The University of Tehran Press

Public Law Studies Quarterly

Homepage: http://jplsq.ut.ac.ir

Online ISSN: 2423-8139

Volume: 56, **Issue:** 1
Spring 2026

Cyberattacks on Healthcare Infrastructure from the Perspective of International Law

Kian Biglarbeigi[1] | **Sattar Azizi**[2]✉

1. Ph.D. Student in International Law, Faculty of Law and Political Science, Tehran University, Tehran, Iran. Email: kian.biglarbeigi@gmail.com
2. Corresponding Author; Prof., Department of Law, Faculty of Humanities, Bu-Ali Sina University, Hamedan, Iran. Email: s.azizi@basu.ac.ir

Article Info

Article Type:
Research Article

Pages: 1-35

Received:
2024/11/30
Received in Revised form:
2025/05/25
Accepted:
2025/08/04
Published online:
2026/03/21

Keywords:
Cyberattacks Healthcare Infrastructure Right to Health Human Rights Humanitarian Law Tallinn Manual 2.0.

Abstract

Today, there is no doubt that technology has strengthened the realization of the right to health; however, it has also led to violations and weakening of this right, exposing the world to an increasing risk of cyberattacks. Healthcare programs and medical data are significantly more sensitive and complex than many other types of data and programs, necessitating a high level of protection. Nevertheless, the rise in cyberattacks targeting healthcare and medical facilities is accelerating, with substantial impacts on the provision of healthcare services globally. Consequently, the healthcare industry has lagged behind other industries in protecting its most critical stakeholders (patients), and hospitals must now invest considerable capital and effort to safeguard their systems. In examining cyberattacks, it is essential to distinguish between two categories of such attacks: those reaching the threshold of the use of force and those that do not. Thus, the rules governing these attacks can be categorized and differentiated into two frameworks: peacetime and armed conflict. Therefore, this article employs a descriptive-analytical approach and relies on a library-based method of data collection to address the question of what legal rules govern such attacks.

How To Cite

Biglarbeigi, Kian; Azizi, Sattar (2026). Cyberattacks on Healthcare Infrastructure from the Perspective of International Law. *Public Law Studies Quarterly*, 56 (1), 1-35.
DOI: https://doi.com/10.22059/jplsq.2025.386188.3639

DOI 10.22059/jplsq.2025.386188.3639

Publisher The University of Tehran Press.

انتشارات دانشگاه تهران

فصلنامه مطالعات حقوق عمومی

Homepage: http://jplsq.ut.ac.ir

شاپا الکترونیکی: ۸۱۳۹-۲۴۲۳

دوره: ۵۶، شماره: ۱

بهار ۱۴۰۵

حملات سایبری به زیرساخت‌های بهداشت و درمان از منظر حقوق بین‌الملل

کیان بیگلربیگی[۱] | ستار عزیزی[۲]✉

۱. دانشجوی دکتری حقوق بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران. رایانامه: kian.biglarbeigi@gmail.com

۲. نویسندهٔ مسئول؛ استاد، گروه حقوق، دانشکدهٔ علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران. رایانامه: s.azizi@basu.ac.ir

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱-۳۵

تاریخ دریافت:
۱۴۰۳/۰۹/۱۰

تاریخ بازنگری:
۱۴۰۴/۰۳/۰۴

تاریخ پذیرش:
۱۴۰۴/۰۵/۱۳

تاریخ انتشار برخط:
۱۴۰۵/۰۱/۰۱

کلیدواژه‌ها:
حملات سایبری، حق بر سلامتی، حقوق بشر، حقوق بشردوستانه، راهنمای تالین ۲، زیرساخت‌های بهداشت و درمان.

چکیده

امروزه بدون شک فناوری توانسته است احقاق حق سلامتی را تقویت کند، اما از سویی موجب نقض و تضعیف این حق شده و جهان را با خطر فزاینده‌ای از حملات سایبری مواجه کرده است. برنامه‌های بهداشتی و داده‌های پزشکی به‌مراتب حساس‌تر و پیچیده‌تر از بسیاری دیگر از انواع داده‌ها و برنامه‌ها هستند و به حفاظت سطح بالایی نیاز دارند. با این حال، افزایش حملات سایبری به مراکز بهداشتی و درمانی در حال افزایش است و تأثیرات زیادی بر ارائهٔ خدمات بهداشتی در سرتاسر جهان دارد. بنابراین صنعت بهداشت و درمان در حفاظت از مهم‌ترین ذی‌نفع خود (بیماران) نسبت به سایر صنایع عقب مانده است و بیمارستان‌ها اکنون باید سرمایه و تلاش شایان توجهی را برای حفاظت از سیستم‌های خود به‌عمل آورند. البته در بررسی حملات سایبری باید به تفکیک دو گونه از این حملات پرداخت؛ حملاتی که به آستانهٔ توسل به زور می‌رسند و آنهایی که به این آستانه نمی‌رسند. بنابراین قواعد حاکم بر این حملات در دو قالب زمان صلح و زمان مخاصمات مسلحانه قابل تفکیک و دسته‌بندی است؛ از این‌رو در این مقاله با استفاده از روش توصیفی ـ تحلیلی و گردآوری اطلاعات به‌صورت کتابخانه‌ای به بررسی قواعد حاکم بر این‌گونه حملات می‌پردازیم.

استناد

بیگلربیگی، کیان؛ عزیزی، ستار (۱۴۰۵). حملات سایبری به زیرساخت‌های بهداشت و درمان از منظر حقوق بین‌الملل. *مطالعات حقوق عمومی*، ۵۶ (۱)، ۱- ۳۵.
DOI: https://doi.com/10.22059/jplsq.2025.386188.3639

DOI 10.22059/jplsq.2025.386188.3639

ناشر مؤسسهٔ انتشارات دانشگاه تهران.

۱. مقدمه

امروزه با گسترش دانش بشری و توسعهٔ فناوری، باید فضای سایبر را نیز به قلمرو تحت صلاحیت دولت‌ها اضافه کرد؛ هرچند که هر کدام از فضاهای پیشین دارای نظام حقوقی خاص خود هستند، اما فضای سایبر از بُعد قاعدهٔ حقوقی خلأهای بی‌شماری دارد. همچنین تأثیر پیشرفت فناوری در زندگی روزمرهٔ افراد و در بُعد وسیع‌تر آن، یعنی ارتباطات و تعاملات دولت‌ها با یکدیگر قابل کتمان نیست. این پیشرفت‌ها از یک سو، موجب تسهیل در امور بشر، زندگی راحت‌تر و توسعهٔ هنجارهای زندگی دموکراتیک می‌شود، اما از سوی دیگر آثار و تبعات مخربی نظیر مواجههٔ روزافزون دولت‌ها با حملات سایبری دارد. این‌گونه حملات با توجه به فضای شکل‌گیری آنها دارای ویژگی‌هایی مانند هزینهٔ کم، نامشخص و مبهم بودن، گمنامی، دشواری اثبات مرتکب و غیره است که این ویژگی‌ها سبب افزایش تمایل دولت‌ها نسبت به استفاده از عملیات سایبری خصمانه علیه دولت‌های دیگر شده است.

حق بهره‌مندی از پیشرفت‌های علمی، از جمله فناوری‌های نوین، همواره یکی از حقوق اساسی بشر قلمداد شده است. امروزه فناوری به ابزاری بسیار مفید برای شناسایی نقص‌ها در یک صنعت خاص و همچنین رفع سریع و کارامد مشکلات تبدیل شده است. این فناوری که به‌سرعت در حال پیشرفت است، به‌ویژه در حوزهٔ بهداشت و درمان اهمیت زیادی دارد (Nandy & Dubey, 2024: 322). با این حال، همان‌طور که تلالنگ موفوکنگ[1]، گزارشگر ویژهٔ شورای حقوق بشر در مورد حق همهٔ افراد برای برخورداری از بالاترین استاندارد قابل دستیابی سلامتی جسمی و روانی[2]، با ارائهٔ گزارش خود در مورد نوآوری دیجیتال، فناوری‌ها و حق سلامتی در ۲۲ ژوئن ۲۰۲۳ بیان می‌دارد: «نوآوری دیجیتال حق سلامتی را برای برخی تقویت کرده است، اما می‌تواند سبب نقض و تضعیف این حق شود» (OHCHR, 2023)[3]. برای مثال، سوگیری‌های موجود در هوش مصنوعی، نه‌تنها به ناکارامدی در صنعت، مانند تولید منجر می‌شود، همچنین می‌تواند عواقب خطرناکی در بخش مراقبت‌های بهداشتی داشته باشد (صلح‌چی و همکاران، ۱۴۰۳: ۳). علاوه بر این، پیشرفت‌هایی در تدابیر امنیت سایبری هنوز ضروری است. بر اساس گزارشی از شرکت بین‌المللی ماشین‌های تجاری[4] و مؤسسه پونه‌مون[5] در سال ۲۰۱۶، فراوانی نقض داده‌ها

1. Tlaleng Mofokeng
2. Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.
3. OHCHR. (2023). Special Rapporteur on the Right to Health Says Digital Innovation Has Strengthened the Right to Health for Some, but Warns it Could Enable Violations and Undermine this Right. *OHCR*. Retrieved November 5, 2023 from https://www.ohchr.org/en/news/2023/06/special-rapporteur-right-health-says-digital-innovation-has-strengthened-right-health.
4. International Business Machines (IBM)
5. Ponemon Institute

در صنعت بهداشت و درمان از سال ۲۰۱۰ به‌طور مداوم در حال افزایش بوده و اکنون این صنعت یکی از بخش‌های هدف حملات سایبری در سطح جهانی است (Argaw *et al*., 2020: 1).

