Contemporary Challenges to the Law of Neutrality: Analyzing the Interaction Between the Law of Neutrality and Cyber Operations Within the Framework of the Tallinn Manual 2.0

Kian Biglarbeigi
Ph.D. Candidate in International Law, Faculty of Law and Political Science, University of Tehran, Tehran, Iran
kian.biglarbeigi@gmail.com

Sattar Azizi
Professor, Department of Law, Faculty of Humanities, Bu-Ali Sina University, Hamedan, Iran (Corresponding Author)
s.azizi@basu.ac.ir

Journal of Research and Development in Public Law

Iranian Law and Legal Research Institute

Vol. 2 | No. 4 | Fall 2025 Winter 2026 (Original Article)

https://jrpl.illrc.ac.ir

DOI: 10.22034/jrpl.2025.2065349.1159

Abstract

War, perhaps the most explicit manifestation of the use of force, has been formally prohibited under Article 2(4) of the United Nations Charter. Yet this prohibition has not eliminated armed conflict from contemporary international relations; war continues to persist as an undeniable reality. Against this backdrop, international law, while acknowledging the persistence of armed conflict, establishes a set of rights and obligations for both belligerent states and third states that remain outside the hostilities. This body of rules is collectively known as the "law of neutrality."Simultaneously, the rapid development of information technologies has increased states' dependence on cyberspace and digital infrastructure. Although this reliance has enabled new forms of political, economic, and military engagement, it has also fostered the emergence of a novel form of conflict: cyber warfare.

Cyber operations differ fundamentally from traditional armed conflict in their nature, methods, and operational environments. The absence of dedicated treaty law and the limited formation of customary norms governing cyber operations constitute significant challenges for contemporary international law.In this context, the Tallinn Manual 2.0, one of the most comprehensive academic efforts to articulate applicable legal principles in cyberspace, holds considerable importance. It examines relevant international legal rules governing cyber operations and attempts to construct a coherent framework for addressing emerging challenges. Notably, Chapter 20 of the Manual, through five specific rules, analyzes the legal status of cyber operations from the perspective of the law of neutrality and provides valuable interpretive guidance.The central question of this article is therefore: What obligations and limitations govern cyber activities in light of the principles and rules of the law of neutrality? Using a descriptive-analytical method and relying on library-based sources, this study evaluates the approach of the Tallinn Manual 2.0 and assesses its compatibility with the established rules of neutrality in international law.

Keywords: Cyberspace, Cyber Infrastructure, Law of Neutrality, International Armed Conflict, Tallinn Manual 2.0

چالش‌های نوین حقوق بی‌طرفی؛ واکاوی تقابل حقوق بی‌طرفی با عملیات سایبری در چارچوب راهنمای تالین ۲

کیان بیگلربیگی
پژوهشگر دکتری حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.
kian.biglarbeigi@gmail.com

ستار عزیزی
استاد گروه حقوق، دانشگاه علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران (نویسنده مسئول)
s.azizi@basu.ac.ir

دوفصلنامه تحقیق و توسعه در حقوق عمومی
پژوهشکده حقوق و قانون ایران

دوره ۲| شماره ۴ | پاییز و زمستان ۱۴۰۴
(مقاله پژوهشی)

https://jrpl.illrc.ac.ir

DOI:
10.22034/jrpl.2025.2065349.1159

چکیده

جنگ، به‌عنوان بارزترین نمود توسل به زور، پس از تصویب منشور ملل متحد و به‌موجب بند ۴ ماده ۲ آن، صراحتاً ممنوع اعلام شده است. با این حال، این ممنوعیت نتوانسته مانع از وقوع مخاصمات مسلحانه در دوران معاصر گردد و پدیده جنگ هم‌چنان به‌عنوان یکی از واقعیات انکارناپذیر حیات جامعه بین‌المللی باقی‌مانده است. در این‌چارچوب، نظام حقوق بین‌الملل به‌موازات پذیرش واقعیت جنگ، برای طرف‌های درگیر در مخاصمه و نیز دولت‌های ثالثی که مستقیماً در جنگ مشارکت ندارند، حقوق و تکالیفی پیش‌بینی کرده است. این مجموعه قواعد تحت عنوان «حقوق بی‌طرفی» مورد شناسایی و تبیین قرار گرفته‌اند. در سوی دیگر، با گسترش روزافزون فناوری اطلاعات، دولت‌ها بیش از پیش به زیرساخت‌های فضای سایبر وابسته شده‌اند. این وابستگی، ضمن ایجاد بسترهای جدیدی برای تعاملات سیاسی، اقتصادی و نظامی، زمینه‌ساز نوع نوینی از مخاصمات موسوم به «جنگ‌های سایبری» نیز شده است؛

جنگ‌هایی که در ماهیت و شیوه اجرا، تفاوت‌های بنیادینی با جنگ‌های سنتی دارند. با وجود این، فقدان مقررات معاهده‌ای مشخص و نیز فقر قواعد عرفی در زمینه تنظیم حقوقی عملیات‌های سایبری، از چالش‌های اصلی حقوق بین‌الملل معاصر به‌شمار می‌رود. در این راستا، راهنمای تالین ۲ به‌عنوان یکی از جامع‌ترین تلاش‌های علمی در جهت قاعده‌مند ساختن فضای سایبر، واجد اهمیت ویژه‌ای است. این سند، ضمن بررسی قواعد قابل اعمال بر عملیات‌های سایبری، می‌کوشد چارچوبی حقوقی برای مواجهه با چالش‌های نوظهور این عرصه ترسیم نماید. فصل بیستم این راهنما در قالب پنج قاعده، به بررسی وضعیت عملیات سایبری از منظر حقوق بی‌طرفی پرداخته و نکات تحلیلی قابل توجهی را در این زمینه ارائه می‌دهد. بر همین اساس، پرسش اصلی این مقاله آن است که چه الزامات و محدودیت‌هایی بر فعالیت‌های سایبری در پرتو قواعد حقوق بی‌طرفی حاکم است؟ به‌منظور پاسخ به این پرسش، پژوهش حاضر با بهره‌گیری از روش توصیفی-تحلیلی و اتکاء بر منابع کتابخانه‌ای، می‌کوشد مواضع ارائه شده در راهنمای تالین ۲ را در تطبیق با قواعد موجود در حقوق بی‌طرفی مورد بررسی قرار دهد.

کلیدواژه‌ها: فضای سایبر، زیرساخت سایبری، حقوق بی‌طرفی، ماصمه مسلحانه بین‌المللی، راهنمای تالین ۲.

مقدمه

بی‌طرفی در جریان یک درگیری مسلحانه، معمولاً ناشی از اراده یک‌جانبه کشوری است که خواهان شرکت در آن درگیری نمی‌باشد؛ چراکه اصولاً هر کشوری به هنگامی که در مقابل یک درگیری مسلحانه قرار می‌گیرد، باید میان شرکت یا عدم شرکت در آن درگیری، یعنی میان جنگ و بی‌طرفی، یکی را انتخاب کند. هیچ کشوری نمی‌تواند در زمان حمله متخاصم باشد، حمله کند و هنگامی که به او حمله می‌شود، مدعی بی‌طرفی شود. ازاین‌رو کشورهای متخاصم و کشورهای بی‌طرف در مناسبات متقابل خود تابع قواعد و مقررات حقوقی به نام «حقوق بی‌طرفی» هستند (ضیایی بیگدلی (الف)، ۱٤۰۰: ۳۱۳).

البته باید اشاره داشت، قواعد و مقررات ناظر بر زمان بی‌طرفی، یعنی حقوق بی‌طرفی، بخشی از حقوق جنگ نیست؛ زیرا حقوق جنگ حاکم بر مناسبات کشورهای متخاصم با یکدیگر است، در حالی که حقوق بی‌طرفی بر روابط میان کشورهای متخاصم و کشورهای بی‌طرف حاکم است و چون کشورهای بی‌طرف را نمی‌توان «متخاصم» دانست، لذا حقوق جنگ این‌گونه مناسبات را تحت نظم در نمی‌آورد. اما جنگ به حدی در زندگی جامعه بین‌المللی نفوذ کرده است که حتی موجد حقوق و تکالیفی برای کشورهایی که در آن دخالتی ندارند نیز شده است و ازسوی‌دیگر، روابط متخاصمان با بی‌طرف‌ها را نیز تحت‌تأثیر جدی قرار داده و منجر به ایجاد حقوق و تکالیفی در مناسبات آن‌ها با یکدیگر شده است. بنابراین، حقوق بی‌طرفی در ضمن جدا بودن از حقوق جنگ، نمی‌تواند چندان مستقل و بی‌ارتباط با آن باشد (ضیایی بیگدلی (ب)، ۱٤۰۰: ۳۲۵-۳۲٦). ازاین‌رو، حقوق بی‌طرفی از یک سو روابط میان طرف‌های یک مخاصمه مسلحانه بین‌المللی و ازسوی‌دیگر دولت‌هایی که طرف مخاصمه نیستند را تنظیم می‌کند که اهداف اصلی این حقوق عبارت‌اند از: ۱) حمایت از دولت‌های بی‌طرف و شهروندان آن‌ها در برابر آثار زیان‌بار مخاصمه؛ [۱] ۲) حفظ حقوق دولت‌های بی‌طرف، نظیر انجام تجارت[۲] در دریاهای آزاد؛ و

---

[۱] حق بر دور ماندن از آثار نامساعد جنگ به این معنا است که رابطه میان دولت‌های متخاصم و بی‌طرف تحت حاکمیت قواعد زمان صلح است، قواعدی که صرفاً در مواردی خاص از رهگذر حقوق بی‌طرفی اصلاح شده است؛ به‌ویژه دولت بی‌طرف باید نظارت‌هایی خاص در حوزه تجارت دریایی را پذیرا شود (فلک، ۱۳۹۵: ٦۳۷).

[۲] از دید حقوقی، کشور بی‌طرف می‌تواند روابط تجاری خود را با همه کشورها، از جمله متخاصمان حفظ کند و کشتی‌های تجاری که پرچم او را دارا هستند، می‌توانند در دریاها تردد نمایند؛ اما این آزادی در عمل محدود شده است (ضیایی بیگدلی (ب)، ۱٤۰۰: ۳٥٤-۳٥٥).

۳) حمایت از طرف‌های مخاصمه در برابر اقدام یا خودداری از اقدام دولت‌های بی‌طرف که به نفع دشمن آن‌ها تمام شود (Tallinn Manual 2.0, 2017 : 553-554).

ازسوی‌دیگر، حق بر فناوری از آن جهت که دنبال ترویج توزیع عادلانه منافع تکنولوژیکی فناوری‌های اساسی و بنیادی است، با رشد و رفاه انسان در عصر فناوری پیوند خورده است. حق بر فناوری از انسان در برابر کاربردهای مضر و آسیب‌های فناوری جلوگیری می‌کند و برای حفظ تمامیت جسمی و معنوی، آزادی و امنیت انسان لازم است (انصاری، اسدی، ۱۴۰۳: ۹۲). ازاین‌رو از آغاز «عصر اطلاعات» [1]، کشورها به‌شدت به استفاده از فناوری رایانه برای تنظیم مؤثر جوامع خود وابسته شده‌اند. بااین‌حال، همان‌طور که رویدادهای اخیر نشان داده است، بازیگران متخاصم این وابستگی را تشخیص داده‌اند و به طور فزاینده‌ای به دنبال حمله به سرورهای رایانه و اطلاعاتی هستند که آن‌ها در اختیار دارند[2] (Buchan, 2012 : 211). امروزه استفاده از عملیات سایبری در زمان جنگ به یک

[1] Information Age.

[2] برای نمونه، رخنه MOAB در ژانویه ۲۰۲٤، که به‌طور گسترده‌ای با عنوان «مادرِ همه‌ی رخنه‌ها» شناخته می‌شود، شامل کشف پایگاه‌داده‌ای بود که حاوی ۲٦ میلیارد رکورد اطلاعاتی افشاشده بود. این رخنه بر شرکت‌ها و سازمان‌های متعددی تأثیر گذاشت که از جمله آن‌ها می‌توان به نام‌های بزرگی مانند Tencent QQ، Weibo، MySpace، Twitter، Deezer، LinkedIn، Adobe، Canva و Dropbox اشاره کرد. به‌دلیل حجم عظیم اطلاعات افشاشده، این رخنه خطرات جدی‌ای در زمینه‌ی سرقت هویت، طرح‌های فیشینگ، حملات سایبری هدفمند و دسترسی غیرمجاز به حساب‌های شخصی و حساس ایجاد کرده است (Trend Micro, 2024). در ژانویه ۲۰۲٤، یک حمله سایبری گسترده شامل برداشت داده از پلتفرم مدیریت پروژه Trello صورت گرفت. در این حمله، جزئیات شخصی بیش از ۱۵ میلیون کاربر برای فروش در دارک‌وب قرار گرفت. این رخنه که توسط مجرمان سایبری موسوم به «emo» انجام شد، اطلاعات حساسی از جمله آدرس‌های ایمیل، نام‌ها و نام‌های کاربری کاربران را در معرض خطر قرار داد (Hope, 2024). در فوریه ۲۰۲٤، هکرها موفق به تولید ۱.۷۹ میلیارد توکن رمزارز از پلتفرم بازی PlayDapp شدند. این حمله حول محور استفاده غیرمجاز از یک کلید خصوصی سرقت‌شده برای ایجاد و سرقت بیش از ۱.۷۹ میلیارد توکن PLA — رمزارز اصلی مورد استفاده در این پلتفرم — متمرکز بود. کیف پول غیرمجاز هکرها، ۲۰۰ میلیون توکن PLA به ارزش ۳٦.۵ میلیون دلار ضرب کرد، که موجی در جامعه رمزارز ایجاد کرد (Toulas, 2024). حمله باج‌افزاری به شرکت Johnson Controls International در سپتامبر ۲۰۲۳ منجر به هزینه‌هایی بیش از ۲۷ میلیون دلار شد. مجرمان سایبری پشت این حمله که با نام Dark Angels شناخته می‌شوند، مدعی شدند که بیش از ۲۷ ترابایت داده از این شرکت سرقت کرده و برای رمزگشایی و حذف فایل‌های دزدیده‌شده، ۵۱ میلیون دلار باج درخواست کرده‌اند (Kovacs, 2024). در اوت ۲۰۲۳، شرکت Dollar Tree هدف یک حمله سایبری در زنجیره تأمین قرار گرفت که از سوی یک ارائه‌دهنده خدمات ثالث با نام Zeroed-In Technologies انجام شد. این حمله اطلاعات شخصی حدود ۲ میلیون نفر از جمله نام، تاریخ تولد و شماره‌های تأمین اجتماعی را به خطر انداخت (Battle, 2023). سه مورد از این حوادث اخیر سایبری تنها در یک ماه رخ داده‌اند. این امر تعجب‌آور نیست؛ چراکه روزانه یک آسیب‌پذیری جدید کشف می‌شود و به مهاجمان

