**فصلنامه سیاست خارجی**
**سال سی و پنجم، شماره ۴، زمستان ۱۴۰۰، صص ۱۷۴- ۱۵۵**

# ۶

# اعمال مقررات حقوق بین‌الملل بشردوستانه در عرصه جنگ‌های سایبری: چالش‌ها و راهکارها

*دکتر مهدی حیدری فرد* [۱]

تاریخ دریافت مقاله:۱۴۰۰/۷/۱۵ تاریخ پذیرش مقاله:۱۴۰۰/۸/۳۰

[۱]. دکتری تخصصی، رشته حقوق بین‌الملل عمومی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، دامغان، ایران
mahdiheydarifard@yahoo.com

# چکیده

افزایش روزافزون سطح اتکای عملکرد بسیاری از زیرساخت‌های شهری به فضای مجازی، هشدارها نسبت به آسیب‌پذیری آنها را به دنبال داشته است. در حوزه حقوق بشردوستانه، بحث در رابطه با قابلیت اعمال اصول و قواعد حاکم برهدایت مخاصمات (تفکیک، تناسب و اتخاذ اقدامات احتیاطی) و تفسیرهای موجود از آنها در حوزه جنگ‌های سایبری، با توجه به ویژگی‌های خاص فضای سایبری، از اهمیت خاصی برخوردار می باشد. بخصوص وقتی که بدانیم ترتیبات قراردادی این حوزه حقوقی (کنوانسیونهای چهارگانه ژنو (۱۹۴۹) و پروتکل های الحاقی اول و دوم ۱۹۷۷) بر مبنای شرایط عینی بروز جنگ‌های کلاسیک تدوین و تفاوت‌های ماهوی آن با نبرد سایبری، همچنین پیوندهای درون‌شبکه‌ای فضای سایبری، طبیعتا چالش‌های اساسی در اعمال قواعد هدایت مخاصمات در این عرصه را باعث می‌گردد. این مقاله سعی دارد با در پیش گرفتن روش تحقیق تبیینی و در نظر گرفتن ویژگی‌های منحصربفرد فضای سایبر، چگونگی تفسیر و اعمال قواعد اصلی هدایت مخاصمات درعرصه جنگ‌های سایبری را بررسی و راهکارهایی را پیشنهاد نماید. در این راستا سوال اصلی این است که با توجه به تبعات و عواقب سوء عملیات خصمانه در فضای سایبری بر جمعیت غیرنظامی، آیا اصول حقوق بین‌الملل بشردوستانه بر مخاصمات و جنگهای سایبری قابل اعمال می‌باشد و در صورت پاسخ مثبت، چالش‌ها و موانع فراروی اعمال و تفسیر مقررات اساسی هدایت مخاصمات و حقوق بشردوستانه بر جنگ های سایبری کدامند؟.

• *واژگان کلیدی*

**حقوق بشردوستانه بین‌المللی، تسلیحات سایبری، حمله سایبری، عملیات سایبری، مقررات هدایت مخاصمات.**

**مقدمه**

طی سالیان اخیر نگرانی کشورها در برخورد با این شیوه مدرن جنگی بیشتر بعد حفاظتی امنیتی داشته وکمتر بر لزوم نظم بخشی حقوقی وبررسی چالش‌های حقوقی این حوزه به ویژه نحوه اعمال و تفسیر قواعد حقوق بشردوستانه توجه شده است.شاید ریشه این کم‌توجهی را بتوان در تصور غلط عمومی نسبت به عواقب جنگ سایبری جستجو کرد، بطوری‌که عرف موجود عبارت "جنگ بدون خونریزی[1]" را در توصیف جنگ‌های سایبری بکار می‌برد[2].در نگاه اول ممکن است چنین به نظر رسد که یک عملیات سایبری فقط منجر به اختلال در ظرفیت‌های ارتباطی یا عملکرد زیرساخت‌های متکی بر سایبر گردیده و تاثیرات آن بر جمعیت غیرنظامی نمی‌تواند بشدت اقدامات جنگی کلاسیک مثل بمباران یک منطقه باشد, اما به دلیل تنوع دامنه تاثیرات سو حملات سایبری بر جوامع غیرنظامی, این حملات گاهی بسیار فاجعه‌بارتر از یک حمله نظامی در دنیای فیزیکی می باشند (Schmitt.M.2017:78). لذا اعمال قواعد اصلی هدایت مخاصمات برخاسته از کنوانسیونهای چهارگانه ژنو (۱۹۴۹) و پروتکل های الحاقی اول و دوم (۱۹۷۷) بر عرصه جنگ های سایبری، همچنین بررسی چالشهای اعمال قواعد مذکور بر فضای سایبری و مجازی اجتناب ناپذیر می باشد.

**جنگ در فضای مجازی، ویژگی های منحصر بفرد**

جنگ سایبری برخی از اساسی‌ترین مفروضات حقوق بشردوستانه را که بر مبنای اصول و شرایط حاکم بر جنگ‌های کلاسیک در دنیای واقعی تدوین شده به چالش می‌کشد:

۱- حقوق بشردوستانه کلاسیک در شرایط زمانی تدوین شد که عموم درگیری های مسلحانه در میدان باز، صحنه جنگ واقعی و عموما بین کشورها متداول بود. لذا مفروض اصلی آن این است که غالبا طرفین بیشتر درگیری‌های نظامی، حتی مخاصمات غیربین‌المللی، شناخته شده هستند، در حالی که در عملیات سایبری "ناشناس بودن[3]" یک اصل است و بقیه فاکتورها استثناء هستند (Lobel,Hanna,2012:623) این

---

1. War Without Bloodshed
2. Shane, Scotte, Cyber Warfare Emerges From Shadows of Public Discussions By US Officials, An Article in The New York Times,26 September 2012, P. A10
3. Anonymity

عامل شناخت عامل اصلی حمله و انتساب عمل متخلفانه به وی را با مشکلاتی مواجه خواهد نمود[۱].

۲- طبق مفروض دیگر حقوق بشردوستانه، درگیری نظامی تاثیرات مخرب و شدیدی، به شکل فیزیکی و ملموس، بدنبال دارد، در حالی‌که جنگ سایبری تحرکات نظامی معمول جنگ‌های کلاسیک را نداشته و تاثیرات بسیاری از این جنگ‌ها گرچه مخرب، در عین حال عموما بصورت فیزیکی و ملموس نمی باشد[۲].

۳- ساختار قواعد هدایت مخاصمات در حقوق بشردوستانه، به ویژه اصل تفکیک بر این پیش فرض بنا شده که اصولا اهداف نظامی و غیرنظامی جدا و مهم‌تر از همه قابل تشخیص باشند. در صورتی‌که در عرصه یک جنگ سایبری این وضعیت جدای از اینکه یک مفروض اصلی باشد، بیشتر یک استثناء می‌باشد، چرا که بیشتر تاسیسات سایبری به‌عنوان مثال کابل های زیردریایی، سرورهای رایانه‌ای، ماهواره‌ها، مسیریاب‌ها و... کاربرد دوگانه[۳] دارند، از طرف دیگر وجود ارتباطات درونی و بهم‌پیوستگی فضای سایبر امکان تسری عواقب سوء حمله به سایر سیستم‌های رایانه‌ای را افزایش خواهد داد،(Schmitt.M, 2013: 249).

