مطالعات حقوق انرژی، دورهٔ ۶، شمارهٔ ۱، بهار و تابستان ۱۳۹۹، صفحات ۱۹۳ - ۱۷۳

حمایت از زیرساخت‌های انرژی در مخاصمات مسلحانهٔ بین‌المللی

غلامعلی قاسمی*
دانشیار گروه حقوق بین‌الملل دانشکدهٔ حقوق دانشگاه قم
محمد عاکفی قاضیانی
دانشجوی دکتری حقوق بین الملل، گروه حقوق بین الملل، دانشکده حقوق، دانشگاه قم

(تاریخ دریافت: ۱۳۹۹/۲/۲۸ - تاریخ تصویب: ۱۳۹۹/۵/۲۷)

چکیده

زیرساخت‌های انرژی از منظر اقتصادی و اجتماعی اهمیت بسزایی برای کشورها دارد. وقوع مخاصمات مسلحانهٔ بین‌المللی، این زیرساخت‌ها را در معرض تخریب و یا اختلال قرار می‌دهد. با توسعهٔ فناوری، این زیرساخت‌ها با تهدیدات نوین سایبری نیز روبه‌رو شده است. بنابراین، حمایت‌های حقوقی بین‌المللی و حقوق بشردوستانه از این تأسیسات ضرورت بیشتری پیدا می‌کند. این حمایت‌های حقوقی به موجب حقوق بین‌الملل بشر و حقوق بشردوستانه قابل اعمال است. مقررات کنوانسیون‌های ژنو و پروتکل الحاقی اول، نقش مهمی در این خصوص ایفا می‌کند. این مقاله با هدف درک ماهیت الزامات حقوقی بین‌المللی در این زمینه و دریافت کیفیت این قواعد و مقررات، با شیوهٔ توصیفی و تحلیلی نگاشته شده است و به این نتیجه می‌رسد که حمایت‌های مقرر در این اسناد، به واسطهٔ پدیداری شیوه‌های نوین جنگی و گسترش روزافزون تهدیدات علیه زیرساخت‌های انرژی، تا حدود زیادی ناکارآمد جلوه می‌نماید. نوآوری‌های دولت‌ها و سازمان‌های بین‌المللی برای تدوین قواعد و مقررات حقوقی نیز کُند و عمدتاً با ماهیت حقوقی غیرالزام‌آور همراه بوده است.

واژگان کلیدی

حقوق بشردوستانه، حملهٔ سایبری، زیرساخت‌های انرژی، قاعدهٔ عرفی، مخاصمهٔ مسلحانه.

* نویسندهٔ مسئول
Email: g.ghasemi43@gmail.com

مقدمه

محرومیت از انرژی مشکلات متعددی در دوران صلح به بار می‌آورد که پیامدهای ویرانگرش در هنگام مخاصمات مسلحانهٔ بین‌المللی که خطرناک‌ترین وضعیت‌ها برای زندگانی بشر می‌باشد، دوچندان است. موانع پیش روی دستیابی به انرژی[1]، اغلب در مواقع مخاصمات مسلحانه افزایش می‌یابد و به میزان چشمگیری امکان درمان مجروحان نظامی و غیرنظامی را کاهش می‌دهد. از سوی دیگر، زیرساخت‌های تولید برق عمدتاً با استناد به ضرورت نظامی[2]، به عنوان اهداف با اهمیت از حیث نظامی تخریب می‌شوند. پیامدهای اختلال و یا قطع خدمات انرژی، حیات غیرنظامیان را نیز تهدید می‌کند. براساس گزارش‌ها، در جنگ دوم خلیج فارس در سال ۱۹۹۱، یعنی اشغال کویت توسط عراق و حملهٔ نیروهای ائتلاف بین‌المللی به رهبری آمریکا به عراق، قسمت اعظم کشتارها، نه بر اثر بمباران، بلکه به دنبال تخریب شبکهٔ برق و در نتیجه، فروپاشی نظام سلامت همگانی و آب و فاضلاب و درپی آن شیوع اسهال خونی، وبا و دیگر بیماری‌های ناشی از آب بوده است (Ngai, 2012: 582-583). امروزه با پیشرفت فناوری، زیرساخت‌های حیاتی[3] کشورها، به‌ویژه زیرساخت‌های انرژی، به شکل سامانه‌های فیزیکی- سایبری گسترده‌ای درآمده‌اند که بیش از پیش نیازمند حمایت در برابر حملات فیزیکی و یا سایبری هستند. این زیرساخت‌ها، به‌ویژه در برابر تهاجمات تلفیقی سایبری- فیزیکی که احتمالاً در آینده شکل غالب تهدیدات خواهد بود، نیاز به حمایت دوچندان دارند (CEIS-SG, November 2018: 7). اما این زیرساخت‌ها چیست؟ چه حمایت‌هایی در حقوق بین‌الملل و حقوق مخاصمات مسلحانه از این زیرساخت‌های انرژی به عمل آمده است؟ وضعیت مقررات و اسناد بین‌المللی در مورد زیرساخت‌های انرژی، به‌ویژه در مخاصمات مسلحانهٔ بین‌المللی چگونه است؟ بررسی و پاسخ به این پرسش‌ها دارای وصف میان‌رشته‌ای است که در این نوشتار، به اختصار از منظر حقوق انرژی، حقوق بین‌الملل بشر و حقوق مخاصمات مسلحانه انجام شده است.

۱. زیرساخت‌های انرژی

زیرساخت، تجهیزاتی مستقر است که برای حمایت از فناوری حمل‌ونقل، ارتباطات، فعالیت‌های دولتی و صنایع ضرورت دارد. زیرساخت‌ها، تولید کالا و خدمات و

1. Energy Access
2. Military Necessity
۳. زیرساخت حیاتی (Critical Infrastructure)، زیرساختی است که توقف یا تخریب آن، تأثیر چشمگیری بر سلامت، ایمنی، امنیت، اقتصاد و بهبود اجتماعی خواهد داشت. تعطیلی اینگونه زیرساخت‌ها، حتی ممکن است به ورود خسارات اقتصادی به یک یا چند کشور دیگر و زیرساخت‌هایشان بینجامد (Zio, 2016: 137-150).

تحقق مصالح عمومی در حوزه‌هایی همچون آموزش، نظام سلامت و نیز تأمین انرژی را تسهیل می‌کنند. زیرساخت‌های انرژی[1]، تولیدکنندگان و مصرف‌کنندگان انرژی را در فواصل جغرافیایی گوناگون، به هم متصل می‌کند. این زیرساخت‌ها نفت و فرآورده‌های نفتی، گاز و برق را برای مردم و کارخانه‌ها فراهم می‌آورد (Kuzemco et al., 2016: 169). زیرساخت‌های انرژی شامل سه دستهٔ عمده می‌شوند: ۱. شبکه‌های تولید، انتقال و توزیع حامل‌های انرژی، از جمله چاه‌های نفت و گاز، لوله‌های نفت و گاز، نفت‌کش‌ها، شبکه‌های برق، سیستم‌های گرمایش و سرمایش منطقه‌ای که گاز، برق، گرما و یا سرما را انتقال می‌دهند؛ ۲. واحدهای تبدیل انرژی همچون پالایشگاه‌ها، بویلرهای تولید گرما[2]، نیروگاه‌های تولید برق، نیروگاه‌های تولید هم‌زمان برق و گرما[3]، پمپ‌های حرارتی و فناوری‌هایی که برق را به سوخت‌هایی مانند هیدروژن و متان تبدیل می‌کنند؛ ۳. مخازن ذخیره‌سازی انرژی که گاز، برق یا ترکیبات شیمیایی[4] را در بازهٔ زمانی کوتاه یا بلند ذخیره می‌کند (Guelpa et al., 2019: 4). البته امروزه اصطلاح «زیرساخت انرژی»، قلمرو گسترده‌تری از تسهیلات را که شامل قطارهای زغال سنگ، سامانه‌های کنتور برق، ساختمان‌های هوشمند و سامانه‌های کنترل نیروگاه‌های تولید برق می‌شود نیز دربر می‌گیرد (Cecchetti & Jakson, 2017: 17)[5]. از آنجا که رشد اقتصادی کشورها به این زیرساخت‌ها گره خورده است، بخش مهمی از سرمایهٔ مادی جوامع شمرده می‌شوند. مؤسسهٔ جهانی مک کینزی[6] برآورد کرده است که «زیرساخت‌ها، از جمله زیرساخت‌های انرژی به طور متوسط تقریباً معادل هفتاد درصد تولید ناخالص داخلی کشورها را تشکیل می‌دهد» (Kuzemco et al., 2016: 169). برنامه‌ریزان نظامی هم غالباً به لحاظ راهبردی در جریان حملات و یورش‌ها، زیرساخت‌های انرژی را به عنوان هدف اولیه انتخاب می‌کنند. پژوهشی که پس از جنگ، در مورد نبرد هوایی سال ۱۹۹۱ خلیج فارس انجام شد، آشکار ساخت که راهبرد آمریکا فراتر از بمباران نیروهای مسلح و اهداف نظامی بوده و شامل آماج‌های دیگری هم شده است. در نخستین موج حملات هوایی سال ۱۹۹۱، بیش از بیست نیروگاه برق و سه رآکتور هسته‌ای مورد حمله قرار گرفته‌اند (سوواکول، ۱۳۹۱: ۵۸-۵۹). امروزه در بسیاری از کشورهای دارای ذخایر عظیم

1. Energy Infrastructure
2. Heat only boilers (gas to heat)
3. Cogeneration Plants (gas to heat and power)
4. Chemical species
5. https://www.designingbuildings.co.uk/wiki/Energy infrastructure
6. McKinsey Global Institute

نفت و گاز نیز مخاصمات مسلحانه موجب می‌شود که هزینه‌های سرمایه‌گذاری در این کشورها افزایش یافته، تولید و بهره‌برداری متوقف شود و از همه مهم‌تر، تأسیسات و پایانه‌های نفتی مورد حملهٔ نظامی قرار گیرد (امین‌زاده و دیگران، ۱۳۹۷: ۶۹).