واقعیت تبدیل شده است. اگرچه تنها تعداد معدودی از کشورها به طور علنی استفاده از چنین عملیاتی را اعلام کرده‌اند، اما تعداد فزاینده‌ای از کشورها درحال‌توسعه قابلیت‌های سایبری نظامی خود هستند و به احتمال زیاد، عملیات سایبری در آینده افزایش خواهد یافت (ICRC, n.d). فضای مجازی این امکان را ایجاد کرده است که برای پیروزی در مخاصمات مسلحانه دیگر نیاز چندانی به فتوحات سرزمینی نباشد، بلکه با تسلط بر فناوری سایبری و حمله به سیستم رایانه‌ای دشمن از طرق مختلف از جمله ارسال ویروس می‌توان کلیه زیرساخت‌های آن را مورد حمله و آسیب جدی قرار داد و حتی تا مرحله خارج‌کردن کنترل مرزهای آن پیش رفت. این حملات، می‌توانند هم به طور مستقل انجام شوند و هم اجرای آن‌ها در جریان مخاصمات مسلحانه ممکن است (بیگ‌زاده، ۱۴۰۱: ۱۵۲۱). ازاین‌رو این مسئله در حال حاضر در چارچوب مخاصمات بین‌المللی توجه زیادی را به خود جلب کرده است. اخبار به طور منظم درباره جنگ سایبری[1] و جنگ اطلاعاتی[2] گزارش می‌دهند، جایی که مرزها بین جنگ سنتی - که در آن تنها بازیگران دولتی شرکت

فرصت می‌دهد تا داده‌ها را به سرقت ببرند. لذا هیچ کسب‌وکاری نباید فرض کند که هدف حمله نیست، زیرا امروزه به‌طور فزاینده‌ای اقتصاد جهانی به فضای سایبر وابسته است. گزارش «مجمع جهانی اقتصاد» در سال ۲۰۱۸ درباره خطرهای منطقه‌ای برای انجام کسب‌وکار، که بر اساس نظرسنجی از ۱۲،۵٤۸ رهبر تجاری جهانی تهیه شده بود، حملات سایبری را در رتبه پنجم فهرست جهانی خطرهای کسب‌وکار قرار داد. با این حال، در مناطق و کشورهای دارای دیجیتالی‌شدگی بالا، حملات سایبری در رتبه نخست قرار گرفتند. در اروپا، آمریکای شمالی، منطقه آسیا-اقیانوسیه شرقی و در اقتصادهای دیجیتالی درحال رشد سریع مانند هند، مدیران تجاری حملات سایبری و نقض داده‌ها را به‌عنوان مهم‌ترین خطر فعلی و آتی معرفی کردند. دولت‌ها نیز با این دیدگاه موافق به نظر می‌رسند. در بسیاری از کشورها، جرایم سایبری، حملات سایبری، جاسوسی اقتصادی، جنگ سایبری و کارزارهای اطلاعات نادرست در صدر فهرست‌های ارزیابی تهدیدات رسمی دولت‌ها قرار دارند، اگرچه شواهد تجربی که مبنای این ارزیابی‌ها هستند، اغلب پراکنده و ناکامل‌اند (Broeders, 2021: 2). بنابراین، این واقعیت که اقتصاد جهانی به شدت به فضای سایبری وابسته است، به همان اندازه که فرصتی برای گسترش تجارت و صنعت فراهم می‌کند، زمینه‌ساز حملات سایبری هولناک و سایر آسیب‌پذیری‌های منحصربه‌فرد سایبری نیز می‌باشد (Sang, 2016: 206)؛ چراکه برای مثال، متأسفانه، انتساب در فضای سایبر به همان اندازه که ضروری است، چالش‌برانگیز نیز می‌باشد. در اینترنت، اطلاعات معمولاً در قالب بسته‌هایی (packets) انتقال می‌یابند که واحدهای مجزایی از داده هستند و دارای دستورالعمل‌های تحویل، مانند آدرس‌های مقصد، می‌باشند. ماشین‌های اختصاصی (روترها) این بسته‌ها را منتقل می‌کنند. بسته‌ها حاوی یک آدرس پروتکل اینترنت (IP) منبع هستند، اما این اطلاعات برای کسانی که به‌دنبال تأیید منبع یک بسته هستند، چندان مفید نیست؛ زیرا عملکرد اصلی یک روتر انتقال بسته به مقصد است و روترها معمولاً به‌دنبال تأیید صحت آدرس منبع نیستند. در واقع، معماران اینترنت چنین تأییدی را در تضاد با نقش روتر در انتقال داده‌ها می‌دانستند (Margulies, 2008: 8).

[1] Cyber Warfare.
[2] Information Warfare.

دارند - و اشکال جدید دشمنی و جنگ که شامل بازیگران غیردولتی و غیرنظامیان نیز می‌شود، محو شده است (Valuch, Gábriš & Hamuľák, 2017 : 65).

بااین‌حال، خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه فضای سایبر بسیار مشهود است. به استثنای کنوانسیون سال ۲۰۰۱ بوداپست موضوع جرایم سایبری که در چارچوب «شورای اروپا» [۱] منعقد گردید؛ [۲] و پروتکل الحاقی به آن [۳] که صرفاً به جرایم افراد مربوط می‌شود، سند بین‌المللی مهم دیگری در حوزه عملیات سایبری موجود نیست و شاید تنها بتوان به راهنماهای تالین اشاره کرد که در سال‌های ۲۰۱۳ [۴] و ۲۰۱۷ [۵] توسط جمعی از کارشناسان بین‌المللی در چارچوب سازمان ناتو تهیه گردیده‌اند (بیگلربیگی، ۱۴۰۲ : ۲).

در این سیاق، فضای سایبر، به دلیل ویژگی‌های مرموزش، به‌عنوان «بُعد پنجم» یا «قلمرو پنجم» توصیف شده است. به نظر می‌رسد باور گسترده‌ای وجود دارد دائر بر این‌که این فضا از قواعد و اصول سنتی حقوق بین‌الملل گریزان است و نیاز فوری به قواعد جدیدی دارد که منحصراً برای فضای سایبر طراحی شده باشند. در گذشته نیز بارها با سردرگمی چشمگیری نسبت به فناوری‌های نوظهور مواجه بودیم که منجر به

---

[1] The Council of Europe.

[2] Convention on Cybercrime (Budapest Convention). (2001). Council of Europe. European Treaty Series – No. 185., Entered into Force on 1 July 2004.

[۳] این پروتکل درخصوص « لزوم جرم انگاری اقدام‌های نژادپرستانه و بیگانه هراسی که با استفاده از رایانه ارتکاب می‌یابند» است.

Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System. (2003).

[۴] از ترکیب بیست و سه نفری این کارشناسان، نه نفر از ایالات متحد آمریکا بودند و کشورهای دارای قابلیت‌های سایبری یا کشورهای قربانی حملات سایبری مانند روسیه، ایران و چین نماینده ای در این مجموعه نداشتند که این امر انتقادات شدیدی را برانگیخت (Liivoja, McCormack, 2013: 4-12).

[۵] راهنمای تالین در حقوق بین‌الملل قابل اعمال در نبردهای سایبری متعلق به بازهٔ زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در کشور استونی است که توسط مایکل اشمیت در مورد مقررات حاکم بر اقدام‌ها و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبرد ناتو در ولز بریتانی، در قالب اصل ٤ پیمان ناتو، تهیه شده است. به‌رغم پیوند راهنمای تالین ۲ با ناتو، در مقدمه این راهنما تصریح شده است که قواعد بیان شده در این راهنما، دیدگاه کشورهای متبوع کارشناسان تدوین‌کننده، ناتو یا مرکز عالی پدافند مشترک سایبری ناتو (CCDCOE) نیست؛ بلکه تنها محصول مطالعه مستقل کارشناسان و متخصصان تدوین‌کننده می‌باشد.

درخواست‌های اضطراری مشابهی برای تدوین هنجارهای جدید شده است؛ بااین‌حال، در موارد نادری چنین درخواست‌هایی موجه بوده‌اند. اگر این موضوع به طور واقع‌گرایانه تحلیل شود، حقوق بین‌الملل موجود، نه به دلیل نو بودن فناوری پایه فضای سایبر و نه به‌خاطر تهدیدهایی که پیش از عصر دیجیتال وجود نداشتند، نیازی به عقب‌نشینی ندارد. جالب آنکه به نظر می‌رسد دولت‌ها توافق دارند که حقوق بین‌الملل عرفی از لحاظ اصولی بر فضای سایبر قابل اعمال است، هرچند ممکن است نیاز به تطبیق توافقی با ویژگی‌های خاص این فضا وجود داشته باشد (Heintschel von Heinegg, 2013 : 123-124). لذا باید خاطرنشان نمود که فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به عملیات سایبری نمایند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت در خصوص عملیات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیه اروپا و دولت‌های متعدد؛ از جمله ایالات متحد آمریکا، ایران، بریتانیا، روسیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالی این نظریه را پذیرفته‌اند (Roscini, 2014 : 19-22).

ازاین‌رو در خلأ هنجاری و رویه واحد دولتی، راهنمای تالین ۲ به‌عنوان معتبرترین و پراستنادترین اثر در زمینه حقوق بین‌الملل قابل‌اعمال بر عملیات سایبری، بررسی دقیقی از نحوه اعمال قواعد و مقررات بین‌المللی موجود[1] در تطابق با حوزه پیچیده و در حال تحول فضای سایبر ارائه می‌کند و می‌تواند به خوبی دیدگاه کارشناسان و اندیشمندان حقوقی و فنی آشنا با مسائل سایبری در مورد نحوه رفتار دولت‌ها که دست به ارتکاب عملیات سایبری می‌زنند، روشن سازد (بیگلربیگی و عزیزی، ۱٤۰٤: ۲۱۸).

در این راستا، گروه بین‌المللی کارشناسان راهنمای تالین ۲ به طور متفق‌القول[2] توافق داشتند، حقوق بی‌طرفی که صرفاً در زمان مخاصمات مسلحانه بین‌المللی قابل‌اجرا است

[1] راهنمای تالین ۲ بازتاب‌دهنده قواعد و مقرراتی است که در زمان تدوین این راهنما وجود داشته (Lex lata)؛ نه این‌که قواعد و مقررات جدیدی به گسترده حقوق بین‌الملل بیفزاید و از اظهاراتی که منعکس‌کننده Lex ferenda باشد، اجتناب می‌کند (Wallace & Visger, 2018: 19).

[2] Unanimously.

و بر پایه کنوانسیون‌های پنجم[1] و سیزدهم[2] لاهه و حقوق بین‌الملل عرفی استوار است، [3] در مورد عملیات سایبری نیز قابل اعمال است[4] (Tallinn Manual 2.0, 2017 : 553)؛ چراکه توزیع جهانی دارایی‌ها و فعالیت‌های سایبری، به همراه وابستگی جهانی به زیرساخت‌های سایبری، بدان معناست که عملیات سایبری طرف‌های درگیر به‌آسانی می‌تواند زیرساخت سایبری عمومی یا خصوصی دولت‌های بی‌طرف را تحت‌تأثیر قرار دهد. براین‌اساس، اصل بی‌طرفی در مخاصمات مسلحانه مدرن اهمیت ویژه‌ای دارد (همان: ۵۵۴). بدین جهت، نوشتار حاضر با استناد به قواعد و تفسیرهای راهنمای تالین ۲، در قالب دو گفتار به بررسی موضوع می‌پردازد. در گفتار نخست، مفاهیم و تعاریف بنیادین در حوزه حقوق بی‌طرفی و فضای سایبر تبیین می‌گردد؛ و در گفتار دوم، به تحلیل شرایط و الزامات حاکم بر عملیات سایبری در چارچوب حقوق بی‌طرفی پرداخته می‌شود.

---

[1] عهدنامه پنجم لاهه که اختصاصاً در زمینه بی‌طرفی در جنگ زمینی است، حقوق و تکالیف کشورهای بی‌طرف و متخاصم را در مقابل یکدیگر در جنگ زمینی معین کرده است و رعایت آن‌ها را برای کشورها (اعم از بی‌طرف یا متخاصم) فرض دانسته است.

[2] عهدنامه سیزدهم لاهه مربوط به حقوق و تکالیف کشورهای بی‌طرف در جنگ دریایی است. البته شایان اشاره است، به‌طور کلی بی‌طرفی در جنگ دریایی دارای همان ویژگی‌ها و آثاری است که در جنگ زمینی بیان شده است. لذا حقوق بی‌طرفی در جنگ زمینی در اکثر موارد شامل بی‌طرفی در جنگ دریایی نیز می‌شود. به بیان بهتر، مقررات حاکم بر بی‌طرفی در جنگ دریایی مشتمل دو دسته قواعد است: یکی قواعد عام که همان قواعد بی‌طرفی در جنگ زمینی است؛ و دیگری قواعد خاص که صرفاً مربوط به جنگ دریایی می‌باشد (ضیایی بیگدلی (ب)، ۱۴۰۰: ۳۵۳).

[3] DoD Manual, para. 16.4 and Chapter 15; German Manual, paras. 1101–1155; AMW Manual, Sec. X.
راهنمای بریتانیا و سان‌رمو (San Remo Manual) بر تداوم اعتبار حقوق بی‌طرفی در سراسر اسناد تأکید دارند، در حالی که راهنمای کانادا فصل ۱۳ را به این موضوع اختصاص داده است. شایان ذکر است که دولت‌های بی‌طرف در برخی موارد، علی‌رغم وضعیت غیرمتخاصم خود، ملزم به رعایت حقوق مخاصمات مسلحانه هستند: ماده ۱۹ پروتکل الحاقی اوّل کنوانسیون‌های ژنو، ، ماده ٤ کنوانسیون اوّل ژنو؛ ماده ۵ کنوانسیون دوم ژنو.

[4] اعتبار مستمر اصول و قواعد اصلی حقوق بی‌طرفی در یک درگیری مسلحانه بین‌المللی که با استفاده از تسلیحات سنتی و جنبشی انجام می‌گیرد، بی‌تردید است. اما وقتی پای خصومت‌ها و اقدامات خصمانه‌ای که در فضای سایبر یا از طریق آن انجام می‌شوند به میان می‌آید، برخی ممکن است قابلیت اعمال این اصول را رد کنند. در واقع، اگر فضای سایبر به عنوان «بُعد پنجم» یا «قلمروی جهانی مشترک» که «در هیچ بُعد فیزیکی یا پیوستار زمانی–مکانی قابل اندازه‌گیری نیست» در نظر گرفته شود، دشوار خواهد بود که بر اعمال حقوق بی‌طرفی تأکید شود. با این حال، اگر بپذیریم که فضای سایبر «برای وجود داشتن نیازمند معماری فیزیکی است»، بسیاری از این دشواری‌ها قابل رفع خواهند بود (Heintschel von Heinegg, 2013: 143).

۱. تعاریف و مفاهیم کلی

با توجه به این‌که بررسی چارچوب حقوقی عملیات سایبری در بستر حقوق بی‌طرفی مستلزم درک مقدماتی از مفاهیم بنیادین آن است، این گفتار به طور اجمالی به تبیین کلیات و مفاهیم اساسی مرتبط با این حوزه اختصاص می‌یابد.

۱/۱. بی‌طرفی، دولت بی‌طرف، قلمرو بی‌طرف و زیرساخت سایبری بی‌طرف

«بی‌طرفی» که در کلمه لاتین «neuter» ریشه دارد و به معنای «هیچ‌کدام از هر دو طرف» است، در حقوق بین‌الملل به‌عنوان وضعیت دولتی تعریف می‌شود که در مخاصمه مسلحانه میان سایر دولت‌ها مشارکت[۱] ندارد (فِلِک، ۱۳۹۵: ۶۳۵). «دولت بی‌طرف» [۲] به دولتی اطلاق می‌شود که طرف مخاصمه مسلحانه بین‌المللی مورد نظر نیست. [۳] «قلمرو بی‌طرف» [٤] شامل قلمرو زمینی دولت‌های بی‌طرف، هم‌چنین آب‌هایی است که تحت حاکمیت سرزمینی آن‌ها قرار دارند (آب‌های داخلی؛ دریای سرزمینی؛ و در صورت وجود، آب‌های مجمع‌الجزایری) [٥] و فضای هوایی[٦] بالای این مناطق را نیز در بر می‌گیرد. [۷]

---

[۱] تفکیک میان مشارکت و بی‌طرفی یک تصمیم سیاسی، نه نظامی، است. جایی‌که بی‌طرفی مستلزم اتخاذ تصمیاتی توسط فرمانده نظامی باشد، دولت ذی‌ربط باید دستورالعملی سیاسی صادر کند و موضعی را که در ارتباط با یک مخاصمه خاص دارد، به‌نحو شفاف اعلام نماید (فلک، ۱۳۹۵: ٦٤٢).

