Culminatin of Law Quarterly

15th Year, No. 4, Winter 2024

http://dx.doi.org/10.22034/thdad.2024.2009825.2541

From The Hague to Tallinn Assessing the Standards Governing Cyber Operations in the Course of Military Occupation under Tallinn Manual 2.0

Shahram Zarneshan[1], Mousa Karami[2*], Reyhaneh Zandi[2]

1. Associate Professor, Department of Public and International Law, Faculty of Law and Political Science, Allameh Tabatabaei University, Tehran, Iran.

2. Ph. D. Candidate in Public International Law, Faculty of Law, University of Qom, Qom, Iran.

Article Type:

Original Research

Pages: 3-39

Received: 2023 August 22

Revised: 2023 October 28

Accepted: 2024 January 10

Abstract

Tallinn Manual 2.0 on *International Law Applicable on Cyber Operations* (hereinafter, Tallinn Manual 2.0 or Manual), which is prepared in 2017, has addressed cyber operations in occupation situation in its Chapter 19. Employing a descriptive-analytical method, the present article tries to assess the standards governing cyber operations in the course of military occupation from the perspective of the aforementioned Manual. According to Tallinn Manual 2.0, cyber operations cannot alone suffice to establish or maintain the degree of authority over territory necessary to constitute an occupation. However, these operations can be employed to help establish or maintain the requisite authority to constitute occupation. Additionally, they may be employed to disrupt or degrade computer systems used by and Occupying Power to maintain authority over the occupied territory. Pursuant to the Manual, protected persons in occupied territory must be respected and protected from the harmful effects of cyber operations. Furthermore, the Occupying Power shall take all the measures in its power to restore and ensure public order and safety, while respecting the laws in force in the country, including the laws applicable to cyber activities. In addition, the Occupying Power may take measures necessary to ensure its general security, including the integrity and reliability of its own cyber systems. And finally, to the extent the law of occupation permits the confiscation or requisition of property, taking control of cyber infrastructure or systems is likewise permitted. It appears that the traditional rules governing law of military occupation stipulated in 1907 Hague Regulations as well as the Fourth Geneva Convention are applied during the conduct of cyber operations and on cyber activities and properties. In spite of its undeniable role in the effort to clarify international law on cyber operations, the Manual is faced with challenges and gaps such as non-binding nature, non-incorporation of all rules of military occupation and non-sufficient attention to requirements of cyberspace. It is expected that at least some of them would be taken into consideration in Tallinn Manual 3.0 which is managed to be published in 2026.

Keywords: International Law, Military Occupation, Cyberspace, Cyber Operation, Tallinn Manual 2.0

* Corresponding Author: mosakarami136767@gmail.com

فصلنامه تعالی حقوق

سال پانزدهم، شماره ۴، زمستان ۱۴۰۳

http://dx.doi.org/10.22034/thdad.2024.2009825.2541

از لاهه تا تالین
ارزیابیِ موازین حاکم بر عملیات‌های سایبری در جریان اشغال نظامی به‌موجب دستورالعمل تالین ۲

شهرام زرنشان[۱]، موسی کرمی[۲*]، ریحانه زندی[۲]

۱. دانشیارگروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران.

۲. دانشجوی دکتری حقوق بین‌الملل عمومی، دانشکده حقوق، دانشگاه قم، قم، ایران.

نوع مقاله: علمی پژوهشی

صفحات: ۳۹-۳

تاریخ دریافت: ۱۴۰۲/۰۵/۳۱

تاریخ بازنگری: ۱۴۰۲/۰۸/۰۶

تاریخ پذیرش: ۱۴۰۲/۱۰/۲۰

چکیده

دستورالعمل تالین ۲ راجع به حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری (دستورالعمل تالین ۲ یا دستورالعمل)، که در سال ۲۰۱۷ آماده گردیده است، در فصل نوزدهم خود به بحث عملیات‌های سایبری در وضعیت اشغال می‌پردازد. در این مقاله، کوشش می‌شود تا از رهگذر شیوه توصیفی-تحلیلی، موازین حاکم بر عملیات‌های سایبری در جریان اشغال نظامی از نظرگاه دستورالعمل یادشده ارزیابی گردد. بر پایه دستورالعمل تالین ۲، عملیات‌های سایبری به‌تنهایی نمی‌توانند برای سلطه بر سرزمین که جهت شکل‌گیری وضعیت اشغال ضروری است، کفایت کنند. با وجود این، می‌توان آن‌ها را برای کمک به سلطه لازم جهت ایجاد وضعیت اشغال به‌کارگرفت. به علاوه، می‌توان آن‌ها را برای ایجاد اختلال یا ازکارانداختن سامانه‌های رایانه‌ای به‌کاررفته به‌دست قدرت اشغالگر به‌منظور حفظ سلطه بر سرزمین اشغال استفاده کرد. پیرو دستورالعمل، اشخاص تحت حمایت در سرزمین اشغالی باید مورد احترام قرارگیرند و در برابر آثار زیان‌بار عملیات‌های سایبری تحت حمایت واقع شوند. افزون بر این، قدرت اشغالگر باید، ضمن رعایت قوانینِ جاری در کشور و از جمله قوانین قابل اِعمال بر فعالیت‌های سایبری، کلیه اقداماتی که در توان دارد را برای اعاده یا تضمینِ نظم و امنیت عمومی اتخاذ نماید. علاوه بر این، قدرت اشغالگر می‌تواند اقدامات ضروری را برای تضمین امنیت عمومی خود و از جمله یکپارچگی و پایایی سامانه‌های سایبری خویش، اتخاذ کند. و در نهایت، به میزانی که حقوق اشغال اجازه ضبط یا مصادره اموال را بدهد، تحت کنترل درآوردن زیرساخت‌ها یا سامانه‌های سایبری به‌نحوی مشابه مجاز است. به نظر می‌رسد همان قواعدِ سنتیِ حاکم بر حقوق اشغال نظامی مندرج در مقررات لاهه ۱۹۰۷ و نیز کنوانسیون چهارم ژنو، در زمان انجام عملیات‌های سایبری و بر فعالیت‌ها و اموال سایبری مُجری است. دستورالعمل، به‌رغم نقش انکارناپذیری که در تلاش برای روشن‌سازیِ حقوق بین‌الملل حاکم بر عملیات‌های سایبری دارد، با چالش‌ها و کاستی‌هایی مانند سرشت غیرالزام‌آور، عدم گنجاندنِ همه قواعد اشغال نظامی و عدم توجه کافی به بایسته‌های فضای سایبر روبه‌روست. انتظار می‌رود در دستورالعمل تالین ۳ که قرار است در سال ۲۰۲۶ منتشر گردد، دست‌کم بعضی از این موارد مطمح‌نظر قرارگیرد.

واژگان کلیدی: حقوق بین‌الملل، اشغال نظامی، فضای سایبر، عملیات سایبری، دستورالعمل تالین ۲

* نویسنده مسئول: mosakarami136767@gmail.com

درآمد

گویی بی مطالعه تاریخ جنگ‌ها، نمی‌توان به کُنه اقلیم وجود آدمی پی برد. به‌خاطر نقش جنگ و درگیری مسلحانه در اقلیم انسانی، حقوق بین‌الملل وجود آن را به‌سانِ یک واقعیت می‌پذیرد و راه تنظیم آن را پیش می‌گیرد. یکی از پیامدهای درگیری‌های مسلحانه بین‌المللی، اشغال نظامی سرزمین دشمن است. اشغال نظامی زمانی آغاز می‌شود که ارتش دشمن به داخل سرزمینی که تحت حاکمیت دولت دیگر است و یا دست‌کم تحت حاکمیت قدرت حمله‌کننده نیست نفوذ کند و اقدام به کنترل مؤثر و انحصاری بر آن نماید. این وضعیت زمانی پایان می‌پذیرد که نیروهای نظامی دشمن به اِعمال کنترل بر سرزمین اشغال‌شده پایان دهند (کولب و هاید، ۱۳۹۴، ص. ۳۶۳-۳۶۱). حقوق اشغال نظامی،[1] شاخه‌ای از حقوق بین‌الملل بشردوستانه است که به‌ویژه پس از اشغال عراق در سال ۲۰۰۳ اهمیت و جان تازه‌ای یافت (Gross, ۲۰۱۷, p. ۱). این نظام حقوقی، به منزله متولیِ تنظیم و تدوینِ تعهدات و حقوق یک طرفِ درگیریِ مسلحانه‌ای که سرزمین طرف دیگرِ درگیری را اشغال کرده است (Dörmann and Gasser, ۲۰۱۳, p. ۲۶۴)، تنها در درگیری‌های مسلحانه بین‌المللی اعمال می‌شود و در درگیری‌های مسلحانه غیربین‌المللی موضوعیت ندارد. حقوق اشغال نظامی، برای نخستین بار در جریان کنفرانس‌های صلح لاهه و به‌طور خاص در مقررات لاهه در خصوص جنگ‌های زمینی (۱۹۰۷) تدوین گردید و در کنار آن، کنوانسیون چهارم ژنو راجع به حمایت از افراد غیرنظامی در زمان جنگ[2] مورخ ۱۲ اوت ۱۹۴۹، دیگر منبع اصلی این شاخه از حقوق بشردوستانه محسوب می‌شود.

سده بیست‌ویکم را عصر حاکمیت اینترنت بر تمام عرصه‌های زندگی بشر

---

1 Law of military occupation

2 Geneva Convention Relative to the Protection of Civilian Persons in Time of War (12 August 1949)

دانسته‌اند (فرشاسعید و جلالی، پاییزو زمستان ۱۴۰۱، ص. ۱۷۵)که درآن، فضای سایبر[1] به بستری جدید برای مناسبات بین‌المللی کشورهای جهان مبدل شده است (Polański, June ۲۰۱۷, p. ۳۷۱). در این میان، رژیم حقوقی اشغال و اعمال این نظام در عرصه ناپیدای سایبر، از موضوعات مهمِ کنونی شمرده می‌شود. در سال ۲۰۱۷ میلادی یک گروه کارشناسان بین‌المللی با مدیریت عالیه پروفسور مایکل اشمیت، و به سفارش و دعوت مرکز عالی پدافند مشترک سایبری ناتو،[2] در شهر تالین[3] کشور استونی گرد هم آمدند و با تکمیل دستوالعمل تالین راجع به حقوق بین‌الملل قابل اعمال بر نبردهای سایبری سال ۲۰۱۳ که در پی حملات سایبری به استونی در سال ۲۰۰۷ (خلیل‌زاده، ۱۳۹۳، ص ۳۹) در دستور کار مرکز یادشده در ناتو قرارگرفته بود، به تهیه و تدوین دستورالعملی دست زدند که نام کامل آن دستورالعمل تالین ۲ راجع به حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری[4] (زین پس، دستورالعمل تالین ۲ یا دستورالعمل) است. این دستورالعمل، که از ۲۰ فصل و ۱۵۴ قاعده تشکیل شده است، در فصل ۱۹ خود، به بحث عملیات‌های سایبری در وضعیت اشغال نظامی می‌پردازد. در خصوص جایگاه حقوقی این سند، به‌کوتاهی می‌توان گفت اگرچه این دستورالعمل سندی الزام‌آور نیست، ولی کارشناسان تدوین‌کننده آن قواعد مندرج در دستورالعمل را بازتاب حقوق بین‌الملل عرفی می‌دانند (Manual Tallinn ۲,۰, ۲۰۱۷, pp. ۲-۳) افزون بر این، با توجه به اهمیت و چالش‌های فراروی قاعده‌گذاری در فضای سایبر (شکیب‌نژاد، ۱۳۹۶، ص ۱۹)، حتی سخن از نقش آن در قاعده‌گذاری بین‌المللی در عرصه حقوق بین‌الملل سایبری در میان است (Tanodomdej, ۲۰۱۹, pp. ۶۷-۸۵).