۲. زیرساخت‌های انرژی در مخاصمات مسلحانهٔ بین‌المللی

اصطلاح «مخاصمهٔ مسلحانه»[1]، نخست در کنوانسیون‌های ژنو به‌کار رفت (برادران و حبیبی، ۱۳۹۸: ۱۴۳). مادهٔ ۲ مشترک کنوانسیون‌های ژنو، مخاصمهٔ مسلحانه میان دو یا چند کشور را فارغ از این‌که رسماً وضعیت جنگی میان آن‌ها اعلام شده باشد یا خیر، مخاصمهٔ مسلحانهٔ بین‌المللی می‌نامد (Geneva Conventions I-IV, 1949, Common Art: 2). عملیات نظامی سازمان‌های بین‌المللی علیه دیگر کشورها نیز در شمار مخاصمات مسلحانهٔ بین‌المللی تلقی می‌شود (ضیائی بیگدلی، ۱۳۹۶: ۵۱). مخاصمات مسلحانه در مواردی که بازیگران غیردولتی[2] همچون گروه‌های تروریستی و شورشی متخاصم، تحت کنترل کلی دولتی دیگر باشند نیز بین‌المللی تلقی خواهد شد (برادران و حبیبی، ۱۳۹۸: ۱۴۵). پای مقولهٔ انرژی در مخاصمات مسلحانه از سه طریق به میان می‌آید: ۱. انرژی در صحنهٔ مخاصمات مسلحانه در قالب موشک‌ها و جنگ‌افزارها به یک‌باره آزاد می‌شود؛ ۲. جنگ‌های امروزی متکی به تسلیحاتی هستند که ساخت و تولید آن‌ها نیازمند انرژی و مواد انرژی‌بر است؛ ۳. جنگ‌ها به زیرساخت‌های انرژی خسارت می‌زنند. در جنگ‌های امروزی تأسیسات تولیدکنندهٔ برق، ذخایر نفت و گاز و سکوهای نفتی در میان اهداف اولیه برای تخریب قرار دارند. این زیرساخت‌ها در بسیاری از موارد، اهداف نظامی قلمداد شده است؛ برای مثال، در مخاصمهٔ سال ۲۰۱۴ میان روسیه و اوکراین، زیرساخت‌های انرژی هدف حملات نظامی روسیه قرار گرفت (Cecchetti & Jakson, 2017: 16). این کشور تنها شبه‌جزیرهٔ کریمه را به خاک خود ملحق نکرد، بلکه زیرساخت‌های انرژی در کریمه و تأسیسات روی آب در دریای سیاه را نیز تصاحب کرد (Ruhle, 2017: 5). بر این‌گونه مخاصمات، قواعد حقوق بین‌الملل و حقوق بشردوستانه حاکم است (ضیائی بیگدلی، ۱۳۹۶: ۵۱). البته وقوع مخاصمهٔ مسلحانه، دولت‌ها را از اجرای موازین حقوق بشری معاف نمی‌سازد (حاتمی، ۱۳۹۷: ۹۹). اگرچه موازین حقوق بشر در همهٔ زمان‌ها، مکان‌ها و نسبت به تمامی افراد لازم‌الاتباع است (UN. Doc. A/8052, September 1970)، اما این حقوق بشردوستانه است که در جریان مخاصمات مسلحانهٔ بین‌المللی ماهیت حقوقی خاص[3] دارد و بررسی قواعد و مقررات آن اهمیت دوچندانی می‌یابد (Ngai, 2012: 584-588). به منظور احراز حمایت‌های حقوقی از

1. Armed conflict
2. Non-State actors
3. "lex specialis derogat legi generali"

زیرساخت‌های انرژی در جریان مخاصمات مسلحانهٔ بین‌المللی باید به دو دسته قواعد و مقررات رجوع کرد؛ دستهٔ اول، حمایت‌های قراردادی است که از برجسته‌ترین آن‌ها، مقررات کنوانسیون‌های چهارگانهٔ ژنو ۱۹۴۹ و پروتکل اول الحاقی[۱] ۱۹۷۷ است؛ دستهٔ دوم نیز اصول کلی حقوق بشردوستانه است که برخی از این اصول امروزه ماهیت حقوق عرفی نیز یافته است. اهمیت این زیرساخت‌ها موجب شده است که بازیگران بین‌المللی همچون دولت‌ها و سازمان‌ها، برای حمایت از آن‌ها به طور مشترک یا جداگانه سیاست‌هایی را اجرایی کنند. تقویت سازمان‌های بین‌المللی و در رأس آن سازمان ملل، می‌تواند نقش مهمی در حمایت از زیرساخت‌های انرژی، به واسطهٔ اتخاذ اقدامات پیشگیرانه، تنش‌زدایی و یا حل‌وفصل اختلافات ایفا کند (ممتاز و رنجبریان، ۱۳۸۶: ۲۹۴). سازمان پیمان آتلانتیک شمالی نیز همواره در حمایت از زیرساخت‌های انرژی نقش‌آفرینی کرده است. حملات به نفت‌کش‌ها در خلیج عدن و تنگهٔ باب‌المندب، این سازمان را بر آن داشت تا از سال ۲۰۰۹ به اعمال گشت‌های دریایی برای تضمین امنیت انرژی در این ناحیه بپردازد[۲] (Dugulin & Cussac, 2015: 91-92). عملیات ارادهٔ جدی[۳]، عملیات طوفان صحرا[۴]، عملیات مجاهدت فعال[۵]، عملیات آزادی عراق[۶]، عملیات آتلانتا[۷] و عملیات سپر اقیانوس[۸]، همگی فعالیت‌های نظامی است که ناتو و یا اعضای این سازمان به طور جداگانه عهده‌دار شده و بدین‌وسیله برقراری امنیت در حمل‌ونقل انرژی و حمایت از زیرساخت‌های انرژی را دنبال کرده‌اند (Endicott, 2010: 37). رهبران ناتو آشکارا حمایت خود از اقدامات بین‌المللی در ارزیابی مخاطرات متوجه زیرساخت‌های انرژی و ارتقای امنیت آن‌ها را در بیانیهٔ پایانی اجلاس ریگا اعلام داشته و اجلاس دایمی شورای آتلانتیک شمالی را به بررسی مخاطرات قریب‌الوقوع حوزهٔ امنیت انرژی، جهت نقش‌آفرینی سازمان موظف ساخته‌اند (Riga Summit Declaration, November 2006, Para. 45).

۱. پروتکل حمایت از قربانیان مخاصمات مسلحانهٔ بین‌المللی، ۱۹۷۷.

2. Operation Ocean Shield (2009).
3. Operation Earnest Will (1987-1988).
4. Operation Desert Storm (1991).
5. Operation Active Endeavour (2001-2016).
6. Operation Iraqi Freedom (2003-2011).
7. Operation Atalanta (2008- present).
8. Operation Ocean Shield (2009-2016).

۲. ۱. حملات سایبری و زیرساخت‌های انرژی

به دنبال توسعهٔ فناوری اطلاعات و ارتباطات، به‌ویژه گسترش فضای سایبر از طریق اینترنت اشیا[۱]، حملات سایبری[۲] به‌مثابه شیوهٔ جدید جنگی مورد توجه بسیاری قرار گرفته است (U.S. Department of Energy, 2018: 9). این حملات، نوعی وجه اخلاقی و حقوقی نیز در مقایسه با شیوه‌های کلاسیک نظامی یافته‌اند؛ زیرا بدین‌سان طرفین مخاصمه می‌توانند بدون ایراد خسارات فیزیکی یا تحمیل تخریب دایمی، به مقاصد خود در جریان مخاصمات مسلحانه دست یابند. عملیات سایبری منتسب به اسرائیل علیه سامانهٔ دفاع هوایی سوریه در سال ۲۰۰۷، یا حملهٔ ویروسی خرس پُرانرژی[۳] به تأسیسات نزدیک به ۲۵۰ شرکت فعال در حوزهٔ انرژی در ایالات متحده و اروپای غربی بین سال‌های ۲۰۱۱ و ۲۰۱۴ (Desarnaud, 2017: 18)، از برجسته‌ترین این حملات است (Gisel & Olejnik, 2018: 14-15). بنابر گزارش وزارت امنیت داخلی آمریکا، بخش انرژی متحمل بیشترین حملات سایبری نسبت به دیگر بخش‌هاست و در سال‌های ۲۰۱۳–۲۰۱۵، نزدیک به ۳۵ درصد حملات ناظر به همین صنایع بوده است (U.S. Department of Energy, 2018: 9). حملات سایبری علیه زیرساخت‌های انرژی، از دههٔ هشتاد میلادی مورد ثبت و شناسایی قرار گرفته است. اما پس از کشف ویروس استاکس‌نت در سال ۲۰۱۰ بود که شوک جدیدی در صنعت انرژی پدید آمد. این حملات موجب پیدا شدن نقاط ضعف و روشن شدن ابعاد مهم سیاسی و اقتصادی حملات سایبری علیه صنایع انرژی شد. از آن زمان، این‌گونه حملات روند فزاینده‌ای را نشان می‌دهد؛ به گونه‌ای که بین سال‌های ۲۰۱۴ و ۲۰۱۵، شاهد رشد ۳۸۰ درصدی این حملات بوده‌ایم (Desarnaud, 2017: 19-21). بدین‌ترتیب، حملات سایبری را باید معضل قرن ۲۱ دانست که حتی می‌تواند بازارهای اقتصادی را فلج کند؛ از جمله در رآکتورهای هسته‌ای یا سامانهٔ کنترل سدها و آب‌بندها اخلال ایجاد کرده و در نتیجه، خسارات هنگفتی به بار آورد (قاسمی و نامدار، ۱۳۹۷: ۲۰۰–۲۰۱). روند رو به افزایش این حملات، موجب شده است که بررسی تهدیدات سایبری علیه زیرساخت‌های انرژی به عنوان شیوهٔ نوین جنگی، از اهمیت بسزایی برخوردار باشد. از نظر تحلیلی نیز جنگ در این فضا به منزلهٔ یکی از روش‌های جنگ، و فضای سایبر به منزلهٔ میدان جنگ مورد توجه

---

۱. ایترنت اشیا (Internet of things) مفهومی است که کاربردهای متعددی را به واسطهٔ هم‌گرایی میان اشیای هوشمند و اینترنت و ایجاد یکپارچگی میان فضای مجازی و دنیای واقعی به ارمغان می‌آورد. کارکردهای اینترنت اشیا طیف گسترده‌ای، از لوازم خانگی خانه‌ای هوشمند تا تجهیزات پیشرفتهٔ کارخانه‌های صنعتی را دربر می‌گیرد (Zarpelo et al., 2017: 25-37).