[2] Neutral State.

[3] DoD Manual, para. 15.1.2.2; UK Manual, para. 12.11; Canadian Manual, para. 1302; German Manual, para. 1101; AMW Manual, Rule 1(aa); San Remo Manual, para. 13 (d); ICRC 2016 Geneva Convention I 1952 Commentary, para. 916.

[4] Neutral Territory.

[٥] آب‌های داخلی، آب‌های مجمع‌الجزایری و دریای سرزمینی دولت‌های بی‌طرف باید مورد احترام قرار گیرند (ماده ۱ کنوانسیون سیزدهم لاهه). دست یازیدن به هر اقدام جنگی در این آب‌ها ممنوع است (ماده ۲ کنوانسیون سیزدهم لاهه). طرف‌های مخاصمه از به‌کارگیری بنادر کشور بی‌طرف یا آب‌های سرزمینی به‌عنوان پایگاهی برای عملیات جنگی دریایی ممنوع شده‌اند (ماده ۵ کنوانسیون سیزدهم لاهه). لذا آب‌های سرزمینی کشور بی‌طرف از تعرض کشورهای متخاصم مصون است و این کشورها حق مبادرت به عملیات جنگی و حتی حرکت خصمانه را در آن‌ها ندارند. هرگونه عملی که موجب نقض این بی‌طرفی شود، کشور بی‌طرف را مجاز به مقابله کرده و می‌تواند مانع از بروز تخاصم در قلمرو دریایی خود شود. در این موقعیت، حتی توسل به زور و استفاده از نیروی نظامی از جانب کشور بی‌طرف مجاز بوده و به‌عنوان عمل خصمانه به‌حساب نمی‌آید (ضیایی بیگدلی (ب)، ۱٤۰۰: ۳٥٤).

[٦] به‌موجب ماده ٤۰ مقررات لاهه در مورد جنگ هوایی ۱۹۲۳، قلمرو هوایی دولت بی‌طرف غیرقابل نقض است. طرف‌های مخاصمه هم‌چنین از فرستادن هواپیمای نظامی، راکت یا سایر تکنولوژی‌های موشکی به قلمرو هوایی دولت بی‌طرف ممنوع شده‌اند.

[۷] برای نمونه منابع زیر را مشاهده نمایید:

«زیرساخت سایبری بی‌طرف» [1] نیز به زیرساخت سایبری عمومی یا خصوصی‌ای اطلاق می‌شود که در قلمرو بی‌طرف واقع شده باشد (از جمله زیرساخت سایبری غیرنظامی متعلق به یکی از طرف‌های مخاصمه یا اتباع آن طرف) یا تابعیت یک دولت بی‌طرف را داشته باشد (و در خارج از قلمرو متخاصم قرار گرفته باشد) (Tallinn Manual 2.0, 2017: 553).

۱/۲. اعمال حقوق متخاصمانه، اقدام خصمانه و عمل خصومت‌آمیز

اصطلاح «اعمال حقوق متخاصمانه» [2] مترادف با اصطلاح «اقدام خصمانه» [3] در کنوانسیون پنجم لاهه و «عمل خصومت‌آمیز» [4] در کنوانسیون سیزدهم لاهه است. [5] گروه بین‌المللی کارشناسان راهنمای تالین ۲ تصمیم گرفت از اصطلاح «حقوق متخاصمانه» [6] در فصل بیستم (حقوق بی‌طرفی) راهنما استفاده کند تا از سردرگمی با اصطلاح «اقدام خصمانه» که یک اصطلاح فنی عملیاتی است، جلوگیری شود. ازاین‌رو، اعمال حقوق متخاصمانه باید به معنای وسیع آن درک شود، یعنی اقداماتی که (از جمله عملیات سایبری) یک طرف مخاصمه در ارتباط با مخاصمه مجاز به انجام آن است. حقوق متخاصمانه محدود به «حملات» [7] به معنای تعریف‌شده در قاعده ۹۲ راهنمای تالین ۲ نیست؛ [8] بااین‌حال، باید توجه داشت که این اصطلاح شامل جاسوسی انجام‌شده علیه

German Manual, paras. 1108, 1118; AMW Manual, commentary accompanying Rule 166; San Remo Manual, para. 14.

[1] Neutral Cyber Infrastructure.

[2] Exercise of Belligerent Rights.

[3] Hostile Act.

[4] Act of Hostility.

[5] ماده ۱۰ کنوانسیون پنجم لاهه؛ ماده ۲ کنوانسیون سیزدهم لاهه؛ San Remo Manual, paras. 15–16.

[6] Belligerent Rights.

[7] Attacks.

[8] «حمله سایبری» یک اصطلاح جامع است که برای توصیف تهدیدی دیجیتالی به‌کار می‌رود. این تهدیدات از اکسپلویت‌ها (exploits) و بردارهای (vectors) مختلفی استفاده می‌کنند، اما همگی موجب زمان از کارافتادگی (downtime)، آسیب به داده‌ها، سرقت و نصب بدافزار می‌شوند. نوع تهدید، مراحل واکنش به حادثه را که برای ریشه‌کنی تهدید لازم است، تعیین می‌کند؛ اما هرگونه نفوذ نیازمند حضور متخصصان مناسب برای بررسی، مهار و رفع آسیب‌پذیری‌ها است (Proofpoint, n.d). از این‌رو در مورد تعریف حملات سایبری هیچ‌گونه اتفاق نظری وجود ندارد و این موضوع هم‌چنان بین دولت‌ها و سازمان‌های بین‌المللی مورد اختلاف است (اصلانی، رنجبریان، ۱۳۹٤: ۲۷۵). با وجود این، تعریف‌هایی از آن صورت گرفته است؛ در قاعده ۹۲ راهنمای تالین ۲ بدین‌گونه تعریف شده است: «حمله سایبری، عملیات سایبری تهاجمی یا تدافعی است که

دولت بی‌طرف نمی‌شود[۱] (Tallinn Manual 2.0, 2017 : 554-555)؛ زیرا جاسوسی که هدف از آن جمع‌آوری اطلاعاتِ معمولاً محرمانه، مهم و حساس دولت‌های دیگر است، در حقوق بین‌الملل برخلاف حقوق داخلی دولت‌ها ممنوع نشده است. به نظر می‌رسد علت این عدم ممنوعیت به حدی است که جاسوسی یا صِرف دخول در زیرساخت‌های سایبری به‌خودی‌خود و مستقیماً موجد خسارت و صدمه نیستند. به‌علاوه، به‌جرئت می‌توان گفت که تقریباً تمامی دولت‌ها این‌گونه اعمال را برای حفظ امنیت خود ضروری می‌دانند (شایگان، ۱۳۹۵: ۳٤۱).

۱٫۳. سایبر و فضای سایبر

واژه سایبر از لغت یونانی (کی‌برنتز) [۲] به معنی سکان‌دار یا راهنما مشتق شده است. نخستین‌بار این اصطلاح «سایبرنتیک» توسط ریاضی‌دانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹٤۸ به کار برده شده است. همچنین از این واژه به معنا و مفهوم مطالعه پیام‌ها، به‌ویژه بررسی کنترل مؤثر در قلمرو فیزیولوژیک و مهندسی یاد می‌شود (بیگلربیگی و عزیزی، ۱٤۰٤: ۲۲۰-۲۲۱). اما به‌طورکلی، فضای سایبر در اصل یک فضا و محیطی مشابه سایر حوزه‌های رقابتی همچون دریا، زمین و هوا است با یک تفاوت و آن هم این‌که این محیط برخلاف بقیه محیط‌ها ساخته دست بشر بوده، غیرملموس است (Libicki, 2009 : 11) و به‌طورکلی فضای سایبر منبعی برای تبادل اطلاعات تلقی می‌شود.

۱٫٤. فعالیت و عملیات سایبری

اصطلاحات «فعالیت سایبری» [۳] و «عملیات سایبری» [٤] مفاهیم عامی هستند و بسته به سیاق متن ممکن است معانی متفاوتی داشته باشند، اما در این نوشتار، به‌جای یکدیگر به

از آن به‌طور معقول انتظار مرگ یا صدمه به اشخاص و یا وارد کردن خسارت به اشیا می‌رود» (Tallinn Manual 2.0, 2017: 415).

[۱] در این‌سیاق، قاعده ۱۲۷ راهنمای تالین ۲ (استفاده نادرست از نشان‌های بی‌طرفی) بیان می‌دارد: «در عملیات‌های سایبری، استفاده از پرچم‌ها، نشان‌ها، علامت‌های نظامی یا یونیفرم‌های دولت‌های بی‌طرف یا دیگر دولت‌هایی که طرف درگیر در منازعه نیستند، ممنوع است». برای مطالعه بیشتر به تفاسیر قاعده ۱۲۷ راهنمای تالین ۲ مراجعه شود.

[2] Kybernetes.
[3] Cyber Activities.
[4] Cyber Operations.

کار رفته‌اند. چنانچه بخواهیم تعریفی یکپارچه از این دو اصطلاح ارائه دهیم، می‌توان گفت انواع مختلفی از فعالیت‌ها هستند که از فضای سایبر با هدف تأثیرگذاری بر اطلاعاتی که در قلمرو سایبری جریان دارند، استفاده می‌شوند (Tallinn Manual 2.0, 2017 : 564).

۲. عملیات سایبری در چارچوب حقوق بی‌طرفی در پرتو راهنمای تالین ۲

فناوری نقش مهمی در شکل‌گیری و تکوین هر قاعده حقوقی دارد. فناوری که زاده اختراع و یا عامل کشفی جدید قلمداد می‌شود، از آن جهت که به سرعت وارد زیست اجتماعی بشر می‌شود، مستلزم تمهید چارچوب حقوقی مناسب برای استفاده و مقابله با سوءاستفاده از آن است (زمانی، ۱۴۰۳: ۳۲۵).

در آغاز، بی‌طرفی در زمان جنگ را نباید با بی‌طرفی در زمان جنگ و صلح درهم آمیخت. در حالی که بی‌طرفی در زمان جنگ عموماً ناشی از اراده یک‌جانبه است، جنبه موقتی دارد و صرفاً دررابطه‌با یک مخاصمه مسلحانه جاری است؛ بی‌طرفی در زمان جنگ و صلح وضعیتی است که از سوی یک کشور اعلام‌شده، حالت دائمی دارد[1] و در قبال همه مخاصمات مسلحانه مجرا است. بنابراین، هدف مورد نظر در این سلسله مباحث، صرفاً بی‌طرفی در زمان جنگ است؛ هرچند کشورهایی که در وضعیت بی‌طرفی دائم هستند نیز مشمول آن رفتار هستند (ضیایی بیگدلی (ب)، ۱۴۰۰: ۳۲۳).

افزون بر این، گروه بین‌المللی کارشناسان راهنمای تالین ۲ با درنظرداشتن این واقعیت که حقوق بی‌طرفی بر پایه وضعیت‌هایی شکل گرفته است که ورود به قلمرو یک دولت بی‌طرف یا خروج از آن یک اقدام فیزیکی تلقی می‌شده، به بررسی موضوع حقوق بی‌طرفی در فضای سایبر پرداخته است. این در حالی است که فضای سایبر با فراهم‌آوردن اتصال جهانی بدون توجه به مرزهای ژئوپلیتیکی، برخی از فرض‌های اساسیِ حقوق بی‌طرفی را به چالش می‌کشد. برای نمونه، یک پیام ایمیل که از قلمرو متخاصم ارسال می‌شود، ممکن است به‌صورت خودکار از طریق زیرساخت سایبری یک دولت بی‌طرف هدایت شود تا به

[1] بی‌طرفی دائمی وضعیتی است که در زمان صلح یک دولت قانوناً بر بی‌طرف ماندن در یک مخاصمه مسلحانه میان دو دولت دیگر تعهد می‌کند. وضعیت فوق مستلزم این است که دولت بی‌طرف در زمان صلح هیچ تعهد نظامی نپذیرد و از اعمالی که موجب عدم‌امکان انجام تعهداتش طبق حقوق بی‌طرفی می‌شود، اجتناب ورزد. هنگامی که مخاصمه مسلحانه رخ دهد، باید میان تکلیف قانونی بر بی‌طرف ماندن و خط‌مشی (سیاست) بی‌طرفی تفکیک قائل شد (فلک، ۱۳۹۵: ٦٤٣).

مقصد نهایی برسد؛ در این میان، فرستنده یا مالک زیرساخت سایبری بی‌طرف، الزاماً کنترلی بر مسیر طی‌شده ندارد. لذا قواعد ارائه‌شده در این فصل از راهنمای تالین ۲، با در نظر گرفتن این واقعیت تنظیم شده‌اند. همچنین، با توجه به دشواری در کنترل زیرساخت‌ها و مسیرهای سایبری، هرگونه نتیجه‌گیری در خصوص نقض بی‌طرفی یک دولت یا این‌که آیا یک دولت بی‌طرف تعهدات خود تحت حقوق بی‌طرفی را نقض کرده است، باید تنها پس از بررسی دقیق صورت گیرد؛ چراکه زیرساخت سایبری واقع در قلمرو یک دولت بی‌طرف نه‌تنها تحت صلاحیت آن دولت قرار دارد، بلکه تحت حمایت حاکمیت سرزمینی آن نیز قرار می‌گیرد. چنین زیرساختی، صرف‌نظر از آنکه مالکیت آن عمومی یا خصوصی باشد و صرف‌نظر از تابعیت مالکان، دارای ماهیت بی‌طرف تلقی می‌شود (مشروط بر آنکه برای اعمال حقوق متخاصمانه مورداستفاده قرار نگیرد) [۱] (Tallinn Manual 2.0, 2017: 554).

بنابراین، عملیات سایبری در فضای سایبر، حقوق بی‌طرفی را با سؤال‌ها و چالش‌هایی روبرو می‌سازد. ازاین‌رو در ادامه، با توجه به این‌که راهنمای تالین ۲ تحلیل حقوقی عملیات سایبری در چارچوب حقوق بی‌طرفی را در قالب پنج محور اصلی سامان‌دهی کرده است، ساختار این نوشتار نیز به‌صورت تطبیقی و در هماهنگی با همان چارچوب، در پنج بخش بررسی خواهد شد: نخست، «حمایت از زیرساخت سایبری بی‌طرف»؛ دوم، «عملیات سایبری در قلمرو بی‌طرف»؛ سوم، «تعهدات دولت بی‌طرف»؛ چهارم، «واکنش طرف‌های مخاصمه به نقض بی‌طرفی»؛ و پنجم، «بی‌طرفی و اقدامات شورای امنیت». این شیوه تقسیم‌بندی، ضمن حفظ انسجام مفهومی با راهنمای تالین ۲، امکان تحلیل تطبیقی دقیق‌تر و منسجم‌تری از الزامات حقوقی عملیات سایبری در چارچوب حقوق بی‌طرفی را فراهم می‌آورد.

