بسم الله الرحمن الرحيم

جنگ سایبری

از منظر حقوق بین‌الملل

نگارش

دکتر نازنین برادران

استادیار دانشکده حقوق و علوم انسانی

عضو هیئت علمی دانشگاه آزاد اسلامی واحد شیراز

مؤسسه مطالعات و پژوهشهای حقوقی

تهران ـ ۱۳۹۸

سرشناسه : برادران، نازنین، ۱۳۶۲ فروردین-
عنوان و نام پدیدآور : جنگ سایبری از منظر حقوق بین‌الملل/ نگارش نازنین برادران؛ نرگس صادقی.
مشخصات نشر : تهران: موسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۸.
مشخصات ظاهری : ۲۳۳ ص.
شابک : ۹۷۸-۶۰۰-۸۰۴۰-۲۱-۷
وضعیت فهرست‌نویسی : فیپا
یادداشت : کتابنامه:ص.۲۲۵ - ۲۳۳.
موضوع : جنگ اطلاعاتی (حقوق بین‌الملل)
موضوع : Information warfare (International law)
موضوع : جنگ سایبری
موضوع : Cyberspace operations (Military science)
موضوع : حقوق بین‌الملل
موضوع : International law
رده بندی کنگره : KZ۶۷۱۸/ب۴ج۹/۱۳۹۸
رده بندی دیویی : ۳۴۱/۶۳
شماره کتابشناسی ملی : ۵۶۶۷۶۲۹

با مراجعه به فروشگاه اینترنتی شهر دانش از مزایای خرید آنلاین و تخفیف ویژه برخوردار شوید

www.**shahredanesh**.com

عنوان : **جنگ سایبری از منظر حقوق بین‌الملل**
تألیف : **نازنین برادران**
ناشر : مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش
صفحه آرا : سودابه رسولی
ویراستار و طراح جلد : نرگس صادقی
نوبت چاپ : اول
تاریخ چاپ : ۱۳۹۸
شمارگان : ۲۰۰
شابک : ۹۷۸-۶۰۰-۸۰۴۰-۲۱-۷
بهاء : ۱۳۸,۰۰۰ تومان

حق چاپ محفوظ است.

تهران ـ خیابان کریم‌خان زند ـ خیابان سنایی ـ خیابان نهم ـ خیابان گیلان ـ پلاک ۵
کد پستی ۱۵۸۵۷۴۳۱۱۱ صندوق پستی: ۱۵۸۷۵/۴۵۳۹ تلفن: ۸۸۸۱۱۵۸۱ نمابر: ۸۸۸۱۱۵۸۰
Website: http://www.sdil.ac.ir Email: publication@sdil.ac.ir

«سپاس و قدردانی»

بر خود لازم می‌بینم که مراتب تشکر و قدردانی صمیمانه خودم را از اساتید فرهیخته‌ای که اینجانب را مورد لطف و مهربانی خود قرار داده‌اند، اعلام نمایم. از این‌رو ابتدا لازم می‌دانم که از زحمات، دلگرمی‌ها، راهنمایی‌ها و نقادی‌های موشکافانه استاد عزیز و معلم اخلاقم جناب آقای دکتر همایون حبیبی و همچنین از الطاف، محبت‌ها و نکته‌سنجی‌های بی‌دریغ اساتید محترم، جناب آقای دکتر سید علی هنجنی و جناب آقای دکتر سید قاسم زمانی کمال تشکر و امتنان را داشته باشم.

تقدیم به:

مادر عزیزم

که همیشه همراه و پشتیبان من است.

به نام خداوند جان و خرد

سخن ناشر

توسعه ادبیات حقوقی در هر کشور، نقش مهمی در پیشرفت نظام حقوقی آن کشور ایفاء می‌نماید. اندیشمندان و پژوهشگران دنیای بیکران حقوق که شیفته نظم‌اند و سرباز عدالت، آموزه‌های علمی و تجربیات عملی خویش را به جامعه حقوقی عرضه می‌دارند تا بتوانند در تثبیت و تنویر نظم اجتماعی و استقرار عدالت و اصلاح و پیشرفت کشور سهیم گردند.

قانون‌گذار فهیم و آگاه، هیچ‌گاه در مقام تهیه پیش‌نویس و مهیا شدن جهت وضع قانون، خود را بی‌نیاز از ادبیات و دکترین حقوقی کشور و مشورت با خبرگان نخواهد یافت و هیچ‌گاه مصوبات قبلی خویش را دائمی و مصون از نقد و اصلاح قلمداد نخواهد نمود. قضات متخصص و عدالت‌پیشه نیز نقد علمی و منصفانه آرای خود را مایه تکامل و پیشرفت می‌دانند.

دانشکده‌های حقوق که به مأموریت خطیر تربیت قضات، وکلا، مشاوران حقوقی، سردفتران، پژوهشگران و اساتید حقوق و فقه همت می‌گمارند علاوه‌بر اینکه از آموزه‌های علمی و قضایی کشور بسیار بهره می‌برند متقابلاً رسالت مهمی در غنی‌سازی ادبیات و دکترین حقوقی کشور برعهده دارند.

کشور ایران به ویژه در دو دهه اخیر پیشرفت قابل توجهی در توسعه کمّی ادبیات حقوقی کشور را شاهد بوده است. تعداد کتب و نشریات حقوقی منتشره در کشور طی بیست سال اخیر، به نسبت گذشته به مراتب افزایش یافته است. این دستاورد را باید به فال نیک گرفت و امیدوار بود که این پیشرفت کمّی به همین میزان با توسعه‌ای کیفی در بارور شدن دکترین حقوقی مورد نیاز کشور همراه باشد و با احترام به حقوق مالکیت فکری دیگران انتشار یابد.