## اصول مهم مقررات هدایت مخاصمات در حقوق بشردوستانه و چالش های اعمال آنها در عرصه حمله سایبری

### ۱) اصل تفکیک

اصل تفکیک افراد و اهداف نظامی و غیرنظامی یکی از اصول اساسی حقوق بشردوستانه و هدایت مخاصمات مسلحانه می باشد. طبق این اصل، در برنامه‌ریزی و اجرای یک عملیات سایبری، تنها اهداف مشروع از نظر حقوق بشردوستانه اهداف نظامی یعنی ظرفیت‌های ارتباطی و زیرساخت‌های متکی بر سیستم‌های کامپیوتری که نقشی موثر در پیشبرد عملیات نظامی دارند، می

---

[1]. Michael.N.Schmitt,"Classification of Cyber Conflict",The Journal of Conflict and Security Law, Volume 17, Issue 2, Summer 2012P.252

[2]. Report of the 31th International Conference of the Red Cross and Red Crescent (28 November – 1th December 2011), Report on international Humanitarian Law and the Challenges of contemporary Armed Conflicts, Prepared by the International Committee of the Red Cross and the International Federation of Red Cross and Red Crescent Societies, Geneva

[3]. Dual use

باشند. (Shulmann.M,1999:75). مشکل اینجاست که در فضای سایبری، تعیین نظامی بودن یا نبودن یک هدف، همواره با یک‌سری پیچیدگی‌ها وابهاماتی همراه است. با این وجود جمله‌بندی بند دوم ماده ۵۲ پرتکل الحاقی اول در خصوص تعریف هدف نظامی که پیشتر آورده شد، ، بیانگر لزوم وجود ارتباط درونی بین هدف بالقوه و عملیات نظامی می‌باشد. این پیوند درونی از طریق چهار شاخص ماهیت، موقعیت، هدف و کاربرد یک هدف ایجاد می گردد.(Kelsey, 2007-8:1439).

اهم ابهامات در رابطه با تعیین نظامی بودن یا نبودن یک هدف در عرصه سایبری بدین شرح می باشند:

۱- این واقعیت که در دنیای کنونی، بیشتر زیرساخت‌های سایبری موجود، در عمل دارای کاربرد دو گانه هستند.

۲- اطلاق "هدف نظامی" به کارخانه‌های تولیدکننده نرم‌افزارو سخت‌افزار بکار رفته در صنایع تسلیحاتی

۳- مفهوم "کمک موثر زیرساخت سایبری به توانمندی‌های جنگی بالقوه یا بالفعل یک کشور؟"

۴- مشروعیت جهت‌گیری حمله به سوی شبکه‌های اجتماعی و دفاتر رسانه‌ای مورد استفاده برای مقاصد نظامی(Schmitt,2013:84)

### اهداف با کاربرد دوگانه در فضای سایبری

بخش‌هایی از تاسیسات زیربنایی شهروندی مثل نیروگاه‌ها و شبکه توزیع برق کار پشتیبانی عملیات نظامی را انجام می دهند. گاهی نیز عملکرد ارتباطی یک زیرساخت سایبری جهت انتقالاطلاعات نظامی بکار می رود. چنین تاسیساتی بر اساس شاخص "کاربرد" در تعریف هدف نظامی و مورد بهره‌برداری قرار گرفتن تاسیسات مذکور برای مقاصد نظامی، آنها جزء اهداف قانونی حمله محسوب خواهند شد. با در نظرداشتن این واقعیت که در شرایط درگیری، طرفین بدنبال ساقط کردن عملکرد زیرساخت‌های نظامی بوده و ممکن است از فضای سایبری در جهت پیشبرد عملیات نظامی استفاده شود، همواره ریسک مورد هدف قرار گرفتن زیرساخت‌های سایبری کشورها وجود دارد. در یک درگیری نظامی، طبیعی است که هر طرف بر اساس منافع استراتژیک خود سعی در تضعیف شبکه‌های ارتباطی طرف دیگر داشته و در این راستا اقدام به هدف قرار دادن زیرساخت‌های متکی بر سیستم کامپیوتری در کشور هدف و کاهش دسترسی دشمن به مسیرهای اصلی فضای سایبر و دسترسی به گره های اصلی ارتباطی[1] نماید (Schmitt,M,2002:45).

[1]. Mode

امروزه نظریه غالب این است که یک هدف در یک زمان نمی‌تواند هم نظامی و هم غیرنظامی باشد. بطور کلی، مادام که یک هدف به‌منظور کمک به عملیات نظامی بکار گرفته شود، به عنوان یک هدف نظامی مشروع در نظر گرفته می شود. گاهی برخی قسمت‌های اهداف مذکور، به عنوان مثال ساختمان‌های مختلف یک بیمارستان، غیرنظامی باقی می‌مانند، در این شرایط، در صورتی که قسمت‌های فوق قابل تشخیص باشد، آنها غیرنظامی تلقی خواهند شد.

در سال ۱۹۵۶ در جریان مجادلاتی که در خصوص پیشنهاد کمیته بین‌المللی صلیب سرخ حول محور این موضوع درگرفت، بسیاری از منتقدین و کارشناسان معتقد بودند که جدای از تاسیساتی که صد درصد نظامی هستند، یک‌سری تاسیسات مخابراتی، ارتباطات شهری، حمل و نقل و یا صنعتی اهمیت اساسی در پیشبرد جنگ دارند نیز نظامی قلمداد می شوند. آنها معتقد بودند که بطور کلی حتی اگر درصد پایینی از تولیدات کارخانه‌ای کوچک، سوخت مورد استفاده در عملیات نظامی را تامین نماید، اگر تولید سوخت موردنظر در حاشیه تولید محصول اصلی کارخانه باشد، آن کارخانه هدف نظامی مشروع تلقی می‌گردد.خطر داشتن چنین رویکردی بسیار واضح و مشهود است، چرا که کلیه زیرساخت‌های سایبری بین‌المللی شامل شبکه‌های رایانه‌ای، کابل‌ها و ماهواره‌های ارتباطی و... با مقاصد نظامی و غیرنظامی از آنها بهره‌برداری می شود(Jesen.E,2010:1534).

با این تعریف، یک کابل زیردریایی که منتقل کننده ارتباطات نظامی است، نظامی بوده و در نتیجه نه تنها می‌تواند هدف یک عملیات سایبری با هدف اختلال و از کارانداختن جریان انتقال اطلاعات باشد، بلکه می‌تواند هدف یک حمله سایبری به منظور ایراد صدمه در دنیای واقعی باشد، یا یک سرور کامپیوتر تنها با داشتن ۵ درصد اطلاعات نظامی، می تواند هدف مشروع نظامی باشد. همچنین حمله به شبکه بانکداری الکترونیک، شبکه برق، سیستم ارتباطی دارای کاربرد دوگانه یا از کارانداختن کابل‌های مخابراتی، تخریب گره‌های ارتباطی، مسیریاب‌ها و یا ماهواره‌هایی که سیستم‌ها به آنها متکی هستند، تنها به این دلیل که آنها دارای کاربرد انتقال اطلاعات نظامی نیز هستند، تقریبا همیشه قابل توجیه خواهد بود. حال با این فرض که بخشی از فضای اینترنت برای نیل به یک هدف نظامی بکار رود، چالش‌ها در خصوص این سوال که آیا کلیت فضای اینترنت یا بخش‌هایی از آن که مورد کاربری نظامی قرار گرفته اند، می تواند مورد حمله قرار بگیرد یا نه، بالا گرفته است. گرچه طبق بند دو ماده ۵۲ پرتکل الحاقی اول(Melzer,2011:135) از عملکرد ساقط نمودن و اختلال و حتی خنثی‌سازی آن مزیت نظامی برای طرف درگیری به همراه داشته و حمله به آن قابل توجیه است.

