فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۶، شمارهٔ ۲، تابستان ۱۳۹۵: ۳۳۷-۳۵۷

اعمال حقوق بی‌طرفی در فضای سایبر

فریده شایگان*

چکیده

افزایش سریع استفاده از فضای سایبر و ویژگی‌های منحصربه‌فرد آن، از جمله به‌هم‌پیوسته بودن زیرساخت‌های سایبر در سراسر جهان و فاقد مرز بودن شبکهٔ جهانی اینترنت، از یک سو؛ و امکان استفاده از این فضا و قابلیت‌های آن برای انجام حملات سایبری و عبور دادن سلاح سایبر با استفاده از زیرساخت‌های سایبری سایر دولت‌ها، از سوی دیگر؛ رعایت بی‌طرفی در مخاصمات مسلحانهٔ بین‌المللی را با دشواری‌های جدی مواجه می‌سازد. در این شرایط اصل احترام به تعرض‌ناپذیری سرزمین دولت‌های بی‌طرف به‌شدت آسیب‌پذیر می‌شود و احتمال درگیر شدن دولت بی‌طرف در مخاصمه و در نتیجه گسترش آن افزایش می‌یابد؛ نتیجه‌ای که حقوق بی‌طرفی در پی اجتناب از آن است. بنابراین مطالعه و بررسی قابلیت اعمال حقوق بی‌طرفی بر فضای سایبر، به‌خصوص تعهدات متخاصمان و دولت‌های بی‌طرف و چگونگی اجرای آنها و آثار حقوقی نقض تعهدات بی‌طرفی ضروری می‌نماید.

واژگان کلیدی

تعهدات متخاصمان، تعهدات دولت بی‌طرف، جلوگیری از نقض بی‌طرفی خاتمه دادن به نقض بی‌طرفی، حاکمیت بر فضای سایبر، حقوق بی‌طرفی، فضای سایبر، مخاصمات مسلحانهٔ بین‌المللی.

---

* استادیار گروه حقوق پردیس بین‌المللی کیش دانشگاه تهران.

Email: farideh.shaygan@ut.ac.ir

تاریخ دریافت: ۱۳۹۴/۰۸/۲۸، تاریخ پذیرش: ۱۳۹۴/۱۰/۰۵

مقدمه

اصول و قواعد حقوق بی‌طرفی بر مخاصمات مسلحانهٔ بین‌المللی اعمال می‌شود و بی‌طرفی به وضع حقوقی دولتی اشاره دارد که طرف یک مخاصمهٔ مسلحانهٔ بین‌المللی نیست (Heinegg, 2012: 35). در واقع، حقوق بی‌طرفی با دادن امکان حفظ روابط با تمام متخاصمان، به دولت‌هایی که در مخاصمه شرکت ندارند، همزیستی جنگ و صلح را به نظم می‌کشد (Kelsey, 2008: 1442). قواعد بی‌طرفی عمدتاً به موجب کنوانسیون‌های پنجم و سیزدهم لاهه در سال ۱۹۰۷م تدوین شده‌اند. به اجرا در آمدن منشور ملل متحد، در عده‌ای تردیدهایی را در خصوص قابل اجرا بودن حقوق سنتی بی‌طرفی در مخاصمات مسلحانهٔ بین‌المللی ایجاد کرد. دلیل این تردیدها آن بود که گسترهٔ اِعمال حقوق بی‌طرفی با توجه به الزامات ناشی از نظام امنیت جمعی منشور کاهش یافته است. به این معنا که چنانچه شورای امنیت براساس فصل هفتم منشور تصمیم به انجام اقدامات اجرایی علیه یک دولت متجاوز یا ناقض صلح بگیرد، تعهدات دولت‌های عضو سازمان ملل متحد آنها را از بی‌طرفی در قبال مخاصمهٔ میان دولت متجاوز و دولت قربانی تجاوز باز می‌دارد. به این ترتیب مواد ۲۵ و ۱۰۳ منشور ملل متحد دولت‌هایی را که طرف چنین مخاصمهٔ مسلحانه‌ای نیستند و براساس حقوق بی‌طرفی می‌بایست از هر گونه مداخله به نفع یک طرف مخاصمه و به زیان طرف دیگر خودداری ورزند، ملزم به تبعیت از تصمیمات شورای امنیت علیه یک طرف مخاصمه می‌کند. تعهدات ناشی از این‌گونه قطعنامه‌های شورای امنیت، حداقل شامل خودداری از هر گونه فعالیتی است که برای انجام عملیات اجرایی مورد نظر این رکن مزاحمت یا ممانعت ایجاد کند، و می‌تواند الزام برخی از دولت‌ها به همکاری برای تسهیل انجام اقدامات نظامی – مانند دادن اجازهٔ عبور نیروها و تجهیزات و تسلیحات نظامی از سرزمینشان - را در بربگیرد و در نهایت به برخی از دولت‌ها اجازهٔ شرکت در اقدامات نظامی علیه متخاصم متجاوز را بدهد.

با وجود این دولت‌ها قابل اِعمال بودن حقوق بی‌طرفی بر مخاصمات مسلحانهٔ کنونی را پذیرفته‌اند، هرچند رفتارشان همیشه با اصل عدم جانبداری منطبق نبوده است (Schindler, 1991: 386). مؤید این امر مجموعه قواعد سن رمو (San Remo Manual, 1994: paras.14 et seq)، اچ پی سی آر[1] (HPCR Manual, 2009: Section X)، تالین (Tallinn Manual, 2013) اصول هلسینکی انجمن حقوق بین‌الملل (ILA Helsinki Principles, 1998: 497 et seq) و دستورالعمل‌های نظامی کشورهای مختلف، از جمله ایالات متحدهٔ آمریکا (US Commander's Handbook on the Law of Naval Operations, 1997: Chapter 7)، بریتانیا (UK Joint

۱. مجموعه قواعد HPCR که توسط گروهی از متخصصان حقوق بین‌الملل در چارچوب نهادی در دانشگاه هاروارد تهیه شده، اقدام به شناسایی یا بازگویی قواعد حقوق بین‌الملل قابل اِعمال بر جنگ هوایی و موشکی کرده است. این برنامه در سال ۲۰۰۴م آغاز و در ماه می ۲۰۰۹ منتشر شده است.

(Service Manual of the Law of Armed Conflict, 2004: para.1.42, Chapters 12 & 13، کانادا: Canadian Law of Armed Conflict at the operational and tactical levels, 2001) و آلمان (Manual of Germany on Humanitarian Law in Armed Conflicts, 1992: Chapter 11) است.

هرچند به‌صراحت می‌توان گفت که حقوق بی‌طرفی با رعایت تصمیمات شورای امنیت براساس فصل هفتم منشور، بر روابط میان دولت‌های متخاصم و دولت‌هایی که طرف مخاصمه نیستند حاکم است، آیا می‌توان با همین سهولت و روشنی حکم به قابل اِعمال بودن این حقوق بر عملیات یا حملات خصمانه در فضای سایبر[1] کرد؟ براساس یک تعریف، فضای سایبر «قلمرویی جهانی در محیط اطلاعات مشتمل بر شبکه‌های وابسته به یکدیگر زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابرات دور، سیستم‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های نصب‌شده است» (US Department of Defense Dictionary of Military and Associated Terms, 2012: 58). چنانکه ملاحظه می‌شود براساس این تعریف فضای سایبر به اینترنت خلاصه نمی‌شود و فراتر از آن است. اما راهبرد امنیت سایبری آلمان فضای سایبر را مشتمل بر «تمام زیرساخت‌های اطلاعاتی قابل دسترسی از طریق اینترنت فراسوی تمام مرزهای سرزمینی» می‌داند (Cyber Security Strategy for Germany, 2011: 2).

با توجه به وابستگی شبکه‌های زیرساخت‌های سایبری در سراسر جهان، چگونه می‌توان حقوق بی‌طرفی را بر این فضای پنجم که بر خلاف فضاهای چهارگانهٔ طبیعی – زمین، دریا، هوا و فضا – تماماً ساختهٔ انسان است، قابل اِعمال دانست؟ فضایی که مورد استفادهٔ دوگانهٔ نظامی و غیرنظامی است و در آن به‌علت ارتباط متقابل و به‌هم‌پیوسته بودن زیرساخت‌های سایبری در سراسر جهان، مرزی وجود ندارد و تحت حاکمیت هیچ دولتی نیست. ازاین‌رو برخی به‌درستی آن را همانند دریای آزاد، فضای هوایی بین‌المللی و فضای ماورای جو، "مشترکات جهانی" (global common)[2] به‌شمار آورده‌اند که «از هر گونه اندازه‌گیری در بعد مادی یا تداوم فضا زمانی سرباز می‌زند» (Wingfield, 2000: 17). این در حالی است که حقوق بی‌طرفی وجود مرز، یعنی مشخص بودن محدودهٔ سرزمینی دولت‌های طرف یک مخاصمهٔ مسلحانهٔ بین‌المللی

---

۱. استراتژی نظامی ملی ایالات متحده برای عملیات در فضای سایبر، این فضا را این‌گونه تعریف می‌کند: «قلمرویی است که به‌وسیلهٔ استفاده از طیف ادوات الکترونیکی و الکترومغناطیسی برای ذخیره‌سازی، تعدیل و تغییر داده‌ها از طریق سیستم‌های شبکه شده و زیرساخت‌های فیزیکیِ مرتبط مشخص می‌گردد» (Lopez, C. Todd, 2007).