امروزه متأسفانه زیرساخت‌های مراقبت‌های بهداشتی به‌عنوان یکی از زیرساخت‌های حیاتی کشورها مورد آماج حملات سایبری قرار می‌گیرند.[1] گروه بین‌المللی کارشناسان راهنمای تالین ۲ تأکید کرد که به‌نظر می‌رسد دولت‌ها به‌طور فزاینده‌ای نگران عملیات سایبری هستند که به خسارت اقتصادی شدید یا تأثیر بر زیرساخت‌های حیاتی منجر می‌شود (Tallinn Manual 2.0, 2017: 25). حملات سایبری به زیرساخت‌های مراقبت‌های بهداشتی، تهدیدی جهانی است که نمی‌توان آن را نادیده گرفت؛ افزایش نگران‌کنندهٔ حملات باج‌افزاری[2]، زیرساخت‌های مراقبت‌های بهداشتی جهان را در معرض خطر جدی قرار داده، ایمنی بیماران را به خطر انداخته و سیستم‌های بهداشتی را متزلزل کرده است. برای نمونه حملهٔ باج‌افزاری نوعی حملهٔ سایبری است که در آن هکرها نرم‌افزار مخربی (بدافزار) را به‌کار می‌گیرند که داده‌های یک بیمارستان یا ارائه‌دهندهٔ خدمات سلامت را رمزگذاری کرده و آنها را غیرقابل دسترسی می‌سازد. مهاجمان سپس در ازای رمزگشایی داده‌ها، درخواست باج می‌کنند که به‌طور معمول به‌صورت ارز دیجیتال پرداخت می‌شود. در صورت عدم پرداخت باج، مجرمان سایبری ممکن است داده‌ها را به‌طور

---

۱. مؤسسات بهداشت و درمان با افزایش نگران‌کنندهٔ تهدیدهای سایبری روبه‌رو هستند، به‌طوری‌که مهاجمان با روش‌های پیچیده‌تر درصدد سوءاستفاده از ضعف‌های سامانه‌ها هستند. برخی از رایج‌ترین تهدیدهای سایبری در بخش بهداشت و درمان عبارت‌اند از:

- حملات باج‌افزاری: هکرها داده‌های بیمارستانی را رمزگذاری کرده و برای رمزگشایی آن درخواست باج می‌کنند، که اغلب خدمات حیاتی سلامتی را فلج می‌کند؛
- نشت داده‌ها و سرقت هویت بیماران: پرونده‌های پزشکی به سرقت‌رفته در وب تاریک (dark web) به فروش می‌رسند و به تقلب مالی و نقض حریم خصوصی منجر می‌شوند؛
- حملات فیشینگ و مهندسی اجتماعی: مجرمان سایبری کارکنان حوزهٔ سلامتی را فریب می‌دهند تا اطلاعات ورود خود را فاش کنند و از این طریق به داده‌های محرمانه دسترسی غیرمجاز پیدا می‌کنند؛
- هک تجهیزات پزشکی: دستگاه‌های پزشکی متصل به اینترنت، مانند ضربان‌سازها و پمپ‌های انسولین، در معرض خطر نفوذ قرار دارند و تهدیدی برای جان بیماران به‌شمار می‌آیند؛
- تهدیدهای داخلی: کارکنان یا فروشندگان ثالث که به سامانه‌های پزشکی دسترسی دارند، ممکن است به‌صورت عمدی یا سهوی اطلاعات حساس را افشا کنند.

بنابراین، این تهدیدها نه‌تنها ایمنی بیماران و تمامیت نهادهای بهداشت و درمان را به خطر می‌اندازند، بلکه هزینه‌های مالی سنگینی نیز به سازمان‌های بهداشت و درمان تحمیل می‌کنند؛ از جمله جریمه‌های نظارتی، اقدامات حقوقی و آسیب به اعتبار آنها (Kulkarni, 2025: 30).

2. Ransomware Attacks

دائمی حذف کرده یا پرونده‌های حساس بیماران را به‌صورت آنلاین منتشر کنند (Kulkarni, 2025: 31). در این زمینه تدروس آدهانوم گبریسوس[1]، مدیر کل سازمان جهانی سلامت[2]، در جریان جلسه‌ای که در شورای امنیت سازمان ملل متحد برای بررسی راهبردهای مقابله با این تهدید فزاینده برگزار شد، این هشدار را اعلام کرد، بر لزوم مقابلهٔ فوری با این بحران تأکید کرد و خواستار اقدام جهانی هماهنگ برای محافظت از سیستم‌های بهداشتی در برابر تأثیرات مخرب و بالقوه تهدیدآمیز این حملات سایبری شد (The United Nations Office at Geneva, 2024)[3]. او هشدار داد که هکرها از «تهدید علیه ایمنی بیماران، محرمانگی و اختلال در خدمات» برای افزایش درخواست‌های باج‌گیرانهٔ خود سوءاستفاده می‌کنند و تحقیقات نشان داده که حملات به بخش‌های بهداشتی از نظر مقیاس و تکرار افزایش یافته‌اند و این، به‌دلیل «موفقیت هکرها در حمله به بیمارستان‌ها یا مراکز بهداشتی» است (Aydogan, 2024)[4]. برای نمونه، قطع خدمات تلفن در یک بیمارستان از طریق حملات سایبری می‌تواند بر نحوهٔ هشدار دادن به کارکنان در مواقع اضطراری، چگونگی تدوین و اجرای برنامه‌های درمانی توسط تیم‌های بالینی و همچنین نحوهٔ ارتباط آنها با خانواده‌های بیماران برای تصمیم‌گیری‌های مهم تأثیر بگذارد. از این‌رو در بسیاری از نقاط جهان که خدمات اورژانس پیش بیمارستانی در دسترس است و کمک از طریق تلفن درخواست می‌شود؛ قطع چنین خدماتی ممکن است دسترسی عمومی به مراقبت را به تأخیر بیندازد. برای مثال در سال ۲۰۱۸، هنگامی‌که سنتری‌لینک[5]، خدماتی به چندین مرکز تماس اضطراری در ایالات متحده ارائه می‌داد، با قطعی مواجه شد. این موضوع بر خدمات اضطراری در یک منطقهٔ جغرافیایی وسیع تأثیر گذاشت و عموم مردم نتوانستند با سیستم اضطراری ۹۱۱ تماس بگیرند تا درخواست کمک کنند (Cimpanu, 2018)[6]. بنابراین، استفاده از فناوری‌های دائر بر اینترنت در برخی از سیستم‌های تماس اضطراری ممکن است پاسخگویی را بهبود بخشد، اما همچنین آسیب‌پذیری جدیدی به شکل حملهٔ سایبری ایجاد کند.

---

1. Tedros Adhanom Ghebreyesus
2. World Health Organization (WHO)
3. The United Nations Office at Geneva. (2024). Cyberattacks on healthcare: A global threat that can't be ignored. *UNGENEVA*. Retrieved November 10, 2024 from https://www.ungeneva.org/en/news-media/news/2024/11/100103/cyberattacks-healthcare-global-threat-cant-be-ignored
4. Aydogan, M. (2024). Ransomware attacks on hospitals are 'issues of life and death,' warns WHO chief. *Anadolu Ajansi*. Retrieved November 10, 2024 from https://www.aa.com.tr/en/world/ransomware-attacks-on-hospitals-are-issues-of-life-and-death-warns-who-chief/3388792
5. CenturyLink
6. Cimpanu, C. (2018). CenturyLink outage takes down several 911 emergency services across the US. *ZDNET*. Retrieved November 12, 2024 from https://www.zdnet.com/article/centurylink-outage-takes-down-several-911-emergency-services-across-the-us/

از این‌رو، از آنجا که استفاده از پدیده‌های نوظهور به‌طور معمول با استقبال کل جامعهٔ بین‌المللی همراه می‌شود، نباید از این نکته غافل شویم که حقوق بین‌الملل به‌عنوان اصول و قواعد حاکم بر جامعهٔ بین‌المللی بر همهٔ اموری که در جامعهٔ بین‌المللی در حال وقوع است حکومت می‌کند (شهبازی و آقاجانی‌رونقی، ۱۳۹۹: ۱۴۸۸). در ادامه چارچوب حقوقی حملات سایبری به زیرساخت‌های بهداشت و درمان در دو قالب زمان صلح و زمان مخاصمات مسلحانه به‌تفکیک به بررسی پرداخته شده است.

۲. حملات سایبری

رشد فناوری‌های مخرب، مانند اینترنت اشیا[1] و بیش از ۵۰ میلیارد دستگاه متصل به اینترنت تا سال ۲۰۲۰، به این معناست که جهان با خطر فزاینده‌ای از حملات سایبری مواجه است (Lis & Mendel, 2019: 25-26). در برآوردهای جدیدتر، در سال ۲۰۲۳، تعداد دستگاه‌های اینترنت اشیا ۱۶/۶ میلیارد بود که نسبت به سال ۲۰۲۲ رشد ۱۵ درصدی داشته است. تعداد این دستگاه‌ها در سال ۲۰۲۵ در یک نگاه کلی برآورد می‌شود به ۱۸/۸ میلیارد برسد که انتظار می‌رود تا سال ۲۰۳۰ استفاده از دستگاه‌های اینترنت اشیا به ۴۰ میلیارد افزایش یابد؛ چراکه امروزه دوسوم از کل دستگاه‌های جهان دارای قابلیت اتصال به اینترنت اشیا هستند (Kumar, 2024)[2].

با این حال، در مورد تعریف حملات سایبری هیچ‌گونه اتفاق‌نظری وجود ندارد و این موضوع همچنان بین دولت‌ها و سازمان‌های بین‌المللی مورد اختلاف است (اصلانی و رنجبریان، ۱۳۹۴: ۲۷۵). با وجود این، تعریف‌هایی از آن صورت گرفته است؛ در قاعدهٔ ۹۲ راهنمای تالین ۲ این حملات بدین‌گونه تعریف شده است: «حملهٔ سایبری، عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول انتظار مرگ یا صدمه به اشخاص و یا وارد کردن خسارت به اشیا می‌رود» (Tallinn Manual 2.0, 2017: 415). علاوه بر این، خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی نیز در عرصهٔ فضای سایبر بسیار مشهود است. به استثنای کنوانسیون سال ۲۰۰۱ بوداپست موضوع جرایم سایبری که در چارچوب «شورای اروپا»[3] منعقد شد[4] و پروتکل الحاقی به آن[5] که صرفاً به جرایم افراد مربوط می‌شود، سند بین‌المللی مهم

---

1. Internet of Things (IoT)
2. Kumar, N. (2024). How Many IoT Devices Are There (2025-2030 Data). Demandsage. Retrieved May 20, 2025 from https://www.demandsage.com/number-of-iot-devices/
3. The Council of Europe
4. Convention on Cybercrime (Budapest Convention), Council of Europe, 23 November 2001, European Treaty Series – No. 185., Entered into Force on 1 July 2004.
۵. این پروتکل در خصوص «لزوم جرم‌انگاری اقدام‌های نژادپرستانه و بیگانه هراسی که با استفاده از رایانه ارتکاب می‌یابند» است.
Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature

دیگری در حوزهٔ حملات سایبری موجود نیست و شاید تنها بتوان به راهنماهای تالین اشاره کرد که در سال ۲۰۱۳[1] و ۲۰۱۷[2] توسط جمعی از کارشناسان بین‌المللی در چارچوب سازمان ناتو تهیه شده‌اند (بیگلربیگی، ۱۴۰۲: ۲). البته باید خاطرنشان کرد که فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به حملات سایبری کنند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت در خصوص حملات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیهٔ اروپا و دولت‌های متعدد، از جمله ایالات متحدهٔ آمریکا، ایران، بریتانیا، روسیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالی این نظریه را پذیرفته‌اند (Roscini, 2014: 19-22). همچنین بدیهی است در رویهٔ دولت‌ها، زمینهٔ فعالیت‌ها و اقدام‌های سایبری به‌طور عمده طبقه‌بندی شده، اظهارات معطوف به باور حقوقی[3] کمیاب‌اند؛ لیکن این کمبود بدان معنا نیست که عملیات سایبری در خلأ هنجاری قرار دارد. در مذاکره‌های تالین ۲ (۲۰۱۷)، وظیفهٔ گروه بین‌المللی کارشناسان منتخب، تعیین چگونگی اعمال چنین حقوقی در بافت فضای سایبر و شناسایی ابعاد منحصر به فضای آن بود. قواعد مطروح در این خصوص، بازتاب حقوق بین‌الملل عرفی اعمالی در فضای سایبر است و قواعد مزبور مادامی که به‌درستی مبین حقوق بین‌الملل عرفی باشند، تمامی دولت‌ها را ملتزم می‌سازند (محقق‌هرچقان و همکاران، ۱۴۰۲: ۱۵۴۰). از این‌رو در خصوص حملات سایبری نظریهٔ غالب در سطح بین‌المللی بر این است که حقوق بین‌الملل برای در برگرفتن حملات سایبری کافی است. این دیدگاه در بعضی مقاله‌ها و اسناد بین‌المللی همانند راهنمای تالین نیز منعکس شده و حاکی از این است که اصول عام بین‌المللی می‌بایستی در خصوص حملات سایبری اعمال شوند (Valo, 2014: 7). در اینجا با همین رویکرد، چارچوب حقوقی حملات سایبری به زیرساخت‌های بهداشتی بررسی می‌شود.

Committed through Computer System, 2003.

۱. از ترکیب ۲۳ نفری این کارشناسان، نه نفر از ایالات متحدهٔ آمریکا بودند و کشورهای دارای قابلیت‌های سایبری یا کشورهای قربانی حملات سایبری مانند روسیه، ایران و چین نماینده‌ای در این مجموعه نداشتند که این امر انتقادات شدیدی را برانگیخت (Liivoja & McCormack, 2013: 4-12).

۲. راهنمای تالین در حقوق بین‌الملل قابل اعمال در نبردهای سایبری متعلق به بازهٔ زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در استونی است که توسط مایکل اشمیت در مورد مقررات حاکم بر اقدام‌ها و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبرد ناتو در ولز بریتانی، در قالب اصل ۴ پیمان ناتو، تهیه شده است.

3. Opinio Juris Sive Neccessitatis

۳. زیرساخت‌های حیاتی

زیرساخت‌های حیاتی[1] اصطلاحی جهانی است که برای توصیف دارایی‌ها و تأسیسات ضروری برای عملکرد یک جامعه استفاده می‌شود (Taubman *et al*., 2023: 660). راهنمای تالین ۲ زیرساخت‌های حیاتی را این‌گونه تعریف می‌کند: «سیستم‌ها و دارایی‌های فیزیکی یا مجازی یک دولت که به‌قدری حیاتی هستند که ناتوانی یا تخریب آنها ممکن است به امنیت، اقتصاد، بهداشت عمومی یا ایمنی دولت، یا محیط زیست آسیب جدی وارد کند» (Tallinn Manual 2.0, 2017: 564). برای نمونه می‌توان به بمب‌گذاری در تأسیسات شرکت تلفن و تلگراف آمریکا[2] در نشویل، مرکز ایالت تنسی (ایالات متحدهٔ آمریکا)[3]، در سال ۲۰۲۰ اشاره کرد. قطع ارتباطات تلفن همراه سبب اختلال در خدمات پزشکی اضطراری، پاسخ پلیس و آتش‌نشانی شد، زیرا سیستم تماس اضطراری ۹۱۱ از کار افتاد و همچنین عملکرد سوابق پزشکی الکترونیکی[4] در چندین بیمارستان مختل شد که این امر به خدمات بهداشتی آسیب بیشتری رساند (Rojas *et al*., 2020)[5]. از این‌رو یکی از مفاهیم مهم در حوزهٔ حکمرانی مطلوب[6]، توجه به زیرساخت‌های حیاتی است، از این‌رو کشورها بر اساس سیاست‌های کلان خود اقدام به ترسیم و تعریف زیرساخت‌های حیاتی خود می‌کنند.

قطعنامهٔ ۲۳۴۱ (۲۰۱۷) شورای امنیت به‌صراحت در مقدمهٔ خود به رسمیت می‌شناسد که «هر کشور تعیین می‌کند که چه چیزی زیرساخت حیاتی آن را تشکیل می‌دهد».[7] با این حال، این قطعنامه معیارهای خاصی را که کشورهای عضو باید برای انتخاب دارایی‌ها و فرایندهای خاص از میان بی‌شمار موارد موجود در قلمرو خود استفاده کنند، مشخص نمی‌کند. همچنین هیچ راهنمایی در این زمینه توسط سایر اسناد بین‌المللی ارائه نشده است. از این‌رو دولت‌ها از اختیار شایان توجهی در انتخاب معیارهای شناسایی زیرساخت‌هایی که در قلمرو آنها فعالیت می‌کنند و آستانهٔ «حیاتی بودن»[8] را برآورده می‌کنند، برخوردارند. این وظیفه ساده نیست: مشخص کردن زیرساخت‌هایی که باید وضعیت «حیاتی» به خود بگیرند، برای اولویت‌بندی منابع محدود برای حفاظت از دارایی‌ها، سیستم‌ها و فرایندهای متعدد کلیدی است. از یک سو، گنجاندن تعداد زیادی از اشیا در دستهٔ «حیاتی» ممکن است غیرقابل مدیریت شود (علاوه بر اینکه از نظر مالی پایدار نیست)، از سوی دیگر،

---

1. Critical infrastructure (CI)
2. American Telephone and Telegraph (AT&T)
3. Nashville, Tennessee (USA)
4. Electronic Medical Records (EMRs)
5. Rojas, R.; McGee, J.; Lee. E.; & Cavendish, S. (2020). When Nashville Bombing Hit a Telecom Hub, the Ripples Reached Far Beyond. ***New York Times***. Retrieved June 5, 2023 from https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html
6. Good Governance
7. Adopted by the Security Council at its 7882nd meeting on 13 February 2017
8. Critical

رویکرد بیش‌ازحد محدودکننده، خطر بی‌حفاظ ماندن تعدادی از دارایی‌ها و فرایندهای کلیدی را به‌همراه دارد که در صورت وقوع حادثه می‌تواند پیامدهای فاجعه‌باری داشته باشد. از این‌رو دولت‌ها تمایل دارند فهرست‌های ملی زیرساخت‌های حیاتی خود را گسترش دهند نه اینکه آنها را محدود کنند (United nations office of Counter-Terrorism *et al*., 2022: 21). این امر به این دلیل رخ می‌دهد که همان‌طور که بخش امنیت بین‌الملل چتم‌هاوس[1] بریتانیا اشاره کرده است، «تعداد بسیار کمی از تصمیم‌گیرندگان مایل به پذیرش ریسک سیاسی احتمالی ناشی از حذف یک مورد از فهرست «حیاتی» هستند و وسوسه این است که دایرهٔ مواردی را که حیاتی تلقی می‌شوند مدام گسترش دهند» (Clemente, 2013: ix).

بنابراین، دولت‌ها با صلاحدید خود در انتخاب معیارها برای شناسایی زیرساخت‌های فعال در قلمرو آنها، آستانهٔ «حیاتی» را مشخص می‌کنند. بر همین اساس، دولت‌ها زیرساخت‌های بهداشتی را اغلب بر اساس اهمیتی که برای جان انسان، حق حیات، حق بر سلامتی و حق بر برابری و عدم تبعیض در حوزهٔ سلامتی قائل‌اند و به‌عنوان منافع اساسی آنها تلقی می‌شود، به‌منزلهٔ زیرساخت‌های حیاتی تلقی می‌کنند.

۴. حملات سایبری در زمان صلح

حقوق بشر ناظر بر احترام به انسان، هم به‌عنوان یک فرد و هم به‌عنوان عضوی از گونهٔ انسانی بوده و تضمین‌کنندهٔ کرامت انسانی است (Council of Europe, n.d)[2]. از این‌رو حقوق بشر، حقوقی‌اند که صرفاً به‌دلیل انسان بودن از آن برخورداریم؛ این حقوق توسط هیچ دولتی اعطا نمی‌شوند. این حقوق جهانی، ذاتی همهٔ ما، فارغ از ملیت، جنسیت، منشأ ملی یا قومی، رنگ، دین، زبان یا هر وضعیت دیگری هستند. این حقوق از اساسی‌ترین آنها — مانند حق حیات — تا حقوقی را شامل می‌شوند که زندگی را معنادار می‌کنند، از جمله حق برخورداری از غذا، آموزش، کار، سلامت و آزادی (OHCHR, n.d)[3]. همچنین شایان اشاره است حقوق بشر بر خلاف حقوق بشردوستانه که فقط در مخاصمات مسلحانه قابل اجراست، در تمامی شرایط قابل اجراست. با این حال، تمام مفاد آن به‌جز مقررات غیرقابل تعلیق، ممکن است در شرایط خاصی در موقعیت‌هایی که زندگی ملت را تهدید می‌کنند، به حالت تعلیق درآیند. از آنجا که این موقعیت‌ها فقط شامل مخاصمات مسلحانه نمی‌شوند، مکمل بودن این دو نظام حقوقی کامل نیست؛ به‌ویژه در وضعیت‌های ناآرامی‌ها و تنش‌های داخلی، یک خلأ (حقوقی) وجود دارد (ICRC, n.d)[4].