۲/۱. حمایت از زیرساخت سایبری بی‌طرف

یکی از اصول تثبیت‌شده در حقوق بی‌طرفی آن است که طرف‌های مخاصمه از انجام اقدامات خصمانه در قلمرو بی‌طرف ممنوع هستند. مصونیت قلمرو بی‌طرف در ماده ۱

[۱] قاعده ۱۵۳ راهنمای تالین ۲ در این راستا بیان می‌دارد: «چنان‌چه یک دولت بی‌طرف در متوقف ساختن اعمال حقوق متخاصمانه در قلمرو خود قصور ورزد، طرف متضرر در مخاصمه می‌تواند اقداماتی، از جمله از طریق عملیات سایبری، اتخاذ کند که برای مقابله با آن رفتار لازم و ضروری باشد».

کنوانسیون پنجم لاهه و ماده ۱ کنوانسیون سیزدهم لاهه تصریح شده است و دارای ماهیت عرفی است. [۱] لذا زیرساخت سایبری بی‌طرف که به‌صورت فیزیکی در فضای هوایی بین‌المللی، مناطق دریای آزاد یا فضای ماورای جو قرار دارد، به‌موجب حاکمیت دولت متبوع آن موردحمایت قرار می‌گیرد[۲] (Tallinn Manual 2.0, 2017 : 555). در این راستا، مهم نیست که زیرساخت سایبری در مالکیت یا استفاده انحصاری دولت، شرکت‌ها یا اشخاص خصوصی باشد. همچنین، حمایت از این زیرساخت‌ها وابسته به تابعیت مالک آن‌ها نیست. با توجه به اصل مصونیت حاکمیتی، همین میزان حمایت نسبت به زیرساخت‌های سایبری موجود بر روی کشتی‌ها و هواپیماهای دولتی دولت بی‌طرف یا در اماکن دیپلماتیک نیز اعمال می‌شود (Heintschel von Heinegg, 2013 : 145).

علاوه بر این، ماهیت غیرقابل‌نقض قلمرو دولت بی‌طرف مستلزم این نکته نیز است که دولت‌های بی‌طرف نباید تحت‌تأثیر آثار تبعی عملیات مسلحانه قرار بگیرند. طرف‌های متخاصم حق تعرض به قلمرو دولت بی‌طرف به واسطه عملیات جنگی خود را ندارند. بنابراین، هیچ قاعده‌ای دائر بر مقبولیت ایراد ضرر و زیان تبعی به دولت بی‌طرف وجود ندارد. اگر تأثیر حملات مسلحانه‌ای که مستقیماً علیه اهداف موردنظر در سرزمین دولت طرف مخاصمه صورت می‌گیرد در قلمرو دولت بی‌طرف نیز محسوس باشد، این اقدامات غیرقانونی هستند (فِلِک، ۱۳۹۵: ۶۴۰-۶۵۰).

در این سیاق، اوّلین قاعده از این فصل راهنمای تالین ۲، یعنی قاعده ۱۵۰، بیان می‌دارد: «اعمال حقوق متخاصمانه از طریق ابزارهای سایبری که علیه زیرساخت سایبری بی‌طرف باشد، ممنوع است». در توضیح این قاعده باید بیان داشت، اصطلاح «علیه» [۳] به عملیاتی اطلاق می‌شود که با هدف واردآوردن اثرات زیان‌بار بر زیرساخت سایبری بی‌طرف

---

[1] DoD Manual, para. 15.3.1.1; UK Manual, para. 1.43; German Manual, paras. 1108, 1118, 1149; San Remo Manual, para. 15; Hague Air Warfare Rules, Arts. 39–40.

[۲] چنان‌که قاضی مکس هوبر در رأی داوری جزایر پالماس بیان کرده است: «حاکمیت در روابط میان دولت‌ها به‌معنای استقلال است. استقلال نسبت به بخشی از کره زمین، عبارت از حق اِعمال وظایف یک دولت در آن ناحیه، به‌طور انحصاری از سایر دولت‌ها، است». (Permanent Court of Arbitration, 1928: 8). هم‌چنین دیوان بین‌المللی دادگستری در قضیه کورفو تأکید کرده است که: «در روابط میان دولت‌های مستقل، احترام به حاکمیت سرزمینی، بنیان اساسی روابط بین‌الملل به شمار می‌رود» (ICJ, 1949: 35).

[3] Directed Against.

انجام می‌گیرد. [۱] البته گروه بین‌المللی کارشناسان راهنمای تالین ۲ در مواجهه با وضعیتی که طی آن یک حمله سایبری[۲] علیه یک هدف نظامی در قلمرو متخاصم دارای اثرات ناخواسته‌ای در قلمرو بی‌طرف باشد، با چالش‌هایی مواجه شد. برای نمونه، یک حمله سایبری به سروری در قلمرو متخاصم ممکن است به طور قابل‌توجهی بر خدمات ارائه‌شده در قلمرو بی‌طرف تأثیر بگذارد. کارشناسان توافق داشتند که اگر این اثرات قابل‌پیش‌بینی[۳] نباشند، حمله مزبور ناقض حقوق بی‌طرفی محسوب نمی‌شود. در مورد اثرات قابل‌پیش‌بینی، گروه کارشناسان بین‌المللی خاطرنشان کرد که حقوق بی‌طرفی در پی ایجاد توازنی میان حق طرف‌های متخاصم برای انجام مؤثر عملیات نظامی و حق دولت‌های بی‌طرف برای مصون‌ماندن کلی از آثار مخاصمه است. هر مورد باید به‌صورت مستقل و بر پایه ارزیابی این حقوق متعارض بررسی شود. کارشناسان توافق داشتند که اثرات وارد بر دولت بی‌طرف که در این ارزیابی باید مدنظر قرار گیرد، صرفاً محدود به اثرات فیزیکی نیست. آنان همچنین توافق داشتند که دولت‌ها در عمل بعید است اثرات جزئی و ناچیز[٤] را مانعی برای انجام حمله‌ای که در غیر این صورت مشروع تلقی می‌شود، به شمار آورند (Tallinn Manual 2.0, 2017 : 555).

البته همان‌طور که پیش‌تر ذکر شد، صرف نفوذ به زیرساخت سایبری دولت بی‌طرف مشمول این ممنوعیت نمی‌شود، زیرا حقوق بین‌الملل، جاسوسی را ممنوع نکرده است. بااین‌حال، باید در نظر داشت که اصل حاکمیت سرزمینی شامل ممنوعیت اعمال صلاحیت در قلمرو دولت خارجی نیز می‌شود؛ بنابراین، یک عملیات سایبری که به‌عنوان

---

[۱] در مورد عملیات‌هایی که از چنین زیرساختی عبور می‌کنند یا از آن برای انجام عملیات علیه دشمن استفاده می‌شود، به قاعده ۱۵۱ راهنمای تالین ۲ مراجعه شود.

[۲] ممنوعیت مداخله زیان‌بار در زیرساخت‌های سایبری دولت‌های بی‌طرف محدود به حملات سایبری به‌معنای مضیق کلمه نیست؛ یعنی محدود به عملیات‌های سایبری‌ای که موجب یا متضمن ایجاد خسارت، تخریب، مرگ یا جراحت باشند، نمی‌گردد. بلکه این ممنوعیت شامل تمام فعالیت‌ها، اعم از جنبشی یا سایبری، می‌شود که یا تأثیر منفی بر کارکرد این زیرساخت‌ها داشته باشند یا استفاده از آن‌ها را ناممکن سازند. به بیان دیگر، انجام «استفاده از توانمندی‌های مبتنی بر شبکه برای مختل کردن، انکار، تضعیف، دست‌کاری یا نابودی اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای، یا خود رایانه‌ها و شبکه‌ها»ی یک دولت بی‌طرف، ممنوع است (Heintschel von Heinegg, 2013: 145-146).

[3] Foreseeable.

[4] *de minimis.*

اعمال صلاحیت تلقی شود، نقض حاکمیت دولت هدف خواهد بود. این ممنوعیت ماهیتی عام دارد و در نتیجه بخشی از حقوق بی‌طرفی به معنای دقیق کلمه[1] محسوب نمی‌شود (Heintschel von Heinegg, 2013 : 146).

در پایان شایان توجه است، زیرساخت سایبری بی‌طرف واقع در قلمرو بی‌طرف ممکن است در صورت تحقق شرایط مندرج در قاعده ۱۵۳ راهنمای تالین ۲[2]، حمایت خود را از دست بدهد. [3] افزون بر این، زیرساخت سایبری بی‌طرفی که خارج از قلمرو بی‌طرف قرار دارد، برای مثال کابل‌های زیردریایی، در صورتی که یک هدف نظامی مشروع محسوب شود، ممکن است مورد حمله قرار گیرد. چنین زیرساختی همچنین می‌تواند موضوع توقیف واقع شود (Tallinn Manual 2.0, 2017 : 556).

۲٫۲. عملیات سایبری در قلمرو بی‌طرف

وظایف عدم مشارکت و بی‌طرفی نتیجه قهری و ضروری حق بر مصون‌ماندن از آثار سوء مخاصمه است. لذا تعهد به عدم مشارکت به این معنا است که هر دولت باید از حمایت یک طرف مخاصمه خودداری کند. وظیفه حمایت نکردن، همچنین این معنا را دارد که دولت بی‌طرف متعهد است که به یک طرف مخاصمه اجازه استفاده از منابع خویش را به‌رغم رضایت دیگر طرف مخاصمه ندهد (فِلِک، ۱۳۹۵: ۶۳۸). این اصل، برخاسته از اصل بنیادین برابری حاکمیت دولت‌ها در حقوق بین‌الملل است و به‌موجب آن، هرگونه اعمال صلاحیت یک‌جانبه در قلمرو سرزمینی دولت دیگر، ممنوع و فاقد مشروعیت تلقی می‌شود. [4] در این سیاق، قاعده ۱۵۱ راهنمای تالین ۲ بیان می‌دارد: «اعمال حقوق متخاصمانه از طریق ابزارهای سایبری در قلمرو بی‌طرف، ممنوع است».

---

[1] *strictu sensu*.

[2] در ادامه، در بخش واکنش طرف‌های مخاصمه به نقض بی‌طرفی، به این مبحث پرداخته شده است.

[3] برای نمونه، یک دولت بی‌طرف نباید به طرف مخاصمه کمک کند. این دولت خصوصاً از ارائه کشتی‌های جنگی، مهمات یا سایر اقلام جنگی منع شده است (ماده ٦ کنوانسیون سیزدهم لاهه). البته کمک بشردوستانه به قربانیان جنگی به‌منزله نقض بی‌طرفی نیست، حتی جایی‌که فقط به نفع یک طرف درگیر در مخاصمه انجام پذیرد (ماده ١٤ کنوانسیون چهارم لاهه).

[4] در این‌خصوص دیوان دائمی بین‌المللی دادگستری در قضیه لوتوس بیان داشت: «نخستین و مهم‌ترین محدودیتی که حقوق بین‌الملل بر یک کشور تحمیل می‌کند این است که - در غیاب یک قاعده‌ی مجازکننده که خلاف آن را تصریح کند - یک کشور نمی‌تواند قدرت خود را به هیچ شکلی در قلمرو کشور دیگر اعمال کند. از این منظر، صلاحیت (قضایی یا حاکمیتی) بدون تردید ماهیتی سرزمینی دارد؛ یعنی یک کشور نمی‌تواند صلاحیت خود را خارج از قلمرو سرزمینی‌اش اعمال کند، مگر بر اساس

در توضیح باید بیان داشت، این قاعده بر مواد ۲ و ۳ کنوانسیون پنجم لاهه و مواد ۲ و ۵ کنوانسیون سیزدهم لاهه استوار است و بازتاب‌دهنده حقوق بین‌الملل عرفی است. [۱] درحالی‌که قاعده پیش‌گفته (قاعده ۱۵۰) به عملیات علیه زیرساخت سایبری بی‌طرف می‌پردازد، این قاعده ناظر بر استفاده از چنین زیرساختی در قلمرو بی‌طرف توسط یکی از طرف‌های مخاصمه است. [۲] این قاعده نیروهای مسلح یکی از طرف‌های مخاصمه را از انجام عملیات سایبری از قلمرو بی‌طرف منع می‌کند. علاوه بر انجام عملیات سایبری از درون قلمرو بی‌طرف، این قاعده شامل به دست‌گرفتن کنترل از راه دور زیرساخت سایبری بی‌طرف و استفاده از آن برای مقاصد پیش‌گفته نیز می‌شود. بااین‌حال، این قاعده در مورد اشخاص خصوصی (از جمله غیرنظامیانی که مستقیماً در مخاصمات مشارکت دارند) [۳]، نهادها[٤] یا گروه‌ها[٥] قابل‌اجرا نیست، مگر آنکه رفتار آن‌ها به یکی از طرف‌های مخاصمه مسلحانه بین‌المللی قابل‌انتساب باشد[٦] (Tallinn Manual 2.0, 2017 : 556).

ازسوی‌دیگر، اگرچه این قاعده صرفاً به اعمال حقوق متخاصمانه در قلمرو بی‌طرف می‌پردازد، استفاده از زیرساخت سایبری دولتیِ غیرتجاریِ متعلق به دولت بی‌طرف که در خارج از قلمرو بی‌طرف واقع شده باشد (اما نه در قلمرو متخاصم)، برای اهداف

یک قاعده‌ی مجازکننده که از عرف بین‌المللی یا از یک معاهده نشأت گرفته باشد» (PCIJ, 1927:18-19). هم‌چنین در این‌خصوص رجوع کنید به پرونده مناطق آزاد بالای ساوری و ژِکس مطروح در دیوان دائمی بین‌المللی دادگستری، صفحات ۱٦٨-۱٦٦.

[1] DoD Manual, para. 15.3.1.2; UK Manual, para. 1.43.b; Canadian Manual, para. 1304; German Manual, paras. 1108, 1120, 1150; AMW Manual, Rule 167(a) and accompanying commentary; San Remo Manual, para. 15.

[۲] درخصوص عبور ناوهای جنگی متخاصم از دریای سرزمینی یک دولت بی‌طرف، به قاعده ٤۹ راهنمای تالین ۲ (عملیات‌های سایبری در دریای سرزمینی در طول مخاصمه مسلحانه) با عنوان «عبور صِرف» (mere passage) مراجعه شود. هم‌چنین ملهم از ماده ۱۰ کنوانسیون سیزدهم لاهه، عبور بی‌ضرر از آب‌های سرزمینی و آب‌های مجمع‌الجزایری یک دولت بی‌طرف با کشتی‌های متعلق به یک طرف درگیر جنگ و غنائم گرفته‌شده توسط یک طرف مخاصمه، نقض اصل بی‌طرف نیست. در حالی که عبور از خطوط کشتی‌رانی مجمع‌الجزایری شامل حق پرواز در مواد ۳۸ و ۵۳ کنوانسیون حقوق دریاها می‌شود، حق عبور بی‌ضرر زیر دریایی، خارج از محدوده آبراه‌های بین‌المللی وجود ندارد.

[۳] مطابق با آنچه در قاعده ۹۷ راهنمای تالین ۲ (غیرنظامیانی که مستقیماً در مخاصمات مشارکت می‌کنند) بیان شده است.

[4] Entities.

[5] Groups.

[٦] مواد ٤ و ۸ پیش‌نویس مواد راجع به مسئولیت دولت‌ها برای افعال متخلفانه بین‌المللی دولت ۲۰۰۱؛ قواعد ۱۵ (انتساب عملیات‌های سایبری توسط ارگان‌های دولتی) و ۱۷ راهنمای تالین ۲ (انتساب عملیات‌های سایبری توسط بازیگران غیردولتی).