۲. در *استراتژی دفاعی ایالات متحدهٔ آمریکا برای وطن و پشتیبانی غیرنظامی* نیز، تصریح شده است که: «مشترکات جهانی عبارت‌اند از آب‌های بین‌المللی، فضای هوایی، فضا و فضای سایبر» (US Department of Defense, 2005: 12).

و دولت‌های بی‌طرف را مفروض می‌دارد. چراکه هدف دوگانهٔ حقوق بی‌طرفی از یک سو، حمایت از حاکمیت سرزمینی دولت‌های بی‌طرف و جمعیت آنها در برابر آثار زیانبار مخاصمات است؛ و از سوی دیگر، حمایت از منافع متخاصمان در مقابل هر گونه مداخلهٔ دولت‌های بی‌طرف و اتباع آنها به نفع یک طرف مخاصمه و به ضرر طرف دیگر، و بدین‌سان جلوگیری از گسترش مخاصمه است(Heinegg, 2013: 143) .

به این ترتیب، از آنجا که مفهوم حاکمیت در فضای سایبر در این نوشتار اهمیت اساسی دارد، مشخص کردن آن پیش از ورود به مباحث اصلی ضروری به‌نظر می‌رسد. براساس قاعدهٔ ۱ از مجموعه قواعد تالین «یک دولت می‌تواند بر زیرساخت‌ها و فعالیت‌های سایبری در سرزمین تحت حاکمیتش کنترل اعمال کند» (Tallinn Manual, .2013: 25). این قاعده حاکی از آن است که هرچند هیچ دولتی نمی‌تواند ادعای حاکمیت بر فضای سایبر را نماید، با وجود این، می‌تواند بر هر گونه زیرساخت سایبری و فعالیت‌های سایبری در سرزمینش حقوق حاکمیتی اعمال کند. در واقع، برخورداری از حاکمیت دلالت بر آن دارد که یک دولت می‌تواند دسترسی به سرزمینش و استفاده از آن را، از جمله دسترسی به زیرساخت‌های سایبری و استفاده از آن را از حیث حقوقی و عملی – به لحاظ برخورداری از قدرت انحصاری تصمیم‌گیری در خصوص اقدامات تقنینی، اجرایی و قضایی - کنترل کند، چراکه دولت به‌طور کلی در حدود معین‌شده به موجب معاهدات و حقوق بین‌الملل عرفی از حق انحصاری اعمال صلاحیت و قدرت در سرزمینش برخوردار است (Tallinn Manual, .2013: commentary to the rule 1, paras.1, 4; Tuukkanen, 2013: 38; Island Palmas arbitral award, 1928, p.838).

به‌رغم ویژگی‌های فضای سایبر که ممکن است در خصوص قابل اعمال بودن حقوق بی‌طرفی در این فضا ایجاد تردید کند، از آنجا که فضای سایبر نیازمند وجود زیرساخت‌های فیزیکی است (Franzese, 2009: 33)، پذیرفته شده است که ویژگی‌های این فضا مانعی برای اعمال حاکمیت و صلاحیت سرزمینی و در نتیجه، برای قابل اعمال بودن قواعد و اصول بی‌طرفی در این فضا ایجاد نمی‌کند؛ هرچند مشکلات این اعمال صلاحیت را افزایش می‌دهد (Tallinn Manual, .2013: 202-209; Heinegg, 2013: 134). این نوشتار تعهدات دولت‌های متخاصم (۱) و بی‌طرف (۲) در قبال عملیات خصمانه در فضای سایبر و آثار حقوقی نقض این تعهدات از سوی آنها را بررسی و تحلیل می‌کند. به این منظور، در موارد لزوم به مطالعهٔ تطبیقی حقوق بین‌الملل و مقررات ملی برخی دولت‌ها نیز پرداخته شده است.

تعهدات دولت‌های متخاصم

براساس اصول و قواعد حقوق بی‌طرفی که در کنوانسیون‌های پنجم و سیزدهم لاهۀ ۱۹۰۷ درج

شده‌اند، متخاصمان ملزم به احترام به تعرض‌ناپذیری سرزمین دولت‌های بی‌طرف و ممنوع از هدایت مخاصمات، اِعمال حقوق متخاصم[1] و ایجاد پایگاه‌های عملیاتی در سرزمین دولت‌های بی‌طرف هستند (Hague Convention V, 1907: arts. 1, 2, 3; Hague Convention XIII, 1907: arts.1, 2, 5).

تعهد به عدم مداخلهٔ زیانبار در زیرساخت‌های سایبری دولت بی‌طرف

با توجه به تعهداتی که بیان شد، می‌توان نتیجه گرفت که حقوق بی‌طرفی از زیرساخت‌های سایبری واقع در سرزمین یک دولت بی‌طرف در برابر مداخلهٔ زیانبار متخاصمان حمایت می‌کند. مقصود از مداخلهٔ زیانبار در زیرساخت‌های سایبری دولت بی‌طرف، صرفاً حمله به معنای مورد نظر در حقوق بین‌الملل بشردوستانه - یعنی عملیات سایبری «در تهاجم یا در دفاع، که به‌طور منطقی انتظار می‌رود موجب جراحت یا مرگ اشخاص یا صدمه به اموال یا نابودی آنها شود» (Tallinn Manual, 2013: rule 30; Additional Protocol I, 1977: arts.49 (1), 51(5)(b)) - نیست.[2] تکلیف دولت‌های متخاصم به احترام به سرزمین بی‌طرف را می‌بایست به‌نحو موسع در نظر گرفت، بدین معنا که اعمال ممنوعه تمام اقدامات و عملیاتی را هم در برمی‌گیرد که بر کارکرد زیرساخت‌های سایبری و شبکه‌های کامپیوتری اثر منفی داشته باشند یا استفاده از آنها را غیرممکن سازند (Schaap, 2009 : 127 ; Talbot Jensen, 2012 : 822).

وصف زیانبار برای مداخلهٔ ممنوع، صِرف دخول در زیرساخت‌های سایبری دولت بی‌طرف را از شمول این منع خارج می‌کند، زیرا جاسوسی که هدف از آن جمع‌آوری اطلاعاتِ معمولاً محرمانه، مهم و حساس دربارهٔ دولت‌های دیگر است، در حقوق بین‌الملل بر خلاف حقوق داخلی دولت‌ها[3] ممنوع نشده است. به‌نظر می‌رسد علت این عدم ممنوعیت به‌حدی است که جاسوسی یا صرف دخول در زیرساخت‌های سایبری به‌خودی‌خود و مستقیماً موجد خسارت و صدمه نیستند. به‌علاوه، به‌جرأت می‌توان گفت که تقریباً تمامی دولت‌ها این‌گونه اعمال را برای حفظ امنیت خود ضروری می‌دانند.

وفق مادهٔ ۲ کنوانسیون پنجم لاههٔ ۱۹۰۷، متخاصمان نمی‌توانند سپاهیان، سلاح‌ها یا سایر ادوات جنگی خود را از سرزمین یک دولت بی‌طرف عبور دهند یا به آن منتقل کنند. بنابراین

---

1. belligerent rights

۲. عملیات سایبری فی‌نفسه خشونت‌بار نیستند، اما می‌توانند آثار خشونت‌بار، مانند جراحت، مرگ، صدمه و نابودی اموال را ایجاد کنند و در این صورت حمله‌ای مسلحانه محسوب خواهند شد (Shaygan, 2014: 69).

۳. برای مثال براساس مادهٔ ۳ قانون جرایم رایانه‌ای ایران، مصوب ۱۱ بهمن ۱۳۸۸، جاسوسی رایانه‌ای جرم شناخته شده و برای آن مجازات تعیین شده است.

چنانچه استفاده از اینترنت از سوی یک طرف مخاصمه برای هدایت و انجام حملات سایبری علیه طرف دیگر مخاصمه، از طریق عبور دادن یک بدافزار از نُدهای اینترنتی یک دولت بی‌طرف صورت بگیرد، ناقض حقوق بی‌طرفی خواهد بود؛ چراکه این امر عبور سلاحِ یک طرف متخاصم از قلمرو تحت صلاحیت و حاکمیت دولت بی‌طرف محسوب می‌شود (Brown, 2006: 210) و از آنجا که سلاح‌های سایبری نیز می‌توانند همان آثاری را ایجاد کنند که انواع سلاح‌ها در مفهوم سنتی و رایج، عبور دادن آنها از سرزمین دولت بی‌طرف[1] ممنوع است. اندازهٔ - بزرگی و کوچکی - سلاح تأثیری در این ممنوعیت ندارد، ولو آنکه به اندازهٔ یک الکترون باشد (Kelsey, 2008: 1444). مادهٔ ۲ کنوانسیون پنجم لاهه در این خصوص استثنایی قائل نشده است.