در این رابطه دستورالعمل تالین[۱] معتقد است که در حال حاضر، پیش آمدن شرایطی که در آن فضای اینترنت(در کلیت خود) مورد حمله قرار گیرد، بسیار بعید به نظر می‌رسد[۲].

موضوع بعدی که تاحدودی چالش‌زاست، انعطاف پذیر بودن فضای سایبری است. بطوری‌که اطلاعات نمی‌توانند تنها از طریق یک کانال منتقل شوند. بلکه ممکن است از طریق مسیرهای چندجانبه و جایگزین جابجا گردند. دستورالعمل تالین در این خصوص می گوید:

در این حوزه عملیات سایبری، با چالش‌های منحصر بفردی مواجه است. در روند بررسی یک شبکه ارتباطی با کاربرد دوگانه، دانستن اینکه کدام قسمت از اطلاعات از شبکه انتقالات نظامی متمایز از غیرنظامی عبور خواهد کرد، غیرممکن است و این وضعیت عملا اصل تفکیک را به عنوان زیربنای حقوق بشردوستانه به چالش خواهد کشید. در چنین شرایطی کل شبکه یا حداقل بخشی از آن که انتقال از طریق آن معقول به نظر برسد، به عنوان یک هدف نظامی تعبیر خواهد شد. پیامد این تفسیر چنین خواهد بود که عملا تمام بخش‌های اینترنت می‌توانند به عنوان یک هدف نظامی تلقی شوند، زیرا بطور بالقوه ممکن است مسیرهای انتقال اطلاعات نظامی باشند. این تفسیر موسع از اهداف با کاربرد دوگانه که آنها را بعنوان هدف نظامی تفسیر می کند، در دنیای واقعی می تواند بوجود آورنده مشکلات حادی گردد که در فضای سایبری این چالش‌ها دوچندان خواهد شد. با این تفسیر ممکن است وضعیت به نقطه ای برسد که هیچ هدف غیر نظامی باقی نمانده و اصل کلی حمایت و حفاظت کلی جمعیت غیرنظامی در مقابل خطرات ناشی از درگیری مسلحانه، به عنوان فلسفه وجودی حقوق بشردوستانه با سوالات جدی مواجه گردد.

در نهایت، اگر قرار باشد بیشتر زیرساخت‌های سایبری دارای کاربرد دوگانه دنیا "هدف نظامی" محسوب شوند، چنین تفسیری منجر به گسترده شدن محدوده جغرافیایی صحنه یک مخاصمه مسلحانه خواهد شد، زیرا هیچ حد و مرزی نمی توان برای یک جنگ سایبری قائل شد. سیستم‌های کامپیوتری می‌توانند از هر کجا مورد حمله و دستکاری قرار گرفته و مضافا سیستم‌های کامپیوتری

---

[۱]. کارشناسان مرکز سایبری سازمان پیمان آتلانتیک شمالی(ناتو) متشکل از افسران نظامی، حقوقدانان و کارشناسان سایبری، در سال ۲۰۱۳ در شهر تالین کشور استونی اقدام به جمع آوری و تدوین مجموعه ای جامع از مقررات و رهنمودهای حقوقی و تفاسیر موجود در موضوع جنگ های سایبری نموده اند که با وجود اینکه مصوب و بصورت معاهده درنیامده و تنها جنبه غیرالزام آور و ارشادی دارد، در عین حال مرجع مناسبی در رابطه با مواجهه پدیده عملیات سایبری با الزامات حقوق بین الملل می‌باشد.

[2]. Jonjic.Beitter, Andrea(2013),Tallin Manual Publishes on Cyber conflicts, two Comments, available on https://netzpolitik.org/2013/tallinn-manual-nato-veroffentlicht-handbuch-mit-cyberwar-regeln

مورد حمله قرار گرفته شده دست به اقدام تلافی‌جویانه[1] زنند. به عنوان مثال یک شبکه Botnet[2] ممکن است که بمنظور تخریب زیرساخت‌های سایبری دشمن بکارگرفته شوند. برای هدایت چنین عملیاتی، طرف درگیری شروع به حمله به هزاران، بلکه میلیون‌ها کامپیوتر در سراسر دنیا، از طریق کنترل از راه دور و انتقال بدافزارهای رایانه‌ای به کامپیوترهای هدف می کند. با چنین رویکردی، ما تمام آن هزاران و میلیون‌ها کامپیوتر در سراسر دنیا را مسئول حملات و در نتیجه آنها را به عنوان "هدف نظامی" قلمداد کنیم. با این تفسیر شاهد راه افتادن یک جنگ سایبری تمام عیار همگانی خواهیم بود. به علاوه نتیجه منطقی اینکه همه کامپیوترهای سراسر دنیا "هدف نظامی و مشروع" تلقی شوند، در تضاد کامل با اصول حقوقی موضوع"بی‌طرفی[3]" در مخاصمات مسلحانه خواهد بود. اصول مذکوربا بر اساس این منطق تدوین شده اند که کشور ثالث بی‌طرف در یک درگیری مسلحانه از تاثیرات آن مصون و جدا نگه داشته شود. در صورتی‌که با این تفسیر همه کامپیوترها، حتی شبکه رایانه‌ای کشورهای بی‌طرف، نیز از تاثیرات حمله سایبری مصون نخواهند بود. پیامد این رویکرد تغییر و توسعه صحنه نبرد و تبدیل آن به یک آوردگاه جهانی خواهد بود(Csosseck,2012:185).

## شرکت‌های تولیدکننده نرم‌افزار و سخت‌افزار فن‌آوری اطلاعات

از آنجا که نرم‌افزار و سخت‌افزارهای به کاربرده شده در تجهیزات نظامی توسط شرکت‌های حوزه فن‌آوری اطلاعات تولید می شوند، شرکت‌های مذکور تنها با این توجیه که اقدام به ارائه اقلام و زیرساخت‌های اطلاعاتی و مخابراتی به نظامیان می نمایند، می‌توانند به عنوان هدف نظامی در نظر گرفته شوند.این تفسیر درست مشابه تفسیری است که در قبال کارخانجات تولید تسلیحات و مهمات نظامی وجود دارد (Shane,2012:10).

