فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱
وبگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN:2821-126X

Challenges of Applying the Principles of Armed Conflict to Cyber Attacks Case Study: Observance of the Principle of Prohibition of the Use of Force and the Principle of Distinction in Cyber Attacks

Zohre Sadeghi

Graduate of Master's Degree Program of International Law
University of Tehran, Farabi College

Mohammad Javad Arabian

PhD in International Law, Cyber International Law Researcher
Zohre.sadeghi@ut.ac.ir

DOI: 10.30495/CYBERLAW.2022.693933

Keywords:
Cyber Attacks, International Law, Law of Armed Conflict, Principle of Prohibition of the Use of Force, Principle of Distinction

Abstract

Due to the many advantages of cyber attacks as a new method of warfare compared to the conventional and traditional methods of war, the attention of different countries has been drawn to this phenomenon over the recent years. Furthermore, noting the point that the efforts of some countries and international assemblies to systematize the tools, methods and effects of this style of attack and conflict still face a lack of consensus and, as a consequence, have not resulted in creation of an international document, the international lawyers have faced many challenges in dealing with this phenomenon and its destructive effects on the important and vital infrastructure of countries and defending the rights of nations against cyber attacks.There are now many legal rules governing the situations in which states can resort to force as well as the point as how they can resort to force in armed conflicts. Some of these rules do not apply specifically to cyber attacks including the rules related to the protection of the Wounded, Sick and Shipwrecked. Other rules include general principles that apply to cyberattacks. Nevertheless, it seems that the gap between conventional weapons such as biological and chemical weapons and methods of cyber-attack can be very large. This article addresses the Principle of Prohibition of the Use of Force and the Principle of Distinction and examines the challenges of applying the same to the cyber attacks.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

چالش‌های کاربرد حقوق بین‌الملل بشردوستانه در جنگهای سایبریچالش‌های تطبیق اصول حاکم بر مخاصمات مسلحانه بر حملات سایبری بررسی موردی: رعایت اصل ممنوعیت توسل به زور و اصل تفکیک در حملات سایبری

زهره صادقی*

دانش‌آموخته کارشناسی ارشد حقوق بین‌الملل پردیس فارابی، دانشگاه تهران، تهران، ایران

محمد جواد عربیان

دکتری حقوق بین الملل، پژوهشگر حقوق بین الملل سایبری

Zohre.sadeghi@ut.ac.ir

تاریخ دریافت : ۰۹ خرداد ۱۴۰۱ تاریخ پذیرش: ۲۵ مرداد ۱۴۰۱

چکیده

نظر به مزایای حمله سایبری، به‌عنوان یک روش نوین جنگی در مقایسه با روش‌های متعارف و سنتی؛ توجه کشورهای مختلف در سال‌های اخیر به این پدیده جلب شده و ازآنجاکه تلاش‌های برخی کشورها و مجامع بین‌المللی برای نظام‌مندسازی ابزارها، شیوه‌ها و اثرات این سبک حمله و مخاصمه هنوز با عنایت به عدم اجماع و وفاق جامعه جهانی، منتهی به یک سند بین‌المللی نشده است؛ حقوقدانان بین‌المللی را در مواجهه با این پدیده و آثار مخرب آن بر زیرساخت‌های مهم و حیاتی کشورها و دفاع از حقوق ملت‌ها در مقابل حملات سایبری با مشکلات عدیده‌ای مواجه ساخته است. در حال حاضر قواعد حقوقی فراوانی بر وضعیت‌هایی که دولت‌هامی‌توانند متوسل به‌زور شوند[1]و چگونگی توسل به‌زور توسط آنها در مخاصمات مسلحانه[2]، حاکم است. برخی از این قواعد، قابل تطبیق بر حملات سایبری به طور خاص نیست؛ همانند قواعد مرتبط با حمایت از مجروحان، بیماران و غریقان. دیگر قواعد مشتمل بر اصول کلی است که حملات سایبری را هم در برمی‌گیرد؛ اصولی همانند ممنوعیت توسل به‌زور، تفکیک، ضرورت نظامی، تناسب و... . بااین‌وجود، به نظر می‌رسد فاصله‌ی بین سلاح‌های متعارف نظیر سلاح‌های بیولوژیکی و شیمیایی و روش‌های انجام حملات سایبری می‌تواند بسیار زیاد باشد. این نوشته نگاهی کلی به دو اصل ممنوعیت توسل به‌زور و اصل تفکیک داشته و دشواری تطبیق آن‌ها بر حملات سایبری را مورد بررسی قرار می‌دهد.

کلید واژگان: حملات سایبری، حقوق بین‌الملل، حقوق مخاصمات مسلحانه، اصل تفکیک، اصل ممنوعیت توسل به‌زور

[1]. the jus ad bellum.
[2] .the jus in bello.

مقدمه

حملات سایبری در معنای خاص خود نیز حتی اعم از جنگ سایبری است؛ درواقع یک رابطه عام و خاص مطلق بین آنها وجود دارد که حملات سایبری عام و جنگ سایبری نوعی خاص از آن است. کمیته دائمی پدافند غیرعامل کشور در سند راهبردی پدافند سایبری کشور جنگ سایبری را این‌گونه تعریف نموده است: بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یاگروه‌های سازماندهی شده تحت حمایت دولت‌های متخاصم علیه منافع ملی کشورها انجام می‌شود جنگ سایبری است.