متخاصمانه نیز نقض بی‌طرفی محسوب می‌شود. [1] برای مثال، ارسال ارتباطات نظامی از طریق سامانه‌های سایبری مستقر در کشتی‌های دولتی یا هواپیماهای دولتی یک دولت بی‌طرف ممنوع است؛ چراکه این سکوها از مصونیت حاکمیتی[2] برخوردارند. به‌علاوه، استفاده از یک شبکه عمومی، بین‌المللی و آزاد مانند اینترنت برای اهداف نظامی، ناقض حقوق بی‌طرفی محسوب نمی‌شود؛ حتی اگر این شبکه، یا اجزایی از آن، در قلمرو بی‌طرف واقع شده باشد. [3] اگرچه هیچ مقرره صریحی در معاهدات به طور مستقیم به این موضوع نپرداخته است، اکثریت گروه بین‌المللی کارشناسان راهنمای تالین ۲ توافق داشتند که ماده ۸ کنوانسیون پنجم لاهه[4] قابل تسری به سامانه‌های ارتباطات سایبری نیز هست. آنان همچنین توافق داشتند که این ماده بازتاب‌دهنده حقوق بین‌الملل عرفی است. [5] بااین‌حال، اقلیتی از کارشناسان بر این باور بودند که ماده ۸ تنها به ابزارهای صراحتاً پیش‌گفته در آن محدود می‌شود و استفاده از سایر ابزارهای ارتباطات سایبری از طریق قلمرو بی‌طرف را ممنوع می‌دانستند (همان: ۵۵۶-۵۵۷).

همچنین گروه بین‌المللی کارشناسان راهنمای تالین ۲ موضوع انتقال سلاح‌های سایبری[6] از طریق قلمرو بی‌طرف را مورد بررسی قرار داد. کارشناسان توافق داشتند که

---

[1] با قطعیت نمی‌توان گفت که این ممنوعیت شامل استفاده از زیرساخت سایبری متعلق به یک شرکت خصوصی یا فردی که در خارج از قلمرو دولت بی‌طرف واقع شده نیز می‌شود. با این حال، در چنین وضعیتی، این زیرساخت سایبری می‌تواند به‌عنوان عامل مشارکت در اقدامات نظامی دشمن تلقی گردد و دشمن متخاصم حق خواهد داشت آن را به‌عنوان یک هدف نظامی مشروع مورد حمله قرار دهد (Heintschel von Heinegg, 2013: 146-147).

[2] قاعده ۵ راهنمای تالین ۲ (مصونیت حاکمیتی و غیرقابل تعرض بودن) در این‌خصوص بیان می‌دارد: «هرگونه مداخله یک دولت در زیرساخت سایبری موجود در یک سکو (platform) – در هر مکانی که قرار داشته باشد – که از مصونیت حاکمیتی برخوردار است، نقض حاکمیت تلقی می‌شود».

[3] البته دولت بی‌طرف نباید استقرار یا استفاده از وسایل ارتباطی ویژه‌ای را برای طرف مخاصمه اجازه دهد (ماده ۳ کنوانسیون پنجم لاهه).

[4] ماده ۸ کنوانسیون پنجم لاهه مقرر می‌دارد که یک قدرت بی‌طرف ملزم نیست استفاده از کابل‌های تلگراف یا تلفن یا تجهیزات بی‌سیم متعلق به خود یا شرکت‌ها یا اشخاص خصوصی را به نمایندگی از طرف‌های مخاصمه ممنوع یا محدود کند.

[5] گروه بین‌المللی کارشناسان راهنمای تالین ۲ به منابع زیر اشاره می‌نمایند:

DoD Manual, para. 16.4.1; AMW Manual, Rule 167(b).

[6] مطابق با قاعده ۱۰۳ راهنمای تالین ۲ (تعاریف ابزار و روش‌های جنگ) که بیان می‌دارد: «برای مقاصد این راهنما: الف) «ابزار جنگ سایبری» شامل سلاح‌های سایبری و سامانه‌های سایبری مرتبط با آن‌ها هستند؛ و ب) «روش‌های جنگ سایبری» شامل تاکتیک‌ها، تکنیک‌ها و رویه‌های سایبری هستند که از طریق آن‌ها خصومت‌ها هدایت می‌شوند».

انتقال فیزیکی سلاح‌های سایبری، بر اساس ماده ۲ کنوانسیون پنجم لاهه که عبور مهمات جنگی یا تدارکات از قلمرو یک قدرت بی‌طرف را ممنوع می‌سازد، ممنوع است. [۱] در این راستا، اکثریت کارشناسان بر این نظر بودند که انتقال سلاح‌های سایبری از طریق زیرساخت سایبری واقع در قلمرو یک دولت بی‌طرف نیز بر اساس ماده پیش‌گفته ممنوع است. [۲] آنان خاطرنشان کردند که بدافزارها[3] هنگام انتقال ممکن است به بسته‌هایی[4] تقسیم شوند، اما دلیلی برای تمایز میان انتقال یک سلاح سایبری کامل و انتقال آن به‌صورت بسته‌بندی‌شده وجود ندارد؛ چراکه انتقال اجزای منفرد یک سلاح متعارف نیز ناقض بی‌طرفی محسوب می‌شود. بااین‌حال، کارشناسان هشدار دادند که تعهد دولت بی‌طرف به اقدام برای جلوگیری از چنین انتقالی تنها زمانی ایجاد می‌شود که آن دولت از وقوع انتقال آگاه[5] باشد و بتواند اقداماتی برای متوقف‌سازی آن انجام دهد. [٦] بااین‌حال، اقلیتی از کارشناسان با استناد به ماده ۸ کنوانسیون پنجم لاهه، آن را به‌عنوان استثنایی صریح بر قاعده کلی تلقی کردند. [۷] این کارشناسان با کاربرد قیاسی[8] ماده ۲ در خصوص انتقال داده، حتی در صورتی که آن داده به‌عنوان سلاح سایبری تلقی شود، مخالفت کردند؛ زیرا به باور آنان موضوع و هدف از ماده ۲ صرفاً جلوگیری از انتقال فیزیکی سلاح‌هاست، همان‌گونه که درج ماده ۸ در این کنوانسیون نیز مؤید آن است[۹] (همان: ۵۵۷).

---

[۱] دولت بی‌طرف می‌تواند اجازه عبور مجروحان و کالاهای امدادی را صادر کند (ماده ١٤ کنوانسیون پنجم لاهه).

[۲] به‌عنوان نمونه، چنان‌چه کشتی تحت پرچم یکی از دولت‌های متخاصم، ضمن عبور از آب‌های سرزمینی یک دولت بی‌طرف، اقدام به انتقال یا هدایت یک سلاح سایبری از طریق زیرساخت‌های سایبری مستقر در قلمرو آن دولت بی‌طرف نماید، این امر نقض صریح قواعد حقوق بی‌طرفی محسوب خواهد شد.

[3] Malware.
[4] Packets.
[5] Knowledge.

[٦] مطابق با قاعده ۱۵۲ راهنمای تالین ۲.

[۷] این دیدگاه در منابع زیر پذیرفته شده است:

AMW Manual, commentary accompanying Rule 167(b); DoD Manual, para. 16.4.1.

[8] Analogous.

[۹] دستورالعمل HPCR میان ارتباطات صرف از یک‌سو و انتقال تسلیحات سایبری از سوی دیگر، تمایزی قائل نمی‌شود. عبارت «استفاده برای اهداف نظامی» به‌اندازه کافی گسترده است تا هر دو مورد را در بر گیرد. این برداشت به‌نظر می‌رسد تطبیقی معقول از قواعد سنتی حقوق بی‌طرفی به فضای سایبر باشد. با توجه به پیچیدگی و وابستگی متقابل شبکه‌های معاصر، مانند اینترنت، اعمال کنترل لازم برای مداخله مؤثر در ارتباطات از طریق چنین شبکه‌هایی غیرممکن است. این امر با این واقعیت برجسته

درنهایت، گروه بین‌المللی کارشناسان توافق داشتند که یک دولت بی‌طرف می‌تواند استفاده از زیرساخت سایبری خود توسط طرف‌های مخاصمه را محدود یا ممنوع کند. در صورت اتخاذ چنین تدابیری، این اقدامات باید به‌صورت بدون تبعیض نسبت به تمامی طرف‌های مخاصمه اعمال شود[1] (همان: ۵۵۸).

۲/۳. تعهدات دولت بی‌طرف

حقوق بی‌طرفی، با توجه به موضوع و هدف خود، نه‌تنها تعهداتی را برای طرف‌های متخاصم، بلکه برای کشورهای بی‌طرف نیز ایجاد می‌کند. تکالیف کشور بی‌طرف تابع ضرورت مضاعف خودداری از مداخله در درگیری و عدم‌جانبداری از طرف‌های درگیر است. عدم رعایت اصول دوگانه پیش‌گفته از سوی کشور بی‌طرف، صرفاً نقض بی‌طرفی نیست، بلکه می‌تواند آن کشور را خواسته یا ناخواسته وارد درگیری کرده و او را در جرگه طرف‌های

می‌شود که اکثر این ارتباطات معمولاً نه قابل ردیابی‌اند و نه قابل پیش‌بینی، چراکه از طریق خطوط ارتباطی و مسیریاب‌هایی که از کشورهای مختلف عبور می‌کنند، به مقصد نهایی خود می‌رسند. با در نظر گرفتن این واقعیت‌ها، مطابق این دیدگاه، صرف این‌که ارتباطات نظامی، از جمله حملات سایبری، از طریق زیرساخت سایبری یک دولت بی‌طرف منتقل شده باشند، نقض تعهدات بی‌طرفی آن دولت محسوب نمی‌شود. اگرچه رویکرد راهنمای HPCR برای هر دو دسته از دولت‌های متخاصم و بی‌طرف جذاب به‌نظر می‌رسد، با این حال اذعان می‌شود که مشخص نیست چنین انطباق دور از انتظاری از ماده ۸ با عملیات‌های سایبری انجام‌شده برای مقاصد نظامی، در نهایت به‌عنوان بازتابی از حقوق بین‌الملل عرفی معاصر پذیرفته شود. رویه دولت‌ها در دوران مدرن، به‌ویژه عملیات‌های سایبری در جریان کمپین کوزوو در سال ۱۹۹۹، درگیری‌های افغانستان (۲۰۰۱) و عراق (۲۰۰۳) و منازعه مسلحانه میان گرجستان و روسیه (۲۰۰۷)، شواهد کافی برای اثبات این‌که یک عملیات سایبری، از جمله انتقال تسلیحات سایبری از طریق زیرساخت سایبری بی‌طرف، ناقض بی‌طرفی دولت‌هایی که انتقال از طریق قلمرو آن‌ها انجام شده نیست، ارائه نمی‌دهد. اوّل، هیچ اطلاعات منبع‌باز مشخصی وجود ندارد که نشان دهد این عملیات‌های سایبری معادل با حملات سایبری بوده‌اند یا از طریق زیرساخت‌های سایبری بی‌طرف هدایت شده‌اند. دوم، حملات محروم‌سازی از سرویس علیه گرجستان، به‌معنای دقیق کلمه حملات سایبری (*strictu sensu*) محسوب نمی‌شوند و بنابراین نمی‌توان آن‌ها را با عبور «مهمات جنگی» موضوع ماده ۲ کنوانسیون پنجم لاهه همسان دانست. از سوی دیگر، گزارش سیاست فضای سایبر وزارت دفاع ایالات متحد آمریکا (DoD) نشان می‌دهد که ایالات متحد آمریکا هرگونه «فعالیت سایبری مخرب» را ناقض حقوق بی‌طرفی تلقی می‌کند، صرف‌نظر از این‌که این فعالیت‌ها از زیرساخت‌های سایبری یک کشور ثالث بی‌طرف منشأ گرفته یا صرفاً از آن عبور کرده باشند (Heintschel von Heinegg, 2013: 149).

[1] ماده ۹ (۱) کنوانسیون پنجم لاهه؛ DoD Manual, para. 16.4.1. البته شایان اشاره است، وظیفه بی‌طرفی به این معنا نیست که دولت بی‌طرف ملزم به رفتار دقیقاً همسان با متخاصمان است، بلکه رفتار تبعیض‌آمیز ممنوع است. به‌طور مثال دولت بی‌طرف تنها از آن رفتار متفاوت با متخاصمان منع شده که با توجه به مسئله خاص مخاصمه مسلحانه توجیه‌ناپذیر است (فلک، ۱۳۹۵: ۶۳۸).

درگیری قرار دهد (ضیایی بیگدلی (الف)، ۱٤۰۰: ۳۲٤). امروزه دیگر بی‌طرفی دوستانه یا خیرخواهانه که بعضاً «بی‌طرفی تفاضلی» نامیده می‌شد، مورد پذیرش نیست، بی‌طرفی دوستانه حاکی از رجحان یکی از متخاصمان بر دیگری از سوی کشور بی‌طرف است یا گرایش دوستانه کشور بی‌طرف نسبت به یکی از متخاصمان است. لذا یکی از روش‌های خاتمه وضعیت بی‌طرفی، زمانی است که کشور بی‌طرف به تعهدات بی‌طرفی خود عمل نکند یا در موقعیت دفاع از بی‌طرفی خود نباشد. در نتیجه، قلمرو آن کشور، عملاً به صحنه عملیات جنگی تبدیل می‌شود (ضیایی بیگدلی (ب)، ۱٤۰۰: ۳٤۰ و ۳٤٤).

ازاین‌رو قاعده ۱۵۲ راهنمای تالین ۲ در این‌خصوص مقرر می‌دارد: «یک دولت بی‌طرف نباید با آگاهی، اجازه دهد که طرف‌های مخاصمه از طریق زیرساخت سایبری واقع در قلمرو آن یا تحت کنترل انحصاری‌اش، به اعمال حقوق متخاصمانه بپردازند». در توضیح باید بیان داشت، این قاعده که بازتاب‌دهنده حقوق بین‌الملل عرفی است، [1] برگرفته از ماده ۵ کنوانسیون پنجم لاهه می‌باشد که طبق آن «قدرت بی‌طرف نباید اجازه دهد هیچ‌یک از اقدامات مندرج در مواد ۲ تا ۴ در قلمرو آن رخ دهد». در زمینه عملیات سایبری، توجه به این نکته حائز اهمیت است که ماده ۳ کنوانسیون پنجم لاهه مقرر می‌دارد که: «طرف‌های متخاصم از انجام اقدامات زیر منع شده‌اند: الف) احداث ایستگاه تلگراف بی‌سیم یا دستگاهی دیگر در قلمرو یک قدرت بی‌طرف به‌منظور ارتباط با نیروهای متخاصم در خشکی یا دریا؛ ب) استفاده از چنین تأسیساتی که پیش از جنگ در قلمرو قدرت بی‌طرف توسط آن‌ها ایجاد شده و صرفاً برای مقاصد نظامی به‌کار گرفته می‌شود، مشروط بر آن‌که این تأسیسات برای ارائه خدمات عمومی پیام‌رسانی افتتاح نشده باشد». لذا با تطبیق موضوع و هدف کنوانسیون پنجم لاهه با عملیات سایبری، یک دولت بی‌طرف نباید اجازه دهد که یکی از طرف‌های مخاصمه از زیرساخت سایبری پیش‌موجود [2] خود در قلمرو بی‌طرف برای مقاصد نظامی استفاده کند یا هرگونه زیرساخت سایبری جدیدی را برای آن مقاصد ایجاد نماید (Tallinn Manual 2.0, 2017 : 558).

---

[1] DoD Manual, para. 15.3.2; UK Manual, para. 1.43.a; German Manual, para. 1111; AMW Manual, Rule 168(a); San Remo Manual, para. 22.