---

1. Chathamhouse
2. Council of Europe. (n.d). What are human rights?. *Council of Europe*. Retrieved June 6, 2025 from https://www.coe.int/en/web/portal/what-are-human-rights
3. OHCHR. (n.d). What are human rights?. *United Nations*. Retrieved June 6, 2025 from https://www.ohchr.org/en/what-are-human-rights#:~:text=Human%20rights%20are%20rights%20we,of%20international%20human%20rights%20law
4. Retrieved May 20, 2025 *casebook.icrc*. ICRC. (n.d). Human Rights applicable in armed conflicts. 4

در این زمینه گروه بین‌المللی کارشناسان راهنمای تالین ۲ توافق کردند که هم حقوق بشر معاهداتی و هم حقوق بشر بین‌المللی عرفی به فعالیت‌های مرتبط با سایبر اعمال می‌شود، اما هشدار دادند که اغلب مشخص نیست که آیا برخی از حقوق بشر منعکس‌شده در حقوق معاهداتی به‌عنوان قواعد حقوق عرفی شکل گرفته‌اند یا نه. علاوه بر این، جنبه‌هایی از حقوق بشر معاهداتی بین‌المللی ممکن است در تفسیر آنها توسط دولت‌ها و نهادهای منطقه‌ای در ارتباط با فعالیت‌های سایبری متغیر باشد. کارشناسان همچنین خاطرنشان کردند که دولت‌ها ممکن است در شرایط خاص (قاعدهٔ ۳۷ راهنمای تالین ۲) حق محدود کردن اجرای برخی از حقوق را طبق حقوق بشر بین‌المللی داشته باشند. با این حال، به‌طور گسترده‌ای پذیرفته شده است که بسیاری از حقوق بشر بین‌المللی که افراد در دنیای «آفلاین» از آن بهره‌مندند، همچنین در دنیای «آنلاین» نیز تحت حمایت قرار دارند (Tallinn Manual 2.0, 2017: 179).

ادغام فزایندهٔ فناوری‌های دیجیتال در حوزهٔ سلامتی، انقلابی در مراقبت از بیماران، مدیریت داده‌ها و تحقیقات پزشکی ایجاد کرده است. با این حال، این پیشرفت فناورانه، سامانه‌های بهداشت و درمان را در معرض تهدیدهای فزایندهٔ امنیت سایبری قرار داده است. جرم سایبری[1] در حوزهٔ سلامتی به هرگونه فعالیت مجرمانه‌ای اطلاق می‌شود که شامل دسترسی غیرمجاز، سرقت یا دستکاری داده‌های بهداشتی و زیرساخت‌های فناوری اطلاعات می‌شود. مجرمان سایبری با بهره‌برداری از آسیب‌پذیری‌های موجود در شبکه‌های بیمارستانی، پایگاه‌های دادهٔ پزشکی و سامانه‌های پزشکی از راه دور، اغلب از تکنیک‌های پیشرفته‌ای مانند حملات باج‌افزاری، کلاه‌برداری‌های فیشینگ و تهدیدهای داخلی استفاده می‌کنند. حمله به خدمات سلامت همگانی[2] در سال ۲۰۲۰ یکی از حملات سایبری مهم بود که بیش از ۴۰۰ مرکز درمانی در ایالات متحدهٔ آمریکا را مختل کرد. این رویداد آسیب‌پذیری سامانه‌های سلامت در برابر جرائم سایبری را برجسته ساخت و بر ضرورت فوری تقویت پروتکل‌های امنیت سایبری و راهبردهای پاسخ به حوادث برای حفاظت از مراقبت‌های درمانی و داده‌های حساس بیماران تأکید کرد (Kulkarni, 2025: 30-31). از این‌رو افزایش وابستگی به سیستم‌های متصل، داده‌های حساس بیمار را در معرض حملات سایبری قرار می‌دهد که ممکن است حریم خصوصی بیماران، ثبات مالی و حتی کیفیت خدمات درمانی را به خطر بیندازد (Burke *et al*., 2024: 4). در نتیجه با توجه به روندهای نوظهور امنیت سایبری، حملات سایبری ممکن است در هر پیوند شبکه[3] و هر نقطهٔ انتهایی رخ دهند. قابلیت همکاری برنامه‌ها، پلتفرم‌های عملیاتی، رابط‌های دستگاه‌های پزشکی و شبکه‌های اشتراک‌گذاری اطلاعات برای مدیریت ریسک‌های امنیت سایبری در یک سیستم بهداشتی دیجیتال حیاتی است. جریان‌های سایبر-

from https://casebook.icrc.org/a_to_z/glossary/human-rights-applicable-armed-conflicts

1. Cybercrime
2. Universal Health Services (UHS)
3. Network Link

فیزیکی پزشکی[1]، شبکه‌های بی‌سیم و معرفی برنامه‌های پزشکی در مراقبت‌های بهداشتی، همگی سطوح و بردارهای حمله را به طرز چشمگیری گسترش داده‌اند و اکنون تأمین امنیت هر نقطهٔ ورودی به سیستم بهداشت و درمان دشوار شده است (Adebukola *et al*., 2022: 34). از این‌رو، حملات سایبری به زیرساخت‌های بهداشت و درمان در زمان صلح، با حقوق متعددی در تعارض قرار می‌گیرد. با این حال، در این مقاله با توجه به موضوع و متناسب با چارچوب بحث، تمرکز بر سه حق بنیادین یعنی حق حیات، حق بر سلامتی و حق بر برابری و عدم تبعیض در حوزهٔ سلامتی معطوف شده است. شایان ذکر است که این حقوق در دوران مخاصمات مسلحانه نیز قابل نقض‌اند، چراکه حقوق بشر در هر شرایطی، از جمله در زمان مخاصمات، همچنان جاری و لازم‌الاجراست.

۴. ۱. حق حیات

ترجمان حقوق بشری ارزش حیات، عبارت «حق حیات» است (قاری سیدفاطمی، ۱۳۹۹: ۳۰). از نظر

1. Medical cyber-physical streams

این حوزه شامل اینترنت پزشکی اشیا (MIoT) می‌شود که هم دستگاه‌های پزشکی قابل کاشت (implantable) و هم پوشیدنی (wearable) را در برمی‌گیرد. سامانه‌های سایبر–فیزیکی پزشکی (MCPS) به‌طور فزاینده‌ای در بیمارستان‌ها برای ارائهٔ مراقبت‌های باکیفیت به‌کار می‌روند و به‌عنوان ابزارهای نویدبخشی برای پایش و مدیریت جنبه‌های مختلف سلامت بیماران پدیدار شده‌اند. پیش‌بینی می‌شود تا سال ۲۰۲۸، تعداد دستگاه‌های متصل به ۵۰ میلیارد برسد. تهدیدهای ذاتی امنیتی سامانه‌های سایبر–فیزیکی پزشکی به‌واسطهٔ ویژگی‌های خاص این سامانه‌ها افزایش یافته است. این ویژگی‌ها سامانه‌های سایبر–فیزیکی پزشکی را متنوع، سیار، ناهمگون و روزافزون می‌سازد. آنها اغلب بدون نظارت رها می‌شوند (مانند دستگاه‌های قابل کاشت) تا داده‌های فیزیولوژیکی شخصی را ثبت کنند و از نظر اندازه، توان و حافظه محدودند که تنها امکان اجرای قابلیت‌های امنیتی پایه را فراهم می‌سازد. همچنین به‌دلیل نزدیکی و وابستگی آنها به شبکهٔ سلامت، ویژگی‌های سامانه‌های سایبر–فیزیکی پزشکی آنها را در برابر نفوذ آسیب‌پذیر کرده و ریسک بزرگی را برای کل سامانه سلامت از نظر امنیت سایبری به‌وجود می‌آورد. سامانه‌های سایبر–فیزیکی پزشکی به بردار حملهٔ بالقوه مهمی برای بازیگران مخرب تبدیل شده تا به سامانه‌ها نفوذ کنند، بدافزار نصب کنند و روند ارائهٔ خدمات درمانی را تغییر دهند. تدابیر امنیت سایبری نظیر اسکن آسیب‌پذیری و مدیریت وصله‌ها اغلب در دسترس نیست یا به تولیدکنندگان محدود می‌شود. در سطح جهانی، ابهاماتی در خصوص مالکیت پس از فروش، به‌روزرسانی‌های نرم‌افزاری و مقررات امنیتی سامانه‌های سایبر–فیزیکی پزشکی وجود دارد. از آنجا که این اطلاعات محرمانه تلقی می‌شود، تولیدکنندگان ممکن است از ارائهٔ مستنداتی دربارهٔ آسیب‌پذیری‌های امنیت سایبری سامانه یا سیاست‌های وصله‌زنی و ارتقا خودداری کنند. بنابراین، در غیاب استانداردهای سلامت برای تسهیل قابلیت همکاری سامانه‌های سایبر–فیزیکی پزشکی، ناسازگاری بین سامانه‌های مختلف سلامت و دستگاه‌های پزشکی افزایش می‌یابد و بخشی از بازار تجهیزات پزشکی شکل می‌گیرد که دستگاه‌های بیماران را با شتاب به بازار عرضه می‌کند پیش از آنکه دغدغه‌های امنیت سایبری مرتفع شده باشند (Adebukola *et al.*, 2022: 34-35).

کمیتهٔ حقوق بشر، حق حیات، حق اساسی و بالایی است که حتی در شرایط اضطرار غیرقابل تعلیق است. کمیته همچنین مقرر می‌دارد که حق حیات، اساس تمام حقوق بشر است. حق حیات به‌منزلهٔ بارزترین حق، خاستگاه حقوق و حق غیرقابل تجویز، از بالاترین درجهٔ اهمیت برخوردار است و به‌عنوان هستهٔ مرکزی حقوق بشر و هنجار ضروری حقوق بین‌الملل تلقی شده است (Human Rights Committee, 1984: Para 1). از این‌رو حق حیات بنیادی‌ترین حق انسانی است و دیگر حق‌های پیش‌بینی‌شده در اسناد بین‌المللی حقوق بشر متوقف بر حق حیات است. اهمیت این حق تا به آنجاست که حتی در شرایط اضطراری نیز نمی‌توان آن را نادیده گرفت. در حقیقت به تصریح بخش دوم مادهٔ ۴ میثاق بین‌المللی حقوق مدنی و سیاسی حتی در موارد اضطراری کشورها نمی‌توانند به بهانهٔ اینکه حیات و بقای ملت در معرض تهدید است، حق حیات افراد را نقض کند و مادهٔ ۶ میثاق به‌تفصیل بیشتری از حق حیات سخن می‌گوید (قاری سیدفاطمی، ۱۳۹۹: ۳۸). همچنین در مادهٔ ۳ اعلامیهٔ جهانی حقوق بشر مقرر شده است: «هر کس حق زندگی، آزادی و امنیت ملی دارد» و در اسناد منطقه‌ای نیز از قبیل مادهٔ ۲ کنوانسیون اروپایی حقوق بشر به این حق تصریح شده است.