۲. عمده عملیاتی که از آن، به حملهٔ سایبری تعبیر می‌شود، مصداق توسل به زور نیست و پایین‌تر از حملهٔ مسلحانه قلمداد می‌شود. بنابراین، باید حملات سایبری را از تهدیدات امنیتی سایبری همچون فعالیت مجرمانهٔ سایبری، جاسوسی سایبری و انواع دیگر نفوذ و خرابکاری در سامانه‌های رایانه‌ای جدا کرد (قاسمی و نامدار، ۱۳۹۷: ۲۱۰–۲۲۸).

3. Energetic Bear

قرار گرفته است (اسمعیل‌زاده ملاباشی و دیگران، ۱۳۹۶: ۵۳۹)؛ به گونه‌ای که اعضای ناتو در اجلاس سال ۲۰۱۶ در ورشو، فضای سایبر را به عنوان پنجمین عرصهٔ عملیاتی خود پس از زمین، دریا، هوا و فضا، به رسمیت شناختند (Jakson et al., 2017: 31).

حملات سایبری، حقوق بین‌الملل بشردوستانه را نیز به چالش کشیده است (Clapham & Gaeta, 2014: 33). تاکنون بسیاری از ابعاد حملات سایبری مورد اتفاق حقوق‌دانان قرار نگرفته است. حقوق جنگ و حقوق بین‌الملل عرفی، خالی از قواعد اختصاص‌یافته به فضای مجازی هستند (Solis, 2016: 674). نه کنوانسیون خاصی در این زمینه وجود دارد و نه عرف بین‌المللی یکسانی که حقوق و تکالیف دولت‌ها را تعیین کند (قاسمی و نامدار، ۱۳۹۷: ۲۰۱). عملکرد دولت‌ها در تفسیر هنجارهای حقوقی این حوزه از مخاصمات نیز بسیار کند پیش می‌رود. با وجود این، اعمال قواعد حقوق توسل به زور[1] و حقوق بشردوستانه[2] در خصوص حملات سایبری منعی ندارد (Solis, 2016: 674). در همین راستا، دستورالعمل تالین[3] مقرر می‌دارد که چنانچه توسل به زور، به صدمه، قتل، خسارت یا تخریب اموال بینجامد، می‌توان آن را به عنوان حملات موضوع حقوق بشردوستانه شناسایی کرد[4] و تابع قواعد و مقررات این حوزه دانست (Schmitt, 2017: 415). امروزه در مورد این‌که حملات نابودگر یا حملاتی که موجب خسارات جدی به اموال می‌شود، ماهیت حملهٔ مسلحانه را داراست، اتفاق‌نظر وجود دارد. این حملات لزوماً نباید گسترده باشد؛ از این رو، حملهٔ سایبری‌ای که موجب قتل، صدمه، خسارت یا تخریب تنها یک هدف باشد نیز حملهٔ مسلحانه شمرده می‌شود (Valo, 2014: 62). با وجود این، بسیاری از مفاهیم حقوق بشردوستانه همچون اهداف نظامی، حملات نظامی، خیانت و مشارکت مستقیم در حملات، هم‌خوانی لازم را با واقعیت فضای مجازی ندارد. ماهیت یکپارچه و طبیعت دووجهی فضای سایبری، اعمال اصولی همچون اصل تفکیک را نیز دشوار و یا حتی ناممکن می‌سازد (Sassoli, 2019, Para.10.6). شکل‌گیری قواعد حقوق بین‌الملل عرفی در این زمینه نیز با چالش‌هایی روبه‌رو بوده است؛ از جمله این‌که دولت‌ها عمدتاً نسبت به افشای دستاوردها و اطلاعات خود راجع به عملیات سایبری محتاطانه عمل می‌کنند؛ زیرا در این صورت توانایی‌هایشان در این فضا که از قضا برای تأمین امنیت آن‌ها اهمیت دارد، آشکار خواهد شد (Allhoff et al., 2016: 49-51). از این رو، احراز «عنصر مادی»[5] و رویهٔ دولت‌ها، جهت

1. Jus ad bellum
2. Jus in bello
۳. دستورالعمل تالین (Tallinn Manual)، نظام‌نامه‌ای غیرالزام‌آور راجع به اعمال حقوق بین‌الملل نسبت به عملیات در فضای مجازی است که توسط مرکز عالی مشارکت در دفاع سایبری ناتو، مستقر در تالین تهیه شده است. این دستورالعمل بر ابعاد حقوقی عملیات سایبری که به‌مثابه حملات مسلحانه باشد، متمرکز است (Leetaru, 2017).
4. Tallinn Manual 2.0, Rule 92, February 2017.
5. Objective element (State practice)

شکل‌گیری قواعد حقوق بین‌الملل عرفی در این زمینه با دشواری روبه‌رو شده است[۱] (زرنشان، ۱۳۹۳: ۷۸-۷۹). بدین‌ترتیب، هنجارهای حقوقی قابل اعمال بر فضای سایبر را نیز باید در پرتو تفسیر قواعد عرفی موجود جست‌وجو کرد (Allhoff et al., 2016: 49-51). پُرواضح است که نویسندگان کنوانسیون‌های صلح لاهه و کنوانسیون‌های چهارگانهٔ ژنو قادر به تصور ابعاد حقوقی نوین چنین مخاصماتی نبوده‌اند؛ از این رو، کاستی‌های قواعد حقوق بشردوستانهٔ قابل اعمال در این عرصه امری طبیعی است (Clapham & Gaeta, 2014: 252-253). چگونگی تسری قواعد ناظر بر مخاصمات مسلحانهٔ فیزیکی و کلاسیک، به شیوه‌های نوین جنگی همچون جنگ سایبری[۲]، جنگ الکترونیک[۳]، جنگ فضایی[۴] و جنگ اطلاعاتی[۵]، از مهم‌ترین این کاستی‌هاست (Clapham & Gaeta, 2014: 33-34). برای قاعده‌مندسازی رفتار دولت‌ها در فضای سایبر تاکنون نوآوری‌های متعددی به‌کار بسته شده است که از آن جمله می‌توان به پیشنهاد تصویب قطعنامهٔ «تحولات عرصهٔ اطلاعات و ارتباطات در چهارچوب امنیت بین‌المللی»[۶] از سوی مسکو به مجمع عمومی سازمان ملل در سال ۱۹۹۸ (A/54/213)، ایجاد «گروه کارشناسان دولتی سازمان ملل در خصوص ارتقای رفتار مسئولانهٔ دولت‌ها در فضای سایبر و در چهارچوب امنیت بین‌الملل»[۷] به سال ۲۰۰۴، «پیش‌نویس معاهدهٔ امنیت بین‌المللی اطلاعات»[۸] تهیه‌شده از سوی روسیه، «کنوانسیون جرایم سایبری بوداپست»[۹]، مجموعهٔ قواعد رفتاری تهیه‌شده از سوی روسیه و چین با مشارکت برخی اعضای سازمان همکاری شانگهای در سال‌های ۲۰۱۱ و ۲۰۱۵ (A/69/723; A/66/359)، کنفرانس جهانی فضای سایبر[۱۰] و نیز تأسیس «گروه کاری نامحدود راجع به پیشرفت‌های حوزهٔ اطلاعات و فناوری ارتباطات در چهارچوب

---

۱. لازم به ذکر است که در نظریه‌های کلاسیک، اصرار بر رویهٔ دولت‌ها و اعمال فیزیکی بود، اما در رویکرد مدرن به عنصر معنوی بیشتر توجه می‌شود. از این رو، گروهی از حقوق‌دانان، نظریهٔ «دوعنصری» را کنار گذاشته و به نظریهٔ «تک‌عنصری» در شکل‌گیری قواعد عرفی اقبال نشان داده‌اند. به باور این گروه، رویهٔ دولت‌ها نقش مستقیم در شکل‌گیری عرف ندارد و تنها می‌تواند رویکرد دولت‌ها نسبت به یک قاعده را تحت تأثیر قرار دهد (Guzman, 2005: 122).

2. Cyber warfare
3. Electronic warfare
4. Space warfare
5. Information warfare
6. Developments in the field of information and telecommunications in the context of international security (A/RES/53/70).
7. The United Nations Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security.
8. Draft Convention on International Information Security, 2011.
9. Convention on Cybercrime, 2001.