هم‌چنین درخصوص این مسئله در زمان صلح، به قاعده ٦ راهنمای تالین ۲ (مراقبت مقتضی) رجوع شود.

[2] Pre-Existing.

تعهد مندرج در این قاعده نه‌تنها شامل زیرساخت سایبری متعلق به یکی از طرف‌های مخاصمه در قلمرو بی‌طرف می‌شود، بلکه شامل اعمال حقوق متخاصمانه با بهره‌گیری از سایر زیرساخت‌های سایبری واقع در آن قلمرو نیز هست. البته استثنایی در این زمینه وجود دارد که به شبکه‌های عمومی، بین‌المللی و آزاد مانند اینترنت مربوط می‌شود که می‌توانند برای ارتباطات نظامی مورداستفاده قرار گیرند. [۱] در صورتی که یک دولت بی‌طرف محدودیت‌هایی برای استفاده از چنین شبکه‌هایی وضع کند، این محدودیت‌ها باید به‌صورت بدون تبعیض نسبت به همه طرف‌های مخاصمه اعمال شوند. [۲] البته همان‌طور که در ارتباط با قاعده ۱۵۱ راهنمای تالین ۲ نیز اشاره شد، گروه بین‌المللی کارشناسان در این مورد اختلاف نظر داشتند که آیا انتقال سلاح‌های سایبری از طریق قلمرو بی‌طرف با استفاده از چنین شبکه‌ای ممنوع است یا نه. همچنین در مورد این‌که آیا دولت بی‌طرف موظف به جلوگیری از چنین انتقالی است نیز اختلاف‌نظر وجود داشت[۳] (همان: ۵۵۸-۵۵۹).

در توضیح عبارات به‌کاررفته در این قاعده باید بیان داشت، عبارت «تحت کنترل انحصاری آن» [۴] در اینجا به زیرساخت سایبری دولتیِ غیرتجاری اشاره دارد. [۵] در خصوص چنین زیرساختی، این قاعده صرف‌نظر از محل استقرار آن قابل اعمال است؛ زیرا تعهد مورد نظر ناشی از ماهیت دولتیِ زیرساخت است. علاوه بر این، قاعده ۱۵۲ راهنمای تالین

---

[۱] مطابق با قاعده ۱۵۱ راهنمای تالین ۲.

[۲] ماده ۹ کنوانسیون پنجم لاهه.

[۳] هم‌چنین تفسیرهای متفاوت از ماده ۸ کنوانسیون پنجم لاهه ممکن است پیامدهای گسترده‌ای به‌دنبال داشته باشد. طبق رویکرد راهنمای HPCR، فعالیت سایبری مخربی که از طریق زیرساخت سایبری یک دولت بی‌طرف – که مثلاً می‌تواند بخشی از اینترنت باشد – هدایت شده باشد، به‌منزله اعمال ممنوعه حقوق متخاصمانه (belligerent rights) تلقی نمی‌شود. بنابراین، دولتی بی‌طرف که چنین فعالیتی را مجاز شمرده یا نسبت به آن تساهل داشته باشد، متعهد به نقض حقوق بی‌طرفی نخواهد بود. با این حال، اگر رویکرد راهنمای HPCR بازتاب‌دهنده حقوق بین‌الملل عرفی محسوب نشود، در آن‌صورت انتقال یک حمله سایبری از طریق زیرساخت بی‌طرف باید به‌عنوان استفاده ممنوع از حقوق متخاصمانه تلقی شود و دولت بی‌طرفی که آگاهانه اجازه چنین انتقالی را داده یا نسبت به آن تساهل داشته باشد، ناقض تعهدات بی‌طرفی خود خواهد بود (Heintschel von Heinegg, 2013: 150-151).

[4] Under its Exclusive Control.

[۵] به بحث درباره «کنترل دولتی» (governmental control) در قاعده ٦ راهنمای تالین ۲ (مراقبت مقتضی) مراجعه نمایید.

۲ مبتنی بر وجود آگاهی[1]، اعم از واقعی یا فرضی، توسط دولت بی‌طرف است. یک دولت بی‌طرف زمانی دارای آگاهی واقعی[2] است که نهادهای آن، عملیات سایبری انجام‌شده توسط یکی از طرف‌های مخاصمه را که از قلمرو آن منشأ گرفته شناسایی کرده باشند، یا طرف متضرر در مخاصمه، به‌گونه‌ای معتبر به آن دولت اطلاع داده باشد که یک عملیات سایبری از قلمرو آن آغاز شده است. آگاهی فرضی[3] در مواردی مطرح می‌شود که در آن دولت، با توجه به شرایط موجود، به طور معقول باید از آن فعالیت آگاه می‌بود. گروه بین‌المللی کارشناسان راهنمای تالین ۲ دراین‌خصوص اختلاف‌نظر داشتند که آیا گسترش آگاهی به معنای آگاهی فرضی، مستلزم وجود یک تعهد برای دولت بی‌طرف جهت پایش[4] فعالانه (تاحدامکان) استفاده از زیرساخت سایبری در قلمرو آن است یا نه. در حالی که برخی اعضا معتقد بودند چنین تعهدی وجود دارد و بنابراین دولت بی‌طرف باید با دقت فعالیت‌های متخاصمانه را پایش کند، [5] اکثریت کارشناسان چنین تعهدی را منتفی دانستند (همان: ۵۵۹). ازسوی‌دیگر، عبارت «نباید با آگاهی اجازه دهد» [6] دلالت بر آن دارد که دولت‌های بی‌طرف موظف‌اند تمام اقدامات عملی ممکن را برای متوقف‌ساختن هرگونه اعمال حقوق متخاصمانه‌ای که با بهره‌گیری از زیرساخت سایبری مشمول این قاعده صورت می‌گیرد، اتخاذ نمایند. [7] بااین‌حال، همان‌گونه که در مورد آگاهی فرضی نیز مطرح شد، گروه بین‌المللی کارشناسان دراین‌خصوص به اجماع نرسیدند که آیا دولت بی‌طرف موظف به اتخاذ تدابیری برای جلوگیری از اعمال حقوق متخاصمانه، به‌ویژه از طریق پایش فعالیت‌های سایبری، است یا نه. برخی از کارشناسان بر این باور بودند که این تعهد به طور ضمنی در وظیفه «عدم اجازه آگاهانه» نهفته است. [8] این دسته از کارشناسان پیشنهاد کردند که در صورتی که اقدامات پیشگیرانه مانند پایش،

---

[1] Knowledge.
[2] Actual Knowledge.
[3] Constructive Knowledge.
[4] Monitor.
[5] AMW Manual, Rule 170(b).
[6] May Not Knowingly Allow.
[7] DoD Manual, para. 15.3.2.2; German Manual, paras. 1109, 1125, 1151; AMW Manual, commentary accompanying Rule 168(a); San Remo Manual, paras. 15, 18, 22; Hague Air Warfare Rules, Arts. 42, 47.
[8] ماده ۸ کنوانسیون سیزدهم لاهه؛ AMW Manual, Rule 170(b).

امکان‌پذیر باشد، انجام آن‌ها الزامی است. بدیهی است که امکان‌پذیری[1]، به شرایط موجود از جمله ظرفیت فنی دولت مربوط بستگی دارد. بااین‌حال، اکثریت کارشناسان این دیدگاه را رد کردند و استدلال نمودند که تنها تعهد دولت بی‌طرف، پایان‌دادن به استفاده، نه جلوگیری از آن است. این کارشناسان به‌ویژه به دشواری‌های عملی در اجرای هرگونه تعهد برای تشخیص ماهیت متخاصمانه یک بسته اطلاعاتی عبوری از شبکه‌های آن دولت اشاره کردند (همان: ۵۵۹-۵۶۰).

در پایان، اقداماتی که توسط یک دولت بی‌طرف در چارچوب این قاعده اتخاذ می‌شود، به‌عنوان «اقدام خصمانه» تلقی نمی‌گردد و به طریق اولی[2]، حمله مسلحانه[3] علیه طرفی از مخاصمه که بی‌طرفی آن دولت را نقض کرده نیز محسوب نمی‌شود.[4و5] همچنین، اگر وظیفه دولت بی‌طرف دفاع از بی‌طرفی خود باشد، یا استفاده از سلاح ضروری تلقی شود، مثلاً جایی که طرف مخاصمه تلاش می‌کند تا قسمت‌هایی از سرزمین بی‌طرف را به‌منظور عملیات نظامی مورداستفاده قرار دهد، دولت بی‌طرف ملزم به اتخاذ اقدامات نظامی است. اگر این اقدامات لازمه ایفای چنان تعهدی باشد، اقدامات مزبور باعث منتفی‌شدن مزایای بی‌طرفی تلقی نمی‌شود و علی‌رغم عملیات نظامی که آن دولت با یک طرف مخاصمه درگیر آن شده، آن دولت همچنان بی‌طرف باقی می‌ماند (فِلِک، ۱۳۹۵: ٦٤٧). البته باید اشاره داشت، اگر دولت بی‌طرف از بی‌طرفی خود دفاع کند، باید به حد و مرزهایی که حقوق بین‌الملل بر خشونت نظامی تحمیل می‌کند، احترام بگذارد. وقتی که دولت در قلمرو خود آن اقدامات را انجام دهد، هیچ نیاز خاصی برای اثبات مشروعیت بین‌المللی اقدامات نظامی وی نیست، به طور مثال می‌تواند نیروهای نظامی خارجی را از قلمرو خود دفع کرده و بیرون براند. اگر اقدامات نظامی خارج از محدوده سرزمینی دولت بی‌طرف انجام شود، این اقدامات فقط تا جایی قابل‌قبول است که اقدام در مقابل یک

---

[1] Feasibility.

[2] *a fortiori.*

[3] مطابق با قاعده ۷۱ راهنمای تالین ۲ (دفاع مشروع در مقابل حمله مسلحانه).

[4] ماده ۱۰ کنوانسیون پنجم لاهه؛ San Remo Manual, Rule 22 and accompanying commentary.

[5] درخصوص فعالیت‌هایی که در قلمرو بی‌طرف انجام می‌شوند ولی ارتباطی با مخاصمه ندارند، به قاعده ٦ راهنمای تالین ۲ (مراقبت مقتضی) مراجعه شود.

حمله مسلحانه طبق ماده ۵۱ منشور ملل متحد باشد و واکنش متقابل ضروری و متناسب با حمله باشد. بنابراین، ماده ۵۱ منشور ملل متحد، معمولاً سطح بالاتری از اقدام قانونی دولت بی‌طرف را خاطرنشان می‌سازد. به‌عبارت‌دیگر، منشور ملل متحد مجوز حق استفاده از نیروی متقابل را صادر می‌کند. حقوق بی‌طرفی تحت شرایطی خاص می‌تواند اجرای این حق را الزامی سازد (همان: ٦٥١).

۲/٤. واکنش طرف‌های مخاصمه به نقض بی‌طرفی

صرف‌نظر از مقررات عام مربوط به مسئولیت بین‌المللی که در قبال نقض حقوق بی-طرفی به کشور بی‌طرف تحمیل می‌شود و آثاری از این بابت به بار می‌آورد، ضمانت اجرای دیگری نیز در این مورد مقرر شده و آن این‌که، اگر کشور بی‌طرف به تعهدات و تکالیف خود عمل نکند یا آن‌ها را نقض کند، کشورهای متخاصم، دیگر تعهدی به رعایت بی‌طرفی آن کشور ندارد و می‌توانند او را در زمره متخاصمان قلمداد کنند و علیه او مبادرت به عملیات جنگی نمایند؛ اما چنانچه کشور بی‌طرف جهت انجام تکالیف مقرر تمام سعی و کوشش خود را در محدوده امکاناتی که در اختیار داشته به کار برده، ولی بااین‌حال موفق به حفظ بی‌طرفی خود نشده باشد، دیگر مسئولیت بین‌المللی متوجه او نیست و در نتیجه، ضمانت اجرایی هم در مورد او اِعمال نمی‌شود (ضیایی بیگدلی (ب)، ۱۴۰۰: ۳۵۰).

در این راستا، قاعده ۱۵۳ راهنمای تالین ۲ بیان می‌دارد: «چنان‌چه یک دولت بی‌طرف در متوقف ساختن اعمال حقوق متخاصمانه در قلمرو خود قصور ورزد، طرف متضرر در مخاصمه می‌تواند اقداماتی، از جمله از طریق عملیات سایبری، اتخاذ کند که برای مقابله با آن رفتار لازم و ضروری باشد». در توضیح باید بیان داشت، این قاعده به‌طور کلی به‌عنوان بخشی از حقوق بین‌الملل عرفی پذیرفته شده است. این قاعده نوعی «خودیاری» [1] به شمار می‌رود که به طرف متضرر در مخاصمه امکان می‌دهد در برابر اقدامات غیرقانونی دشمن در قلمرو بی‌طرف، از جمله استفاده متخاصمانه از زیرساخت سایبری بی‌طرف که دولت بی‌طرف در قبال آن اقدامی نکرده است، واکنش نشان دهد و جبران کند. [2] با این حال، این قاعده در مورد هرگونه نقض بی‌طرفی قابل اجرا نیست، بلکه صرفاً شامل مواردی

[1] Self-Help.
[2] DoD Manual, para. 15.4.2; UK Manual, para. 1.43(a); Canadian Manual, para. 1304 (3); AMW Manual, Rule 168(b); San Remo Manual, Rule 22.

می‌شود که اثر منفی بر طرف مقابل در مخاصمه داشته باشند. سایر نقض‌ها، منحصراً به کشور بی‌طرف مربوط می‌شود. برای مثال، اگر یکی از طرف‌های مخاصمه عملیات محروم‌سازی از سرویس[1] را علیه زیرساخت سایبری بی‌طرف انجام دهد، این اقدام لزوماً مزیت نظامی‌ای در برابر دشمن ایجاد نمی‌کند. در چنین مواردی، طرف مقابل حق ندارد به‌موجب این قاعده آن عملیات را متوقف کند و هرگونه واکنش در این زمینه صرفاً در اختیار دولت بی‌طرف خواهد بود (Tallinn Manual 2.0, 2017 : 560).

بنابراین، اجرای این قاعده منوط به تحقق دو شرط است. نخست، نقض قلمرو دولت بی‌طرف باید «جدی»[2] باشد؛ نقض‌های جزئی موجب اجرای این قاعده نمی‌شوند.[3] به بیان دیگر، طرف ناقض وضعیت بی‌طرفی باید از طریق آن نقض، برتری نظامی معناداری نسبت به دشمن خود به دست آورده باشد. جدی بودن نقض را نمی‌توان به‌صورت انتزاعی[4] تعیین کرد، بلکه این امر به شرایط حاکم در زمان وقوع بستگی دارد. معیار جدی بودن می‌تواند بر مبنای گستردگی[5] نقض یا مزیتی که ناقض به واسطه آن به دست آورده، سنجیده شود. برای نمونه، گروه بین‌المللی کارشناسان راهنمای تالین ۲ توافق داشتند که صِرف ایجاد توانایی برای نفوذ به حساب‌های ایمیل شخصی اعضای رده‌پایین نیروهای مسلح دشمن، اجرای این قاعده را توجیه نمی‌کند. در مقابل، فرض کنید یکی از طرف‌های مخاصمه به دلیل شرایط جنگی، توانمندی سایبری‌اش تضعیف شده و از زیرساخت سایبری یک دولت بی‌طرف برای انجام عملیات سایبری علیه دشمن بهره می‌گیرد؛ در این صورت، این استفاده «جدی» تلقی شده و مشمول قاعده خواهد بود. دوم، اعمال حقوق متخاصمانه توسط یکی از طرف‌های مخاصمه در قلمرو دولت بی‌طرف باید تهدیدی فوری برای امنیت طرف متضرر ایجاد کند و هیچ جایگزین عملی و به موقعی برای اقدام در قلمرو

---

[1] Denial of Service (DoS).

