Volume 14, Issue 51, Spring 2021
Received: 2021/05/05
Date of acceptance: 2021/09/20
Pages: 277-305

فصلنامه علمی تحقیقات حقوقی آزاد
Azad Law Researches Quarterly

دوره چهاردهم/ شماره ۵۱/ بهار ۱۴۰۰
تاریخ دریافت: ۱۴۰۰/۰۲/۱۵
تاریخ پذیرش: ۱۴۰۰/۰۶/۲۹
صفحه: ۲۲۷ الی ۳۰۵

doi: 10.30495/ALR.2021.1872408.1562 **سامانه:** alr.iauctb.ac.ir

Article Type: Research

نوع مقاله: پژوهشی

حملات سایبری و لزوم رعایت اصول اساسی حقوق بشردوستانه در آنها

آذر گیوکی[۱]، محمدعلی کفایی فر[۲]✉، محمدتقی رضایی[۳]

چکیده

زمینه و هدف: همزمان با پیشرفت‌های روزافزون علوم ارتباطات و فناوری اطلاعات، شاهد تغییر جبهه‌های نبرد، از سرزمین به مفهوم سنتی آن به سرزمین در مفهوم مجازی و اعمال توسل‌به‌زور و اقدامات خصمانه در فضای سایبری از طریق حملات سایبری هستیم. حملات سایبری، همچون سایر حملات به روش‌های سنتی، به عنوان مظهر قوه قهریه کشورها علیه یکدیگر شناسایی شده و با توجه به آثار مخرب و گاه، فاجعه‌بار آنها، لزوم رعایت اصول و قواعد حقوق بین‌الملل بشردوستانه در آنها، موضوعی بااهمیت است که مورد توجه محققان زیادی بوده و در اسنادی چون دستورالعمل‌های تالین، بررسی شده است.

روش: این تحقیق، با نگاهی توصیفی-تحلیلی و با استفاده از شیوه مطالعات کتابخانه‌ای انجام شده است.

یافته‌ها و نتایج: در این تحقیق، تلاش شده است اصول اساسی حقوق بشردوستانه بین المللی، در ارتباط با حملات و جنگ‌های سایبری، پس از بیان تعاریفی از اصول اساسی حقوق بین‌الملل بشردوستانه و بررسی این اصول در اسناد مرتبط و نیز، دستورالعمل‌های تالین، به عنوان سندی غیرالزام‌آور در راستای عرفی‌کردن حقوق بین‌المللی مربوط به حملات سایبری، هدف تحقیق، یعنی، لزوم رعایت این اصول با توجه به شرایط قابل‌پیش‌بینی در حملات سایبری را اثبات نموده و به شیوه تعمیم این اصول اساسی، به حملات سایبری پرداخته شود.

واژگان کلیدی: اصول حقوق بشردوستانه، جنگ سایبری، حملات سایبری، حقوق بشردوستانه، فضای سایبری.

❋ استناددهی (APA): گیوکی، آذر؛ کفایی فر، محمدعلی؛ رضایی، محمدتقی. (۱۴۰۰). **حملات سایبری و لزوم رعایت اصول اساسی حقوق بشردوستانه در آنها.** تحقیقات حقوقی آزاد. ۱۴(۵۱): ۳۰۵-۲۲۷. قابل بازیابی از:
http://alr.iauctb.ac.ir/article_686224.html

۱. دانشجوی دکتری حقو بین‌المللی عمومی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران. رایانامه: azarg1359@gmail.com
۲. استادیار حقوق بین‌الملل عمومی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران. (نویسنده مسئول). رایانامه: ma.kafaeifar@gmail.com
۳. استادیار حقوق، دانشکده علوم اجتماعی، دانشگاه پیام نور، تهران، ایران. رایانامه: rezaei.mt@yahoo.com

مقدمه

به دنبال نوآوری‌هایی که پس از اختراع رایانه‌ها در عرصه ارتباطات و فناوری اطلاعات رخ داد، جان وون نویمان، یک ریاضیدان و طراح اولیه سیستم‌های محاسباتی، در سال ۱۹۴۹ به ارائه یک سری سخنرانی‌ها در دانشگاه ایلینوی پرداخت که امکان توسعه ماشین‌آلاتی که خود تکثیر می‌کنند، مورد بررسی قرار داد و ماشینهایی را که می‌توانند کپی خود را تولید و به زیرمجموعه‌های خود منتقل کنند (ماشین‌های خودهمسان‌ساز[1])؛ این تئوری، در حالی که به لحاظ علمی و کاربردی بودن، مشروع می‌نمود، اما پیش‌برنده تئوری ویروس‌ها و کرم‌های کامپیوتری مدرن امروزی، به عنوان سیستم‌های خودهمسان ساز شدکه اغلب، نرم‌افزارهایی مخرب، خصمانه، نفوذی وناخوشایند خواهند بود[2]. نسل اول نرم‌افزارهای مخرب در دهه ۱۹۷۰ اغلب، موجب بروز آسیب کمتری نسبت به حافظه کامپیوتر و قربانیان آن بود؛ پس از آن و هنگامی که رایانه شخصی در دهه ۱۹۸۰ به بازار آمد، بدافزار به چیزی مخرب‌تر تبدیل شد؛ ویروس‌ها، کرم‌ها و سایر انواع بدافزارها به سرعت در سراسر اینترنت گسترش یافت و از بین‌بردن داده‌ها، بیش از حد و به‌طور کلی باعث ویرانی سیستم‌های اطلاعاتی شد.[3]

آژانس پروژه‌های تحقیقاتی پیشرفته آرپا[4]، بخش تحقیق وزارت دفاع ایالات متحده[5]، با تامین مالی یک تیم واکنش اضطراری رایانه در دانشگاه ملون نسبت به هماهنگی و پاسخگویی به مسائل امنیتی کامپیوتر اقدام کرد و علاوه بر این، آرپا از شورای تحقیقات ملی[6] برای مطالعه درباره «امنیت و اعتماد» سیستم‌های فناوری اطلاعات و ارتباطات آمریکا تقاضای انجام تحقیقاتی کرد و در نهایت در سال ۱۹۹۱، شورای تحقیقات ملی گزارش خود را منتشر و اشاره کرد «ممکن است تروریست‌ها هم بتوانند با یک صفحه کلید آسیب بیشتری حتی در مقایسه با یک بمب ایجاد کنند»[7]. در سال‌های اخیر و پس از آنکه شورای تحقیقات ملی، خطرات مربوط به استفاده از رایانه را برجسته کرده است، جامعه جهانی بیشتر و بیشتر به رایانه و استفاده روزمره از اینترنت، وابسته شده است و همین وابستگی موجب پیدایش و افزایش حملات سایبری شده است؛ چرا که با تکامل سیستم‌های رایانه‌ای و استفاده از اینترنت، باید امنیت سیستمها نسبت به حمله به زیرساخت‌های سیستم مالی، تجارت، عملیات دولتی، از جمله نظامی و در نهایت، امنیت ملی را در نظر داشت (روشینی[8]، ۲۰۱۰: ۹۷-۹۸).

---

[1] Self-replicate
[2] See www.oed.com
[3] See www.virus-scansoftware.com
[4] Advanced Research Projects Agency(ARPA)
[5] DARPA
[6] National Research Council(NRC)
[7] See www.cert.org
[8] Roscini

با این توضیحات، می‌توان گفت فضای سایبری به یک میدان جدید نبرد تبدیل شده است و روزبه‌روز بر تعداد حملات به انحاء مختلف افزوده می‌گردد.

شاید بتوان نخستین حمله اینترنتی سازمان‌یافته و دولتی را حمله سرویس‌های اطلاعاتی روسیه به شبکه‌های اینترنتی استونی در سال ۲۰۰۷ دانست که طی آن، برای چند ساعت شبکه‌های اینترنتی بانک‌های اصلی استونی مختل و انتشار تمامی روزنامه‌های اصلی و همچنین، ارتباطات دولتی این کشور متوقف شد (جاشوآ[1]، ۲۰۰۷)؛ پس از آن و در ادامه حملات مختلف سایبری صورت گرفته در جای جای جهان، حمله‌ای موسوم به گوست نت[2] در طی سال‌های ۲۰۰۹-۲۰۰۷ سفارتخانه‌های بسیاری از کشورها نظیر آمریکا و دفتر تبعیدیان تبت در هند را هدف قرار داد و موجب ایجاد آسیب‌های فراوان و اختلال در امور آنها شد؛ حمله سایه در ابر[3] طی سالهای ۲۰۱۰-۲۰۰۹ دفاتر دولتی هند و تبت و دفتر سازمان ملل در هند را دوباره مورد هدف قرار داد؛ حمله آرورا[4] در آمریکا و در سال ۲۰۰۹ موتور جستجوگر گوگل را هدف قرار داد منجر به سرقت رمز عبور کاربران گوگل شد؛ طی سال‌های اخیر چهار ویروس رایانه‌ای فلیم[5]، دوکو[6]، وایپر[7] و استاکس نت[8] تأسیسات هسته‌ای و نفتی ایران را مورد هدف قرار داده‌اند.

در حالی‌که قانونی بودن جنگ سایبری هنوز مورد بحث است، زیرا هر حمله سایبری را نمی‌توان جنگ سایبری قلمداد کرد و قواعد مربوط به مخاصمات مسلحانه و حقوق جنگ را بر آن بار نمود، جامعه بین‌المللی می‌کوشد تا با استفاده از ابزارهای بین‌المللی، قوانین جنگ‌های سنتی را به جنگ با فن‌آوری‌های جدید تعمیم دهد.

۱. حملات سایبری و حقوق بشردوستانه بین‌المللی

حقوق مخاصمات مسلحانه، یا حقوق بشردوستانه بین المللی، مجموعه قواعد حقوق بین‌المللی است که ضمن تعیین حقوق افراد انسانی و کشورها در مخاصمات مسلحانه، اعم از بین‌المللی یا غیربین‌المللی، تکالیف افراد و کشورها را نیز در آن مخاصمات مشخص می‌کند؛ با محدود کردن صدمات و لطمات ناشی از مخاصمات مسلحانه و ممنوع کردن استفاده از برخی سلاح‌ها، از افراد نظامی و غیرنظامی و نیز اهداف غیرنظامی در مخاصمات مسلحانه حمایت می‌کند (ضیایی بیگدلی، ۱۳۹۰، ۲)؛ بنابراین، حقوق بین‌الملل بشردوستانه، حقوق هدایت رفتار در مخاصمات مسلحانه با نگاهی به کاهش آلام و رنج بشر می‌باشد (دینستین[9]، ۲۰۱۶: ۲۰) که در مورد هدف قرار دادن هر

---

[1] Jashua
[2] Ghostnet
[3] Shadow in cloud
[4] Arora
[5] Flame
[6] Duku
[7] Viper
[8] Stuxnet
[9] Dinstein

شخص یا شیءای صرفنظر از ابزارها و روشهای جنگی به کار رفته، اعمال میشود (دستورالعمل تالین۱ [1]، ۲۰۱۳: قاعده ۳۰).

پیششرط اعمال حقوق بشردوستانه در حملات سایبری، شناسایی آن وضعیت، به عنوان یک مخاصمه مسلحانه است. به این ترتیب، مطابق آنچه در قاعده ۲۰ دستور العمل تالین۱ و قاعده ۸۰ دستورالعمل تالین ۲، مقرر است، عملیات سایبری انجام شده در بستر یک مخاصمه مسلحانه، تابع حقوق مخاصمات مسلحانه است. کما اینکه در سال ۲۰۰۷ دولت استونی به دفعات مکرر هدف عملیات سایبری قرار گرفت، با این حال حقوق مخاصمات مسلحانه در آن خصوص اعمال نشد؛ زیرا آن وضعیت به سطح یک مخاصمه مسلحانه نرسیده بود. در مقابل، طی مخاصمه مسلحانه میان گرجستان و روسیه در سال ۲۰۰۸ به دلیل توسل به عملیات سایبری در راستای کمک به مخاصمه، شناسایی شد و حقوق مخاصمات مسلحانه بر عملیات سایبری حادث شده، حاکم شد.

۱-۱. معیارهای شناسایی عملیات سایبری به عنوان حمله سایبری

ژان پیکته [2]، در تفسیر ماده ۲ مشترک، معیاری را مطرح نموده است که مطابق آن، توسل به زور زمانی به حد مخاصمه مسلحانه میرسد که توسل به زور اعمال شده حائز شرایط «شدت»، «استمرار» و «محدوده کافی» باشد (شارپ [3]، ۱۹۹۹: ۶۰-۶۱) ؛ با برداشت از این معیار در خصوص مخاصمات مسلحانه یا توسل به زورهای مدرن، از جمله حملات سایبری، سه دیدگاه مطرح شده است:

نخستین دیدگاه، دیدگاه ابزارمحور است که با اعمال آن باید ارزیابی کرد که آیا خسارتهای حاصله از یک حمله سایبری که قبلاً از طریق حملات سنتی حاصل میشد؛ به عنوان مثال با اعمال این مدل، حمله سایبری که منجر به قطع شبکه برق میشود، میتواند حمله مسلحانه قلمداد شود؟ زیرا قبل از پیشرفت و توسعه ابزارها و قابلیتهای سایبری، تخریب و انقطاع شبکه برق، نوعاً مستلزم بمباران ایستگاهها و نیروگاههای برق یا استفاده از سایر ابزارهای انفجاری سنتی بوده است (دینستین [4]، ۲۰۰۵: ۱۰۰). مزیت اصلی رویکرد مبتنی بر ابزار، ساده بودن کاربرد است، زیرا استفاده از اسلحه و نیروهای نظامی نسبتا آسان است.

