Some legal challenges posed by remote attack

برخی چالش‌های حقوقی ناشی از حملات از راه دور[1]

ویلیام بوثبای[2]

چکیده

حمله از راه دور پدیده‌ای تازه نیست اما در پی ظهور برخی فناوری‌های جدید، حملات می‌توانند به نحوی انجام شوند که مهاجم از صحنه‌ی اعمال زور فاصله داشته باشد. در این مقاله مسائل حقوقی ناشی از به کار گیری وسایل دارای سرنشین، فناوری‌های خودکار حمله و قابلیت‌های سایبری بررسی می‌شود و اصول و قواعد حقوقی هدفگیری از جمله تمایز، تبعیض، تناسب و قواعد احتیاطی ملاحظه و مشاهده می‌شود که تمامی آن‌ها بر حملات از راه دور اعمال می‌شوند و سپس چالش‌های ناشی از اجرای الزامات حقوقی مورد بررسی قرار می‌گیرد. تعهد حقوقی دولت‌ها جهت بازبینی سلاح‌ها، روش‌ها و ابزارهای جنگی جدید به طور مقتضی مورد توجه قرار می‌گیرد؛ تعهدی که موید این نقطه نظر است که حقوق موجود منشوری را ارائه می‌دهد که از طریق آن فناوری‌های جدید در حمله باید توسط دولت‌ها مورد ارزیابی قرار گیرند. سپس این مقاله به این موضوع می‌پردازد که چگونه مفهوم مسئولیت در رابطه با حملات از راه دور اعمال می‌شود و به این امر پرداخته می‌شود که آیا بدون سرنشین بودن یا از راه دور بودن در یک حمله مسئله حقوقی اساسی است.

واژگان کلیدی: حمله از راه دور، وسایل هدایت شونده از راه دور، ادوات هوایی بدون سرنشین (UAVs)، حملات سایبری، حمله مستقل، بازبینی حقوقی ابزارهای جدید، ابزار یا روش‌های جنگی، مسئولیت.

---

[1] برگردان به فارسی: علی اکبر سیاپوش

[2] دکتر ویلیام بوثبای در جولای ۲۰۱۱ از سمت معاونت خدمات حقوقی (رویال ایر فورس) با درجه ناخدای نیروی هوایی بازنشسته شد. رساله دکترای وی را تحت عنوان «تسلیحات و حقوق مخاصمات مسلحانه» انتشارات آکسفورد در سال ۲۰۰۹ به چاپ رساند و کتاب دوم او تحت عنوان «حقوق هدفگیری» توسط انتشارات مذکور در آگوست ۲۰۱۲ منتشر شد.

روزنامه گاردین در گزارش مورخ ۲۹ نوامبر ۲۰۱۱ این سؤال را مطرح کرد: «چرا نیروهای ناتو صبح روز شنبه چندین سرباز پاکستانی را در مقر مرزی در منطقه مهماند کشتند، در حالی که تقریباً ۳۰۰ یارد با مرز افغانستان فاصله داشتند؟»[۳] نگارنده گزارش ضمن تعمق در مورد توضیحات متفاوت در باب حادثه، اعلام کرد «برای آنچه رخ داد توضیح بسیار ساده ای وجود دارد، ارتش ایالات متحده همیشه مرتکب خطاهایی مرگبار می‌شود و علیرغم مهارت فنی و قدرت نظامی عظیم، درعمل هوشمندی ناچیزی دارد.» بر اساس گزارش‌ها در سال ۲۰۱۰ «تحقیقی در مورد خدمه پهپاد نیروی هوایی ارتش آمریکا مستقر در نِوادا و فرماندهان زمینی ایالات متحده در افغانستان را به علت اشتباه گرفتن غیرنظامیان با شورشیان طی عملیات نیروهای ویژه ارتش ایالات متحده در استان اروزگان در ماه فوریه که منجر به مرگ ۲۳ غیرنظامی شد به شدت مورد انتقاد قرار داد.»[۴]

از یک نوع «عملیات نظامی از راه دور» یا حمله از راه دور که این پدیده را این‌گونه می‌نامیم، می‌گذریم و به پدیده‌ای دیگر به نام عملیات‌های سایبری می‌پردازیم. در تاریخ ۲۷ و ۲۸ آوریل ۲۰۰۸ زمانی که سلسله عملیات‌های عدم ارائه خدمات، که آشکارا هماهنگ شده بود، به وبسایت های استونی طی اختلاف میان آن کشور و روسیه ضرباتی وارد نمود، استفاده نظامی از عملیات‌های سایبری[۵] رخ داد. درخواست پینگ[۶] با کوارِی‌های ناقص در وبسایت های دولتی و رسانه ای همراه می‌شود. از تاریخ ۳۰ آوریل تا ۱۸ می ۲۰۰۷ عملیات‌های پراکنده با هدف اجتناب از خدمت رسانی در سایت‌های مورد هدف (اجتناب گسترده از ارائه خدمات یا DDoS) ادامه داشت. زمان بندی دقیق عملیات‌های سایبری کارایی آن‌ها را به حداکثر رساند و وبسایت های صدمه دیده به طور موقت از دسترس خارج شدند. گویا روبات‌های نرم افزاری خودکار به کار گرفته شده بودند و نتیجه آشکار آن ایراد یک صدمه‌ی دقیق بود.[۷] برخی وبسایت های استونی به وسیله حمله‌ی هکرهای معروف به وطن‌پرست متضرر شدند اما هرگز به طور رسمی مشخص نشد که کدام دولت مسئول این کار است، البته اگر از سوی یک دولت انجام شده

---

[۳] P. Chatterjee, ‘Should we allow NATO free rein to attack and kill people?’, in The Guardian, 29 November 2011, available at: http://www.guardian.co.uk/commentisfree/2011/nov/29/nato-free-range-to-kill (this and all subsequent links last visited April 2012).

[۴] For reference to the earlier cited incident, see David Zucchino, ‘US Report faults Air Force drone crew, ground commanders in Afghan civilian deaths’, in Los Angeles Times, 29 May 2010, available at: http://articles.latimes.com/2010/may/29/world/la-fg-afghan-drone-20100531.

[۵] برای اهداف مقاله‌ی حاضر حمله‌ی سایبری شامل به‌کارگیری یک رایانه برای ارتباط با رایانه‌ای دیگر در تحقق اهداف یک مخاصمه‌ی مسلحانه است. بنابراین حمله‌ی سایبری شامل استفاده از یک رایانه برای حمله به یک رایانه‌ی دیگر و درنتیجه ایجاد آثار خشونت‌بار از جمله‌ی خسارت به اموال و جان یا مجروح کردن یک شخص نیز می‌شود. ر.ک. Michael N. Schmitt, ‘Cyber operations and the *jus in bello*: key issues’, in *International Law Studies*, Vol. 87, 2011, pp. 93–94.

[۶] Ping

[۷] Eneken Tikk, Kadri Kaska and Liis Vihul, International Cyber Incidents: Legal Considerations, CCD COE Publications, Talllinn, 2010, pp. 18–25. Note also that a DDoS operation on 26–28 April 2008, which targeted the website of Radio Free Europe/Radio Liberty’s Belarus service, is reported and discussed at E. Tikk, ibid., pp. 39–48, as is a cyber operation that targeted Lithuania on 17 June 2008, E. Tikk, ibid., pp. 51-64.

بود.[۸] سپس در سال ۲۰۰۸ عملیات‌های سایبری علیه گرجستان طی مخاصمه مسلحانه آن کشور با روسیه صورت گرفت.

عملیات استاکسنت[۹] در سال ۲۰۱۰ علیه ایران نیز شاید از جمله عملیات‌های سایبری بود که بعد نظامی آن چشمگیرتر بود. استاکسنت مجموعه ای ادغام شده از عناصری است که جهت حمله به شبکه‌های رایانه‌ای مورد استفاده قرار گرفت. استاکسنت با استفاده از یک کرم به عنوان مکانیزم انتقال، به عنوان مثال از طریق استفاده از فلش درایو یا سی. دی. رام تا اندازه ای خود را بر روی شبکه‌های غیرمتصل قرار می‌دهد و به دنبال یک مدل ویژه از تجهیزات کنترل رایانه می‌گردد (در قضیه حمله به ایران یک سیستم کنترل ساخت زیمنس به کار گرفته شده بود) و آن را می‌یابد و خود را بر روی گره مربوطه جایگزین می‌کند و فعالیت از پیش برنامه ریزی شده را به اجرا در می‌آورد. گزارش‌ها حاکی از آن است طی عملیات جولای ۲۰۱۰ که بدافزارها به سانتریفیوژهایی که آشکارا با برنامه هسته ای ایران در ارتباط بودند حمله و ظاهراً خساراتی وارد کردند.[۱۰] در حالی که تخریب وبسایت ها که در نمونه مربوط به استونی تبیین شد، گویا از حیث حقوق جنگ مطرح نبوده است[۱۱] اما محتمل است که حمله استاکست از لحاظ حقوقی به دلیل خسارات احتمالی که به سانتریفیوژها وارد شده است چنین تلقی شود.

استفاده از این تکنیک‌های سایبری طی مخاصمات مسلحانه جهت ارتکاب حملات، به معنای کشتار، صدمه یا خسارت یا تخریب یا به کارگیری سکوهای هدایت از راه دور[۱۲] یا سکوهای خودکار بدون سرنشین در آینده جهت انجام حملات در راستای هدف مقاله حاضر در حیطه‌ی تعریفی می‌گنجد که ما آن را «حمله از راه دور» می‌نامیم.

---

[۸] William A. Owens, KennethW. Dam and Herbert S. Lin, Technology, Policy, Law and Ethics Regarding US cquisition and Use of Cyberattack Capabilities, National Research Council of the National Academies, The National Academies Press, Washington D.C., 2009, pp. 173–176.