حملات سایبری شیوه‌ای مدرن از جنگ است که شدیداً استعداد ایجاد تغییرات بنیادین در روابط بین‌المللی را دارد. قابلیت های فناورانه رایانه ای و اینترنت در شکل دهی حملات سایبری امروزه تا بدانجا پیش رفته است که توانایی واردکردن جراحت، کشتن و ایجاد خسارت‌های فیزیکی از طریق فضای مجازی را دارد. دامنه ی حملات سایبری می‌تواند از خشونت‌های شبکه‌ای بی‌ضرر تا حملات شدید به زیر ساختارهای ملی و حتی ترور افراد و کشتار دسته جمعی در نوسان باشد. درحالی‌که ازکارانداختن موقت سایت‌های اینترنتی یک دولت شاید آسیب چندانی به آن دولت وارد نکند، اما تهدید ارائه ی اطلاعات نادرست به فرماندهان نظامی در صحنه ی جنگ‌های فیزیکی، یا یک تهاجم سنگین به شبکه‌های تأمین برق، آبرسانی، ارتباطی و ترافیکی یک دولت می‌تواند خطراتی جدی برای سربازان و شهروندان دولت مزبور به بار آورد. نفوذ به شبکه‌های اطلاعاتی دولت‌ها و دست‌اندازی به اطلاعات طبقه‌بندی‌شده ی آن‌ها که در اصطلاح با عنوان جاسوسی رایانه‌ای خوانده می‌شود نیز بخشی از گستره ی جنگ سایبری به شمار می‌رود. این اعمال امروزه به دلیل وابستگی روزافزون آژانس‌های دولتی به ارتباطات الکترونیکی به‌مراتب ساده‌تر شده است.

در کنار کم کاری یا ناکارآمدی خاص سازمان ملل از جمله کمیسیون حقوق بین الملل و نیز کمیته بین المللی صلیب سرخ، اگرچه بخش قابل‌توجهی از قواعد توسل به‌زور اختصاص به اقدامات دولت‌ها در توسل به زور نظامی دارد، قابلیت اعمال این بخش به فضای مجازی نیز در هاله‌ای از ابهام قرار دارد و سؤالات بسیاری را پدیدار نموده است؛ از جمله این سؤال اساسی که بر اساس چه قواعدی از حقوق بین‌الملل می‌توان نبرد سایبری را بررسی و تحلیل حقوقی نمود. این نوشته نگاهی کوتاه به چالش‌های تطبیق قواعد حقوق مخاصمات مسلحانه بر این‌گونه نوین از جنگ می‌پردازد و به طور خاص بر دو اصل ممنوعیت توسل به‌زور و اصل تفکیک در حملات سایبری اشاره دارد.

۱. اصل ممنوعیت توسل به‌زور

مطابق بند ۴ ماده ۲ منشور، «کلیه اعضا، در روابط بین‌المللی خود از تهدید به‌زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی دولت‌های دیگر یا هر روش دیگری که مغایر با اهداف ملل متحد باشد خودداری خواهند نمود». این ممنوعیت اگرچه انحصاراً بر اعضای ملل متحد اِعمال می‌شود، ولی ممنوعیت ذی‌ربط از رهگذر حقوق بین‌الملل عرفی به کشورهای غیرعضو نیز تسری می‌یابد.

توجه به این نکته مهم است که ممنوعیت مقرره منشور ملل متحد، در مواردی که شورای امنیت سازمان ملل متحد مجوز لازم را داده باشد یا وقتی در راستای اعمال حق ذاتی دفاع مشروع در پاسخ به یک حمله‌ی مسلحانه، توسل به‌زور صورت بگیرد را شامل نمی‌شود(منشور ملل متحد ماده ۲(۴) و مواد ۴۲ و۵۱).

تدوین‌کنندگان منشور ملل متحد باهدف تقویت و تحکیم بیشتر مبانی صلح و امنیت بین‌المللی درجهان به هنگام بحث‌وبررسی ممنوعیت زور و جنگ در روابط بین‌الملل به این نتیجه رسیدند که تهدید توسل به‌زور نیز همانند خود توسل به‌زور می‌تواند پایه‌های صلح و امنیت بین‌المللی را به مخاطره اندازد و ازاین‌رو بود که ممنوعیت تهدید به توسل به‌زور در بند ۴ ماده ۲ منشور مقرر گردید. مسئله این است که آیا حملات سایبری می‌تواند در قلمرو موضوعی این مقرره قرار گیرد؟ اگرچه معنای متداول و متبادر از واژه «زور»آن‌چنان گسترده است که اجبار نظامی و غیرنظامی را نیزدر برمی‌گیرد، اما به نظر بیشتر حقوق‌دانان این مقرره ناظر به زور نظامی و مسلحانه است.

به لحاظ تاریخی دولت‌ها «زور» را در ارتباط با آن سلاحی که استفاده می‌شود تعریف کرده‌اند، یعنی «زور مسلحانه» است که ممنوع شده است نه اَشکال سیاسی و اقتصادی اعمال فشار و زور(Haslam,2000:53). اگرچه بی‌تردید این تفکیک در هر اقدامی که برای جلوگیری از اعمالی که به نظر می‌رسد در تناقض و تعارض با اهداف ملل متحد یعنی حفظ صلح و امنیت بین‌المللی باشد، انعکاس پیدا می‌کند.

امروزه با توجه به تمایل استفاده از شیوه‌های مدرن از جمله حملات سایبری بین دولت‌ها لزوم بررسی این مسئله ضروری است و در این راستا باید گفت در تطبیق ممنوعیت توسل به‌زور با حملات سایبری با مشکلات جدی مواجه خواهیم بود. از جمله مهاجمین، ابزارها، روش‌ها و شیوه‌های حمله، سطوح حمله و اهداف موردنظر (زیرساخت‌های مهم، حساس و حیاتی) و سایر چالش‌ها. در این زمینه نظریات مختلفی مطرح شده است که در این نوشتار به‌اختصار به بررسی دیدگاه‌های ابزار محور، [۳] هدف محور[۴] و دیدگاه نتیجه محور [۵] می‌پردازیم.

[3] .Instrumentality.
[4] .Target- based.
[5].Consequentiality.

بر اساس**دیدگاه ابزار محور** سنتی چنین استدلال می‌شود که حمله‌ی سایبری به‌عنوان نوعی زور نظامی توصیف نمی‌شود، زیرا فاقد ویژگی‌های فیزیکی است که زور نظامی دارد(P. Kanuck,2006:288). طرفداران این نظریه در حمایت از دیدگاه خود به ماده‌ی ۴۱ منشور ملل متحد استناد می‌کنند؛ این ماده به اقداماتی نظیرقطع کامل یا موقتی ... تلگراف رادیو و دیگر ابزارهای ارتباطاتی که مستلزم توسل به‌زور نظامی نیست اشاره می‌نماید.

بر اساس رویکرد **هدف محور**، حمله‌ی سایبری زمانی نوعی توسل به‌زور یا حمله‌ی مسلحانه محسوب می‌شود که به ساختارهای حیاتی ملی[6] نفوذ یابد.