۱۰. کنفرانس جهانی فضای سایبر، مجموعه‌ای از نشست‌های دو سالانه است که از سال ۲۰۱۱، با هدف ایجاد قواعد مورد توافق بین‌المللی راجع به رفتار در فضای سایبر و با مشارکت دولت‌ها، سیاست‌گذاران، بخش خصوصی و متخصصان فضای مجازی برگزار شده است (برای اطلاع بیشتر، ر.ک: "Global Conference on Cyber Space (GCCS 2017)", available at: https://www.internetsociety.org/events/gccs-last accessed on 5 April 11, 2020, (2017/

امنیت بین‌الملل»[1] در سال ۲۰۱۸ توسط مجمع عمومی سازمان ملل، اشاره داشت (Tikk & Kerttunen, 2017: 4; A/RES/73/27). کمیتهٔ بین‌المللی صلیب سرخ نیز در جریان «کنفرانس شصت سالگی کنوانسیون‌های ژنو و دهه‌های پیش رو»[2]، چالش‌ها، تهدیدات و شیوه‌های نوین جنگی را به بحث و گفت‌وگو گذاشت. بیشتر شرکت‌کنندگان این کنفرانس، قائل به قابلیت قواعد حقوق مخاصمات مسلحانه، جهت اعمال نسبت به چالش‌های جدید، از جمله حملات سایبری بودند (Kodar, 2012: 110-111). این کمیته همواره عملکرد دولت‌ها در فضای سایبر را زیر نظر داشته است. در همین راستا، کمیتهٔ بین‌المللی صلیب سرخ خطاب به نشست سال ۲۰۱۷ کمیتهٔ اول مجمع عمومی سازمان ملل، توجه این نهاد را به روند رو به رشد حملات سایبری که عملکرد شبکه‌های برق، مراکز پزشکی و نیروگاه‌های هسته‌ای را هدف قرار می‌دهد، جلب کرد و تصریح داشت که حقوق بین‌الملل بشردوستانه در خصوص کاربرد توانایی‌های سایبری به‌مثابه شیوه و روشی جنگی، هنگام مخاصمات مسلحانه قابل اعمال بوده و آن را محدود و مقید می‌سازد. بدین‌ترتیب، حملات سایبری علیه اهداف و شبکه‌های غیرنظامی ممنوع بوده و اینگونه حملات، بدون رعایت اصل تفکیک و تناسب میان اهداف نظامی و غیرنظامی مورد نهی قرار گرفته است (Christen et al., 2020: 355). امروزه شدت آثار حملات سایبری، بسیاری از حقوق‌دانان و پژوهشگران را به احراز آستانهٔ مخاصمهٔ مسلحانه، برای این‌گونه حملات سوق داده است. از این رو، خرابکاری و یا انهدام یک نیروگاه می‌تواند به عنوان حملهٔ مسلحانه، موضوع حقوق مخاصمات مسلحانه به‌شمار آید (خلف رضایی، ۱۳۹۲: ۱۲۶).

۳. حقوق حمایت از زیرساخت‌های انرژی

حق افراد در برخورداری از انرژی، در حقوق بین‌الملل بشر و قوانین داخلی کشورها[3] مورد شناسایی قرار گرفته است. این حق، از مصادیق حقوق افراد در مقابل دولت‌ها شمرده می‌شود. حق برخورداری از انرژی مؤید این است که هر فرد، از منابع انرژی برای تأمین نیازهای خود استفاده کند (سلیمی ترکمانی، ۱۳۹۴: ۶۹-۷۰). این حق خودبه‌خود، تأسیس و حمایت از

1. The Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) 2018.
2. The Conference "60 Years of the Geneva Conventions and the Decades Ahead", Geneva, 9–10 November 2009.
۳. امروزه بسیاری از کشورها، حمایت از زیرساخت‌های انرژی در قوانین داخلی را به طور مستقیم و یا در پرتو حمایت از زیرساخت‌های حیاتی (Critical Infrastructures) به طور عام، دنبال می‌کنند. از این میان، می‌توان به «قانون امنیت و حمایت از زیرساخت‌های حیاتی سال ۲۰۱۱ بلژیک» و یا «راهبرد امنیت ملی سال ۲۰۱۴ جمهوری لهستان» اشاره کرد.

زیرساخت‌های انرژی و بهره‌مندی تمامی افراد جامعه از آن را ملزم می‌دارد[۱]. حق برخورداری از انرژی تاکنون به صراحت در اسناد حقوقی بین‌المللی با ماهیت الزام‌آور گنجانده نشده است؛ اما رویهٔ سازمان‌های دولتی و برخی معاهدات نیز بر حق برخورداری از انرژی و به دنبال آن، حمایت از زیرساخت‌های انرژی مُهر صحت می‌نهد (سلیمی ترکمانی، ۱۳۹۴: ۷۲). ذیل بند اول مادهٔ ۱۱ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی[۲]، دولت‌های عضو، حق تمامی افراد در بهره‌مندی از استاندارد مناسب زندگی، از جمله مسکن و بهبود پیوستهٔ شرایط زندگی را به رسمیت شناخته‌اند. دسترسی به برق نیز بر همین اساس، ذیل حق بر مسکن مناسب مورد اشاره قرار گرفته است. دولت‌های عضو کنوانسیون رفع هرگونه تبعیض علیه زنان[۳] نیز موظف شده‌اند که تمامی تدابیر لازم برای رفع تبعیض علیه زنان در مناطق روستایی و به طور مشخص، حق بهره‌مندی آن‌ها از شرایط مناسب زندگی، به‌ویژه در مورد بهره‌مندی از برق را پیش‌بینی کنند (Tully, 2006: 31). تکلیف دولت‌ها به احترام به حقوق بشر، اقتضا دارد که از اعمال منجر به انکار یا عدم بهره‌مندی برابر از برق، دخالت غیرقانونی، کاهش عرضه و یا تخریب زیرساخت‌های انرژی برق خودداری کنند (Tully, 2006: 36). بنابراین، دولت‌ها ملزم به اتخاذ تدابیر لازم جهت ممانعت از نقض حق بر انرژی از سوی دیگر طرف‌ها، از تولیدکنندگان انرژی در بخش خصوصی[۴] گرفته تا بازیگران غیردولتی هستند (Ngai, 2012: 618). شاید بر همین اساس، مجموعه‌ای از معاهدات، حمایت‌های حقوقی از زیرساخت‌های انرژی را به طور خاص به ارمغان آورده‌اند؛ برای مثال، کنوانسیون ملل متحد در مورد حقوق دریاها، دولت‌های عضو را مکلف می‌سازد تا ایراد خسارت و یا تخریب خطوط لولهٔ زیردریایی انتقال انرژی و کابل‌های برق با ولتاژ بالا را جرم‌انگاری کنند (UNCLOS, 1982: Art.113; Wagner, 1995: 136). در کنوانسیون حقوق بهره‌برداری‌های غیرکشتی‌رانی از آبراه‌های بین‌المللی[۵] نیز حمایت از آبراه‌ها و تأسیسات مرتبط با آن‌ها که شامل سدها، آب‌بندها و برخی دیگر از زیرساخت‌های

---

۱. تأسیس و حمایت از زیرساخت‌های انرژی، به دنبال شناسایی حق برخورداری از انرژی، امری عقلی و مستند به قاعدهٔ «اذن در شیء، اذن در لوازم آن» است؛ به گونه‌ای که وجود تأسیسات مرتبط با تولید و بهره‌برداری از انرژی، از لوازم ذاتی، عرفی و قانونی حق برخورداری از انرژی است (برای اطلاع بیشتر، ر.ک: محقق داماد، سید مصطفی، قواعد فقه بخش مدنی، چاپ چهل و پنجم، ۱۳۹۴، تهران، مرکز نشر علوم اسلامی، ص.۲۳۵-۲۳۹).

2. International Covenant on Economic, Social and Cultural Rights, 1966.

3. Convention on the Elimination of all Forms of Discrimination against Women (1977) Art. 14(2) (h).

۴. گفتنی است که خصوصی‌سازی بخش انرژی، دولت‌ها را از تعهدات حقوق بشری ایشان مبرّا نمی‌سازد. تعهد دولت‌ها برای فراهم ساختن برق برای همگان، از طریق اتخاذ اقدامات مثبت (ایجابی) و برنامه‌ریزی‌شده جهت تسهیل، ارتقا و فراهم نمودن خدمات انرژی و اعمال قوانین و سیاست‌های مقتضی اجرایی می‌گردد (Bradbrook & Gardam, 2006: 411-415).

5. See UN Convention on the Law of the Non-Navigational Uses of International Watercourses, 1997, Arts. 26, 29.

انرژی است، در جریان مخاصمات مسلحانه مورد تصریح قرار گرفته است (Report of the Commission to the General Assembly on the Work of its forthy-sixth session 1994, 1997: 127-131). افزون بر این، بسیاری از زیرساخت‌های انرژی که به واسطهٔ سرمایه‌گذاری خارجی ایجاد شده‌اند و یا تابع حمایت‌های موضوع موافقت‌نامه‌های سرمایه‌گذاری هستند نیز از حمایت‌های اختصاصی مندرج در این موافقت‌نامه‌ها بهره‌مند هستند (Clifford Chance, 2018: 58-59)؛ برای مثال، می‌توان از معاهدهٔ منشور انرژی[1] نام برد که سرمایه‌گذاران دولت‌های طرف معاهده را در صورتی که در نتیجهٔ مخاصمه‌ای مسلحانه متحمل خسارتی شوند، مستحق دریافت غرامت و مطلوب‌ترین جبرانی که دولت میزبان به هر سرمایه‌گذار دیگری روا می‌دارد، دانسته است ((ECT, 1994, Art.12(1)). در منشور جهانی انرژی[2] نیز دولت‌ها به توسعهٔ زیرساخت‌های حیاتی برای امنیت انرژی در سطوح منطقه‌ای و جهانی، توسعه و اتصال زیرساخت‌های انرژی به شبکهٔ بین‌المللی و نوسازی و بهره‌وری این زیرساخت‌ها متعهد شده‌اند ((IEC, 2015, Title.1(1)). توسعه و اتصال زیرساخت‌های انرژی به شبکهٔ بین‌المللی در امنیت و حمایت از این تأسیسات نقش مهمی ایفا خواهد کرد؛ زیرا وابستگی متقابل دولت‌ها در زمینهٔ انرژی، همواره احتمال تعرض و تخاصم میان کشورها را به میزان چشمگیری کاهش می‌دهد (Proninska, 2007: 228). می‌توان به سادگی دریافت که برای مثال، تأمین و اتصال شبکه‌های برق شهرهای فلسطینی کرانهٔ غربی رود اردن به شبکهٔ برق اسرائیل در دههٔ هفتاد میلادی، دقیقاً با همین هدف کاهش مخاصمات و درگیری‌ها و به عنوان مشوقی برای طرف فلسطینی اجرایی شده است (Herman & Fischhendler, 2019: 6-7). شورای امنیت سازمان ملل نیز در قطعنامهٔ ۲۳۴۱ راجع به حمایت از زیرساخت‌های حیاتی و ارتقای توانایی دولت‌ها برای مقابله با حملات علیه زیرساخت‌های حیاتی، از تمامی دولت‌ها خواست تا اهمیت حملات تروریستی علیه این زیرساخت‌ها را مدنظر قرار داده و از طریق راهبردها و قوانین ملی، تدابیر پیشگیرانهٔ لازم را پیش‌بینی کنند. این قطعنامه، دولت‌ها را در تعیین مصادیق زیرساخت‌های حیاتی و تعیین نحوهٔ حمایت از این زیرساخت‌ها مختار می‌داند ((S/RES/2341(2017)). اگرچه دولت‌ها بخش‌های گوناگونی را در قلمرو زیرساخت‌های حیاتی خود شناسایی کرده‌اند، بخش انرژی و زیرساخت‌های مرتبط با آن همواره از برجسته‌ترین این موارد بوده است[3] (CTED & UNOCT, 2018: 33-34). زیرساخت‌های انرژی در قالب کنوانسیون‌های چهارگانهٔ ژنو و