دیدگاه دوم، دیدگاه نتیجهمحور یا اثرگراست. این دیدگاه به اثر و نتیجه کلی حمله سایبری نسبت به دولت قربانی نظر دارد؛ به عنوان مثال، با توجه به این دیدگاه، دستکاری در اطلاعات

---

[1] Tallin Manual 1.0

[1] Jean Pictet

ژان پیکته (۲۰۰۲-۱۹۱۴) حقوقدان برجستهی سوئیس، کارشناس حقوق بشردوستانهی بینالمللی، عضو عالیرتبه و نائب رئیس اسبق کمیته بینالمللی صلیب سرخ و طراح اصلی کنوانسیونهای چهارگانهی ژنو و پروتکل الحاقی آن بوده است.

[3] Sharp

[4] Dinstein

مؤسسات مالی و بانکی یک کشور از طریق فضای سایبر که موجب برهم خوردن سیستم اقتصادی آن می‌شود، می‌تواند حمله مسلحانه تلقی گردد؛ زیرا چنین اعمالی هرچند شبیه حملات سنتی نیست، اما از آنجا که در اثر دستکاری و نفوذ در سیستم‌های اقتصادی صدماتی به آنها وارد آمده و موجب از کار افتادن آنها می‌شود، این نتیجه با اثر یک حمله مسلحانه برابری می‌کند. پروفسور مایکل اشمیت، معروف‌ترین مفسر رویکرد مبتنی بر اثرات برای تعیین زمان یک حمله مسلحانه، استدلال می‌کند که اثرات حمله سایبری باید با توجه به شش عامل تعیین شود: (۱) شدت: نوع و مقیاس آسیب؛ (۲) فوریت: چطور به سرعت آسیب پس از حمله رخ می‌دهد؛ (۳) مستقیم بودن: طول زنجیره بین حمله و آسیب؛ (۴) تهاجم: درجه‌ای که حمله به قلمرو کشور قربانی نفوذ می‌کند؛ (۵) اندازه‌گیری: درجه‌ای که آسیب را می‌توان اندازه‌گیری کرد؛ و (۶) مشروعیت احتمالی: اهمیت داده شده به فعالیت‌های سایبری؛ به طور کلی، حملات سایبری استثنا بر قاعده هستند (اشمیت[1]، ۱۹۹۹: ۹۱۵).

دستورالعمل تالین ۲، نیز، در این زمینه، دیدگاه مخالفی را مطرح ساخته است که تصدیق می‌نماید براساس قضیه نیکاراگوئه، هرگونه استفاده غیرقانونی از زور که حمله مسلحانه به شمار می‌آید، موجب بروز حق دفاع از خود می‌گردد؛ هیچ آستانه شدتی وجود ندارد که توسل به زور را از حمله مسلحانه تفکیک کند و به این ترتیب، هیچ فاصله‌ای میان توسل به زور غیرقانونی و حمله مسلحانه وجود ندارد. رویکرد اخیر بیانگر آن است که احتمال دارد دولت‌ها از جمله در حین اتخاذ تصمیم راجع به توصیف یک عملیات همچون عملیاتی سایبری به عنوان توسل به زور، عواملی را که ذیلاً بیان می‌شود، مطمح‌نظر قرار دهند و اهمیت قابل‌توجهی برای آن‌ها قائل شوند. لازم به تأکید است که این عوامل صرفاً اسبابی هستند که انجام ارزیابی از سوی دولت‌ها راجع به توسل به زور را تحت تأثیر قرار می‌دهند؛ این عوامل معیارهای حقوقی رسمی نمی‌باشند؛ این عوامل عبارتند از (۱) شدت؛ (۲) فوریت؛ (۳) بی‌واسطگی؛ (۴) میزان نفوذپذیری[2]؛ (۵) سنجش‌پذیری آثار؛ (۶) ماهیت نظامی؛ (۷) مشارکت دولت؛ (۸) مشروعیت فرضی. عوامل پیش‌گفته حصری نیستند، بلکه بسته به شرایط پیرامونی، ممکن است دولت‌ها به دیگر عوامل همچون فضای غالب سیاسی، حکایتِ عملیات سایبری از توسل به زور نظامی در آینده، هویت مهاجم، سابقه عملیات‌های سایبری مهاجم و ماهیت هدف (مانند زیرساخت حساس) توجه کنند (گیوکی و دیگران، ۱۳۹۷: ۱۷۹)

[1] Schmit
[2] Invasiveness

سومین دیدگاه، جنبه مطلق داشته و هر نوع حمله علیه زیرساخت‌های حیاتی ملی[1] یک دولت را بر مبنای نتایج سنگینی که از حمله به چنین سیستم‌های زیرساختی حاصل می شود، حمله مسلحانه می‌داند (شارپ، ۱۹۹۹:۱۳۱).

هرچند محتوای هر سه دیدگاه مورد مجادلات و مباحثات فراوانی واقع شده، اما اهمیت اساسی آنها در این حقیقت نهفته است که هر سه دیدگاه به این نکته مهم تأکید دارند که عملیات سایبری می‌تواند تنها در برخی حالات، حمله مسلحانه محسوب شود.

از دیگر سوی، اکثر مفسران، امروزه واژه «زور»[2] در بند ۴ ماده ۲ منشور ملل متحد را عملاً مترادف با نیروی نظامی یا مسلح، می‌دانند، اما این لزوماً به این معنی نیست که جلوگیری از توسل به زور بین دولتها، محدود به استفاده از تسلیحات شیمیایی، بیولوژیکی، یا هسته‌ای می‌شود. با توجه به نظر مشورتی دیوان بین‌المللی دادگستری، درباره قانونی بودن تهدید یا استفاده از تسلیحات هسته‌ای (نظریه مشورتی دیوان بین‌المللی دادگستری درباره تهدید یا استفاده از سلاح‌های هسته‌ای[3]، ۱۹۹۶: ۳۹)، منظور از این ممانعت، «ممانعت از هرنوع توسل به زور، بدون توجه به تسلیحات به کار گرفته شده» است. تردیدی نیست که عملیات سایبری، از این جهت که اثرات آنها قابل مقایسه با سلاح‌های شیمیایی، بیولوژیکی یا هسته‌ای است، تحت حکومت بند ۴ ماده ۲ منشور ملل متحد قرار می گیرند. این قطعاً شامل استفاده از عملیات سایبری به عنوان ابزار تهاجمی یا دفاعی که برای کشتن یا واردکردن آسیب به افراد یا تخریب زیرساخت‌ها هم می‌شود، بدون توجه به اینکه این چنین تخریبی شامل خسارات فیزیکی، صدمات کارکردی یا هر دوی آنها باشد (ملزر[4]، ۲۰۱۱: ۷). دیوان بین المللی دادگستری در سال ۱۹۸۶ در قضیه نیکاراگوئه[5] (پاراگراف‌های ۱۷۶-۱۸۸) تأکید کرد تعریفی از حمله مسلحانه نه در منشور و نه در حقوق قراردادی نشده است. با این وجود، دیوان در رأی مشورتی خود درباره سلاح‌های هسته ای ۱۹۹۶، متذکر شده که ماده ۵۱ منشور اشاره به سلاح خاصی نداشته و در خصوص هرگونه توسل به زور صرف نظر از نوع سلاح کاربردی اعمال می‌شود. در واقع، نه نقش یک آلت یا ابزار، نه استفاده معمول از یک اسلحه آن را سلاح نمی‌سازد، بلکه قصدی که پشت توسل به آن سلاح نهفته است و اثرات آن است که آن را سلاح می‌سازد. به عبارت دیگر، کاربرد هرگونه ابزار یا تعدادی از ابزارها که با قصد وارد آوردن ضرر و زیان قابل‌توجه به زندگی افراد و تخریب گسترده همراه اموال می‌شود، از شروط حمله مسلحانه می‌باشد (زمانک[6]، ۲۰۱۰:۲۱). چنین نتیجه‌گیری با تأیید حق دفاع مشروع ایالات متحده در پاسخ به حملات ۱۱ سپتامبر ۲۰۰۱ توسط شورای امنیت تقویت

---

[1] National Critical Infrastructure.
[2] Force
[3] ICJ, Legality of the Threat or Use of Nuclear Weapons advisory opinion
[4] Melzer
[5] ICJ Judgment, Nicaragua V. United states, 1986
[6] Zemanek

می‌شود؛ زیرا سلاح‌های به کارگرفته شده در آن قضیه، هواپیماهای ربوده شده بودند (قطعنامه شورای امنیت ۱۳۰۸، ۲۰۰۱ و قطعنامه شورای امنیت ۱۳۷۳، ۲۰۰۱[1]). به این ترتیب، این نکته که در حملات سایبری از سلاح‌های کلاسیک استفاده نمی‌شود، به این معنا نیست که نمی‌توان آنها را به مثابه حمله مسلحانه در نظر گرفت (روشینی، ۱۱۴:۲۰۱۰).

حمله سایبری، به عنوان «هر اقدامی که به منظور تخریب کارکرد شبکه‌های کامپیوتری انجام شده و یک هدف امنیت ملی یا سیاسی، ورای آن وجود داشته باشد» (هاثاوی و دیگران[2]، ۲۰۱۲: ۸۲۳)، به تعبیر قاعده ۳۱ دستورالعمل تالین ۱ و قاعده ۹۲ دستورالعمل تالین ۲، «به عملیات سایبری، (خشونت‌آمیز)، خواه تهاجمی یا دفاعی، اطلاق می‌شود که منطقاً انتظار می‌رود باعث صدمه یا مرگ اشخاص، خسارت یا خرابی اشیاء گردد».

در راستای بیان توضیحات و مثالهایی از حملات سایبری، می‌توان به مواردی اشاره کرد؛ از جمله اینکه یک عملیات سایبری که کار سامانه اسکادا در کنترل یک شبکه برق را تغییر می‌دهد و منجر به آتش‌سوزی می‌شود؛ از آنجا که پیامد آن مخرب است، یک حمله تلقی می‌شود؛ لازم به ذکر است که خرابی یا خسارت جزئی، به آستانه صدمه مورد نیاز در این قاعده نمی‌رسد؛ رها نمودن آب سد از طریق دستکاری سامانه اسکادا که منجر به اختلال در مسیر رودخانه می‌شود، بدون اینکه خسارتی به سامانه اسکادا وارد نماید، یک حمله سایبری محسوب است؛ کما اینکه اگر این عملیات، با استفاده از ابزارهای فیزیکی نظیر بمباران سد انجام می‌شد، جای هیچ‌گونه تردیدی برای قلمداد کردن آن به عنوان یک حمله نیست؛ جراحت یا مرگ اشخاص یا خرابی و خسارت اشیاء فیزیکی بر اثر عملیات سایبری، مبین موضوع حمله بوده و این عملیات یک حمله سایبری محسوب می‌شود. بیماری و آسیب‌های شدید ذهنی که معادل جراحت هستند، در صورتیکه بر اثر عملیات سایبری عارض شده باشد، مورد حمایت حقوق بشردوستانه خواهد بود؛ عملیات سایبری، علیه داده که عاملیت اشیاء فیزیکی به آن وابسته است، منجر به شکل‌گیری یک حمله می‌شود. اعمال خشونت‌آمیز یا فعالیت‌هایی که دارای آثار خشونت‌بارند، چنانچه علیه غیرنظامیان یا اشیاء غیرنظامی یا سایر افراد یا اشیاء حمایت شده بکار گرفته شود، حمله تلقی می‌شود؛ آسیب یا تخریب اموال فرهنگی دیجیتال، نیز موضوع حقوق مخاصمات مسلحانه قرار خواهد گرفت؛ اختلال در کارکرد یک شیء که مستلزم بازسازی داده‌ها است، اما نیازمند جابجایی اجزای فیزیکی یا نصب دوباره سیستم عامل نیست، یک حمله تلقی می‌شود؛ یک عملیات سایبری که باعث خسارت جانبی قابل‌پیش‌بینی در سطح بیان شده، معادل حمله‌ای است که حقوق مخاصمات مسلحانه مرتبط به‌ویژه در خصوص اصل تناسب، اعمال می‌کند؛ اشاعه یک بدافزار یا عیوب در مرحله تولید که یا زمان را به تأخیر می‌اندازد یا با وقوع حادثه خاصی فعال می‌شود، چنانچه نتایج

[1] S.C/Res/1308, 2001 and S.C/Res/1373, 2001
[2] Hathaway and others

مورد نظر آنها به آستانه مورد نظر آسیب برسد، حمله تلقی می‌شوند. حمله‌ای که با موفقیت جلوی آن گرفته شده است و هیچ خسارت واقعی به بار نیاورده است، به موجب حقوق مخاصمات مسلحانه همچنان به عنوان یک حمله است. از این رو، یک عملیات سایبری که توسط دفاع غیرعامل سایبری نظیر فایروال‌ها (دیواره آتش)، نرم‌افزار آنتی‌ویروس و یا سیستم‌های عیب‌یاب یا سیستم‌های ممانعت‌کننده شکست می‌خورد، چنانچه در صورت فقدان چنین اقدامات دفاعی، به احتمال زیاد عواقب لازمه یک حمله را در برداشته باشد، به عنوان حمله تلقی می‌شود. حمله‌ای که با بمب‌های هدایت شده لیزری انجام شود، از مصادیق حملات سایبری خواهد بود (دستورالعمل تالین ۱، ۲۰۱۳: ۹۳-۹۶).