1 Cyber space

2 NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

3 Tallinn

4 Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (Tallinn Manual 2.0)

در این مقاله می‌کوشیم تا با به‌کارگیری نوشته‌های مرتبط با حقوق اشغال نظامی و حقوق قابل اِعمال بر فضای سایبر از یک‌سو و تکیه بر دستورالعمل تالین ۲ از سوی دیگر، به این پرسش پاسخ دهیم که موازین ناظر بر عملیات‌های سایبری در جریان اشغال نظامی از نظرگاه تدوین‌کنندگان دستورالعمل یادشده کدامند و دستورالعمل یادشده در این زمینه چه کاستی‌هایی دارد؟ به یک بیان، ما سفری خواهیم داشت از لاهه به‌عنوان جایی که نخستین بار قواعد حقوق اشغال نظامی تدوین شد تا تالین که قواعد دستورالعمل تالین راجع به اشغال نظامی مدون گردید. بر پایه جست‌جوی نویسندگان، تا زمان نگارش این نوشتار (آبان ۱۴۰۲ خورشیدی)، هیچ نوشته‌ای چه در قالب کتاب و چه به شکل مقاله، به تشریح رویکرد دستورالعمل تالین ۲ در قبال اشغال نظامی نپرداخته است و تنها مقالاتی یافت می‌شوند که به بررسی موضع این دستورالعمل درباره مواردی مانند قابلیت اعمال حقوق بشردوستانه بر عملیات‌های سایبری (گیوکی و دیگران، بهار ۱۳۹۷)، مداخله در امور داخلی دولت‌ها از رهگذر عملیات‌های سایبری (گیوکی و حکاک‌زاده، بهار ۱۴۰۱)، اعمال حقوق بی‌طرفی بر عملیات سایبری، زرنشان و دیگران، تابستان ۱۴۰۲)، عملیات سایبری در مناطق دریایی (زرنشان و دیگران، پاییز و زمستان ۱۴۰۲) و مسائلی مانند اثربخشی این دستورالعمل بر صلاحیت دیوان کیفری بین‌المللی در ایجاد و صلح و امنیت سایبری بین‌المللی (محقق هرچقان و دیگران، بهار-تابستان ۱۴۰۱) و توسعه صلاحیت دیوان بین‌المللی کیفری در بستر حقوق بین‌الملل سایبری (محقق هرچقان و دیگران، پاییز ۱۴۰۲) پرداخته‌اند.

واقع، نوآوری و وجه ممیزه این اثر نسبت به این مقالات، نخست پرداختن به موازین حاکم بر عملیات‌های سایبری در جریان اشغال نظامی در دستورالعمل و سپس ارزیابیِ ولوکوتاه دستورالعمل تالین ۲ در این زمینه است. به این منظور، از آنجایی که دستورالعمل تالین ۲ محورِ این مطالعه است، به تبعیت از این سند و قواعد ذی‌ربط آن، مطالب خود را در چهار پی گیریم. به این ترتیب که نخست به تبیین حمایت از اشخاصِ

تحت حمایت در سرزمین اشغالی در برابر عملیات‌های سایبری در چارچوب دستورالعمل دست می‌زنیم (۱). در ادامه، رویکرد دستورالعمل در قبال فعالیت‌ها و سامانه‌های سایبری نظم و امنیت عمومی سرزمین اشغالی را برمی‌رسیم (۲). سپس، این کار را در خصوص ضبط و مصادره اموال و تحت کنترل در آوردن زیرساخت‌ها یا سامانه‌های سایبری پی می‌گیریم (۳) . افزون بر این، با اتخاذ رویکردی انتقادی، کاستی‌ها و ناراستی‌های دستورالعمل در زمینه حقوق اشغال نظامی را نیز تشریح می‌کنیم (۴). قواعد مربوط به اشغال نظامی در حقوق بشردوستانه بسیار مفصل هستند و ما در این مقاله، تنها به آن دسته از قواعدی می‌پردازیم که در دستورالعمل به آن‌ها ورود شده است. گفتنی است روش ما در تبیین مباحث، بیان کلیاتی بسیار کوتاه از حقوق اشغال نظامی و سپس ورود به قواعد دستوالعمل تالین ۲ و شرح آن‌ها ذیل هرگفتار است.

۱- حمایت از اشخاص تحت حمایت در سرزمین اشغالی در برابر عملیات‌های سایبری

به باور ما، همه اصول و سازِکارهای حقوق بین‌الملل بشردوستانه سرانجام برای پاسداری از نوع بشر و حمایت از افراد درگیر در مخاصمات تدبیر و تعبیه شده‌اند. جلوه بارز این مدعا، اصل تفکیک میان رزمندگان و غیررزمندگان به‌عنوان یکی از اصول کلیدی و محوری این نظامِ حمایتی است. در این عرصه، «غیرنظامیان همیشه مستحق احترام به شخصیت، ناموس، حقوق خانوادگی، اعتقادات مذهبی و آداب و رسوم خود هستند و دارایی خصوصی آن‌ها محافظت می‌شود» (ICRC, ۲۰۰۲, p. ۲). بایستگی حمایت از غیرنظامیان در زمان اشغال سرزمین به‌دست نیروهای مسلح دشمن در این نکته نهفته است که دولت آن سرزمین به‌خاطر از دست دادن کنترل، توانایی حفاظت از شهروندان خود را دارا نیست (Cohen, ۲۰۰۶, p. ۵۰۲). اینجاست که حقوق به‌مثابه عاملی برای پیشگیری و پایان‌بخشی به خودسری، وارد کارزار می‌شود و حمایت از غیرنظامیان را

بر دوش قدرت اشغالگر می‌گذارد. این مقوله بسیار مهم، در دستورالعمل مورد مطالعه ما، مدنظر قرارگرفته است. در این زمینه، طبق قاعده ۱۴۶ دستورالعمل که بر ماده ۲۷ کنوانسیون چهارم ژنو استوار و بازتاب حقوق بین‌الملل عرفی است، «اشخاص تحت حمایت در سرزمین اشغالی باید مورد احترام قرارگیرند و از آن‌ها در برابر آثار زیان‌بار عملیات‌های سایبری حمایت به عمل آید». بر اساس دستورالعمل، اصطلاح «اشخاص تحت حمایت»[1] به غیرنظامیانی اشاره دارد که «خود را در.... دستان» قدرت اشغالگری می‌بینند که تبعه آن نیستند. این اصطلاح، غیرنظامیان سرزمین اشغالی را در بر می‌گیرد. شایسته یادکرد است که وفق ماده ۴ کنوانسیون ژنو، در صورتی که غیرنظامیان تبعه یک دولت بی‌طرف یا شریک مخاصمه باشند که در آن دولت نمایندگی دیپلماتیک عادی دارد، حمایت ذیربط به ایشان اِعطا نمی‌شود. طبق دستورالعمل، مبتنی بر ماده ۸ کنوانسیون چهارم ژنو، هیچ‌یک از حقوق اشخاص مورد حمایت تحت هیچ شرایطی به‌موجب حقوق اشغال سلب نمی‌شود (Manual Tallinn ۲,۰, p. ۵۴۴). باید به یاد داشت این تنها قواعد حقوق بشردوستانه نیستند که در چارچوب درگیری‌های مسلحانه و ازجمله حقوق اشغال از غیرنظامیان حمایت به‌عمل می‌آوردند، بلکه نظام بین‌المللی حقوق بشر نیز در این زمینه به یاری ایشان می‌شتابد.

پژوهشگران از سرشتِ حقوق بشریِ حقوق اشغال نظامی سخن به میان آورده‌اند که منطقاً حمایت از غیرنظامیان را باید مهم‌ترین جلوه‌گاه و مؤیدِ این مدعا دانست. به باور ایشان، اگرچه متونِ اصلیِ حقوق بشری به‌ندرت حاوی اصولِ راهنمایی در خصوص قابلیت اعمال این حق‌ها در درگیری‌های مسلحانه‌اند و نیز نه حقوق لاهه و نه حقوق ژنو صراحتاً از منظری حقوق بشری نگارش نیافته‌اند، تلاش این دو نظام برای تضمینِ حمایتی حداقلی از افراد در برابر فعالیت دولت‌ها انکارناپذیر است (Campanelli, ۲۰۰۸, p. ۶۶۵). این ماهیتِ حقوق بشری، در دستورالعمل موضوع مطالعه ما نیز بازتاب یافته

1 Protected persons

است. از نظر کارشناسان دستورالعمل، مطابق مواد ۱۳ و ۲۷ کنوانسیون چهارم ژنو، با لحاظ مقررات ویژه در رابطه با سلامتی، سن و جنسیت و بدون هرگونه تمایز زیان‌بار به‌ویژه بر مبنای نژاد، مذهب یا عقیده سیاسی، قدرت اشغالگر باید با کلیه اشخاص تحت حمایت رفتار یکسانی داشته باشد. بر این اساس، مسدودسازی دسترسی اینترنتی به یکی از مؤلفه‌های جمعیت غیرنظامی که با نژاد، مذهب یا وابستگی سیاسی تعریف می‌شود، به موجب این قاعده ممنوع خواهد بود (Manual Tallinn ۲,۰ ,p. ۵۴۵). البته باید توجه داشت که حقوق اشغال نظامی تنها مصالح جمعیت غیرنظامی در سرزمین اشغالی را در نظر نمی‌گیرد، بلکه منافع دولت اشغالگر را نیز مطمح نظر قرار می‌دهد (Cam-panelli ,۲۰۰۸ ,p. ۶۶۶). به همین سبب است که قدرت اشغالگر می‌تواند اقدامات کنترلی و امنیتی که مخاصمه آن‌ها را ضروری می‌سازد در رابطه با اشخاص تحت حمایت اتخاذ کند (Manual Tallinn ۲,۰ ,p. ۵۴۵).

پرسشی که در اینجا مطرح می‌شود و در دستورالعمل مورد توجه قرار نگرفته این است که چگونه می‌توان تعهد اشغالگر به اعمال حقوق بشر و حقوق بشردوستانه را- که ممکن است گاهی مستلزم اصلاحات قانونی باشد - با اصل تداوم نظام حقوقی داخلی که در قلب نظام حقوقی حاکم بر وضعیت اشغال قرار دارد، تطبیق داد. اصلاحات انجام‌شده تا چه اندازه با قاعده مندرج در ماده ۴۳ مقررات لاهه و ماده ۶۴ کنوانسیون چهارم ژنو سازگار است؟ در پاسخ به این پرسش، باید احتیاط پیشه ساخت. اشغالگر می‌تواند تحت پوشش اجرای تعهدات بین‌المللی خود، بدون انجام مشورت دموکراتیک با مردم مربوطه، تحولات ساختاری را در کشور اشغال‌شده انجام دهد. این خطر در زمینه به حقوق اقتصادی، اجتماعی و فرهنگی حتی بیشتر است، زیرا قواعد موجود در آن حوزه گاهی نادقیق هستند و قابلیت تفسیرهای متعارض را دارند. هک پایگاه‌های اطلاعاتی رأی‌دهندگان یا دستکاری در شمارش آرا به‌منظور تغییر نتایج انتخابات یکی از مصادیق روشن در این زمینه قلمداد می‌شود (Lehto, ۲۰۲۳ ,p. ۴). وقوع این امر در شرایطی که

قدرت اشغالگر مدعی برگزاری همه‌پرسی جهت حفظ حضور خود در سرزمین اشغالی و یا حتی الحاق قلمروی مذکور به کشور خود است، محتمل می‌نماید. در واقع، در چنین وضعیتی، قدرت اشغالگر به به‌کارگیری ابزارهای سایبری و امکانات موجود در فضای سایبر، به‌جای تلاش جهت ایفای تعهدات خود به‌موجب حقوق اشغال، در راستای دور زدن آن‌ها و تثبیت وضعیت اشغال گام برمی‌دارد.