منوعیت‌های ذکرشده در حقوق بی‌طرفی در حمایت از دولت‌های بی‌طرف، در واقع از اصل برابری حاکمیت دولت‌ها ناشی می‌شود که هر گونه اِعمال صلاحیت در سرزمین یک دولت دیگر را ممنوع می‌سازد. دیوان دائمی بین‌المللی دادگستری در قضیهٔ *لوتوس* اظهار داشت: «یک دولت نمی‌تواند قدرت خود را به هیچ صورتی در سرزمین دولت دیگر اعمال کند. در این معنا صلاحیت مطمئناً سرزمینی است؛ یک دولت نمی‌تواند در خارج از سرزمین خود آن را اِعمال کند، مگر به‌واسطهٔ [وجودِ] یک قاعدهٔ تجویزی ناشی از عرف بین‌المللی یا یک کنوانسیون» (PCIJ, 1927: 18-19). به همین دلیل، هواپیماهای نظامی متخاصمان نمی‌توانند وارد حوزهٔ صلاحیت یک دولت بی‌طرف شوند. هرچند کشتی‌های یک طرف متخاصم می‌توانند از آب‌های یک دولت بی‌طرف عبور نمایند، اما مادام که در آن آب‌ها هستند نمی‌توانند به هیچ اقدام خصمانه‌ای مبادرت ورزند (Hague Convention XIII, 1907: arts.1, 2). بنابراین، چنانچه از کشتی متعلق به یک دولت متخاصم هنگام عبور از آب‌های یک دولت بی‌طرف، اقدام به عبور دادن یک سلاح سایبری از زیرساخت‌های سایبری واقع در سرزمین دولت بی‌طرف شود، نقض حقوق بی‌طرفی تلفی خواهد شد.

---

۱. سرزمین یک دولت بی‌طرف مشتمل است بر «قلمرو زمینی [دولت] بی‌طرف و مناطق دریایی تحت حاکمیت سرزمینی دولت ساحلی بی‌طرف، یعنی، آب‌های داخلی، دریای سرزمینی و در صورت قابل اجرا بودن، آب‌های مجمع‌الجزایری و فضای هوایی بالای این مناطق» (Commentary on the HPCR, 2010: 307, Commentary on Rule 166, para.2). اموال و اشیای واقع در سرزمین دولت بی‌طرف نیز تحت صلاحیت آن دولت بی‌طرف قرار دارند و به‌واسطهٔ بی‌طرفی آن دولت مورد حمایت قرار می‌گیرند، صرف‌نظر از مالکیت عمومی یا خصوصی و تابعیت مالکان آنها (*see* San Remo Manual, 1994: Part.II, Section I, para. 16(a)).

تعهد به عدم استفاده از زیرساخت‌های سایبری واقع در سرزمین دولت بی‌طرف برای اعمال حقوق خود به‌عنوان متخاصم

ممنوعیت اِعمال حقوق متخاصم[1] با استفاده از زیرساخت‌های سایبری واقع در سرزمین دولت بی‌طرف از فروعات اصل تعرض‌ناپذیری سرزمین دولت بی‌طرف است. حقوق متخاصم منحصر به حمله نیست و تمام اقداماتی را شامل می‌شود که یک متخاصم براساس حقوق مخاصمات مسلحانه محق به اتخاذ آنها علیه طرف دیگر مخاصمه، اتباع دشمن یا حتی اتباع دولت‌های بی‌طرف است؛ اعمالی چون بازداشت، مصادرهٔ اموال و به اسارت گرفتن (Heinegg, 2013: 146 and note 98). مقصود از استفادهٔ ممنوع از زیرساخت‌های سایبر، اقداماتی چون آغاز و انجام حمله یا تسهیل آن با استفاده از زیرساخت‌های سایبری دولت بی‌طرف برای دخول در زیرساخت‌های سایبری دشمن به‌منظور هدایت اقدامات زیانبار علیه آن است. این‌گونه اقدامات نقض حقوق بی‌طرفی محسوب می‌شوند؛ حقوقی که دولت‌های متخاصم را از هدایت مخاصمات از سرزمین یک دولت بی‌طرف منع می‌کند (Talbot Jensen, 2012: 825).

هدف این ممنوعیت به‌عنوان جزیی از حقوق بی‌طرفی، جلوگیری از تشدید و گسترش مخاصمهٔ مسلحانهٔ بین‌المللی، از طریق منع متخاصمان از استفاده از زیرساخت‌های سایبری واقع در سرزمین دولت بی‌طرف یا واقع در کشتی‌های جنگی، هواپیماهای نظامی، اماکن دیپلماتیک و سایر اموالی است که از مصونیت حاکمیتی برخوردارند (Tallinn Manual, 2013: rules. 4, 92 and its commentary, para.3). در این خصوص که آیا این ممنوعیت بر استفاده از زیرساخت‌های سایبری متعلق به اشخاص حقیقی یا حقوقی تبعهٔ دولت بی‌طرف که در خارج از سرزمین این دولت قرار دارند نیز، اعمال می‌شود، تردیدهایی ابراز شده است (Heinegg, 2013: 146). با وجود این، برخی صاحب‌نظران ممنوعیت یادشده را به‌صراحت شامل این دسته از زیرساخت‌های سایبری نیز می‌دانند (Walker, 2000: 1149-50).

در هر حال، چنانچه این‌گونه زیرساخت‌های سایبری برای مساعدت به اقدام نظامی یکی از متخاصمان به‌کار روند، طرف دیگر مخاصمه می‌تواند آنها را به این دلیل قانوناً هدف عملیات نظامی خود قرار دهد، مشروط بر آنکه انهدام کلی یا جزیی یا از کار انداختن آن مزیت نظامی مشخصی در برداشته باشد (Additional Protocol I, 1977: art.52(2)). شایان ذکر است که تعریف اهداف نظامی در پروتکل اول الحاقی در حال حاضر وضعیت حقوق بین‌الملل عرفی را دارد (Henckaert & Doswald-Beck, 2005: rule 8).

همچنین از مادهٔ ۳ کنوانسیون لاهۀ ۱۹۰۷ مستفاد می‌شود که حقوق بی‌طرفی به

1. belligerent rights

متخاصمان اجازه نمی‌دهد از زیرساخت‌های سایبری خود، درصورتی‌که در سرزمین دولت بی‌طرف واقع شده باشند، برای اهداف نظامی استفاده کنند. بر همین اساس قاعدهٔ ۹۲ از مجموعه قواعد تالین که به استفاده از زیرساخت‌های سایبری واقع در سرزمین دولت بی‌طرف توسط یک طرف مخاصمه اختصاص دارد، اشعار می‌دارد: «اعمال حقوق متخاصم با ابزارهای سایبری در سرزمین بی‌طرف ممنوع است». این قاعده مبتنی بر مواد ۲ و ۳ کنوانسیون پنجم و مواد ۲ و ۵ کنوانسیون سیزدهم لاهۀ ۱۹۰۷ بوده و از وضعیت حقوق بین‌الملل عرفی برخوردار است (Tallinn Manual, 2013: rule 92 and its commentary, para.1).

مادهٔ ۳ کنوانسیون پنجم لاهه متخاصمان را از اعمال زیر منع می‌کند:

«الف) ایجاد یک ایستگاه تلگراف بی‌سیم یا تأسیسات دیگر به‌منظور برقراری ارتباطات با نیروهای متخاصم در زمین یا دریا؛

ب) استفاده از هر گونه تأسیسات از این نوع که توسط آنها پیش از جنگ در سرزمین یک دولت بی‌طرف صرفاً برای اهداف نظامی ایجاد شده و برای [مبادلهٔ] پیام‌های عمومی دایر نگردیده است».

براساس مفاد این ماده، با اعمال آن در فضای سایبر، باید تأکید شود این امر که زیرساخت‌های سایبری مورد نظر به‌وسیلهٔ یکی از متخاصمان پیش یا پس از مخاصمه در سرزمین دولت بی‌طرف ایجاد شده باشد، فاقد اهمیت است و ممنوعیت هر دو مورد را در برمی‌گیرد و در مدتی که مخاصمه جریان دارد، متخاصم مزبور نمی‌تواند از آنها علیه طرف دیگر مخاصمه استفاده کند. بی‌شک درصورتی‌که هدف یک متخاصم از ایجاد و استقرار زیرساخت‌های سایبر در سرزمین دولت بی‌طرف پس از آغاز مخاصمه، صرفاً برقراری ارتباط با نیروهای نظامی آن باشد، براساس بند «الف» مادهٔ ۳ مذکور، اصولاً ایجاد آنها ممنوع است. بنابراین مسئلهٔ ممنوعیت استفاده از این‌گونه زیرساخت‌ها فقط به مواردی محدود می‌شود که پیش از آغاز مخاصمه در سرزمین دولت بی‌طرف ایجاد شده باشند.