۴. ۲. حق بر سلامتی

حق بر سلامتی، یکی از حقوق بنیادین بشری است که از سوی نظام حقوق بین‌الملل به رسمیت شناخته شده و از جایگاه ویژه‌ای برخوردار است. نخستین و کلی‌ترین اشاره‌ای که به این حق شده است، در مادهٔ ۵۵ منشور ملل متحد است که بر اساس «بند ب» این ماده، دولت‌ها متعهد به ترویج راه‌حل‌هایی برای برون‌رفت از مشکلات مربوط به سلامتی هستند. پس از منشور ملل متحد، سند دیگری که به بازتاب سلامتی به‌عنوان حقی بشری پرداخته، اساسنامهٔ سازمان جهانی سلامت است که در مقدمهٔ خود بیان کرد: «سلامتی عبارت از برخورداری از آسایش کامل جسمی، روانی و اجتماعی و نه‌فقط نداشتن بیماری و نقص عضو است» و هدف سازمان را ارتقای سطح سلامتی همهٔ فرزندان بشر تا بالاترین حد ممکن اعلام کرد. یکی دیگر از اسنادی که به سلامتی به‌عنوان حقی بشری پرداخته، مادهٔ ۲۵ اعلامیهٔ جهانی حقوق بشر است که بیان می‌دارد: «هر کس حق دارد سطح زندگانی، سلامتی و رفاه خود و خانواده‌اش را از حیث خوراک و مسکن و مراقبت‌های پزشکی و خدمات الزام اجتماعی تأمین کند و همچنین حق دارد در مواقع بیکاری، بیماری، نقص عضو، بیوگی، پیری یا در تمام موارد دیگری که به علل خارج از اراده انسان وسایل امرار معاش از دست‌رفته باشد از شرایط آبرومندانه زندگی برخوردار شود». البته باید اشاره داشت، برخی از مفاد اعلامیهٔ جهانی حقوق بشر که در سال ۱۹۴۸ توسط مجمع عمومی سازمان ملل متحد به تصویب رسید، امروزه به جایگاه حقوق بین‌الملل عرفی دست یافته است. مفاد اعلامیه در میثاق

بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی به‌تفصیل بیان شده است. شاید به‌جرأت بتوان گفت صریح‌ترین و کامل‌ترین بیان از حق بر سلامتی، مادهٔ ۱۲ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی است. میثاق، جامع‌ترین مفاد در مورد حق بر سلامتی را با مشخص کردن اقداماتی که باید توسط دولت‌ها انجام شود، از جمله کاهش میزان مرده‌زایی و مرگ‌ومیر نوزادان؛ بهبود بهداشت محیطی و صنعتی؛ پیشگیری، درمان و کنترل بیماری‌های همه‌گیر، بومی، شغلی و سایر بیماری‌ها؛ تضمین دسترسی به خدمات بهداشتی برای همه (مادهٔ ۱۲) بیان می‌دارد (صلح‌چی و دیگران، ۱۴۰۳: ۴-۵). بنابراین، انسان در هر نقطه از جهان حق برخورداری از حق بر سلامتی را دارد (Yustina, 2019: 191).

۴. ۳. حق بر برابری و عدم تبعیض در حوزهٔ سلامتی

دسترسی بدون تبعیض به خدمات بهداشتی و درمانی یکی از اصول اساسی حق بر سلامتی و اخلاق پزشکی است (Hartlev, 2013: 342). این حق به‌عنوان جنبه‌ای از حق بر سلامتی، در معاهدات بین‌المللی مختلف، برای مثال مقدمهٔ اساسنامهٔ سازمان جهانی سلامت ۱۹۴۸، میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی ۱۹۶۶، کنوانسیون بین‌المللی حمایت از حقوق همهٔ کارگران مهاجر و اعضای خانواده‌یشان در سال ۱۹۹۰ (Orzechowski *et al*., 2020: 2) و یا مادهٔ ۴۲ مقررات بین‌المللی سلامتی[1] بیان شده است. همچنین در آخرین گزارش شورای حقوق بشر در خصوص حق همهٔ افراد برای برخورداری از بالاترین استاندارد قابل دستیابی سلامتی جسمی و روانی در ۲۲ ژوئن ۲۰۲۳ نیز بیان شد: «نیاز به مراقبت‌های بدون تبعیض وجود دارد. فناوری‌ها به‌عنوان ابزاری برای ارائهٔ اطلاعات به زنان و دختران در مورد سلامتی جنسی و باروری عمل می‌کنند. خدمات دیجیتال باید بیشتر در اختیار گروه‌های آسیب‌پذیر مانند زنان، کودکان و مردم بومی قرار گیرد. دولت‌ها باید تلاش کنند تا اطمینان حاصل شود که شکاف دیجیتال به نابرابری بیشتر در سلامتی منجر نمی‌شود. رویکردی مبتنی بر برابری در مورد فناوری‌های سلامتی دیجیتال مورد نیاز است» (OHCHR, 2023)[2].

۴. ۴. تلاقی حملات سایبری با حق حیات، حق بر سلامتی و حق بر برابری و عدم تبعیض در حوزهٔ سلامتی

حملات سایبری علیه بخش بهداشت و درمان به‌ویژه نگران‌کننده‌اند، زیرا این حملات افزون بر تهدید امنیت سیستم‌ها و اطلاعات، سلامتی و ایمنی بیماران را نیز به خطر می‌اندازند. بیمارستان‌ها به‌طور خاص

---

۱. مادهٔ ۴۲ (اجرای تدابیر بهداشتی) بیان می‌دارد: «تدابیر بهداشتی که بر اساس این مقررات اتخاذ می‌شوند، باید بدون تأخیر آغاز و تکمیل شده و به شیوه‌ای شفاف و غیرتبعیض‌آمیز اجرا شوند».

2. OHCHR. (2023), *op.cit*

به حملات سایبری حساس‌اند، زیرا هرگونه اختلال در عملیات یا حتی افشای اطلاعات شخصی بیماران می‌تواند عواقب گسترده‌ای داشته باشد (Lehto, 2022: 26). در حدود ساعت ۱۱ صبح ۲۸ اکتبر ۲۰۲۰، شبکهٔ بهداشت دانشگاه ورمانت[1] به‌دلیل یک حملهٔ سایبری با چندین اختلال در سیستم‌های بالینی مواجه شد. در نتیجه، تمامی سوابق پزشکی الکترونیکی بیمارستان، آزمایشگاه، داروخانه، پاتولوژی، رادیولوژی و سیستم‌های تلفن و ایمیل بیمارستان غیرقابل دسترسی شدند (Nelson *et al*., 2022: 1). از سوی دیگر، مطابق گزارش‌ها بیش از ۱۱۰ میلیون بیمار در ایالات متحده در سال ۲۰۱۵ اطلاعاتشان به خطر افتاد. از میان ۲۲۳ سازمانی که در سال ۲۰۱۶ بررسی شدند، تنها نیمی از این ارائه‌دهندگان معتقدند که قادر به دفاع از خود در برابر حملات سایبری هستند و این امر سبب می‌شود که بخش بهداشت و درمان گزینه‌ای جذاب برای حمله‌کنندگان سایبری باشد (Martin *et al*., 2017)[2]. حمله‌کنندگان سایبری به‌دلیل چندین عامل، روی بخش بهداشت و درمان تمرکز کرده‌اند: این بخش منبعی غنی از داده‌های ارزشمند است و سازمان‌های بهداشتی فاقد یک چارچوب امنیت سایبری منظم، هدفمند و جامع هستند که توانمندی سایبری را ترویج دهد؛ یعنی توانایی یک سازمان برای تحمل تأثیرات، ادامهٔ عملیات و بازگشت به وضعیت اولیه (Chon *et al*., 2019: 539-540).

در این زمینه تدروس آدهانوم گبریسوس، مدیر کل سازمان جهانی سلامت، در توضیحات خود به نمایندگان کشورهای حاضر در جلسهٔ مورخ روز جمعه ۸ نوامبر ۲۰۲۴ (برابر با ۱۸ آبان ۱۴۰۳) شورای امنیت سازمان ملل متحد که برای بررسی راهبردهای مقابله با تهدید فزایندهٔ حملات سایبری به زیرساخت‌های بهداشتی تشکیل شده بود، به تأثیر شدید حملات سایبری بر بیمارستان‌ها و خدمات مراقبت‌های بهداشتی اشاره کرد و خواستار اقدام فوری و جمعی جهانی برای مقابله با این بحران فزاینده شد. او گفت: «حملات باج‌افزارها[3] و سایر حملات سایبری به بیمارستان‌ها و سایر مراکز بهداشتی تنها مسائل امنیتی و محرمانه نیستند؛ آنها می‌توانند به مقولهٔ مرگ و زندگی مربوط باشند ... در بهترین حالت، این حملات سبب اختلال و زیان مالی می‌شوند و در بدترین حالت، اعتماد به سیستم‌های بهداشتی را که مردم به آن وابسته‌اند، تضعیف می‌کنند و حتی موجب آسیب و مرگ بیماران می‌شوند». وی ادامه داد که

---

1. University of Vermont Health Network (UVMHN)
2. Martin, G.; Martin, P.; Hankin, C.; Darzi, A.; & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ*. Retrieved November 20, 2024 from https://www.bmj.com/content/358/bmj.j3179
۳. حملات باج‌افزاری نوعی حملهٔ سایبری است که در آن یک عامل مخرب فایل‌ها را در یک کامپیوتر یا کل شبکه هک و رمزگذاری کرده و برای رمزگشایی از آن داده‌ها، تقاضای پرداخت وجه می‌کند. این حملات با گذشت زمان در مقیاس و پیچیدگی رشد کرده‌اند، به‌طوری‌که اکنون هزینهٔ آنها به ده‌ها میلیارد دلار در هر سال می‌رسد.
Fortinet. "Types Of Cyber Attacks". (n.d). Retrieved May 20, 2025 from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