در سوی دیگر این معادله، اگر قدرت اشغالگر در سرزمینی قرار گیرد که تبعیض در سیستم‌های اطلاع‌رسانی اینترنتی و یا ثبت داده‌های فردی اقلیتی خاص با اهداف خصمانه در آن رواج داشته است، به نظر می‌رسد در سازگاری با اصول حقوق بشری مندرج در میثاقین ۱۹۶۶ و سایر اسناد بنیادین حقوق بشری که طرف آن‌هاست و به این سبب، نسبت به این دولت و سرزمین‌های تحت صلاحیت آن از جنبه الزام‌آوری برخوردار است، مجاز به اعمال تغییر و اصلاحات در سیستم‌های اطلاعاتی رایانه‌ای و اینترنتی و نیز سطوح ارتباطی سایبری خواهد بود. در بعضی موارد ممکن است اشغالگر ملزم به نسخ قوانین داخلی کشور محل اشغال و تصویب متون قانونی جدید برای انجام تعهدات خود باشد. ازجمله قوانینی که قدرت اشغالگر می‌تواند آن‌ها را نسخ و قوانین جدیدی را وضع کند، می‌توان به قوانینِ مغایر با قواعد بین‌المللی مانند قواعد حقوق بشری و قوانین مانع از اجرای کنوانسیون چهارم ژنو را نام برد. امری که در ماده ۶۴ کنوانسیون چهارم ژنو درج شده است. در شرایطی که دوران اشغال بنا به دلایل متعدد به درازا بینجامد و در همین زمان فضای همیشه در حال تحول و دگرگونی سایبر با پیشرفت‌های روزافزون خود، امکانات جدیدی را برای کاربران این فضا فراهم سازد، آیا قدرت اشغالگر می‌تواند به بهانه عدم تغییر در قوانین ازپیش‌موجود در سرزمین اشغالی، از تأمین امکانات جدید برای غیرنظامیان تحت اشغال خودداری نماید؟ و آیا عملکردی که در ابتدا به‌عنوان اجرای اصول حقوقی بین‌المللی حاکم بر وضعیت اشغال سرزمینی صورت می‌پذیرد، در تضاد با اصول مسلم حقوق بشر و اصل پذیرفته‌شده «تضمین امکان ادامه زندگی عمومی

مردم در سرزمین اشغالی» نخواهد بود؟ این‌ها از مواردی هستند که دستورالعمل به آن‌ها ورودی نداشته است.

ایجادِ توازن میان مصالح جمعیت غیرنظامی در یک‌سو و منافع قدرت اشغالگر در سوی دیگر، جلوه‌های دیگری نیز دارد. می‌دانیم که طبق ماده ۲۵ کنوانسیون چهارم ژنو، اشخاص تحت حمایت در سرزمین اشغالی باید اجازه داشته باشند اخبار واجد ماهیتِ اکیداً شخصی را به اعضای خانواده خویش، صرف‌نظر از محل سکونت آن‌ها، انتقال دهند و بدون تأخیر ناروا اخبار ایشان را دریافت کنند. اگرچه بر اساس ماده یادشده از کنوانسیون چهارم ژنو، ممکن است قدرت اشغالگر اجازه دهد چنین مکاتباتی شامل مکاتبات ایمیلی یا مدخل‌های رسانه‌های اجتماعی باشند، ولی می‌تواند بر انتقال آن‌ها محدودیت‌هایی بار نماید. در این زمینه، دستورالعمل ذیل قاعده ۱۴۶ خود یادآور می‌شود که قدرت اشغالگر می‌تواند در زمان‌های خاصی از روز دسترسی به اینترنت را محدود سازد، از ارسال پیوست‌ها ممانعت به عمل آورد، سرعت اتصال را کاهش دهد یا بکارگیری خدمات جریان‌سازی[1] رسانه‌ای یا همتا به همتا[2] را تضییق نماید (Tallinn Manual ۲,۰ ,p. ۵۴۵). با وجود این، باید ابزاری باقی بماند که انتقال اخبار خانوادگی به‌صورت ادواری را میسر سازد. برای نمونه، ممکن است مقامات دولت اشغالگر بنا به دلایل امنیتی ترافیک اینترنتی را محدود کنند، ولی اجازه انتقال مکاتبات خانوادگی از طریق سامانه پستی را بدهند (Manual Tallinn ۲,۰ ,p. ۵۴۵). در واقع، در اصل حقِ اشخاص تحت حمایت مبنی بر اطلاع‌گیری از اعضای خانواده، نباید خدشه‌ای وارد گردد. همچنین قدرت اشغالگر باید، به میزان ممکن در شرایط ذیربط و بدون هرگونه تمایز زیان‌بار، تداومِ عملیات‌های رایانه‌ایِ حیاتی برای بقای جمعیتِ غیرنظامیِ سرزمین اشغالی را تضمین نماید. از جمله می‌بایست فعالیت سامانه‌های ضروری برای کارکرد

1 Streaming
2 Peer-to-peer

خدمات شهری همچون شبکه برق‌رسانی، دستگاه‌های تصفیه آب یا تأسیسات فراوری فاضلاب را دربربگیرند (Manual Tallinn ۲٫۰, p. ۵۴۶).

اما در همین مقررات نیز جای تردید و تأمل همچنان باقی است. حقوق بشر، به‌صورت آنلاین و آفلاین اعمال می‌شود؛ اصلی مسلم و تثبیت‌شده که نخستین بار در قطعنامه شورای حقوق بشر در سال ۲۰۱۲ در مورد ترویج، حمایت و برخورداری از حقوق بشر در اینترنت[1] بیان شد (Council Rights Human, ۲۰۱۲, para. ۱). بر پایه این اصل، البته با نظرداشت محدودیت‌های مجازِ وارد بر حق‌های بشری در شرایط عادی و احیاناً تعلیق بعضی تعهدات دولت‌ها در شرایط استثنایی و اضطراری، همان مسئولیت‌ها و تعهدات حقوق بشری که دولت‌ها در دنیای فیزیکی دارند در دنیای دیجیتال نیز اعمال می‌شود. اگرچه حقوق بشر جهانی و غیرقابل تقسیم است، برخی از آن‌ها به‌صورت ویژه با استفاده از اینترنت مرتبط هستند؛ ازجمله آزادی عقیده، بیان و اطلاعات، آزادی اجتماعات و حریم خصوصی. برای ایجاد امکان بهره‌مندی کامل از حقوق بشر به‌صورت آنلاین، بسیار مهم است که اینترنت باز، رایگان و امن با دسترسی برابر و فراگیر برای همه باقی بماند (Sweden of Offices Government, ۲۰۲۲, p. ۸). بنابراین، حتی اگر دسترسی به دیگر راه‌های ارتباطی میسر و ممکن باشد، برخورداری مردم سرزمین اشغالی از امکانات فضای سایبر بدون وجود توجیه قابل قبول از سوی اشغالگر، مسموع و مقبول نخواهد بود.

گروه‌های آسیب‌پذیری مانند کودکان، قربانیانِ بی‌دفاع و بی‌گناهِ جنگ‌ها و پیامدهای آن‌ها ازجمله اشغال نظامی هستند. از این‌رو، شایسته و نیازمند حمایت‌های ویژه‌ای هستند. برای نمونه، وفق ماده ۵۱ کنوانسیون چهارم ژنو، تنها اشخاصِ تحت حمایتی که بالاتر از ۱۸ سال دارند را می‌توان تحت شرایط معین به کار اجباری گمارد. ملهم از این ماده، بر اساس دستورالعمل، الزام کودکان به هرگونه کار مرتبط با فضای سایبر، صرفنظر از هدف آن، ممنوع است (Manual Tallinn ۲٫۰, p. ۵۴۵). ماده (ح)۲۳

1 The Promotion, Protection and Enjoyment of Human Rights on the Internet

مقررات لاهه، طرف مخاصمه را از وادار ساختن اتباع دشمن به مشارکت در عملیات‌های نظامی منع می‌کند. نیز طبق ماده ۵۱ کنوانسیون چهارم ژنو، قدرت اشغالگر نمی‌تواند اشخاص تحت حمایت را به خدمت در نیروهای مسلح یا کمکی خویش مجبور سازد. از این‌رو، هرچند ممکن است اشخاص تحت حمایت دارای مهارت‌های زبانی، ادراک فرهنگی، دانش سامانه‌های رایانه‌ایِ فعال در کشور خویش یا سایر اطلاعاتی باشند که انجام عملیات‌های نظامیِ سایبریِ مؤثر برای قدرت اشغالگر را میسر می‌سازند، ولی این‌گونه مشارکت اجباری ممنوع است. بنابراین، با وجود اینکه در زمینه مورد بحث در این نوشتار، چالش اصلی دولت‌ها این است که اطمینان حاصل کنند که مردم سرزمین اشغالی در درجه اول از جرم و جاسوسی در اینترنت محافظت می‌شوند، تطبیق مشکل امنیت اینترنت در مقوله‌های اشغال نیز منجر به تحمیل وظایف جدیدی اعم از فعل و ترک فعل نسبت به قدرت اشغالگر خواهد شد (O'Connell et al, 2012, p. 3). به باورگروه کارشناسان، این ممنوعیت به فعالیت‌های سایبریِ مقدماتی برای عملیات‌های نظامی، اقدامات سایبری احتیاطی برای حفاظت از شبکه‌های رایانه‌ای خود قدرت اشغالگر و نگاهداری کلی شبکه‌های رایانه‌ای قدرت اشغالگر که برای عملیات‌های نظامی به کار می‌روند تسری می‌یابد (Tallinn Manual 2.0, p. 546).

۲- فعالیت‌ها و سامانه‌های سایبری نظم و امنیت عمومی سرزمین اشغالی

یکی از اصول بنیادین حقوق بین‌الملل ناظر بر اشغال نظامی، بایستگی حفظ و اجرای قوانین کشور اشغال‌شده اعم از قانون اساسی یا قوانین عادی و تداوم‌بخشی به نهادهای قانون‌گزاری است، به‌گونه‌ای که حتی قدرت اشغالگر نیز باید بنابه‌مورد آن قوانین را اجرا نماید و به هیچ‌روی حق فسخ، ابطال یا تغییر آن‌ها را ندارد. این خود یکی از جلوه‌ها قاعده «منع تغییر وضعیت حقوقی سرزمین اشغالی بر اثر اشغال» است. با این حال، این اصل کلی، استثنائاتی دارد و اگر نظم و امنیت عمومی سرزمین اشغالی اقتضای

آن را داشته باشد، قدرت اشغالگر می‌تواند به وضع قوانین و به‌ویژه قوانین کیفری خاص دست بزند و در سرزمین تحت اشغال به مرحله اجرا درآورد (ضیایی بیگدلی، ۱۳۹۶، ص. ۲۷۶). استثنای یادشده، در دستورالعمل مورد توجه قرارگرفته است. وفق قاعده ۱۴۷ دستورالعمل، «قدرت اشغالگر باید، جز در صورت ممانعت مطلق، ضمن رعایت قوانینِ جاری درکشور و از جمله قوانین قابل اِعمال بر فعالیت‌های سایبری، کلیه اقداماتی که در توان دارد را برای اعاده یا تضمینِ حتی‌الامکان نظم و امنیت عمومی اتخاذ نماید» (Tal-linn Manual ۲,۰, p. ۵۴۶).