[۹] Stuxnet

[۱۰] این خسارات از سوی ایران مورد تأیید قرار نگرفت. با این حال ر.ک. Jonathan Fildes, ‘Stuxnet worm “targeted high value Iranian assets”’, in BBC News, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and William J. Broad, John Markoff and David E. Sanger, ‘Israeli test on worm called crucial in Iran nuclear delay’, in New York Times, 15 January 2011, available at: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

[۱۱] ر.ک. ماده ۴۹ پروتکل الحاقی اول که حمله را به عنوان توسل به خشونت، چه در حمله و چه در دفاع، تعریف می‌کند.

[۱۲] درخصوص مباحث مطرح شده پیرامون استفاده از تجهیزات بدون سرنشین برای انجام حمله در عملیات‌های کنونی ر.ک. Karen DeYoung, ‘U.S. officials cite gains against Al-Qaeda in Pakistan’, in Washington Post, 1 June 2009, available at: http://www.washingtonpost.com/wp-dyn/content/article/2009/05/31/AR2009053102172.html; the associated analysis by Kenneth Anderson in ‘The continuing predator drone campaign in Pakistan’, in Opinio Juris Blog, 1 June 2009, available at: http://opiniojuris.org/2009/06/01/the-continuing-predator-drone-campaign-in-pakistan/; and Karen DeYoung, ‘CIA idles drone flights from base in Pakistan’, in Washington Post, 1 July 2011, available at: http://www.washingtonpost.com/world/national-security/cia-idles-drone-flights-from-base-in-pakistan/2011/07/01/AGpOiKuH_story.html. درخصوص استقبال ایالات متحده از اهمیت راهبردی حملات به القاعده با استفاده از تجهیزات بدون سرنشین. ک. Eric Schmitt and Mark Mazzetti, ‘Obama adviser outlines plans to defeat Al Qaeda’, New York Times, 29 June 2011, available at: http://www.nytimes.com/2011/06/30/world/30terror.html.

چنین حملاتی از این حیث «از راه دور» هستند که کاربرِ وسیله‌ی هدایت از راه دور یا آغاز کننده‌ی مأموریت خودکار یا حمله سایبری احتمالاً در فاصله‌ای قابل توجه از صحنه‌ای واقع شده است که در آن حمله منجر به صدمه یا تخریب شده است. هدف مقاله‌ی حاضر بررسی این موضوع است که آیا انجام حملات از راه دور با استفاده از چنین تکنیک‌هایی طی مخاصمات مسلحانه منجر به مطرح شدن مسائل حقوقی می‌شود یا خیر. مؤلف از این نکته آغاز می‌کند که حملات سایبری طی مخاصمات مسلحانه تحت عنوان عملیات‌های نظامی که در آن‌ها ابزارهای سایبری برای کشتار، صدمه، خسارت یا تخریب طرف مقابل مخاصمه به کار گرفته می‌شوند، توسط حقوق مخاصمات مسلحانه تنظیم می‌شود و از این رو کشورهای عضو پروتکل الحاقی به کنوانسیون‌های ژنو مورخ ۱۲ آگوست ۱۹۴۹ و کنوانسیون ژنو مربوط به حمایت از قربانیان مخاصمات مسلحانه بین المللی (پروتکل اول)[۱۳] ملزم به رعایت قواعد مذکور در مواد ۴۸ تا ۶۷ آن معاهده هستند.[۱۴] برای کشورهای که به عضویت پروتکل اول در نیامده اند، اصول و قواعد عرفی به ویژه اصل عرفی تفکیک و قواعد عرفی تمایز، تناسب و اقدامات احتیاطی در حملات اعمال خواهد شد.[۱۵] هم چنین به نظر می‌رسد عموماً پذیرفته شده است که مجموعه‌ی قواعد مذکور بر حملاتی که از ادوات فاقد سرنشین یعنی هواپیماها، وسایل زمینی، کشتی‌ها یا سایر ابزارهای دریایی که حامل خدمه نیستند و یا توسط عاملی کنترل می‌شوند که در فاصله‌ای دور قرار دارد یا آن که هدایت خودکار و فناوری حمله را به کار می‌گیرند، اعمال می‌شوند.[۱۶] در ابتدا با ارجاع به قلمرو هوایی به بحث در مورد این مسائل می‌پردازیم

---

[۱۳] Adopted in Geneva, 8 June 1977

[۱۴] درخصوص مباحث موجود بر سر این مساله ر.ک. Michael N. Schmitt, 'Cyber operations and the jus in bello: key issues', in US Naval War College Blue Book, 'International Law and the Changing Character of War', Vol. 87, 2011, p. 89.

[۱۵] درعمل بسیاری از قواعد پروتکل اول، مواد ۴۸ لغایت ۶۷، دارای ماهیت عرفی هستند و بنابراین برای تمام دولت‌ها الزام‌آور تلقی می‌شوند، ر.ک. Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, Vol. 1: Rules, Cambridge University Press, 2005 (hereafter 'ICRC Study')؛ گرچه به عقیده‌ی نگارنده قواعد موجود در مواد ۳۵(۳) و ۵۵ و ۵۶ پروتکل اول دارای وضعیت عرفی نشده‌اند، به اصل تفکیک به‌صورتی که در قاعده‌ی یک از مطالعه‌ی قواعد عرفی توسط صلیب سرخ درج شده است توجه کنید: «طرف‌های مخاصمه باید در تمام زمان‌ها میان غیرنظامیان و رزمندگان تفکیک قائل شوند. حملات تنها می‌توانند علیه رزمندگان باشند. حملات نباید علیه غیرنظامیان صورت گیرد.» همچنین به این حکم دیوان بین‌المللی دادگستری توجه کنید که عنوان می‌داد اصل تفکیک «یکی از اصول غیرقابل تخطی حقوق بین‌الملل عرفی است» International Court of Justice, Advisory Opinion on the Threat or Use of Nuclear Weapons, ICJ Reports, 8 July 1996, p. 257, para. 79.؛ مطالعه‌ی صلیب سرخ اصل تفکیک را در قواعد ۱۱ در صفحه‌ی ۳۷، قاعده‌ی ۱۲ در صفحه‌ی ۴۰، قاعده‌ی ۱۳ در صفحه‌ی ۴۳ و قاعده‌ی ۱۴ در صفحه‌ث ۴۶ منعکس می‌کند. این قواعد به ترتیب حملات غیر تفکیکی را ممنوع کرده، آنچه را که شامل حمله می‌شود تعیین کرده، و سپس بازتاب ماده‌ی (الف)(۵)۵۱ و (ب) از پروتکل اول هستند که در این معاهده به عنوان مصادیق حمله‌ی غیر تفکیکی ذکر شده‌اند، و بعداً بدان پرداخته می‌شود. این قواعد عرفی احتیاطی طرف حمله‌کننده را ملزم می‌دارد درحملات خود اقدامات معینی را انجام دهد. این قواعد احتیاطی عرفی در قواعد ۱۸ تا ۲۰ در صفحات ۵۸ تا ۶۵ قید شده است. درخصوص مباحث مربوط به قواعد عمل هدف گیری ر.ک. William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, Chapter 5.

[۱۶] See, for example, the discussion in 'Targeting operations with drone technology: humanitarian law implications', in Background Note for the American Society of International Law Annual Meeting, Human Rights Institute, Columbia Law School, 25 March 2011.

و ابزارهای کنترل شده توسط کاربر را «ابزارهای کنترل از راه دور» می‌نامیم، در حالی که اشاره به خودکار بودن بر ادواتی اعمال می‌شود که بدون نظارت عامل انسانی تصمیم به حمله می‌گیرند. از این رو سؤال مورد بحث در رابطه با هر دو روش حمله این است که آیا غایب بودن شخصی که حمله را انجام می‌دهد از موقعیت عملیاتی موجب طرح مسائل حقوقی می‌شود یا خیر.

در ابتدا حملاتی را مورد ملاحظه قرار می‌دهیم که در آن‌ها از تجهیزات کنترل از راه دور استفاده می‌شود. سپس به صورت مختصر مسائل مرتبط با اقدامات احتیاطی در حملات فناوری‌های حمله خودکار را بر می شمریم. در بخش سوم مقاله به طور خلاصه به این موضوع می‌پردازیم که چگونه قواعد هدف گیری در پروتکل اول بر حملات سایبری قابل اعمال است. سپس در بخش چهارم تحلیل می‌کنیم که چالش‌های مربوط به دور بودن در چه مواقعی بروز می‌یابد. در بخش پنجم بررسی می‌شود که مسئولیت این حملات متفاوت بر عهده کیست. در آخرین بخش ماهوی این سؤال مطرح می‌شود که آیا این فناوری‌های جدید تغییری کیفی در اقدامات جنگی یا توسعه بیش از پیش روندی تکاملی و پیشرفته تلقی می‌شوند و این نیز اساساً منجر به طرح این سؤال می‌شود که آیاموضوع مورد بحث حقیقتاً از لحاظ ماهوی پدیده جدیدی است. در نهایت می‌کوشیم نتایجی استخراج کنیم.

وسایل کنترل از راه دور و حقوق

دور بودن کنترل کننده از حمله به خودی خود مانع از اعمال حقوق [حاکم بر] هدف‌گیری بر چنین فعالیت‌هایی نمی‌شود. اصل حقوقی تفکیک،[۱۷] ممنوعیت حملات غیر تفکیکی،[۱۸] قواعد اقدامات احتیاطی و مفاد جزئی تری که حمایت از برخی اشخاص و اشیاء را الزامی کنند[۱۹] بر چنین عملیات‌هایی اعمال می‌شود. کنترل کننده یک وسیله هوایی بدون خلبان پریدیتور یا ریپر (UAV)[۲۰] گرچه هزاران مایل با صحنه مورد حمله فاصله دارد، تصمیمات خود را بر مبنای اطلاعات کسب شده ازحسگرها و سایر منابع اتخاذ می‌کند و ملزم به رعایت قواعد هدفگیری از

---

[۱۷] ماده ۴۸ پروتکل اول مقرر می‌دارد: «به منظور تضمین احترام به و حمایت از جمعیت غیرنظامی و اشیاء غیر نظامی، طرف‌های مخاصمه باید همواره میان جمعیت غیرنظامی و رزمندگان و میان اشیاء غیرنظامی و اهداف نظامی تفکیک قائل شوند و بنابراین باید عملیات خود را تنها علیه اهداف نظامی هدایت کنند.» در ماده ۵۲(۲) پروتکل اول اصطلاح «اهداف نظامی» تاجایی که به اشیاء مربوط می‌شود، تعریف شده است.