اریک تالبوت ینسن در این مورد که با توجه به ارائه خدمات پشتیبانی و تسهیلات عملیات نظامی ارتش آمریکا که شرکت میکروسافت انجام می دهد، آیا شرکت مذکور می تواند هدف مشروع نظامی باشد؟ معتقد است: «با عنایت به این واقعیت که ارائه محصولات و خدمات شرکت میکروسافت برای ادامه عملیات نظامی ارتش آمریکا اساسی است، این مورد می‌تواند دلیل کافی برای نتیجه‌گیری ما در خصوص کاربرد دوگانه داشتن این شرکت و در نتیجه هدف نظامی تلقی

---

[1]. Counter Hack

[2]. شبکه هایی هستند که با در اختیار گرفتن مجموعه ای از کامپیوترها که Bot نامیده می شوند، تشکیل شده و توسط یک یا چند مهاجم (Botmasters) با هدف انجام عملیات مخرب سایبری کنترل می گردند.

[3]. neutrality

کردن آن باشد. در عین حال وی در رابطه با اینکه مزایای مشخص نظامی از این حمله بدست می‌آید، دچار تردید شده است » (Jesen,2010:125).

البته، نباید در رابطه با هم راستا قرار دادن شرکت‌های تولیدکننده نرم‌افزار و سخت‌افزارهای رایانه‌ای با کارخانجات تولید تسلیحات و مهمات نظامی زیاده‌روی نمود. معیار اصلی بند دو ماده ۵۲ پرتکل الحاقی اول این است که هدفی نظامی محسوب می شود که کمک موثری به عملیات نظامی ارائه دهد. ابهام موجود به تفاوت "ابزار[1]" و "تسلیحات[2]" در این حوزه مربوط است. تسلیحات بنا به ماهیتشان جزء اهداف نظامی محسوب می شوند(Kelsey,2014:87). در این عرصه باید بین کارخانجاتی که اقدام به طراحی, تولید و توسعه[3] آنچه در اصطلاح تسلیحات سایبری هستند مثل کدهای رایانه‌ای مشخص، ویروس‌ها و بدافزارهایی که جهت حمله به شبکه رایانه‌ای معینی طراحی می شوند و... با کارخانجاتی که اقدام به تولید و تامین سخت‌افزارهای کامپیوتری نیروهای مسلح می نمایند، تفاوت قائل گردید.

## مفهوم کمک موثر به عملیات نظامی چیست؟ کمک به ظرفیت‌های بالقوه و پایدار جنگی کشور یا توانمندی‌های کشور در جنگ فعلی

ملاحظه دیگر در رابطه با نحوه و آستانه کمک زیرساخت سایبری به عملیات نظامی است. یکی از شروط ماده ۵۲ برای تغییر وضعیت یک هدف غیرنظامی به نظامی، کمک موثر به پیش‌برد عملیات نظامی" است. در این عرصه تاسیسات به دو طریق می توانند "کمک موثر"ی به درگیری نظامی داشته باشند. برخی از تاسیسات از طریق تقویت ظرفیت‌های بالفعل جنگی باعث تغییر معادله جنگ شده و کفه ترازو رویارویی نظامی را به نفع کشور سنگین می‌کند. در مقابل برخی زیرساخت‌ها بطور کلی توسعه پایدار ظرفیت عمومی و بالقوه نظامی کشور، بدون در نظر گرفتن حالت جنگی که کشور در حال حاضر گریبان گیر آن است، کمک خواهد نمود. در جنگ سایبری نیز اگر یک هدف، صرفا به حفظ وتوسعه پایدار قابلیت‌های عمومی و بالقوه نظامی کشور مساعدت نماید، دیگر هدف نظامی نخواهد بود(Yenssen,2010:168).

---

1. Tools
2. Weapons
3. Develop

## شبکه‌های اجتماعی و رسانه‌ها

### امکان جهت‌گیری حملات به سوی شبکه‌های اجتماعی

دستورالعمل تالین در خصوص ابهامات حقوقی کاربرد روزافزون شبکه‌های اجتماعی با مقاصد نظامی به عنوان نمونه کاربرد فیس‌بوک جهت سازماندهی جنبش‌های مقاومت مسلحانه و یا کاربرد توییتر جهت انتقال اطلاعات با ارزش نظامی سه نکته هشداردهنده عنوان می نماید:

بعنوان ملاحظه اول چنانچه با استناد به قانون کلی "نظامی محسوب شدن اهداف دارای کاربرد نظامی و غیرنظامی" ما شبکه های اجتماعی را نظامی محسوب کنیم، چنین تفسیری بی‌توجهی محض به الزامات قواعد هدایت مخاصمات خواهد بود. در ثانی، هدف نظامی محسوب شدن شبکه‌های اجتماعی منوط به این است که کاربرد نظامی آن به سطح و آستانه یک حمله برسد، اگر به این حد نرسید، محاسبه آن به عنوان یک هدف نظامی جای بحث دارد. سوما این رویکرد بدین معنی نیست که ممکن است فیس‌بوک و توییتر مورد هدف قرار گیرند, تنها ممکن است بخش‌هایی با کاربرد نظامی، آن‌هم‌در تطبیق کامل با الزامات حقوق بین الملل، مورد حمله قرار بگیرند (Schmitt.M,2014:55).

در نظر گرفتن فیس‌بوک و توییتر به عنوان یک هدف نظامی می‌تواند چالش‌هایی را به‌دنبال داشته باشد. مهم‌ترین مشکل موجود عدم امکان تفکیک اطلاعات موجود در شبکه‌های اجتماعی اینچنینی است. در واقع چنین شبکه‌هایی حجم عظیمی از اطلاعات را شامل می شوند که نسبت به اطلاعاتی که مستحق حمله هستند، بطور کلی نامربوط هستند. لذا توصیف این‌گونه شبکه‌ها به عنوان یک هدف نظامی مشکل به نظر می رسد. در نهایت، سوال مهم این است که از نظر فنی، در بین آن همه اطلاعات پراکنده و سازمان‌نیافته در چنین شبکه‌هایی، آیا حمله تنها به آن بخش‌هایی که دارای کاربرد نظامی هستند، اساسا امکان‌پذیر خواهد بود؟

### گزارشات رسانه‌ای

در رابطه با امکان نظامی محسوب شدن موسسات رسانه ای تولید و مخابره کننده گزارش طبق دستورالعمل تالین، اگر گزارشی از طریق ارائه تصویر عملیات نظامی به نفع دشمن، به روند جنگ کمک موثر نموده و باعث محروم شدن یک طرف از مزیت‌های نظامی مشخص و فواید قطعی جنگ گردد، موسسه تولید کننده چنین گزارشی می‌تواند هدف نظامی باشد. حتی به زعم برخی زیرساخت‌های سایبری که انتقال و مخابره این گزارش‌ها را نیز حمایت می کند، در تطابق کامل با مقررات هدایت مخاصمات، هدف مشروع نظامی خواهد بود. البته عملیات سایبری پیشگیرانه باید با هدف بلاک کردن پخش گزارش‌های رسانه‌ای موردنظر باشد نه بیشتر(Schmitt.M, 2014:73).