رویکرد **نتیجه محور** بر آثار و پیامدهای ناشی از عملیات‌های اطلاعاتی متمرکز است. زمانی که یک حمله‌ی سایبری آثاری نظیر همان آثاری که توسل به‌زور متعارف ایجاد می‌کند داشته باشد، آن حمله به‌نوعی توسل به‌زور یا حمله‌ی مسلحانه را شکل داده است.

فقدان اطلاع از جزئیات بیشتر و نو بودن شیوه‌های عملیاتی در جنگ‌های سایبری و اطلاعاتی موجب ایجاد نوعی ابهام می‌شود به‌عنوان‌مثال در رویکرد ابزار محور، حمله‌ی سایبری تنها به سیستم‌های ارتباطاتی محدود نمی‌شود. اما آیا این بدین معناست که حمله‌ی سایبری نظیر خاموش‌کردن سیستم ارتباطاتی حمل‌ونقل هوایی مسافربری به‌عنوان نوعی توسل به‌زور توصیف نمی‌شود و حق دفاع مشروع را برای طرف مورد حمله ایجاد نمی‌کند؟

در مقابل، دیدگاه هدف محور ممکن است به‌خاطر گستردگی و دامنه‌ی شمول وسیع آن دچار مشکل شود. حمله‌ی سایبری می‌تواند طیف وسیعی از آثار از قطع سامانه‌های الکترونیکی تا قطع موقت سیستم‌ها، ایجاد خطرات محتمل نظیر نفوذ یک ویروس که آسیب فوری بر جا نمی‌گذارد اما پتانسیل ایجاد آسیب بیشتر را دارد تا تخریب و اختلالات فوری نظیر ازکارانداختن دائمی یک سیستم از طریق یک ویروس را در پی داشته باشد و سؤالی که مطرح می‌شود این است که آیا ماهیت هدف به‌گونه‌ای که تا حدی هدفی «حیاتی» [7] باشد، به‌تنهایی چنین اعمال مختلفی را نوعی توسل به‌زور یا حملات مسلحانه محسوب می‌نماید؟

در نهایت هرچند از منظر رویکرد نتیجه محور، آثار حملات سایبری معادل آثار ناشی از حملات متعارف تلقی می‌شود؛ اما این رویکرد تبعات حملات سایبری که آنها را از حملات متعارف متمایز می‌کند را مستثنی می‌کند. به‌عنوان نمونه، توسل به‌زور وتحریم‌های اقتصادی و سیاسی، نمی‌تواند سیستم بورس یا بانکی را به طور کامل از کار بیندازد، اما یک حمله‌ی سایبری می‌تواند آن‌ها را بدون برجاگذاشتن مجروح، قربانی یا تخریب و خسارات فیزیکی و به‌صورت فوری از کار بیندازند. علی‌هذا، همچنان ابهاماتی در این زمینه باقی می‌ماند از جمله اینکه: آیا در جایی که حمله‌ی سایبری، آثار متفاوتی از توسل به‌زور متعارف داشته باشد، باید آن را خارج از چارچوب منشور و اصل ممنوعیت توسل به زور دانست یا در مواردی

[6] .Critical National Infrastructure.
[7].Critical.

که آثار ناشی از حمله‌ی سایبری دارای فوریتی باشد که نظیر آن در فشار اقتصادی و سیاسی دیده نشده است، می‌تواند مشمول ممنوعیت مندرج در منشور قلمداد شود؟

دیوان بین‌المللی دادگستری ابراز داشته است که مواد ۲ (۴) و ۵۱ منشور ملل متحد به ترتیب دررابطه‌با ممنوعیت توسل به زور و دفاع از خود، بر «هرگونه توسل زور فارغ از تسلیحات به‌کاررفته» اِعمال می‌گردد (Nuclear Weapons advisory opinion, para. 39) .

بنابراین، صرف اینکه یک رایانه (و نه یک اسلحه، سامانه‌ی تسلیحاتی یا بستر سنتی) در خلال یک عملیات به کار می‌رود، تأثیری بر «توسل به زور» قلمداد شدن یا نشدن آن عملیات (یا در این باب، ذی‌حق بودن یا نبودن یک دولت در توسل به زور در قالب دفاع از خود) ندارد. در بستر سایبری، این نه ابزار بکار رفته بلکه پیامدهای عملیات ذی‌ربط و شرایط پیرامونی آن است که تعیین کننده عبور یا عدم عبور از آستانه‌ی توسل به زور است. دیدگاهی در این زمینه وجود دارد که بر اساس آن هرگونه به‌کارگیری شیوه یا ابزارهای جنگی توسط یک دولت علیه دولت دیگر، موجب شکل‌گیری به‌کارگیری زور می‌گردد. با وجود این، شیوه یا ابزار جنگی سایبری را می‌توان برای ایجاد پیامدهایی مانند اختلال جزئی در فعالیت‌های سایبری به کار گرفت که آشکارا توسل به زور به شمار نمی‌آیند(TallinnManual 2.0,2017:328).

به نظر می‌رسد راهکار حل ابهامات دست یازیدن به سنجه‌ای مورد توافق است تا بتوان باتوجه‌به پیشرفت سریع این حوزه مصادیق را بر آن اساس بررسی نمود. این‌گونه می‌توان دریافت که مثلاً تأثیر ماهیت زیرساخت هدف در توسل به‌زور قلمداد کردن حمله‌ای سایبری چیست. بر اساس دستورالعمل تالین[۸]"یک عملیات سایبری، زمانی که مقیاس و آثار آن با عملیات‌های غیر سایبری نائل آمده به سطح به‌کارگیری زور برابر باشد، موجب شکل‌گیری به‌کارگیری زور می‌شود."