تحول دیجیتالی مراقبت‌های بهداشتی، همراه با ارزش بالای داده‌های سلامتی، این بخش را به هدف اصلی مجرمان سایبری تبدیل کرده است. او به مواردی مانند حملهٔ باج‌افزاری سال ۲۰۲۰ به بیمارستان دانشگاه برنو در چک[1] که بیمارستان را مجبور به خاموش کردن شبکه‌اش کرد و نقض امنیتی سرویس بهداشتی ایرلند[2] در مه ۲۰۲۱ اشاره کرد که خدمات پرتودرمانی را در پنج مرکز اصلی متوقف ساخت. حملات سایبری همچنین فراتر از بیمارستان‌ها، زنجیرهٔ تأمین زیست‌پزشکی[3] را مختل کرده‌اند. در طول همه‌گیری، آسیب‌پذیری‌هایی در شرکت‌های تولیدکنندهٔ واکسن‌های کووید-۱۹، فروشندگان نرم‌افزارهای آزمایش‌های بالینی و آزمایشگاه‌ها آشکار شد.[4] او واقعیت نگران‌کننده‌ای را برجسته کرد که حتی در صورت پرداخت باج، دسترسی به داده‌های رمزگذاری‌شده تضمین نمی‌شود و این مسئله مسیر مقاومت سیستم‌های بهداشتی در سطح جهانی را پیچیده‌تر می‌کند؛ چراکه بر اساس یک نظرسنجی جهانی در سال ۲۰۲۱، بیش از یک‌سوم از مؤسسات بهداشتی پاسخ‌دهنده، حداقل یک حملهٔ باج‌افزاری را در سال گذشته گزارش داده و یک‌سوم از آنها اعلام کرده‌اند که باج پرداخت کرده‌اند. با این حال، ۳۱ درصد از پاسخ‌دهندگان، دسترسی به داده‌های رمزگذاری‌شدهٔ خود را بازیابی نکردند (The United Nations Office at Geneva, 2024)[5].

همچنین بیانیه‌ای مشترک که توسط بیش از ۵۰ کشور – از جمله کرهٔ جنوبی، اوکراین، ژاپن، آرژانتین، فرانسه، آلمان و بریتانیا – امضا شده بود، هشداری مشابه داد. این بیانیه که توسط آنه نیوبرگر[6]، هماهنگ‌کنندهٔ سیاست امنیت ملی ایالات متحدهٔ آمریکا در زمینهٔ سایبر و فناوری‌های نوظهور، ارائه شد، بیان کرد: «این حملات تهدیدی مستقیم برای ایمنی عمومی بوده و جان انسان‌ها را با تأخیر در ارائهٔ خدمات بهداشتی حیاتی به خطر می‌اندازند، خسارت اقتصادی زیادی وارد می‌کنند و می‌توانند تهدیدی برای صلح و امنیت بین‌المللی باشند». این بیانیه همچنین کشورهایی را محکوم کرد که «آگاهانه»[7] به کسانی که مسئول حملات باج‌افزاری هستند اجازهٔ فعالیت از خاک خود را می‌دهند. برای نمونه ادواردو

1. Brno University Hospital in Czechia
2. Irish Health Service Executive (HSE)
3. Biomedical Supply Chain
۴. کلاه‌برداری واکسن کووید-۱۹ در سال ۲۰۲۱ یک جرم سایبری گسترده بود که با سوءاستفاده از همه‌گیری جهانی، کارکنان حوزهٔ سلامت و افراد عادی را هدف قرار داد. مجرمان سایبری با جعل هویت سازمان‌های معتبر، از جمله سازمان جهانی سلامت، اقدام به ارسال ایمیل‌های فیشینگ کردند که اطلاعات جعلی مربوط به واکسن یا دسترسی زودهنگام به واکسن‌ها را ارائه می‌دادند (Kulkarni, 2025: 32).
5. The United Nations Office at Geneva. (2024). *op.cit*
6. Anne Neuberger
7. Knowingly

کونرادو[1]، رئیس شرکت آسِنشن[2] – سومین سیستم بهداشتی بزرگ ایالات متحدهٔ آمریکا – مؤسسهٔ کاتولیک مذهبی است که سالانه به بیش از شش میلیون نفر مراقبت‌های بهداشتی غیرانتفاعی در ایالات متحدهٔ آمریکا ارائه می‌کند، بینش‌های دست اولی از واقعیت‌های تلخ حملات باج‌افزاری ارائه داد. او جزئیات حملهٔ سایبری مه ۲۰۲۴ به «آسِنشن» را تشریح کرد که به‌شدت عملیات را در ۱۲۰ بیمارستان آن مختل ساخت. این حمله، هزاران سیستم کامپیوتری را رمزگذاری کرد و دسترسی به پرونده‌های الکترونیک سلامتی را مختل ساخت و خدمات تشخیصی کلیدی از جمله تصویربرداری پرتو مغناطیسی[3] و سی‌تی‌اسکن[4] را تحت تأثیر قرار داد. آقای کونرادو چالش‌های عملی به‌وجودآمده را شرح داد: «پرستاران قادر نبودند از ایستگاه‌های کامپیوتری خود پروندهٔ بیماران را مشاهده کنند و مجبور بودند در پشتیبان‌های کاغذی جست‌وجو کنند ... تیم‌های تصویربرداری نمی‌توانستند به‌سرعت آخرین اسکن‌ها را به جراحانی که در اتاق عمل منتظر بودند ارسال کنند و مجبور بودیم از افرادی برای ارسال نسخه‌های چاپی اسکن‌ها به دستان تیم‌های جراحی استفاده کنیم». این اختلالات نه‌تنها مراقبت را به تعویق انداخت، بلکه خطرهای بیماران را افزایش داد و بار فوق‌العاده‌ای بر کارکنان پزشکی که در شرایط پرتنش کار می‌کردند، وارد کرد. بازیابی عملیات ۳۷ روز طول کشید، در این مدت حجم پرونده‌های کاغذی به اندازهٔ معادل یک مایل رشد کرد. او افزود «آسِنشن»، که در حال همکاری نزدیک با مقامات ایالات متحدهٔ آمریکاست و در حال طی کردن فرایند طولانی دیجیتال‌سازی داده‌های تمام سوابق بیمار است که طی آن دوره به‌صورت کاغذی ایجاد شده است، از نظر مالی، حدود ۱۳۰ میلیون دلار برای پاسخ به این حمله هزینه کرد و تقریباً ۰/۹ میلیارد دلار درآمد عملیاتی خود را تا پایان سال مالی ۲۰۲۴ از دست داد (The United Nations Office at Geneva, 2024)[5].

با توجه به توضیحات داده‌شده، حملات سایبری به زیرساخت‌های بهداشتی، ناقض حق حیات، حق بر سلامتی و حق بر برابری و عدم تبعیض در حوزهٔ سلامتی است. در این زمینه راهنمای تالین ۲ بیان می‌دارد: «بر اساس بند «الف» از قاعدهٔ ۳۶[6]، دولت‌ها مسئول نقض قواعد بین‌المللی حقوق بشرند که خود مرتکب می‌شوند. علاوه بر این، اگر فعالیت‌های یک بازیگر غیردولتی یا یک دولت دیگر مانع از توانایی افراد برای انجام فعالیت‌های سایبری شود که تحت حمایت قواعد بین‌المللی حقوق بشر قرار

1. Eduardo Conrado
2. Ascension Healthcare
3. MRI
4. CT
5. The United Nations Office at Geneva. (2024). *op.cit*
۶. قاعدهٔ ۳۶ راهنمای تالین ۲ بیان می‌دارد: « با توجه به فعالیت‌های سایبری، یک دولت باید: الف) حقوق بشر بین‌المللی افراد را رعایت کند؛ ب) حقوق بشر افراد را از سوءاستفاده‌های اشخاص ثالث حمایت کند».

دارند، دولت‌ها ممکن است موظف به تضمین این باشند که افراد مشمول حقوق پیش‌گفته بتوانند از آنها بهره‌مند شوند (بند «ب» از قاعدهٔ ۳۶) (Tallinn Manual 2.0, 2017: 182).

از سوی دیگر، قاعدهٔ ۱۰ راهنمای تالین ۱، عملیات سایبری را که به سطح توسل به زور نمی‌رسد، همچنان مغایر مقررات حقوق بین‌الملل می‌دانست و بیان می‌کرد: «عملیات سایبری که به آستانهٔ توسل به زور نمی‌رسد، لزوماً به معنای قانونی بودن آن تحت حقوق بین‌الملل نیست. به‌ویژه، یک عملیات سایبری ممکن است نقض ممنوعیت مداخله محسوب شود» (Tallinn Manual 1.0, 2013: 44). این مقرره مجدداً در قاعدهٔ ۶۸ راهنمای تالین ۲ نیز تکرار شده است و بیان می‌دارد: «عملیات سایبری که به آستانهٔ توسل به زور نرسد، لزوماً به معنای قانونی بودن آن تحت حقوق بین‌الملل نیست. به‌طور خاص، یک عملیات سایبری ممکن است به‌عنوان نقض حاکمیت (قاعدهٔ ۴) یا نقض ممنوعیت مداخله (قاعدهٔ ۶۶) تلقی شود» (Tallinn Manual 2.0, 2017: 330). در این راستا کارشناسان راهنمای تالین ۲ بیان کرده‌اند: «اصل حاکمیت شامل زیرساخت‌های سایبری واقع در قلمرو یک کشور می‌شود، صرف‌نظر از اینکه این زیرساخت‌ها دولتی یا خصوصی باشند. برای مثال، اگر یک کشور عملیات سایبری انجام دهد که به زیرساخت سایبری یک شرکت خصوصی واقع در کشور دیگری آسیب برساند، مانند زیرساخت‌های حیاتی متعلق به بخش خصوصی، اقدامات کشور اول به‌منزلهٔ نقض حاکمیت کشور اخیر محسوب می‌شود. این موضوع حتی در شرایطی که هیچ تأثیری بر روی زیرساخت‌ها، دارایی‌ها یا فعالیت‌های دولتی وجود نداشته باشد، همچنان صادق است» (Tallinn Manual 2.0, 2017: 18).