۱-۲. اعمال حقوق مخاصمات مسلحانه بر عملیات سایبری

حقوق مخاصمات مسلحانه در شرایط سه‌گانه ذیل، بر عملیات سایبری قابل اعمال خواهد بود:

۱.در جایی که حملات سایبری به عنوان بخشی از یک مخاصمه سنتی و در راستای آن صورت گیرد. مخاصمه میان روسیه و گرجستان، در سال ۲۰۰۸، نمونه عینی اینگونه حملات محسوب است.

۲.در جایی که حملات سایبری، به طور مستقل شروع می‌شوند. حمله ویروس استاکس نت در سال ۲۰۰۹- ۲۰۱۰، به تأسیسات هسته‌ای ایران، نمونه بارز حملات مستقل است.

۳. در جایی که اقدامات نظامی صورت گرفته در سطحی نیست که بتوان آنها را حمله مسلحانه تلقی کرد و در این حال، حملات سایبری وسیع نیز با اقدامات مذکور توأمان می‌شوند (دینیس، ۱۳۹۵: ۱۳۹). عملیات سایبری ممکن است جزء مکمل یک عملیات گسترده که یک حمله را شکل می‌دهد، باشد؛ برای مثال، ممکن است یک عملیات سایبری به منظور از کار انداختن اقدامات دفاعی در قبال هدفی که متعاقباً مورد حمله قرار می‌گیرد، به کار رود. در این صورت، این عملیات سایبری یکی از اجزاء عملیاتی است که به عنوان یک حمله محسوب می‌شود.

عملیات سایبری که به عنوان مخاصمه مسلحانه شناسایی شده است، ممکن است مخاصمه مسلحانه بین‌المللی یا غیربین‌المللی شناخته شده و از این رو، تابع اصول و قواعد حقوق بشردوستانه بین‌المللی واقع شود.

ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو۱۹۴۹، در ارتباط با شناسایی یک وضعیت به عنوان مخاصمه مسلحانه بین‌المللی، مقرر داشته است: «علاوه بر مقرراتی که باید در زمان صلح به موقع اجرا گذاشته شود، کنوانسیون حاضر، در صورت وقوع جنگی که رسماً اعلام شده باشد و یا هرگونه، مخاصمه مسلحانه میان دو یا چند کشور معظم متعاهد بروز نماید، اجرا خواهد شد؛ ولو اینکه یکی از دولتهای مزبور، وجود چنین مخاصمه‌ای را تصدیق نکرده باشد. این کنوانسیون در

هر مورد که تمام و یا قسمتی از خاک دولت معظم متعاهد اشغال شود نیز به موقع اجرا گذاشته خواهد شد، حتی اگر این اشغال با هیچ‌گونه مقاومت نظامی مواجه نشده باشد»؛ به این ترتیب و با توجه به اینکه کنوانسیون‌های ژنو۱۹۴۹، به عنوان بخشی از حقوق بین‌الملل عرفی، درباره همه دولت‌های متعاهد و غیرمتعاهد، قابل‌اعمال خواهد بود، این ماده بیانگر این مطلب است که اولاً، مخاصمات مسلحانه بین‌المللی، مخاصماتی هستند که میان دولت‌ها روی می‌دهند و این وضعیت، زمانی است که یک و یا چندین دولت در مقابل دولتی دیگر به نیروی مسلح متوسل می‌شوند. ثانیاً، عدم اعلام حالت جنگی و یا عدم شناسایی آن از سوی طرفین مخاصمه، ملاک و ضابطه‌ای برای تشخیص مخاصمات مسلحانه بین‌المللی نیست؛ بنابراین، می‌توان گفت که هر اختلافی که میان دولت‌ها به وجود آمد و موجب درگیری و در نتیجه، به‌کارگیری نیروی مسلح میان آنها شود، یک مخاصمه مسلحانه بین‌المللی در معنای ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو می‌باشد (دینیس، ۱۳۹۵: ۱۳۰). به اتکای این تعاریف، حقوق مخاصمات مسلحانه، مجموعه قواعدی مرتبط با قانونمند ساختن و محدود کردن اعمال ارتکابی در زمان وقوع مخاصمه مسلحانه از طریق تعیین حقوق و تکالیفی برای طرفین مخاصمه و دولت‌های ثالثی که شرکتی در جنگ ندارند، می‌باشد و شامل قواعدی الزام‌آور برای مسائل مربوط به ترک مخاصمه، ایجاد ممنوعیت متقابل در خصوص برخی ابزارهای جنگی به دلیل قدرت تخریبی فوق‌العاده آنها مثل سلاح‌های سمی، ایجاد ممنوعیت در خصوص برخی ابزارها و شیوه‌های جنگی و حمایت از قربانیان جنگی مانند غیرنظامیان، زخمیان، بیماران و اسیران جنگی است (کولب و هاید، ۱۳۹۳: ۳۳).

قاعده ۸۲ دستورالعمل تالین ۲، بیان داشته است «یک مخاصمه مسلحانه بین‌المللی، در صورت وجود عملیات‌های متخاصمانه میان دو یا چند کشور که ممکن است شامل یا محدود به عملیات‌های سایبری باشند، وجود دارد»؛ معیارهای عموماً پذیرفته شده برای وجود یک مخاصمه مسلحانه بین‌المللی، که بازتاب حقوق بین‌الملل عرفی هستند، از کنوانسیون‌های ۱۹۴۹ ژنو گرفته شده‌اند که مقرر می‌دارد: «کنوانسیون حاضر بر کلیه موارد اعلام شده به عنوان جنگ و هر مخاصمه مسلحانه دیگری که ممکن است میان دو یا چند طرف معظم متعاهد در بگیرد، حتی اگر وضعیت جنگی از سوی یکی از آن‌ها به رسمیت شناخته نشده باشد، اِعمال خواهد شد. کنوانسیون همچنین بر کلیه موارد اشغال جزئی یا کلیِ قلمرو یکی از طرفین معظم متعاهد، حتی اگر اشغال مزبور با هیچ مقاومتی روبرو نشود، اِعمال خواهد گردید»؛ مخاصمه مسلحانه ذیل این قاعده که به موارد اساسی بسنده کرده است، توأمان مستلزم مؤلفه‌های «بین‌المللی» و «مسلحانه» است.

همچنین، زمانیکه بازیگران غیردولتی تحت کنترل کلی یک دولت در خصومت علیه دولت دیگر نقش داشته باشند، مخاصمه بین‌المللی می‌شود؛ به عنوان مثال، در زمان اجرا، اگر دولت (الف) بر یک گروه سازمان‌یافته از هکرهای رایانه‌ای که به زیرساخت سایبری دولت (ب) نفوذ

کرده و منجر به خسارت فیزیکی قابل توجه شده، کنترل کلی داشته باشد، ماهیتاً مخاصمه مسلحانه بین‌المللی محسوب می‌شود (دستورالعمل تالین ۱، ۲۰۱۳: ۷۱-۷۳).

ماده ۳ مشترک کنوانسیون‌های چهارگانه ژنو و پروتکل الحاقی دوم، علیرغم اشاره به مخاصمات مسلحانه غیربین‌المللی، تعریفی دقیق از آن ارائه نداده‌اند؛ کما اینکه ماده ۳ مشترک، هر مخاصمه مسلحانه‌ای را که بین‌المللی نباشد، غیر بین‌المللی معرفی کرده است و ماده ۱ پروتکل الحاقی به کنوانسیون‌های ژنو نیز، شرایطی را درجهت شناسایی یک وضعیت به عنوان مخاصمه مسلحانه غیربین‌المللی در نظر گرفته است؛ از جمله وقوع مخاصمه در قلمرو یک کشور متعاهد؛ وقوع مخاصمه میان نیروهای مسلح یک کشور و نیروهای مسلح مخالف؛ دارا بودن یک فرمانده مسئول؛ همچنین، کنترل بخشی از قلمرو کشور و انجام عملیات خصمانه به صورت مداوم و منسجم. پروتکل دوم، تضمین‌های اساسی را در مورد افرادی که در مخاصمه مسلحانه شرکت ندارند، قائل شده است؛ من جمله تنبیه دسته جمعی، تروریسم، گروگانگیری و غارت را منع کرده و حداقل حمایت را از افراد بازداشت و اسیر شده پیش‌بینی کرده و مقرراتی در خصوص حمایت از جمعیت غیرنظامی در مقابل خطرات ناشی از عملیات نظامی دارد. به علاوه، حمله به ابنیه و تأسیسات حاوی نیروهای خطرناک مثل ایستگاههای برق اتمی، سدها و آب بند ها را منع کرده است (بلدسو و بوچک، ۱۳۷۵: ۵۱۸). دیوان بین‌المللی کیفری نیز در تعریف مخاصمه مسلحانه غیربین‌المللی، سه معیار را ملاک قرار داده است که عبارتند از وقوع درگیری در قلمرو یک کشور، وقوع درگیری میان نیروهای دولتی و گروه‌های مسلح مخالف با آنها و یا با گروه‌های مسلح مخالف و در نهایت، درگیری طولانی‌مدت (ضیایی بیگدلی، ۱۳۹۲: ۵۲- ۵۳).

قاعده ۲۳ دستورالعمل تالین۱، نیز در ارتباط با مخاصمات مسلحانه غیربین‌المللی مقرر داشته است: «مخاصمه مسلحانه غیربین‌المللی زمانی به وجود می‌آید که خشونت مسلحانه طولانی‌مدت، شامل عملیات سایبری یا محدود به آن بین نیروهای مسلحانه دولتی و نیروهای یک یا چندین گروه مسلحانه یا بین چنین گروه‌هایی رخ دهد. چنین مخاصمه‌ای باید به یک سطح حداقلی از شدت رسیده باشد و طرفین مخاصمه، سازماندهی حداقلی داشته باشند». همچنین، قاعده ۸۳ دستورالعمل تالین ۲ مقرر می‌دارد: یک مخاصمه مسلحانه غیربین‌المللی، در صورت وقوع خشونت مسلحانه طولانی میان نیروهای مسلح دولتی و گروه‌های مسلح سازمان‌یافته یا میان چنین گروه‌هایی که ممکن است شامل یا محدود به عملیات‌های سایبری باشد، وجود دارد. منازعه باید به آستانه‌ای حداقلی از شدت برسد و طرفین دیگر در مخاصمه می‌بایست واجد میزانی حداقلی از سازمان‌یافتگی باشند. این قاعده واگویه کلیِ حقوق بین‌الملل عرفیِ مخاصمات مسلحانه در رابطه با آستانه وجود یک مخاصمه مسلحانه غیربین‌المللی است. جمله نخست بر ماده ۳ مشترک کنوانسیون‌های ۱۹۴۹ ژنو استوار است که حقوق بین‌الملل عرفی را منعکس می‌سازد. ماده مزبور بر

«مخاصمات مسلحانه فاقد ماهیت بین‌المللی که در قلمرو یکی از طرفین معظم متعاهد رخ می‌دهد، یعنی وضعیت‌هایی که در آنها عملیات‌های متخاصمانه میان نیروهای مسلح دولتی و گروه‌های مسلح سازمان‌یافته غیردولتی یا میان چنین گروه‌هایی به وقوع می‌پیوندند، اِعمال می‌گردد. جمله دوم بر تحول رویه قضایی در باب مقولات مرتبط با شدت و سازمان‌یافتگی مبتنی است.

۲. اصول حقوق بشردوستانه و حملات سایبری

با شناسایی عملیات سایبری به عنوان یک مخاصمه (حمله) مسلحانه، اعم از بین‌المللی و غیربین‌المللی، و با عنایت به قاعده ۲۰ دستورالعمل تالین۱ که پیشتر مورد اشاره قرارگرفت، اصول اساسی حقوق بشردوستانه بین‌المللی، نظیر اصل تفکیک، اصل تناسب، اصل ضرورت و ممنوعیت تحمیل درد و رنج غیرضروری، درست همان طور که برای دیگر ابزارها و روش‌های جنگ و مخصمات مسلحانه به کار می‌رود، در مورد عملیات سایبری نیز اعمال خواهد شد.

۱-۲. اصل تفکیک[1]

اصل تفکیک (تمایز)، به عنوان یکی از اصول اساسی حقوق مخاصمات مسلحانه، اولین بار در اعلامیه ۱۸۶۸ سن پترزبورگ به این صورت مورد اشاره واقع شد: «تنها هدف مشروعی که دولت‌ها باید در حین جنگ تلاش در انجام آن داشته باشند، تضعیف نیروهای نظامی دشمن است»؛ این اصل، همچنین، توسط دیوان بین‌المللی دادگستری در رأی مشورتی در مورد مشروعیت تهدید یا توسل به سلاح‌های هسته‌ای به عنوان یکی از حقوق بین‌الملل عرفی، به رسمیت شناخته شده است و غیرقابل‌تخطی می‌باشد (نظریه مشورتی سلاح‌های هسته‌ای، ۱۹۹۶: ۱۷۹)[2].