[۱۸] با توجه به ماده‌ی ۵۱(۴) حملات اگر بر ضد یک هدف نظامی مشخص نباشند، اگر از ابزار یا روشی استفاده کنند که نمی‌توان آن را بر ضد یک هدف نظامی مشخص به‌کار گرفت، یا آثار آن را نمی‌توان بدانگونه که در حقوق بین‌الملل مقرر شده است محدود کرد، و در تمام مواردی که دارای چنان ماهیتی هستند که به اهداف نظامی و غیرنظامیان یا به اشیاء غیر نظامی بدون تفکیک حمله می‌کنند، غیر تفکیکی و در نتیجه ممنوع محسوب می‌شوند. حمله‌ای که انتظار می‌رود جراحت تصادفی بیش از اندازه به غیرنظامیان و/یا اشیاء غیرنظامی وارد می‌کند طبق ماده‌ی ۵۱(۵) نمونه‌ای از یک حمله‌ی غیرتفکیکی است.

[۱۹] برای مثال ممنوعیت هدف قراردادن جمعیت غیرنظامی، افراد غیرنظامی، یا اشیاء غیرنظامی به عنوان موضوع حمله در مواد ۵۱(۲) و ۵۱(۱) از پروتکل اول.

[۲۰] Predator or Reaper Unmanned Aerial Vehicle

جمله قواعد اقدامات احتیاطی در حملات، همچون سایر کاربران نظامی در میدان نبرد از جمله خلبان یک هواپیمای باسرنشین است.

بر این اساس کاربر یک وسیله‌ی هوایی بدون سرنشین باید پیوسته به مراقبت از غیرنظامیان و اهداف غیرنظامی هنگام انجام عملیات‌های نظامی به صورت کلی توجه داشته باشد؛[۲۱] او باید به هر اقدام عملی یا عملاً ممکن[۲۲] متوسل شود تا «اطمینان حاصل کند که اهداف مورد حمله از جمله افراد یا اهداف غیرنظامی و موضوع حمایت‌های خاص نیستند و اهداف نظامی هستند و این که حمله به آن‌ها ممنوع نیست.» او باید هنگام انتخاب ابزارها و روش‌های حمله، با هدف اجتناب از و تحت هر شرایطی، به حداقل رساندن آسیب احتمالی به جان غیرنظامیان، آسیب به غیرنظامیان و خسارت به اشیاء غیرنظامی به هر اقدام عملی یا عملاً ممکن متوسل شود؛[۲۳] او باید از «تصمیم گیری در مورد آغاز حمله ای که انتظار می‌رود منجر به صدمه و/یا خسارت احتمالی نامتناسب به غیرنظامیان می‌شود»[۲۴] خودداری کند؛ اگر روشن شود که هدف حمله هدفی نظامی نیست او باید حمله را به حال تعلیق درآورد یا لغو کند ، هدف آن موضوعِ یک حمایت خاص است یا آن که انتظار می‌رود حمله منجر به خسارت و آسیب احتمالی نامتناسب به غیرنظامیان شود؛[۲۵] او باید اطمینان حاصل کند که اگر ممکن است غیرنظامیان از حمله آسیب ببینند، هشدار مؤثر پیش از موعد داده شده است مگر آن که شرایط اجازه چنین کاری ندهد؛[۲۶] و باید اطمینان حاصل کند که «زمانی که انتخاب از میان چند هدف نظامی برای حصول یک امتیاز نظامی مشابه ممکن است، هدف منتخب هدفی است که پیش بینی می‌شود «حمله به آن ممکن است منجر به کمترین خطر برای جان غیرنظامیان و اهداف غیرنظامی شود.»»[۲۷] این قواعد احتیاطی طرفین را به پایبندی به کنوانسیون حمایت از قربانیان مخاصمات مسلحانه به عنوان موضوعی در چارچوب حقوق معاهدات ملزم می‌کنند و همان طور که پیش از این گفته شد تا حد زیادی عرفی هستند و در نتیجه تمام دولت‌ها را ملزم می‌کنند. از تحلیل مذکور این نتیجه حاصل می‌شود که وظایف احتیاطی فرد کنترل کننده‌ی یک وسیله‌ی هوایی بدون سرنشین مسلح هم

---

[۲۱] Article 57(1) of API.

[۲۲] ادبیات به‌کار رفته در ماده ()(الف)(۲)۵۷ عنوان می‌دارد «هرآنچه امکان‌پذیر است» (Everything Feasible) که به عقیده‌ی انگلستان به معنی هرآنچه «به صورت عملی یا از نظر عملی ممکن است با درنظر گرفتن تمام اوضاع و احوال حاکم در آن زمان از جمله ملاحظات بشردوستانه و نظامی» UK statement (b) made on ratification of API on 28 January 1998. Consider also Eritrea/Ethiopia Claims Commission, Partial Award, Central Front, Ethiopia's Claim 2, 28 April 2004, para. 110, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

[۲۳] Article 57(2)(a)(ii) of API.

[۲۴] Article 57(2)(a)(iii) of API.

[۲۵] Article 57(2)(b) of API.

[۲۶] Article 57(2)(c) of API.

[۲۷] Article 57(3) of API.

چون مواردی که بر خلبان هواپیمان دارای سرنشین تحمیل می‌شود، سخت گیرانه است. وظایف مذکور به خاطر عدم وجود شخص در کابین فرمان از بعد حقوقی کاسته نمی‌شود.[۲۸]

حمله مستقل و حقوق

واژه «استقلال» در راستای اهداف بحث حاضر جهت اشاره به تصمیم گیری در مورد حمله مستقل به کار می‌رود که به عنوان مثال توسط فناوری الگوریتم-محور در یک وسیله‌ی فاقد سرنشین هم چون یک هواپیما صورت می‌گیرد.[۲۹] این فناوری به عنوان مثال می‌تواند به نوعی طراحی شود که اهداف نظامی خاصی مانند یک تانک، یک توپ یا نفربرهای زرهی را شناسایی کند. اگر فناوری مذکور به قدر کافی بین اشیاء نظامی و اشیاء غیرنظامی تفکیک قائل شود، به نظر می‌رسد که الزام مقرر در ماده 57(2)(a)(i) پروتکل اول[۳۰] می‌تواند رعایت شود، مشروط به آن که بتوان به درستی گفت «هرآنچه ممکن است» صورت گرفته تا تمایز مدنظر انجام شود. در پرتو بیانیه تفسیری بریتانیا که پیش‌تر ذکر شد، ملاحظات نظامی را می‌توان مد نظر قرار داد تا این که مشخص شود چه اقدامی عملاً ممکن و از این رو به عنوان اقدام احتیاطی ممکن، الزامی است. این استدلال که فقدان عامل انسانی از جهت استقلال روند تصمیم گیری اجرای وظایف احتیاطی را ناممکن می‌کند و از این رو این اقدامات باید از نظر نظامی ناممکن تلقی شوند، از دید مؤلف قانع کننده نیستند، به ویژه به این دلیل که روش‌های جایگزین برای صورت دادن این حملات اتخاذ اقدامات احتیاطی را مجاز می‌کند. از این رو دیدگاه بهتر از این قرار است که کل مجموعه اقدامات احتیاطی مقرر در ماده ۵۷ پروتکل اول و خلاصه شده در بخش قبلی مقاله حاضر باید در رابطه با حملات مستقل رعایت شود.

در حالی که پایبندی به ماده 57(2)(a)(i) پروتکل اول همان طور که در بخش قبل ذکر شد،[۳۱] قابل تحقق است، اگر قواعد ارزیابی اقدامات احتیاطی را مد نظر قرار دهیم، مسائل دشوارتر می‌شود. این وظایف احتیاطی مضاعف که در بخش قبل برشمرده شده و تکرار آن‌ها ضروری نمی‌نماید، این سؤال چالش برانگیز را پیش می‌آورد

---

[۲۸] مساله‌ی جالب این است که آیا عدم حضور یک فرد در کابین فرمان تبعیت از این قواعد را سهل‌تر یا دشوارتر می‌گرداند. پاسخ دادن به این پرسش شامل درنظر داشتن این امر می‌شود که آیا مشاهدات مستقیم در مقایسه با مشاهادات مبتنی بر حسگر از هدف مورد نظر، توسط فردی که درمورد یک حمله‌ی خاص تصمیم گیری می‌کند، در اوضاع و احوال مربوطه در صورتی که از ادوات با سرنشین استفاده می‌شد، ممکن بوده است؛ آیا چنین مشاهدات مستقیمی در اوضاع و احوال غالب درخصوص کیفیت تصمیم گیری در حمله تغییری ایجاد می‌کرد؛ آیا اقدامات دشمن توجه خلبان را از امر هدفگیری منحرف کرده است؛ آیا دیگر موانع وجود داشته‌اند؛ و بسیاری از موارد مربوطه‌ی دیگر.

[۲۹] واژه‌ی استقلال گاه برای اشاره به برخی از جنبه‌های سیستم‌های ناوبری تجهیزات به‌کار می‌رود. در مقاله‌ی حاضر، این واژه به‌طور خاص به روش حمله اشاره دارد، خصوصاً در روشی که از طریق آن هدف سلاح انتخاب می‌شود.