بنابراین، چنانکه مطابق با مادهٔ ۲ پیش‌نویس مواد راجع به مسئولیت دولت‌ها برای افعال متخلفانهٔ بین‌المللی ۲۰۰۱ و همچنین قاعدهٔ ۱۴ راهنمای تالین ۲ که بیان می‌دارد: «یک دولت مسئولیت بین‌المللی را به‌سبب یک عمل مرتبط با سایبر که به آن دولت نسبت داده می‌شود و به‌عنوان نقض یک تعهد حقوقی بین‌المللی محسوب می‌شود، بر عهده دارد» (Tallinn Manual 2.0, 2017: 84)، اگر حملات سایبری به زیرساخت‌های بهداشتی یک کشور قابل انتساب به دولتی باشد و نقض تعهد بین‌المللی آن دولت تلقی شود (دولت حمله‌کننده)، موجب مسئولیت بین‌المللی آن دولت در جامعهٔ بین‌المللی خواهد بود.

۵. حملات سایبری در زمان مخاصمات مسلحانه

صلح و امنیت سایبری در سطح بین‌الملل، همراه با پیشرفت فناوری و ایجاد ابزارهای مجهز به فناوری‌های روز دنیا، نظام حق و تکلیف را در عرصهٔ بین‌الملل با تحولات چشمگیری از حیث مقررات بین‌المللی روبه‌رو ساخته است (محقق‌هرچقان و همکاران، ۱۴۰۱: ۲۷۰). بدون شک هر حملهٔ سایبری،

آثار و تبعات سوء و مخربی را از خود به‌جای می‌گذارد. عمده‌ترین و اصلی‌ترین آنها، متأثر کردن رایانه، سیستم رایانه‌ای یا شبکهٔ مورد حمله با حذف، تحریف، تغییر داده یا نرم‌افزار، قطع سیستم از طریق محروم‌سازیِ توزیع‌شدهٔ خدمات[1] یا سایر حملات سایبری است (شایگان و صفوی‌کوهساره، ۱۳۹۷: ۴۲۷). این آثار و تبعات منفی گاهی به‌صورت مستقیم و اغلب به‌صورت غیرمستقیم و ثانویه به هدف موردنظر (قربانی) آسیب می‌رسانند و خسارت وارد می‌کنند. برای مثال، وقتی‌که حملهٔ سایبری بر روی سیستم کنترل هوایی یا راکتورهای اتمی صورت بگیرد و آسیب‌های انسانی و مالی وسیعی به‌بار آورد، به‌مثابهٔ یک حملهٔ مسلحانه محسوب می‌شود و آثار مخرب حملهٔ سایبری به‌صورت مستقیم ایجاد می‌شود (بیگلربیگی، ۱۴۰۲: ۱۳).

بنابراین باید گفت امروزه فضای مجازی این امکان را ایجاد کرده است که برای پیروزی در مخاصمات مسلحانه دیگر نیاز چندانی به فتوحات سرزمینی نباشد، بلکه با تسلط بر فناوری سایبری و حمله به سیستم رایانه‌ای دشمن از طرق مختلف از جمله ارسال ویروس می‌توان تمامی زیرساخت‌های آن را مورد حمله و آسیب جدی قرار داد و حتی تا مرحلهٔ خارج کردن کنترل مرزهای آن پیش رفت. حملات سایبری می‌توانند هم به‌طور مستقل انجام شوند و هم اجرای آنها در جریان مخاصمات مسلحانه ممکن است (بیگ‌زاده، ۱۴۰۱: ۱۵۲۱). از این‌رو استفاده از رایاجنگ‌های ناقض حقوق بشردوستانهٔ بین‌المللی میان دولت‌ها و آسیب به غیرنظامیان و زیرساخت‌های حیاتی ملی کشورها، تنظیم‌گریِ رایاجنگ‌ها و وضع محدودیت‌های کیفری مربوط به جنایات جنگی بر آنها را ناگزیر ساخته است تا آنجا که دادستان دیوان کیفری بین‌المللی در سال ۲۰۲۳، به‌صراحت از امکان تعقیب برخی رفتارهای ارتکاب‌یافته در چارچوبِ رایاجنگ‌ها با عنوان جنایت جنگی سخن گفته است (شاملو و حسینی، ۱۴۰۳: ۶۲۹).

در این زمینه باید به این پرسش پرداخت که چه زمانی این حملات به مخاصمات مسلحانه یا به تعبیری جنگ سایبری منجر می‌شود؟ و در واقع آستانهٔ موردنظر در تعیین این حملات به‌عنوان مخاصمهٔ مسلحانه چیست؟ از این‌رو در ادامه ابتدا به پاسخ این پرسش و سپس به امکان‌سنجی اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری در پرتو حمله به زیرساخت‌های بهداشتی پرداخته می‌شود.

۵. ۱. جنگ سایبری و حقوق توسل به زور

راهنمای تالین ۲ در قاعدهٔ ۶۸ خود مطابق بند ۴ مادهٔ ۲ منشور ملل متحد[2] بیان می‌دارد: «یک عملیات

1. Distributed Denial of Service (DDoS)

۲. بند ۴ مادهٔ ۲ منشور ملل متحد بیان می‌دارد: «کلیهٔ اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد، خودداری خواهند نمود».

سایبری که تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر دولتی را تشکیل دهد، یا به هر نحو دیگری با اهداف سازمان ملل متحد ناسازگار باشد، متخلفانه است» (Tallinn Manual 2.0, 2017: 329). همچنین در قاعدهٔ ۷۰ راهنمای تالین ۲ بیان می‌شود: «یک عملیات سایبری، یا تهدید به عملیات سایبری، زمانی‌که اقدام تهدید شده، در صورت انجام، به‌عنوان استفادهٔ متخلفانه از زور تلقی شود، به‌عنوان تهدید متخلفانه از زور محسوب می‌شود» (Tallinn Manual 2.0, 2017: 338). در این زمینه دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه سابقاً بیان کرده بود: «مادهٔ ۲ (۴) منشور سازمان ملل متحد مقرر می‌دارد: «تمام اعضای [سازمان ملل متحد] باید در روابط بین‌المللی خود از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر کشور، یا به هر نحو دیگری که با اهداف سازمان ملل متحد مغایرت داشته باشد، خودداری کنند»، این ممنوعیت بدون شک یک قاعده از حقوق بین‌الملل عرفی است» (ICJ, 1986: Paras. 188-190).

از سوی دیگر، برای تعیین «آستانهٔ» مخاصمهٔ مسلحانه در حمله‌های سایبری باید گفت طبق مادهٔ ۴۹ پروتکل شمارهٔ یک سال ۱۹۷۷ منضم به کنوانسیون‌های سال ۱۹۴۹ ژنو، «حمله» عبارت از «اعمال خشونت‌بار اعم از تهاجمی یا تدافعی بر ضد دشمن» است. اعمال خشونت‌بار باید در پرتو آثار و نه وسایل مورد استفاده برای ارتکابشان مورد توجه و ارزیابی قرار گیرد. به دیگر سخن، «حمله» به صِرف نفوذ در سیستم رایانه‌ای یک کشور تحقق پیدا نمی‌کند، بلکه در گستره و آثار ناشی از آن است که می‌توانند چنین نفوذی را به «حملهٔ مسلحانه» و یا به «توسل به زور» تبدیل کنند (بیگ‌زاده، ۱۴۰۱: ۱۵۲۲). در این زمینه در قاعدهٔ ۶۹ راهنمای تالین ۲ بیان شده است: «یک عملیات سایبری زمانی به‌عنوان توسل به زور محسوب می‌شود که مقیاس و آثار آن با عملیات غیرسایبری که به آستانهٔ توسل به زور می‌رسند، قابل مقایسه باشد». بنابراین، اگر نفوذ در سیستم رایانه‌ای به ورود جراحت و مرگ افراد یا خسارت به اموال منجر شود، در آن صورت می‌توان آن را «حمله» در مفهوم حقوق بشردوستانه لحاظ کرد؛ چنانکه قاعدهٔ ۹۲ راهنمای تالین ۲ هم حملهٔ سایبری را هرگونه «عملیات سایبری، اعم از تهاجمی یا تدافعی» لحاظ می‌کند که «به‌طور منطقی باید انتظار مرگ و ورود جراحت به افراد، خسارت یا تخریب اموال را داشت» (Tallinn Manual 2.0, 2017: 415). به دیگر سخن، برای تعیین «آستانهٔ» مخاصمهٔ مسلحانه در حمله‌های سایبری باید به گستره و آثار آن توجه داشت. با لحاظ کردن آنهاست که می‌توان حملهٔ سایبری را «توسل به زور» دانست (بیگ‌زاده، ۱۴۰۱: ۱۵۲۲).

همچنین در این زمینه باید گفت از آنجایی که منشور ملل متحد هیچ معیاری برای تعیین اینکه چه عملی به‌عنوان توسل به زور محسوب می‌شود، ارائه نمی‌دهد. در بحث‌های مربوط به آستانهٔ مناسب برای توسل به زور، گروه بین‌المللی کارشناسان راهنمای تالین ۲ به رأی نیکاراگوئه توجه کردند (Tallinn Manual 2.0, 2017: 330). در آن پرونده، دیوان بین‌المللی دادگستری بیان کرد که «مقیاس و

تأثیرات» باید در تعیین اینکه آیا اقدامات خاصی به‌عنوان «حملهٔ مسلحانه» محسوب می‌شود یا نه، در نظر گرفته شود. کارشناسان بر این باور بودند که تمرکز بر مقیاس و تأثیرات، رویکردی مفید برای تمایز بین اقداماتی است که به‌عنوان توسل به زور واجد شرایط هستند و آنهایی که نیستند. به‌عبارت دیگر، «مقیاس و تأثیرات» یک اصطلاح مختصر است که عوامل کمی و کیفی را که باید در تعیین اینکه آیا یک عملیات سایبری به‌عنوان استفاده از زور محسوب می‌شود، تجزیه‌وتحلیل کرد، در برمی‌گیرد. کارشناسان توافق کردند که هیچ دلیلی برای خارج کردن عملیات سایبری از دامنه اقداماتی که ممکن است به‌عنوان توسل به زور محسوب شوند، وجود ندارد، اگر مقیاس و تأثیرات عملیات موردنظر با عملیات غیرسایبری که واجد شرایط چنین هستند، قابل مقایسه باشد. علاوه بر این اشاره می‌کنند توسل به زور لزوماً نیازمند به‌کارگیری نیروهای نظامی یا دیگر نیروهای مسلح توسط دولت موردنظر نیست. در پروندهٔ نیکاراگوئه، دیوان بین‌المللی دادگستری دریافت که مسلح کردن و آموزش یک نیروی چریکی که درگیر مخاصمه علیه یک دولت دیگر است، به‌عنوان توسل به زور محسوب می‌شود. بنابراین، دولتی که یک گروه مسلح سازمان‌یافته را با بدافزار و آموزش لازم برای انجام عملیات سایبری علیه یک دولت دیگر تجهیز کند، به این معنا که آن تأمین و آموزش به گروه اجازه می‌دهد تا عملیات سایبری‌ای انجام دهد که به‌عنوان توسل به زور تلقی می‌شود، در واقع به آن دولت دیگر توسل به زور کرده است. این وضعیت باید از مواردی که در آن اقدامات یک گروه غیردولتی به موجب حقوق مسئولیت بین‌المللی دولت (قواعد ۱۵ و ۱۷ راهنمای تالین ۲) یا دفاع مشروع (قاعدهٔ ۷۱ راهنمای تالین ۲) به یک دولت نسبت داده می‌شود، متمایز شود (Tallinn Manual 2.0, 2017: 330-331).