حمله محروم‌سازی از سرویس (DoS) نوعی حمله سایبری است که در آن عامل مخرب با هدف از کار انداختن یک رایانه یا دستگاه دیگر برای کاربران مورد نظر آن، عملکرد عادی دستگاه را مختل می‌کند. حملات محروم‌سازی از سرویس معمولاً از طریق بارگذاری بیش از حد یا سیل درخواست‌ها به یک ماشین هدف انجام می‌شوند تا جایی که ترافیک عادی نتواند پردازش شود و در نتیجه خدمات به کاربران اضافی نیز محروم‌سازی شود (Cloudflare, n.d).

[2] Serious.

[3] San Remo Manual, Rule 22.

[4] *in abstracto.*

[5] Pervasiveness.

دولت بی‌طرف وجود نداشته باشد. [1] بنابراین، این قاعده تنها زمانی اجرا می‌شود که دولت بی‌طرف یا مایل [2] به انجام تعهدات خود بر اساس قاعده ۱۵۲ راهنمای تالین ۲ نباشد یا از انجام آن ناتوان [3] باشد. در چنین حالتی، طرف متضرر حق دارد پس از آنکه دولت بی‌طرف تمام اقدامات در دسترس خود را برای پایان‌دادن به نقض بی‌طرفی انجام داده اما موفق نبوده است، شخصاً برای رفع نقض بی‌طرفی از سوی دشمن اقدام نماید. بدیهی است، همچنین اگر دولت بی‌طرف هیچ اقدامی برای پایان‌دادن به نقض انجام ندهد، طرف متضرر مجاز به اقدام خواهد بود (همان: ٥٦٠-٥٦١).

در پایان این نکته نیز شایان اشاره است، اقدامات مبتنی بر «خودیاری» مشمول الزام به اطلاع‌رسانی قبلی هستند، به‌گونه‌ای که به دولت بی‌طرف فرصت معقولی داده شود تا نسبت به رفع نقض اقدام کند. تنها در صورتی که نقض بی‌طرفی تهدیدی فوری برای امنیت طرف متضرر ایجاد کند و هیچ جایگزین عملی و به موقعی وجود نداشته باشد، آن طرف می‌تواند از نیروی فوری و ضروری برای پایان‌دادن به نقض استفاده کند. به‌عنوان نمونه، فرض کنید یکی از طرف‌های مخاصمه عملیات سایبری خود علیه دشمن را از طریق سروری در قلمرو یک دولت بی‌طرف هدایت می‌کند. دولت متضرر، دولت بی‌طرف را مطلع کرده و خواستار جلوگیری از استفاده از زیرساخت سایبری آن می‌شود. چنانچه دولت بی‌طرف در مدت زمان معقولی موفق به متوقف‌سازی آن عملیات نشود، طرف متضرر از نظر حقوقی مجاز است عملیاتی سایبری برای ازکارانداختن عملکرد آن سرور انجام دهد (همان: ٥٦١).

۲/۵. بی‌طرفی و اقدامات شورای امنیت

به اجرا در آمدن منشور ملل متحد، در عده‌ای تردیدهایی را در خصوص قابل‌اجرابودن حقوق سنتی بی‌طرفی در مخاصمات مسلحانه بین‌المللی ایجاد کرد. دلیل این تردیدها آن بود که گستره اِعمال حقوق بی‌طرفی با توجه به الزامات ناشی از نظام امنیت جمعی منشور کاهش یافته است. به این معنا که چنانچه شورای امنیت بر اساس فصل هفتم منشور تصمیم به انجام اقدامات اجرایی علیه یک دولت متجاوز یا ناقض صلح بگیرد، تعهدات

[1] San Remo Manual, Rule 22.
[2] Unwilling.
[3] Unable.

دولت‌های عضو سازمان ملل متحد آن‌ها را از بی‌طرفی در قبال مخاصمه میان دولت متجاوز و دولت قربانی تجاوز باز می‌دارد (شایگان، ۱۳۹۵: ۳۳۸). ازاین‌رو، مفهوم بی‌طرفی نسبت به دولت‌هایی که اقدام‌های قهرآمیز یا اقداماتی دیگر از این قبیل را بر طبق دستور شورای امنیت سازمان ملل متحد به‌موجب فصل هفتم منشور ملل متحد انجام می‌دهند، تسری نمی‌یابد (راجرز، مالرب، ۱۳۸۷: ۱۷۷). منشور سازمان ملل متحد و تصمیمات شورای امنیت بر طبق منشور می‌توانند در شرایط ویژه‌ای حقوق سنتی بی‌طرفی را اصلاح کنند. بنابراین اتخاذ اقداماتی توسط سازمان ملل متحد بر قواعد خاصی متفاوت از حقوق سنتی بی‌طرفی مبتنی است. بااین‌حال، حقوق عام بی‌طرفی توسط منشور نسخ نشده است (فِلِک، ۱۳۹۵: ٦٤٠). در این راستا، آخرین قاعده این فصل از راهنمای تالین ۲، یعنی قاعده ۱۵۴، بیان می‌دارد: «هیچ دولتی نمی‌تواند برای توجیه رفتاری (از جمله عملیات سایبری) که با اقدامات پیشگیرانه یا اجرایی اتخاذشده از سوی شورای امنیت به‌موجب فصل هفتم منشور ملل متحد ناسازگار باشد، به حقوق بی‌طرفی استناد کند».

در تشریح این قاعده باید بیان داشت، این قاعده بر اساس ماده ۲۵ منشور ملل متحد بنا شده است که اعضای سازمان را ملزم به اجرای تصمیمات اتخاذشده از سوی شورای امنیت در قالب قطعنامه‌های آن می‌کند. همچنین، از ماده ۱۰۳ منشور نیز ناشی می‌شود که برتری تعهدات ناشی از منشور نسبت به سایر تعهدات معاهده‌ای، مانند تعهدات ناشی از کنوانسیون‌های لاهه پنجم و سیزدهم، را در صورت تعارض با اقدامات شورای امنیت تحت فصل هفتم، تضمین می‌نماید. [۱] با رعایت ممنوعیت اقدامات مغایر با هنجارهای قاعده آمره، همین اصل در مورد تعهدات ناشی از حقوق بین‌الملل عرفی که با تصمیمات شورای امنیت ناسازگارند نیز صدق می‌کند (Tallinn Manual 2.0, 2017 : 562).

بنابراین، قاعده ۱۵۴ هم در مواردی که شورای امنیت در واکنش به نقض صلح یا اقدام تجاوزکارانه تصمیم به اتخاذ اقدامات اجرایی می‌گیرد و هم در مواردی که در مواجهه با تهدید علیه صلح اقدام می‌کند، قابل اعمال است. [۲] این قاعده در سه وضعیت عملیاتی می‌شود: نخست، اگر قطعنامه‌ای از سوی شورای امنیت دولت‌ها را ملزم به انجام اقدام

[۱] هم‌چنین به منابع زیر رجوع شود:
German Manual, para. 1103; AMW Manual, Rule 165; San Remo Manual, paras. 7–9.

[۲] ماده ۳۹ منشور ملل متحد که این وضعیت‌ها را بیان می‌کند.

مشخصی کند، آن دولت‌ها نمی‌توانند با استناد به حقوق بی‌طرفی از اجرای آن سر باز زنند. دوم، ممکن است شورای امنیت در قطعنامه‌ای انجام اقدام خاصی را برای دولت‌ها ممنوع اعلام کند؛ در چنین حالتی نیز حقوق بی‌طرفی توجیهی برای نقض آن ممنوعیت نخواهد بود. سوم، دولت‌ها بر اساس این قاعده از انجام هرگونه فعالیتی که ممکن است در روند اجرای اقدامات سایر دولت‌ها بر اساس قطعنامه شورای امنیت اخلال ایجاد کند، منع شده‌اند. فرض کنید شورای امنیت تشخیص داده است که یک دولت خاص مرتکب نقض صلح شده است. در این صورت، وضعیت موجود واجد شرایط یک مخاصمه مسلحانه بین‌المللی خواهد بود. در میان سایر اقدامات، این دولت در حال انجام حملات سایبری بسیار مخرب علیه زیرساخت‌های سایبری غیرنظامی دشمن است. در واکنش، شورای امنیت قطعنامه‌ای صادر می‌کند که به تمامی دولت‌های عضو اجازه می‌دهد از ظرفیت‌ها و قابلیت‌های سایبری خود برای پایان‌دادن به این حملات استفاده کنند. در چنین شرایطی، دولت‌هایی که در راستای اجرای این قطعنامه اقدام می‌کنند، حتی اگر از منظر حقوقی در مخاصمه بی‌طرف باشند، تعهدات خود را تحت حقوق بی‌طرفی نقض نخواهند کرد (همان: ٥٦٢).

نتیجه‌گیری

با شتاب روزافزون تحولات در عرصه فناوری اطلاعات و ظهور عملیات سایبری به‌عنوان ابزار نوین در منازعات مسلحانه، حقوق بی‌طرفی - که یکی از ارکان سنتی و بنیادین حقوق مخاصمات مسلحانه به شمار می‌رود - با چالش‌های پیچیده و بی‌سابقه‌ای روبه‌رو شده است. در چنین بستری، فقدان صریح معاهدات الزام‌آور بین‌المللی و قواعد عرفی تثبیت‌شده در حوزه فضای سایبر، موجب شده است که تفسیر و تطبیق اصول حقوق بشردوستانه و به‌ویژه حقوق بی‌طرفی با وضعیت نوپدید عملیات سایبری، ضرورتی اجتناب‌ناپذیر یابد. در این زمینه، همان‌گونه که در بخش‌های پیشین مقاله تشریح شد، راهنمای تالین ۲ به‌عنوان یکی از مهم‌ترین و جامع‌ترین تلاش‌های صورت‌گرفته توسط جامعه علمی و حقوقی بین‌المللی در راستای تدوین قواعد ناظر بر عملیات سایبری، جایگاه ویژه‌ای یافته است. پژوهش حاضر با تمرکز بر تبیین و تحلیل مواضع مندرج در راهنمای پیش‌گفته، در صدد آن بوده است تا سازگاری این دیدگاه‌ها را با مفاهیم و الزامات حقوق بی‌طرفی بررسی کرده و به پرسش اصلی تحقیق دائر بر امکان‌سنجی اعمال اصول بی‌طرفی در بستر منازعات سایبری پاسخ دهد. بر اساس یافته‌های این مطالعه، پنج نتیجه‌گیری کلیدی به دست آمده است: نخست، استفاده از ابزارهای سایبری برای اعمال حقوق متخاصمانه علیه زیرساخت‌های سایبری دولت بی‌طرف، مغایر با اصول بنیادین بی‌طرفی تلقی شده و ممنوع است؛ دوم، انجام عملیات سایبری متخاصمانه در قلمرو دولت بی‌طرف نیز ممنوع بوده و با تعهدات آن دولت در قبال حقوق بین‌الملل مغایرت دارد؛ سوم، دولت بی‌طرف موظف است از فراهم‌سازی یا تسهیل آگاهانه دسترسی طرف‌های درگیر به زیرساخت‌های سایبری واقع در قلمرو یا تحت کنترل حاکمیتی خود، به‌منظور انجام اقدامات خصمانه، خودداری کند؛ چهارم، در صورتی که دولت بی‌طرف از ایفای مسئولیت خود در جلوگیری از چنین اقداماتی قصور ورزد، دولت متضرر می‌تواند اقداماتی - از جمله از طریق ابزارهای سایبری - را اتخاذ کند، مشروط بر آنکه چنین اقداماتی متناسب، ضروری و در چارچوب قواعد بین‌المللی باشد؛ پنجم، استناد به حقوق بی‌طرفی نمی‌تواند مشروعیت‌بخش اقداماتی باشد که در تعارض با تدابیر الزام‌آور شورای امنیت سازمان ملل متحد بر اساس فصل هفتم منشور قرار دارند، از جمله اقداماتی که با

ماهیت تحریمی (ماده ٤١ منشور ملل متحد) یا نظامی (ماده ٤٢ منشور ملل متحد) مصوب شورای امنیت در تضاد هستند.

در مجموع، نتایج حاصل از این پژوهش مؤید آن است که هرچند حقوق بی‌طرفی هنوز هم ظرفیت‌های قابل توجهی برای اعمال در بستر درگیری‌های مسلحانه نوین دارد، اما برای حفظ کارایی و انسجام مفهومی خود در حوزه عملیات سایبری، نیازمند بازنگری و تفسیر نوین بر پایه واقعیت‌های فناورانه و تهدیدات سایبری معاصر است.

فهرست منابع

فارسی

۱. بیگ‌زاده، ابراهیم (۱۴۰۱). حقوق بین‌الملل. جلد دوم: روابط تابعان. چاپ اوّل. تهران: بنیاد حقوقی میزان.

۲. راجرز، آنتونی پ.و. و مالرب، پل (۱۳۸۷). قواعد کاربری حقوق مخاصمات مسلحانه. ترجمه کمیته ملی حقوق بشردوستانه. تهران: مؤسسه انتشارات امیرکبیر.

۳. فِلِک، دیتر. (۱۳۹۵). حقوق بشردوستانه در مخاصمات مسلحانه. ترجمه جمعی از مترجمان به اهتمام سیدقاسم زمانی و نادر ساعد. چاپ چهارم. تهران: مؤسسه مطالعات و پژوهش‌های حقوقی.

٤. ضیایی بیگدلی، محمدرضا (۱۴۰۰) (الف). حقوق بین‌الملل بشردوستانه. چاپ پنجم. تهران: انتشارات گنج دانش، با همکاری کمیته بین‌المللی صلیب سرخ.

۵. ضیایی بیگدلی، محمدرضا (۱۴۰۰) (ب). حقوق جنگ: حقوق بین‌الملل مخاصمات مسلحانه. چاپ هفتم. تهران: انتشارات دانشگاه علامه طباطبایی.

٦. اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹٤). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی، ۱۸ (۷۱)، ۲۵۷-۲۷۸.

۷. انصاری، باقر و اسدی، زهرا (۱۴۰۳). «حق بر فناوری در حقوق بین‌الملل؛ از شناسایی تا تحقق»، دوفصلنامه تحقیق و توسعه در حقوق عمومی، ۱ (۲)، ۷۹-۱۱۱.

۸. بیگلربیگی، کیان و عزیزی، ستار (۱۴۰۴). «شرایط و الزامات حاکم بر عملیات سایبری در زمان اشغال نظامی در پرتو راهنمای تالین ۲». نشریه حقوق و مطالعات سیاسی، ۵ (۲)، ۲۱۵-۲۳۲.

۹. زمانی، سیدقاسم (۱۴۰۳). «تأثیر فناوری بر توسعه مرزهای حقوق بین‌الملل». دوفصلنامه تحقیق و توسعه در حقوق عمومی، ۱ (۲)، ۳۱۹-۳۳۶.

۱۰. شایگان، فریده (۱۳۹۵). «اعمال حقوق بی‌طرفی در فضای سایبر». فصلنامه مطالعات حقوق عمومی، ٤٦ (۲)، ۳۳۷-۳۵۷.

۱۱. بیگلربیگی، کیان (۱۴۰۲). حملات سایبری و نقض اصل عدم مداخله. پایان‌نامه کارشناسی ارشد حقوق بین‌الملل. به راهنمایی ابراهیم بیگ‌زاده. تهران: دانشگاه شهید بهشتی، دانشکده حقوق، تاریخ دفاع ۱۴۰۲/۰۶/۱۹.