انتشارات مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش که همواره سعی داشته است علاوه‌بر انتشار آثار حاصل از تحقیقات پژوهشکده حقوق، به صورتی هدفمند و با ارزیابی علمی به گزینش و چاپ و انتشار کتاب‌های حقوقی در حوزه‌ها و موضوعات مورد نیاز جامعه حقوقی کشور مبادرت ورزد، زحمات خانم **دکتر نازنین برادران** در تألیف کتاب **جنگ سایبری از منظر حقوق بین‌الملل** را ارج نهاده، امیدوار است این کتاب مورد استقبال جامعه حقوقی کشور و مورد استفاده متولیان امر قرار گیرد.

وحید اشتیاق

فهرست اختصارات

AJIL ⇨ American Journal of International Law.
ALJST ⇨ Albany Law Journal of Science and Technology.
AMW Manual ⇨ Manual on International Law Applicable to Air and Missile Warefare, 15 May 2009.
AUILR ⇨ American University International Law Review.
CCDCOE ⇨ CO - Operative Cyber Defense Center of Excellence.
CM ⇨ Canadian Manual (Canada, Office of the Judge Advocate General, Law of Armed Conflict at the Operational and Tactical Levels, B-GJ-005-104/FP-021, 2001).
CNA ⇨ Computer Network Attack.
CNO ⇨ Computer Network Operation.
Col.J.Trans.L ⇨ Columbia Journal of Transnational Law.
CSIS ⇨ Center for Strategic and International Studies.
CUP ⇨ Cambridge University Press.
DDoS ⇨ Distributed Denial of Service .
ED ⇨ Editor.
EJIL ⇨ European Journal of International Law.
EUCOM ⇨ The United States European Command.
German Manual ⇨ (The Federal Ministry of Defence of the Federal Republic of Germany, Humanitarian Law in Armed Conflicts Manual, zdV 15/2, 1992).
Har V.J.L. Tech ⇨ Harvard Journal of Law & Technology.
HNSJ ⇨ Harvard National Security Journal.
ICJ ⇨ International Court of Justice.
ICRC ⇨ International Committee of Red Cross.
ICTY ⇨ International Criminal Tribunal for the Former Yugoslavia.
IHL ⇨ International Humanitarian Law.
IIHL ⇨ International Institute of Humanitarian Law.
JCSL ⇨ Journal of Conflict and Security Law.
L.Rev ⇨ Law Review**.**
LJIL ⇨ Leiden Journal of International Law.
MLNIAC ⇨ The Manual on the Law of Non-International Armed Conflict.
N.Y.U.J.Int'l L. & Pol ⇨ New York University Journal of International Law and Politics.
NATO ⇨ North Atlantic Treaty Organization.
NRC ⇨ National Research Council.

OUP ⇨ Oxford University Press.
PCIJ ⇨ Permanent Court of International Justice.
SJIL ⇨ Stanford Journal of International Law.
SMILAACS ⇨ San Remo Manual on International Law Applicable to Armed Conflicts at Sea.
SWJ ⇨ Small Wars Journal.
TMILACW ⇨ Tallinn Manual on the International Law Applicable to Cyber Warfare.
U.K.Manual ⇨ U.K.Ministry of Defence, The Joint Service Manual of the Law of Armed Conflict, JSP 383, 2004.
UN ⇨ United Nation.
UNDOC ⇨ United Nations Document.
UNYB ⇨ United Nations Yearbook.
VJIL ⇨ Virginia Journal of International Law.
Vol. ⇨ Volume.
YBK *Int'1 L* ⇨ Yearbook of International Law.
YJIL ⇨ Yale Journal of International Law.