1. Energy Charter Treaty, 1994.
2. International Energy Charter, 2015.
۳. برای مثال، در ایالات متحده به موجب بخشنامهٔ شمارهٔ ۲۱ راهبردی ریاست جمهوری (Presidential Policy Directive-21) در سال ۲۰۱۳، راجع به امنیت و تاب‌آوری زیرساخت‌های حیاتی، این زیرساخت‌ها در شانزده بخش تقسیم‌بندی شده است که حوزهٔ انرژی هم قسمی از آن است. این حوزه شامل: زیرساخت‌های تولید، پالایش، ذخیره‌سازی، توزیع نفت و گاز و برق و نیز بخش تجاری نیروگاه‌های هسته‌ای و سدهاست.

پروتکل‌های الحاقی آن که امروزه به عنوان اصلی‌ترین منبع قراردادی حقوق مخاصمات مسلحانه شناخته می‌شود نیز تلویحاً مورد حمایت قرار گرفته است.

۳. ۱. کنوانسیون‌های ژنو و حمایت از زیرساخت‌های انرژی

مخاصمات مسلحانهٔ بین‌المللی تابع مقررات مندرج در کنوانسیون‌های چهارگانهٔ ژنو و پروتکل اول الحاقی به این کنوانسیون‌هاست (برادران و حبیبی، ۱۳۹۸: ۱۴۴). در جای‌جای مقررات کنوانسیون‌های چهارگانهٔ ژنو، تخریب و یا تصرف اموال ممنوع انگاشته شده است. بی‌گمان زیرساخت‌های انرژی و تأسیسات مرتبط با آن نیز در شمول اموال مورد حمایت این کنوانسیون‌ها قرار دارد[1] (Ngai, 2012: 597). اما این حمایت‌ها ثانویه بوده و همواره تابعی از قوه‌ای قاهره، به نام ضرورت نظامی است (Luban, 2013: 316). معیار ضرورت نظامی به معنای شدت و حدت مورد نیاز برای تحمیل شکست و سلطه بر دشمن، با صرف کمترین هزینهٔ مالی، جانی و در کوتاه‌ترین زمان است (U.S Navy, 2017, para. 5.3.1). البته این اصل امروزه دامنهٔ محدودتری یافته است و صرفاً به عنوان استثنایی ذیل مقررات کنوانسیون‌های ژنو مقرر شده و خود نیز تابع حدود و قیود جداگانه‌ای با عنوان «الزامات ضرورت نظامی» تعریف می‌شود (نوری و دیگران، ۱۳۹۸: ۷۳۱). پروتکل الحاقی اول به کنوانسیون‌های ژنو نیز زیرساخت‌های انرژی را در جریان مخاصمات مسلحانه، در قالب اموال غیرنظامی، اموال حیاتی برای بقای جمعیت غیرنظامی، کارگاه‌ها و یا تأسیسات حاوی انرژی خطرناک و نیز ملاحظات محیط زیستی مورد حمایت قرار می‌دهد (Tignino, 2016: 3-4). لزوم تفکیک میان اهداف نظامی و غیرنظامی از سوی طرفین مخاصمه، در مادهٔ ۴۲ این پروتکل، به عنوان قاعده‌ای مبنایی[2] شناخته می‌شود. در همین راستا، ذیل بند دوم مادهٔ ۵۲، حملات باید فقط و فقط محدود به اهداف نظامی باشد. این بند، اهداف نظامی را محدود به آن‌هایی که ماهیت، مقر یا هدف و کاربرد آن‌ها به نحو مؤثری از فعالیت نظامی پشتیبانی می‌کند و یا تخریب، تصرف یا از کار انداختن آن‌ها به طور کامل یا نسبی، در شرایط حاکم بر مخاصمه، مزیت مسلم نظامی شمرده می‌شود، تعریف کرده است. این بند، معیاری کلی ارائه می‌دهد و ممکن است از سوی هریک از طرفین مخاصمه تفسیر موسع گردد و زیرساخت‌های انرژی را نیز بدین‌ترتیب از اهداف نظامی به‌شمار آورند (Bohm, 2015: 76). کاستی‌های تبیین دقیق مصادیق اهداف نظامی و ابعاد آن در

1. See Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949, Art. 50; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 1949, Art. 51; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 1949: Art. 53, 147.
2. Basic rule

این پروتکل و ابهامات پیرامونی، موجب طرح پیشنهادهایی شده است؛ ابتکارِ «کتابچهٔ راهنمای فرماندهان، راجع به حقوق عملیات دریایی نیروی دریایی آمریکا»[1] در تعریفِ عبارت «اهداف نظامی» مندرج در بند (۲. ۸) که سعی داشته، اصطلاح «توانایی جنگ»[2] یا «توانایی ادامهٔ جنگ»[3] را جایگزین عبارت «فعالیت نظامی» در متن پروتکل کند، در همین ردیف است (Dinstein, 2002: 145-153). به هر حال، هدف نظامی در تعریف پروتکل، لزوماً باید به نحو مؤثری عملیات نظامی را پشتیبانی کند و چنین پشتیبانی‌ای برای فعالیت نظامی یکی از طرفین مخاصمه انجام شود. از سوی دیگر، مزیت نظامی مسلم، امری ضروری برای وجاهت حملات است که مزیت نظامی در این معنا، باید امری مسلم و معقول باشد، نه فرضی یا انتزاعی (Tignino, 2016: 37). مصادیق اهداف نظامی، به واسطهٔ مقررات دیگر این پروتکل، از جمله مواد ۵۴ تا ۵۸، به شکل مضاعفی محدود و مقید شده و در نتیجه، حمایت‌های بیشتری از زیرساخت‌های انرژی، به شکل مستقیم و غیرمستقیم به ارمغان آورده شده است. به موجب مقررات بند دوم مادهٔ ۵۴، «حمله، تخریب، برچیدن یا از کار انداختن اموالی که جهت بقای جمعیت غیرنظامی ضروری است، از جمله مواد غذایی، زمین‌های کشاورزی تولید مواد غذایی، محصولات زراعی، دام، تأسیسات آب آشامیدنی، عرضه و آبیاری، در مخاصمات مسلحانهٔ بین‌المللی ممنوع است»[4]. با توجه به این‌که امروزه دسترسی به انرژی برای بقای جمعیت غیرنظامی، تولید مواد غذایی و یا بهره‌برداری از تأسیسات مربوط به آبیاری، تولید آب آشامیدنی و بسیاری دیگر از خدمات اجتماعی، ضرورتی انکارناپذیر تلقی می‌شود، تأسیسات تولید انرژی برق برای جمعیت غیرنظامی نیز داخل در مفهوم «اموال ضروری برای بقای جمعیت غیرنظامی» قرار گرفته و از این حمایت‌ها برخوردار است (Ngai, 2012: 590). حمایت‌های این بند به طور مطلق بیان شده است و بدین‌ترتیب، استثنای وضع‌شده در مادهٔ ۵۳ کنوانسیون چهارم که تخریب اموال شخصی، عمومی و دولتی را تنها در صورت وجود ضرورت نظامی مسلم مجاز می‌داند، تخصیص زده است (نوری و دیگران، ۱۳۹۸: ۷۳). مادهٔ ۵۵ پروتکل نیز طرفین را مکلف می‌کند تا در هنگام جنگ، از محیط زیست در برابر آسیب‌های گسترده، بلندمدت و شدید، پاسداری کنند[5]. پیروی از محدودیت‌های این ماده نیز به روشنی

1. The United States' Commander's Handbook on the Law of Naval Operations.
2. War-fighting capability
3. War-sustaining capability

۴. الزامات این بند، در مادهٔ ۱۴ پروتکل الحاقی دوم به کنوانسیون‌های ژنو، راجع به حمایت از قربانیان مخاصمات مسلحانهٔ داخلی نیز تصریح شده است.

۵. در بند سوم مادهٔ ۳۵ پروتکل الحاقی اول، در مقرراتی مشابه، «کاربرد شیوه‌ها یا وسایل جنگی که هدف از آن‌ها وارد آوردن خسارت شدید، گسترده و بلندمدت بر محیط زیست باشد یا احتمال رود که منجر به چنین اثراتی خواهد شد»، ممنوع انگاشته شده است.