به باورکارشناسان دستورالعمل، قدرت اشغالگر متعهد به اعاده و تضمین نظم و امنیت عمومی و از جمله اداره سرزمین به نفع جمعیت و حفظ زیرساخت‌های حساس آن است. این التزام شامل تعهد به ترمیم و نگاهداری زیرساخت سایبری ضروری برای کارکرد سرزمین تحت اشغال همچون سامانه‌های ترابری و الکتریکی و شبکه تهیه آب می‌گردد. به همین شکل، اگر دولت اشغالگر از وجود تارنماها یا شبکه‌های اجتماعی که برای تحریک خشونت فرقه‌ای یا کمک به جرم سایبری به‌کار می‌روند اطلاع یابد، مکلف است آنچه که می‌تواند را برای مسدودسازی یا به طریقی دیگر پیشگیری از چنین فعالیت‌هایی به انجام رساند (Manual Tallinn ۲,۰, p. ۵۴۷). نکته حائز اهمیت آن است که هنگام ارزیابی ظرفیت ابزارها و روش‌های سایبری برای مقابله با آسیب ممنوعه، باید اثرات مستقیم و غیرمستقیم قابل پیش‌بینی آن‌ها بر سایر امور مربوط به جمعیت غیرنظامی در نظرگرفته شوند. برای اطمینان از حفاظت از غیرنظامیان و اشیاء غیرنظامی، از جمله زیرساخت‌های غیرنظامی ضروری، خدمات غیرنظامی و داده‌های غیرنظامی، می‌بایست مراقبت دائمی و مقتضی انجام پذیرد (Géry and Delerue, ۲۰۲۲, p. ۱۲). بر این پایه، توجه به اصول ضرورت و تناسب در این زمینه حائز اهمیت است و قدرت اشغالگر نمی‌تواند به بهانه مقابله با اقدامات ناقض منافع خود، منافع حیاتی جمعیت غیرنظامی را به مخاطره افکند.

قاعده ۱۴۷ دستورالعمل تالین ۲، بر ماده ۴۳ مقرات لاهه و مواد ۳۷ و ۶۴ کنوانسیون چهارم ژنو استوار و بازتاب حقوق بین‌الملل عرفی است. گفتنی است طبق ماده ۴۳ مقررات لاهه، قدرت اشغالگر می‌بایست قوانین قابل اِعمال در سرزمین تحت اشغال را حفظ کند و به آن‌ها احترام بگذارد، مگر این‌که واقعاً چاره‌ای جز الغای آن‌ها نداشته باشد. بر پایه دستورالعمل، اشاره به «قوانین کیفری» در ماده ۶۴ کنوانسیون چهارم ژنو، به‌صورت گسترده‌ای به‌عنوان تسری به کلیه قوانین مجری پذیرفته شده است. بنابراین، قوانین داخلیِ تنظیم‌کننده فعالیت‌های سایبری اعتبار خود را حفظ می‌کنند. قوانین کیفری راجع به جرم سایبری و استراق سمع ارتباطات از راه دور، قوانینی که با ارائه‌دهندگان خدمات اینترنت سر و کار دارند و قوانینی که بر آزادی بیان یا مداخله در حریم خصوصی حاکمند، از مصادیق مرتبط در این زمینه هستند. گفتنی است این قاعده قوانینی که مستقیماً فعالیت‌های سایبری را مطمح نظر قرار نمی‌دهند ولی با آن‌ها در ارتباطند را دربرمی‌گیرد. یکی از مصادیق چنین قوانینی، قانونی است که آزادی بیانِ مذهبی را مقرر می‌دارد. در نبود توجیهی معتبر در حقوق اشغال، این قاعده قدرت اشغالگر را از ممنوع‌سازیِ اِعمال آزادی بیان به‌وسیله ابزارهای سایبری بازمی‌دارد (Tal-linn Manual ۲,۰ ,p. ۵۴۷).

تردید نمی‌توان کرد که امروزه فضای سایبر و اینترنت، به بستری تازه برای اِعمال حق آزادی بیان مبدل شده است (Kerremann and Benedek, ۲۰۱۳, p. ۱۳-۱۵)؛ هرچند نمی‌توان نقض این حق در و از طریق فضای سایبر را نیز نادیده گرفت. یکی از نکات مطرح‌شده در دستورالعمل، امکانِ تحدید آزادی بیان از سوی قدرت اشغالگر در شرایطی معین است. توضیح آن‌که طبق دستورالعمل، قدرت اشغالگر حق دارد به‌رغم وجود مقررات مغایر در قوانین کشور اشغال‌شده، در صورت وجود ضرورت برای امنیت خود، آزادی بیان در فضای سایبر را محدود سازد. این کار می‌تواند مثلاً از طریق اِعمال سانسور برای مقابله با جنبش‌های مقاومت جهت سازمان‌دهی یا اجتماع با استفاده از رسانه‌های

اجتماعی صورت گیرد. به علاوه، قدرت اشغالگر می‌تواند در صورتی که شبکه‌های رایانه‌ای او در خارج از سرزمین اشغالی قربانی حملات سایبریِ ناشی از سرزمین تحت اشغال شوند، اقداماتی مغایر با قانون موجود را نیز اتخاذ کند (Manual Tallinn ۲٫۰, p. ۵۴۷-۵۴۸). در حقیقت، همچنان‌که در زمان صلح و در چارچوب نظام بین‌المللی حقوق بشر، امکان تحدیدِ حقوق بشر و ازجمله آزادی بیان وجود دارد، در صورت تحقق شرایط لازم، دولت اشغالگر نیز می‌تواند در زمان اشغال و درگیری‌های مسلحانه، محدودیت‌هایی را بر برخی حقوق مانند آزادی بیان در فضای سایبر بار نماید. اما باید در نظر داشت که حذف یا دستکاری داده‌های ضروری غیرنظامی می‌تواند به سرعت خدمات دولتی و مشاغل خصوصی را به توقف کامل برساند. برای جامعه بین‌المللی، یافتن یک درک مشترک در مورد قواعد بین‌المللی که به اندازه کافی از جمعیت غیرنظامی در برابر اثرات عملیات سایبری محافظت می‌کند، حیاتی است (ICRC, ۲۰۱۹). از این‌رو، اگر قرار است قوانینی در سطح ملی و قواعد جدیدی در سطوح منطقه‌ای و بین‌المللی تدوین شوند، باید بر اساس چارچوب قانونی موجود، از جمله حقوق بین‌الملل حقوق بشر، ایجاد و تقویت گردند. بی‌تردید این توصیه در خصوص دستورالعمل حاضر نیز صادق است.

افزون بر این، در دستورالعمل آمده است که قدرت اشغالگر حق دارد در مواردی که امنیت او را تهدید می‌کنند، قوانین مجرایی که به عملیات‌های سایبری یا ارتباطات نظامی آن خدشه وارد می‌سازند را لغو نماید یا به حالت تعلیق در آورد. همچنین دستورالعمل یادآور می‌شود که قدرت اشغالگر می‌تواند قوانین مغایر با تعهدات خویش به‌موجب کنوانسیون چهارم ژنو یا سایر قواعد حقوق بین‌الملل را نیز ملغی سازد (Tallinn Manual ۲٫۰, p. ۵۴۸). برای نمونه، قدرت اشغالگر می‌تواند قوانینی برای جایگزینی با قوانین داخلیِ تبعیض‌آمیز تصویب کند که در صورت ابقاء، گروه‌های مشخصی از مردم را بر مبنای نژاد، مذهب یا وابستگی سیاسی، از ابراز نظرات و باورهای خویش باز می‌دارند. بنا بر شرح دستورالعمل ذیل قاعده ۱۴۷، قدرت اشغالگر می‌تواند برای توزیع چنین قوانینی

و تضمین پایبندی به آن‌ها مطابق با قواعد حقوقی بین‌المللی، از ابزارهای سایبری استفاده کند. همچنین بر پایه ماده ۶۴ کنوانسیون چهارم ژنو و نیز ماده ۴۳ مقررات لاهه، می‌تواند زمانی که تصویب قوانین جدید برای قادر ساختنِ او در تضمین نظم و امنیت عمومی، ایفای تعهدات خویش به موجب حقوق اشغال یا حفظ اداره منظم سرزمین اشغالی ضروری باشد، به این کار دست بزند. برای مثال، در بافت فضای سایبر، قدرت اشغالگر می‌تواند مقرراتی را با هدف مقابله با جرمی سایبری که به نحو چشمگیری به ثبات پولی سرزمین اشغالی آسیب می‌زند، به تصویب برساند (Manual Tallinn ۲,۰ ,p. ۵۴۸).

پیش‌تر اشاره رفت که حقوق اشغال نظامی، تنها مصالح جمعیت غیرنظامیِ سرزمین اشغالی را مورد توجه قرار نمی‌دهد، بلکه منافع قدرت اشغالگر را نیز در نظر می‌گیرد و از این رهگذر، توازنی میان آن مصالح و این منافع برقرار می‌سازد. در این زمینه، بر اساس قاعده ۱۴۸ دستورالعمل، «قدرت اشغالگر می‌تواند اقدامات ضروری برای تضمین امنیت عمومی خود و از جمله یکپارچگی و پایایی سامانه‌های سایبری خویش را اتخاذ کند». طبق نظر کارشناسان، این قاعده بر مواد ۲۷ و ۶۴ کنواسیون چهارم ژنو استوار و بازتاب حقوق بین‌الملل عرفی است. قاعده حاضر اتخاذ اقدامات سایبری در رابطه با امنیت قدرت اشغالگر در کل را مد نظر دارد. بند پایانی قاعده تأکید می‌کند که دامنه آن به حفاظت از سامانه‌های سایبری قدرت اشغالگر تسری می‌یابد (Manual Tallinn ۲,۰ ,p. ۵۴۸). دستورالعمل به مصادیق اقداماتی که مطابق با این قاعده می‌توان آن‌ها را اتخاذ کرد می‌پردازد و آن‌ها را عبارتند از اقدام در راستای: بستن سامانه‌های ارتباطیِ مورد استفاده برای انتقال اطلاعات مربوط به قدرت اشغالگر به نیروهای شورشی؛ ممنوع کردن ارجاعات ایمیلی به تحرکات، آرایش، تسلیحات، توانمندی‌ها یا فعالیت‌های نظامی؛ اجرای محدودیت‌های ضروری از نظر نظامی بر به‌کارگیری برخی سرورهای معین؛ تحمیل محدودیت‌های زمانی بر به‌کارگیری اینترنت در هنگام نیاز مقامات نظامی به پهنای باند؛

یا اِعمال محدودیت بر استفاده از اینترنت توسط افرادی که تهدید امنیتی ایجاد می‌کنند (Manual Tallinn ۲٫۰, p. ۵۴۸-۵۴۹). در عین حال، از منظر مقررات لاهه اصلاحات ساختاری که بر آینده بلندمدت سرزمین‌های اشغالی تأثیر می‌گذارد، ممنوع است (Vite, ۲۰۰۸, p. ۶۳۴). به این خاطر، تمامی اقدامات یادشده در بالا و یا اعمالی که در راستای تضمین امنیت و تسهیل عملکرد قدرت اشغالگر مورد استفاده قرار می‌گیرند، تنها با رعایت همین شرط قابلیت اعمال و مشروعیت خواهند داشت.

کارشناسان تدوین‌کننده دستورالعمل، برای تبیین مطلب، از قدرت اشغالگری سخن به میان می‌آورند که به‌صورت مستدل و مستند متقاعد می‌شود برای انتقال دستورالعمل‌های ساخت بمب به اعضای جنبشی شورشی از پنهان‌نگاری[1] استفاده می‌گردد. اگر راه مؤثری برای تعیین این‌که کدامین فایل‌ها محتوی پیام‌های رمزگذاری شده هستند وجود نداشته باشد، قدرت اشغالگر می‌تواند ارتباطات سایبری افرادی که منطقاً باور دارد در چنین فعالیت‌هایی دخیل هستند را ممنوع یا محدود سازد. تحت شرایط مضیق، قدرت اشغالگر می‌تواند در صورت وجود ضرورت ارتباطات را به‌طورکل تا زمانی که وضعیت به گونه‌ای رضایت‌بخش حل‌وفصل شود، محدود سازد. گفتنی است کارشناسان دستورالعمل خاطرنشان می‌سازند که محدودیت‌های وارد بر اشخاص تحت حمایت نباید از محدودیت‌هایی که برای مقابله با دغدغه‌های امنیتیِ مشروعِ قدرت اشغالگر ضروری است فراتر بروند. تعیین ضرورت باید برکلیه شرایط پیرامونی همچون در دسترس بودن سایر اَشکال ارتباطی مبتنی باشد (Manual Tallinn ۲٫۰, p. ۵۴۹).