فهرست مطالب

سخن ناشر ۹

فهرست اختصارات ۱۰

مقدمه ۱۷

بخش اول: جنگ سایبری و حقوق بین‌الملل توسل به زور ۲۵

فصل اول: جنگ سایبری و دفاع مشروع از منظر حقوق بین‌الملل ۲۷

مبحث اول: ترمینولوژی و تعاریف ۲۷

گفتار اول: تعریف فضای سایبر ۲۸

گفتار دوم: گسترهٔ فضای سایبر ۳۰

گفتار سوم: ویژگی‌های فضای سایبر ۳۲

بند اول: سرعت و روزآمدی فضای سایبر ۳۲

بند دوم: سهولت تغییر هویت در فضای سایبر ۳۳

بند سوم: گسترده و فراگیر بودن فضای سایبر ۳۳

بند چهارم: آزادی در فضای سایبر ۳۴

بند پنجم: فرامکانی و فرازمانی بودن فضای سایبر ۳۴

بند ششم: نامتمرکز بودن فضای سایبر ۳۵

گفتار چهارم: حملات سایبری ۳۶

مبحث دوم: زمینه‌های تاریخی ۳۹

مبحث سوم: اقدامات جامعه بین‌المللی در مقابل تهدیدات سایبری ۴۲

مبحث چهارم: حملات سایبری به مثابهٔ استفاده از زور در حقوق بین‌الملل ۴۷

گفتار اول: حملات سایبری به‌عنوان یک حملهٔ مسلحانه ۵۰

گفتار دوم: جنگ سایبری و استثنای دفاع مشروع ۵۴

بند اول: ضرورت ۵۶
بند دوم: تناسب ۵۷
بند سوم: قریب‌الوقوع بودن و فوریت ۵۸
گفتار سوم: دفاع مشروع جمعی ۶۲
گفتار چهارم: شورای امنیت و حملات سایبری ۶۴
گفتار پنجم: سازمان‌های منطقه‌ای ۶۷
مبحث پنجم: بررسی برخی موارد مهم‌ترین حملات سایبری در سال‌های اخیر ۶۹
گفتار اول: حملهٔ سایبری سال ۲۰۰۷ میلادی به استونی ۶۹
گفتار دوم: حملهٔ سایبری سال ۲۰۱۰ میلادی به ایران ۷۱
فصل دوم: حملات سایبری و اصل عدم مداخله ۷۴
مبحث اول: حاکمیت دولت و اصل عدم مداخله ۷۵
مبحث دوم: اقدامات دولت قربانی در مقابل نقض اصل عدم مداخله ۸۱
فصل سوم: قابلیت انتساب در حملات سایبری ۸۴
مبحث اول: ارگان‌های دولت ۸۸
مبحث دوم: نمایندگی‌های دولت ۹۰
مبحث سوم: عدم تمایل دولت به جلوگیری از اقدامات اشخاص خصوصی یا تحمل اقدامات آنان ۹۷
بخش دوم : قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری ۱۰۱
فصل اول: اعمال قواعد حقوق بین‌الملل بشردوستانه در حملات شبکه‌ای کامپیوتری ۱۰۳
مبحث اول: طبقه‌بندی مخاصمات سایبری به لحاظ محدودهٔ جغرافیایی ۱۰۵
گفتار اول: طبقه‌بندی به‌عنوان مخاصمات مسلحانهٔ بین‌المللی ۱۰۷
گفتار دوم: طبقه‌بندی به‌عنوان مخاصمات مسلحانهٔ غیربین‌المللی ۱۱۴
مبحث دوم: اصل اساسی تفکیک ۱۲۱
گفتار اول: غیرنظامیان و اموال غیرنظامی در مقابل رزمندگان و اهداف نظامی ۱۲۳

گفتار دوم: ممنوعیت حملات عمدی علیه غیرنظامیان و اهداف غیرنظامی ۱۲۴
گفتار سوم: حملات غیرقادر به تمایز میان اهداف نظامی و غیرنظامی ۱۲۵
مبحث سوم: اصل تناسب و ممنوعیت ایراد خسارات جانبی بیش از حد ۱۲۷
مبحث چهارم: احتیاط‌های ممکن ۱۳۲
مبحث پنجم: شرط مارتنس ۱۳۴
مبحث ششم: اقدامات احتیاطی خاص ۱۳۶
گفتار اول: اقدامات احتیاطی در قبال اماکن و اموال مورد حمایت خاص ۱۳۷
بند اول: محیط زیست ۱۳۷
بند دوم: اموال فرهنگی ۱۴۰
بند سوم: کارگاه‌ها و تأسیسات حاوی انرژی‌های خطرناک ۱۴۴
بند چهارم: اشیاء ضروری برای حفظ و حیات جمعیت غیرنظامی ۱۴۸
گفتار دوم: اقدامات احتیاطی در قبال اشخاص مورد حمایت خاص ۱۵۰
بند اول: بیماران و کارکنان بهداری و مذهبی ۱۵۱
بند دوم: کودکان ۱۵۴
بند سوم: روزنامه‌نگاران ۱۵۶
بند چهارم: اشخاص بازداشت‌شده ۱۵۹
فصل دوم: وسایل و روش‌های جنگ ۱۶۴
مبحث اول: قواعد حاکم بر سلاح‌ها ۱۶۶
گفتار اول: منع صدمه اضافی و رنج غیرضروری ۱۶۷
گفتار دوم: ممنوعیت سلاح‌های غیرقادر به تفکیک ۱۷۰
مبحث دوم: سلاح‌های سایبری و ممنوعیت برخی تسلیحات متعارف ۱۷۱
مبحث سوم: تعهدات مادۀ ۳۶ و قواعد حاکم بر سلاح‌ها ۱۷۳
فصل سوم: ممنوعیت شیوه‌های خائنانه ۱۷۵
مبحث اول: حیله‌های جنگی ۱۷۵
مبحث دوم: خیانت‌های جنگی ۱۷۷

فصل چهارم: اشغال ۱۸۰
مبحث اول: احترام به اشخاص تحت حمایت ساکن در سرزمین‌های اشغالی ۱۸۲
مبحث دوم: نظم عمومی و امنیت در مناطق اشغال‌شده ۱۸۴
مبحث سوم: امنیت قدرت اشغالگر ۱۸۶
مبحث چهارم: مصادره و توقیف اموال ۱۸۷
فصل پنجم: بی‌طرفی ۱۹۱
مبحث اول: حفاظت از زیرساخت‌های سایبری بی‌طرف ۱۹۳
مبحث دوم: تعهدات دول بی‌طرف ۱۹۴
مبحث سوم: عملیات سایبری در قلمرو بی‌طرف ۱۹۶
نتیجه‌گیری ۱۹۹
الف: بهرهٔ کلام ۱۹۹
ب: تحلیل دستورالعمل تالین ۲۱۴
ج: راه پیش رو ۲۲۱
منابع و مآخذ ۲۲۵