[۳۰] این قاعده دارای ماهیت عرفی است ر.ک. Rule 18 of the ICRC Study and the discussion at W. Boothby, p. 73.

[۳۱] See Bill Boothby, ‘The law relating to unmanned aerial vehicles, unmanned combat aerial vehicles and intelligence gathering from the air’, in Humanitäres Völkerrecht – Informationsschriften, Vol. 24, issue 2, 2011, p. 81.

که آیا فناوری قادر به مکانیزه کردن قضاوت‌های اساساً ارزشی هست یا خیر. این قضاوت‌ها این سؤال را نیز در بر می‌گیرد که آیا ابزارها و روش‌های منتخب برای انجام حمله‌ی برنامه‌ریزی‌شده در حقیقت صدمه به غیرنظامیان و خسارت به اشیاء غیرنظامی را به حداقل می‌رساند و آیا صدمه به غیرنظامیان و خسارت به اشیاء غیر نظامی که انتظار می‌رود از یک حمله با طبقه‌ای خاص از هدف نظامی در یک حادثه خاص نسبت به امتیاز نظامی پیش‌بینی‌شده فراتر خواهد بود یا خیر. بیانیه بریتانیا و سایر دولت‌ها در مورد تصویب پروتکل اول مبنی بر این که امتیاز نظامی آن مزیتی است که از حمله مد نظر به صورت یک کل حاصل می‌شود،[۳۲] متضمن آن است که ارزیابی تناسب باید بر چیزی بیش از مداخله‌ی یک هدف منفرد [در احتساب مزیت نظامی] اعمال شود.[۳۳]

مع الوصف، این احتمال وجود داردکه یک ابزار یا روش جنگی[۳۴] از نظر حقوقی نامقبول تلقی شود اگر: مانع اتخاذ اقدامات احتیاطی در ارزیابی شود که از منظر حقوقی الزامی هستند. روش‌های حمله مستقل به هر صورت الزاماً مانع اتخاذ اقدامات احتیاطی نمی‌شود. از این رو برنامه‌ریزان و تصمیم‌گیران عملیات که به انجام عملیات مستقل می‌اندیشند احتمالاً در موقعیتی هستند که داده‌های مربوط به الگوی زندگی مرتبط با منطقه‌ی مورد بررسی را مورد بازبینی قرار دهند. آن‌ها به بازبینی داده‌ها می‌پردازند تا پیش از آغاز مأموریت مستقل بتوانند کشتار، صدمه و خسارت به غیرنظامیان را که پیش بینی می‌شود در اثر حمله به یک گروه برنامه‌ریزی‌شده از اهداف نظامی در منطقه‌ای خاص طی دوره تحقیقاتی برنامه‌ریزی‌شده با استفاده از سلاح‌های بارشده بر تجهیزات رخ دهد، مورد ارزیابی قرار دهند. مزیت نظامی که پیش بینی می‌شود از حمله به هدفی برنامه ریزی شده که فناوری الگوریتم آن را تشخیص می‌دهد حاصل شود، در مرحله برنامه ریزی تعیین خواهد شد و از این رو به الگوی زندگی در منطقه مربوطه وابسته بوده و ممکن است بر قواعد اقدامات احتیاطی ارزیابی در مرحله برنامه ریزی مأموریت منطبق باشد و از این رو موجب شود استفاده از فناوری حمله مستقل احتمالاً قانونی تلقی شود. به احتمال زیاد اگر منطقه تحقیقاتی برنامه‌ریزی‌شده از غیرنظامیان و اهداف غیرنظامی فاصله داشته باشد این امر محقق خواهد شد؛ مناطق بیابانی، مناطق کوهستانی دور افتاده و مناطق دریایی دوردست نمونه‌هایی از این دست هستند. هم چنین ممکن است اگر به هر دلیلی، داده‌های الگوی زندگی آشکارا نشان دهند که غیرظامیان در زمان تحقیقات برنامه ریزی شده در یک منطقه‌ی کمتر دورافتاده حضور ندارند، این امر محقق گردد.

---

[۳۲] UK statement (i) made on ratification of API on 28 January 1998.

[۳۳] این اعلامیه با اشاره به مواد ۵۱ و ۵۷ صورت پذیرفته است. نگریستن به اقدامات خصمانه منفرد به صورت مجذا «ممکن است مشکلات ناشی از راهبردهای امروزین جنگی را نادیده انگارد، که بدون استثنا بر مجموعه‌ای یکپارچه از اقدامات منفرد مبتنی شده‌اند که یک عملیات نهایی ترکیبی را تشکیل می‌دهند.... عملیات نظامی جمعی متخاصمان را شاید نتوان به اقدامات منفرد بسیاز زیاد تقسیم کرد، در غیر این صورت هدف عملیاتی که عملیات کلی برای آن طراحی شده است از نظر دور خواهد ماند.» Stefan Oeter, ‘Methods and means of combat’, in D. Fleck (ed.), The Handbook of International Humanitarian Law, 2nd edn, 2009, p. 186.

[۳۴] تجهیزات نظامی خاص بخشی از سیستم تسلیحاتی را تشکیل می‌دهند که با یک موشک و غیره مرتبط است. این تجهیزات بخشی از آن ابزار جنگی تلقی می‌شود.

در مقابل اگر قضاوت‌های مربوط به کاهش مرگ، آسیب و صدمه به غیرنظامیان و نیز متناسب بودن حملات در مرحله برنامه ریزی حمله به عنوان مثال به دلیل ماهیت متراکم شهری مربوط به محدوده‌ی مورد بررسی یا به هر دلیل دیگری ممکن نباشد، پیش بینی مرگ، آسیب یا صدمه به غیرنظامیان پیش از انجام مأموریت با یک اطمینان قابل قبول ممکن نیست و در نتیجه اقدامات احتیاطی ارزیابانه قابل اتخاذ نیست و این نتیجه را در پی دارد که تصمیم گیری در مورد به‌اجرا در آوردن عملیات مستقل در چنین شرایطی، نقض ماده ۵۷ تلقی می‌شود.

تمرکز بحث حاضر بر آن دسته از حملات مستقل است که اهداف ذاتاً نظامی را هدف قرار می‌دهند و دارای ویژگی‌هایی هستند که تشخیص مکانیکی را تسهیل می‌نماید. تا جایی که مشخص شده است، در حال حاضر فناوری که از تفکیک مستقل پرسنل نظامی از غیرنظامیان پشتیبانی کند وجود ندارد. تنها زمانی که فناوری حمله خودکار بتواند این تفکیک را تا میزان قابل قبولی قائل کند و تنها زمانی که، پس از تفکیک قائل شدن، این فناوری اتخاذ تصمیمات ارزیابانه مذکور در چارچوب حملاتی که انسان‌ها را هدف قرار می‌دهد ممکن سازد، مبنایی برای بحث در مورد حمله مستقل به انسان‌ها وجود خواهد داشت. مؤلف از وجود چنین سیستمی که تاکنون معرفی شده باشد آگاهی ندارد و بر این اساس نتیجه گیری می‌کند که حمله مستقل به پرسنل می‌تواند دست کم در حال حاضر، بر این اساس مستثنی شود که امکان پایبندی به قواعد مربوط به اقدامات احتیاطی در حمله وجود ندارد.[۳۵]

حملات سایبری و حقوق

[۳۵] برای مطالعه‌ی مباحث مربوط به رویکردهای فناوری به تصمیم گیری روباتیک برای فائق آمدن بر مسائل مطرح شده در این مقاله ر.ک. See, however, Ronald C. Arkin, Governing Lethal Behavior in Autonomous Robots, CRC Press Taylor & Francis Group, Boca Raton, F.A., 2009, برای مطالعه‌ی این نظر که ملزومات فناوری پیش از حمله‌ی مستقل احتمالاً از نظر حقوقی قابل قبول خواهد شد ر.ک. Tony Gillespie and Robin West, 'Requirements for autonomous unmanned air systems set by legal issues', in The International C2 Journal, Vol. 4, No. 2, 2010, pp. 1–32, available at: http://www.dodccrp.org/files/IC2J_v4n2_02_Gillespie.pdf. درخصوص وجود یک تعهد اخلاقی برای استفاده از ادوات هوایی بدون سرنشین ر.ک. Bradley J. Strawser, 'Moral predators: the duty to employ uninhabited aerial vehicles', in Journal of Military Ethics, Vol. 9, No. 4, 2010, pp. 342–344. برای مطالعه‌ی این تحلیل که چرا انسان‌ها ممنوعیت‌های حقوقی و اخلاقی در حمله به غیرنظامیان را نقض می‌کنند و این مساله که تکنیک‌های حملات روباتیک احتمالاً چنین رفتار غیرقابل پذیرشی را حذف خواهد کرد ر.ک. Ronald C. Arkin, 'The case for ethical autonomy in unmanned systems', in Journal of Military Ethics, Vol. 9, No. 4, 2010, pp. 332.