مستثنیات ممنوعیت اِعمال حقوق متخاصم با استفاده از زیرساخت‌های سایبری بی‌طرف

ممنوعیت‌های موجود در حقوق بی‌طرفی برای متخاصمان از یک سو، و تعهدات مقررشده برای دولت‌های بی‌طرف از سوی دیگر، مبتنی بر این فرض‌اند که دولت بی‌طرف بر تمام سرزمینش کنترل کامل و مؤثر اِعمال می‌کند. اما مادهٔ ۸ کنوانسیون پنجم لاهه چنین فرضی را در مورد سیستم‌های ارتباطی که مورد استفادهٔ عمومی‌اند، جاری ندانسته و استفاده از آنها را برای هر یک از طرف‌های مخاصمه حتی به‌منظور اِعمال حقوق خود به‌عنوان متخاصم علیه طرف دیگر

مخاصمه، منع نکرده است. مادهٔ ۸ یادشده مقرر می‌دارد: «از یک قدرت بی‌طرف خواسته نمی‌شود که استفاده از کابل‌های تلگراف یا تلفن یا دستگاه‌های تلگراف بی‌سیم متعلق به خود یا شرکت‌ها یا افراد خصوصی را برای متخاصمان ممنوع یا محدود کند» (Hague Convention V, 1907: art.8). هر گونه ممنوعیت یا محدودیت یا تجویز استفاده از این سیستم‌های ارتباطی باید به‌نحو غیرجانبدارانه نسبت به هر دو طرف مخاصمه اجرا شود (Hague Convention V, 1907: art.).

ویژگی‌های فضای سایبر، یعنی، فاقد مرز بودن، به‌هم‌پیوسته بودن زیرساخت‌های سایبر در سراسر جهان، ماهیت دوگانهٔ نظامی و غیرنظامی بیشتر آنها، دسترسی آزاد به اینترنت به‌عنوان شبکه‌ای عمومی که امکان ارسال و جریان‌یابی اطلاعات و بستهٔ داده‌های حاوی بدافزار[1] یا کُدهای بدخواهانه[2] را از مسیرهای متعدد میسر می‌سازد (*see* Droege, 2012: 564-565)، رعایت بی‌طرفی در برابر متخاصمان را اگر نه غیرممکن، حداقل بسیار دشوار ساخته است. این وضعیت، یعنی، دشوار یا حتی غیرممکن بودن اِعمال کنترل مؤثر بر فضای سایبر ممکن است اِعمال مادهٔ ۸ کنوانسیون پنجم لاهه را بر عملیات سایبری انجام‌گرفته از سوی یک دولت متخاصم با استفاده از زیرساخت‌های سایبری و نُدهای اینترنتی دولت بی‌طرف علیه دشمنش منطقی و موجه جلوه دهد، زیرا تکلیفی که بر دولت بی‌طرف بار می‌شود، باید در عمل اجراشدنی باشد و به‌طور منطقی بتوان از آن دولت انتظار ایفا و رعایت تعهداتش را داشت.

با وجود این، باید توجه داشت که مادهٔ ۸ یادشده فقط بر سیستم‌های ارتباطی و صرف ارتباطات اِعمال می‌شود، و نه بر سیستم‌های دیجیتالی تولیدکنندهٔ اطلاعات. ازاین‌رو، دفتر مشاور کل وزارت دفاع ایالات متحده اظهار داشته است که «به‌نظر می‌رسد زبان روشن این موافقت‌نامه [کنوانسیون پنجم لاهه] بر ماهواره‌های ارتباطی و تسهیلات ارتباطی مستقر در زمین اعمال می‌گردد» (US Department of Defense, 1999: 10). به این ترتیب از نظر وزارت دفاع آمریکا قابلیت اِعمال مادهٔ ۸ کنوانسیون پنجم لاهه در فضای سایبر به صِرف ارتباطات محدود می‌شود و حملات سایبری و ارسال و عبور دادن یک سلاح سایبری از زیرساخت‌های دولت بی‌طرف را در برنمی‌گیرد.

شایان توجه آنکه، مجموعه قواعد راهنمای اچ پی سی آر در خصوص *حقوق بین‌الملل قابل اعمال بر جنگ هوایی و موشکی* براساس شناخت از ماهیت فضای سایبر به نتیجه‌ای متفاوت رسیده و مقرر می‌دارد که «وقتی طرف‌های متخاصم شبکه‌ای عمومی و قابل دسترسی آزاد در سطح بین‌المللی را برای اهداف نظامی مورد استفاده قرار می‌دهند، این واقعیت که بخشی از این زیرساخت‌ها در قلمرو صلاحیت یک [دولت] بی‌طرف قرار دارد، نقض بی‌طرفی محسوب

1. malware
2. malicious codes

نمی‌شود» (HPCR Manual, 2009: rule 167(b)). عبارتِ «برای اهداف نظامی مورد استفاده قرار می‌دهند»، بین صِرف ارتباط میان دولت متخاصم با نیروهایش و ارسال یا انتقال بدافزار یا سلاح سایبری از زیرساخت‌های دولت بی‌طرف تمایزی قائل نمی‌شود. در واقع به‌نظر می‌رسد که اچ پی سی آر با توجه به ماهیت و ویژگی‌های کنونی اینترنت و فضای سایبر، اِعمال کنترل مؤثر از سوی دولت بی‌طرف بر ارتباطات و عملیاتی که روی این شبکه‌های عمومی مجازی صورت می‌گیرد و ردیابی آنها را غیرممکن تلقی می‌کند، به‌خصوص اینکه روی خطوط ارتباطی و از مسیرهایی ارسال می‌شوند که پیش از رسیدن به مقصد نهایی خود، از کشورهای مختلف می‌گذرند. این واقعیت‌ها موجب شد که نگارندگان مجموعه قواعد اچ چی سی آر ارتباطات نظامی را اعم از آنکه صرفاً یک ارتباط باشد یا حمله‌ای سایبری از طریق زیرساخت‌های دولت بی‌طرف، ناقض حقوق بی‌طرفی، از جمله ناقض تعهدات دولت بی‌طرف نشمارند.

جالب آنکه بیشتر اعضای گروه کارشناسان بین‌المللیِ تنظیم‌کنندهٔ مجموعه قواعد تالین نیز از این نظر تبعیت کرده‌اند[۱] (Tallinn Manual, 2013: rule 92 and its commentary, para.4). تأکید بر این نکته ضرورت دارد که این نگرش با نص صریح مادهٔ ۸ کنوانسیون پنجم لاهه انطباق ندارد و از آن بسیار فراتر رفته است، به‌نحوی که ممنوعیت مذکور در مادهٔ ۲ همان معاهده که متخاصمان را از عبور دادن «مهمات جنگی یا ملزومات از سرزمین یک دولت بی‌طرف» منع می‌کند، به‌کلی نادیده گرفته است. بعید به‌نظر می‌رسد که رویهٔ امروزی و آیندهٔ دولت‌ها از این برداشت و تفسیر حمایت کند. در واقع، در گزارش سیاست سایبریِ وزارت دفاع ایالات متحده اعلام شده است که این دولت هر "فعالیت سایبری بدخواهانه" را به‌مثابهٔ نقض حقوق بی‌طرفی تلقی می‌کند، صرف‌نظر از اینکه از طریق «رایانه‌ها یا سایر زیرساخت‌های واقع در یک کشور ثالث بی‌طرف انجام گرفته یا صرفاً از طریق آنها ارسال شده باشد» (US Department of Defense, Cyberspace Policy Report, 2011: 8).

پذیرش دیدگاه اچ پی سی آر می‌تواند آثار بسیار خطرناک و غیرقابل قبولی را به‌بار آورد، چراکه در عمل به متخاصم مقابل نیز اجازه می‌دهد در پاسخ به حملهٔ طرف دیگر مخاصمه، از زیرساخت‌های سایبری دولت بی‌طرف استفاده کند. چنین وضعیتی احتمال درگیری دولت بی‌طرف در مخاصمه را بسیار افزایش داده و موجب خواهد شد که وضع حقوقی غیرمتخاصم یا بی‌طرف را از دست بدهد و این نتیجه‌ای است که حقوق بی‌طرفی درصدد اجتناب از آن است (Neff, 2000: 1).

با وجود این، نظر به معضلات رعایت بی‌طرفی در فضای سایبر، شناسایی و ردیابی مرتکبان

---

۱. تر کیب کارشناسان در هر دو گروهی که مجموعه قواعد اچ پی سی آر و تالین را تهیه کرده‌اند و همچنین نهادهایی که اقدامات مذکور در چارچوب آنها صورت گرفته است - دانشگاه هاروارد و مرکز عالی دفاع سایبری تعاونی ناتو - موجب نفوذ واضح دیدگاه‌های ایالات متحده در این اسناد شده است.

حملات سایبری بسیار دشوار است و این احتمال قوی که ممکن است دولت بی‌طرف از این‌گونه حملات سایبریِ متخاصمان مطلع نشود، ضرورت متناسب ساختن قواعد بی‌طرفی و در مواردی بازتعریف برخی مفاهیم حقوق مخاصمات مسلحانه و از جمله حقوق بی‌طرفی را برای اِعمال در فضای سایبر نمایان می‌سازد. مجموعه قواعد تالین که حاصل مطالعه و تلاش گروهی از کارشناسان در چارچوب ناتو برای متناسب کردن قواعد سنتی حقوق بین‌الملل برای کاربرد در فضای سایبر است، حداقل در قواعد ۹۱ تا ۹۵ در زمینهٔ بی‌طرفی، در واقع تکرار قواعد سنتی قراردادی و عرفی حقوق بین‌الملل در این زمینه است و هیچ‌گونه نوآوری در تفسیر قواعد بی‌طرفی برای سازگار کردن آنها با ضرورت‌های مخاصمه و حملات در فضای سایبر در برندارد.