اصل تفکیک، طرفین مخاصمه را مکلف می‌کند که همواره میان اهداف نظامی، از یک سو و اهداف غیرنظامی از سوی دیگر تفکیک قائل شوند و صرفاً اهداف نظامی را هدف قرار دهند. علیرغم اینکه این اصل ریشه در قواعد حقوق بین‌الملل عرفی دارد، در ماده ۴۸ پروتکل الحاقی اول به کنوانسیون‌های ژنو[3] هم (در مورد مخاصمات مسلحانه بین‌المللی و غیربین‌المللی) مورد تأکید قرار گرفته است (کولب و هاید، ۱۳۹۳: ۸۵). بند ۲ ماده ۸ اساسنامه دیوان کیفری بین‌المللی نیز ضمن اشاره به این مطلب که هدایت حملات علیه اشیای غیرنظامی، مبین جرایم جنگی در

---

[1] Distinction

[2] مطابق رأی دیوان: «دولت‌ها نباید غیرنظامیان را هدف حمله قرار دهند و متعاقباً هرگز نباید از سلاح‌هایی استفاده کنند که قابلیت تفکیک بین اهداف نظامی و غیرنظامی را ندارد.»

[3] ماده ۴۸ پروتکل الحاقی اول: در راستای تضمین احترام و حمایت از جمعیت غیرنظامی و اهداف غیرنظامی، طرفین مخاصمه، همواره باید میان جمعیت غیرنظامی و رزمندگان و همچنین، میان اهداف غیرنظامی و اهداف نظامی، تفکیک قائل شوند و بر این اساس، عملیات خودشان را فقط علیه اهداف نظامی هدایت نمایند.

مخاصمات مسلحانه است، این اصل را مورد شناسایی قرار داده است. همچنین، دادگاه بین‌المللی کیفری برای یوگسلاوی سابق در قضیه تادیچ (پاراگراف ۱۲۲-۱۲۷)[1] نیز اصل تفکیک را در مخاصمات مسلحانه غیربین‌المللی، قابل‌اعمال دانسته است و به این ترتیب، طرفین مخاصمه را متعهد می‌سازد تا بین غیرنظامیان از یک طرف و اعضای نیروهای مسلح دولتی و اعضای گروه‌های مسلح سازمان‌یافته از جمله نیروهای سازمان‌یافته منظم یا مخالف، از طرف دیگر تمایز قائل شوند.

مطابق بند ۴ و ۵ ماده ۵۱ پروتکل الحاقی اول به کنوانسیونهای چهارگانه ژنو، حملات کورکورانه نیز ممنوع اعلام شده‌اند (مطالعه حقوق بشردوستانه عرفی[2]، قواعد ۱۱-۱۲). حملات کورکورانه، حملاتی هستند که نمی‌توانند به سمت یک هدف نظامی خاص روانه شوند یا اینکه نتایج آنها نمی‌توانند محدود شوند و در نتیجه این حملات، اهداف نظامی و غیرنظامیان و اهداف غیرنظامی را بدون تفکیک شامل می‌شوند. بند ۲ ماده ۵۲ پروتکل مزبور نیز منعکس‌کننده اصل تمایز میان نظامیان و غیرنظامیان می‌باشد، چراکه حملات را به شدت محدود به اهداف نظامی دانسته و اهداف نظامی را بیشتر به عنوان اشیایی معرفی می‌کند که ماهیت، موقعیت، هدف یا استفاده و مزیت نظامی ازجمله، تخریب کامل یا جزئی آنها، ضبط یا خنثی‌سازی داشته باشند؛ قاعده ۳۱ دستورالعمل تالین ۱ نیز، به تفصیل، نسبت به اصل تفکیک در خصوص حملات سایبری به این صورت اشاره کرده است. همچنین، قاعده ۹۳ دستورالعمل تالین ۲ مقرر داشته است: «اصل تفکیک بر حملات سایبری اِعمال می‌شود». قاعده ۳۲ دستورالعمل تالین ۱ نیز مقرر داشته است «جمعیت غیرنظامی همانند افراد غیرنظامی نباید هدف حمله سایبری قرار گیرند».

قاعده ۳۳ دستورالعمل تالین ۱، در تکمیل قواعد ۳۱ و ۳۲ آن، به بیان یک فرض پرداخته است و بیان می‌دارد که «در صورت وجود تردید نسبت به اینکه شخصی نظامی است یا غیرنظامی، فرض بر غیرنظامی بودن آن شخص است». در نهایت، قاعده ۳۴ نیز اشخاصی را که می‌توانند به عنوان هدف مشروع حمله سایبری قرار گیرند، به این صورت مشخص می‌کند:

الف) اعضای نیروهای مسلح؛

ب) اعضای گروه‌های سازمان‌یافته؛

ج) افراد غیرنظامی‌ای که مستقیماً در درگیری‌ها مشارکت دارند؛ و

د) مشارکت‌کنندگان در مخاصمه مسلحانه بین‌المللی به عنوان بسیج عمومی؛

به این ترتیب، افراد خارج از این طبقه‌بندی، در شمار غیرنظامیان، محسوب و از حملات، مصون خواهند بود.

[1] ICC Tadić Decision on The Defence Motion for Interlocutory Appeal
[2] ICRC Customary IHL Study

پس از مشخص شدن غیرنظامیان، اهداف غیرنظامی نیز مورد توجه اصل تفکیک قرار گرفته و بنابراین، از دیدگاه انتخاب اهداف، هر فرمانده نظامی جهت رهانیدن خود از اتهام جنایت جنگی، می‌تواند از انتخاب اهداف صرفاً غیرنظامی، از جمله، بورس اوراق بهادار، سیستم بانکداری، دانشگاه‌ها و زیرساخت‌های غیرنظامی خودداری نماید (آفرودیتی[1]، ۲۰۱۰: ۲۵).

از سوی دیگر، ماده ۵۵ پروتکل الحاقی به کنوانسیون‌های چهارگانه ژنو، استفاده از روش‌ها و ابزارهای جنگی که منجر به تهدید سلامت یا حیات جمعیت می‌شود را ممنوع اعلام می‌کند. همچنین، دیوان بین‌المللی دادگستری در نظریه مشورتی درباره استفاده از سلاح‌های هسته‌ای در سال ۱۹۹۶ اعلام کرد دولت‌ها هرگز نباید غیرنظامیان را هدف حمله خود قرار دهند و درنتیجه، هرگز نباید از سلاح‌هایی استفاده کنند که قادر به تشخیص بین اهداف غیرنظامی و نظامی نباشند؛ این موضوع همچنین در قاعده ۴۲ دستورالعمل تالین ۱، به این صورت بیان شده است: «به کار بردن ابزارها و روش‌های جنگ سایبری که ماهیتاً تفکیک‌ناپذیر هستند، ممنوع است. شیوه‌ها یا روش‌های جنگ سایبری زمانی ماهیتاً تفکیک‌ناپذیر است که:

الف) نتواند علیه یک هدف نظامی معین هدایت شود و

ب) اثرات آنها طبق الزامات حقوق مخاصمات مسلحانه، محدود نبوده

و در نتیجه، ماهیتی دارد که اهداف نظامی، غیرنظامیان یا اشیاء غیرنظامی را بدون تمایز مورد هدف قرار می‌دهد»؛ به این ترتیب، ابزار و روشهایی که با تغییر شرایط زندگی منجر به آزار غیرنظامیان شود، ممنوع است.

نتایج حملات سایبری می‌توانند آزاری برای غیرنظامیان تلقی شوند؛ پس اگر حمله سایبری سبب بی‌نظمی و آشوب در کشوری شود، اگرچه آن حمله به صورت فیزیکی به آنها لطمه وارد نکند، اما بر همه جنبه‌های زندگی غیرنظامیان تأثیر گذاشته است؛ البته، این موضوع که یک حمله سایبری می‌تواند به طور مستقیم یا غیرمستقیم، منجر به مرگ یا خسارات فیزیکی افراد شود را نمی‌توان نادیده گرفت (کلسی[2]، ۲۰۰۹: ۱۴۳۶). بنابراین، استفاده از سلاح سایبری، در جنگ، ممنوع نیست و صرفاً شیوه کاربرد سلاح‌های سایبری است که می‌تواند به نقض اصل تفکیک منتهی شود (ممتاز و شایگان، ۱۳۹۳: ۱۰۳).

از دیدگاه مفهومی، برخی پژوهشگران حقوقی و کارشناسان قانونی و نظامی، از جمله، چارلز داونلاپ (دانلاپ[3]، ۲۰۰۰: ۱۴)، معاون پیشین دادستان کل نیروی هوایی ایالات متحده، در حمایت از دیدگاه مبتنی بر اثر، چنین استدلال می‌کنند که دیگر نمی‌توان نسبت به این اصل احترام قائل شد؛ چرا که از آنجا که نظریه جنگ مبتنی بر اثراتی چون فشار سیاسی، اقتصادی و حملات شدید

[1] Afroditi
[2] kelsey
[3] Dunlap

در مقابل یک نتیجه سریع است، نیازمند یک پارادیم جدید در توسل به زور علیه جوامع خواهیم بود که طرف مخاصمه را تهدید کنیم که جهانشان را از بین خواهیم برد.

با توجه به اینکه امکان مداخله سیگنال‌های مورد استفاده در حملات سایبری در شبکه‌های غیرنظامی را نمی توان نادیده گرفت، امکان اعمال اصل تفکیک در فضای سایبر بسیار مشکل است؛ زیرا فضای سایبر، فضایی مبتنی بر گمنامی بوده و انتساب عمل و تشخیص اهداف قانونی از اهداف غیر قانونی نیز مشکل است.

تجزیه و تحلیل انطباق حمله سایبری با اصل تمایز بسیار شبیه به تجزیه و تحلیل برای یک حمله متعارف خواهد بود، و در بسیاری از عملیات حملات سایبری به وضوح با اصل تمایز مطابقت دارد. همانطور که ارتش در حال برنامه‌ریزی برای استفاده از سلاح‌های سایبری است، جوامع نظامی و حقوقی نیز به تفسیر مجدد اصل تمایز، برای تأثیر بیشتر بر استفاده از سلاح‌های سایبری نیاز دارند. بعضی از اپراتورهای نظامی معتقدند که امتیازات یک هدف نظامی مشروع برای یک حمله سایبری نیز مشروع می‌باشد. به همین ترتیب، ممنوعیت‌های مرتبط با حقوق بشردوستانه بین‌المللی نیز به نوع سلاح یا جنگ مورد استفاده بستگی ندارد و باید بدون شک درباره سلاح‌های سایبری اعمال شود. این اصل به احتمال زیاد به یک کشور اجازه می‌دهد که از یک سلاح سایبری برای حمله به یک هدف کاملاً نظامی استفاده کند. پرواضح است که با چنین استفاده‌ای، اصل تمایز نقض نمی‌شود؛ به عنوان مثال، حمله به یک ایستگاه دفاع هوایی که بخشی از یک مرکز را خنثی می کند، یک امتیاز نظامی مشخص را به نفع جنگجویان ارائه می‌دهد. در هر حال، این فرماندهان نظامی هستند که می‌توانند با در نظرگرفتن نوع حمله، پیامدهای آن را پیش‌بینی کنند. از سوی دیگر، حقوق بشردوستانه بین‌المللی احتمالا حمله سایبری که «علت مستقیم و عمدی مرگ و نابودی غیرنظامیان» باشد را ممنوع می کند. نمونه‌هایی از این نوع حمله‌ها ممکن است شامل «اختلال در یک سیستم کنترل ترافیک هوایی باشد که می‌تواند به سقوط یک هواپیمای غیرنظامی منجر شود؛ یا اختلال و توقف در یک پایگاه داده پزشکی باعث شد به غیرنظامیان یا سربازان زخمی خون متفاوت از گروه خونی آنها منتقل شود (کلسی، ۲۰۰۹: ۱۴۳۷-۱۴۳۸).

برخی عملیات‌های صورت گرفته علیه جمعیت غیرنظامی مشروع است؛ برای مثال، عملیات روانی نظیر پخش اعلامیه یا ساخت تبلیغات تلویزیونی، حتی اگر غیرنظامیان مخاطبان موردنظر آنها باشند، ممنوع نیست. در بستر جنگ سایبری، ارسال پیام از طریق ایمیل به افراد دشمن به منظور اصرار به تسلیم شدن نیز مطابق حقوق مخاصمات مسلحانه خواهد بود.[1] صرفاً زمانی که عملیات سایبری علیه غیرنظامیان یا اشیاء غیرنظامی (یا سایر اشخاص و اشیاء حمایت شده) به سطحی از

[1]. در خلال تجاوز ۲۰۰۳ عراق، «هزاران افسر ارتش عراق تنها قبل از شروع جنگ ایمیلی از سامانه ایمیل وزارت دفاع عراق دریافت کردند.» به آنها گفته شده بود که تانک‌ها و خودروهای زرهی را معرفی، ترک نموده و به منزل بروند.