رویکرد مزبور به‌صورت هم‌زمان بر سطح آسیب وارده و برخی عناصر کیفی یک عملیات سایبری خاص متمرکز است. این رویکرد تا اندازه‌ی زیادی به‌منظور تعیین عملیات‌های سایبری مشابه سایر اقدامات فیزیکی یا غیرفیزیکی که جامعه‌ی بین‌المللی آن ها را با عنوان به‌کارگیری زور توصیف می‌کند، تعبیه شده است. به میزانی که طبق ارزیابی چنین عملیات‌هایی به آستانه‌ی به‌کارگیری زور برسند، عملیات‌های سایبری واجد مقیاس و آثار یکسان با آن ها نیز به‌کارگیری زور خواهند بود.(TallinnManual 2.0,2017:328). در این صورت لازم است شرایط و اقتضائات خاص هر قضیه را سنجید تا بر اساس قاعده محوری و لحاظ نمودن شدت حمله سایبری بتوان آن را توسل به‌زور و واجد وصف ممنوعیت آن دانست.

[۸] راهنمای منتشر شده توسط موسسه تالین (وابسته به ناتو) در خصوص قواعد قابل اعمال حقوق بین الملل در نبردها و عملیات سایبری که در سال ۲۰۱۳ و با مدیریت مایکل اشمیت توسط کارشناسان متعدد فنی، حقوقی از کشورهای مختلف تدوین شده است و نسخه ی جدید و بروزرسانی شده آن در سال ۲۰۱۷ منتشر شد.

در قضیه نیکاراگوئه، دیوان بین‌المللی دادگستری ابراز داشت که «مقیاس و آثار» را باید در حین تعیین اینکه آیا اقداماتی خاص یک «حمله‌ی مسلحانه» به شمار می‌رود یا خیر، مورد بررسی قرار داد(Nicaragua judgment, para. 195). تمرکز بر مقیاس و آثار در هنگام تفکیک میان اقدامات واجد وصف توسل به زور از اقدامات فاقد آن وصف نیز به همان اندازه رویکرد سودمندی است. به بیان دیگر، «مقیاس و آثار» اصطلاحی اختصاری است که عوامل کمی و کیفی را برای تجزیه‌وتحلیل در حین تعیین اینکه یک عملیات سایبری توسل به زور محسوب می‌شود یا خیر در بر می‌گیرد. اگر مقیاس و آثار عملیات‌های سایبری با مقیاس و آثار عملیات‌های غیر سایبری که توسل به زور هستند مشابه باشد، هیچ مبنایی برای حذف آن ها از دامنه‌ی اقداماتی که می‌توانند موجب شکل‌گیری توسل به‌زور گردند وجود ندارد.

به‌عنوان‌مثال، نه عملیات‌های روانی سایبری غیرمخرب که انحصاراً برای کاهش اعتماد به یک دولت طراحی شده‌اند و نه ممنوعیت تجارت الکترونیک با دولت دیگر از جانب یک دولت که برای ایراد تبعات منفی اقتصادی تدارک گردیده است، به‌کارگیری زور محسوب نمی‌شوند. به‌علاوه، دیوان بین‌المللی دادگستری در قضیه‌ی نیکاراگوئه اظهار داشت که صرف تأمین مالی پارتیزان‌های دخیل در عملیات علیه دولت دیگر، به آستانه‌ی توسل به‌زور نمی‌رسد .Nicaragua judgment, para). (228 از این‌رو، برای نمونه، صرف تأمین مالی یک گروه هکری که به‌عنوان بخشی از یک شورش به عملیات‌های سایبری دست می‌زند، به‌کارگیری زور علیه دولتی که درگیر مخاصمه‌ی مسلحانه با شورشیان است نخواهد بود.

از سوی دیگر در همین قضیه‌ی نیکاراگوئه، دیوان تشخیص داد که تسلیح و آموزش نیرویی پارتیزانی که به عملیات‌های خصمانه علیه دولت دیگر می‌پردازد، توسل به‌زور به شمار می‌رود(Nicaragua judgment, para. 228). بنابراین، دولتی که بدافزار یا آموزش لازم برای انجام عملیات‌های سایبری علیه دولت دیگر را در اختیار یک گروه مسلح سازمان‌یافته قرار می‌دهد، مادامی که آن اعمال انجام عملیات‌های سایبری واجد وصف توسل به‌زور را برای گروه ذی‌ربط میسر ساخته باشد، به توسل به‌زور علیه دولت دوم مبادرت جسته است(TallinnManual 2.0,2017:332). همچنین اقداماتی که اشخاص را مجروح می‌سازند یا می‌کشند یا به‌صورت فیزیکی به اشیاء آسیب می‌رساند یا آنها را نابود می‌سازند، به‌کارگیری زور به شمار می‌روند.

نکته قابل‌توجه در راستای این قاعده که یک عملیات سایبری، زمانیکه مقیاس و آثار آن با عملیات‌های غیر سایبری نائل آمده به سطح به‌کارگیری زور برابر باشد، موجب شکل‌گیری به‌کارگیری زور می‌شود؛ آن است که هرگونه به‌کارگیری غیرقانونی زور که حمله‌ی مسلحانه به شمار می‌آید، موجب بروز حق دفاع از خود نیز می‌گردد؛ البته بدیهی است که رعایت الزامات توسل به حق دفاع از خود همچون تناسب نیز باید مدنظر قرار گیرد.

۲. اصل تفکیک

زمانی که دولت‌ها وارد مخاصمه‌ی مسلحانه می‌شوند، قواعد حاکم بر جنگ اعمال می‌شود. در این میان، بر اساس اصل تفکیک دول متخاصم باید در تمامی لحظات مخاصمه، بین جمعیت غیرنظامی و نظامیان و بین اهداف نظامی و غیرنظامی تفکیک نمایند و براین‌اساس تمامی عملیات‌هایشان را صرفاً علیه مقاصد نظامی هدایت کنند.

در ابتدا، با وقوع جنگ تمام ساکنین کشورهای متخاصم دشمن محسوب می‌شدند اما با پدیدارشدن ملاحظات بشردوستانه و ضرورت‌های نظامی در فعالیت‌های نظامی موضوع اصل تفکیک و تمایز بین رزمندگان و غیرنظامیان به‌طورجدی موردتوجه قرار گرفت. چنان که نخستین‌بار اعلامیه‌ی ۱۸۶۸ سن‌پترزبورگ ضمن تصریح به این موضوع، مقرر نمود: «تنها هدف مشروع در جنگ تضعیف نیروهای نظامی دشمن است.» به همین دلیل، حمله به افراد و اموال غیرنظامیان در درگیری‌های مسلحانه (بین‌المللی و غیر بین‌المللی) ممنوع گردید (عربیان،۱۳۹۳: ۴۵).