پیامدهای پذیرش این تفسیر به عنوان مثال در رابطه با عملکرد یک شبکه رسانه‌ای بین المللی مثل بی‌بی‌سی بسیار خطرناک خواهد بود. حتی اگر یک گزارش خاص رسانه‌ای بتواند کمک موثری به عملیات نظامی کند، نتیجه چنین تفسیری نباید این باشد که هم شرکت رسانه‌ای و هم زیرساخت‌های مخابره‌کننده آن گزارش هدف قانونی حمله تلقی گردند. حتی اگر گزارش رسانه‌ای شامل یک‌سری اطلاعات تاکتیکی با اهداف خاص باشد، امکان هدف قرار گرفتن شرکت رسانه‌ای می تواند بسیار چالش‌برانگیز باشد. با این فرض، به غیر از شرکت رسانه‌ای مولد گزارش، تمام زیرساخت‌های سایبری(ماهواره، فیبر نوری و....) که گزارشات از آن طریق مخابره می شوند، هدف نظامی مشروع تلقی و در چنین شرایطی، قسمت اعظم زیرساخت‌های سایبری و ظرفیت‌های ارتباطی جهان می تواند تخریب و مورد صدمه قرار گیرد. این وضعیت محدودیت جغرافیایی صحنه نبرد را به صحنه جهانی توسعه و اصل بی‌طرفی را خدشه دار خواهد نمود(جعفری، افشین۱۳۹۷:۱۹۹). بر این نکته تاکید می‌گردد که ایجاد ارتباط بین عملکرد تاسیسات سایبری و "کمک موثر آن به پیشبرد عملیات نظامی"بعید و بار اثبات آن بسیار مشکل است، در نتیجه ارزیابی یک زیرساخت سایبری به عنوان هدف نظامی مشروع باید در شرایط مکانی و زمانی مخاصمه مسلحانه صورت پذیرد.

**۲) اصل ممنوعیت حملات کورکورانه و کاربرد ابزار و شیوه‌های جنگی بدون تفکیک**

حقوق بشردوستانه ممنوعیت حمله کورکورانه را مورد تاکیدقرار داده است. بر این اساس حملات بدون تفکیک حملاتی هستند که:

۱- به سوی یک هدف نظامی معین و مشخصی نشانه‌گیری نشوند.

۲- در آن از ابزارها و شیوه‌های جنگی استفاده شود که توانایی جهت‌گیری به سوی یک هدف مشخص را ندارند.

۳- ابزار و شیوه‌های جنگی بکار رفته در حمله وتاثیرات آنها نمی توانند الزامات حقوق بشردوستانه را برآورده کنند.

۴- حملاتی که ذاتا به شیوه بدون تفکیک به سوی افراد و اهداف نظامی و غیرنظامی جهت گیری می شوند[1].

[1]. 1st Additional protocol to Geneva Convensions,1977, article 51, Para 4

بر پایه اصل تفکیک کشورها هرگز نباید از سلاح‌هایی استفاده کنند که در ایجاد تمایز بین افراد و اهداف نظامی و غیرنظامی ناتوان است ( عسگری، هنکرتز، ۱۳۹۰: ۱۶۷).

در رابطه با فضای سایبر با توجه به قابلیت کاربرد دوگانه اهداف،تفکیک نظامی از غیرنظامی تا حدود زیادی دشوار است، حتی در شرایط قابل تمایز بودن، باز هم این خطر وجود دارد که به واسطه پیوند درونی و به هم‌پیوستگی فضای سایبر حملات کورکورانه و غیرمتمایز صورت پذیرد. فضای سایبری مشتمل بر سیستم‌های بی‌شمار رایانه‌ای است که دارای پیوندهای درون سیستمی در سراسر دنیا هستند. حتی اگر سیستم‌های رایانه‌ای نظامی از سیستم‌های غیرنظامی جدا باشند، در اغلب موارد با سیستم‌های تجاری و غیرنظامی پیوند درونی داشته، یا بصورت جزئی و کلی بر آنها متکی و یا از همدیگر تاثیر می پذیرند. لذا غیرممکن است که یک حمله سایبری به زیرساخت های نظامی صورت بگیرد و عواقب و تاثیرات آن فقط به آن هدف مورد حمله محدود بماند. ویروس‌ها، کرم‌ها و در کل بدافزارهای رایانه‌ای نمونه‌هایی از روش‌های حمله به شبکه‌های رایانه‌ای هستند. چنان‌چه تاثیرات آنها توسط طراحان و بوجودآورندگان آنها محدود نشود، کاربرد کرم‌ها و ویروس‌هایی که قابلیت تکثیر خود را داشته و غیرقابل کنترل هستند و در نتیجه باعث ایراد صدمات قابل توجه به زیرساختهای شهری خواهد شد (Kelsey, 2007:8).

حملات سایبری در صورتی موفقیت‌آمیز خواهند بود که هدفمند عمل کرده و تاثیرات مخرب آن به سایر سیستم‌ها تسری پیدا نکند. در واقع اگر یک ویروس کامپیوتری جهت حمله به یک سیستم رایانه‌ای معین (هدف نظامی مشخص و بسته) و جلوگیری از انتشار آن به سایر سیستم‌ها طراحی و ایجاد شود، دیگر ریسکی برای تاسیسات غیرنظامی خارج از آن حوزه وجود نخواهد داشت.ب ا این وجود، کاملا قابل‌تصور است که طرف مخاصمه این‌گونه اقدامات احتیاطی را اتخاذ نکرده و سلاح‌های سایبری خود را به‌نحوی طراحی نموده و توسعه دهد که تاثیرات غیرقابل پیش بینی بر سایر شبکه‌ها داشته باشد. وجود این واقعیت به این معنی نیست که هیچ پتانسیل بالایی برای ایجاد تفکیک در حملات وجود ندارد. طبق گزارشات رسانه‌ای، حتی ویروس استاکس نت فقط به سوی تاسیسات هسته ای ایران جهت‌گیری و با هدف جلوگیری از انتشار تاثیرات مخرب آن برکامپیوترهای خارج حوزه طراحی شده بود. ولی بر خلاف انتظارات، به نحوی اقدام به تکثیر خود خارج از شبکه رایانه‌ای هدف نمود (اصلانی، ۱۳۹۳: ۱۸۶). می توان گفت طرفین درگیر در یک جنگ سایبری، دو تعهد بشردوستانه دارند:

- ممنوعیت طراحی، توسعه، دستیابی و کاربرد سلاح‌های سایبری که ذاتا بدون تفکیک عمل می کنند، مثل ویروس‌ها و کرم‌هایی که بدون امکان کنترل توانایی تکثیر و انتشار به سایر سیستم‌های رایانه‌ای را دارند.
- سلاح سایبری اولا به سوی یک هدف نظامی جهت‌گیری شده باشد و در ثانی تاثیرات جانبی و تصادفی حمله بر افراد و اهداف غیرنظامی قابل کنترل و راستی‌آزمایی باشد(خلف رضایی،۱۳۹۲:۷۸).

**۳) اصل تناسب**

پرتکل اول الحاقی بصورت قاعده‌مندی به این اصل پرداخته که در حقوق بین‌الملل عرفی انعکاس داشته است. طبق این اصل:

"درانجام یک حمله, چنان‌چه انتظار رود, ایراد صدمات و آسیب‌های جانبی احتمالی بر زندگی غیرنظامیان در مقایسه با مزیت نظامی پیش‌بینی شده بیشتر باشد، انجام آن حمله ممنوع است[1]".