حمله برسد، براساس اصل تفکیک و قواعدی از حقوق مخاصمه مسلحانه که از این اصل ناشی می‌شود، ممنوع است (دستورالعمل تالین ۱، ۲۰۱۳: ۹۷).

رعایت اصل تمایز، در جنگ‌های سایبری، یک مسأله بسیار پیچیده است، زیرا این گونه سلاح‌ها می‌توانند به واسطه اهداف دقیق، وضعیت را ساده‌تر کنند، اما از سوی دیگر، می‌توانند نتایج حملات را گسترش داده یا حتی از کنترل خارج کنند. بنابراین، رعایت اصل تمایز در حملات و جنگ‌های سایبری ضروری به نظر می‌رسد، زیرا یکی از انواع حمایت از غیرنظامیان است.

۲-۲. اصل تناسب[1]

این اصل، که در بند ۵ ماده ۵۱ پروتکل اول الحاقی[2] به کنوانسیون‌های ژنو، اشاره شده است، بیان می‌دارد که کلیه اقدامات نظامی که توسط متخاصمین انجام می‌شود، باید متناسب با هدفی باشد که آنها به دنبال رسیدن به آن هستند. تناسب در حقوق مخاصمات مسلحانه بدین معناست که منفعت نظامی حاصل از یک عملیات خاص باید بیشتر از خسارتی باشد که در اثر آن عملیات به غیرنظامیان و اهداف غیرنظامی وارد می گردد. در زمان طراحی هر عملیات نظامی هر کدام از متخاصمین مکلفند منفعت نظامی حاصل از آن، تجهیزات جایگزینی که همان منفعت را می‌توانند تأمین کنند و زیان‌هایی که انتظار می‌رود به غیر نظامیان وارد آید را ارزیابی نمایند. اهمیت منافع نظامی احتمالی و میزان خسارت غیرنظامی احتمالی باید نسبت به یکدیگر متوازن باشند؛ برای مثال، اگر این احتمال وجود داشته باشد که در اثر حمله، احتمال کشته شدن تعداد زیادی از غیرنظامیان وجود دارد، حال آنکه منفعت نظامی احتمالی هرگز منطبق با این میزان تلفات نیست، انجام آن حمله ممنوع است (کولب و هاید، ۱۳۹۴: ۸۷).

قاعده ۵۱ دستورالعمل تالین ۱، بر اساس بند ۵ ماده ۵۱ و بند ۲ ماه ۵۷ پروتکل اول الحاقی، این چنین به اصل تناسب اشاره کرده است: «حمله مسلحانه‌ای که پیش‌بینی می‌شود منجر به مرگ غیرعمدی غیرنظامیان، مجروح‌شدن غیرنظامیان، خسارت به اشیاء غیرنظامی یا همه آنها شود که زیاده از مزیت نظامی عینی و مستقیم مورد انتظار باشد، ممنوع است». این قاعده، وارد شدن آسیب به غیرنظامیان و اشیای غیرنظامی را لزوماً سببی برای غیرقانونی شناخته شدن یک حمله سایبری نمی‌داند، بلکه غیرقانونی بودن این حملات، به ارتباط میان صدمه‌ای که انتظار دارد به صورت معقول، ناخواسته به آسیب‌های جانبی وارد شود و اهداف نظامی موردنظر آنها بستگی دارد؛

---

[1] Proportionality

[2] یک حمله، بدون تفکیک و ممنوع محسوب می‌شود اگر احتمال ورود خسارت ضمنی به حیات غیر نظامیان، مجروح کردن آنها، خسارت به اهداف غیرنظامی و یا مجموعه‌ای از اینها، بسیار بیشتر از منافع نظامی مستقیم و واقعی پیش‌بینی از انجام آن حمله باشد.

همچنین، قاعده ۱۱۳ دستورالعمل تالین ۲، با بیانی مشابه، با در نظر گرفتن اصل تناسب در حقوق بشردوستانه، این اصل را اینچنین به عملیات‌های سایبری تعمیم می‌دهد: «حمله‌ای سایبری که انتظار می‌رود موجب مرگ غیرنظامیان، ایراد جراحت به افراد غیرنظامی، ورود خسارت به اشیاء غیرنظامی یا آمیزه‌ای از آن‌ها شود، که نسبت به مزیت نظامی واقعی و مستقیمِ مورد انتظار مفرط خوهد بود، ممنوع است».

این قاعده، به وضعیت‌هایی می‌پردازد که در آن‌ها غیرنظامیان یا اشیاء غیرنظامی به صورت تصادفی آسیب می‌بینند، یعنی اهداف از پیش تعیین شده حمله نیستند. به مرگ یا جراحت غیرنظامیان یا خسارت یا تخریب اشیاء غیرنظامی به صورت تصادفی غالباً «خسارت جانبی» اطلاق می‌شود. همانطور که این قاعده روشن می‌سازد، اینکه غیرنظامیان یا اشیاء غیرنظامی در خلال حمله‌ای سایبری علیه یک هدف نظامیِ مشروع متحمل آسیب می‌شوند، ضرورتاً حمله مزبور را به‌خودی‌خود غیرقانونی نمی‌سازد. در عوض، قانونی بودن حمله‌ای که در آن خسارت جانبی به بار می‌آید، به رابطه میان آسیبی که مهاجم منطقاً انتظار دارد به صورت تصادفی به غیرنظامیان یا اشیاء نظامی وارد شود و مزیت نظامی که مهاجم پیش‌بینی می‌کند در نتیجه حمله به دست آورد، بستگی دارد.

این قاعده، آسیب‌های جانبی را به آسیب‌های مستقیم یا غیر مستقیم تقسیم‌بندی می‌کند و اعلام می‌کند که تناسب همه این اثرات، با حملات، باید درنظر گرفته شود؛ تأثیرات مستقیم عبارتند از تبعات فوری و اولیه حمله سایبری که با رویدادها یا مکانیسم‌های میانی تغییر نمی‌یابد؛ در مقابل، تأثیرات غیرمستقیم حمله سایبری شامل تبعات به تأخیر افتاده یا جابجا شده دومین و سومین یا بالاتر اقدام است که از طریق رویدادها یا مکانیسم‌های واسط ایجاد می‌شود. خسارت جانبی که در ارزیابی تناسب لحاظ می‌شود، شامل هرگونه تأثیر غیرمستقیمی است که مورد انتظار اشخاص برنامه‌ریز، تأییدکننده و مجری حمله سایبری است؛ برای مثال، در صورتی که اطلاعات ماهواره‌ای مکان‌یاب جهانی مسدود یا مختل شود، حوادثی نظیر تصادفات در سیستم‌های حمل ونقل که متکی به این اطلاعات است، در مدت کوتاهی یا حداقل تا زمان اتخاذ سایر روش‌ها یا تکنیک‌های جهت‌یابی انتظار می‌رود. به همین نحو، یک مهاجم ممکن است تصمیم بگیرد بدافزاری را وارد سیستم رایانه نظامی کند که نه تنها آن سیستم را مختل می‌کند، بلکه وارد تعداد محدودی از رایانه‌های غیرنظامی می‌شود و آنها را نیز ویروسی می‌کند و منجر به خسارتی می‌شود که به عنوان خسارت جانبی در این قاعده تلقی می‌شود. در صورت وجود یا پیش‌بینی چنین تاثیراتی باید آنها را در تحلیل تناسب در نظر گرفت. در مقابل، اگر بدافزار به صورت غیرمنتظره یا غیرقابل‌پیش‌بینی از طریق حافظه قابل‌حمل ذخیره اطلاعات، به سیستم‌های غیرنظامی وارد شود، عواقب بعدی آن در زمان ارزیابی این قاعده در نظرگرفته نخواهد شد (دستورالعمل تالین۱، ۲۰۱۳: ۱۳۳).

۲-۳. اصل ضرورت نظامی[1]

مطابق این اصل، طرفین مخاصمه، مکلفند صرفاً تدابیری اتخاذ نمایند که برای غلبه بر دشمن و پیروزی بر او لازم و ضروری باشد. هدف جنگ نباید در تخریب هرچه گسترده‌تر اموال دشمن طرف مخاصمه و کشتن هرچه بیشتر نیروهای نظامی دشمن تا آنجا که ممکن است، قرار داده شود. از اینرو، هدف منطقی در جنگ، بایستی حداقل تخریب و کشتار تا آنجا که امکان‌پذیر است باشد و صرفاً آن میزان از خساراتی به دشمن وارد گردد که برای غلبه بر دشمن و پیروزی بر او لازم باشد(کولب و هاید، ۱۳۹۳: ۳۸۵).

اصل ضرورت نظامی، توسل به زور در انجام عملیات را مجاز دانسته و در عین حال، ارتکاب اعمالی را که حقوق مخاصمات مسلحانه ممنوع دانسته است را غیر مجاز قلمداد کرده است (گراهام[2]، ۲۰۱۰: ۹۸).

این اصل، در اعلامیه سن پترزبورگ ۱۸۶۸ مورد اشاره قرار گرفته[3]، همچنین، ماده ۲۳ کنوانسیون چهارم لاهه، ممنوعیت تخریب یا انهدام اموال را اعلام کرده است، مگر اینکه چنین تخریبی ضرورتا برای جنگ، لازم و ضروری باشد؛ در عین حال ماده ۵۲ پروتکل الحاقی اول، که اهداف قانونی را "آن دسته از اشیائی که حسب طبیعت، محل، هدف یا استفاده از آن در اقدام نظامی، موثر هستند و تخریب کامل یا جزئی آن، گرفتن، یا خنثی‌سازی، درشرایط حاکم در آن زمان، یک امتیاز نظامی مشخص ارائه می‌دهد" را به عنوان مزیت نظامی برشمرده است، از سوی دیگر، ضمن بند ۳ ماده ۵۷ پروتکل الحاقی اول به کنوانسیون‌های ژنو، به این صورت بیان شده است "هنگامی که امکان انتخاب بین چند هدف نظامی برای دستیابی به مزیت نظامی یکسانی وجود داشته باشد، هدفی انتخاب خواهد شد که انتظار می‌رود حمله به آن موجب کمترین خطر برای جان واهداف غیرنظامی خواهد شد"(کیتی شیایزری[4]، ۲۰۱۷: ۱۹۲). اساسنامه رم، نقض این اصل را ضمن بند ۲ ماده ۸، به عنوان جرم جنگی شناسایی نموده است (Rome Statute of the International Criminal Court, 1998, art: 8(2)(a)(iv)).

اصل ضرورت، در حقیقت، بیان کننده این است که در عملیات نظامی، می‌بایست با توسل به کمترین اقدام تخریبی، به امتیازی نظامی دست یافت؛ این اصل، مانع از هرگونه عملیاتی می‌شود

---

[1] Military necessity

[2] Graham

[3] تنها هدف مشروعی که کشورها باید در اثنای جنگ برای تحقق آن تلاش کنند این است که نیروهای نظامی دشمن را تضعیف کرده و به همین منظور کافی است که تا حداکثر امکان تعداد نفرات را ناتوان سازند؛ چنانچه در جنگ، سلاحهایی به کار گرفته شوند که درد و رنج افراد ناتوان شده را به طور بی ثمری افزایش داده یا مرگ آنها را حتمی سازند، آنگاه این هدف، نادیده گرفته شده است

[4] Kittichaisaree

که هیچ مزیت نظامی را به همراه ندارد، همچنین، هیچ نقشی در پیشرفت و تقویت هدف جنگ ندارد و بنابراین، ممنوع خواهد بود (نواده توپچی، ۱۳۹۳: ۷۹).

این اصل، ضمن قاعده ۵۶ دستورالعمل تالین ۱ و تحت عنوان اقدامات احتیاطی، بیان شده است که به بند ۳ ماده ۵۷ پروتکل الحاقی اول اشاره دارد و به این ترتیب، لزوم رعایت آن در حملات سایبری را می‌توان درک کرد: «برای دولت‌های عضو پروتکل الحاقی اول، زمانی که برای کسب مزیت نظامی مشابه، امکان انتخاب بین چندین هدف نظامی وجود دارد، باید اهدافی برای حمله سایبری انتخاب شود که انتظار می‌رود حمله به آنها باعث صدمه کمتری به جان غیرنظامیان و اشیاء غیرنظامی شود». این قاعده برای آن دسته از عملیات سایبری که حمله تلقی می‌شوند، کاربرد دارد. باید به خاطر داشت که این قاعده صرفاً برای اهدافی به کار می‌رود که حمله به آنها منجر به مزایای نظامی مشابه می‌شود. این مزایا نباید از نظر کمی و کیفی یکسان باشند. مزیت نظامی نیز باید با توجه به کل عملیات مشخص شود، نه بر اساس مزیتی که تنها از یک حمله حاصل می‌شود. از این رو، حتی اگر حمله جایگزین، احتمالاً خسارات جانبی کمتری داشته باشد، چنانچه منجر به حصول اهداف نظامی که حمله اصلی برای آنها طراحی شده نشود، هیچ مسئولیتی برای به عهده گرفتن آن وجود نخواهد داشت؛ به عنوان مثال، وضعیتی را در نظر بگیرید که یک مهاجم به دنبال ایجاد اختلال در سیستم فرماندهی و کنترل دشمن است؛ یک گزینه آن است که حملات سایبری علیه عناصر شبکه الکترونیکی دوکاره که سیستم ارتباطی دشمن به آن وابسته است، صورت گیرد. با این وجود، احتمال دارد چنین حملاتی منجر به خسارات مهم جانبی و اگرچه متناسب، شود؛ گزینه نظامی ممکن دوم، انجام حملات سایبری مستقیم علیه شبکه کنترل و فرماندهی دشمن است. چنانچه انتظار رود گزینه دوم تأثیرات مطلوبی بر سیستم کنترل و فرماندهی دشمن (همان مزیت نظامی) با خسارات جانبی کمتر حاصل خواهد نمود، این گزینه باید انتخاب شود (دستورالعمل تالین ۱، ۲۰۱۳: ۱۴۲).