انگلیسی

1. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. (2017). Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation, Cambridge University Press.

2. Libicki, M. C., (2009). Cyberdeterrence and cyberwar, RAND Corporation.
3. Liivoja, R., & McCormack, T. (2013). Law in Virtual Battlespace: The Tallinn Manual and the jus in bello. Yearbook of International Humanitarian Law, Vol. 15. Asser Press
4. Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford University Press.
5. Broeders, D. (2021). "Private active cyber defense and (international) cyber security—pushing the line?", Journal of Cybersecurity, Vo;. 7, Iss. 1, pp. 1-14.
6. Buchan, R. (2012). "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Vol. 17, No. 2 (2012), pp. 211-227.
7. Heintschel von Heinegg, W. (2013). "Territorial Sovereignty and Neutrality in Cyberspace". International Law Studies, Vol. 89. pp.123-156.
8. Margulies, P. (2015). "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", Melbourne Journal of International Law, Vol. 14, pp. 1-24.
9. Sang, I. (2016). "Cyber-Attacks and the Exploitable Imperfections of International Law", Strathmore Law Journal, Vol. 2, No. 1. pp. 205-211.
10. Valuch, J., Gábriš, T., & Hamuľák, O. (2017). "Cyber attacks, information attacks, and postmodern warfare", Baltic Journal of Law & Politics, Vol. 10, Iss. 1, pp. 63-89.
11. Wallace, D., & Visger, M. (2018). "Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community". Journal of Law & Cyber Warfare, Vol. 6, No. 2 (Winter 2018), pp. 3-55.
12. Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System. (2003). Retrieved November 17, 2024 from https://rm.coe.int/168008160f
13. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.)1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949?activeTab=1949GCs-APs-and-commentaries
14. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea.)1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949?activeTab=1949GCs-APs-and-commentaries
15. Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-v-1907

16. Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, The Hague, 18 October 1907. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-xiii-1907
17. Convention on Cybercrime (Budapest Convention). (2001). Council of Europe. European Treaty Series - No. 185., Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https://rm.coe.int/1680081561
18. ICRC. (2016). Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1952. Retrieved February 4, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949
19. International Law Commission. (2001). Draft articles on responsibility of states for internationally wrongful acts, with commentaries. United Nations. Retrieved June 15, 2025 from https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
20. Joint Doctrine Manual Law of Armed Conflict: At the operational and tactical levels. Canadian Manual. Retrieved February 6, 2025 from https://www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf
21. Joint Service Regulation of the Law of Armed Conflict. German Manual. Retrieved February 4, 2025 from https://www.bmvg.de/resource/blob/93610/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual-law-of-armed-conflict-data.pdf
22. Law of Manual. DoD Manual. Retrieved February 6, 2025 from https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF
23. Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University. (2013). Manual on international law applicable to air and missile warfare (AMW Manual) (Yoram Dinstein, B. Demeyere & C. Bruderlein, Eds.). Cambridge University Press. Retrieved June 14, 2025 from https://cdn.ca9.uscourts.gov/datastore/library/2013/09/06/Flores_Manual.pdf
24. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1). (1977). Retrieved November 14, 2024 from https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf

25. San Remo Manual on International Law Applicable to Armed Conflicts at Sea. (12 June 1994). International Institute of Humanitarian Law. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994
26. The Hague Rules of Air Warfare. (1923). Retrieved June 14, 2025 from http://lawofwar.org/hague_rules_of_air_warfare.htm
27. The Joint Service Manual of the Law of Armed Conflict. UK Manual. Retrieved February 4, 2025 from
https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf
28. United Nations. (1945). Charter of the United Nations. Retrieved June 15, 2025 from https://www.un.org/en/about-us/un-charter

D. Case

29. ICJ. (1949). Corfu Channel, United Kingdom of Great Britain and Northern Ireland v. Albania, Judgment, 9 April 1949. Retrieved June 17, 2025 from https://www.icj-cij.org/case/1
30. PCIJ, (1927). The Case of the S.S. Lotus, France v. Turkey, Judgment, 7 September 1927. Retrieved June 14, 2025 from https://www.icj-cij.org/sites/default/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf
31. PCIJ. (1932). Free Zones of Upper Savoy and the District of Gex, France vs. Switzerland, Judgment, 7 June 1932. Retrieved June 17, 2025 from https://jusmundi.com/en/document/decision/en-free-zones-of-upper-savoy-and-the-district-of-gex-judgment-tuesday-7th-june-1932
32. Permanent Court of Arbitration. (1928). Island of Palmas, USA v. Netherlands, Award, Hague, 4 April 1928. Retrieved June 18, 2025 from https://pcacases.com/web/sendAttach/714
33. Battle, P. (2023). Dollar Tree supply chain attack could affect millions of people. MSSP Alert. Retrieved June 16, 2025 from https://www.msspalert.com/news/dollar-tree-supply-chain-attack-could-affect-millions-of-people/
34. Cloudflare. (n.d.). Denial-of-service (DoS) attack. Cloudflare Learning Center. Retrieved June 16, 2025 from https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
35. Hope, A. (2024). Massive Trello user data leak: Hacker lists 15 million records on a dark web hacking forum. CPO Magazine. Retrieved June 16, 2025 from

https://www.cpomagazine.com/cyber-security/massive-trello-user-data-leak-hacker-lists-15-million-records-on-a-dark-web-hacking-forum/

36. International Committee of the Red Cross (ICRC). (n.d.). Cyber and information operations. ICRC. Retrieved June 16, 2025 from https://www.icrc.org/en/law-and-policy/cyber-and-information-operations
37. Kovacs, E. (2024). Johnson Controls ransomware attack: Data theft confirmed, cost exceeds $27 million. SecurityWeek. Retrieved June 16, 2025 from https://www.securityweek.com/johnson-controls-ransomware-attacks-data-theft-confirmed-cost-exceeds-27-million/
38. Proofpoint. (n.d). Cyber attack. Proofpoint Threat Reference. Retrieved June 16, 2025 from https://www.proofpoint.com/uk/threat-reference/cyber-attack
39. Toulas, B. (2024). Hackers mint 1.79billion crypto tokens from PlayDapp gaming platform. Bleeping Computer. Retrieved June 16, 2025 from https://www.bleepingcomputer.com/news/security/hackers-mint-179-billion-crypto-tokens-from-playdapp-gaming-platform/
40. Trend Micro. (2024). Mother of all breaches: 26 billion records compromised. Trend Micro Security News. Retrieved June 16, 2025 from https://news.trendmicro.com/2024/01/23/mother-of-all-breaches-26-billion-records-compromised-data-leak/

References

1. Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System. (2003). Retrieved November 17, 2024 from https://rm.coe.int/168008160f
2. Ansari, B. & Asadi, Z. (2025). "The Right to Technology in International Law: From Identification to Realization". Journal of Research and Development in Public Law, 1 (2), 79-111. (In Persian)
3. Aslani, J., & Ranjbarian, A. H. (2015). "Comparative Review and Analysis of the Notion of CyberAttack in the Light of Doctrine, States Practice andInternational Organizations within International Law". Legal Research Quarterly (Shahid Beheshti University) , 18(71), 257-278. (In Persian)
4. Battle, P. (2023). Dollar Tree supply chain attack could affect millions of people. MSSP Alert. Retrieved June 16, 2025 from https://www.msspalert.com/news/dollar-tree-supply-chain-attack-could-affect-millions-of-people/
5. Beigzadeh, E. (2022). International law. Volume 2: Relations of Subjects (1st ed.). Tehran: Mizan Legal Foundation. (In Persian)
6. Biglarbeigi, K. (2023). Cyber Attacks and Violation of the Principle of Non-Intervention. Master's thesis, International Law. Supervised by Ebrahim Beigzadeh. Tehran: Shahid Beheshti University, Faculty of Law. Defense date: September 10, 2023. (In Persian)
7. Biglarbeigi, K., & Azizi, S. (2025). "Conditions and requirements governing cyber operations during military occupation in light of the Tallinn Manual 2.0". Journal of Law and Political Studies, 5(2), 215-232. [in Persian]
8. Broeders, D. (2021). "Private active cyber defense and (international) cyber security—pushing the line?", Journal of Cybersecurity, Vo;. 7, Iss. 1, pp. 1-14.
9. Buchan, R. (2012). "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Vol. 17, No. 2 (2012), pp. 211-227.
10. Cloudflare. (n.d.). Denial-of-service (DoS) attack. Cloudflare Learning Center. Retrieved June 16, 2025 from https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
11. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.)1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949?activeTab=1949GCs-APs-and-commentaries
12. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea.)1949). Geneva, 12 August 1949. Retrieved November 19,

2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949?activeTab=1949GCs-APs-and-commentaries

13. Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-v-1907
14. Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, The Hague, 18 October 1907. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-xiii-1907
15. Convention on Cybercrime (Budapest Convention). (2001). Council of Europe. European Treaty Series - No. 185., Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https://rm.coe.int/1680081561
16. Fleck, D. (2016). Humanitarian Law in Armed Conflict (S. G. Zamani & N. Saed, Eds., Trans., 4th ed.). Tehran: The SD Institute of Laaw Research and Study. [in Persian]
17. Heintschel von Heinegg, W. (2013). "Territorial Sovereignty and Neutrality in Cyberspace". International Law Studies, Vol. 89. pp.123-156.
18. Hope, A. (2024). Massive Trello user data leak: Hacker lists 15 million records on a dark web hacking forum. CPO Magazine. Retrieved June 16, 2025 from https://www.cpomagazine.com/cyber-security/massive-trello-user-data-leak-hacker-lists-15-million-records-on-a-dark-web-hacking-forum/
19. ICJ. (1949). Corfu Channel, United Kingdom of Great Britain and Northern Ireland v. Albania, Judgment, 9 April 1949. Retrieved June 17, 2025 from https://www.icj-cij.org/case/1
20. ICRC. (2016). Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1952. Retrieved February 4, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949
21. International Committee of the Red Cross (ICRC). (n.d.). Cyber and information operations. ICRC. Retrieved June 16, 2025 from https://www.icrc.org/en/law-and-policy/cyber-and-information-operations
22. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. (2017). Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation, Cambridge University Press.
23. International Law Commission. (2001). Draft articles on responsibility of states for internationally wrongful acts, with commentaries. United Nations. Retrieved June 15, 2025 from https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

24. Joint Doctrine Manual Law of Armed Conflict: At the operational and tactical levels. Canadian Manual. Retrieved February 6, 2025 from https://www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf
25. Joint Service Regulation of the Law of Armed Conflict. German Manual. Retrieved February 4, 2025 from https://www.bmvg.de/resource/blob/93610/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual-law-of-armed-conflict-data.pdf
26. Kovacs, E. (2024). Johnson Controls ransomware attack: Data theft confirmed, cost exceeds $27 million. SecurityWeek. Retrieved June 16, 2025 from https://www.securityweek.com/johnson-controls-ransomware-attacks-data-theft-confirmed-cost-exceeds-27-million/
27. Law of Manual. DoD Manual. Retrieved February 6, 2025 from https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF
28. Libicki, M. C., (2009). Cyberdeterrence and cyberwar, RAND Corporation.
29. Liivoja, R., & McCormack, T. (2013). Law in Virtual Battlespace: The Tallinn Manual and the jus in bello. Yearbook of International Humanitarian Law, Vol. 15. Asser Press
30. Margulies, P. (2015). "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", Melbourne Journal of International Law, Vol. 14, pp. 1-24.
31. PCIJ, (1927). The Case of the S.S. Lotus, France v. Turkey, Judgment, 7 September 1927. Retrieved June 14, 2025 from https://www.icj-cij.org/sites/default/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf
32. PCIJ. (1932). Free Zones of Upper Savoy and the District of Gex, France vs. Switzerland, Judgment, 7 June 1932. Retrieved June 17, 2025 from https://jusmundi.com/en/document/decision/en-free-zones-of-upper-savoy-and-the-district-of-gex-judgment-tuesday-7th-june-1932
33. Permanent Court of Arbitration. (1928). Island of Palmas, USA v. Netherlands, Award, Hague, 4 April 1928. Retrieved June 18, 2025 from https://pcacases.com/web/sendAttach/714
34. Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University. (2013). Manual on international law applicable to air and missile warfare (AMW Manual) (Yoram Dinstein, B. Demeyere & C. Bruderlein, Eds.). Cambridge University Press. Retrieved June 14, 2025 from https://cdn.ca9.uscourts.gov/datastore/library/2013/09/06/Flores_Manual.pdf

35. Proofpoint. (n.d). Cyber attack. Proofpoint Threat Reference. Retrieved June 16, 2025 from https://www.proofpoint.com/uk/threat-reference/cyber-attack
36. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1). (1977). Retrieved November 14, 2024 from https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf
37. Rogers, A. P. V., & Malherbe, P. (2008). Model Manual on the Law of Armed Conflict for Armed Forces (K.N. Humanitarian Law Committee, Trans.). Tehran: Amir Kabir Publishing Institute. (In Persian)
38. Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford University Press.
39. San Remo Manual on International Law Applicable to Armed Conflicts at Sea. (12 June 1994). International Institute of Humanitarian Law. Retrieved June 14, 2025 from https://ihl-databases.icrc.org/en/ihl-treaties/san-remo-manual-1994
40. Sang, I. (2016). "Cyber-Attacks and the Exploitable Imperfections of International Law", Strathmore Law Journal, Vol. 2, No. 1. pp. 205-211.
41. Shayegan, F. (2016). "Application of the Law of neutrality in cyberspace". Public Law Studies Quarterly, 46(2), 337-357. [in Persian]
42. The Hague Rules of Air Warfare. (1923). Retrieved June 14, 2025 from http://lawofwar.org/hague_rules_of_air_warfare.htm
43. The Joint Service Manual of the Law of Armed Conflict. UK Manual. Retrieved February 4, 2025 from https://assets.publishing.service.gov.uk/media/5a7952bfe5274a2acd18bda5/JSP3832004Edition.pdf
44. Toulas, B. (2024). Hackers mint 1.79billion crypto tokens from PlayDapp gaming platform. Bleeping Computer. Retrieved June 16, 2025 from https://www.bleepingcomputer.com/news/security/hackers-mint-179-billion-crypto-tokens-from-playdapp-gaming-platform/
45. Trend Micro. (2024). Mother of all breaches: 26 billion records compromised. Trend Micro Security News. Retrieved June 16, 2025 from https://news.trendmicro.com/2024/01/23/mother-of-all-breaches-26-billion-records-compromised-data-leak/

46. United Nations. (1945). Charter of the United Nations. Retrieved June 15, 2025 from https://www.un.org/en/about-us/un-charter
47. Valuch, J., Gábriš, T., & Hamuľák, O. (2017). "Cyber attacks, information attacks, and postmodern warfare", Baltic Journal of Law & Politics, Vol. 10, Iss. 1, pp. 63-89.
48. Wallace, D., & Visger, M. (2018). "Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community". Journal of Law & Cyber Warfare, Vol. 6, No. 2 (Winter 2018), pp. 3-55.
49. Zamani, S. G. (2025). "Impacts of Technology on Development of Frontiers of International Law". Journal of Research and Development in Public Law, 1 (2), 319-336. (In Persian)
50. Ziaei Bigdeli, M. R. (2021). International humanitarian law (5th ed.). Tehran: Ganj-e Danesh Publishing, in collaboration with the International Committee of the Red Cross. (In Persian)
51. Ziaei Bigdeli, M. R. (2021). The Law of War: International Law of Armed Conflicts (7th ed.). Tehran: Allameh Tabataba'i University Press. (In Persian)