
- Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.

- Madani, Seyed Jalaladin (1998), Public International Law and Principles of State Relations (Volume 1,2,3), Tehran, Paydar Publications. [in Persian]
- Mazarr, Michael J. (2015). Mastering the Gray Zone: Understanding a Changing Era of Conflict. United States Army War College Press.
- Moradi, Ali; Tabibi Jabali, Morteza & Heidari, Mohammad Ali (2016). A Jurisprudential and Legal Analysis of Psychological Operations Islamic Law Research Journal, 17(2), 149-173. [in Persian]
- Moradpiri, Hadi & Khezraie, Hamid Reza (2020). "The Role of New Information Technologies in Future Wars." Soft Power Studies Quarterly, 10(23), 159-177.. [in Persian]
- Mosaffa, Nasrin, et al. (1986). The Concept of Aggression in International Law. Tehran: Center for Advanced International Studies, University of Tehran. [in Persian]
- Moser, P. T. (2012). Non-Recognition of State Immunity as a Judicial Countermeasure to Jus Cogens Violations: The Human Rights Answer to the ICJ Decision on the Ferrini Case. Goettingen Journal of International Law, 4(3), 809-852
- Mostaghimi, Bahram & Taremsari, Masoud (1998). State Responsibility with Regard to Iraq's Aggression Against Iran. Tehran: University of Tehran Press. [in Persian]
- Mousazadeh, Reza & Azarpandar, Ahmadreza (2024). International Humanitarian Law and New Technologies. Tehran: Mizan Publishing. . [in Persian]
- Namdar, Saeed (2019). Cyber Attacks and Public International Law. Tehran: Educational and Research Institute of Defense Industries Press. [in Persian]
- Nikoonahad, Ayoub & Biyouk, Mohsen (2024). Designing and Visualizing the Desired Model of "Jihad of Clarification" in Confrontation with the Phenomenon of Cognitive Warfare Based on the Thoughts of the Supreme Leader of the Islamic Revolution. Islamic Revolution Futures Studies, 5(17), 11-36. [in Persian]
- Nye, Joseph S., (2014), The Regime Complex for Managing Global Cyber Activities, Harvard Kennedy School of Government, Global Commission on Internet Governance Paper Series No. 1
- Rashidzadeh, Fathollah (2006). "The Information Age and Information Warfare." Military Management Quarterly, 7(21), 41-70. [in Persian]
- Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35 (1), 5-32. <https://doi.org/https://doi.org/10.1080/01402390.2011.60893>
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, 21 (6), 11-25. [in Persian]
- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- Schmitt, Michael and Biller, Jeffrey(2017), The NotPetya Cyber Operation as a Case Study of International Law. <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/>
- Shackelford, S. J. (2010). State responsibility for cyber attacks: Competing standards for a growing problem. Georgetown Journal of International Law, 42 (4), 197- 208.
- Sharifi Taraz Kouhi, Hossein (1996). Peremptory Norms and the International Legal Order. Tehran: Center for International Political Studies. [in Persian]
- Sheikholeslami, M.H. and Seddighi, M. (2025). The Responsibility of States in Managing Information Warfare during the Transition to a Multipolar Order: Challenges and Requirements. Journal of cognitive research in political studies, 2(4), 28-54 doi: 10.20241403/CRPS.2509.1075.4.7.2. [in Persian]
- Tadić, Appeals Chamber judgment: Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber judgment (Intl'l Crim. Trib. for the Former Yugoslavia 15 July 1999).

- Talaei, Safieh (2025). "Artificial Intelligence and Cyber Warfare: Legal Dimensions of State Responsibility in International Law." *Journal of Modern Jurisprudence and Law*, 12(22), 1–13. [in Persian]
- Torabi, Ghasem & Taherizadeh, Mohammad Naser (2021). "The Cyber Revolution and the Transformation of the Concept of Information Warfare in International Relations." *International Studies Quarterly*, 17(4), 47–65.. [in Persian]
- Torabi, Hassan & Ahmadi, Fatemeh (2025). "Cognitive Resilience Against Cognitive Warfare Targeting Iran: Components, Analysis, and Strategies for Enhancement." *Cognitive Research in Political Studies Quarterly*, 2(1), 101–121. [in Persian]
- UN Charter. (1945). Charter of the United Nations. United Nations.
- Ziaee Bigdeli, Mohammad Reza (1992). *Public International Law*. Tehran: Ganj Danesh. [in Persian]
- Ziaee, Seyed Yaser & Khalilzadeh, Mona (2013). "State Responsibility for Cyber Attacks." *Legal Research Journal*, 12(23), 87–122.. [in Persian]