مزیتی که حمله سایبری به سیستم کامپیوتری نظامی دشمن، شرایط ضرورت نظامی را ایجاد می‌کند، ارتباط نظامی منحصر به فرد آنها است. فرصت‌های زیادی برای حمله به سیستم‌های کامپیوتری ارتش مدرن، که از سیستم‌های کامپیوتری استفاده می‌کند، وجود دارد. با این حال، هنگام تعیین اینکه آیا یک هدف «مزیت قطعی نظامی» ایجاد می‌کند یا خیر، مبهم است. ارزش یک سلاح سایبری اغلب در اثر فراگیر و پی‌درپی آن بر روی سیستم‌هایی است که مؤثر در هدف اولیه هستند. اکثر مهاجمان اینترنتی اطلاعات کافی برای پیش‌بینی اثرات غیرمستقیم را ندارند. یک حمله‌کننده سایبری، که به صورت غیرمستقیم، یک سیستم کامپیوتری نظامی را هدف قرار می‌دهد، ممکن است ناموفق باشد. مهاجم سایبری که به کامپیوترهای سیستم الکتریکی نفوذ می‌کند، ممکن است یک مزیت نظامی به دست آورد؛ اما سیستم ممکن است لایه‌های پیش‌بینی

نشده‌ای داشته باشد که از وقوع چنین مزیتی جلوگیری کند. در این شرایط، مزیت نظامی وجود ندارد. ارزیابی اینکه آیا یک حمله سایبری، یک ضرورت نظامی خواهد بود، مانند ارزیابی ضرورت نظامی در حملات سنتی، تصمیم‌گیری موردی است؛ در هرکدام به عنوان مثال، یک مهاجم اینترنتی باید به طور قطعی تعیین کند که حمله سایبری یک مزیت نظامی برای رسیدن به یک هدف نظامی را ارائه می‌دهد یا خیر؟ (گراویس[1]، ۲۰۱۲: ۵۶۴).

۲-۴. اقدامات احتیاطی

بند ۳ ماده ۴۹ پروتکل الحاقی اول، مقررات مربوط به اقدامات احتیاطی را چنین بیان داشته است: «در نبرد دریایی، هوایی یا زمینی که بر جمعیت غیرنظامی، اشخاص غیرنظامی یا اشیاء غیرنظامی تاثیر می‌گذارد، اعمال می‌شود. این مقررات همچنین در مورد تمامی حملات از دریا یا هوا علیه اهداف روی زمین به کار می‌رود، ولی تأثیری بر حقوق بین‌المللی قابل اعمال در مخاصمه مسلحانه دریایی یا هوایی، ندارد». همچنین، بند ۲ ماده ۵۷ پروتکل الحاقی اول، در مقام معرفی این اصل، مقرر کرده است: «کسانی که حملات را برنامه‌ریزی یا در مورد اجرای حملات تصمیم‌گیری می‌کنند، باید کلیه احتیاط‌های ممکن را در انتخاب وسایل و شیوه‌های حمله به عمل آورند تا هنگام حمله از خسارت جانی اتفاقی به غیرنظامیان و نیز آسیب رساندن به اموال غیرنظامی اجتناب ورزند یا آن را به حداقل برسانند». احتیاط‌های ممکن می‌تواند به تعبیر بند ۱۰ ماده ۳ پروتکل دوم کنوانسیون ممنوعیت یا محدودیت در استفاده از برخی سلاح‌های متعارف[2]، همه شرایطی باشد که در زمان حمله، حاکم بوده است؛ از جمله ملاحظات نظامی و انسانی.

قاعده ۵۲ دستورالعمل تالین ۱ نیز، اعلام می‌دارد: «در درگیری‌هایی که مشتمل بر عملیات سایبری است، باید مراقبت‌های مستمری برای حفظ جمعیت غیرنظامی، اشخاص غیرنظامی و اشیاء غیرنظامی اتخاذ شود». این قاعده که مبتنی بر بند ۱ ماده ۵۷ پروتکل الحاقی اول است، در هر دو مخاصمه مسلحانه بین‌المللی و غیربین‌المللی مرسوم است[3].

از آنجا که مخاصمات مسلحانه تعریفی از اصطلاح «مراقبت مستمر» ارائه نمی‌کند، در عملیات سایبری وظیفه مراقبت، فرماندهان و کلیه افراد دخیل در عملیات را موظف می‌کند تا نسبت به تأثیرات فعالیت خود بر غیرنظامیان و اشیاء غیرنظامی، همیشه حساس بوده و از هرگونه اثرات غیرضروری اجتناب کنند[4]؛ واژه «مستمر» به این مسئله دلالت دارد که مراقبت برای حمایت غیرنظامیان و اشیاء غیرنظامی از یک ماهیت مستمر در سراسر عملیات سایبری برخوردار است و کلیه افرادی که در این عملیات‌ها مشارکت می‌کنند، باید به این وظیفه عمل کنند. این قاعده در

---

[1] Gervais
[2] Amended Mines Protocol
[3] See also AMW MANUAL, Rules 30
[4] See U.K. MANUAL, para. 5.32.1

هیچ وضعیت زمانی یا مکانی این مسأله را نمی‌پذیرد که ممکن است افرادی که در برنامه‌ریزی و اجرای فرآیند شرکت دارند، اثرات عملیات خود را نسبت به غیرنظامیان یا اشیاء غیرنظامی نادیده بگیرند[1]. چنین امری در بستر سایبری مستلزم آگاهی از وضعیت در کلیه زمان‌ها است، نه صرفاً در طول مرحله مقدماتی عملیات.

قاعده ۵۳ دستورالعمل تالین ۱، با ابتنای بر قسمت (I) از شق الف بند ۲ ماده ۵۷ پروتکل الحاقی اول، افرادی را که حمله سایبری را طراحی یا در مورد آن تصمیم‌گیری می‌کنند، ملزم می‌کند که هر اقدام ممکن برای تعیین این که اهداف مورد حمله، افراد غیرنظامیان یا اشیاء غیرنظامی نیستند و تحت هیچ حمایت خاصی نمی‌باشند را انجام دهند[2].

ویژگی مهم این قاعده، تمرکز آن بر برنامه‌ریزان و تصمیم‌گیران است. از این رو، چنین افرادی که در موقعیتی هستند که در مورد انجام حمله تصمیم‌گیری می‌کنند، موظف می‌شوند تا برای تشخیص اینکه شخص یا وسیله مورد حمله، قانونی است، تمام توان خود را به کار برند[3]. به این ترتیب، آنگونه که قاعده ۵۴ دستورالعمل مذکور، مقرر می‌کند: «برنامه‌ریزان یا تصمیم‌گیران در مورد حمله سایبری، باید کلیه اقدامات احتیاطی ممکن را در انتخاب ابزارها و روش‌های جنگی قابل‌اعمال در حمله سایبری اتخاذ نمایند، با نظر به اینکه از صدمات ناخواسته به غیرنظامیان، سلب حیات غیرنظامیان و آسیب یا تخریب اشیاء غیرنظامی اجتناب نموده یا در هر حال، آن را به کمترین مقدار برسانند».

به عنوان یک وظیفه در راستای انجام اقدامات احتیاطی، افرادی که یک حمله سایبری را طراحی، تأیید یا اجرا می‌کنند، باید آن حمله را متوقف کنند یا به تعویق بیاندازند، اگر معلوم شود:

الف) اشیاء نظامی نیستند یا تحت حمایت ویژه می‌باشند؛

ب) انتظار می‌رود که حمله منجر به سلب ناخواسته حیات غیرنظامیان، مجروح‌شدن آنها، خسارت به اموال آنها یا مجموعه‌ای از این موارد که زیاده از مزایت نظامی عینی و مستقیم پیش‌بینی شده باشد (دستورالعمل تالین۱، ۲۰۱۳: قاعده ۵۷). به عنوان مثال، حالتی را در نظر بگیرید که در آن، قبل از شروع عملیات خصمانه، دولت (الف) بدافزار روتکیت را در بخشی از شبکه ارتباطی دولت (ب) پخش می‌نماید. بعد از شروع درگیری‌ها، انجام یک عملیات سایبری برای فعال کردن بمب‌های منطقی روی این روتکیت‌ها تأیید می‌شود. در طی این عملیات، اجزای کنترل ترافیک بدافزار روتکیت تشخیص می‌دهد که دولت (ب) اخیراً سیستم ارتباطی خدمات ضروری خود را به شبکه ارتباطی نظامی متصل نموده است؛ دراینجا مسئله تناسب مطرح می‌شود. دولت (الف) موظف است حمله سایبری خود را به تعویق بیندازد، تا زمانی که قانع شود حمله متناسب

---

[1] See AMW MANUAL: Rule 30
[2] See also Galić Trial Chamber Judgement: para. 58 & ICRC CUSTOMARY IHL STUDY, Rule 16
[3] See AMW MANUAL: Rule 35

است؛ برای مثال، از طریق انجام تفحص بیشتر برای مشخص نمودن صدمه احتمالی نسبت به جمعیت غیرنظامیان که با از کار انداختن سیستم ارتباطی خدمات ضروری صورت خواهد گرفت (دستورالعمل تالین ۱، ۲۰۱۳: ۱۴۴).

مطابق قاعده ۵۸ دستورالعمل تالین ۱، درنهایت، باید هشدار اولیه مؤثری در مورد حملات سایبری که ممکن است بر جمعیت غیرنظامی تاثیر داشته باشد، داده شود، مگر اینکه شرایط اجازه ندهد[1]. روش‌ها و ابزارهای هشدار صرفاً باید مؤثر باشند؛ لزومی ندارد ابزاری که انتخاب می‌شود، مؤثرترین ابزار موجود باشد. برای مثال، یک طرف مخاصمه شاید تصمیم بگیرد تا به تأمین‌کننده خدماتی که مورد استفاده کاربران غیرنظامی و نظامی است، حمله کند. آن مهاجم می‌تواند به جای ارسال پیامک‌هایی به کاربران غیرنظامی، از طریق رسانه‌های خبری ملی در مورد حمله قریب‌الوقوع هشدار دهد. حتی اگر روش ارسال پیامک‌ها راه مؤثری برای هشدار باشد، توجه به رسانه‌ها برای تامین ضروریات این قاعده مناسب‌تر خواهد بود. «مگر اینکه شرایط ایجاب ننماید» بیانگر این حقیقت است که هشدارها می‌توانند روی حمله تأثیر منفی داشته باشد (دستورالعمل تالین ۱، ۲۰۱۳: ۱۴۹)[2].

در بستر حملات سایبری، اقدامات احتیاطی ممکن می‌تواند شامل جمع‌آوری اطلاعات شبکه از طریق نقشه‌برداری یا فرآیندهای دیگر باشد تا به کسانی که مسئول هستند، این اجازه را بدهد تا به طور معقول تاثیرات احتمالی حمله علی‌الخصوص بر غیرنظامیان و اشیاء غیرنظامی را تشخیص دهند. هیچ تعهدی برای انجام اقداماتی که ممکن نیستند، وجود ندارد. برای مثال، ممکن است نقشه‌برداری هدف، به دلیل افشای عملیات، ممکن نباشد و بنابراین، دشمن را قادر به دفاع علیه عملیات مورد نظر کند.

مثال‌هایی در مورد اقدامات احتیاطی غیرعامل شامل این موارد است: تفکیک زیرساخت نظامی از زیرساخت سایبری غیرنظامی، تفکیک سیستم‌های رایانه‌ای که زیرساخت غیرنظامی حیاتی از طریق اینترنت با آن مرتبط است، تهیه نسخه پشتیبان از داده‌های مهم غیرنظامی، هماهنگی از قبل برای اطمینان از تعمیر به موقع سیستم‌های رایانه‌ای مهم، بایگانی اسناد فرهنگی یا دینی به صورت دیجیتال برای تسهیل بازسازی در مواقع آسیب یا خرابی آنها، استفاده از آنتی‌ویروس‌ها برای حمایت از سیستم‌های غیرنظامی که باعث خسارت یا نابودی به سازمان سایبری نظامی در حین حمله می‌شود (همان).