دیوان بین‌المللی دادگستری در رأی مشورتی ۱۹۹۶ هنگامی که توسل به سلاح‌های هسته‌ای را در پرتو اصول و قواعد حقوق بین‌الملل بشردوستانه مورد بررسی قرار می‌داد، در بندهای ۸۷-۷۴، اصل تفکیک بین رزمندگان و غیر رزمندگان (غیرنظامیان) را به‌عنوان «اصل بنیادین و غیر قابل تخطی (تجاوزناپذیر) حقوق بین‌المللی عرفی»[9] مورد تاکید قرارداد. وصفی که قبل از آن در ادبیات حقوقی وجود نداشت و چنان که مقرر نمود: «دولت‌ها حق ندارند غیرنظامیان را هدف حمله قرار دهند و در نتیجه هرگز نباید سلاح‌هایی به کار گیرند که قادر به تفکیک اهداف نظامی و غیرنظامی نیستند.» (ICJ, Advisory opinion, 1996. para. 78)

نظامیان تنها می‌توانند حملات را علیه اهداف نظامی هدایت نمایند؛ اهدافی که بر اساس ماهیت، مکان، هدف یا نحوه کاربردشان، عملیات نظامی را به نحو مؤثری تسهیل می‌کنند و بنابراین تخریب، تسخیر یا خنثی‌سازی و ازکارانداختن جزئی یا کلی آن ها، در شرایط و وضعیت حاکم بر آنها، مزیت قطعی نظامی به همراه دارد. تمامی اهداف دیگر، غیرنظامی و دارای محدودیت به شمار می‌روند.

اعمال این اصل حتی در مخاصمات مسلحانه‌ی بین‌المللی متعارف نیز دشوار بوده و سؤالاتی ازاین‌دست را مطرح می‌سازد که آیا ایستگاه‌های تلویزیونی یا سیستم برق کمک مؤثری به تحقق اهداف نظامی می‌نماید؟ حملات سایبری ابهامات موجود را تشدید کرده و حتی ممکن است مفهوم اصل تفکیک را به‌طورکلی زیر سؤال برده و تغییر دهد.

از مهم‌ترین چالش‌های پیش روی اصل تفکیک، از جمله این موارد است که ابهام در خصوص تفکیک غیرنظامیان در کدام حمله‌ی سایبری باید صورت گیرد؟ و نیز ماهیت کاربرد دوگانه اغلب ساختارهای اطلاعاتی در حملات سایبری چگونه تحلیل می‌شود؟

[9]Fundamental and Intransgressible Principle of Customary International Law.

گفتنی است توسعه‌ی حملات سایبری ممکن است منجر به جنگ‌هایی شود که بیشتر غیرنظامیان را هدف قرار دهد و در چنین شرایطی اعمال اصل تفکیک را مورد چالش قرار می‌دهد.

حقوق جنگ مسئولیت تفکیک جمعیت و اهداف غیرنظامی از اهداف نظامی و خطرات ناشی از عملیات‌های نظامی را تا بالاترین حد ممکن بر دولت‌ها تحمیل می‌کند. در جایی که سیستم، تأسیسات یا مکانی دارای کاربردی دوگانه است، به‌گونه‌ای که هم می‌تواند در خدمت اهداف نظامی و هم اهداف غیرنظامی قرار گیرد، این مکان به‌عنوان یک مقصد نظامی هدف حمله قرار می‌گیرد. اگر چنین موردی در خصوص حملات سایبری هم مطرح شود تمامی شبکه‌های رایانه‌ای ممکن است هدف حملات واقع شوند و اعمال اصل تفکیک غیرنظامیان نسبت به حملات سایبری نه‌تنها متزلزل است، بلکه تنش بیشتری را نیز در خصوص هدف ادعایی این اصول که همانا محدودکردن ارتش‌ها و نیروهای نظامی به اهداف نظامی، نظامیان و اموال آنها تا حد ممکن در جریان مخاصمه است، موجب می‌شود.

مطالب فوق، دامنه و عمق ابهامی که حملات سایبری در چارچوب مخاصمات مسلحانه به وجود می‌آورد را آشکار می‌سازد. موارد مرتبط با اصل توسل به‌زور و اصل تفکیک به‌سادگی و وضوح قابل تعبیر و تفسیر نیستند. از سوی دیگر نمونه‌های فوق منحصربه‌فرد نبوده بلکه مشکلات مشابهی در زمینه تشخیص چگونگی توسعه و اعمال قواعد مربوط به بی‌طرفی در خصوص حملات سایبری نیز ظاهر می‌شود.

بااین‌وجود به نظر می‌رسد همان گونه که در بحث توسل به‌زور در حملات سایبری گذشت، در اینجا نیز تنها زمانی که عملیاتی سایبری علیه غیرنظامیان یا اشیاء غیرنظامی (دیگر اشخاص و اشیاء تحت حمایت) به سطح حمله مسلحانه برسد به وسیله‌ی اصل تفکیک و آن دسته از قواعدِ حقوق مخاصمات مسلحانه که از اصل ذی‌ربط مشتق می‌شوند ممنوع می‌گردد. (TallinnManual 2.0,2017:422).

البته برخی عملیات‌های هدایت شده علیه جمعیت غیرنظامی قانونی هستند. عملیات‌های روانی مانند انداختن جزوات و پخش تبلیغات، حتی اگر غیرنظامیان مخاطب آن باشند ممنوع نیست. در بستر جنگ سایبری، ارسال پیام‌های رایانامه‌ای به جمعیت دشمن به‌قصد انگیزش برای تسلیم، به‌گونه‌ای مشابه با حقوق مخاصمات مسلحانه سازگار است. (TallinnManual 2.0,2017:400).