مقدمه

امروزه اطلاعات، تکنولوژی و ارتباطات بخش مهمی از زندگی انسان‌ها را دربرگرفته است و دولت‌ها جهت انجام فعالیت‌های خود به تکنولوژی و استفاده از کامپیوتر به‌شدت نیازمندند و فضای سایبر و ارتباطات دیجیتال، در عین اینکه دارای آثار مفید بسیاری هم برای اشخاص خصوصی و هم دولت‌هاست، اما می‌تواند منبع بسیاری از تهدیدات و آسیب‌ها نیز باشد و به همین دلیل حفظ امنیت در فضای سایبر به یکی از اولویت‌های دولت‌ها تبدیل شده است. درواقع در دوران کنونی یکی از چالش‌هایی که امنیت دولت‌ها را مورد تهدید قرار می‌دهد، حملات سایبری است و همین مسئله باعث شده که جنگ نیز از مفهوم سنتی خود که در آن از سلاح‌های کلاسیک استفاده می‌شد، فاصله گرفته و پیشرفت تکنولوژی ابزارهای جدیدی را در اختیار دولت‌ها قرار داده است که از جمله مهم‌ترین آنها استفاده از فضای سایبر جهت انجام حملات سایبری علیه دولت‌های موردنظر است. امروزه فضای سایبر در حال تبدیل شدن به یک میدان جدید به منظور پیگیری عملیات نظامی است و به اذعان کارشناسان نظامی، فضای سایبر به‌عنوان یک عرصه نوین جنگ درحال ظهور است. این درحالی است که قدرت‌های بزرگ در حال تجهیز هرچه سریع‌تر و گسترده‌تر نیروهای خود برای جنگ‌های سایبری هستند و علیه دشمنان و رقبای خود به‌نحو فعالانه‌ای از آن بهره می‌گیرند و بنا به گزارش هیئت پانزده‌نفره متخصصان سازمان ملل که در ژانویه ۲۰۱۳ تهیه شده است[1] امروزه چهل دولت در دنیا برای جنگ‌های سایبری تهاجمی خود را تجهیز کرده‌اند. نشانه‌های عملی این ادعا آن است که در سال‌های اخیر شاهد بروز موارد متعدد حملات سایبری میان دولت‌ها بوده‌ایم، برای مثال کشور آمریکا هدف حملات متعدد سایبری قرار گرفته که ادعا می‌شود از طرف کشور چین صورت گرفته است[2]. مورد معروف دیگر حمله به استونی در آوریل ۲۰۰۷ میلادی است که به مدت سه هفته، این کشور هدف حملات سایبری قرار گرفت که باعث از کار افتادن وب‌سایت‌های رسمی دولتی، ایستگاه‌های تلویزیونی، بانک‌ها و ... گردید و ادعا می‌شود که از سوی فدراسیون روسیه صورت گرفته است. حملات سایبری علیه گرجستان در ژوئیه و آگوست سال ۲۰۰۸ میلادی قبل از درگیری و نیز در جریان حملات مسلحانه این کشور با فدراسیون روسیه اتفاق افتاد و باعث شد که وب‌سایت‌های دولتی از شبکه خارج شده و تغییر شکل دهند و محتوای آنها با

1. “On the Developments in the Field of Information and Telecommunications in the Context of International Security”.
2. SJ Shacketford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law”, *Berkeley Journal of International Law*, Vol.27, Iss. 1 (2009), pp.191-251, p.204.

تبلیغات روسیه جایگزین گردد[۱]. موارد متعدد دیگر حملات سایبری در سایر کشورها از جمله انگلستان، تایوان، کره جنوبی، قزاقستان، سوئیس و ... نیز رخ داده است[۲] و کشورمان ایران نیز در سال ۲۰۱۰ میلادی هدف حملات سایبری با هدف ایجاد اختلال در فعالیت‌های هسته‌ای از طریق ویروس استاکس‌نت[۳] قرار گرفت و به تعدادی از سانتریفیوژهای فعال در مرکز هسته‌ای نطنز آسیب وارد گردید که ظاهراً ازسوی دولت آمریکا صورت گرفته‌اند. موارد حملات سایبری بسیار متعدد بوده و اشاره به همهٔ آنها در این مقال نمی‌گنجد اما یکی از بحث‌برانگیزترین موارد اخیر ادعای نامزد دموکرات‌ها در انتخابات ریاست جمهوری در سال ۲۰۱۶ می‌باشد که سرویس‌های اطلاعاتی روسیه را به هک کردن کامپیوترهای کمیته ملی دموکراتیک متهم نموده است[۴].

با توجه به موارد فوق‌الذکر و این واقعیت که تهدیدات سایبری نه‌تنها کاهش نخواهند یافت بلکه در آینده نیز با پیشرفت هرچه بیشتر تکنولوژی رو به افزایش خواهند بود، دولت‌ها مجبور هستند که در مقابل این‌گونه تهدیدها واکنش نشان دهند و همین ضرورت منجر به طرح این سؤال اساسی می‌شود که قواعد حقوق بین‌الملل تا چه حدی بر فعالیت‌های سایبری قابل اعمال خواهد بود؟ پاسخ به این سوال ساده نیست زیرا حملات سایبری با پیچیدگی‌های فنی و تکنیکی خاصی همراه هستند که آنها را از حملات کلاسیک متمایز می‌سازد مانند گمنامی و مشخص نبودن هویت اجراکنندگان حملات، سرعت و دسترسی وسیع به سلاح‌های سایبری برای برخی دول خاص و حتی دسترسی آسان بازیگران غیردولتی به این‌گونه سلاح‌ها و آثار مخرب مستقیم یا غیرمستقیمی که این‌گونه سلاح‌ها می‌توانند ایجاد کنند.