با این حال، هنگامی که رایانه‌ها یا شبکه‌های یک کشور مورد نفوذ یا مسدود شدن قرار می‌گیرند، ممکن است خطر محرومیت غیرنظامیان از وسایل ضروری اولیه مانند آب آشامیدنی، مراقبت‌های پزشکی و برق وجود داشته باشد. اگر سیستم‌های جی‌پی‌اس فلج شوند، ممکن است خطر تلفات غیرنظامیان برای مثال، از طریق اختلال در عملیات

1 Steganography

پرواز بالگردهای نجات که جان انسان‌ها را نجات می‌دهند ایجاد گردد. سدها، نیروگاه‌های هسته‌ای و سیستم‌های کنترل هواپیما، به دلیل اتکا به رایانه، در برابر حملات سایبری نیز آسیب‌پذیر هستند. شبکه‌ها به قدری به هم متصل هستند که ممکن است محدود کردن اثرات حمله به یک قسمت از سیستم بدون آسیب رساندن به قسمت‌های دیگر یا اختلال در کل سیستم دشوار باشد. رفاه، سلامتی و حتی زندگی صدها هزار نفر ممکن است تحت تأثیر قرار گیرد. یکی از نقش‌های قدرت اشغالگر این است که باید مراقبت دائمی برای نجات غیرنظامیان و تضمین بهره‌وری آنان از امکانات معمول زندگی انجام شود. امری که ریشه در قاعده لزوم حفاظت از اشیاء ضروری برای بقای جمعیت غیرنظامی دارد که یکی از قواعد مهم حقوق بشردوستانه محسوب می‌شود و طبق قاعده شماره ۵۴ مطالعه سال ۲۰۰۵ کمیته بین‌المللی صلیب سرخ، به بخشی از حقوق بین‌الملل عرفی مبدل شده است (هنکرتز و دوسوالدبک، ۱۳۸۷، ص. ۳۰۵). اشغال فیزیکی قواعد و محدودیت‌هایی دارد که به همان اندازه برای اقدام در فضای سایبر قابل اعمال هستند.

۳- ضبط و مصادره اموال و زیرساخت‌ها و سامانه‌های سایبری

بحث از زیرساخت‌ها یا سامانه‌های سایبری و امکان توقیف، ضبط و مصادره آن‌ها به‌ویژه در پرتو قواعد دستورالعمل، جالب و سودمند می‌نماید و می‌تواند در روشن شدنِ حقوق و مسئولیت‌های قدرت اشغالگر در این زمینه به کار آید. دولت اشغالگر موظف است از تخریب اموال و سرقت آن‌ها در سرزمین اشغالی خودداری و پیشگیری نماید. این وظیفه کلی دولت اشغالگر در مناطق تحت اشغال اوست (دهقانی، ۱۳۸۹، ص. ۱۴۵). در این زمینه، اموال موجود به دو دسته کلی اموال عمومی (دولتی) و اموال خصوصی تقسیم می‌شوند. اموال عمومی در حقوق بشردوستانه به آن دسته از اموال اطلاق می‌شود که به فرد یا گروهی خاص تعلق ندارد و همه مردم در استفاده و بهره‌برداری از آن ذی‌نفع هستند. به سخنی دیگر، در مورد آن‌ها مالکیت همگانی وجود دارد. بناهای عمومی،

پارک‌ها، جنگل‌ها و معادن از این دست اموال محسوب می‌شوند. اموال دولتی خود به دو دسته غیرمنقول و منقول تقسیم می‌گردند (دهقانی، ۱۳۸۹، ص. ۱۴۶-۱۴۵). قواعد مربوط به اموال غیرمنقول عمومی در ماده ۵۵ مقررات لاهه مندرج است که مطابق با آن، اشغالگر باید تنها اداره‌کننده و استفاده‌کننده از ساختمان‌های عمومی، املاک، جنگل‌ها و زمین‌های کشاورزی متعلق به دولت دشمن باشد که در سرزمین اشغال موجودند. بر اساس ماده ۵۵ مقررات لاهه، اشغالگر باید در حفظ این اموال کوشا باشد و آن‌ها را طبق اصول استفاده، اداره نماید. فهرست اموال نام‌برده در ماده ۵۵ حصری نیست. از ماده ۵۵، چند نکته مهم قابل استخراج است. یکم، مالکیت اموال غیرمنقول دولتی از دولت سرنگون‌شده به اشغالگر منتقل نمی‌شود. دوم، اشغالگر حق اداره این اموال و جمع‌آوری منافع آن را دارد و سوم، اشغالگر متعهد است که از اموال مزبور محافظت کند و تداوم موجودیت آن‌ها را تضمین نماید (لسانی، ۱۳۸۹، ص. ۱۷۲-۱۷۱). به سخنی دیگر، اشغالگر حق ضبط و مصادره اموالِ غیرمنقول دولتی را دارا نیست.

هرچند اموال منقول عمومی و دولتی کشور اشغال‌شده در اساس همچون اموال غیرمنقول مصون از تعرض هستند، ولی در دو مورد بر اصل مصونیت آن‌ها استثنا وارد می‌شود: ۱) طبق قاعده ۵۱ مطالعه سال ۲۰۰۵ کمیته بین‌المللی صلیب سرخ در خصوص حقوق بشردوستانه عرفی، قدرت اشغالگر می‌تواند اموال منقولی که جنبه نظامی دارند و برای مقاصد نظامی به‌کار می‌روند (مانند سلاح‌ها، مهمات و ادوات جنگی) را ضبط، تصرف و مصادره کند و در واقع، این اموال، «غنیمت جنگی» قلمداد می‌گردند (هنکرتز و دوسوالدبک، ۱۳۸۷، ص. ۲۹۴-۲۹۰)؛ و ۲) بر پایه ماده ۵۵ کنوانسیون چهارم ژنو، قدرت اشغالگر می‌تواند خواربار، مواد غذایی، اشیاء و لوازم پزشکی موردنیاز نیروهای اشغالگر و دستگاه اداره‌کننده سرزمین اشغالی را ضبط و مصادره نماید، به شرطی که غرامت آن‌ها را به بهای واقعی و بر اساس معاهدات بین‌المللی پرداخت کند. این تجویز، ضبط و مصادره لوازم و کالاهای موجود در انبار بیمارستان‌های غیرنظامی را شامل نمی‌شود، البته مادامی

که این اقلام برای نیازهای جمعیت غیرنظامی لازم باشند. گفتنی است در زمان اشغال نظامی، در چارچوب اصل حمایت از اموال فرهنگی در درگیری‌های مسلحانه، اموال مذهبی، تاریخی و فرهنگیِ متعلق به سرزمین اشغالی، چه منقول باشند و چه غیرمنقول، از هرگونه تعرضی مصون هستند. در خصوص اموال خصوصی، بر پایه قاعده‌ای بنیادین در حقوق بین‌الملل اشغال و به‌طور مشخص‌تر در کد لیبر، اعلامیه بروکسل، دستورالعمل آکسفورد و نیز ماده ۴۶ مقررات لاهه که طبق قاعده ۵۱ مطالعه سال ۲۰۰۵ کمیته بین‌المللی صلیب سرخ به بخشی از حقوق بین‌الملل عرفی نیز مبدل شده است، قدرت اشغالگر باید به مالکیت خصوصی در سرزمین اشغالی احترام بگذارد (هنکرتز و دوسوالدبک، ۱۳۸۷، ص. ۲۹۲). اموال خصوصی اشخاص حقیقی و حقوقیِ ساکن در سرزمین اشغالی، اعم از اتباع یا بیگانگان، مصون از هرگونه تعرض‌اند؛ مگر آن‌که ضبط و تصرف آن‌ها یک ضرورت مبرم نظامی باشد که در این صورت نیز، مشروط است به پرداخت غرامت متناسب و مناسب از سوی قدرت اشغالگر به صاحب یا صاحبان مال ذی‌ربط (ماده ۵۳ کنوانسیون چهارم ژنو). افزون بر این، تخریب یا انهدام اموال خصوصی ساکنان سرزمین اشغالی، بدون ضرورت مبرم نظامی، اکیداً منع شده است (ضیایی بیگدلی، ۱۳۹۶، ص. ۲۸۶-۲۸۵). بنابراین، عملیات سایبری در چارچوب وضعیت اشغال نه تنها باید از موازین حاکم بر وضعیت اشغال پیروی کند، بلکه افراد، اشیاء و فعالیت‌های خاصی مانند پرسنل و واحدهای پزشکی، از جمله زیرساخت‌های سایبری آن‌ها، و پرسنل و اشیاء مذهبی یا بشردوستانه تحت حمایت ویژه قرار دارند (Sweden of Offices Government, ۲۰۲۲, p. ۷).

دستورالعمل، به مقوله ضبط و مصادره اموال سایبری نیز ورود کرده است. طبق قاعده ۱۴۹، «به میزانی که حقوق اشغال اجازه ضبط یا مصادره اموال را بدهد، تحت کنترل در آوردن زیرساخت‌ها یا سامانه‌های سایبری به نحو مشابهی مجاز است». این قاعده بر مواد ۴۶، ۵۲، ۵۳، ۵۵ و ۵۶ مقررات لاهه و ماده ۵۵ کنوانسیون چهارم ژنو مبتنی

و بازتاب حقوق بین‌الملل عرفی است. کارشناسان یادآور می‌شوند که باید میان استعمال اصطلاحات «ضبط»[1] و «مصادره»[2] در این قاعده قائل به تفکیک شد. قدرت اشغالگر می‌تواند اموال منقول دولت از جمله اموال سایبری مانند رایانه‌ها، سامانه‌های رایانه‌ای و سایر ابزارهای کامپیوتری و حافظه‌ای را برای استفاده در عملیات‌های سایبری «ضبط» کند. اموال خصوصی را نمی‌توان ضبط کرد. «مصادره» توسط قدرت اشغالگر دریافت کالاها یا خدمات در ازای پرداخت غرامت است. چنین مالکیتی تنها برای اداره سرزمین تحت اشغال یا به خاطر نیازمندی‌های نیروهای اشغالگر و بنابراین، صرفاً در صورت مطمح نظر قرارگرفتن ملزومات و نیازمندی‌های جمعیت غیرنظامی، مجاز است (Manual Tallinn ۲٫۰, p. ۵۴۹-۵۵۰).

ظهور و توسعه سریع فناوری اطلاعات و ارتباطات، همزمان فرصت‌ها و چالش‌هایی را برای جامعه بین‌المللی به همراه آورده است. از یک‌سو، اینترنت و سایر فناوری‌های اطلاعاتی و ارتباطاتی، تبادل اطلاعات بین بازیگران مختلف را تسهیل کرده و ارائه خدمات عمومی و خصوصی را در جوامع بهبود بخشیده است؛ با کاهش هزینه‌ها و موانع فیزیکی، اتصال دیجیتال عامل مهمی برای توسعه اقتصادی و حقوق بشر بوده است. این امر به‌ویژه برای گروه‌های آسیب‌پذیر در کشورهای در حال توسعه صادق است. در عین حال، فراگیر بودن و وابستگی به این فناوری‌ها، آسیب‌پذیری نوع بشر را در برابر استفاده از آن‌ها برای اهداف مخرب توسط بازیگران دولتی و غیردولتی افزایش داده است (Foreign Affairs Ministry of, ۲۰۲۰, p. ۱-۲). به همین ترتیب، سرشت داده‌های رایانه‌ای در چارچوب حقوق بشردوستانه، یکی از مسائل محل مناقشه در میان پژوهشگران این عرصه است (Pomson, ۲۰۲۳, p. ۱). در زمینه موضوع این قاعده، اکثریت گروه بین‌المللی کارشناسان قائل به این بود که که در معنای خاص و مضیق،[3] داده‌ها در زمره اموال تلقی

---

1 Confiscation

2 Requisition

3 Sensu stricto

نمی‌گردند. با وجود این، این امر قدرت اشغالگر را از به‌کارگیری داده‌ها برای عملیات‌های نظامی خود منع نمی‌کند (Manual Tallinn ۲٫۰, p. ۵۵۰).