عصر رایانه محیطی دیگر را به‌وجود آورده است که در آن مخاصمات می‌توانند به اجرا درآیند.[۳۶] وابستگی جوامع مدرن و نیروهای مسلح آن‌ها به سیستم‌های رایانه‌ای این سیستم‌ها را به هدف اولیه حمله یا انتخابی واسط تبدیل کرده است که از طریق آن می‌توان برخی اهداف یا اشخاص مرتبط را هدف قرار داد.[۳۷] رخدادهای سال ۲۰۰۷ در استونی،[۳۸] گرجستان ۲۰۰۸[۳۹] و ۲۰۱۰ در ایران[۴۰] نشان می‌دهد که استفاده خصمانه از عملیات‌های سایبری به صورت فزاینده به بعدی مهم از نبردها در دهه‌های آینده تبدیل خواهد شد. عملیات‌های سایبری را می‌توان عملیات‌هایی نظامی قلمداد کرد که در آن‌ها یک رایانه دستگاه رایانه‌ی دیگری را مورد هدف قرار می‌دهد یا از آن به عنوان ابزاری استفاده می‌شود که از طریق آن خسارت یا آسیب به طرف مقابل در مخاصمه وارد می‌شود. استفاده از هر ابزاری از جمله یک رایانه جهت کشتن، صدمه یا آسیب و تخریب طرف مقابل در مخاصمات مسلحانه موجب می‌شود آن ابزار یا رایانه مذکور به سلاح یا ابزار جنگی تبدیل شود.[۴۱] خسارت یا صدمه ممکن است به کاربران سیستم رایانه‌ای مورد هدف وارد شود یا خود سیستم هدف ممکن است آسیب ببیند. در هرصورت این رخداد موجب می‌شود عملیات سایبری حمله سایبری تلقی شود. مسئله حیاتی در راستای هدف مقاله‌ی حاضر این است که ممکن است عملیات از بعد زمان و مکان در فاصله‌ای بسیار دور از زمان و مکانی که بناست که عواقب مخرب رخ دهد، واقع شده باشد. مفهوم دور بودن کاربر از نتایج عمل خود با این مسئله ترکیب شده است، که احتمالاً به هنگام پاسخ به این مسئله و ممکن بودن پاسخ به آن مطرح می‌شود، که اولاً چه کسی حمله سایبری مورد نظر را

---

[۳۶] واژه‌ی «محیط» به این دلیل به‌کار رفته است که دیدگاه‌ها درخصوص این امر که آیا می‌توان فضای سایبری را به درستی به عنوان یک «قلمرو» (domain) تعریف کنیم، بسیار متفاوت هستند. Michael V. Hayden, 'The future of things "cyber"', in Strategic Studies Quarterly, Vol. 5, No. 1, Spring 2011, pp. 3–4; John A. Shaud, 'An Air Force strategic vision for 2020–2030', in Strategic Studies Quarterly, Vol.5, No. 1, Spring 2011, pp. 8–17.

[۳۷] برای مثال به عملیاتی توجه کنید که درماه می ۲۰۰۹ موجب خاموش شدن شبکه‌ی رایانه‌های اف. بی. آی. شد. Bill Gertz, 'Inside the ring', in The Washington Times, 18 June 2009, available at: http://www.washingtontimes.com/news/2009/jun/18/inside-the-ring-95264632/?page=all؛ برای معرفی مقیاس و گستره‌ی جاسوسی سایبری ر.ک. Sean Rayment, 'How safe are Britain's cyber borders?', in The Sunday Telegraph, 26 June 2011, available at: http://www.telegraph.co.uk/news/uknews/defence/8598952/How-safe-are-Britainscyber-borders.html.،

[۳۸] See E. Tikk, et al., above note 4, pp. 18–25; and W. A. Owens, et al., above note 5, pp. 173–176.

[۳۹] J. Markoff, 'Georgia takes a beating in the cyberwar with Russia', in New York Times, Bits Blog, 11 August 2008, available at: http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar- with-russia/; European Union Independent International Fact Finding Mission on the Conflict in Georgia, Report (2009); and see also E. Tikk, et al., above note 4, pp. 67–79.

[۴۰] J. Fildes, 'Stuxnet worm attacked high value Iranian assets', in BBC News, 23 September 2010, available at: http://www.bbc.co.uk/news/technology-11388018; and W. J. Broad, et al., above note 12.

[۴۱] For the meaning of weapon see Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol 1', in International Review of the Red Cross, Vol. 85, No. 850, June 2003, p. 397. For the meaning of 'means of warfare', see William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 4.

انجام داده است و دوما آن که از جانب کدام دولت یا سازمان عملیات انجام شده است و سوم آن که هدف چه بوده است.

در این راستا موضوع حقوقی از مشکلی ناشی می‌شود که برنامه‌ریز و تصمیم‌گیرنده احتمالاً هنگام ارزیابی پیش‌دستانه به نتایج مورد انتظار از حمله سایبری برنامه ریزی شده با آن مواجه بوده‌اند. جهت انجام هر گونه ارزیابی عملی از مشروعیت حمله برنامه ریزی شده آن‌ها باید به قدر کافی از پیوندهای سایبری میان رایانه‌ی ارسال کننده و رایانه‌ی هدف مطلع باشند تا به قدر کفایت اطمینان حاصل کنند که حمله مذکور در حقیقت هدف مورد نظر را در بر می‌گیرد. دوما آن‌ها باید به قدر کافی از ویژگی‌های قابلیت سایبری خاص جهت انجام حمله آگاهی داشته باشند تا به قدر کافی اطمینان حاصل کنند که حمله مذکور به روش مورد نظر هدف را درگیر می‌کند. سوما آن‌ها باید در مورد سیستم رایانه‌ی هدف، وابسته‌های آن و شبکه متصل به آن اطلاعات کافی داشته باشند تا بتوانند متناسب بودن حمله مورد نظر را مورد ارزیابی قرار دهند. در نهایت اگر قابلیت سایبری که بناست در حمله استفاده شود ممکن است هنگام انتقال به سیستم هدف بر سایر شبکه‌ها صدمه بزند، تاثیرات مورد انتظار بر روی سایر شبکه‌ها باید ارزیابی شود تا اندازه ای که آن شبکه‌ها خود شامل اهداف نظامی نباشند، خسارت وارده به آن‌ها، خسارت یا صدمه غیرمستقیم به کاربران آن‌ها باید در ارزیابی تناسب که پیش از تصمیم گیری جهت انجام حمله سایبری صورت می‌گیرد، لحاظ شود.

ترسیم نقشه سیستم هدف، وابسته‌های آن و پیوندهای واسط بدین روش احتمالاً وظیفه‌ای چالش برانگیز است. ترسیم نقشه به روشی غیرمستقیم احتمالاً دشوارتر هم خواهد بود. حفظ امنیت عملیات با عدم ارزیابی متناسب بودن حمله برنامه ریزی شده احتمالاً به همان دلایل گفته شده در بخش قبل نقض ماده ۵۷ قلمداد می‌شود.

زمانی که چالش دور بودن مطرح می‌شود

آن چه از تحلیل بالا حاصل می‌شود این است که فاصله‌ی زمانی و مکان به تنهایی نمی‌تواند موجب غیرقانونی شدن حمله شود. تاثیری که دور بودن بر توانایی تصمیم گیرندگان و برنامه ریزان جهت اقدامات احتیاطی لازم و دستیابی به اطلاعات جهت پشتبانی از ارزیابی عملی قانونی بودن یک حمله برنامه ریزی شده می‌گذارد، در عمق مسئله نهفته است. به بیان ساده تر، تنها هنگامی که پیشرفت‌های فناوری که حمله از راه دور را ممکن می‌کنند، خواه سایبری، مستقل یا کنترل از راه دور، توسط قابلیت فنی هماهنگ شوند تا در مورد اقدامات احتیاطی استاندارد که بر اساس حقوق در رابطه با تمام حملات لازم است، استفاده از قابلیت‌های حمله از راه دور مشروع خواهند شد. این موضوع به صورت گسترده در رابطه با مأموریت‌های کنترل از راه دور محقق و اثبات شده است. همان طور که در بندهای آغازین مقاله آمده است آشکار است که در برخی موارد خطاهایی صورت می‌گیرد، اما بروز خطا قانونی

بودن روش جنگی را زیر سؤال نمی‌برد. بلکه مسئله از این قرار است که آیا می‌توان روش مذکور را همسو با الزامات حقوقی مقرر شده که بر اساس حقوق تسلیحات اساسی تلقی می‌شوند، به کار بست یا خیر.[۴۲]

همان طور که در بخش پیشین مشخص شد، در برخی موقعیت‌های عام که به صورت مضیق تعریف شده‌اند حملات مستقل نیز می‌توانند بر اساس الزامات حقوق مخاصمات مسلحانه انجام شوند. با این حال، در حوزه سایبری تا حد زیادی به ابزار سایبری ویژه ای بستگی دارد که بناست از آن استفاده شود و نیز به ویژگی‌های آن محصول و این موضوع که آیا تأثیر خسارت بار ابزار سایبری می‌تواند به صورت منطقی به هدف مورد نظر حمله محدود شود و آیا در مورد سیستم رایانه‌ای هدف آشنایی کافی حاصل شده است تا امکان قضاوت درست در مورد اقدامات احتیاطی، از نوعی که در بالا بررسی شد، وجود داشته باشد.

پروتکل اول مقرر می‌دارد: «در مطالعه، توسعه، استحصال یا به کارگیری سلاح، ابزار یا روش جنگی جدید، کشور معظم عضو ملزم است تعیین کند که آیا به کار گیری آن در برخی یا تمام موارد، توسط کنوانسیون حاضر یا توسط سایر قواعد حقوق بین الملل قابل اعمال بر کشور معظم عضو ممنوع شده است یا خیر.»[۴۳] پس از حصول این نتیجه که قابلیت‌های سایبری که بناست جهت کشتار، صدمه یا خسارت یا تخریب طرف مقابل مخاصمه استفاده شود، بر اساس اهداف ماده ۳۶ ابزار جنگی تلقی می‌شود، روشن است که بازبینی حقوقی چنین قابلیت‌هایی الزامی است و موضوعات مورد بحث در بند قبل باید هنگام تصمیم گیری در باب این موضوع که آیا قابلیت مذکور ماهیتاً تفکیکی است یا خیر، مدنظر واقع شود.[۴۴]

ملاحظات مرتبط با مسئولیت

مسئولیت خطا در حملات از راه دور

بحث حقوقی در مورد فناوری‌های حمله از راه دور اغلب بر مسئله مسئولیت متمرکز می‌شود. هنگام بروز خطا مسئولیت بر عهده کیست؟ در مورد حملات سایبری ممکن است بسیار دشوار باشد که تعیین کنیم دقیقاً چه کسی و با کدام هدف مشخص حمله را صورت داده است. رایانه‌ای که حمله از آن آغاز شده است ممکن است در برخی موارد قابل شناسایی باشد، اما نام شخصی که سلاح سایبری را اختراع کرده، نام افراد بالقوه متفاوتی که سلاح سایبری را در مسیر خود قرار می‌دهند و دولت، گروه یا نهادهای دیگری که این اشخاص برای آن‌ها فعالیت

---

[۴۲] برای مطالعه درخصوص قابلیت اعمال قواعد جنگ بر عملیات‌های سایبری ر.ک Charles J. Dunlap, ‘Perspectives for cyber strategists on law for cyberwar’, in Strategic Studies Quarterly, Spring 2011, pp. 81–99.