تعهدات دولت‌های بی‌طرف

حقوق بی‌طرفی دولت‌های بی‌طرف را از جانبداری و پشتیبانی و کمک به یک طرف متخاصم به زیان متخاصم دیگر منع می‌کند (Doswald-Beck, 2002: 174). دولت‌های بی‌طرف صرف‌نظر از تکلیف عدم جانبداری، تعهدات دیگری نیز دارند؛ تعهد به ندادن اجازه یا تحمل اِعمال حقوق متخاصم در سرزمینشان و تعهد به پایان دادن و جلوگیری از نقض بی‌طرفی خود از سوی یکی از متخاصمان. عدم رعایت و ایفای این تعهدات از سوی یک دولت بی‌طرف برای آن آثاری حقوقی به‌صورت تکلیف پذیرش اجرای قهریِ حقوق بی‌طرفی از سوی متخاصم زیان‌دیده را در پی خواهد داشت.

تعهد به ندادن اجازه یا عدم تحمل اِعمال حقوق متخاصم

وفق مادهٔ ۵ کنوانسیون پنجم لاهه ۱۹۰۷، یک «دولت بی‌طرف نباید اجازه دهد که هیچ‌یک از اعمال اشاره‌شده در مواد ۲ تا ۴ در سرزمینش روی دهند». مجموعه قواعد تالین با انتقال این تعهدِ دولت‌های بی‌طرف به فضای سایبر، در قاعدهٔ ۹۳ اشعار می‌دارد که «یک دولت بی‌طرف نمی‌تواند آگاهانه اجازهٔ اِعمال حقوق متخاصم به‌وسیلهٔ طرف‌های یک مخاصمهٔ مسلحانه از زیرساخت‌های سایبری واقع در سرزمین یا تحت کنترل انحصاری خود را بدهد» (Tallinn Manual, 2013: rule 93).

چنانکه ملاحظه می‌شود در این قاعده آنچه منع شده اجازهٔ اِعمال حقوق متخاصم به‌طور آگاهانه است که در مادهٔ ۵ کنوانسیون پنجم لاهه دیده نمی‌شود. اهمیت تصریح واژهٔ "آگاهانه" در این قاعده در جای خود روشن خواهد شد. این ماده تعهدی را بر عهدهٔ دولت بی‌طرف می‌نهد مبنی بر اینکه نباید به طرف‌های یک مخاصمهٔ مسلحانه اجازهٔ اِعمال حقوق متخاصم با استفاده از زیرساخت‌های سایبری واقع در سرزمینش یا زیرساخت‌های تحت کنترل انحصاری

آن در خارج از سرزمینش را بدهد. در ضمن بدان معناست کـه چنـین اقـداماتی را تحمـل هـم نباید بکند.

با توجه به اینکه استفاده از زیرساخت‌هـای سـایبری بـی‌طـرف چنانچـه صـرفاً محـدود بـه برقراری ارتباطات نباشد و برای انتقال یک سلاح یا انجام یک حملـهٔ سـایبری یـا یـک فعالیـت بدخواهانهٔ دیگر صورت گیرد، دولت بی‌طرفی که عالماً اجازهٔ چنین استفاده‌ای را بدهد یا چنـین اقدامی را به رغم اطلاع از آن تحمل کند، بر خلاف تعهدات بی‌طرفی خود عمل کرده است. واژهٔ "اجازه" در مادهٔ ۵ کنوانسیون لاهه، علم و آگاهی دولت بی‌طرف را از انجام عملی مغایر مـواد ۲ تا ۴ این معاهده مفروض می‌دارد. ازاین‌رو با آنکه در این ماده تصریح نشده، نگارندگان مجموعـه قواعد تالین با توجه به خصوصیات فضای سایبر ذکر آن را در قاعدهٔ ۹۳ لازم دانسته‌اند.

وجود علم و اطلاع در صورتی احراز خواهد شد که دولت بی‌طرف حمله یا فعالیـت سـایبریِ بدخواهانه را کشف کرده یا مطلع شده باشد که آن فعالیت‌ها از طریق زیرساخت‌هـای سـایبری آن صورت گرفته‌اند. این اطلاع در صورتی به‌منزلهٔ نقض حقوق بی‌طرفی از سوی دولت بی‌طرف خواهد بود که فعالیت سایبری بدخواهانه همچنان ادامه یابـد و دولـت بـی‌طـرف اقـدامی بـرای خاتمه دادن به آن نکند. در واقع، با توجه به سرعت بالای حملات سایبری، اطلاع از وقـوع آنهـا تنها پس از واقعه میسر خواهد بود. در این وضعیت، منطقی به‌نظر نمی‌رسـد کـه ادعـای نقـض تعهدات بی‌طرفی از سوی دولت بی‌طرف پذیرفته شود، درحالی‌کـه مجـالی بـرای جلـوگیری از حمله یا عملیات سایبری بدخواهانه نداشته است. چنین ادعایی در صورتی قابل پـذیرش اسـت که ممنوعیت دادنِ اجازهٔ اِعمال حقوق متخاصم، به‌نحوی تفسیر شود که دولت‌های بی‌طـرف را ملزم به نظارت فعال بر عملیات سایبری نشأت‌گرفته از زیرساخت‌های سـایبری آن یـا از طریـق آنها، کند.

تعهد به پایان دادن و جلوگیری از نقض بی‌طرفی

تکلیف دولت بی‌طرف به ندادن اجازهٔ اِعمال حقوق متخاصم از زیرساخت‌های سـایبری واقـع در سرزمین یا تحت کنترل انحصاری آن، تعهد دیگری را برای دولـت بـی‌طـرف در پـی دارد و آن، تعهد به خاتمه دادن به اِعمال حقوق متخاصم و هر گونه نقض دیگرِ بی‌طرفـی خـود بـه‌وسـیلهٔ یکی از متخاصمان است (San Remo Manual, 1994: para.18 ; HPCR Manual, 2009: rule 168(a) ; US Commander's Handbook, 1997: para.7.3 ; German Manual, 1992: para.1109).

در اینجا این سؤال مطرح می‌شود که آیا تعهد دولـت بـی‌طـرف بـه خاتمـه دادن بـه نقـض بی‌طرفی‌اش تعهدی مطلق است؟ در پاسخ به این پرسش باید گفـت کـه تعهـد مـذکور مطلـق

نبوده و محدود است به آنچه انجامش برای دولت بی‌طرف امکان‌پذیر است. دولت بی‌طرف ملـزم است برای پایان دادن به اِعمال حقوق متخاصم در سرزمین خود، از تمام وسـایلی کـه بـه‌طـور متعارف و معقول برایش فراهم است، استفاده کنمایـد (San Remo Manual, 1994: para.22 ; HPCR Manual, 2009: rule 168(a) ; US Commander's Handbook, 1997: para.7.3 ; German Manual, 1992 : para.1109). این تعهد دولت بی‌طرف دربردارندهٔ تعهدی به استفاده از تمام وسایل ضروری برای پایـان دادنِ مـؤثر بـه اِعمـال حقـوق متخاصـم از زیرسـاخت‌هـای سایبری‌اش، از جمله با توسل به زور است.

به‌نظر می‌رسد که اقدام دولـت بـی‌طـرف از لحـاظ حقـوقی نـوعی اقـدام متقابـل محسـوب می‌شود، با این تفاوت که اقدامات متقابل با توجه به ممنوعیت توسل به زور در روابط بین‌المللی براساس مادهٔ ۲(۴) منشور ملل متحد، شامل توسل به زور نمـی‌شـود (ILC Draft Articles on Responsibility of States, 2001: art.50(1)(a)). اما در اینجا بـه‌دلیـل وجـود یـک مخاصـمهٔ مسلحانهٔ بین‌المللی و به‌منظور جلوگیری از گسترش مخاصمه، دولت بی‌طرف می‌تواند و باید در اجرای تعهد بی‌طرفی خود از تمـام وسـایلی کـه در اختیـار دارد، بـرای پاسـخگویی بـه اِعمـال غیرقانونیِ حقـوق متخاصـم در سـرزمنش اسـتفاده کنـد. ایـن اقـدامات نبایـد از سـوی دولـت متخاصمی که علیه آن انجام مـی‌گیرنـد، خصـمانه تلقـی شـوند (HPCR Manual, 2009: rule 169 ; Hague Convention V, 1907: art.10).

در تعهد دولت بی‌طرف به پایان دادن به نقض بی‌طرفی‌اش، علم و اطـلاع واقعـی یـا فرضـی این دولت از وقوع و در جریان بودن نقض بـی‌طرفـی، مفـروض اسـت (HPCR Manual, 2009: rule 167(b); Heinegg, 2013: p.152). با وجود این، نظر به مجموع ویژگی‌های فضای سـایبر، از یک طرف بسیار احتمال دارد که دولت بی‌طرف از سوء اسـتفاده از زیرسـاخت‌هـای سـایبری خود بی‌اطلاع باشد؛ و از سوی دیگر، تا بخواهـد اقـدام بـه تحقیـق در خصـوص منشـأ حملـه و ردیابی مرتکبان کند، عملیات سایبری مورد نظر به احتمـال زیـاد خاتمـه یافتـه اسـت. در ایـن صورت، آیا تعهد دولت بی‌طرف به‌کلی منتفی می‌شود؟ پاسخ به این پرسش در سـطور بعـد، در ضمن بررسی تعهد دولت بی‌طرف به جلوگیری از اِعمال حقوق متخاصم، داده خواهد شد.