در اینجا منظور از صدمه لزوما صدمه فیزیکی نیست. صدمه به اهداف به معنی" ایراد آسیب و ایجاد نقص در عملکرد هدف و ناکارآمد و غیرموثر ساختن آن است. با این تعریف روشن است که صدمه مورد نظراین ماده نه تنها شامل صدمه فیزیکی می شود، بلکه اختلال در عملکرد هدف را نیز شامل می شود (Hathaway,2012:817).

دو ویژگی ذاتی یعنی کاربرد دوگانه داشتن اکثر زیرساخت‌ها و پیوندهای درون‌سیستمی فضای سایبری باعث می شود که همواره ریسک سرایت پیامدهای خطرناک حمله به زیرساخت‌های غیرنظامی را افزایش می‌دهد. دراین عرصه نیز مثل جنگ‌های کلاسیک، ممکن است تاثیرات احتمالی و جانبی حمله به یک زیرساخت سایبری نظامی بر سایر تاسیسات غیر نظامی تاثیر و به عنوان مثال باعث قطعی آنها گردد.اولین مشکل این بخش نحوه تفسیر و اندازه‌گیری "صدمه جانبی و احتمالی یک حمله بیشتر از مزیت پیش بینی شده" است. معیار این محاسبه چیست؟این ابهام بیشتر کمی است تا کیفی، بدین معنی که به دلیل پیوندهای درون‌سیستمی شبکه‌های رایانه‌ای، در بیشتر موارد باید ایراد صدمات جانبی را انتظار داشت، اما میزان آن را به سختی می توان ارزیابی نمود(Oconell,2012:78).

[1]. 1st Additional Protocol to Geneva Conventions, 1977, Article 51,Sec 5, Para 2.

**۴) اصل لزوم اتخاذ اقدامات احتیاطی**

حقوق بشردوستانه، الزامات ناشی از تعهد اتخاذ اقدامات احتیاطی مناسب با هدف مصون ماندن افراد و اهداف غیرنظامی از تاثیرات سوء یک حمله نظامی را هم برای کشور حمله‌کننده و هم برای کشور مورد حمله واقع شده بار می کند.

**لزوم رعایت اصل احتیاط در حملات**

اصل کلی در حقوق بشردوستانه این است که در هدایت عملیات نظامی، طرفین درگیری باید مراقبت های لازم برای مصون ماندن جمعیت و افراد غیرنظامی را صورت دهند. اقداماتی مثل:

- اقدامات عملی برای اطمینان از اینکه هدف مورد نظر یک " هدف نظامی و مشروع" است.
- اقدامات عملی در انتخاب ابزار و شیوه‌های جنگی جهت اجتناب از تاثیرات حمله به افراد و اهداف غیرنظامی و به حداقل رساندن تلفات

طبق این اصل، کشور حمله‌کننده متعهد است در صورتی که روشن گردید که حمله مورد نظر باعث تلفات و صدمات جانبی بیش از حدخواهد شد، آن حمله را متوقف یا معلق سازد.در این راستا طرفین درگیری متعهد به جمع‌آوری اطلاعات برای حصول اطمینان از نظامی بودن هدف و تاثیرات جانبی و بالقوه حمله می باشند.در عرصه سایبری احتیاط‌ها می تواند شامل نقشه‌برداری سیستم کامپیوتری دشمن باشد. در صورتی که اطلاعات در دسترس کامل نباشد، با توجه به ارتباطات سیستماتیک شبکه‌های رایانه‌ای، بهتر است حمله تعلیق یا صرفا به اهدافی محدود شود که در خصوص آنها اطلاعات کافی بدست آمده باشد. نتیجه این که در مقایسه با سایر اصول هدایت مخاصمات در حملات سایبری، اعمال اصل احتیاط به تخصص فنی خاصی نیاز دارد،کارشناسان ناتو در دستورالعمل تالین با تایید این مطلب عنوان کرده‌اند:

"با توجه به پیچیدگی عملیات سایبری و احتمال بالای تاثیرات آن بر تاسیسات غیرنظامی ضروری‌است که طراح یک حمله سایبری به منظور ارزیابی دقیق ماهیت هدف و اتخاذ اقدامات احتیاطی مناسب بهره‌گیری از مشاوره متخصصین فنی حوزه سایبری را در دستور کار خود قرار دهد. البته وقتی عملیات سایبری در مقام دفاع از پیش برنامه‌ریزی شده در مقابل نفوذ سیستم رایانه خارج و بطور اتوماتیک طراحی شده (هک متقابل[1]) باشد، تعهد موردنظر پیشاپیش برآورده شده است."(Schmitte,2014:128)

[1]. Reciprocal hacking

به هر حال، با فرض این‌که حملات سایبری از میلیون‌ها کامپیوتر نشات گرفته باشد، در پرتو اصل احتیاط، کشورها نسبت به دقت حداکثری در خصوص قانونی بودن عملیات هک متقابل متعهدند.در برخی موارد رعایت اصل احتیاط مستلزم بکارگیری و توسل به سایر ابعاد تکنولوژی‌های در دسترس در فضای سایبراست. در واقع، تکنولوژی سایبری هم می تواند در قامت یک مشکل باعث ایراد تلفات و صدمات به افراد و اهداف غیرنظامی ظاهر شود و هم این قابلیت را دارد که به عنوان راه‌حلی برای اتخاذ اقدامات احتیاطی مطرح گردد.(Queguiner, 2006.801).

**اتخاذ اقدامات احتیاطی توسط کشور قربانی حمله**

کشور قربانی حمله نیز باید حداکثر اقدامات عملی برای حفاظت از افراد و اهداف غیرنظامی تحت حاکمیت خود در مقابل عواقب فاجعه بار آن را بکار ببندد. در این راستا حتی‌الامکان آنها را از مجاورت اهداف نظامی دور ساخته و احتیاط‌های ضروری برای حمایت ایشان را بکار گیرد[1]. این مطلب در دستورالعمل تالین بدین شرح آمده است:

اتخاذ اقدامات احتیاطی مناسب در دنیای سایبری می‌تواند شامل تفکیک تاسیسات سایبری نظامی از غیرنظامی، تفکیک سیستم‌های یارانه‌ای که زیرساخت‌های نظامی مهم بر آن متکی هستند از زیرساخت‌ها و سیستم‌هایی که اینترنت و سایر خدمات رایانه‌ای شهروندی بر آن متکی هستند، تهیه نسخه پشتیبان از داده‌های مهم شهروندان، ایجاد ترتیبات پیشرفته برای اطمینان از اینکه در سازوکار هک متقابل در مقابل حملات قابل پیش بینی به سیستم های کامپیوتری مهم تعهدات حقوق بشردوستانه رعایت خواهد شد، ثبت دیجیتالی اهداف سایبری مهم از جمله اهداف فرهنگی جهت تسهیل بازسازی آنها در مواقع صدمه، کاربرد اقدامات ضد ویروس برای حفاظت از سیستم های یارانه ای و....باشد (Segal,2011:3).در تئوری ممکن است اجرای تعهد مذکور عملی باشد، اما در دنیای واقع اجرای دقیق آن طبق مندرجات ماده ۵۸ بسیار پرهزینه و در نتیجه غیرعملی خواهد بود. در این راستا کشورها ملزم خواهند بود اقدام به طراحی و ساخت نرم افزار و سخت افزارهای مجزا برای کاربرد نظامی کرده و بعلاوه خطوط ارتباطی مثل کابل‌های فیبر نوری، مسیریاب‌ها، ماهواره‌ها و... جداگانه‌ای برای انتقال اطلاعات نظامی داشته باشند. پرتکل الحاقی اول با درک صحیح از مشکلات جداسازی، کشورها را ملزم می‌کند حداقل برای تضمین ادامه عملکرد