جهت درک بهتر ویژگی‌های فوق‌الذکر توضیح برخی عبارات از جمله فضای سایبر و حملات سایبری ضروری می‌باشد. فضای سایبر فضایی غیرمادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه‌ای به وجود آمده است و دنیایی مجازی را در کنار دنیای واقعی ایجاد نموده است[۵]، این فضا فراتر از اینترنت توسعه یافته است و تمامی فعالیت‌های دیجیتال شبکه‌ای را

1. J Markoff, “Before the Gunfire, Cyber Attacks”, *The New York Times*, 12, August, 2008.
2. M Roscini, “World Wide Warfare - Jus ad Bellum and Use of Cyber Force”, *Max Plank Yearbook of United Nations Law*, Vol.14 (2010), pp.85-130, p.89.
3. Stux net.
4. http://tnews.ir/news/48d767754311.html.
۵. فضلی، م.، *مسئولیت کیفری در فضای سایبر*، تهران: خرسندی، ۱۳۸۹، چاپ اول، ص ۱۷.

دربر می‌گیرد، فضای مذکور دارای گستره‌ای جهانی و بدون مرز، پوشیده و پنهان بوده و ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد[۱].

جهت درک بهتر عملکرد یک حملهٔ سایبری این نکته قابل‌ذکر است که به‌طور سنتی، اهداف متعارف امنیت در محیط اطلاعاتی متشکل از سه هدف است: محرمانه بودن[۲]، یکپارچگی[۳] و در دسترس بودن[۴]. به این ترتیب بهترین روش جهت طبقه‌بندی حملات این است که ببینیم کدامیک از این اهداف موردتهدید واقع شده‌اند.

حملاتی که در دسترس بودن را مورد هدف قرار می‌دهند، سعی می‌کنند که از دسترسی به شبکه (خواه با پیاده‌سازی حملهٔ DoS[۵] خواه با آفلاین کردن یا خاموش کردن فیزیکی فرایندهای مجازی و ...) جلوگیری کنند. حملاتی که محرمانه بودن را مورد هدف قرار می‌دهند، تلاش می‌کنند تا ورود به شبکه‌های کامپیوتری را به‌منظور نظارت بر فعالیت‌ها و استخراج اطلاعات سیستم‌ها و داده‌های کاربران، به‌دست آورند. ارزیابی این نوع حمله، هم به اطلاعات استخراج‌شده و هم به مقیاس تلاش بستگی دارد. چالش واقعی این حملات هنگامی رخ می‌دهد که استخراج اطلاعات در یک روش سازمان‌یافته و عظیم اتفاق بیفتد.

درنهایت، حملاتی که یکپارچگی و صحت داده‌ها را مورد هدف قرار می‌دهند شامل ورود به سیستم برای تغییر اطلاعات به‌جای استخراج آن می‌باشند. این حملات، داده‌هایی را در دنیای مجازی دستکاری می‌کنند که افراد در دنیای واقعی به آن داده‌ها وابستگی دارند. در بیشتر موارد، این حملات قصد دارند که یا ادراک کاربر را تغییر دهند یا شناخت وضعی از او داشته باشند یا دستگاه‌های فیزیکی، فرایندهای هدایت‌شده یا سیستم‌های اطلاعاتی را خراب‌کاری یا براندازی کنند.

باتوجه‌به مطالب فوق‌الذکر می‌توان حملات سایبری را این‌گونه تعریف نمود: حملات سایبری در چارچوب طیف گسترده‌تری از آنچه عملیات اطلاعاتی نامیده می‌شود، قرار می‌گیرند. عملیات اطلاعاتی که جنگ اطلاعاتی نیز زیرمجموعه‌ای از آن است و هنگام مخاصمه مسلحانه به آن توسل می‌شود[۶]، به‌کارگیری منسجم توانمندی‌های جنگ الکترونیکی، عملیات

---

۱. پاکزاد، ب.، «تروریسم سایبری»، *مجله تحقیقات حقوقی*، دانشگاه شهید بهشتی، ویژه‌نامه شماره ۴ (بهار ۱۳۹۰)، ص ۲۱۶.

2. Confidentiality.
3. Integrity.
4. Availability.
5. Denial of Service.
6. MN Schmitt, "Computer Network Attack and the Use of Force in International Law, Thoughts on a Normative Framework" ,*Colum.J.Transnat'lL.*, No.37 (1998-1999), pp.890-891.

شبکه‌ای رایانه‌ای، عملیات روانی، حیطه‌های نظامی و عملیات هماهنگ با قابلیت‌های پشتیبانی است که به‌منظور تأثیرگذاری، متوقف نمودن، تخریب یا سرقت اطلاعات دشمن و درعین‌حال پشتیبانی از فرایندهای تصمیم‌گیری ملی صورت می‌گیرد.