دولت بی‌طرف علاوه‌بر تعهد به پایان دادن به نقض بی‌طرفی‌اش از سوی یکی از متخاصمان، براساس مادهٔ ۵ کنوانسیون پنجم لاهه، مکلف بـه جلـوگیری از اسـتفاده از سـرزمینش توسـط متخاصمان نیز است (Talbot Jensen, 2012: 822-823). دولت بی‌طرف برای ایفای ایـن تعهـد خود ملزم است با اتخاذ تمام اقدامات ممکن و با استفاده از تمام وسایل در اختیار خود از نقـض بی‌طرفی‌اش جلوگیری به‌عمـل آورد (San Remo Manual, 1994: para.15 ; HPCR Manual, 2009: rule 168(a)). این شامل تعهد دولت بی‌طرف به نظارت بر فعالیت‌هـا در سـرزمین خـود به‌منظور جلوگیری از نقض بی‌طرفی‌اش توسط متخاصمان تا آن حدی می‌شـود کـه وسـایل در

اختیارش اجازه می‌دهد :Hague Convention XIII, 1907: art.8 ; San Remo Manual, 1994: para.15 ; HPCR Manual, 2009: rule 168(a) ; German Manual, 1992: para.1109 ; 1125, 1151).

گروه کارشناسان بین‌المللی نگارندهٔ مجموعه قواعد تالین در خصوص وجود تعهد به جلوگیری از اِعمال حقوق متخاصم پیش از وقوع آن به توافق نرسیدند. برخی از اعضای گروه معتقد بودند که این تکلیف در عبارت "آگاهانه اجازه ندهد"(not knowingly allow) مستتر است و اظهار داشتند تا آنجا که اقدامات پیشگیرانه مانند نظارت امکان‌پذیر باشد، ضروری است. البته امکان‌پذیر بودن به شرایط موجود، مثل قابلیت فناورانهٔ دولت بی‌طرف، بستگی دارد. عده‌ای دیگر از اعضای گروه، فقط تعهد دولت بی‌طرف به خاتمه دادن به نقض بی‌طرفی را پذیرفته‌اند و به‌عنوان دلیل به‌ویژه به دشواری‌های ذاتی در اجرای تکلیفی برای احراز خصیصهٔ خصمانه یا بدخواهانهٔ بستهٔ داده‌هایی که از شبکه‌های این دولت عبور داده می‌شوند، اشاره کرده‌اند (Tallinn Manual, 2013: rule 93 and its commentary, paras.3, 6).

همان طورکه دیوان بین‌المللی دادگستری در قضیهٔ *تنگهٔ کورفو* اظهار داشته است، احترام به حاکمیت ارضی سایر دولت‌ها دربردارندهٔ تعهدی برای هر دولت است به اینکه «آگاهانه اجازه ندهد که سرزمینش برای اعمال مغایر حقوق سایر دولت‌ها مورد استفاده قرار گیرد» (ICJ, Reports 1949: 22). بنابراین، دولت‌ها براساس حقوق بین‌الملل مکلف‌اند اقدامات مقتضی برای حفظ منافع سایر دولت‌ها را اتخاذ کنند (ICJ, Reports 1980: para.68). پذیرش وجود تعهدی برای دولت بی‌طرف به پیشگیری، مستلزم نظارت فعالِ چنین دولتی بر عملیات سایبریِ نشأت‌گرفته یا انجام‌گرفته از طریق زیرساخت‌های سایبری واقع در سرزمین آن است.

برخی صاحب‌نظران حقوق مخاصمات مسلحانه معتقدند که دولت بی‌طرف ملزم به اتخاذ تمام اقدامات ممکن برای جلوگیری از اِعمال حقوق متخاصم قبل از وقوع آن است (Kastenberg, 2009: 56-64). بدان معنا که نه تنها اطلاع واقعی یا بالفعل دولت‌های بی‌طرف از فعالیت‌های سایبری بدخواهانه مدنظر است، بلکه وجود چنین اطلاعی مفروض پنداشته می‌شود. لیکن وجود تعهدی برای دولت‌های بی‌طرف به نظارت فعال بر فعالیت‌های سایبری نشأت‌گرفته از زیرساخت‌های سایبری آنها یا انتقال سلاح سایبر یا یک بدافزار از طریق آن زیرساخت‌ها مورد تردید است. بند ۱۵ مجموعه قواعد سَن رِمو در خصوص موارد نقض سرزمین بی‌طرف در فضایی طبیعی، یعنی دریاها، مقرر می‌دارد که «دولت بی‌طرف باید اقداماتی را به‌منظور جلوگیری از نقض بی‌طرفی خود به‌وسیلهٔ نیروهای متخاصم اتخاذ کند، از جمله نجام مراقبت و نظارت تا آنجا که وسایلی که در اختیار دارد، اجازه می‌دهد» (San Remo Manual, 1994: para.15). اما در این خصوص که دولت‌ها، به‌ویژه دولت‌هایی که از آزادی ارتباطات اینترنتی دفاع می‌کنند، با گسترش این تعهد به نظارت و مراقبت، به زیرساخت‌های

سایبری واقع در سرزمینشان موافقت کنند، تردید وجود دارد، چراکه شبکهٔ جهانی اینترنت آزادانه در دسترس همگان است و عملیات سایبری بدخواهانه یا خصمانه می‌تواند از مسیرهای متعدد و با سرعت بالا صورت گیرد.

تسری تعهد به جلوگیری از عبور داده‌های بدخواهانه یا سلاح‌های سایبری ساده به‌نظر می‌رسد، اما کسانی که از این نظر حمایت می‌کنند، معمولاً به پیچیدگی فضای سایبر توجه ندارند، برای مثال، ممکن است داده‌های در حال عبور از زیرساخت‌های سایبری بی‌طرف به‌خودی‌خود بی‌ضرر باشند، اما جزیی از یک بستهٔ بزرگ‌تر از داده‌ها باشند. اگرچه بستهٔ بزرگ‌تر که اجزای سازندهٔ آن از طریق نُدهای اینترنتی کشورهای مختلف ارسال می‌شوند، ممکن است "سلاح سایبری" تلقی شود، اما دولت بی‌طرف محل عبور از این امر اطلاع ندارد. به عقیدهٔ دیوان بین‌المللی دادگستری حتی اگر «یک عمل خلاف حقوق بین‌الملل [در سرزمین یک دولت] روی دهد، نمی‌توان از صِرف واقعیت کنترل اِعمالی ... بر سرزمینش نتیجه گرفت که آن دولت لزوماً می‌دانسته یا می‌بایست از هر گونه عمل غیرقانونی ارتکابی در آن [سرزمین] اطلاع می‌داشت» (ICJ, Reports 1949: 18). به‌علاوه، در بیشتر موارد چنانچه دولت محل عبور ملزم به اتخاذ اقدام پیشگیرانه باشد، بی‌فایده خواهد بود، زیرا ممکن است داده‌ها تغییر مسیر داده شوند و در نهایت بدین‌سان به مقصد نهایی خود در کشور هدف برسند (Heinegg, 2013: 137-138).

درصورتی‌که مقامات دولت بی‌طرف از عملیات سایبری آتی یکی از متخاصمان راجع به انتقال یک سلاح سایبری از طریق زیرساخت‌های سایبری واقع در سرزمین یا تحت کنترل انحصاری خود مطلع شود، بی‌تردید ملزم به اتخاذ تمام اقدامات ممکن برای جلوگیری از عبور آن سلاح سایبری خواهند بود (see Hague Convention XIII, 1907: art.8). در هر حال، می‌توان وجود تعهدی کلی برای دولت بی‌طرف به محفوظ داشتن سیستم‌های سایبری ملی خود از سوء استفاده توسط متخاصمان را پذیرفت. برخی معتقدند که تکلیف پیشگیری از حملات سایبری تکالیف کوچک‌تری را شامل می‌شود، از جمله، وضع قوانین کیفری بر ضد حملات و جرایم رایانه‌ای، تعقیب مرتکبان و همکاری با دولت‌های قربانی حملات سایبری نشأت‌گرفته از درون مرزهای آنها در جریان تحقیق و تعقیب (Sklerov, 2009: 76). همچنین اتخاذ رویکرد مبتنی بر قصد و نیت[1] نسبت به بی‌طرفی به‌عنوان راه چاره پیشنهاد شده است (Kelsey, 2008: 1448-1449). براساس این رویکرد هدایت و انتقال غیرعمدی سلاح‌های سایبری به‌وسیلهٔ یک متخاصم از طریق نُدهای اینترنتی یک دولت بی‌طرف موجب نقض حقوق بی‌طرفی از سوی این دولت نخواهد شد. بدین‌سان، لازم نیست دولت بی‌طرف اقدامی را برای جلوگیری از عبور غیرعمدی سلاح‌های سایبری از زیرساخت‌های سایبری خود اتخاذ کند.

1. intent-based approach

متخاصم زیان‌دیده نیز نمی‌تواند علیه دولت بی‌طرفی که قادر به جلوگیری از عبور سلاح‌های سایبری از شبکه‌هایش نبوده است، اقدام کند. براساس این رویکرد، تا وقتی دولت بی‌طرف اقدامی را در حمایت از حمله به این یا آن طرف مخاصمه اتخاذ نکند، بی‌طرفی‌اش حفظ شده و به این ترتیب خطر گسترش مخاصمه مهار می‌شود، در غیر این صورت، متخاصم مورد حمله قادر به اتخاذ اقدام لازم علیه دولت بی‌طرف خواهد بود.