[1] See also German Manual, paras. 447, 453, 457 & ICRC Customary IHL Study: Rule 20
[2] See also ICRC Additional Protocol Commentary: para 2223

۲-۵. منع تحمل رنج بیهوده[1]

این قاعده که مبتنی بر ماده ۳۲ دستورالعمل‌های لاهه و بند ۲ ماده ۳۵ پروتکل الحاقی اول است، بازتاب حقوق بین‌الملل عرفی بوده و در هردو مخاصمه مسلحانه بین‌المللی و غیربین‌المللی، قابل‌اعمال است. این قاعده، صرفاً راجع به صدماتی که به رزمندگان، اعضای گروه‌های مسلح سازمان یافته و غیرنظامیانی که مستقیماً در عملیات خصمانه مشارکت می‌کنند، اعمال می‌شود. سایر افراد در وهله اول از حمله در امان می‌مانند یا اصل تناسب و ضرورت اتخاذ اقدامات احتیاطی در حمله بر هرگونه صدمه غیرعمد به آنها در حین حمله حاکم خواهد بود. به عبارتی، صدمات زیاده از حد و درد و رنج غیرضروری با مفهوم صدمات جزئی وارده به افراد برابر نیست.

قاعده ۴۲ دستورالعمل تالین ۱ نیز، در راستای توجه به این اصل، مقرر داشته است: «به کار گرفتن روش‌ها و ابزارهای جنگ سایبری که ماهیتاً صدمه زیاده از حد و درد و رنج غیرضروری به همراه دارد، ممنوع است».

این اصل اساسی حقوق بشردوستانه، ضمن قاعده ۱۰۴ دستورالعمل تالین ۲، اینگونه بیان شده است: «به‌کارگیری ابزارها یا شیوه‌هایی از جنگ سایبری که واجد ماهیتی هستند که موجب جراحت زائد یا رنج غیرضروری می‌گردند، ممنوع است»؛ این قاعده، صرفاً بر جراحت یا رنج ایجاد شده برای رزمندگان، اعضای گروه‌های مسلح سازمان‌یافته و غیرنظامیانی که مستقیماً در عملیات‌های متخاصمانه شرکت می‌کنند، اِعمال می‌شود. سایر افراد، در وهله نخست، در برابر حمله مصون هستند. هر گونه آسیب ضمنی به آنها که در خلال یک حمله ایجاد گردد، تحت شمول قاعده تناسب و قاعده مربوط به اتخاذ اقدامات احتیاطی در حمله قرار می‌گیرد. به عبارت دیگر، جراحت زائد و رنج غیرضروری با مفهوم آسیب ضمنی به غیرنظامیان برابر نیست.

اصطلاح «صدمات زیاده از حد و درد و رنج غیرضروری» به وضعیتی اشاره دارد که در آن یک سلاح و یا استفاده خاصی از یک سلاح، بدون فراهم آوردن مزایای نظامی بیشتر برای مهاجم، منجر به افزایش شدت درد و رنج می‌شود؛ همانطور که دیوان بین‌المللی دادگستری در نظریه مشورتی سلاح‌های هسته‌ای ۱۹۹۶ اشاره نموده است (نظریه مشورتی سلاح‌های هسته‌ای، پاراگراف ۷۸) ، دولتها در انتخاب سلاح، آزادی نامحدود نداشته و نیز، تسلیحات، نباید برای حصول اهداف نظامی مشروع، باعث آسیب بسیار شدید و غیرضروری شود. این ممنوعیت دولتها را تشویق می‌کند تا از سطح مناسب نیروها و امکانات خود برای رسیدن به هدف نظامی خود، استفاده کنند. ایده اصلی این است که آسیب نباید بیش از آن چیزی باشد که برای رسیدن به اهداف نظامی مشروع مورد نظر لازم است. براساس این اصل، سلاح‌های بی‌هدف، مانند سلاح‌های بیولوژیکی یا سلاح‌های شیمیایی غیرقانونی است.

[1] Unnecessary Suffering

حملات سایبری اغلب به دشواری کنترل می‌شوند و در نتیجه اثرات نامطلوب آنها ممکن است محدوده گسترده‌ای را در بر بگیرد؛ چنانکه سلاح‌های سایبری که استفاده از کرم را به کار می‌گیرند، می‌توانند میلیون‌ها کامپیوتر را به طور ناخواسته آلوده کنند. علاوه بر این، یک حمله اینترنتی می‌تواند باعث رنج غیرضروری شود، زیرا می‌تواند یک حمله گسسته باشد که باعث ضرر بیش از حد شود؛ به عنوان مثال، یک حمله سایبری را که به پرونده پزشکی یک فرمانده نظامی دشمن توجه دارد، در نظر بگیرید. از سوی دیگر، سلاح‌های سایبری اغلب پایین‌ترین سطح نیرو هستند که می‌توانند در مقایسه با یک حمله سنتی استفاده شوند. یک حمله جنبشی که به منظور تعطیل یک ژنراتور الکتریکی، توسط یک بمب انجام می‌شود، منجر به آسیب و تخریب بیشتری خواهد شد نسبت به یک حمله سایبری به همان ژنراتور الکتریکی که هدف گرفته شده است. بنابراین، فرماندهان نظامی اغلب استفاده از یک حمله سایبری را ترجیح می‌دهند، زیرا حملات سایبری ممکن است باعث نابودی یک زیرساخت شود و می‌تواند یک سلاح ترجیحی برای دولتها باشد. به این ترتیب، یک حمله سایبری، مانند یک حمله با سلاح جنبشی، زمانی غیرقانونی است که عواقب آن مشابه یک حمله جنبشی منجر به رنج بیهوده باشد (گراویس، ۲۰۱۲: ۵۷۸).

ابزار و روش‌های جنگ سایبری صرفاً در موارد نادری باعث نقض این قاعده می‌شوند. با این حال، ابزار و روش‌های جنگ که به طور کلی مشروع هستند، باعث بروز رنج‌هایی می‌شود که نسبت به مزیت نظامی، غیرضروری است؛ برای مثال، یک رزمنده دشمن را در نظر بگیرید که مجهز به دستگاه کنترل ضربان قلب است که آدرس آن از طریق اینترنت قابل رهگیری است. تحت کنترل درآوردن این دستگاه برای کشتن آن فرد یا برگرداندن آن فرد به خارج از صحنه نبرد برای مثال از طریق پرش‌زدایی که به منظور اختلال در قلب ایجاد می‌شود، مشروع است. ولی اگر این عملیات طوری صورت گیرد که منجر به بروز درد و رنج اضافی شود، یا با هدف مشروع نظامی عملیات بی‌ارتباط بوده یا آشکارا فراتر از آن باشد، غیرقانونی تلقی می‌شود. مثال چنین اقدامات نامشروع شامل اختلال در عملکرد قلب و احیاء نمودن شخص برای چندین بار قبل از کشته شدن شخص است. انجام چنین کاری باعث رنج‌هایی می‌شود که هیچ هدف نظامی ندارد (دستورالعمل تالین ۱، ۲۰۱۳: ۱۲۰).

۲-۶. بی‌طرفی[1]

اصل بی‌طرفی، که در ماده ۱ کنوانسیون لاهه ۱۹۰۷ درباره حقوق و وظایف قدرت‌ها و اشخاص بی‌طرف در صورت وقوع جنگ زمینی، ماده ۱ کنوانسیون لاهه ۱۹۰۷ درباره حقوق و وظایف قدرت‌ها و اشخاص بی‌طرف در جنگ‌های دریایی، کنوانسیون‌های چهارگانه ژنو ۱۹۴۹ و پروتکل

[1] Neutrality

الحاقی اول به کنوانسیون‌های چهارگانه ژنو ۱۹۷۷ بیان شده است، بسیار نزدیک به فرضی است که ممکن است یک منطقه جغرافیایی، به محدوده‌ای که مخاصمه در آن واقع شده است، محدود شود[1] و به این ترتیب، منطقه‌ای برای محافظت از افراد غیرنظامی و اموال آنها و همچنین، سایر نهادهای دولتی که به صورت مستقیم در مخاصمه دخالت ندارند، مشخص شود (نوپووا[2]، ۲۰۱۶: ۵۷). بر اساس این اصل، سرزمین‌های بی‌طرف، که «شامل قلمرو زمینی دولت‌های بی‌طرف و نیز آب‌های مشمول حاکمیت سرزمینی آنها یعنی، آبهای داخلی، دریای سرزمینی و در صورت قابلیت اعمال، آب‌های مجمع‌الجزایری و فضای هوایی فوقانی آن مناطق می‌گردد (دستورالعمل تالین ۲، ۲۰۱۷: ۵۵۳)» از تعرض سایر کشورها مصون هستند و دولت‌های متخاصم ملزم هستند که به مکان‌های بی‌طرف، احترام گذارند و از وارد کردن خسارت به آنها اجتناب کنند؛ اما در صورتی که اشخاص بی‌طرف، به اقدامات خصمانه، علیه متخاصمان مبادرت کنند، از وضعیت بی‌طرفی خارج می‌شوند. ممنوعیت‌های موجود بر اساس اصل بی‌طرفی، از اصل برابری حاکمیت دولت‌ها در حقوق بین‌الملل سرچشمه گرفته است (اسمعیل زاده ملاباشی و دیگران، همان، ۵۵۰).

حقوق بی‌طرفی رابطه میان طرفین یک مخاصمه مسلحانه بین‌المللی از یک سو و دولت‌هایی که طرف مخاصمه ذیربط نیستند، از سوی دیگر را تنظیم می‌کند. اهداف محوری آن عبارتند از: (۱) حفاظت از دول بی‌طرف و شهروندان آنان در برابر پیامدهای زیان‌بار مخاصمه؛ (۲) حراست از حقوق بی‌طرفی همانند مبادرت به بازرگانی در دریاهای آزاد؛ و (۳) حمایت از طرفین مخاصمه در برابر اقدام یا عدم اقدام از جانب دول بی‌طرفی که به نفع دشمن آن‌هاست (دستورالعمل تالین ۲، ۲۰۱۷: ۵۵۵).

ضمن یک جنگ سایبری، ناگزیر، اصل بی‌طرفی، به دلیل ساختار منحصربه‌فرد و پیچیده اینترنت نقض خواهد شد، زیرا مسیر حملات سایبری، با توجه به ساختار فعلی اینترنت، از کشورهای بی‌طرف عبور خواهد کرد؛ به عنوان مثال، هنگامی که یک حمله سایبری علیه یک کشور آغاز می‌شود، حمله ممکن است از طریق گره‌های اینترنتی، به کشورهای بی‌طرف نیز نفوذ کند (کلسی، ۲۰۰۹: ۱۴۴۱)؛ توزیع جهانی تجهیزات و فعالیت‌های سایبری و نیز وابستگی جهانی به زیرساخت سایبری به این معناست که عملیات‌های سایبری طرف‌های یک مخاصمه می‌توانند به آسانی زیرساخت‌های سایبری خصوصی یا عمومی را تحت تأثیر خود قرار دهند. بر این اساس، بی‌طرفی در مخاصمات مسلحانه نوین از موضوعیت و اهمیت ویژه‌ای برخوردار است (دستورالعمل تالین ۲، ۲۰۱۷: ۵۵۵).

قاعده ۱۵۱ دستورالعمل تالین ۲ اعلام می‌کند: «اِعمال حقوق ناشی از مخاصمه به وسیله ابزارهای سایبری در قلمرو بی‌طرف ممنوع است. همچنین، با توجه به قاعده ۱۵۳ دستورالعمل دوم

[1] See AMW MANUAL: Rule 167(a)
[2] Knopova

تالین، «یک دولت بی‌طرف نباید آگاهانه به طرفین منازعه اجازه اِعمال حقوق ناشی از مخاصمه از زیرساخت‌های سایبری مستقر در قلمرو خود یا تحت کنترل انحصاری خویش را بدهد».

با توجه به ماهیت و حقیقت حملات سایبری، زمانی عدم انتقال اطلاعات می‌تواند تنها راه برای ممانعت از حمله سایبری در برابر آسیب‌های عمده به جان مردم و اهداف مادی از جمله زیرساخت و کالاهای عمومی باشد، که تصمیم در خصوص اعمال مفهوم بی‌طرفی در جنگ سایبری بدون تغییر یا با اصلاح قواعد، بدون قید و شرط توسط کشورهای عضو جامعه بین‌الملل اتخاذ شود و به این ترتیب، مشاهده می‌کنیم که دستورالعمل تالین ۲ سعی در شناسایی قواعد بی‌طرفی و تعمیم آنها به عملیات سایبری و تشویق دولتها نسبت به رعایت آنها نموده است.

با توجه به احتمال نقض این اصل در حملات سایبری، دستورالعمل تالین ۱، ضمن قواعد ۹۱ الی ۹۵ و همچنین، دستورالعمل تالین ۲، ضمن قواعد ۱۵۰ تا ۱۵۴، به اصل بی طرفی پرداخته‌اند؛ چنانکه در قاعده ۹۱ دستورالعمل تالین ۱ مقرر شده است، استفاده از حقوق خصمانه، با توسل به ابزار جنگی برای مقاصد سایبری علیه زیرساخت‌های سایبری ممنوع است؛ زیرا زیرساخت‌های سایبری بی‌طرف که به طور فیزیکی در حریم هوایی بین‌المللی، فضای بیرون جو یا دریاهای آزاد واقع شده‌اند، به موجب حق حاکمیت ملی دولت حمایت می‌شوند.