یکی از بحث‌برانگیزترین سؤالاتی که راجع به این‌گونه حملات مطرح می‌شود، نحوهٔ واکنش در برابر این قبیل اقدامات است. اصل عدم توسل به زور به‌عنوان یکی از اصول مهم سازمان ملل متحد موضوع بند ۴ ماده ۲ منشور می‌باشد و ممنوعیت مطرح‌شده در آن هم فقط شامل کاربرد آن نیست بلکه تهدید به کاربرد آن را نیز دربر می‌گیرد. همچنین منظور از زور، توسل به زور نظامی است و بنابراین فشارهای سیاسی یا اقتصادی از حوزهٔ آن خارج می‌گردد. اصل ممنوعیت توسل به زور با استثنائاتی همراه است که توسط حقوق بین‌الملل عرفی و منشور ملل متحد به‌وجود آمده‌اند. در کنار قطعنامه‌های فصل هفتمی شورای امنیت، دفاع مشروع، دومین استثناء وارد بر اصل عدم توسل به زور است که در ماده ۵۱ منشور به آن تصریح شده است.

منشور ملل متحد محصول گفتمان حقوقی بیش از شصت سال پیش است. بنابراین آنچه که در بند ۴ ماده ۲ منشور به‌عنوان منع استفاده از زور نظامی مطرح شده، استفاده از زور به‌وسیلهٔ سلاح‌های کلاسیک و شناخته‌شده است. اما به‌طورکلی حملات سایبری آثارمخرب فراوانی به بار می‌آورند مثلاً با حملات سایبری می‌توان تأسیسات و زیرساخت‌های حیاتی یک کشور را از کار انداخت مانند شبکهٔ برق، تأسیسات آب آشامیدنی، راه‌آهن، خطوط لوله نفت، خطوط هوایی، سیستم‌های حمل‌ونقل، بازارهای مالی و ...

با توجه به مسائل فوق‌الذکر و اهمیت موضوع، این مسئله در حوزهٔ مباحث حق بر جنگ[1] (توسل به زور) مطرح شده است که آیا این ابزارهای جدید از جمله استفاده از فضای سایبر جهت انجام حملات سایبری هم می‌توانند یک مداخله غیرقانونی که منجر به نقض حاکمیت یک دولت گردیده است محسوب و یا اینکه به‌عنوان استفاده از زور نظامی موضوع بند ۴ ماده ۲ منشور و حمله مسلحانه موضوع ماده ۵۱ در نظر گرفته شوند و درمقابل، برای دولت قربانی حق دفاع مشروع از خود را ایجاد کنند؟ در این راستا لازم به ذکر است که از سویی ماده ۵۱ منشور در کنار شرط ضرورت تنها درصورتی برای دولت قربانی، حق دفاع مشروع را شناسایی کرده که توسل به زور انجام‌شده به آستانه یک «حمله مسلحانه» رسیده باشد. بنابراین شناسایی حملات سایبری به‌عنوان حملهٔ مسلحانه مسئله‌ای حقوقی است که باید موردتحقیق و تتبع قرار بگیرد.

از طرف دیگر همین مسئله یک سؤال مهم دیگر را مطرح می‌سازد و آن این است که چگونه یک حمله سایبری ممکن است به یک دولت منتسب شده و برای دولت قربانی حمله

1. Jus ad Bellum.

درمقابل دولتی که این حمله به او منتسب شده است، حق دفاع مشروع از خود را ایجاد می‌کند و آیا اقدامات دفاعی در واکنش به حملات سایبری که از سوی بازیگران غیردولتی صورت گرفته است، امکان‌پذیر است؟ و همچنین آیا اقدامات دفاعی درمقابل حملات سایبری باید در ماهیت سایبری باشند یا اینکه حملات جنبشی[1] نیز می‌توانند در پاسخ به حملات سایبری اجرا شوند. اینها مسائلی هستند که در حوزهٔ مباحث توسل به زور و حق بر جنگ در این کتاب به دنبال پاسخگویی به آنها هستیم.

اما بُعد مهم و پیچیده دیگر مسئله حوزهٔ حق در جنگ[2] و قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه است و این سؤال اساسی قابل طرح است که آیا قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری نیز قابل اعمال هستند؟ با آنکه در قواعد حقوق بین‌الملل بشردوستانه و معاهدات حاکم بر آن به‌خصوص کنوانسیون‌های ۱۹۴۹ ژنو و پروتکل‌های الحاقی، هیچ اشارهٔ معینی به حملات کامپیوتری نشده است اما آن دسته از حملات سایبری که به آستانهٔ لازم برای ایجاد یک حمله مسلحانه رسیده‌اند، تابع قواعد حقوق بین‌الملل بشردوستانه می‌باشند و به این ترتیب مباحث دیگری در این راستا مطرح می‌شود از قبیل اینکه آیا اجرای اصول مهم حقوق بین‌الملل بشردوستانه مانند اصل تفکیک، تناسب و احتیاط در استفاده از سلاح‌های سایبری هم امکان‌پذیر می‌باشند؟ همچنین به این مسئله نیز پرداخته می‌شود که عملکرد دولت‌ها در استفاده از وسایل و روش‌های جدیدی که در جنگ‌های سایبری مورداستفاده قرار می‌گیرند، در چه شرایطی در تطابق با تعهدات آنها طبق قواعد حاکم بر حقوق بین‌الملل بشردوستانهٔ موجود خواهد بود. اینها عمده‌ترین مسائلی هستند که در حوزه حقوق بین‌الملل بشردوستانه و حق در جنگ در این کتاب مورد تحلیل قرار خواهند گرفت.

پاسخ فرضی و البته مقدماتی این کتاب به سؤالات محوری فوق آن است که یک حمله سایبری که به‌طور واقعی و اساسی باعث ایجاد تلفات جانی یا خسارات مادی گسترده شود به نحوی که بتوان گفت به آستانهٔ یک حملهٔ مسلحانه رسیده است، توسل به زور نظامی محسوب شده و درمقابل، برای دولت قربانی حق دفاع مشروع وجود دارد.