[۴۳] Article 36 of API.

[۴۴] W. H. Boothby, above note 43, pp. 69–85 and 345–347.

می‌کنند ممکن است هرگز مشخص یا قابل افشا برای عموم نباشد. بر این اساس این مشکلات انتساب مسئولیت در مورد یک رخداد سایبری خاص را در عمل ناممکن می‌کند.

مسئولیت و مفهوم مرتبط مسئولیت برای اعمال منع نشده[۴۵] ممکن است در چارچوب‌هایی متفاوت از جمله در سطح سیاسی/دیپلماتیک، در رسانه‌ها، در حقوق بین الملل و در حقوق داخلی مطرح شود. ممکن است به شکل مسئولیت فردی از جمله شخص فرمانده، یا مسئولیت دولت درآید.

پوشش رسانه‌ای یک حادثه ممکن است به مسئولیت سیاسی ضمنی برای آن حادثه شکل بدهد یا آن را هدایت کند، همان طور که ارزیابی‌های سیاسی نیز به پوشش رسانه‌ای سمت و سو می‌دهد. گزارش اولیه رسانه‌ها که شاید تا حدی یا به طور کل بر مبنای اطلاعات مخدوش، گمانه زنی و فرضیات و واکنش نسبت به آن باشد، ممکن است در اذهان عموم مفهوم مسئولیت را تثبیت کند که بعدها اگر اطلاعاتی موثق آشکار شود زدودن آن تصورات دشوار است. افشای زودهنگام داده‌های واقعه توسط دولت‌ها از جمله تصاویر آن ممکن است در این مورد حیاتی باشد. از بعد سیاسی این به معنای ضرورت داشتن اطلاعات مرتبط است که به شکلی قابل افشا حاضر و در دسترس باشد درصورتی که دولت‌ها مایل باشند به نحوی موفقیت آمیز در ستادهای امروزین اطلاعات و رسانه مشارکت داشته باشند. مسئولیت مستعد آن است که توسط رسانه‌ها به دولت‌ها نسبت داده شود اما اگر شواهد تخلفات فردی در زمان فعالیت رسانه‌ها ظاهر شود اشخاص مربوطه ممکن است با انتقادات شدید رسانه‌ای مواجه شوند.

هنگامی که انتساب مسئولیت حقوقی مطرح می‌شود، قضاوت‌های پس از حادثه باید بر مبنای اطلاعات تمامی منابع باشد که به صورت منطقی در دسترس تصمیم گیرنده در زمان مربوطه بوده است.[۴۶] در مورد حمله‌ای که در آن از ابزارهای کنترل از راه دوراستفاده می‌شود، تصمیم کنترل کننده‌ی آن تجهیزات جهت انجام آن حمله در اثر آگاهی از اطلاعاتی است که در زمانی که آن تصمیم را مورد ملاحظه قرار می‌داد و اتخاذ می‌کرده است به وی ارائه شده است. مسئله حیاتی این است که آیا تصمیم کنترل کننده برای حمله در شرایطی که آن اطلاعات به وی ارائه شده منطقی بوده است. سؤالات مرتبط می‌تواند از این جمله باشد که آیا اقدامات احتیاطی عملی دیگری وجود داشت که انجام نگرفته باشد و اگر انجام شده باشد، وضعیت هدف به عنوان هدف نظامی را تأیید کرده است، آیا می‌توان انتظار داشت که حمله متناسب باشد و آیا این کار انجام شده بود تا صدمه و آسیب به غیرنظامیان را به حداقل برساند.[۴۷]

---

[۴۵] Liability

[۴۶] See statement (c) made by the UK on ratification of API on 28 January 1998

[۴۷] در اینخصوص به ملاحظاتی توجه کنید که در دستور العمل انگلستان قید شده است و عنوان می‌دارد سطحی که در آن مسئولیت حقوقی برای اتخاذ اقدامات احتیاطی در حمله قرار می‌گیرد در پروتکل اول مشخص نشده است، این امر که آیا یک فرد چنین مسئولیتی دارد یا خیر به این نکته مبتنی است که آیا وی اختیاری درمورد روش اجرای حمله داشته است؛ و این امر که مسئولیت احتمالاً میان طیفی شامل فرمانده ارشد و کارمندان برنامه ریزی تا سربازی که به ابتکار خود شروع به شلیک می‌کند گسترده خواهد بود؛ کسانی که دستورات مربوط به انجام حمله را

این نتیجه حاصل می‌شود که اگر تجهیزات مربوطه به درستی عمل می‌کردند،[۴۸] اپراتور آن تجهیزات مسئول اقدامات خود در رابطه با آن است. به هر جهت اگر داده‌های ارائه شده به کنترل‌گر در اثر نقصان سیستم معیوب شده باشند و اگر بتوان به درستی گفت که آن تقصیر منجر به تصمیمات متعدد جهت حمله شده است، آنگاه نقصان سیستم احتمالاً کنترل‌گر را از مسئولیت حمله تبرئه می‌کند.

هم چنین اگر طرف مقابل مخاصمه، خواه از طریق حیله‌ی نظامی، فریب، سپر انسانی داوطلبانه یا غیرداوطلبانه یا سایر موارد، مانعی مادی در برابر وظیفه کاربر تجهیزات ایجاد کند، این عامل نیز باید هنگام تعیین مسئولیت برای رخدادهای حادث شده مد نظر قرار گیرد. مقصر نشان دادن اپراتور برای خطاهایی که قابل انتساب به سیستم‌های حمایتی، اقدام دشمن یا سایر عوامل فراتر از کنترل است، منطقی به نظر نمی‌رسد. این که حمله خطا به درستی فراتر از کنترل کاربر بوده است، به حقایق موضوع بر می‌گردد و باید هنگامی که اطلاعات مربوطه در دسترس است ارزیابی شود. به نظر می‌رسد عواملی که باید هنگام تعیین مسئولیت بالقوه فرد کنترل کننده یک سامانه کنترل از راه دور مد نظر قرار گیرند اساساً مشابه مواردی هستند که به عنوان مثال در رابطه با خلبانی اعمال می‌شود که ماموریتی مشابه را انجام می‌دهد.

عدم انجام اقدامات احتیاطی در حمله جنایت جنگی به شمار نمی‌رود. جرائم جنگی مربوطه بر اساس اساسنامه رم به عنوان مثال شامل حمله مستقیم به غیرنظامیان،[۴۹] حمله مستقیم به اشیاء غیرنظامی[۵۰] و انجام حملات نامتناسب می‌شود.[۵۱] قصد که عنصری از این تخلفات است البته با عدم انجام اقدامات احتیاطی لازم برابر قلمداد نمی‌شود، گرچه به طور ویژه در شرایط واقعی این عدم انجام اقدام مذکور می‌تواند عنصری در یک حمله ارادی باشد. مسئولیت فرمانده نیز بر مبنایی مشابه با آن چه که در رابطه با عملیات‌های نظامی متعارف به‌کار می‌رود، به عنوان مثال بمباران از داخل هواپیمای دارای سرنشین، معین می‌شود. فرمانده نظامی بر اساس اساسنامه رم برای جرائم ارتکابی توسط نیروهای تحت کنترل و فرماندهی مؤثر او، در نتیجه قصور او در اعمال کنترل درست بر نیروهایش دارای مسئولیت مسئولیت کیفری است. این ماده مقرر می‌دارد فرمانده نظامی باید اطلاع داشته باشد

اجرا می‌کنند درصورتی که موضوع حمله به‌گونه‌ای باشد که تناسب حمله را نقض می‌کند، باید آن را تعلیق کرده یا لغو کنند. UK Joint Service Manual of the Law of Armed Conflict, UK Ministry of Defence, 2004, para. 5.32.9.

[۴۸] این یک مساله‌ی بسیار مهم است- نیروهای معارض ممکن است عامداً این تصور را مخدوش کنند، عملکرد برخی از حسگرهای اساسی را مختل سازند، یا نمونه‌هایی تقلبی یا دیگر حیله‌های نظامی را به‌کار بندند تا این تصویر مخدوش گردد.

[۴۹] Article 8(2)(b)(i) of the Rome Statute of the International Criminal Court, 1998 (hereinafter 'Rome Statute') provides for the crime of 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities'.

[۵۰] Article 8(2)(b)(ii) of the Rome Statute provides for the offence of 'intentionally directing attacks against civilian objects, that is, objects that are not military objectives'.

[۵۱] Article 8(2)(b)(iv) of the Rome Statute provides for the offence of 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or wide-spread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated'.

یا در شرایطی باشد که باید آگاهی داشته باشد که نیروها در حال ارتکاب چنین جرایمی هستند، یا قصد ارتکاب آن را دارند، و این که او در اتخاذ «تمام اقدامات لازم و منطقی در چارچوب صلاحیت خود برای سرکوب یا ممانعت از ارتکاب آن‌ها»[۵۲] کوتاهی کرده است. در حالی که قصور مذکور، تحت عنوان قصور در اتخاذ اقدامات احتیاطی کافی، در مقاله حاضر بررسی می‌شود، براساس اساسنامه رم جنایت جنگی تلقی نمی‌شوند، هر گونه بحث در این چارچوب نیز که فرمانده مسئول قصور است، احتمالاً بر اساس ملاک‌های مشابهی ارزیابی می‌شود. در نهایت مسئله این است که آیا فرمانده آگاهی داشته یا باید آگاهی می‌داشته که روش در حمله‌ی صورت گرفته مانع اتخاذ اقدامات احتیاطی لازم شده است. به نظر می‌رسد به احتمال زیاد فرماندهان از این مسئله آگاهی دارند.