۳. بررسی تفصیلی چالش‌های اعمال اصول فوق در حملات سایبری

۱/۳. معیوب بودن و پیچیدگی

اعمال قواعد کنونی حقوق بین‌الملل نسبت به مخاصمات مسلحانه‌ی بین‌المللی بین دو یا چند دولت متمرکز است. اما حملات و جنگ‌های سایبری اشکال متنوعی می‌تواند داشته باشد که نقش بازیگران غیردولتی از اهمیت خاصی برخوردار است. علاوه بر این تنوع حملات در جنگ‌های سایبری، ابزارها و روش‌های حمله، نقص تحلیل‌های کنونی را آشکار می‌سازد.

با خروج از چارچوب مخاصمات مسلحانه‌ی بین‌المللی، حملات سایبری با یک فضای مبهم‌تر مواجه می‌شود که قراردادن آن در یک چارچوب حقوقی مشکل و دارای پیچیدگی‌های چندجانبه‌ی حقوقی است. از جمله اینکه آیا حملات سایبری که بین دولت‌ها رخ نمی‌دهد، ممکن است در چارچوب قواعد حاکم بر مخاصمات مسلحانه‌ی غیربین‌المللی قرار گیرد؟ آیا مخاصمه‌ای وجود دارد که نه دارای مشخصات مخاصمه‌یبین‌المللی و نه ویژگی‌های مخاصمه‌ی غیر بین‌المللی باشد؟

همان‌طورکه اشاره شد، هرچند ارتش‌های کشورها توان زیادی را صرف گسترش قابلیت عملیات سایبری و دکترین‌های مربوط به آن کرده‌اند، اما نقش بازیگران غیردولتی در این عرصه بسیار پررنگ است. فناوری های رایانه‌ای به‌صورت گسترده و بسیار کم‌هزینه‌تر از سلاح‌های متعارف در دسترس قرار داشته و به‌آسانی قابل‌استفاده است و قابلیت برنامه‌ریزی و انجام حمله در هرجایی از جهان را دارد. این نوع حملات به طور ویژه موردتوجه بازیگران غیردولتی است که به دنبال هدف قراردادن اهداف و منافع عمومی و خصوصی هستند. به عبارتی بستر مناسبی را برای تروریست‌ها و مهاجمین فراهم نموده تا با کمترین هزینه و در کوتاه‌ترین زمان، به اهداف خود دست یابند.

زمانی که حملات سایبری توسط یک بازیگر غیردولتی علیه یک دولت واقع می‌شود به علت پیچیدگی‌های اثبات کنترل یک دولت بر حملات، احراز یک حمله‌ی مسلحانه دشوار بوده و در نتیجه به نظر نمی‌رسد دفاع مشروع در مواجهه با بازیگران غیردولتی به‌عنوان یک گزینه‌ی انتخابی مطرح شود. بلکه از دولت‌ها انتظار می‌رود تا در مواجهه با بازیگران غیردولتی در چارچوب قواعد حقوقی داخلی و نه توسل به‌زور نظامی برخورد کنند (ICJ Adv,2004:43). موضوع تعقیب و یافتن منشأ حملات سایبری نیز در شرایط کنونی فناوری از پیچیدگی‌های خاصی برخوردار است.

بنابراین، مستمسک چنین دولتی که حاکمیت او از طریق یک حمله‌ی سایبری نقض، و خسارت‌ها و صدماتی را متحمل شده کدام یک از قواعد حقوقی و مراجع حقوقی بین‌المللی است؟

به نظر می‌رسد، مطابق قواعد عمومی حقوق بین‌الملل، دولتی که حاکمیتش از طریق انجام حملات سایبری نقض شده، باید به دولتی که مظنون است حمله‌ی سایبری از سرزمین آن دولت آغاز و اعمال شده؛ اعلام و هشدار داده و خواستار توقف انجام حمله‌ی سایبری باشد.

در مقابل انتظار می‌رود دولتی که چنین درخواستی از آن به‌عمل‌آمده است به درخواست‌ها جامه‌ی عمل بپوشاند و اگر این دولت از تحقق درخواست‌ها ناتوان یا تمایلی به انجام آن ها نداشته باشد، تنها در این صورت است که دولت مورد تجاوز می‌تواند اقدام متقابل نموده یا اقدام به دفاع مشروع در برابر دولت متجاوز نماید(Channel,2001:49).

در حملات سایبری، دولت‌ها باید به تعهداتشان در چارچوب نظام‌های مختلف و خاص حقوق بین‌الملل، متعهد باشند. برای مثال ازآنجاکه ساختارهای اطلاعاتی به طور مداوم فضای ماورای جو را برای برقراری ارتباطات یا جمع‌آوری داده به کار می‌گیرند، حقوق فضا بر حملات سایبری مؤثر خواهد بود. به‌موجب ماده‌ی ۴ معاهده‌ی فضای ماورای جو، دولت‌ها توافق

کرده‌اند از ماه و دیگر اجرام سماوی منحصراً برای اهداف صلح‌آمیز استفاده کنند (Treaty on Principles Governing,1967: Art. IV(2)).

اگرچه این امر فعالیت نظامی قانونی و مجاز در فضا را به‌خودی‌خود منع نمی‌کند؛ اما مصادیق «اهداف صلح‌آمیز»[10] موضوع بحث‌های طولانی بوده که در خصوص حملات سایبری مسئله‌ی چندان ساده‌ای نیست.

علاوه بر این ماده‌ی ۴ معاهده‌ی فضای ماورای جو، اعلان رسمی یک دولت را قبل از اقدام به انجام هر نوع حمله‌ی سایبری توسط دولت مزبور که ممکن است منجر به مداخلات زیانمند بالقوه در فعالیت‌های دیگر دول عضو در خصوص کاوش و بهره‌برداری مسالمت‌آمیز از فضای ماورای جو شود را ایجاب می‌نماید (Treaty on Principles Governing,1967: Art. IV).

تعهدی مشابه به این نیز به‌موجب اساسنامه اتحادیه ارتباطات بین‌المللی (ITU) وجود دارد. بند ۱ ماده‌ی ۴۵، مقرر می‌دارد که تمامی ایستگاه‌های ارتباطاتی به‌گونه‌ای عمل می‌کنند که سبب مداخله و نفوذ مخرب و آسیب‌زا به ارتباطات یا سرویس‌های رادیویی دیگر دولت‌ها نشود(ITU, 1994: 1003) . همچنان که طبق قاعده تلاش مکفی یا تلاش مقتضی[11] دولتها متعهد می باشند تا اجازه ندهند آگاهانه از قلمرو آنها برای اقدامات متخلفانه بین المللی مغایر با حقوق سایر دولت ها استفاده شود.