[1]. Queguiner, G. ( 2006). Precautions Under the Low governing the conduct of Hostilities, international Rewie of the Red Cross , Vol 88.No 864

برخی از زیرساخت‌های غیرنظامی حیاتی و حساس مثل نیروگاه‌های اتمی، کارخانجات مواد شیمیایی، بیمارستان‌ها و...اقدامات عملی بکار گیرند[۱].

اریک تالبوت ینسن، بمنظور اجرای تعهد مذکور به دولت آمریکا اقداماتی را توصیه می کند[۲]:

۱- نقشه‌برداری سیستم‌های رایانه‌ای شهروندی که بصورت بالقوه قابلیت این را دارند که هدف نظامی تفسیر شوند.

۲- اطمینان از حفاظت شبکه رایانه‌های شخصی و تاسیسات غیر نظامی

۳- طراحی، توسعه و حفظ راه حل‌های هک متقابل

۴- ایجاد سازوکار حافظه استراتژیک با قابلیت ذخیره حجم عظیم اطلاعات و قابلیت‌های اینترنت (Jensen,2010:88-9).

با وجود ارزیابی مثبت روند گرایش کشورها به اجرای الزامات فوق، بعید به نظر می‌رسد که کشورها در خصوص لزوم اتخاذ اقدامات احتیاطی منفعلانه بدین سادگی به درک مشترک رسیده و اقناع شوند.

## نتیجه‌گیری

نظامی شدن فضای سایبری چالش‌های مهمی در اعمال قواعد حقوق بشردوستانه و نظارت حقوقی بر فضای مذکور را باعث گردیده است. واقعیت این است که تدوین ترتیبات قراردادای حقوق بشردوستانه بین‌المللی، در فضای بروز درگیری‌های مسلحانه کلاسیک در صحنه واقعی شکل گرفته است. با گذر زمان، ابزار و شیوه‌های جنگی مورد نظر کنوانسیون‌های چهارگانه ۱۹۴۹ و پرتکل‌های الحاقی ۱۹۷۷ بر اثر پیشرفت‌های صورت گرفته در صنایع تسلیحاتی و فن‌آوری اطلاعات توسعه یافت که پیدایش پدیده عملیات سایبری، ارمغان مهم این تحول است. به موازات بروز تحولات مذکور، سردرگمی‌ها در حوزه پایبندی کشورها به الزامات ناشی از اعمال مقررات هدایت مخاصمات درفضای سایبر که ریشه در ویژگی‌های ذاتی فضای سایبری از جمله غیرقابل‌شناسایی بودن عامل حمله سایبری، قابلیت کاربرد دوگانه زیرساخت‌های سایبری و ارتباطات درون‌سیستمی شبکه‌های رایانه‌ای دنیا دارد، پدیدار گشت.

با توجه به ریسک سرایت عواقب جنگ‌های سایبری به زیرساخت‌های غیرنظامی، کارشناسان در حال بررسی و ارائه راه حل‌های پیشنهادی متعددی می باشند.

---

[1]. 1st Additional Protocol to Geneva Conventions 1949, 1977, Art. 58, Para 3.

[2]. S Department of Defence Strategy for Operating in Syber Space, July 2011, Available at http//defence.gov/news/d20110714 cyber. Pdf

اولین راهکار ایجاد"پناهگاه‌های امن دیجیتالی[۱]"برای زیرساخت‌های غیرنظامی با هدف غیرنظامی سازی فضای سایبر، مورد نظر ماده ۶۰ پرتکل الحاقی اول است. این بهشت مجازی نسبت به هر گونه عملیات سایبری مصون خواهد بود. گرچه تحقق این امر نیاز به گفتگو و اقدامات اعتمادساز بین کشورها دارد، امابه نظر نمی رسد ایجاد اجماع نسبی بین کشورها در برخی حوزه‌ها مثل بیمارستان‌ها و اطلاعات پزشکی، سیستم‌های مالی و بانکی، شبکه‌های نیرو و زیرساخت‌های اینترنتی چندان مشکل باشد[۲].

راهکار دوم گسترش دامنه اطلاق ماده ۵۶ پرتکل الحاقی اول[۳] و گسترش فهرست"تاسیسات حاوی مواد خطرناک" مندرج در ماده مذکور از طریق مقایسه تطبیقی زیرساخت‌ها است. به نظر می‌رسد بخش‌های معینی از تاسیسات سایبری مثل گره‌های اصلی ارتباطات اینترنتی، سرورهای اصلی که عملکرد میلیون‌ها زیرساخت غیرنظامی مهم مثل نیروگاه‌های تولید برق، سدها، سیستم‌های حمل و نقل ریلی هوایی و جاده ای و.... بدان وابسته است، را می توان به فهرست فوق افزود.

علاوه بر آن راه‌حل، توسعه ترتیبات قراردادی حقوق بشردوستانه و تدوین معاهدات جدید در تطبیق با مقتضیات خاص فضای سایبری نیز می تواند مورد اهتمام محافل حقوقی و فنی فضای سایبر باشد، حتی برخی تدوین نوعی معاهده خلع سلاح متضمن ممنوعیت کلی کشورها در طراحی، توسعه و بکارگیری تسلیحات سایبری را ضروری می دانند.

تردیدی وجود ندارد که مقررات حقوق بشردوستانه در جنگ سایبری قابل اعمال است، اما این که تا چه میزان در حفاظت جمعیت و اهداف غیر نظامی موفق عمل می‌کند، به این مهم بستگی دارد که چگونه تفسیر شود و در چه سطحی مورد احترام و پایبندی[۴] کشورها قرار گیرد.

## منابع و مآخذ

### کتاب‌ها

۱. جعفری، افشین (۱۳۹۷)، **تحدید حملات سایبری در چارچوب قواعد حقوق بین الملل بشردوستانه**، چاپ اول، تهران، انتشارات مجد

---

1. Digital Safe Haven
2. James Andrew Lewis, confidence- Building agreement in cybersecurity, Available at: http//www.unidir.org/Pdf-art3168pdf(Jr, Spring 2011)
۳. طبق این ماده در یک مخاصمه مسلحانه، حمله به مرکز حساسی مثل مراکز نگهداری مواد خطرناک، نیروگاههای هسته‌ای، مراکز نگهداری مواد شیمیایی و ... ممنوع می باشد.
4. Compliance

۲. راجرز، آنتونی و مالر، پل (۱۳۹۲)، ***قواعد کاربردی حقوق مخاصمات مسلحانه***، ترجمه کمیته ملی حقوق بشردوستانه، تهران ، موسسه انتشارات امیر کبیر.