مسئولیت برای حملات قانونی

در حالت کلی در حقوق برای اقدامات نیروهای مسلح یکی از طرفین یک مخاصمه مسلحانه بین المللی که به صورت قانونی منجر به مرگ، صدمه یا خسارت و یا تخریب طرف مقابل مخاصمه می‌شود هیچ مسئولیتی تبیین نشده است.[۵۳] چنین اقداماتی برای آن که قانونی تلقی شوند باید منطبق با حقوق مخاصمات مسلحانه باشند. بنابراین برای خساراتی که به صورت قانونی به اهداف نظامی وارد شده، برای مرگ یا صدمه‌ای که به صورت قانونی به اعضای نیروهای مسلح مقابل وارد شده، برای مرگ، آسیب یا صدمه به غیرنظامیان و اشیاء غیرنظامی که پیش بینی می‌شده است و نسبت به مزیت نظامی مستقیم و عینی فراتر نباشد، برای مرگ یا صدمه به غیرنظامیان یا آسیب به اشیاء غیرنظامی در اثر حملات اشتباه یا دارای خطا که به عنوان مثال در اثر نقصان تجهیزات نظامی رخ داده است، هیچ مسئولیتی وجود ندارد.

مسئولیت برای جبران خسارت که در ماده ۳ کنوانسیون چهارم لاهه ۱۹۰۷ پیش بینی شده است،[۵۴] در مقررات مشابه ماده ۹۱ پروتکل اول[۵۵] تکرار شده است. با اعمال ماده ۹۱ ممکن است به‌نظر برسد که به عنوان قصور در اتخاذ اقدامات احتیاطی ممکن نسبت به عملیات حمله از راه دور، اگر حمله منجر به مرگ یا آسیب افراطی

---

[۵۲] Article 87 of API, and Article 28 of the Rome Statute.

[۵۳] مجاز بودن اقدامات صورت گرفته مانع بروز مسئولیت دولتی می‌شود که آن اقدامات را انجام داده است. ماده ۳ کنوانسیون چهارم لاهه مقرر می‌دارد که نقضی صورت گرفته باشد. درخصوص مسئولیت رزمندگان ماده ۴۳(۲) پروتکل اول عنوان داشته است که اعضای نیروهای مسلح «رزمنده»، یعنی دارای حق مشارکت مستقیم در مخاصمه هستند.

[۵۴] ‘A belligerent party which violates the provisions of the said Regulations shall, if the case so demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces’.

[۵۵] این ماده از عباراتی مشابه به ماده ۳ کنوانسیون چهارم لاهه ۱۹۰۷ استفاده می‌کند، بجز این مساله که ماده ۹۱ به نقض هریک مقررا کنوانسیون ۱۹۴۹ یا پروتکل اشاره دارد، و بنابراین صراحتاً به نقض مقررات مربوط به هدف گیری در پروتکل اول اشاره می‌کند. پاراگراف ۳۶۴۶ از شرح پروتکل اول این نکته را مطرح می‌سازد که مفاد ماده ۳ متناظر است با اصول کلی حقوقی درخصوص مسئولیت دولت، دیدگاهی که توسط کمیسیون حقوق بین‌الملل در شرح مربوط به ماده ۷ پیش‌نویس مواد مسئولیت در سال ۲۰۰۱، مورد قرار گرفته است.

غیرنظامیان یا زیان افراطی به اهداف غیرنظامی نسبت به امتیاز نظامی پیش بینی شده شود، احتمالاً مسئولیتی حقوقی برای جبران خسارت از غیرنظامیان یا نهادهای غیرنظامی آسیب دیده وجود دارد، اگر اقتضای قضیه چنین باشد. شرح پروتکل اول عنوان می‌دارد که نقض ساده‌ی حقوق مخاصمات مسلحانه کافی نیست، و این‌که باید زیان یا آسیب وارد شده باشد و جبران خسارت تنها در صورتی متناسب است که اعاده وضعیت یا بازگرداندن وضعیت به حالت سابق ممکن نیست.[۵۶] این بدین معنا است که به منظور اثبات مسئولیت مدعیان باید ثابت کنند که اقدامات احتیاطی که از بعد حقوقی لازم است صورت نگرفته است،[۵۷] یعنی این که مدعیان متحمل زیانی شده‌اند که دریافت غرامت را توجیه می‌کند و زیان مذکور در نتیجه قصور در اتخاذ اقدامات احتیاطی رخ داده است و اقتضای قضیه پرداخت غرامت است.

اگر آسیب به غیرنظامیان و/یا خسارت به اشیاء غیرنظامی در نتیجه نقص فنی تجهیزات رخ داده باشد، نقص نرم‌افزاری، عیب ساختاری یا ارائه نادرست داده‌ها طی اجرای مأموریت احتمالاً مشکلاتی پیچیده را بر سر راه هر گونه تلاش برای انتساب مسئولیت فردی به‌وجود می‌آورد. پرسنل نظامی که سهل انگارانه اقدام می‌کنند موضوع قوانین نظامی خود خواهند بود، در حالی که اقدام ممکن علیه غیرنظامیان سهل انگار به قرارداد استخدام آن‌ها بستگی دارد. در هر صورت اگر خطای رخ داده به گونه‌ای است که حادثه را نمی‌توان به درستی یک نقض نامید، حقوق مخاصمات مسلحانه پرداخت غرامت را الزامی نمی‌داند.[۵۸] به ویژه، به نظر می‌رسد توصیف ساخت سهل انگارانه‌ی سلاح به عنوان نقض به طوری که مبنای ادعای احتمالی دریافت غرامت را بر اساس ماده ۹۱ تشکیل دهد، مشکل است.[۵۹] این که در یک قضیه خاص ادعایی بر اساس حقوق مسئولیت تولید مطرح شود به مفاد قانون خاص دولت مربوطه و به توانایی مدعیان بستگی دارد که بتوانند دعوی را تحت صلاحیت دادگاه‌های قانون مدنی آن کشور مطرح کنند. چنین مسائلی خارج از حیطه بحث حاضر است.

---

[۵۶] برای مطالعه‌ی مباحث مفصل‌تر درخصوص ترتیبات معاصر ر.ک. API Commentary, paras 3652–3659

[۵۷] برای نمونه به تصمیم کمیسیون دعاوی اریتره-اتیوپی (Eritrea-Ethiopia Claims Commission) توجه کنید که تا حدودی بر برداشت‌های معارض مبتنی است و این نتیجه گیری را تقویت می‌کند که تمام اقدامات احتیاطی توسط اریتره در اجرای حمله‌ی هوایی بر مکله در ۵ جون ۱۹۹۸ انجام نشده است و آن را برای خسارات و جراحات وارده بر غیرنظامیان و اشیاء غیرنظامی مسئول می‌داند. Eritrea-Ethiopia Claims Commission, Partial Award Decision, Central Front, Ethiopia's Claim 2, 28 April 2004, para. 112, available at: http://www.pca-cpa.org/showpage.asp?pag_id=1151.

[۵۸] با این حال پرداخت غرامت می‌تواند از سر لطف (*ex gratia*) باشد، همچون مواردی که طبق گزارشات پس از حمله به سفارت چین در بلگراد توسط هواپیمای ایالات متحده که در ۷ می ۱۹۹۹ با ناتو همکاری می‌کرد، رخ داد. Dumbaugh, 'Chinese Embassy bombing in Belgrade: compensation issues', in CRS Report for Congress, available at: http://congressionalresearch.com/RS20547/document.php.

[۵۹] See T. Gillespie and R. West, above note 37, citing A. Myers, 'The legal and moral challenges facing the 21st century Air Commander', in Royal Air Force Air Power Review, Vol. 10, No. 1, Spring 2007, pp. 76–96, for the view that the responsibility of designers is discharged 'once the UAS [unmanned aerial system] has been certified by the relevant national air authority'; T. Gillespie and R. West, ibid., p. 7.

آیا حمله از راه دور منجر به تغییر حقوقی چشمگیر در عملیات جنگی می‌شود؟

دور بودن حمله درصورتی که قواعد هدف قرار دادن را غیرقابل اجرا کند یا انتساب مسئولیت کیفری برای تخلفات را ناممکن سازد یا حکمی صادر کند مبنی بر این که غرامت برای حملاتی که عواقبی غیررضایت بخش دارند قابل پرداخت است یا خیر، از نظر حقوقی حائز اهمیت خواهد بود.

همانطور که مشاهده شد برخی انواع حملات از راه دور چنین چالش‌هایی را موجب نمی‌شوند. از این رو زمانی که یک وسیله هوایی کنترل از راه دور برای حمله به یک هدف استفاده می‌شود، نقش خلبان از راه دور که معمولاً به آن کاربر گفته می‌شود، هم چون نقش خلبان یک هواپیمای دارای سرنشین است به گونه‌ای که قواعد حقوقی هدف قرار دادن بر آن‌ها به همان نحو یا به صورتی مشابه قابل اعمال است، و به طوری که مسئولیت کیفری علیه کاربر قابل طرح است یعنی، درخصوص حمله‌ی عمدی علیه غیرنظامیان و مسئولیت پرداخت غرامت قابل ارزیابی و تصمیم گیری است، هم چون مورد حمله‌ای که در آن از تجهیزات دارای سرنشین استفاده می‌شود.