---

1. Kinetic Attacks.

(منظور از این اصطلاح آن است که در گذشته جنگ‌افزارها با استفاده از نیروی جنبشی عمل می‌کردند مانند بمباران نمودن یا شلیک گلوله به‌سوی دشمن، اما در قرن ۲۱ ابزارهای جنگ کمتر خشونت‌آمیز بوده و با پیشرفت تکنولوژی حملات به‌طرق غیرجنبشی مثلاً از طریق ایجاد اختلال در سیستم‌های ارتباطی دشمن صورت می‌گیرند. حملات سایبری که در آنها به‌جای استفاده از نیروی جنبشی (مشت، شمشیر، گلوله، بمب و ...) از ابزارهای دیجیتال استفاده می‌شود معمولاً در این دسته قرار می‌گیرند).

2. Jus in Bello.

درخصوص موضوع قابلیت انتساب در حملات سایبری باید گفت که اگر یک حمله سایبری به‌وسیلهٔ ارگان‌های رسمی یک دولت یا اشخاص خصوصی که به‌وسیله دولت هدایت شده یا تحت کنترل کلی دولت بوده‌اند، صورت گیرد و یا این قبیل حملات توسط بازیگران غیردولتی اجرا شود که در سرزمین دولت فعالیت می‌کرده‌اند و دولت میزبان اعمال آنها را تحمل کرده یا سعی و کوشش لازم را در جلوگیری از اقدامات آنان به‌عمل نیاورده باشد، آن اعمال به دولت قابل انتساب خواهد بود.

در ارتباط با موضوع نوع واکنش درمقابل حملات سایبری جهت دفاع مشروع در مقابل این‌گونه حملات باید شرایط دفاع مشروع از جمله ضرورت، تناسب و فوریت رعایت شود اما به دلیل ویژگی‌های متمایز جنگ‌های سایبری از جنگ‌های سنتی نحوهٔ اجرای این شرایط تا حدودی متفاوت است ولی هیچ ضرورتی وجود ندارد که اقدام دفاعی از لحاظ ماهیت و طبیعت مانند حملهٔ انجام‌شده باشد. بنابراین یک استفاده از زور سایبری می‌تواند برای دفاع در مقابل یک حملهٔ جنبشی به کار رود یا بالعکس.

همچنین هرچند که در قواعد حقوق بین‌الملل بشردوستانه و معاهدات حاکم بر آن به‌خصوص کنوانسیون‌های ۱۹۴۹ ژنو و پروتکل‌های الحاقی به آنها، اشارهٔ معینی به حملات کامپیوتری نشده است، اما چون حملات کامپیوتری می‌توانند به‌عنوان یک وسیله و روش جنگ به‌کار روند و توانایی ورود صدمه به غیرنظامیان را هم دارند و نیز با توجه به شرط مارتنس، قواعد حقوق بین‌الملل بشردوستانه از جمله اصل تفکیک میان اهداف نظامی و غیرنظامی در جنگ‌های سایبری هم قابل اعمال هستند، اما به دلیل طبیعت متفاوت حملات سایبری نسبت به سایر سلاح‌های کلاسیک، نحوهٔ اعمال این قواعد در جنگ‌های سایبری تا حدودی متفاوت است.

در مورد پیشینه یا سوابق علمی موضوع باید گفت با آنکه حملات سایبری و قواعد حقوق بین‌الملل قابل اعمال در این‌گونه حملات به یکی از مهم‌ترین موضوعات علمی و پژوهشی در حقوق بین‌الملل به‌عنوان یکی از مواردی که امنیت دولت‌ها را تهدید می‌کند، تبدیل شده است، تحقیقات اندکی دراین‌خصوص در داخل کشور صورت گرفته است و برخی مقالات و تعداد محدودی پایان‌نامه کارشناسی‌ارشد و دکترا به رشتهٔ تحریر درآمده‌اند که به بررسی برخی جنبه‌های خاص حملات سایبری پرداخته‌اند که جهت پاسخگویی به سؤالات طرح‌شده در این کتاب کافی به نظر نمی‌رسند و به بررسی کلیهٔ ابعاد جنگ‌های سایبری و قابلیت اعمال قواعد حقوق مخاصمات مسلحانهٔ بین‌المللی در این‌گونه از نبردها نپرداخته‌اند و بیشتر بر بررسی موضوعاتی از قبیل بررسی آثار ویروس استاکس‌نت در حمله ۲۰۱۰ به تأسیسات هسته‌ای ایران،

جایگاه اقدامات متقابل در مقابل حملات سایبری، حقوق بین‌الملل عمومی و صلاحیت‌ها در فضای مجازی، مسئولیت دولت‌ها در قبال حملات سایبری و ... پرداخته‌اند.

اما درخصوص پیشینه موضوع در خارج از کشور، مسئله حملات سایبری و بررسی ابعاد مختلف آن در حقوق بین‌الملل، از جمله مواردی است که منابع پرشماری به زبان انگلیسی در دسترس محقق قرار دارد و به‌خصوص با تهیهٔ دو سند مهم در سال‌های اخیر، سازمان پیمان آتلانتیک شمالی (ناتو) در این زمینه تلاش‌های مؤثری نموده است. سند اول به سفارش مرکز عالی همکاری‌های دفاع سایبری ناتو[1]، با عنوان «دستورالعمل تالین درباره حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری[2]» بوده و سند دوم، «دستورالعمل تالین ۲ درباره قواعد حقوق بین‌الملل قابل اعمال در عملیات سایبری[3]» می‌باشد که با توجه به موضوع این کتاب که بر بررسی جنگ‌های سایبری تمرکز دارد از سند اول که درخصوص قواعد حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری می‌باشد، استفاده شده و در پایان کتاب نیز نقدی بر این سند ارائه گردیده است.