پیشنهادهای ارائه‌شده بر مبنای رویکرد مبتنی بر قصد یا نیت که با توجه به ویژگی‌های فضای سایبر تنظیم شده‌اند، با آنچه به‌عنوان قواعد ۹۱ تا ۹۴ در مجموعه قواعد تالین در خصوص بی‌طرفی درج شده است، فاصلهٔ بسیار دارد. این مجموعه قواعد راهنما در واقع همان قواعد سنتی عرفی و معاهداتی حقوق بین‌الملل در زمینهٔ بی‌طرفی را برای فضای سایبر تکرار می‌کند و هیچ‌گونه نوآوری در تفسیر آن قواعد برای متناسب ساختن آنها جهت اِعمال در فضای سایبر را در برندارد.

آثار حقوقی عدم ایفای تعهدات از سوی دولت بی‌طرف

چنانچه دولت بی‌طرف قادر یا مایل به ایفای تعهد خود برای پایان دادن به نقض بی‌طرفی‌اش از سوی یکی از متخاصمان نباشد، حقوق بی‌طرفی متخاصمِ مقابل را بدون راه چاره رها نکرده است. در این وضعیت، حقوق بی‌طرفی به متخاصم مورد حمله یا زیان‌دیده اجازه می‌دهد آن اقداماتی را که برای پایان دادن به نقض حقوق بی‌طرفی ضروری است، اتخاذ کند (San Remo Manual, 1994: para.22; HPCR Manual, 2009: rule 168(b); US Commander's Handbook, 1997: para.7.3). اما آیا متخاصم زیان‌دیده حق خواهد داشت به استفاده از زور در فضای سایبر یا به انهدام زیرساخت‌های سایبری دولت بی‌طرف که عمل نقض همچنان از طریق آنها در جریان است، مبادرت ورزد؟

قاعدهٔ ۹۴ مجموعه قواعد تالین مقرر می‌دارد: «درصورتی‌که یک دولت بی‌طرف به اِعمال حقوق متخاصم در سرزمین خود خاتمه ندهد، طرف زیان‌دیدهٔ مخاصمه می‌تواند اقدامات لازم را برای مقابله با این رفتار، از جمله به‌وسیلهٔ حملهٔ سایبری، اتخاذ کند» (Tallinn Manual, 2013: rule 94). دادنِ این حق به متخاصم زیان‌دیده که هر گاه دولت بی‌طرف نخواهد یا نتواند[1] به نقض بی‌طرفی‌اش از سوی طرف دیگر مخاصمه خاتمه دهد، خود به این امر اقدام

---

۱. در خصوص کاربرد معیار یا محک : نخواهد یا نتواند" (unwilling or unable test) در جنگ سایبری به این مقاله که دو سناریو را به‌ترتیب برای مخاصمات مسلحانهٔ بین‌المللی و غیر بین‌المللی طراحی و بررسی کرده است، ر.ک: Deeks, 2013: 1-20

کند، شکل خاصی از خودیاری[1] در برابر نقض تعهد از سوی دولت بی‌طرف محسوب می‌شود (Tallinn Manual, 2013: commentary of rule 94, para.1).

قاعدهٔ ۹۴ تالین بر هر گونه نقض بی‌طرفی اِعمال نمی‌شود، بلکه فقط بر مواردی اِعمال می‌شود که بر طرف مقابل اثر منفی می‌گذارند. پاسخگویی یا عدم پاسخگویی به هر گونه نقض دیگری صرفاً به دولت بی‌طرف مربوط می‌شود و متخاصم زیان‌دیده در صورتی می‌تواند این حق را اِعمال کند که اولاً، نقض سرزمین دولت بی‌طرف "جدی" باشد، یعنی متخاصم ناقض وضعیت بی‌طرفی، با این عمل مزیت نظامی ارزشمندی را بر دشمنش به‌دست آورد (Tallinn Manual, 2013: commentary of rule 94, paras.2-3). جدی بودنِ نقض بی‌طرفی نه به‌طور انتزاعی، بلکه با در نظر گرفتن اوضاع و احوال حاکم در زمان وقوع نقض معلوم می‌شود. نقض بی‌طرفی ممکن است به‌دلیل فراگیر و گسترده بودن نقض یا به‌سبب مزیتی که از این تخلف عاید نقض‌کننده می‌شود، جدی تلقی شود (Tallinn Manual, 2013: commentary of rule 94, para.3).

در ثانی اِعمال حقوق متخاصم در سرزمین دولت بی‌طرف از سوی یک طرف مخاصمه باید تهدیدی فوری متوجه امنیت طرف دیگر مخاصمه کرده باشد و هیچ‌گونه راه عملی و به‌موقعِ دیگری برای اتخاذ اقدام در سرزمین بی‌طرف برای پایان دادن به نقض موجود نباشد (San Remo Manual, 1994: para.22; Tallinn Manual 2013: commentary of rule 94, para.4; HPCR Manual, 2009: rule 168(b)). به‌علاوه، متخاصم زیان‌دیده قبل از اقدام باید به دولت بی‌طرف برای پاسخ به نقض بی‌طرفی مهلت معقولی بدهد (San Remo Manual, 1994: para.22; Tallinn Manual, 2013: commentary of rule 94, para.5).

چنانچه یک طرف مخاصمه به عملیات سایبری بدخواهانه یا حملهٔ سایبری از سرزمین یک دولت بی‌طرف یا با استفاده از زیرساخت‌های سایبری آن اقدام کند، براساس گزارش سیاست سایبری ایالات متحده، این دولت در صورتی اقدام به پاسخ خواهد کرد که آگاه بودنِ دولت بی‌طرف از فعالیت سایبری مورد نظر را احراز کند. در این گزارش ذکر شده است که آمریکا ضمن پایبندی به حقوق مخاصمات مسلحانه، برای تصمیم‌گیری در این مورد چند عامل را در نظر خواهد گرفت: ۱. ماهیت فعالیت سایبری بدخواهانه؛ ۲. نقش کشور ثالث (بی‌طرف)؛ ۳. توانایی و تمایل کشور ثالث به پاسخگویی مؤثر به فعالیت سایبری مزبور؛ و ۴. روش مناسب برای پاسخگویی به مسائل بالقوهٔ حاکمیت شخص ثالث بسته به اوضاع و احوال خاص (US Department of Defense Cyberspace Policy Report, 2011: 8). در ضمن در گزارش یادشده تصریح شده است که این پاسخ‌ها توسل به زور را شامل نخواهد شد.

در واقع گزارش سیاست سایبری ایالات متحده نشان می‌دهد که این دولت قواعد سنتی

1. self-help

حقوق بی‌طرفی را بر رفتار در فضای سایبر قابل اِعمال می‌داند و در ضمن مقررات حاکم بر اقدامات متقابل مندرج در طرح کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت‌ها (ILC, 2001: arts.49-54) را در نظر خواهد گرفت.

با توجه به موضوع و هدف حقوق بی‌طرفی، یعنی جلوگیری از تشدید و گسترش مخاصمهٔ مسلحانهٔ بین‌المللی، ارائهٔ تفسیری از مقررات بی‌طرفی که برای اِعمال در فضای سایبر مناسب باشد، ضروری است. نظر به اینکه حملهٔ سایبری به‌طور بالقوه می‌تواند بر زیرساخت‌های سایبری مورد حمله آثار فاجعه‌بار داشته باشد، این احتمال وجود دارد که متخاصم زیان‌دیده چنانچه منافع امنیتی حیاتی خود را در معرض مخاصره ببیند، اقداماتی را علیه دولت بی‌طرف و زیرساخت‌های سایبری آن، از جمله با استفاده از زور فیزیکی، اتخاذ کند که این امر می‌تواند موجب گسترش مخاصمه شود که مغایر هدف اساسی حقوق بی‌طرفی خواهد بود.

نتیجه

ویژگی‌های فضای سایبر، به‌ویژه وابستگی متقابل زیرساخت‌های سایبر، یکپارچگی شبکهٔ عمومی و جهانی اینترنت، آزادی دسترسی به آن برای همگان و فاقد مرز بودن آن، رعایت حقوق بی‌طرفی و ردیابی موارد نقض بی‌طرفی و شناسایی مرتکبان را دشوار می‌سازد. با افزایش قابلیت‌های سایبری در سطح ملی، اصل حاکمیت سرزمینی به‌خصوص در جریان مخاصمهٔ سایبری تحت فشار فزاینده قرار می‌گیرد، خصوصیات فضای سایبر، هم دولت‌های متخاصم و هم دولت‌های بی‌طرف را در نحوهٔ اعمال حقوق بی‌طرفی به چالش می‌کشد. با وجود این، همان‌طورکه نشان داده شد، حقوق بی‌طرفی بر فضای سایبر قابل اعمال است و ویژگی‌های این عرصهٔ پنجمِ مخاصمات - بعد از زمین، هوا، دریا و فضای ماورای جو – مانعی برای اعمال این حقوق ایجاد نمی‌کند. همان‌طورکه اصل حاکمیت سرزمینی در حقوق سنتیِ بی‌طرفی مانعی برای اعمال حقوق متخاصم از سوی یک طرف مخاصمه در سرزمین دولت بی‌طرفی که به تعهدات خود عمل نکرده و نقض بی‌طرفی‌اش از سوی طرف دیگر مخاصمه را نادیده گرفته است، مانعی برای اعمال این حقوق محسوب نمی‌شود. با توجه به وابستگی متقابل شبکه‌هایی که داده‌ها، از جمله بدافزارها یا سلاح‌های سایبری از طریق آنها ارسال می‌شوند، نباید احتمال هدف قرار گرفتن زیرساخت‌های سایبری دولت بی‌طرف، از جمله با استفاده از زور فیزیکی را از نظر دور داشت. این‌گونه اقدامات نه تنها می‌توانند بر دسترسی با ثبات و قابل اعتماد به شبکهٔ جهانی اطلاعات تأثیر مخرب داشته باشند، بلکه می‌توانند فلسفهٔ وجودی و هدف حقوق بی‌طرفی، یعنی جلوگیری از تشدید مخاصمه را به مخاصره بیندازند.