به علاوه از یک جهت انسان از اعصار نخستین کوشیده است از راه دور مبارزه کند. نگرانی در مورد اخلاقی بودن چنین پیشرفت‌هایی نیز به دوران باستان باز می‌گردد.[۶۰] منجنیق، توپ، کمان تفنگی و کمان بزرگ، توپخانه، بمباران هوایی و ادوات هوایی بدون سرنشین کنترل از راه دور را می‌توان روش‌هایی بهبود یافته برای اعمال نیروی تهاجمی علیه دشمن قلمداد کرد که در عین حال برای نیروهای خودی خطری کمتر به همراه دارند. مفهوم تلاش برای حمایت از خود و درعین حال به خطر انداختن دشمن البته مبنای بسیاری از روش‌های جنگی است که نشان می‌دهد دور بودن کاربر به خودی خود تغییری کیفی و در نتیجه از نظر حقوقی چشمگیر، نسبت به گذشته محسوب نمی‌شود.[۶۱] شاید ایده‌ی کنونی این است که مسئولیت تصمیم به حمله می‌تواند همیشه به سطوح شخصی، فرماندهی و ملی منتسب شود. گاه پیچیدگی‌هایی بروز می‌کند، به عنوان مثال زمانی که پرسنل یک دولت در وظیفه‌ای مجزا حملاتی را با استفاده از تجهیزاتی که به دولتی دیگر تعلق دارند، خواه در قالب ائتلاف یا خارج آن، صورت می‌دهند؛[۶۲] اما این پیچیدگی‌ها این حقیقت را تغییر نمی‌دهد که شخصی که فرمان حمله را صادر کرده است و اشخاصی که آن را به اجرا درآورده‌اند قابل شناسایی هستند و در نتیجه مسئولیتی که از این حیث در اینجا بررسی شد قابل انتساب است. افزایش فاصله میان شخص مهاجم و صحنه وقوع تخریب به خودی

---

[۶۰] اعتراض ایدومنئوس (Idomeneus) در برابر استفاده از کمان: «سلوک من آن نیست که دور از دشمن خود در جنگ حاضر شوم.» Homer, Illiad, 13.262–3.؛ او. کانل معتقد است استفاده از کمان با تصویر منازعات که جوهره‌ی جنگ قهرمانانه بود همخوانی نداشت. Robert L. O'Connell, Of Arms and Men: A History of War, Weapons and Aggression, Oxford University Press, Oxford, 1989, p. 48؛ شاید برخی از انتقادات ما درخصوص جنگ از راه دور ریشه در اصطلاح **هومری** از جنگ قهرمانانه دارد.

[۶۱] B. J. Strawser, above note 37, p. 343.

[۶۲] See Article 6 of the ILC Draft Articles on State Responsibility, 2001, available at: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf, and note para. 3 of the associated commentary.

خود ظاهراً آن را تغییر نمی‌دهد. بلکه، به نظر می‌رسد مسئله بیشتر از آن که بحث فاصله باشد، بحث عدم وجود انسان به طور کلی باشد.

شناختگی یا ناشناختگی احتمالی یک مهاجم سایبری، عدم امکان تشخیص این موضوع برای طرف متضرر که اقدام تخلف آمیز چه کسی موجب حمله به غیرنظامیان به جای هدفی نظامی شده است، نمونه‌هایی از شرایطی هستند که در مورد آن‌ها معتقدیم این گونه از حملات از راه دور چالش‌هایی برای حقوق هدف گیری ایجاد می‌کنند.

از این رو فناوری حمله مستقل را بیشتر مورد بررسی قرار می‌دهیم. اگر تجهیزات متعلق به نیروی مسلح یک دولت باشد و پرسنل همان کشور اقدام به استفاده از آن کرده باشند، عنوان شده است که آن کشور مسئولیتی مشابه مسئولیت ناشی از فعالیت آن تجهیزات در میدان نبرد برای مرگ، صدمه یا خسارت وارده برای مثال در اثر یک موشک یا بمب، دارد که با استفاده از فناوری متداول‌تر و دارای سرنشین شلیک شده است. به عبارت دیگر ماده ۹۱ کنوانسیون مشخص می‌کند که آیا تعهدی حقوقی برای پرداخت غرامت وجود دارد و کشور مذکور مرجع تشخیص این است که آیا در شرایطی که مسئولیت حقوقی قابل تثبیت نیست یا ثابت نشده است پرداخت از سر لطف را انجام دهد.

برخی تلاش می‌کنند این موضوع به این نتیجه برسند که اگر به هر دلیلی تجهیزاتی به صورت خودکار تصمیم بگیرد غیرنظامیان یا اهداف غیرنظامی را هدف حمله قرار دهد، این عمل در نگاه نخست نقص مواد ۵۱(۲) یا ۵۲(۱) پروتکل اول است و از این رو نقض اهداف ماده ۹۱ به شمار می‌رود. دیدگاه دیگر که مؤلف آن را ترجیح می‌دهد، به طراحی نرم افزار کنترل، داده‌های تغذیه شده به تجهیزات کنترل مأموریت، تنظیمات اعمال شده بر فناوری الگوریتم محور و هر اطلاعات دیگری توجه می‌کند که نشان می‌دهد اشخاص طراح و فرمانده عملیات مذکور درنظر داشتند که این ماشین به چه چیزی حمله کند. بر طبق این دیدگاه، «هدف» یک حمله خودکار شامل هدف/اهدافی یا شخص/اشخاصی می‌شود که طراحی یا هدف تجهیزات تشخیص هدف برای درگیری با آن‌هاست. بر اساس دیدگاه دوم، ماشین از قابلیت مستقل خود برای تحصیل هدف یا مقصودی استفاده می‌کند که توسط اشخاص مسئول در مأموریت برای آن‌ها تنظیم شده است، با این پیامد که مسئولیت پرداخت غرامت تنها بر اساس ماده ۹۱ مقرر می‌شود تنها اگر ثابت شود که طراحان و فرماندهان اشخاص یا اشیاء مورد حمایت را به عنوان هدف حمله خود تعیین کرده بودند.

اگر مسئولیت شخصی برای حملات مستقل خطا مطرح باشد، به نظر می سد این نتیجه گیری منطقی است که بگوییم اشخاص عموماً برای اقدامات خود در رابطه با تجهیزات مستقل، هدایت آن و عملیات تهاجمی آن مسئول شناخته شوند.[۶۳] اگر فردی به عمد نرم‌افزار تعیین هدف به صورت مستقل را با این قصد پیکربندی کند که غیرنظامیان و/یا اهداف غیرنظامی را مورد هدف قرار دهد، این نتیجه حاصل می‌شود که این عمل درست مانند

[۶۳] Consider, however, paragraph 5.32.9 of the UK Manual summarized above at note 42.

استفاده از قابلیت‌های متداول با هدفی مشابه است، که جنایت جنگی شمرده می‌شود.[۶۴] با این حال، اگر عدم اتخاذ اقدامات احتیاطی لازم منجر به یک حمله مستقل خطا شود، احتمالاً جنایت جنگی تلقی نمی‌شود؛ غرامت قابل پرداخت است اگر الزامات تعیین مسئولیت بر اساس ماده ۹۱ قابل اثبات باشد؛ و اشخاص مسئول به دلیل قصور در اتخاذ اقدامات احتیاطی ممکن است به عنوان مثال بر اساس اجرای سهل انگارانه وظایف خود، تا حدی تنبیه شوند که در مقررات قابل اعمال نیروهای مسلح یا در قرارداد استخدام غیرنظامیان مقرر شده است.

نتیجه

نتیجه‌ای محتاطانه که از این بحث حاصل می‌شود این است که چارچوب تثبیت شده خواه در رابطه با جنایات جنگی، مسئولیت پرداخت غرامت یا اصول استخدام نیروهای مسلح یا غیرنظامیان باید قابلیت اعمال داشته باشد و از این رو در حقیقت در صورت بروز حملات مستقل خطا باید اعمال شود. اشخاصی که در مخاصمات مسلحانه بین المللی از فناوری مستقل به عمد برای حملات غیرقانونی استفاده می‌کنند مرتکب نقض حقوق مخاصمات مسلحانه می‌شوند هم چون کسانی که از سلاح‌های متعارف برای هدفی مشابه استفاده می‌کنند. این حقیقت که یک ماشین برای فعالیت مستقل طراحی شده است کسانی را که فرمان مأموریت را صادر می‌کنند، کسانی که مأموریت را برنامه ریزی می‌کنند و کسانی که اقدامات لازم را برای عملی شدن مأموریت انجام می‌دهند از مسئولیت اقدامات خود تبرئه نمی‌کند و احتمالاً در چارچوب اقدامات این افراد است که مبنای هر گونه عمل مجرمانه و مسئولیت پرداخت غرامت را می‌توان یافت.

پیشنهادات مربوط به پیگیری‌های قضایی علیه ماشین در حال حاضر ریشه در افسانه‌ها دارد. به هر صورت همان طور که مفاهیم هوش مصنوعی[۶۵] بالغ‌تر می‌شود، قابل درک است که نقطه‌ای پدیدار می‌شود که در آن نقطه مشارکت انسان در مفهوم رابطه‌ی علت و معلول از تصمیم به حمله به قدری دور است که فرماندهان و طراحان دیگر از لحاظ منطقی مسئول قلمداد نمی‌شوند. از دید مؤلف، ما هنوز به آن نقطه نرسیده‌ایم اما با پیچیده‌تر شدن فناوری و با تکیه بیش از پیش تصمیم گیری بر هوش مصنوعی و کمتر از سابق بر برداشت و قضاوت انسانی، پیش بینی می‌شود تمرکز مسئولیت از برنامه ریزان و فرماندهان برداشته و متوجه مهندسان نرم افزار و روبات‌هایی شود آن‌ها که خلق می‌کنند.

---

[۶۴] این مساله که آیا رسیدگی با تکیه بر چنین مبنایی قابل اجرا خواهد بود همچون همیشه به در دسترس بودن ادله بستگی دارد.

[۶۵] Artificial Intelligence (AI)