اقلیتی ازکارشناسان قائل به این بودند که داده‌ها می‌توانند واجد وصف اموال باشند. دستورالعمل مقرر می‌دارد که قدرت اشغالگر متعهد است از ارزش سرمایه‌ای اموال غیرمنقول دولت (که از اموال منقول متمایز هستند) حراست نماید و با احترام و مراقبت مقتضی آن‌ها را اداره کند. چنین اموالی شامل ساختمان‌های محل استقرار زیرساخت سایبری می‌گردند. مال منقول دولتی به شمار آمدن یا نیامدن آن زیرساخت سایبری به امکان یا عدم امکان برداشتن آن بدون ورود خسارت اساسی به ساختمان ذیربط بستگی دارد. اگر نتوان آن را آن‌گونه برداشت، مالی است غیرمنقول که مستحق بهره‌مندی از حمایت اموال دولتی غیرمنقول است. بر این اساس، قدرت اشغالگر از اتخاذ هرگونه اقدامی که ارزش سرمایه‌ای آن راکاهش دهد منع خواهد شد. زیرساخت سایبری که بتوان آن را بدون ایراد خسارت چشمگیر به ساختار ساختمان برداشت، مالی است منقول و مشمول ضوابط موجود در این خصوص. بر اساس و ملهم از مواد ۴۶ و ۵۲ مقررات لاهه، کارشناسان دستورالعمل بر این باور بودند که اموال سایبری (یا خدمات سایبری) خصوصی، اصولاً باید محترم داشته شوند و نمی‌توان آن‌ها را ضبط کرد. چنین اموالی را تنها می‌توان برای نیازمندی‌های ارتش اشغالگر و اداره سرزمین اشغالی مصادره نمود. برای نمونه، مصادره یک سرور تحت مالکیت خصوصی به‌منظور تسهیل اداره سرزمین یا درخواست دسترسی به اینترنت از یک ارائه‌دهنده خصوصی خدمات اینترنتی در زمان نیاز نیروی اشغالگر، مقتضی و متناسب خواهد بود (Manual Tallinn ۲٫۰, p. ۵۵۰).

در دستورالعمل آمده که تفکیک میان اموال سایبری متعلق به دولت از اموال سایبریِ خصوصی دشوار است. زیرساخت سایبری می‌تواند به‌صورت اشتراکی در مالکیت شرکای دولتی و خصوصی باشد یا توسط شرکت‌های خصوصی بر مبنای امتیازات عمومی ایجاد و نگاهداری شود. در زمان بروز تردید راجع به ماهیت خصوصی یا عمومی تجهیزات

سایبری، پاره‌ای از دولت‌ها قائل به اماره‌ای کلی هستند که بر مبنای آن تجهیزات ذیربط عمومی‌اند، مگر این‌که ماهیت خصوصی آن‌ها مشهود و مسلم گردد. جایی که منافع دولتی و خصوصی در رایانه‌ها، شبکه‌های رایانه‌ای یا دیگر اموال سایبری همزمان وجود داشته باشند، مال ذیربط را می‌توان به تصرف درآورد، ولی بابت منافع خصوصی آن باید غرامت پرداخت شود. باید با اموال سایبری (از جمله اموال سایبری دولتی) شهرداری‌ها و نهادهایِ اختصاص‌یافته به مذهب، امور خیریه، آموزش، و امور هنری و علمی همچون اموال خصوصی رفتار شود. به این سان، چنین اموالی را مشروط به تحقق پیش‌شرط‌های مورد اشاره در بالا می‌توان مصادره (و نه ضبط) کرد. بر پایه ماده ۵۳ مقررات لاهه، تجهیزات تعبیه‌شده برای انتقال اخبار را می‌توان در صورتی که مالی خصوصی باشند، توقیف کرد. در صورتی که دیگر نیازی به آن‌ها نباشد، باید به مالکشان بازگردانده و غرامت پرداخت شود. امروزه، کلیه گوشی‌های تلفن همراه یا رایانه‌های متصل به اینترنت قادر به انتقال اخبار هستند. کارشناسانِ تدوین‌کننده دستورالعمل موافقت کردند که تسری اِعمال این قاعده به کلیه این قبیل اقلام با موضوع و هدف مقرره معاهداتیِ مبنا که این قاعده از آن مشتق شده است، مغایرت دارد. بنابراین، «تجهیزات تعبیه‌شده برای انتقال اخبار» را باید به‌عنوان تجهیزاتی که «روزنامه‌نگاران» به‌کار می‌برند و توسط سازمان‌هایی که به آن‌ها تعلق دارند اداره می‌شوند، تلقی کرد (Manual Tallinn ۲٫۰, p. ۵۵۰-۵۵۱). روی‌هم‌رفته، رسانه‌ها را نمی توان یک هدف مشروع برای حمله دانست. رسانه‌ها، حتی اگر برای مقاصد تبلیغاتی استفاده شوند، از تعرض مصون هستند، مگر اینکه برای مقاصد نظامی یا تحریک مردم به ارتکاب نقض فاحش حقوق بشردوستانه بین‌المللی، اقدامات نسل‌کشی یا اعمال خشونت‌آمیز استفاده گردند (Gallois-Balguy, ۲۰۰۴, p. ۳۷ & ۶۷).

طبق دستورالعمل، اصطلاح «به کنترل درآوردن»[1] به ضبط یا مصادره فیزیکی مال اشاره دارد. مسئله دریافت سایبری این است که آیا اصطلاح مزبور به ضبط یا مصادره

1 Taking control

«مجازی» تسری می‌یابد یا خیر. اکثریت گروه بین‌المللی کارشناسان موافقت کردند که به میزانی که (۱) قدرت اشغالگر بتواند مال ذی‌ربط را برای اهداف خویش به‌کارگیرد و (۲) مالک از به‌کارگیری آن منع شده باشد، چنین می‌شود. اقلیت ابراز داشت که مالکیت فیزیکیِ مال مربوطه، جزء ضروری این قاعده است. همچنین کارشناسان بیان می‌دارند که کابل‌های زیردریایی (شامل آن دسته از اجزاء مستقر بر روی زمین) که سرزمین اشغالی را با سرزمین بی‌طرف مرتبط می‌سازند، مشمول رژیم خاص مقرر در ماده ۵۴ مقررات لاهه هستند. آن‌ها را جز در صورت ضرورت مطلق نمی‌توان ضبط یا تخریب کرد و در صورت ضبط یا تخریب باید متعاقباً غرامت پرداخت شود (Manual Tallinn ۲,۰ ,p. ۵۵۲).

۴- کاستی‌ها و ناراستی‌های دستورالعمل تالین ۲ در زمینه حقوق اشغال نظامی

جهان حقوق و به‌ویژه حقوق بین‌الملل، جهانی انقلابی و معرکه نتایج یک‌باره نیست و نباید هم باشد. حقوق بین‌الملل در تاریخِ سرشار از نشیب و فراز خود کوشیده است تا به آرامی، از خودخواهی‌ها و خودبینی‌های افراد و دولت‌ها بکاهد و در راستای برپایی نظمی ولو نسبی در سپهر روابط بین‌الملل بکوشد. از این‌رو، به نظر می‌رسد این شاخه حقوقی را باید در ترازوی تاریخِ خود به قضاوت و نظاره نشست و همواره عنصر زمان را در جریان‌سازیِ حقوق بین‌الملل در نظر گرفت. نگارندگان معتقدند دستورالعمل تالین ۲ را نیز می‌بایست به همین شکل سنجید و نگریست. اگرچه گوشزد کاستی‌ها و ناراستی‌ها در هر عرصه‌ای و ازجمله در زمینه این دستورالعمل، ضرورتی مبرم است و نمی‌توان از آن چشم پوشید، ولی همزمان، باید به سودمندی‌ها و نقاط قوت آن هم اشاره داشت. دستورالعمل مورد مطالعه ما، گامی آغازین و پیشرفتی مهم برای تنظیم عملیات‌های سایبری از دریچه حقوق بین‌الملل است (Wallace et al.., ۲۰۱۹, p. ۲۰۵) و به این خاطر، در سپهر حقوق بین‌الملل حاکم بر عملیات‌های سایبری، یک خط شکن به‌شمار می‌رود.

همان‌گونه که پژوهشگران عرصه حقوق سایبری به‌درستی متذکر شده‌اند، امروز دیگر بر سر اعمال حقوق بین‌الملل بر فضای سایبر هیچ مناقشه‌ای وجود ندارد؛ ولی همچنان «چگونگی» اعمال آن بر فضای سایبر، محل بحث و پرسش است و همین امر، موجب گردیده تا ما با عدم قطعیت حقوقی در این فضا مواجه باشیم (Pijpers, ۲۰۲۳, p. ۳۹۴-۴۲۱). به سخنی دیگر، در حقوق بین‌الملل سایبری «مناطق خاکستری»[1] و غیرشفافی وجود دارند (Schmitt, ۲۰۱۷, p. ۲۱) که و ابهاماتی به چشم می‌خورند (Schmitt, ۲۰۱۹, p. ۳۵۳) که شفاف‌سازی آن‌ها ضرورتی روشن دارد. چنین می‌نماید که دستورالعمل تالین ۲، در زمینه کاهش این عدم قطعیت و تنویر مناطق خاکستری حقوق بین‌الملل سایبری، گام‌های مناسبی برداشته است؛ هرچند نمی‌توان انکار هم کرد که ممکن است گاه به‌واسطه بعضی کاستی‌ها و ابهامات خود، به عدم قطعیت در پاره‌ای موارد نیز دامن زده باشد.

شاید نخستین و برجسته‌ترین نقص دستورالعمل تالین ۲ را بتوان سرشت غیرالزام‌آور آن دانست؛ به همین خاطر است که محققان آن را نه حقوق بین‌الملل، بلکه سندی برای تشریحِ موضع و موقعیت حقوق بین‌الملل در قبال عملیات‌های سایبری نام نهاده‌اند (Wadhwani, ۱۱ September ۲۰۲۳). در بالا ملاحظه شد که طبق دستورالعمل تالین ۲، علی‌الاصول، همان قواعدِ سنتیِ حاکم بر حقوق اشغال نظامی مندرج در مقررات لاهه ۱۹۰۷ و نیزکنوانسیون چهارم ژنو، در زمان انجام عملیات‌های سایبری و بر فعالیت‌ها و اموال سایبری مُجری است و فضای سایبر را نمی‌توان و نباید قلمرویی جدید در حقوق بین‌الملل درکنار زمین، دریا، هوا و فضا برای فعالیت‌های انسانی به‌شمار آورد. هرچند، به همین شکل، نمی‌توان و نباید نیازمندی‌ها و بایسته‌هایِ جدیدی که این فضا با خود به همراه می‌آورد را نادیده گرفت. همان‌گونه که پاره‌ای نویسندگان نیز یادآور شده‌اند، با وجودِ پیشرفت‌ها و پیشروی‌های انکارناپذیرِ دستورالعمل تالین ۲ در بسیاری زمینه‌های

1 Grey zones

مرتبط با اعمال حقوق بین‌الملل بر عملیات‌های سایبری، به‌واسطه سرشت رازآلودِ فضای سایبر، کماکان بعضی عرصه‌های حقوقی از دید آن دور مانده و قواعد مرتبط با آن‌ها مشخص نشده‌اند (Chircop, ۲۰۱۹, p. ۳۵۰). آنچه حتی در نگاهی کلی هم راجع به دستورالعمل و مسئله حقوق اشغال به چشم می‌خورد، محدود بودنِ قواعد آن به سه حوزه مورد بررسی و نادیده گرفتن و نپرداختن به دیگر جنبه‌های حقوق اشغال نظامی است که ممکن است از رهگذر انجام عملیات‌های سایبری و به‌کارگیری فضای سایبر از سوی قدرت اشغال‌گر، تحت تأثیر قرارگیرند.