در هر حالت دولت‌ها باید تأثیرات حملات سایبری را که ممکن است موجب مداخلات و نفوذهای مخرب شود، در نظر بگیرند. چنانچه حملات سایبری با استفاده از دریا یا مسیرهای هوایی مسافربری انجام شود، نظام‌های حقوقی دیگری نیز بر آنها حاکم خواهد بود.

نهایتاً اینکه دولت‌هایی که درصدد انجام حملات سایبری هستند، باید چگونگی اعمال و اجرای قوانین داخلی دیگر دولت‌ها را ارزیابی نمایند. دولت‌هایی که سرزمینشان هدف یک حمله‌ی سایبری واقع می‌شود، باید این امر را در قوانین کیفری خود و بر مبنای آثار این‌گونه حملات بر سرزمینشان جرم‌انگاری نموده و قاعده‌مند سازند. دولت‌هایی که حملات سایبری از سرزمین آنها به سمت سایر اهداف واقع می‌شود نیز می‌بایست چنین قانون‌گذاری و جرم‌انگاری را انجام دهند. چه دولت‌های هدف حملات سایبری و چه دولت‌هایی که حملات سایبری از سرزمین آن‌ها شکل می‌گیرد.

بنابراین این دو مسئله، یعنی عدم شمول قواعد بین‌المللی حاکم بر مخاصمات مسلحانه بر مخاصمات نوین و نظام‌های حقوقی چندگانه که دارای هم‌پوشانی‌هایی با یکدیگر هستند؛ بر حقوق حاکم در جنگ سایبری سایه افکنده است. اگرچه پیچیدگی حقوق جنگ به‌خودی‌خود مشکلی برای دولت‌هایی است که به‌زور متوسل می‌شوند؛ اما حملات سایبری این مشکل را باتوجه‌به ترتب قواعد حقوقی دیگر که موردتوجه قرار گرفته، تشدید کرده است.

[10] .Peaceful Purposes.
[11] due diligence

آیا معقول است که از ارتش‌های سایبری انتظار داشت تا تمامی این موضوعات حقوقی را به طور هم‌زمان، به‌ویژه در وضعیت‌هایی که از آن ها خواسته می‌شود تا فوراً واکنش نشان دهند، اعمال نمایند؟

۲/۳. عدم تعین یا نامعین بودن

ابهام در نوع، سطح، ابزارها و روش‌های جنگ سایبری و فقدان شناخت کافی از این نوع جنگ به دلیل گستره‌ی فضای سایبری و تنوع اقدامات در آن؛ از دشواری‌های تبیین حقوقی مسئله‌ی حملات و جنگ سایبری است.

شناسایی برخی ویروس‌ها و کرم‌ها در سال‌های اخیر و پیش‌بینی ظهور انواع جدیدتر و پیچیده‌تر آن در سال‌های آتی؛ بر تنوع ابزارهای جنگ سایبری افزوده است. از طرفی سیالیت و در جریان بودن فضای سایبری، تهدیدات این فضا را روزبه‌روز نو کرده و هر آینه اَشکال جدیدی از این نوع جنگ رخ خواهد نمود.

از سوی دیگر این سؤال مطرح می‌شود که آیا می‌توان در عمل بازیگران جنگ‌های سایبری (مثلاً در جایی که فرماندهان نظامی هیچ‌گونه تصوری از این که چگونه قواعد حقوقی موجود را در فضای عملیات‌های سایبری هم اعمال کنند ندارند) را ملزم به رعایت کلیه‌ی جوانب و ابعاد حقوقی مسئله نمود؟

به نظر می‌رسد در بسیاری از ابعاد جنگ سایبری ترمیم ضایعات جنگ و جبران آن ساده‌تر از جنگ‌های نظامی باشد. کافی است حملات سایبری طوری طراحی شوند که پس از پایان دوره‌ی محدود حمله، اهدافی که مورد حمله قرار گرفته‌اند به حالت عادی بازگردند. اما مشکل در این است که ابعاد و جزئیات صدمات و اختلال‌های ناشی از حملات سایبری قابل تشخیص نیستند و یا ابعاد صدمات در حدی است که بازسازی و ترمیم آن ها وقت بسیار زیادی نیاز دارد.

۳/۳. عدم شمول

به این معنا که قواعد موجود، در پرداختن به چالش‌های اساسی پیش روی مخاصمات مدرن با مشارکت بازیگران غیردولتی، ناتوان بوده‌اند.

همچنان که اشاره شد، کنوانسیون ژنو و لاهه، فریبکاری را ممنوع نموده‌اند. تمام طرف‌های درگیر در جنگ موظف‌اند از روش‌های فریبکارانه همانند استفاده از اونیفورم امدادرسان‌ها و یا غیرنظامیان پرهیز کنند. اما در جنگ سایبری بخش زیادی از موفقیت حملات به تغییر دادن چهره‌ی مهاجمان و استفاده از پوشش‌ها و مجاری فریبکارانه بستگی دارد. درست است که در جنگ سایبری این نرم‌افزار و سخت‌افزارها هستند که به ما خیانت می‌کنند و نه انسان‌ها اما باید در برابر چنین روش‌هایی نیز درست مثل خیانت و فریبکاری‌های انسان‌ها، قواعد و موازین مناسب مقرر شود.

مشکل دیگر عدم‌پذیرش مسئولیت حملات است. در جنگ سنتی قاعدتاً هر طرف باید مسئولیت حملات خود را برعهده می‌گیرد و معمولاً تروریست‌ها و یا سازمان‌های جاسوسی هستند که در عملیات‌های پنهان چنین اصلی را رعایت

نمی‌کنند. در جنگ سایبری نیز هر گروه، فرد و یا کشوری می‌تواند به‌سادگی چهره خود را پوشانده و از قبول مسئولیت شانه خالی کند.