در نگارش مطالب این کتاب از روش تحقیق توصیفی ـ تحلیلی استفاده شده است و در قسمت‌هایی که به توضیح قواعد موجود حقوق بین‌الملل در باب توسل به زور، قواعد مسئولیت بین‌المللی، قواعد حقوق مخاصمات مسلحانه و قواعد حقوق بین‌الملل بشردوستانه پرداخته شده، از روش توصیفی استفاده شده است، اما قسمت‌هایی که به انطباق مفهوم حملات سایبری با مفهوم حملهٔ مسلحانه و تطبیق مصادیق موجود بر مفهوم موردنظر و قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری می‌پردازد، تلاش شده که با تحلیل‌های ارائه‌شده ابعاد مبهم موضوع روشن گردد.

به‌عنوان نکته پایانی درخصوص ساخت این کتاب، باید گفت که این پژوهش در دو بخش تهیه گشته است. بخش اول به جنگ سایبری و حقوق بین‌الملل توسل به زور می‌پردازد و مطالب آن در سه فصل ارائه می‌شود. فصل اول جنگ سایبری و دفاع مشروع در حقوق بین‌الملل را مورد بررسی قرار می دهد. فصل دوم از بخش اول حملات سایبری و اصل عدم مداخله را مطرح می‌کند و فصل سوم نیز به قابلیت انتساب در حملات سایبری می‌پردازد.

---

1. The Nato Cooperative Cyber Defence Centre of Excellence (CCDCOE).
2. Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, General Editor: Michael N.Schmitt, Cambridge University Press, New York , 2011.
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Schmitt, M. (2017).

بخش دوم این کتاب پس از اثبات این موضوع که حملات سایبری درمواردی خاص می‌توانند به آستانهٔ لازم برای ایجاد یک مخاصمه مسلحانهٔ بین‌المللی برسند، به قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری پرداخته و از پنج فصل تهیه گردیده است. فصل اول اعمال قواعد حقوق بین‌الملل بشردوستانه در حملات شبکه‌ای کامپیوتری را مورد بررسی قرار داده است و در سایر فصول به بررسی مواردی از چگونگی اجرای این قواعد در جنگ‌های سایبری پرداخته می‌شود که این موارد در فصل دوم به موضوع وسایل و روش‌های جنگ اختصاص یافته، در فصل سوم ممنوعیت شیوه‌های خائنانه مورد بررسی قرار گرفته است، در فصل چهارم با پرداختن به بحث اشغال، ارتباط موضوع با عملیات سایبری مورد تحلیل قرار گرفته و در فصل پنجم با پرداختن به موضوع بی‌طرفی، چگونگی اجرای این قواعد در مخاصمات سایبری مطرح می‌گردد.

بخش اول:
جنگ سایبری
و حقوق بین‌الملل توسل به زور

منع توسل به زور و تحریم جنگ یکی از بنیادی‌ترین اصول حقوق بین‌الملل معاصر می‌باشد که به آستانهٔ یک قاعدهٔ آمره رسیده و سنگ‌بنای منشور ملل متحد محسوب می‌گردد و درواقع حفظ صلح و امنیت بین‌المللی در گرو رعایت این امر است. در طول تاریخ بشریت ما شاهد بروز جنگ میان کشورهای مختلف بوده‌ایم و ابزار جنگ در طول تاریخ از مشت و شمشیر به سلاح‌های مدرن امروزی تحول یافته است. در سال‌های اخیر نیز حملات سایبری با آثار مخربی که به بار آورده‌اند خود را به‌عنوان یکی از مصادیق تهدیدکننده صلح و امنیت بین‌المللی نشان داده و جامعهٔ بین‌المللی را در مقابل این پرسش قرار داده‌اند که آیا حملات سایبری می‌توانند به‌عنوان توسل به زور محسوب و در پرتو قواعد حق بر جنگ مورد تحلیل قرار گیرند؟

بنابراین با توجه به ضرورت ارزیابی حملات سایبری به‌عنوان یکی از اشکال توسل به زور، بخش اول این کتاب به حوزهٔ حق بر جنگ اختصاص داده شده و مطالب در قالب سه فصل ارائه می‌گردد. در فصل اول به بررسی این مسئله پرداخته می‌شود که آیا اساساً حملات سایبری را می‌توان به‌عنوان توسل به زور محسوب نمود و برای دولت قربانی حق دفاع مشروع از خود را در نظر گرفت؟ در فصل دوم این مسئله مورد ارزیابی قرار می‌گیرد که چگونه اصل عدم مداخله در حملات سایبری که به آستانهٔ لازم برای ایجاد یک حملهٔ مسلحانه نرسیده‌اند، قابل اعمال است و شرایط اقدامات متقابل در برابر حملات سایبری چیست و در فصل سوم به قواعد حاکم بر مسئولیت بین‌المللی دولت‌ها در زمینهٔ حملات سایبری پرداخته می‌شود و معیارهای حقوق بین‌الملل در باب قابلیت انتساب مورد تحلیل قرار می‌گیرند.