هر چند نگارندگان این نوشتار تا حدودی با نظر کارشناسان تدوین‌کننده دستورالعمل موافقند و بر این باورند که توسعه هنجارهای رفتار دولت در فضای سایبر مستلزم اختراع مجدد حقوق بین‌الملل نیست و همچنین هنجارهای بین‌المللی موجود را منسوخ نمی‌کند، اما این گزاره را نیز رد نمی‌کنند که دستورالعمل تالین ۲ نیز از خلأ، نبود و کمبود قواعد مبری نیست. دستورالعمل در برخی موارد واقعیات حاکم بر عملکرد قدرت اشغالگر را نادیده انگاشته و نکاتی را مورد تأیید قرار داده است که شاید بتوان بدون بزرگ‌نمایی، آن‌ها را تا اندازه‌ای آرمان‌گرایانه و به دور از واقعیاتِ موجود به‌شمار آورد. در عین حال، خلأهای موجود در مفاد دستورالعمل که یا ناشی از عدم توجه و یا عدم تمایل به شفاف‌سازی بعضی نکات ضروری است، راه را برای تفاسیر موردی و البته مضر از نظام حقوقی حاکم بر اشغال سرزمینی در حوزه سایبری بازگذاشته است. تفاسیری که در نهایت به عمل تبدیل شده و قادر ندگزاره مورد تأکید کارشناسان را در خصوص عدم وجود امکان اشغال در فضای سایبر با چالش مواجه سازند و زمینه‌های «اشغال دیجیتال» داده‌ها و اطلاعات، امکانات و زیرساخت‌های ضروری جمعیت غیرنظامی ساکن در سرزمین اشغالی را فراهم نمایند. در زمانه‌ای که داده‌ها و اطلاعات را به راستی باید نفت جدید دانست، تسلط بر آن‌ها از سوی دولت‌های دیگر نباید شتاب‌زده و با تکیه صرف بر قواعد سنتی حقوق بین‌الملل تحلیل کرد.

با این حال، همان‌طور که یکی کارشناسانِ تدوین‌کننده دستورالعمل تالین ۲ نیز یادآور شده، این دستورالعمل تنها نقطه آغازی است برکوشش و پویش‌های بیشتر در حوزه حقوق بین‌الملل ناظر بر فضای سایبر (Jensen, ۲۰۱۷, p. ۷۷۸). در واقع، راه برای تکمیل و بازبینی دستورالعمل تالین ۲ ازجمله در خصوص مباحث مرتبط با حقوق اشغال نظامی همچنان باز است.. مسیری که با تدوین دستورالعمل تالین ۲ در سال ۲۰۱۷، راجع به دستورالعمل تالین سال ۲۰۱۳ طی شد و هم‌اکنون می‌بینیم دستوالعمل تالین ۲، نسبت به سلف خود، گسترش و پیشرفت چشمگیری پیدا کرده است. گفتنی است بیشتر کارشناسانِ دستورالعمل تالین سال ۲۰۱۳، انگلیسی-امریکایی و اعضای پیشین یا کنونی کمیته بین‌المللی صلیب سرخ بودند. این تنوعِ محدود کارشناسان و تکیه بیش از اندازه بر منابع حقوقیِ غربی، انتقادات شدیدی را متوجه دستورالعمل تالین سال ۲۰۱۳ کرد (Fleck, ۲۰۱۳: ۳۳۵-۳۳۶; Eichensehr, ۲۰۱۴: ۵۸۷-۵۸۸). این تنوع اندک کارشناسان و منابع و البته محدودیت دامنه دستوالعمل تالین ۲۰۱۳ به نبردهای سایبری، به بازبینی و توسعه دامنه دستورالعمل به‌دست گروهی دوم از کارشناسان با تنوع بیشتر انجامید که به تدوین دستورالعملی جدید باز هم با مدیریت پروفسور مایکل اشمیت، با نام دستورالعمل تالین ۲ راجع به حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری[1] (زین پس، دستورالعمل تالین ۲ یا دستورالعمل) انجامید که در سال ۲۰۱۷ منتشر گردید (Shany and Efrony, ۲۰۱۸: ۵۸۷) و جایگزین دستورالعمل تالین سال ۲۰۱۳ شد. جالب است بدانیم که بنا به تارنمای مرکز عالی پدافند مشترک سایبری ناتو، پروژه ۵ ساله دستورالعمل تالین ۳ نیز از سوی این مرکز و با سرویراستاری پروفسور اشمیت از سال ۲۰۲۱ آغاز شده و قرار است متن نهایی آن در سال ۲۰۲۶ منتشر گردد.[2]

واقعیت آن است که تعیین قواعد ناظر بر فناوری‌های جدید و فضای سایبر،

---

1 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)

2 https://ccdcoe.org/research/tallinn-manual/

همواره دشوار خواهد ماند. یکی از علل این دشواریِ همیشگی را شاید بتوان در سرشت همواره در حال تکامل و پیشرفت فضای سایبر سراغ گرفت. حقوق بین‌الملل می‌بایست در پیش‌بینی‌پذیری و حفظ و تداوم ثبات بین‌المللی، نقشی مؤثر ایفا کند و به نظر روشن است که با توجه به سرشتی که از فضای سایبر گفته شد، نیل به این اهداف در دسترس و آسان نیست (Corn, ۱۵ February ۲۰۱۷). پروفسور اشمیت به درستی خاطرنشان ساخته است که دستورالعمل تالین ۲ «پایان داستان» نیست و تنها یکی از گذرگاه‌هایی است که باید برای تعیین و تبیین قواعد ناظر بر فضای سایبر و عملیات‌های سایبری، می‌بایست از آن بهره گرفت (Schmitt, ۹ February ۲۰۱۷). همچنان‌که دستورالعمل تالین ۲ بعضی از نواقص مورد اشاره منتقدان در دستورالعمل تالین اول سال ۲۰۱۳ (Adams, ۴ January ۲۰۱۷) را رفع کرد یا کاهش داد شاید ما باید چشم به آینده و زمان انتشارِ دستورالعمل تالین ۳ بدوزیم و ببینیم کارشناسانِ مرکز عالی پدافند مشترک سایبری ناتو، تا چه میزان کاستی‌ها و ناراستی‌های دستورالعمل تالین ۲ را مطمح‌نظر قرار می‌دهند و در راستای کاهش آن‌ها می‌کوشند. آنچه هویداست، بایستگیِ تداوم کوشش‌ها در راستای وضع قواعد روشن و الزام‌آور در فضایِ ناشناخته و رازآلودِ سایبر و رهانیدن حقوق بین‌الملل ناظر بر عملیات‌های سایبری از این سرگردانی حقوقی است.

برآمد

دیدیم که بر پایه دستورالعمل، مفهوم حقوقیِ اشغال در فضای سایبر وجود ندارد. افزون بر این، عملیات‌های سایبری به‌تنهایی نمی‌توانند برای ایجاد یا حفظ درجه اقتدار بر سرزمین که برای شکل‌گیری وضعیت اشغال ضروری است، کفایت کنند. با وجود این، می‌توان این عملیات‌ها را برای کمک به ایجاد یا حفظ اقتدار لازم جهت ایجاد وضعیت اشغال به کارگرفت. به علاوه، می‌توان آن‌ها را برای ایجاد اختلال یا ازکار انداختن سامانه‌های رایانه‌ای به‌کار رفته به‌دست قدرت اشغالگر به‌منظور حفظ اقتدار و سلطه بر سرزمین اشغال مورد استفاده قرار داد. پیرو دستورالعمل، اشخاص تحت حمایت در سرزمین اشغالی باید مورد احترام قرارگیرند و در برابر آثار زیان‌بار عملیات‌های سایبری تحت حمایت واقع شوند. افزون بر این، قدرت اشغالگر باید، ضمن رعایت قوانینِ جاری درکشور و از جمله قوانین قابل اِعمال بر فعالیت‌های سایبری، کلیه اقداماتی که در توان دارد را برای اعاده یا تضمینِ نظم و امنیت عمومی اتخاذ نماید. به علاوه، قدرت اشغالگر می‌تواند اقدامات ضروری را برای تضمین امنیت عمومی خود و از جمله یکپارچگی و پایایی سامانه‌های سایبری خویش، اتخاذ کند. در نهایت، به میزانی که حقوق اشغال اجازه ضبط یا مصادره اموال را بدهد، تحت کنترل درآوردن زیرساخت‌ها یا سامانه‌های سایبری به‌نحوی مشابه مجاز است. ملاحظه می‌شود که از منظر دستورالعمل علی‌الأصول، همان قواعدِ سنتیِ حاکم بر حقوق اشغال نظامی مندرج در مقررات لاهه ۱۹۰۷ و نیز کنوانسیون چهارم ژنو، در زمان انجام عملیات‌های سایبری و بر فعالیت‌ها و اموال سایبری مُجری است و فضای سایبر را نمی‌توان و نباید قلمرویی جدید در حقوق بین‌الملل در کنار زمین، دریا، هوا و فضا برای فعالیت‌های انسانی به‌شمار آورد. در حالی‌که دستورالعمل سندی غیر الزام‌آور است که به‌دست گروهی از کارشناسان تهیه شده، ما امیدواریم که بتواند کمک مفیدی به بحث بیشتر بین اندیشمندان عرصه حقوق بین‌الملل در مورد چنین موضوعات چالش برانگیزی ارائه بنماید و هرگونه استفاده از فضا یا زیرساخت‌های

سایبری در درگیری‌های مسلحانه را به هر شکل که باشد، به سوی انطباق با تعهدات بین‌المللی سوق دهد.

هر چند نگارندگان این نوشتار تا حدودی با نظر کارشناسان تدوین‌کننده دستورالعمل موافقند و بر این باورند که توسعه هنجارهای رفتار دولت در فضای سایبر مستلزم اختراع مجدد حقوق بین‌الملل نیست و همچنین هنجارهای بین‌المللی موجود را منسوخ نمی‌کند، اما این گزاره را نیز رد نمی‌کنند که دستورالعمل تالین ۲ نیز از خلأ، نبود و کمبود قواعد مبری نیست. همان‌گونه که در بخش‌های مختلف این نوشتار و بنا به مورد اشاره گردید، دستورالعمل در برخی موارد واقعیات حاکم بر عملکرد قدرت اشغالگر را نادیده انگاشته و نکاتی را مورد تأیید قرار داده است که شاید بتوان بدون اغراق، آن‌ها را ایده‌آلیستی به شمار آورد. در عین حال، خلأهای موجود در مفاد دستورالعمل که یا ناشی از عدم توجه و یا عدم تمایل به شفاف‌سازی برخی نکات ضروری است، راه را برای تفاسیر موردی و البته مضر از نظام حقوقی حاکم بر اشغال سرزمینی در حوزه سایبری بازگذاشته است. تفاسیری که در نهایت به عمل تبدیل شده و قادرند گزاره مورد تأکید کارشناسان را در خصوص عدم وجود امکان اشغال در فضای سایبر با چالش مواجه سازند و زمینه‌های «اشغال دیجیتال» داده‌ها و اطلاعات، امکانات و زیرساخت‌های ضروری جمعیت غیر نظامی ساکن در سرزمین اشغالی را محقق نمایند. در نهایت، نمی‌توان و نباید نیازمندی‌ها و بایسته‌هایِ جدیدی که این فضا با خود به همراه می‌آورد را نادیده گرفت. سرعتِ سرسام‌آورِ پیشرفت‌های فناورانه و پیامدهایِ آن برای ابعاد گوناگونِ زندگی انسان، توجه بیش از پیش و بررسی موشکافانه‌ترِ مسائلِ مرتبط در این زمینه را به بایسته‌ای گریزناپذیر مبدل ساخته است.