پذیرش مسئولیت در جنگ فقط یک اصل اخلاقی نیست؛ بلکه از نظر حقوقی و جزایی نیز اهمیت دارد. اگر مسئولان حملات شناخته نشوند، هیچ‌کس خطاکار نخواهد بود. به همین خاطر در عرصه‌ی جنگ سایبری نیز باید مراجع و موازینی برای تشخیص هویت مسئولین حملات و جرائم آنها وجود داشته باشد.

۴. نتیجه‌گیری

هر عملیات سایبری که از نظر مقیاس و آثار به سطح یک «حمله‌ی مسلحانه» برسد و توسط یک دولت انجام‌گرفته یا به او قابل انتساب باشد، «توسل به زور» محسوب شده و لازم است در چنین حمله‌ای اصول اساسی مخاصمات مسلحانه همچون اصل تفکیک رعایت شود.

حملات سایبری که عملیات سایبری تهاجمی یا دفاعی هستند که منطقاً انتظار می‌رود موجب ورود آسیب به یا مرگ اشخاص یا ایراد خسارت یا نابودی اشیاء گردد، حاکی از وقوع تهدیدات نوین و فزاینده‌ای است که حقوق بین‌الملل موجود و قوانین داخلی کشورها برای مواجهه با آن تاکنون چارچوب‌های ویژه‌ای تبیین نکرده است. از حقوق مخاصمات مسلحانه تنها می‌توان در پاسخ به حملات سایبری که به سطح حمله مسلحانه ارتقاء یافته، یا در بستر یک مخاصمه مسلحانه جاری به وقوع پیوسته باشند بهره‌برداری نمود. اکثر حملات سایبری به سطح مخاصمه مسلحانه ارتقاء نمی‌یابند؛ البته اینکه عملیاتی سایبری از رسیدن به سطح توسل به زور بازمی‌ماند، ضرورتاً آن را به‌موجب حقوق بین‌الملل قانونی نمی‌سازد. بلکه یک عملیات سایبری می‌تواند به طور خاص، موجب شکل‌گیری نقض حاکمیت یا ممنوعیت مداخله گردد.

مشروط به آنکه حمله سایبری اولیه یکی از تعهدات بین‌المللی دولت مسئول را نقض نماید، به‌موجب حقوق بین‌الملل عرفی، دولت قربانی حق دارد به‌منظور اجبار دولت مسئول به تعهد به هنجارهای بین‌المللی و خودداری از انجام حملات سایبری از داخل قلمروی ارضی خویش عدم اجازه به انجام چنین عملیاتی، اقدامات متقابل و ضروری (غیرمسلحانه) را طراحی نماید؛ درحالی‌که دفاع عامل، عمومی‌ترین نوع اقدامات متقابل است که می‌توان در پاسخ آن را مشروع دانست مشروط بر اینکه اقدام مذکور بایستی متناسب با آسیب وارده به دولت قربانی باشد. به‌علاوه اقدامات متقابل بایستی به‌منظور بازگشت به شرایطی باشد که هم دولت مرتکب عمل و هم دولت قربانی به وظایف قانونی خویش در ارتباط با طرف مقابل بازگردانده شوند. این اقدامات متقابل بایستی موقتی بوده و به‌محض اینکه انجام حملات سایبری متوقف شد، اقدامات متقابل نیز متوقف شوند. فضای مجازی یک شبکه از مجموعه شبکه‌هایی است که هزاران تأمین‌کننده خدمات اینترنتی در سراسر جهان را شامل می‌شود. هیچ دولت یا سازمان خاصی قادر به آن نیست به‌تنهایی از شبکه دفاع سایبری

مؤثر نماید. باوجودآنکه توسعه‌های داخلی خود هنجارهای بین این هنجارها تاکنون تعریفی مورد قبول از حمله سایبری توسط بازیگران بین‌المللی دولتی و غیردولتی ارائه نشده است.

به نظر می‌رسد جامعه بین المللی می بایست به سرعت رویکرد خود در قبال حملات و تهاجمات سایبری را روشن نماید. تلاش های ناکافی کشورهایی همانند روسیه با پیشنهاد هر ساله قطعنامه هایی به مجمع عمومی و نیز کمیته اول مجمع عمومی و سایر مجامع منطقه ای و بین المللی برای تدوین قواعد مشخصی عملیات سایبری تاکنون منتهی به اتفاق کشور ها و صدور سندی بین المللی نشده است. این در حالی است که گسترش وابستگی کشورها به اینترنت و توسعه روزافزون فضای سایبری، حجم تهدیدات و عملیات سایبری را تشدید نموده و آسیب پذیری کشورها را بیش از پیش نمایان ساخته است.

بر این اساس نیاز به قاعده مند سازی این پدیده با توجه به تاثیرات مستقیم آن بر امنیت ملی و امنیت بین الملل کاملا ضرورت می یابد.

منابع:

فارسی:

- عربیان، محمدجواد، **قابلیت اعمال حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری**، رساله دکتری، تهران، مرکز تحصیلات تکمیلی دانشگاه پیام‌نور، ۱۳۹۳.

انگلیسی:

- CCDCOE, TallinnManual 2.0 , Cambridge University Press, 2017.p 328-422

- Charter of United Nations.
- Constitution of the International Telecommunications Union,Annex, 1 July 1994. , art. 45(1), Annex, P. 1003
- Corfu Channel (UK v. Alb), 1949, ICJ, merits; Responsibility of States for Internationally Wrongful Acts, Art. 49, U.N.G.A. Res. 56/83, Annex, 12 December 2001.
- Emily Haslam, Information Warfare: Technological Changes and international Law, J. CONFLICT & SECURITY L. 4.2 (2000).
- ICJ, Advisory opinion, 1996. para. 78. at: https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

- Legal Consequences of the Construction of Wall in the Occupied Palestinian Territory, ICJ Adv. Op., 9 July 2004, 43 I.L.M.1050
- Nicaragua judgment.
- Nuclear Weapons advisory opinion.

- Responsibility of States for Internationally Wrongful Acts, Art. 49, U.N.G.A. Res. 56/83, Annex, 12 December 2001 .
- Sean P. Kanuck, Information Warfare: New Challenges for Public International Law, 37 Harv. Int'l L. J. 272,2006. P 288.
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, 27 January 1967.

lohUN Convention on the Law of the Sea, 10 December 1982, arts. 19, 109 (UNCLOS)