منابع طبیعی انرژی و تأسیسات مرتبط با آن را در جریان مخاصمات مسلحانه، مورد صیانت قرار خواهد داد. از این رو، در گزارش نهایی کمیتهٔ دیوان کیفری بین‌المللی یوگوسلاوی سابق برای بررسی حملات ناتو در جمهوری فدرال یوگوسلاوی، انتشار مواد آلاینده در نتیجهٔ حملات به صنایعی همچون نیروگاه‌های شیمیایی و تأسیسات نفتی، از موارد خسارت به محیط زیست و نقض مقررات این ماده اعلام شد (Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, 2000: Para.14). امروزه در عرف بین‌المللی، تأسیسات مذکور در مادهٔ ۵۵ شامل زیرساخت‌هایی همچون کارخانه‌های شیمیایی و پالایشگاه‌های نفت و گاز نیز هست (امین‌زاده و دیگران، ۱۳۹۷: ۱۵۱). این ماده، ممنوعیت مطلق این نوع حملات را مطرح می‌کند؛ به گونه‌ای که حتی با استناد به ضرورت نظامی نیز قابل تخطی نخواهد بود (Ngai, 2012: 594). حمایت از زیرساخت‌های انرژی در پرتو ملاحظات محیط زیستی، رویهٔ دیرپای سازمان ملل نیز به‌شمار می‌آید؛ به نحوی که در جریان تهاجم عراق به کویت و آتش زدن چاه‌های نفتی این کشور، شورای امنیت قطعنامهٔ ۶۸۷ را صادر کرد و بدین‌وسیله عراق در خصوص خسارات مستقیم، از جمله خسارت به محیط زیست و از بین بردن منابع طبیعی، مسئول شناخته شد (S/RES/687/1991). مادهٔ ۵۶ پروتکل نیز مقرر داشته است که «کارگاه‌ها یا تأسیسات دارای نیروهای خطرناک، از جمله سدها، آب‌بندها و نیروگاه‌های هسته‌ای تولید برق، حتی اگر اهداف نظامی باشند، در صورتی که حمله به آن‌ها احتمالاً موجب رهاشدن نیروهای خطرناک و در نتیجه، صدمات شدید بر سکنهٔ غیرنظامی شود، نباید هدف حمله قرار گیرد. سایر هدف‌های نظامی که این کارگاه‌ها یا تأسیسات در مجاورت آن‌ها واقع شده‌اند نیز در صورتی که حمله به آن‌ها موجب رهاشدن انرژی‌های خطرناک از این کارگاه‌ها یا تأسیسات و در نتیجه، صدمات شدید برای سکنهٔ غیرنظامی شود، نباید هدف حمله قرار گیرد». اما به موجب بندهای بعدی مادهٔ ۵۶، استثناهایی بر این حمایت‌ها وارد شده است. اگر تأسیسات موضوع این ماده به طور دایمی، به نحو چشمگیر و به شکل مستقیم، فعالیت‌های نظامی را پشتیبانی کند و حمله به این تأسیسات، تنها راه توقف چنین پشتیبانی‌ای باشد، قابل توجیه خواهد بود (Additional Protocol one to the Geneva Conventions1949, 1977, Art. 56 (2)). مقررات این ماده، با وجود این‌که حمله به این‌گونه تأسیسات، به موجب قواعد عرفی نیز باید با دقت نظر ویژه به منظور خودداری از رهاشدن انرژی‌های خطرناک و خسارت شدید به جمعیت غیرنظامی انجام شود، همچنان ماهیت عرفی نیافته است (Henckaerts & Dinstein, 2002: 152; Doswald-Beck, 2005: 139). ابهامات زیادی در کیفیت تعیین اهداف نظامی مشروع و شدت متناسب حملات به این‌گونه اهداف وجود دارد. تفکیک و تناسب در این حملات تابع مؤلفه‌هایی همچون اطلاعات در دسترس فرماندهان نظامی است. از این رو، اتخاذ تدابیر

احتیاطی در مادهٔ ۵۷ پروتکل الزامی گشته و بدین‌سان تمامی فرماندهان نظامی، به محاسبهٔ مزیت نظامی حملات، در قبال خسارات بالقوه و آثار غیرمستقیمی که احتمالاً چنین حملاتی به اهداف غیرنظامی وارد خواهد کرد، مکلف شده‌اند (Geneva Water Hub, July 2016: 6). فرماندهان نظامی همچنین باید حداقل شدت را در حملات خود به‌کار برند و از تخریب بیهودهٔ اموال خودداری کنند (Sowers et al., 2017: 5). به نظر می‌رسد حقوق موضوعه[1] در حمایت از اهداف غیرنظامی، مانند زیرساخت‌های انرژی، تا کنون به خوبی ظاهر نشده است و با تحول شیوه‌های نوین جنگی، تعیین مصادیق اهداف نظامی به نحو دقیق‌تر ضرورت می‌یابد؛ تا حقوق مخاصمات مسلحانه از تحولات جنگ‌های مدرن باز نماند (Dinstein, 2002: 172). تنها راهکار غلبه بر این ابهامات در حال حاضر، بررسی موردی نقض مقررات کنوانسیون‌های ژنو و پروتکل‌های آن، در جریان مخاصمات مسلحانه و با تفسیر این حمایت‌ها بر مبنای اصل حسن‌نیت است (Kodar, 2012: 118).

۴. اصول حقوق بشردوستانه در حمایت از زیرساخت‌های انرژی

در مورد حمایت حقوق بشردوستانه از زیرساخت‌های انرژی باید به اصول بنیادین[2] و دیگر اصول مهم حقوق بشردوستانه مراجعه کرد. اصول بنیادین حقوق بشردوستانه که مبنای اصول دیگر است، اصل انسانیت[3] و اصل ضرورت نظامی[4] است که در تفسیر قواعد حقوق بشردوستانه مورد استناد قرار می‌گیرد و اصول حقوقی شناخته‌شده‌ای همچون اصل تفکیک[5] و تناسب[6] نیز در واقع ریشه در همین اصول بنیادین دارد (Tsagourias & Morrison, 2018). اصل انسانیت، ممنوعیت ایراد درد و رنج و نیز تخریب غیرضروری اموال را ملزم می‌دارد (Hague Convention IV, 1907, Art. 23(e)). بنابراین، هیچ‌یک از طرفین مخاصمه نباید به حمله و تخریب، از بین بردن و یا از کار انداختن اهدافی که برای بقای غیرنظامیان حیاتی است، اقدام کند (UNEP, 2009: 13). اصل انسانیت خود برآمده از شرط مارتنس[7] است که در بند دوم مادهٔ ۱ پروتکل الحاقی اول تبلور یافته است (Mourlam, 2018: 23). این مقرره با توجه به برخی کاستی‌ها که در حقوق قراردادی، در حمایت از زیرساخت‌های انرژی احساس می‌شود، اهمیت دوچندانی می‌یابد. این شرط، به بیان ساده اعلان می‌دارد که در خلأ حقوق قراردادی، قواعد

1. lex scripta
2. Fundamental Principles
3. Principle of Humanity
4. Principle of Military Necessity
5. Principle of Distinction
6. Principle of Proportionality
7. Martens Clause

عرفی حقوقی بین‌المللی همواره لازم‌الاتباع خواهد بود[۱]. شرط مارتنس با ارجاع به اصل انسانیت، لزوم اتخاذ رویکرد انسانی و ملاحظات انسان‌دوستانه در تمامی شرایط را مورد تأکید قرار می‌دهد که این، شامل خودداری از تخریب، از کار انداختن و یا حمله به زیرساخت‌های انرژی مورد استفادهٔ جمعیت غیرنظامی هم می‌شود (Larsen et al., 2013: 72-73). با استناد به اصل ضرورت نظامی نیز طرفین متخاصم باید تعادلی میان ملاحظات انسانی ناشی از مخاصمه و ضرورت‌های نظامی برقرار کنند (رنجبریان و بذار، ۱۳۹۷: ۷۲). در اساسنامهٔ دیوان کیفری بین‌المللی نیز تخریب و تصاحب غیرقانونی و خودسرانهٔ اموال که مبتنی بر ضرورت نظامی نباشد، از مصادیق جنایت جنگی دانسته شده است (Rome Statute of ICC, 1998, Art. 8(2) (a) (iv)). رعایت این اصل در کنوانسیون‌های چهارگانهٔ ژنو ۱۹۴۹ و پروتکل‌های الحاقی ۱۹۷۷، با عبارات متنوعی همچون «امنیت و ضرورت نظامی مطلق»، «ضرورت مبرم»، «ضرورت مطلق عملیات نظامی»، «تا حدی که ملاحظات عملی و عملیاتی تجویز نماید» و «هرگاه ضرورت مبرم نظامی ایجاب کند»، تلویحاً و یا به تصریح الزامی شده است (نوری و دیگران، ۱۳۹۸: ۷۱۹–۷۲۰). این اصل امروزه ماهیت حقوق عرفی یافته و در قواعد عرفی کمیتهٔ بین‌المللی صلیب سرخ در سال ۲۰۰۵ نیز به آن تصریح شده است (Henckaerts & Doswald-Beck, 2005: 127-202)[۲]. در حمایت از اهداف غیرنظامی، اصل تفکیک نقش محوری دارد و مطابق آن، حملات خشونت‌آمیز علیه طرف دیگر مخاصمه باید به اهداف نظامی محدود باشد (Dinstein, 2002: 172; Henckaerts & Doswald-Beck, 2005: 25-29). اصل تناسب در حمله نیز از قواعد حقوق بین‌الملل عرفی شمرده شده و به موجب آن، فرماندهان نظامی باید خسارات احتمالی به محیط زیست و زیرساخت‌ها را در تصمیم‌گیری راجع به حملات، در نظر بگیرند (Sowers et al., 2017: 5). اصول حقوق بشردوستانهٔ دیگری نیز می‌تواند در حمایت از زیرساخت‌های انرژی در جریان مخاصمات مسلحانهٔ بین‌المللی نقش‌آفرینی کند که از آن جمله، اصل تدابیر احتیاطی، منع حمله به اموال ضروری برای حیات جمعیت غیرنظامی، منع انجام اعمال تلافی‌جویانه، منع