حقوق بین‌الملل، در رویارویی با مسائلِ نوپدیدِ دنیای جدید، نباید از قافله بازبماند و می‌بایست بتواند از رهگذرِ روزآمدسازیِ همیشگیِ خود، بر مشکلات و دشواری‌هایی که ممکن است در نتیجه نبود قاعده و سنجه‌های حقوقیِ کارآمد گریبان‌گیرش شود و

سودمندیِ و فلسفه وجودی آن را به چالش بکشاند، چیره گردد. سیر در تاریخِ روابط و حقوق بین‌الملل، به‌خوبی به ما نشان داده است که بی‌قاعدگی و نبود قواعدِ مشخص و منقح حقوقی، بیش از همه، مطلوب و محبوب دولت‌های صاحب قدرت بیشتر است که می‌توانند با بهره‌گیری از این وضعیت، مقاصد یکجانبه و صرفاً سودجویانه خویش را پیش ببرند و منافع و مصالح دیگر دولت‌ها و ملت‌ها و جامعه بین‌المللی را نادیده بگیرند. به باور ما، این امر در خصوص فضای سایبر و بحث عملیات‌های سایبری نیز کاملاً صدق می‌کند و به همین سبب، باید در اندیشه چاره‌ای برای وضعیتِ به‌نسبت افسارگسیخته موازین حقوقی حاکم بر فضای سایبر و عملیات‌های سایبری ازجمله در زمینه حقوق اشغال نظامی بود. در چنین اوضاع‌واحوالی، دولت‌های دارایِ سامانه‌ها و امکاناتِ سایبری برتر، می‌توانند قدرت سایبریِ خویش را برای تهدید دیگر دولت‌ها و جامعه بین‌المللی به‌کار ببرند و فضای سایبر را به ابزارِ جدید زورگویی علیه دولت‌ها و ملت‌ها فاقد سامانه‌ها و امکانات یادشده مبدل سازند. ما معتقدیم همان‌گونه که در عرصه حقوق بین‌الملل دریاها، تلاش‌های دولت‌ها و سازمان‌های غیردولتی سرانجام به تدوین کنوانسیون ۱۹۸۲ حقوق دریاها انجامید که به هر روی، تا اندازه‌ای توانسته است ابرقدرت‌ها را از رفتارهایِ یک‌سویه بازدارد، تلاش برای انعقاد کنوانسیونی جامع در سطح بین‌المللی و اسناد الزام‌آور دیگر در سطوح منطقه‌ای در خصوص فضای سایبر و عملیات‌های سایبری، قابلیت آن را دارد تا زمینه سوءاستفاده از آن فضا و این عملیات‌ها را بکاهد. ایران که در سال‌های اخیر، خود یکی از قربانیان حملات سایبری علیه زیرساخت‌های حساس و به‌ویژه تأسیسات هسته‌ای بوده است، باید در این راستا نقشی فعال و مؤثر ایفا کند و در مسیر قاعده‌مندسازی فضای سایبر و عملیات‌های سایبری، از هیچ کوششی فروگذار نکند.

منابع

الف) فارسی

خلیل‌زاده، مونا (۱۳۹۳)، ***مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری***، تهران: مجد.

دهقانی، مریم (۱۳۸۹)، ***اشغال نظامی در حقوق بین‌الملل و قواعد حقوقی حاکم***، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل (استاد راهنما: دکتر سیدعلی هنجنی)، تهران: دانشگاه شهید بهشتی.

زرنشان، شهرام، کرمی، موسی و زندی، ریحانه (تابستان ۱۴۰۲)، ***مفهومی دیرین در بستری نوین: اعمال حقوق بی‌طرفی بر عملیات سایبری در آینه دستورالعمل تالین ۲***، مطالعات بین‌المللی پلیس، دوره ۱۴، شماره ۵۴.

زرنشان، شهرام، زندی، ریحانه و کرمی، موسی (پاییز و زمستان ۱۴۰۲)، ***از آبی دریا تا شبکه سیاه: عملیات‌های سایبری در برخی مناطق دریایی و تنگه‌های بین‌المللی در پرتو دستورالعمل تالین***، حقوق فناوری‌های نوین، دوره ۴، شماره ۸.

شکیب‌نژاد، احسان (۱۳۹۶)، ***قانون‌گذاری در فضای سایبر از منظر حقوق بین‌الملل***، تهران: شهر دانش.

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

فرشاسعید، پرویز و جلالی، محمود (پاییز و زمستان ۱۴۰۱)، ***مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی***، حقوق فناوری‌های نوین، دوره ۳، شماره ۶.

کولب، رابرت و هاید، ریچارد (۱۳۹۴)، ***درآمدی بر حقوق مخاصمات مسلحانه***، ترجمه: سیدحسام‌الدین لسانی، چاپ دوم، تهران: مجد.

گیوکی، آذر، کفایی‌فر، محمدعلی و رضایی، محمدتقی (بهار ۱۳۹۷)، ***قابلیت اعمال قواعد حقوق بشردوستانه بین‌المللی در حملات سایبری با نگاهی به***

دستورالعمل تالین ۲، حقوق پزشکی، دوره ۱۲، شماره ۴۲.

گیوکی، آذر و حکاک‌زاده، محمدرضا (بهار ۱۴۰۱)، ***مداخلی خارجی در امور داخلی دولت‌ها از طریق عملیات سایبری با توجه به دستورالعمل تالین ۲***، مطالعات حقوقی فضای مجازی، دوره ۱، شماره ۱.

لسانی، حسام‌الدین (۱۳۸۹)، ***جایگاه حقوق اشغال نظامی در حقوق بین‌الملل بشردوستانه***، رساله دکتری حقوق بین‌الملل (استاد راهنما: دکتر سیدباقر میرعباسی)، تهران: دانشگاه تهران.

محقق هرچقان، علیرضا، اردبیلی، محمدعلی، بیگ‌زاده، ابراهیم و مهدوی ثابت، محمدعلی (بهار-تابستان ۱۴۰۱)، ***اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد و صلح و امنیت سایبری بین‌المللی***، آموزه‌های حقوق کیفری، دوره ۱۹، شماره ۲۳.

محقق هرچقان، علیرضا، اردبیلی، محمدعلی، بیگ‌زاده، ابراهیم و مهدوی ثابت، محمدعلی (پاییز ۱۴۰۲)، ***حقوق بین‌الملل سایبری و توسعه صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)***، مطالعات حقوق عمومی، دوره ۵۳، شماره ۳.

هنکرتز، ژان ماری و دوسوالدبک، لوئیس (۱۳۸۷)، ***حقوق بین‌المللی بشردوستانه عرفی (جلد اول: قواعد)***، ترجمه: دفتر امور بین‌الملل قوه قضائیه جمهوری اسلامی ایران وکمیته بین‌المللی صلیب سرخ (ویرایش متن: کتایون حسین‌نژاد و پوریا عسکری)، تهران: مجد.

ب) انگلیسی

Adams ,Michael J 4 .January ,(2017) ***A Warning About Tallinn … 2.0Whatever It Says, Lawfare Blo***g, available at: https://www.strategicstudyindia.com/2017/01/a-warning-about-tallinn-20-whatever-it.html

Balguy-Gallois, Alexandre (2004), ***The Protection of Journalists and News Media Personnel in Armed Conflict***, International Review of the Red Cross, Vol. 86, No. 853

Benedek, Wolfgang and Kettemann, Matthias (2013), ***Freedom of Expression and the Internet, Strasburg: Council of Europe Publishing***.

Chircop, Luke (2019), ***Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0***, Melbourne Journal of International Law, Vol. 20, No. 2.

Cohen, Jean (2006), ***The Role of International Law in Post-Conflict Constitution-Making: Toward a Jus Post Bellum for "Interim Occupations"***, New York Law School Law Review, Vol. 51.

Corn, Gary (15 February 2017), ***Tallinn Manual 2.0- Advancing the Conversation, Just Security Blog***, available at: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/

Delerue, François and Géry, Aude (2022), ***International Law and Cyber Security Governance, EU Cyber Direct.***

Efrony, Dan and Shany, Yuval (2018), ***A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber operations and Subsequent State Practice***, American Journal of International Law, Vol. 112, No. 4.

Eichensehr, Kristen (2014), ***Review of The Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)***, American Journal of International Law, Vol. 108.

Fleck, Dieter (2013), ***Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual***, Journal of Conflict and Security Law, Vol. 18, No. 2.

Gasser, Hans-Peter and Dörmann, Knut (2013), ***Protection of the Civilian Population, in Dieter Fleck (ed), The Handbook of International Humanitarian Law, 3rd edition, Oxford: Oxford University Press***.

Government Offices of Sweden (2022), ***Position Paper on the Ap-***

plication of International Law in Cyberspace, available at: https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf

Gross, Aeyal (2017), ***The Writing on the Wall: Rethinking the International Law of Occupation, Cambridge: Cambridge University Press***.

Human Rights Council (16 July 2012), ***The Promotion, Protection and Enjoyment of Human Rights on the Internet***, A/HRC/RES/20/8.

ICRC (2002), ***The Law of Armed Conflict; Belligerent Occupation, International Committee of the Red Cross- Unit for Relations with Armed and Security Forces***, Lesson 9, pp. 1-24.

ICRC (2019), ***Cyber Operations and International Humanitarian Law: Five Key Points, Humanitarian Law and Policy***, available Online at: https://blogs.icrc.org.

ICRC (12 August 1949), ***Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 75 UNTS 287***, available at: https://www.refworld.org/docid/3ae6b36d2.html. [accessed 9 August 2023]

International Conferences (The Hague) (18 October 1907), ***Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land***, available at: https://www.refworld.org/docid/4374cae64.html. [accessed 9 August 2023]

Jensen, Eric Talbot (2017), ***The Tallinn Manual 2.0: Highlights and Insights***, Georgetown Journal of International Law, Vol. 48.

Lehto, Marja (2023), ***Finland's Views on International Law and Cyberspace, Nordic Journal of International Law (Forthcoming)***.

Ministry of Foreign Affairs (2020), ***Costa Rica's Position on the Application of International Law in Cyberspace***, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_In-

ternational_Law_in_Cyberspace.pdf

O'Connell, Mary Ellen and Arimatsu, Louise and Wilmshurst, Elizabeth (2012), ***Cyber Security and International Law, International Law: Meeting Summary- Chatham House***.

Pijpers, Peter B.M.J. (2023), ***Careful What You Wish For: Tackling Legal Uncertainty in Cyberspace***, Nordic Journal of International Law, Vol. 92, No. 3.

Polański, Paul Przemysław (June 2017), ***Cyberspace: A New Branch of International Customary Law?***, Computer Law & Security Review, Vol. 33, Issue 3.

Pomson, Ori (2023), '***Objects'? The Legal Status of Computer Data under International Humanitarian Law***, Journal of Conflict and Security Law, krad002, https://doi.org/10.1093/jcsl/krad002

Schmitt, Michael (ed.) (2017), ***Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge: Cambridge University Press***.

Schmitt, Michael (9 February 2017), ***Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't, Just Security Blog***, available at: https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

Schmitt, Michael N. (2017), ***Grey Zones in International Law of Cyberspace***, Yale Journal of International Law, Vol. 42, Issue 2.

Schmitt, Michael (2019), ***Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations***, International Review of the Red Cross, Vol. 101, No. 1.

Tanodomdej, Papawadee (2019). ***The Tallinn Manuals and the Making of the International Law on Cyber Operations***. Masaryk University Journal of Law and Technology, Vol. 13, No. 1: pp. 67-85.

Vite´, Sylvain (2008), ***The Interrelation of the Law of Occupation and Economic, Social and Cultural Rights: The Examples of Food, Health and Property, International Review of the Red Cross***, Vol. 90, No. 871: pp. 629- 651.

Wadhwani, Sankalp (11 September 2023), ***Revisiting Tallinn Manual 2.0 and Cyber Governance, CESCEBE Blog***, available at: https://www.cescube.com/vp-revisiting-tallinn-manual-2-0-and-cyber-governance

Wallace, David A., McCarthy, Amy H. and isger, Mark (2019), ***Peeling Back the Onion of Cyber Espionage After Tallinn 2.0***, Maryland Law Review, Vol. 78, Issue 2