از دیگر سوی، مطابق قاعده ۹۲ دستورالعمل تالین ۱، «بهره‌مندی از حقوق طرف مخاصمه توسط ابزار سایبری در قلمرو بی‌طرف ممنوع است»؛ این قاعده که مبتنی بر مواد ۲ و ۳ کنوانسیون پنجم لاهه و مواد ۲ و ۵ کنوانسیون هشتم لاهه بوده و بازتاب عرف بین‌المللی است، نیروهای مسلح طرف مخاصمه را از انجام عملیات سایبری از طریق قلمرو بی طرف منع می‌سازد، در حالیکه قاعده ۹۱ عملیات علیه زیرساخت سایبری بی‌طرف را مورد خطاب قرار می‌دهد، این قاعده به استفاده چنین زیرساختی توسط متخاصم در قلمرو بی‌طرف می‌پردازد.

براساس قاعده ۹۳ دستورالعمل تالین ۱ و قاعده ۱۵۲ دستورالعمل تالین ۲، «دولت بی‌طرف نباید آگاهانه اجازه بهره‌مندی از حقوق طرف مخاصمه را به طرفین مخاصمه با توسل به زیرساخت‌های سایبری واقع شده در قلمرو خود یا تحت کنترل خود، بدهد». در فضای عملیات سایبری باید این مهم را در نظر داشت که بر طبق ماده ۳ کنوانسیون ۵ لاهه طرفین مخاصمه مجاز نمی‌باشند:

الف) در قلمرو قدرت بی‌طرف ایستگاه‌های تلگرافی بیسیم یا دستگاه‌های دیگر به منظور ارتباط با نیروهای طرف مخاصمه در دریا یا خشکی بنا نهند.

ب) به علاوه، مجاز نمی‌باشند از هر نوع تأسیساتی از این قبیل که توسط آنها قبل از جنگ در قلمرو بی‌طرف صرفاً برای اهداف نظامی تاسیس شده است و این تاسیسات برای خدمات پیام‌های عمومی در دسترس نمی‌باشد، استفاده کنند.

به موجب قاعده ۱۵۳ دستورالعمل تالین ۲، مقرر شده است که «اگر یک دولت بی‌طرف در پایان بخشیدن به اِعمال حقوق ناشی از مخاصمه در قلمرو خود قصور ورزد، طرف زیان‌دیده مخاصمه می‌تواند اقداماتی همچون عملیات‌های سایبری که برای مقابله با آن رفتار ضروری هستند را اتخاذ کند»؛ اجرای این قاعده به دو معیار وابسته است: نخست، نقش قلمرو دولت بی‌طرف باید «جدی و شدید» باشد. نقض‌های جزئی و ناچیز موجب اِعمال این قاعده نمی‌گردند؛ به دیگر سخن، طرفِ ناقض وضعیت بی‌طرفی باید از رهگذر آن نقض برتری نظامی معناداری بر دشمن پیدا کند؛ جدیت را نمی‌توان به صورت انتزاعی تعیین کرد، بلکه به شرایط حاکم در زمان مربوطه بستگی دارد. این معیار می‌تواند بر فراگیر بودن نقض یا مزیت حاصله برای ناقض به خاطر آن نقض بستگی داشته باشد؛ برای مثال، ایجاد توانمندی نفوذ در حساب‌های ایمیل شخصی اعضای رده‌پایین نیروهای مسلح دشمن موجب بروز این قاعده نمی‌گردد. در مقابل، تصور کنید که توانمندی سایبری یکی از طرفین مخاصمه به خاطر عملیات‌های سایبری کاهش پیدا کرده باشد، استفاده آن طرف از زیرساخت سایبری بی‌طرف جهت انجام عملیات‌های سایبری علیه دشمن، جدی و شدید به شمار خواهد رفت. دوم، اِعمال حقوق ناشی از مخاصمه در قلمرو بی‌طرف توسط یکی از طرفین مخاصمه باید بیانگر تهدیدی فوری برای امنیت طرف زیان‌دیده بوده و هیچ جایگزین ممکن و به‌هنگامی برای اتخاذ اقدام در قلمرو بی‌طرف وجود نداشته باشد[1]؛ بنابراین، قاعده حاضر صرفاً در صورتی که دولت بی‌طرف مایل یا قادر به پایبندی به تعهدات خویش وفق قاعده‌ی ۱۵۲ دستورالعمل تالین ۲ نباشد، اعمال می‌گردد. اگر چنین باشد، طرف زیان‌دیده حق دارد به مجرد اینکه دولت بی‌طرف کلیه اقدامات در دسترس خود را برای پایان بخشیدن به نقض بی‌طرفی توسط دشمن اتخاذ کرده، ولی به هر جهت موفق نبوده باشد، به این کار مبادرت ورزد. بدیهی است که طرف زیان‌دیده می‌تواند زمانی که کاری برای پایان دادن به نقض ذیربط انجام نمی‌دهد نیز دست به اقدام بزند (دستورالعمل تالین ۲، ۲۰۱۷: ۵۵۸).

بحث و نتیجه‌گیری

تاریخ، همزمان با پیشرفت علم و تکنولوژی، شاهد تبدیل سلاح‌های جنگی از جنس سنگ و چوب، به سلاح‌های شیمیایی، هسته‌ای، بیولوژیک و میکروبی بوده است. با رشد و توسعه روزافزون علوم و فناوری اطلاعات و ارتباطات و در مقابل، افزایش تولید و استفاده از بدافزارهایی چون ویروس ها و کرم، فضای سایبر نیز به عنوان فضایی که پتانسیل تبدیل به فضای جنگی مخاطره‌آمیز را خواهد داشت، مطرح است؛ چنانکه مایکل راجرز، فرمانده NSA در فوریه ۲۰۱۳ در مصاحبه با مجله فن‌آوری اطلاعات نظامی[2] گفت: «به شبکه اینترنت، باید به عنوان یک سیستم

[1] See San Remo Manual, Rule 22
[2] Military Information Technology

تسلیحاتی نگاه کرد و ما باید به مبارزه برای حفظ برتری خود در فضای سایبری ادامه دهیم که طبعاً سبب تفوق ما در چهار عرصه جنگی دریا، هوا، زمین و فضا خواهد شد. از آنجا که فضای سایبری، پنجمین عرصه جنگی در آینده خواهد بود، پنتاگون باید در تربیت جنگاوران فضای سایبری سرمایه‌گذاری کند. ما باید نیروی آموزش‌دیده خود در زمینه فضای سایبری و آشنا به جدیدترین فناوری‌ها و پیشرفت‌ها در این عرصه را گسترش دهیم تا بتوانیم مبارزه سایبری در هر نقطه از جهان را عملیاتی کنیم».

عملیات سایبری، با توجه به وابستگی عملکردهای مختلف اقتصادی، اجتماعی و سیاسی دولتها و همچنین زیرساخت‌های مهم، حساس و حیاتی ملتها به فضای سایبری، می‌تواند هم‌رده سلاح‌های سنتی، به عنوان یک سلاح مطرح شده و در شرایط رسیدن به آستانه حمله سایبری، اصل منع توسل به زور درباره عملیات سایبری، قابل اعمال و دفاع مشروع دولتها به ضرورتی اجتناب‌ناپذیر تبدیل خواهد شد.

تاکنون، از جمله مهمترین تحقیقات و تحریرات موجود درباره فضای سایبری، می‌توان به دستورالعمل‌های تالین ۱ و ۲ درباره حملات و عملیات سایبری اشاره کرد که این دو سند، به لحاظ تحقیقی و عدم الزام‌آور بودن، نمی‌توانند خلاء قانونی موجود را در زمینه عملیات سایبری برطرف نمایند و به این ترتیب، قواعد عمومی موجود در حقوق بین‌الملل عمومی و بشردوستانه بر شرایط ایجاد شده بر اثر عملیات سایبری، حکمفرما خواهد بود.

در این تحقیق، کوشیده شد با استفاده از قواعد جدیدترین منابع موجود درباره عملیات سایبری، اصول حقوق بشردوستانه بین‌المللی در ارتباط با حملات سایبری، بررسی شود و مشاهده شد که اصول حقوق بشردوستانه بین‌المللی به صورت عام در دستورالعمل‌های تالین ۱ و ۲ نیز پذیرفته شده است و علیرغم وجود این قواعد، نیاز به قاعده‌مندسازی عملیات در فضای سایبری تحت یک سند الزام‌آور بیش از پیش خودنمایی می‌کند.

منابع

- اسمعیل زاده ملاباشی، پرستو، عبداللهی، محسن و زمانی، سید قاسم (۱۳۹۶). **حملات سایبری و اصول حقوق بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)**. تهران. فصلنامه مطالعات حقوق عمومی. ۴۷(۲).
- بلدسو رابرت و بوچک (۱۳۷۵). **فرهنگ حقوق بین‌الملل**. ترجمه بهمن آقایی، تهران. گنج دانش.
- دینیس، هیتر هریسن (۱۳۹۵). **جنگ سایبری و حقوق جنگ**. ترجمه سعید حکیمی‌ها و هومان شاهرخ. تهران. نشر میزان.
- ضیایی بیگدلی، محمدرضا (۱۳۹۲). **حقوق بین‌الملل بشردوستانه**. ج اول. تهران. گنج دانش.
- کولب، رابرت و هاید، ریچارد، (۱۳۹۳). **درآمدی بر حقوق مخاصمات مسلحانه**. ترجمه حسام‌الدین لسانی. تهران. مجد.
- گیوکی، آذر و کفایی فر، محمد علی و رضایی، محمدتقی (۱۳۹۷). **قابلیت اعمال حقوق بشردوستانه بین‌المللی در حملات سایبری با نگاهی به دستورالعمل تالین ۲**. تهران. مجله حقوق پزشکی. ویژه نامه حقوق بشر و شهروندی. ۱۴.
- ممتاز، جمشید و شایگان، فریده (۱۳۹۳). **حقوق بین‌الملل بشر دوستانه در برابر چالش‌های مخاصمات مسلحانه عصر حاضر**. تهران. شهردانش.
- نواده توپچی، حسین (۱۳۹۳). **حقوق جنگ و مخاصمات مسلحانه**. تهران. خرسندی.

-David, Jashua (2007). **Hackers take down the most wired country in Europe**. Wired Magazine. 15.
-Dinstein, Yoram (2016). **The Conduct of Hostilities under the Law of International Armed Conflict**. Cambridge University Press.
-Dinstein, Yoram (2005). **War, aggression and self- defense**. Cambridge University Press. 4th ED.
-Dunlap, Charles J. (2000). **The End of Innocennce: Rethinking Non-combatancy in the Post-Kosovo Era**. Summer Strategic Review.
-Gervais, Michael (2012). **Cyber Attacks and the law of War**. Berkeley Journal of International Law, Vol. 30.
-Graham David E., (2010). **Cyber Threats and the Law of War**. Journal of National Security Law & Policy. Vol. 4.
- Hathaway, 0ona and Crootof, Rebecca and Levitz, philipe and Nix, Haley and Nowlan, Aileen and Perdue, William and Spiegel, Julia (2012). **The Law of Cyber-Attack**. California Law Review. Vol. 100.
-Kelsey, Jeffrey T.G. (2009). **Hacking in to International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare**. Michigan Law Review. vol.106.
-Kittichaisaree, Kriangsak (2017). **Public International Law of Cyberspace**. Switzerland: Springer.
-Knopova, Eva (2016). **New IHL Framework for Cyber Warfare**. Master thesis of Charles University in Prague.
-Melzer, Nils, (2011). **Cyber Warfare and International Law**. The United nationa Institute for Disarmament Research (UNIDIR).

-Papanastasiou, Afroditi (2010). **Application of International Law in Cyber Warfare Operations**. University of Leicester.
-Roscini, Marco (2010). **World Wide Warfare-Jus Ad Bellum and the Use of Cyber Force**. Max Planck U.N.Y.B. Vol. 85.
-Sharp, Walter Gray (1999). **Cyber Space and the Use of Force**. Aegin Research Corporation.
- 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 Operations**. London. Cambridg University press (2017).
- International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence (2013). **Tallinn Manual 1.0 on the International Law Applicable To Cyber Warfare**. London. Cambridg University press.
-Schmitt, Michael N. (1999). **Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework**, Columbia Journal of Transnational Law. Vol.37.
-Zemanek, Karl (2010). **Armed attack**, Max Plank Encyclopedia of Public International Law.
- ICJ Judgment, Nicaragua V. United states (1986).
- ICJ, Legality of the Threat or Use of Nuclear Weapons advisory opinion (1996).
- Case concerning Military and paramilitary activities in and against Nicaragua (Nicaragua V. United states)(1986).
- S.C/Res/1308, 2001.
- S.C/Res/1373, 2001.
-ICC Tadić Decision on The Defence Motion for Interlocutory Appeal (1999).
-ICRC Customary IHL Study.
-Rome Statute of the International Criminal Court (1998).
-Amended Mines Protocol (1996).
-AMW Manual (Manual on International Law Applicable to Air and Missile Warefare)(2009).
- U.K. MANUAL (UK Ministry of Defence, the joint service manual of armed conflict (2004)
- San Remo Manual.
-OXFORD ENGLISH DICTIONARY ONLINE, http://www.oed.com/view/Entry/267413?redirectedFrom=malware#eid
-The History of Computer Viruses, VIRUS-SCAN-SOFTWARE.COM, http://www.virus-scansoftware.
com/virus-scan-help/answers/the-history-of-computer-viruses.shtml
-Meet CERT, SOFTWARE ENG'G INST., CARNEGIE MELLON UNIV., http://www.cert.org/meet_cert/#bkgd.