---

۱. شرط مارتنس که نخستین‌بار از سوی فردریش مارتنس، نمایندهٔ دولت روسیه، در کنفرانس‌های صلح لاهه مطرح شد و در مقدمهٔ کنوانسیون‌های ۱۸۹۹ و ۱۹۰۷ لاهه نیز درج شد، از این قرار است: «تا زمانی که مجموعه‌ای کامل‌تر از قوانین جنگی تدوین و تصویب شود، طرفین معظم موافقت می‌نمایند که در مواردی که تحت شمول مقررات مصوب قرار نمی‌گیرد، غیرنظامیان و نظامیان تحت حمایت و تابع اصول حقوق بین‌الملل مستنبط از رویهٔ تثبیت‌شده میان ملل متمدن، ضوابط انسانی و تمنیات وجدان عمومی باقی خواهند ماند». این شرط ناظر به حقوق بشردوستانه و حقوق بشر است و عملکرد دیوان بین‌المللی دادگستری، نهادهای حقوق بشری و اسناد متعدد، از جمله کنوانسیون‌های چهارگانهٔ ژنو ۱۹۴۹ (مادهٔ ۶۳ کنوانسیون اول، مادهٔ ۶۲ کنوانسیون دوم، مادهٔ ۱۴۲ کنوانسیون سوم و مادهٔ ۱۵۸ کنوانسیون چهارم) و پروتکل‌های الحاقی ۱۹۷۷، همگی حاکی از مقبولیت جهانی و پذیرش عام این شرط است (زرنشان، ۱۳۹۷: ۳۲۲).

۲. این اصل به طور مشخص ذیل قواعد شمارهٔ ۳۸، ۳۹، ۴۳، ۵۰، ۵۱ و ۵۶ مورد تصریح قرار گرفته است.

حمله به تأسیسات انرژی خطرناک و حفاظت از محیط زیست است (امین زاده و دیگران، ۱۳۹۷: ۱۴۳-۱۴۹).

نتیجه

تا کنون حمایت‌های حقوق بین‌الملل از زیرساخت‌های انرژی، به طور صریح، الزام‌آور و با پذیرش جهانی محقق نشده است. حمایت‌های مقرر در کنوانسیون‌های ژنو و پروتکل الحاقی نیز این زیرساخت‌ها را صریحاً مورد حمایت قرار نمی‌دهد، بلکه به واسطهٔ ملاحظات محیط زیستی و برای صیانت از مال و جان جمعیت غیرنظامی در مخاصمات مسلحانه، مقرراتی به طور مستقیم یا غیرمستقیم و ناظر به این اموال منظور شده است. پس، این زیرساخت‌ها با وجود ارزش اقتصادی و اهمیت راهبردی برای دولت‌ها، تا حدود زیادی مغفول واقع شده‌اند. از سوی دیگر، چندی از مقررات پروتکل الحاقی همچون مادهٔ ۵۶، به طور کامل ماهیت عرفی نیافته است و بدین‌ترتیب، برای دولت‌هایی که پروتکل را امضا نکرده‌اند، تکلیف صریح و درخوری در این خصوص به وجود نمی‌آورد. به هر حال، شناسایی حق برخورداری از انرژی و الزامات این حق، کمک شایانی به حمایت از این زیرساخت‌ها کرده است؛ زیرا قواعد و مقررات حقوق بشر، فارغ از وقوع مخاصمهٔ مسلحانه و به طور موازی با آن، لازم‌الاتباع است. تقویت سازوکارهای نظارتی و تحقق ضمانت اجرا برای اسناد مؤید حقوق انرژی، اما در نهایت به ملاحظه و حمایت از این زیرساخت‌ها در جریان مخاصمات مسلحانه، از سوی دولت‌های عضو این معاهدات خواهد انجامید. فعالیت‌های ناتو و برخی دولت‌های عضو این سازمان به طور جداگانه، برای تأمین امنیت زیرساخت‌های انرژی، گرچه دستاوردهای ارزشمندی به همراه داشته است، عمدتاً ناظر به منافع منطقه‌ای این سازمان و دولت‌های عضو آن بوده است؛ این اقدامات به شکل‌گیری قواعد حقوقی الزام‌آور بین‌المللی نینجامیده است و بیشتر مؤید کارآمدی نظام امنیت جمعی، برای حمایت از حمل‌ونقل جهانی انرژی است. ظهور تهدیدات نوین، مانند حملات سایبری و روند فزایندهٔ این حملات علیه زیرساخت‌های انرژی، دولت‌ها را به تدوین قواعد و الزامات حقوقی در این زمینه سوق خواهد داد. صدور قطعنامهٔ ۲۳۴۱ شورای امنیت در سال ۲۰۱۷ و تصویب قوانین داخلی از سوی برخی دولت‌ها در مقابله با این تهدیدات، حکایت از شکل‌گیری این‌گونه گرایش‌ها دارد. تصریح کمیتهٔ بین‌المللی صلیب سرخ، به اینکه حقوق بشردوستانه در خصوص حملات سایبری نیز قابلیت اعمال داشته و آن را محدود و مقید می‌سازد، تا حدود زیادی راهگشا خواهد بود، اما اصول و قواعد حقوق بشردوستانه، عمدتاً منوط به تفسیر و تدبیر فرماندهان و سیاست‌گذاران نظامی شده است. احراز معیارهایی همچون ضرورت نظامی، مزیت نظامی، مسئلهٔ دقت نظر ویژهٔ

فرماندهان، میزان اطلاعات در دسترس ایشان در مورد محل وقوع اهداف نظامی و غیرنظامی، نحوهٔ پیش‌بینی خسارات احتمالی حمله به این تأسیسات و میزان شدت متناسب برای حملات، در مقام اثبات، دشوار بوده و گرفتار ابهامات جدی است و تاب تفسیرهای متفاوتی دارد. بخش بزرگی از این ابهامات و کاستی‌های حقوقی در حمایت از این زیرساخت‌ها، به واسطهٔ تدوین سند حقوقی بین‌المللی و دارای مقبولیت جهانی که برای این زیرساخت‌ها به طور خاص، شخصیت حقوقی مستقلی قائل باشد، رفع خواهد شد.

منابع

الف) فارسی

۱. اسمعیل‌زاده ملاباشی، پرستو؛ عبداللهی، محسن؛ زمانی، سید قاسم (۱۳۹۶). «حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعهٔ موردی: حملات سایبری به گرجستان)». *فصلنامهٔ مطالعات حقوق عمومی*، دورهٔ ۴۷، شمارهٔ ۲، ص ۵۳۷-۵۵۹.

۲. امین‌زاده، الهام؛ مومنی‌راد، احمد؛ خداپرست، ناصر (۱۳۹۷). *حقوق بین‌الملل و ابعاد سیاسی و نظامی امنیت انرژی‌های فسیلی*. چاپ اول، تهران، انتشارات دانشگاه تهران.

۳. برادران، نازنین؛ حبیبی، همایون (۱۳۹۸). «قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری». *فصلنامهٔ مطالعات حقوق عمومی*، دورهٔ ۴۹، شمارهٔ ۱، ص ۱۵۸- ۱۳۹.

۴. بنجامین کی، سوواکول (۱۳۹۱). *کتاب مرجع امنیت انرژی*. ترجمهٔ علیرضا طیب، چاپ اول، تهران، ابرار معاصر تهران.

۵. حاتمی، مهدی (۱۳۹۷). «نقدی بر نظریهٔ «قتل‌های هدفمند دولت آمریکا» در پرتو رویه و اصول بنیادین حقوق بشردوستانهٔ بین‌المللی». *پژوهش‌نامهٔ انتقادی متون و برنامه‌های علوم انسانی*، دورهٔ ۱۸، شمارهٔ ۵، ص ۱۱۳- ۸۹.

۶. خلف رضایی، حسین (۱۳۹۲). «حملات سایبری از منظر حقوق بین‌الملل (مطالعهٔ موردی: استاکس‌نت)». *فصلنامهٔ مجلس و راهبرد*، دورهٔ ۲۰، شمارهٔ ۷۳، ص ۱۵۳- ۱۲۵.

۷. رنجبریان، امیرحسین؛ بذار، وحید (۱۳۹۷). «رعایت حقوق بین‌الملل بشردوستانه از سوی ربات نظامی خودفرمان و مسئولیت ناشی از اقدامات آن‌ها». *مجلهٔ حقوقی بین‌المللی*، دورهٔ ۳۵، شمارهٔ ۵۹، ص ۸۴- ۶۳.

۸. زرنشان، شهرام (۱۳۹۳). «مفهوم و ماهیت عنصر مادی در فرایند شکل‌گیری قواعد حقوق بین‌الملل عرفی». *پژوهش‌های حقوق تطبیقی*، دورهٔ ۱۸، شمارهٔ ۳، ص ۹۹- ۷۷.

۹. _____ (۱۳۹۷). «نسبت میان شرط مارتنس و حقوق بشر در نظم حقوقی بین‌المللی جدید». *فصلنامهٔ مطالعات حقوق عمومی*، دورهٔ ۴۸، شمارهٔ ۲، ص ۳۳۸- ۳۱۹.

۱۰. سلیمی ترکمانی، حجت (۱۳۹۴). *حقوق بین‌الملل انرژی*. چاپ اول، تهران، شهر دانش.

۱۱. ضیائی بیگدلی، محمدرضا (۱۳۹۶). *حقوق بین‌الملل بشردوستانه*. چاپ چهارم، تهران، گنج دانش.

۱۲. محقق داماد، سید مصطفی (۱۳۹۴). *قواعد فقه- بخش مدنی*. چاپ چهل و پنجم، تهران، مرکز نشر علوم اسلامی.