۳. رضاییان، مهرداد(۱۳۸۳)، ***حقوق بین الملل ناظر بر هدایت مخاصمات (مجموعه کنوانسیونهای لاهه و برخی اسناد بین المللی دیگر)***، تهران، انتشارات سرسم.

۴. فلک، دیتر(۱۳۹۲)، ***حقوق بشر دوستانه در مخاصمات مسلحانه***، ترجمه: آقایان دکتر قاسم زمانی و نادر ساعد، تهران، انتشارات شهردانش.

۵. ضیایی بیگدلی، محمد رضا( ۱۳۸۶)، ***حقوق بین الملل بشر دوستانه***،تهران، موسسه انتشاراتی گنج دانش.

۶. عسگری، پوریا و هنکرتز، ژان ماری (۱۳۹۰)، ***مجموعه مقالات همایش حقوق بین المللی بشردوستانه عرفی، تهرا***ن، مجمع علمی و فرهنگی مجد

**مقالات**

۷. اصلانی، ج ( ۱۳۹۳)"حملات سایبری از منظر حقوق بین الملل، با نگاهی به قضیه استاکسنت و ایران"، ***فصلنامه مطالعات بین الملل***، *شماره ۱۰. صص۴۵- ۷۱*

۸. جعفری، افشین، توتونچیان، مهری، "بررسی راه‌کارهای تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه"، **مجلهاخلاق زیستی( ویژه نامه حقوق شهروندی)**، بهار ۱۳۹۸، صص ۳۳۲ - ۳۴۲

۹. خلف رضایی، حسین(۱۳۹۲)، "حملات سایبری از منظر حقوق بین الملل(مطالعه موردی:استاکس نت)"،**فصلنامه مجلس و راهبرد**، سال بیستم،شماره ۱۷۳ صص،۱۲۵-۱۵۳

10. beck, J. (2005**).** ***Customery international Humanitarian Law***.ICRC and Cambridge University Press , Voll 6.
11. C.Csosseck. (2012),**"Attack"as a term of Art in international Low: the Syber Operation Context,**4th international conference on cyber conflict. NATO CCD COE Publication,Tallinn
12. Kelsey, J. (2007-2008). ***Hacking in to international Humanitarian Law:the principles of Distinction,and Neutrality in the age of Syber Warfare***. Michigan Law Review , Vol 106 .
13. Haslam, E. (2000). ***Information warfare,Technologocal Changes and international law. Conflict and Security law*** , Vol 5. No 2.
14. Hathaway, O, (2012),*the Law of Syber attack,*california Law Review,Vol.100 No 4.
15. Lobel,Hanna(2012), **Cyber War INC: The Law of War Implications of The Private Sectors Role in Cyber Conflict**,Texas International Law Journal,Vol47,Issue 3,pp 617-640
16. Michael.N.Schmitt, (2011). ***Syber operations and"Jus in Bello": Key Issues***. Naval War Collegue international low Studies , Vol.87 p 91.

17. Pejic, e. (2006). ***International Law and Armed Conflict: Exploring the Faultlines***. Geneva: ICRC.Vol 15
18. Queguiner, G. ( 2006). ***Precautions Under the Low governing the conduct of Hostilities*, international Rewie of the Red Cross**, Vol 88.No 864.
19. Schmitt, M. (2002), ***Wired Warfare, Computer Network Attacks and Jus in Bello*. international Review of the Red Cross**, *Vol 84,No 846*.
20. Jensen, E. (2010),***Cyber Warfare And Precautions against the Effect of attacks***,*Texas Law Review* , Vol 88 .

**اسناد، مقالات، آراء و....:**

21. **Annual Review ICRC, (2017),** ***Weapons contamination***. Geneva: International Comittee Of Red Crossand Red Crescent .
22. Departmentof the Navy,Department of Homeland security,USA. (July 2007). **The commanders Handbookon the Law of Naval operations**.
23. ICRC annual Review, (2017). ***Humanity in Action, Protecting the Valenerable and Promoting the Law***. Geneva: internatinal comittee of Red cross.
24. 31st International Conference of the Red Cross and Red Crescent (2011),***Report on international Humanitarian Law and the Challenges of contemporary Armed Conflicts***, Geneva: ICRC,**Yearbook of International Law Commission**. (2001),*draft articles on the Responsibilityof States for international Wrongful Acts*., Vol. 2.
25. **Journal of International Law of Peac and armed Conflict**, (2014), *Cyber warfare and international Humanitarian Law: a Matter of applicability*, German Red cross, volume 27, , PP 196-175
26. Camlus,(May 2016),"*cyber attacks and internatinal law of Armad conflicts: a Jus Ad Bellum Prespective"*, **Journal of internatinal Commercial Law and Technology** , pp 179-189.
27. Dinniss, H. H (2012).*"Syber Warefare and the Law of War".**Cambridge Univercity Press***,
28. Dinstein, Y. (2004).*"Cyber-Attacks and International Law"***,cambridge university press , 48.**
29. Dinstein, Y. (2017). "***War aggression and Self- defens****e"*,6th Edition. Geneva.
30. Mark. R. Shulman, (1999).*"Discrimination in the law of information Warfare"*. **Columbia Journal of Transnatinal Law**, Vol 37.
31. Melzer, N, (2011),"*Syber Warefar and international Law"*. **UNIDIR Resourses Paper .**
32. Oconell, E. ( 2012).*"Cyber mania,in Syber Security and international Low"*. Meeting Summery in chatham House.
33. Schmitt, M. N, (2014).*"Tallinn Manual on the International Law Applicable to Cyber Warfare,*Geneva",***Cambridge University Press** *978*
34. schmitt, M. N. (2013). "Tallinn manual on the international law applicable to syber warfare".***Cambridge Univercity press***.
35. Schmitt, M. N. (1999),*"the Principle of Discrimination in 21th century Warfare"*. **Yale Human rights and Developmen**t.Vol 2.

36. Schmitt, M,(2017). "*Tallin Mannual on the international law applicable to cyber operations"* , Geneva: the Group of Experts in NATo.
37. Schmitt, w. H. (2015). "*the conduct of Hostilities in international Humanitarian Law.*Geneva: the Group of Experts in NATO".
38. Segal, A.(2011),"*Cyber Space Governance:the next step"*,Council of foreign Relations, **Policy innovation Memorandom** .
39. Shane, S, (2012, 26Septamber). "*Cyber warfare emerges from Shadows of public discussion by Us officials"*. **the New York times**.
40. thurer, D. (2014). "*Internatinal Humanitarian Law,Theory,practice,context"*. Hague:**The Journal Published by Hague Academi of international law**.
41. US Department of Defense. (2011). Dictionary of Military and Associated, Washington,Dc
42. Walker,b, (2011),*"Confidence- building and international agreement in sybersecurity*. *Transparency and confidence- building in syber space,towared norms of behaviour*". (p. issue 4). **UNIDIR Disarmamant forum**