به‌علاوه، نظر به اینکه جنگ و هدایت مخاصمات در فضای سایبر به‌طور بالقوه ارزان‌تر و کم‌زیان‌تر از مبادرت به حمله و به‌طور کلی اعمال خصمانه در مفهوم متعارف و سنتی است، چه

از حیث مالی و چه از حیث تلفات و جراحات انسانی، ممکن است متخاصمان انگیزه‌های بسیاری برای اقدام به حملات سایبری با استفاده از زیرساخت‌های دول ثالث و بی‌طرف داشته باشند. ازاین‌رو ضروری است حقوق بی‌طرفی برای کاربرد در فضای سایبر تعدیل شده و درک و برداشت نوینی از قواعد آن که با خصوصیات این فضا همساز باشد، ارائه شود. نیل به این هدف، نیازمند حصول تفاهم و همکاری در سطح جهانی است. همان‌طورکه مشاهده شد، در حال حاضر برخی دولت‌ها، و در رأس آنها ایالات متحدهٔ آمریکا در زمینهٔ بازتعریف قواعد حقوق بین‌الملل، از جمله حقوق بی‌طرفی برای اعمال در فضای سایبر پیشتازند. چنانچه کشورهای در حال توسعه، از جمله کشور ما ایران نمی‌خواهند ابتکار عمل به‌طور کامل به دست آنها بیفتد و می‌خواهند در فرایند بازتعریف قواعد موجود یا وضع قواعد جدید حقوق بین‌الملل برای فضای سایبر ملاحظات و منافع آنها نیز در نظر گرفته شود، مشارکت فعال آنها در امر ساماندهی همکاری بین‌المللی به این منظور اجتناب‌ناپذیر است.

منابع

الف) کتاب‌ها

1. Henckaerts, Jean-Marie & DOSWALD-BECK, Louise (2005), *Customary International Humanitarian Law*, Vol. 1, Cambridge/New York: CICR/Cambridge University Press, 628 p.
2. Neff, Stephen C. (2000), *The Rights and Duties of Neutrals: A General History*, Manchester, Manchester University Press, 246 p.

ب) مقالات

3. Brown, Davis (2006), "A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal*, Vol.47, No.1, pp.179-221.
4. Deeks, Ashley (2013), "The Geography of Cyber Conflict: Through a Glass Darkly", *International Law Studies*, Vol.89, pp.1-20.
5. Doswald-Beck, Louise (2002), "Some Thoughts on Computer Network Attack and the International Law of Armed Conflict", *International Law Studies*, Vol.76, pp.163-185.
6. Droege, Cordula (2012), "Get off my Cloud: Cyberwarfare, International Humanitarian Law, and the Protection of Civilians", *IRRC*, Vol. 94, No. 886, pp.533-578.
7. Franzese, Patrick W. (2009), "Sovereignty in Cyberspace: Can It Exist?", *Air Force Law Review*, Vol. 64, No. 1, pp. 1-42.
8. Heinegg, Wolff Heintschel von (2012), "Neutrality in Cyberspace", 4th International Conference on Cyber Conflict, available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/1_3_von_Heinegg_NeutralityInCyberspace.pdf >. 2014/4/6.

9. Heinegg, Wolff Heintschel von (2013), "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, Vol.89, pp.123-156. 10. Jensen, Eric Talbot (2012), "Sovereignty and Neutrality in Cyber Conflict", *Fordham International Law Journal*, Vol.35, No.3, pp.815-841.
10. Kastenberg, Joshua E. (2009), "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law", *Air Force Law Review*, Vol.64, No.1, pp.43-64.
11. Kelsey, Jeffrey T.G. (2008), "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol.106, No.7, pp.1427-1451.
12. Lopez, C. Todd, "Fighting in Cyberspace Means Cyber Domain Dominance", Air Force Print News, Feb. 28, 2007, available at: http://www.af.mil/News/ ArticleDisplay/ tabid/223/Article/127803/fighting-in-cyberspace-means-cyber-domain-ominance.aspx. 2015/9/17.
13. Schaap, J. (2009), "Cyber Warfare Operations: Development and Use under International Law", *Air Force Law Review*, Vol.64, No.1, pp.121-174.
14. Schindler, Dietrich, "Transformations in the Law of Neutrality since 1945", in: Humanitarian Law of Armed Conflict: Challenges Ahead, Essays in Honour of Frits Kalshoven, Delissen, Astrid J. M. (ed.) (1991), Dordrecht: ,pp. 367-386.
15. Shaygan, Farideh, "International Humanitarian Law and Legitimate targets in Cyber Conflict", AALCO Journal of International Law, Vol. 3, No. 2, 2014, pp.67-93.
16. Sklerov, Matthew J. (2009), "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent", *Military Law Review*, Vol.201, Fall 2009, pp.1-85.
17. Tuukkanen, "Sovereignty in the Cyber Domain", in *The Fog of Cyber Defence*, edited by Rantapelkonen, Jari and Salminen, Mirva, Helsinky: National Defence University, Publications Series 2, Article Collection n. 0 10, 2013, pp.37-45.
18. Walker, George K. (2000), "Information Warfare and Neutrality", *Vanderbilt Journal of Transnational Law*, Vol.33, No.5, 1079-1202.
19. Wingfield, Thomas (2000), "The Law of Information Conflict: National Security Law in Cyberspac", Falls Church, VA: Aegis Research Corporation, 2000, 497 p.

ج) آرای قضایی و داوری

20. ICJ, Reports 1949, Corfu Channel Case, Judgment of 9 April 1949.
21. ICJ, Reports 1980, Case concerning United States Diplomatic and Consular Staff in Tehran, Judgment of 24 May 1980.
22. sland of Palmas Case, Netherland v. USA, Reports of International Arbitral Awards, Vol. II, 4 April 1928.

د) سایر منابع

۲۳. قانون جرایم رایانه‌ای جمهوری اسلامی ایران، مصوب ۱۱ بهمن ۱۳۸۸.
24. Commentary on the HPCR Manual on International Law Applicable to Air and

Missile Warfare, Program on Humanitarian Policy and Conflict Research at Harvard University, 2010.
25. Cyber Security Strategy for Germany, Federal Ministry of Interior, 2011, available at: <https:// www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_ Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf>. 2015/10/22.
26. HPCR Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research, University of Harvard, Bern, 15 May 2009, available at: <ihlresearch.org/amw/HPCR%20Manual.pdf>. 2014/2/25.
27. Humanitarian Law in Armed Conflicts- Manual, Bonn 1992, The Federal Ministry of Defence of the Federal Republic of Germany.
28. International Law Association (1998), Helsinki Principles on the Law of Maritime Neutrality, Taipei, ILA Report of Sixty-Eight Conference.
29. ILC (2001), Draft Articles on Responsibility of States for Internationally Wrongful Act.
30. Law of Armed Conflict at the Operational and Tactical Levels, National Defence of Canada, August 2001.
31. San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994.
32. Schmitt, Michael (ed.) (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Groupe of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge/New York, Cambridge University Press: available at: <http://www. ccdcoe.org/249.html>. 2014/02/24.
33. The Joint Service Manual of the Law of Armed Conflict, 2004, UK Ministry of Defence. .
34. The UK Cyber Security Strategy. Protecting and Promoting UK in a Digital World, November 2011, available at: <https://www.gov.uk/government/uploads/system/ uploads/attachment_data/file/60961/uk-cyber-security-strategy-inal.pdf >. 2015/5/15.
35. US Commander's Handbook on the Law of Naval Operations, Newport 1997.
36. US Department of Defense Office of General Counsel (1999), An Assessment of International Legal Issues In Information Operations, available at: <http://www. maxwell.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>. 2014/11/6.
37. US Department of Defense (2005), The Strategy for Homeland Defense and Civil Support, Washington D. C., available at: available at http://www. defense.gov/news/ Jun2005/d20050630homeland.pdf>. 2015/5/21.
38. US Department of Defense (2011), Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, available at: <https://fas.org/irp/eprint/dod-cyber.pdf>. 2015/5/11.
39. US Department of Defense (2012), Dictionary of Military and Associated Terms, 2012, available at: <www.dtic.mil/doctrine/dod_dictionary/>. 2015/10/17.