۱۳. نامدار، سعید؛ قاسمی، غلامعلی (۱۳۹۷). «بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حملهٔ استاکس‌نت به تأسیسات هسته‌ای ایران)». *مجلهٔ مطالعات حقوقی*، دورهٔ ۱۰، شمارهٔ ۱، ص ۲۳۵- ۱۹۹.

۱۴. نوری، ولی‌الله؛ زمانی، سید قاسم؛ راعی، مسعود (۱۳۹۸). «ضرورت نظامی به عنوان یک استثنا در حقوق درگیری‌های مسلحانه». *فصلنامهٔ مطالعات حقوق عمومی*، دورهٔ ۴۹، شمارهٔ ۳، ص ۷۳۴- ۷۱۷.

۱۵. ممتاز، جمشید؛ رنجبریان، امیرحسین (۱۳۸۶). *حقوق بین‌الملل بشردوستانه- مخاصمات مسلحانهٔ داخلی*. چاپ دوم، تهران، نشر میزان.

ب) خارجی

16. Allhoff Fritz, Henschke Adam; Strawser Bradley Jay (2016). *Binary Bullets- The ethics of Cyberwarfare*. US: Oxford University Press.
17. Bradbrook Adrian J; Gardam Judith G (2006). "Placing Access to Energy Services within a Human Rights Framework". *Human Rights Quarterly*, Vol. 28, No. 2, pp. 389-415.
18. Bohm Erick R (2015). "Targeting Objects of Economic Interest in Contemporary Warfare". *Creighton International and Comparative Law Journal*, Vol. 6, No.1, pp.74-84.
19. Christen Markus; Gordihn Bert; Loi Michele (2020). *The Ethics of Cybersecurity*. Switzerland: Springer.
20. Cecchetti Emanuele Nicola; Jakson Heiki (2017). "The Role Risks and the Strategic Importance of Energy in Conflicts. The Case of Ukraine". *Energy Security: Operational Highlights, NATO Energy Security Centre of Excellence*, No. 11, pp. 16-24.
21. Clapham Andrew; Gaeta Paola (2014). *The Oxford Handbook of International Law in Armed Conflict*. UK: Oxford University Press.
22. Clifford Chance (2018). *Infrastructure: 21st Century Challenges A Legal Perspective*. London: Clifford Chance.
23. Critical Energy Infrastructure Security Stakeholders Group (November 2018). *"CEIS-SG Security Roadmap V1"*, Available at https://defender-project.eu/ceis-sg/
24. CTED; UNOCT (2018). *"The Protection of Critical Infrastructure against Terrorist Attacks: Compendium of Good Practices"*. available at: https://www.un.org/sc/ctc/wp-content/uploads/2018/06/CompendiumCIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf
25. Desarnaud Gabrielle (2017). "Cyber Attacks and Energy Infrastructures-Anticipating Risks". Ifri Center for Energy, Available at: https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf
26. Dinstein Yoram (2002). "Legitimate Military Objectives under the Current Jus in Bello". *International Law Studies*, Vol. 78, pp.139-172.
27. Dugulin Riccardo; Cussac Drum (2015)." *The Potential Cooperation Between NATO and Private Risk Management Companies in the Protection of Critical Energy Infrastructure"*. In Alessandro Niglia (Ed.), The Protection of Critical Energy Infrastructure against Emerging Security Challenges(pp. 89-100), Amsterdam, The Netherlands: IOS Press BV.
28. Endicott Neil (2010). *"Military Responses to Energy Security Problems: What role for Common Security and Defence Policy?"*. Bruxelles: Quaker Council for European Affairs aisbl.
29. Energy Infrastructure (2019, April 23). Retrieved from: https://www.designingbuildings.co.uk/wiki/Energy infrastructure
30. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia (June 2000). United Nations International Criminal Tribunal for the Former Yugoslavia, Available at: https://www.icty.org/sid/10052
31. Geneva Water Hub (July 2016). *The Protection of Water During and after Armed Conflicts*. Geneva: University of Geneva.
32. Gisel Laurent; Olejnik Lukasz (November 2018). *The Potential Human Cost of Cyber Operations*. Geneva: ICRC.
33. Global Conference on Cyber Space (GCCS 2017). Internet Society, Available at: https://www.internetsociety.org/events/gccs-2017/
34. Guelpa Elisa; Bischi Aldo; Verda Vittoria; Chertkov Michael; Lund Henrik (2019). "Towards future Infrastructures for Sustainable Multi-Energy Systems: A Review". *Energy*, Vol. 184, pp.2-21.
35. Guzman Andrew T (2005). "Saving Customary International Law". *Michigan Journal of International Law*, Vol. 27, Issue. 1, pp. 116-176.
36. Henckaerts Jean-Marie; Doswald-Beck Louise (2005). *Customary International Humanitarian Law, Rules*. Volume 1, UK: Cambridge University press.
37. Herman Lior; Fischhendler (2019), "Energy as a Rewarding and Punitive Foreign Policy Instrument: The Case of Israeli–Palestinian Relations". *Studies in Conflict and Terrorism*, DOI: 10.1080/1057610X.2019.1567997.

38. Jakson Heiki; Brendan Byrne; Cecchetti Emanuela Nicola; Ciampor Jan; Hajek Jaroslav; Hausler Maximilian; Dubrova Kateryna (2017), *Energy in Irregular Warfare.* Energy in Conflict Series, Lithuania: NATO Energy Security Centre of Excellence.
39. Kerttunen Mika; Tikk Eneken (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy.* New York: Cyber Policy Institute.
40. Kodar Erki (2012*). "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I"*. In Rain Liivoja & Andres Saumets (Eds.), Cultural, Peace and Conflict Studies Series Volume III: The Law of Armed Conflict: Historical and Contemporary Perspectives (pp. 107-132), Estonia: Tartu University Press.
41. Kuzemco Caroline; Keating Michael F; Goldthau Andreas (2016). *The Global Energy Challenge, Environment, Development and Security.* London, UK: Palgrave.
42. Larsen Kjetil Mujezinovic; Cooper Camilla G. Guldahl; Nystuen Gro (2013). *Searching for a Principle of Humanity in Internatioanl Humanitarian Law.* New York: Cambridge University Press.
43. Leetaru Kalev (2017, February 9). *"What Tallinn Manual 2.0 Teaches Us About The New Cyber Order"*. Retrieved from: https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#323d8565928b
44. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (13 January 2015).
45. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/66/359 (14 September 2011).
46. Liivoja Rain; McCormack Tim (2016). *Routledge Handbook of the Law of Armed Conflict.* London: Routledge.
47. Luban David (2013). "Military Necessity and the Cultures of Military Law". *Leiden Journal of International Law*, Vol.26, No.2, pp. 315-349.
48. Mourlam, Anna C. (2018). "Unarmed Attacks: Cyber Combatants and the Right to Defend". *The California International Law Journal*, Vol. 26, No. 1, pp. 19-30.
49. Ngai Jenny Sing-hang (2012). " Energy as a Human Right in Armed Conflict: A Question of Universal Need, Survival, and Human Dignity". *Brooklyn Journal of International Law*, Vol.37, Issue.2, pp.579-622.
50. Proninska Kamila (2007). *"Energy and Security: Regional and Global Dimensions"*. In Stockholm Internatioal Peace Research Institute (Ed.), Yearbook 2007 Armaments, Disarmament and International Security (pp. 215-243), New York, US: Oxford University press Inc.
51. Riga Summit Declaration (2006, 29 November). *North Atlantic treaty Organization*, Available at: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en
52. Ruhle Michael (2017). "Energy Security: Eight Relevant Lessons". *Energy Security: Operational Highlights, NATO Energy Security Centre of Excellence*, No. 11, pp. 5-7.
53. Sassoli Marco (2019). *International Humanitarian Law.* UK: Edward Elgar Publishing Limited.
54. Schmitt Michael N (2017). *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd Edition, UK: Cambridge University Publication.
55. Solis Gary D (2016). *The Law of Armed Conflict.* 2nd Edition, New York: Cambridge University Press.
56. Sowers Jennie L; Weinthal Erika; Zawahri Neda (2017). "Targeting Environmental Infrastructures, International Law, and Civilians in the New Middle Eastern Wars". *Security Dialogue*, Vol.48, Issue.5, pp.1-21.
57. The Commander's Handbook on the Law of Naval Operation (August 2017). U.S. NAVY, Available at: https://portal.nwdc.navy.mil/NDLS/default.aspx
58. Tignino Mara (2016). *Water During and After Armed Conflicts:What Protection in International Law?.* Leiden, The Netherlands: Koninklijke Brill nv.
59. Tsagourias Nicholas; Morrison Alasdair (2018). *Internatioanl Humanitarian Law"*. UK: Cambridge University Press.
60. Tully, Stephen (2006). "The Human Right to Access Electricity". *The Electricity Journal*, Vol.19, Issue.3, pp. 30-39.

61. U.S Department of Energy (2018). "Multiyear Plan for Energy Sector Cybersecurity". office of Electricity Delivery and Energy Reliability, Available at: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf
62. United Nations Environment Programme (2009). *Protecting the Environment During Armed Conflict An Inventory and Analysis of International Law*. Nairobi, Kenya: United Nations Environment Programme.
63. Valo Janne (January 2014). Cyber Attacks and the Use of Force in International Law. Faculty of Law, University of Helsinki.
64. Wagner Eric (1995). "Submarine Cables and Protections provided by the law of the Sea". *Marine Policy*, Vol. 19, No. 2, pp. 127-136.
65. Zarpelo Bruno Bogaz; Miani Rodrigo Sanches; Kawakani Cludio Toshio; De Alvarenga Sean Carlisto (2017). "A Survey of Intrusion Detection in Internet of Things". *Journal of Network and Computer Applications*, Vol. 84,Issue. C, pp. 25-37.
66. Zio Enrico (2016). "Challenges in the Vulnirability and Risk Analysis of Critical Infrastructures". *Reliability Engineering and System Safety*, Vol. 152, pp. 137-150.