در نهایت گروه بین‌المللی کارشناسان توافق کردند که هر عملیات سایبری که به سطح «حملهٔ مسلحانه» در زمینهٔ مقیاس و تأثیرات مطابق قاعدهٔ ۷۱ راهنمای تالین ۲ (دفاع مشروع) برسد و توسط یک دولت انجام شود یا به آن نسبت داده شود، به‌عنوان «توسل به زور» محسوب می‌شود (Tallinn Manual 2.0, 2017: 332). همچنین اشاره می‌کنند بسته به شرایط موجود، دولت‌ها ممکن است به عوامل دیگری نیز توجه کنند، مانند فضای سیاسی حاکم، اینکه آیا عملیات سایبری نشان‌دهندهٔ استفادهٔ آتی از نیروی نظامی است یا نه، هویت مهاجم، سابقهٔ عملیات سایبری توسط مهاجم و ماهیت هدف (مانند زیرساخت‌های حیاتی) (Tallinn Manual 2.0, 2017: 337). حتی برخی از کارشناسان بر این باور بودند که یک عملیات سایبری که علیه زیرساخت‌های حیاتی یک دولت انجام شود و به آثار شدید، هرچند غیرتخریبی، بینجامد، می‌تواند به‌عنوان یک حملهٔ مسلحانه تلقی شود (Tallinn Manual 2.0, 2017: 343).

در پایان شایان ذکر است با آنکه مادهٔ ۵۲ بند ۲ پروتکل شمارهٔ یک سال ۱۹۷۷ منضم به کنوانسیون‌های چهارگانهٔ ژنو سال ۱۹۴۹، حمله به قصد از کار انداختن هدف بدون تخریب آن را نیز لحاظ کرده است، با وجود این، لحاظ کردن «حمله‌های سایبری» بدون هیچ‌گونه تخریب مادی یا تلفات

انسانی به‌مثابهٔ «توسل به زور» تا حدودی مشکل می‌نماید. به‌ویژه باید به این نکته هم توجه کرد که آثار یک حملهٔ سایبری در مواردی قابل برگرداندن به حالت قبل از حمله را دارند. برای مثال می‌توان سیستم رایانه‌ای را که در اثر حملهٔ سایبری از کار افتاده است، با متوقف کردن آن حمله مجدداً به‌کار انداخت (بیگ‌زاده، ۱۴۰۱: ۱۵۲۳).

۵. ۲. اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ سایبری

حقوق بشر به انسان‌ها تعلق دارد و نظام بین‌المللِ حقوق بشر، از حق انسان‌ها در هر شرایطی در برابر دولت‌ها حمایت می‌کند؛ اما در زمان مخاصمات مسلحانه، علاوه بر حقوق بشر، حقوق بشردوستانه به‌عنوان قواعد خاص چارچوب قواعد حاکم بر روابط بین طرفین خواهد بود (Schwendimann, 2011: 1003). حقوق بشردوستانه به‌دنبال محدود کردن آثار درگیری‌های مسلحانه بر مردم، از جمله غیرنظامیان است و برای دستیابی به این هدف، به حمایت از افراد و اعمال محدودیت در ابزار و روش‌های جنگ می‌پردازد (OHCHR, 2011: 10) و نقض فاحش حقوق مخاصمات مسلحانه به‌منزلهٔ یک جنایت جنگی است که در محاکم داخلی یا دادگاه‌های بین‌المللی قابل تعقیب جزایی است (راجرز و مالرب، ۱۳۸۷: ۳۷).

به‌مانند سایر عملیات، حقوق مخاصمات مسلحانه به عملیات سایبری که در زمینهٔ یک مخاصمات مسلحانه انجام می‌شود نیز اعمال می‌شود. با وجود نوآوری عملیات سایبری و نبود قواعد و مقررات خاص در حقوق مخاصمات مسلحانه که به‌طور صریح به آنها پرداخته شده باشد، گروه بین‌المللی کارشناسان راهنمای تالین ۲ به اتفاق آرا به این نتیجه رسیدند که حقوق مخاصمات مسلحانه به چنین فعالیت‌هایی در طول هر دو نوع مخاصمات مسلحانهٔ بین‌المللی و غیربین‌المللی اعمال می‌شود و قاعدهٔ ۸۰ راهنمای تالین ۲ در این زمینه بیان کرده است: «عملیات سایبری که در چارچوب یک مخاصمهٔ مسلحانه انجام می‌شود، تابع حقوق مخاصمات مسلحانه است» (Tallinn Manual 2.0, 2017: 375). حقوق مخاصمات مسلحانه به هدف‌گیری هر شخص یا شیء در طول مخاصمات مسلحانه، صرف‌نظر از وسایل یا روش‌های جنگی به‌کاررفته، اعمال می‌شود. بنابراین، اصول اساسی مانند تمایز و ممنوعیت رنج غیرضروری به عملیات سایبری نیز اعمال می‌شود. البته قابلیت اعمال قواعد خاص معاهده‌ای به مسائلی همچون اینکه آیا یک دولت طرف آن معاهده است، وضعیت آن به‌عنوان طرف درگیری و نوع مخاصمهٔ مسلحانه بستگی دارد (Tallinn Manual 2.0, 2017: 414). همچنین پیش از این، در گزارش کمیتهٔ بین‌المللی صلیب سرخ به سی‌ویکمین کنفرانس بین‌المللی صلیب سرخ تحت عنوان «حقوق بین‌الملل بشردوستانه و چالش‌های درگیری مسلحانهٔ معاصر» در سال ۲۰۱۱ بیان شده بود که «از نظر کمیتهٔ بین‌المللی صلیب سرخ، در موارد زیر جنگ سایبری موضوع حقوق بشردوستانه قرار می‌گیرد: ۱. اگر در

وسایل و شیوه‌های جنگی از فضای سایبری استفاده شود؛ ۲. اگر در یک درگیری مسلحانه، عملیات سایبری علیه دشمن به‌کار رود و به ورود خسارت به او منجر شود. برای مثال اگر در حین درگیری مسلحانه، یک سیستم کنترل ترافیک هوایی با استفاده از فناوری‌های سایبری دستکاری و به سقوط یک هواناو غیرنظامی منجر شود» (ICRC, 2011: 36-37).

بدین ترتیب، در ادامه به‌نحو مقتضی به برخی از اصول بنیادین حقوق بین‌الملل بشردوستانه، از جمله اصل تفکیک، اصل منع ورود رنج و آلام بیهوده یا غیرضروری و اصل تناسب، پرداخته خواهد شد.

۵. ۲. ۱. اصل تفکیک

با توجه به مطالبی که بیان شد، در مخاصمات سایبری که به آستانهٔ یک حملهٔ مسلحانه می‌رسند، اصول و قواعد حقوق بین‌الملل بشردوستانه قابل اجراست. قواعد حقوق بشر نسبت به کلیهٔ ابنای بشر مجراست، درحالی‌که قواعد حقوق بشردوستانه تنها نسبت به برخی افراد لازم‌الاجراست؛ افراد غیرنظامی، اسیران جنگی، مجروحان و بیماران جنگی و مصدومان دریایی و در شرایطی برخی از نظامیان (ضیایی بیگدلی، ۱۴۰۰الف: ۴۳). با این حال، چالش اصلی فراروی اِعمال حقوق بشردوستانه در حمله‌های سایبری تعیین «رزمنده» و «میدان رزم» است. به علت ویژگی فضای مجازی ممکن است شناسایی «رزمندگان سایبری» و «محل» انجام حمله‌های سایبری نیز وجود نداشته باشند. عدم شناسایی رزمندهٔ سایبری به عدم امکان انتساب حملهٔ سایبری به فاعل آن و طرح مسئولیت احتمالی برای ارتکاب عمل متخلفانه بین‌المللی منجر می‌شود (بیگ‌زاده، ۱۴۰۱: ۱۵۲۳). با وجود این، در خصوص حملات سایبری به زیرساخت‌های بهداشتی در زمان مخاصمات، در ابتدا باید گفت که ناقض اصل ممنوعیت حمله به غیرنظامیان خواهد بود؛ چراکه عمدتاً غیرنظامیان در این مکان‌ها حضور دارند. افراد غیرنظامی اشخاصی هستند که عضو نیروهای مسلح هیچ‌یک از طرف‌های درگیری مسلحانه نیستند؛ جمعیت غیرنظامی شامل تمامی افراد غیرنظامی است.[۱] قاعدهٔ ۹۴ راهنمای تالین ۲ در این خصوص بیان می‌دارد: «جمعیت غیرنظامی به‌طور کلی و همچنین افراد غیرنظامی نباید هدف حملهٔ سایبری قرار گیرند». این قاعده بر اساس اصل تفکیک، که در قاعدهٔ ۹۳ راهنما مطرح شده، بنا شده است. این اصل در مادهٔ ۵۱ (۲) پروتکل یکم الحاقی و مادهٔ ۱۳ (۲) پروتکل دوم الحاقی تدوین شده است و بدون شک منعکس‌کننده حقوق بین‌الملل عرفی در هر دو نوع جنگ مسلحانه بین‌المللی و غیربین‌المللی است (Tallinn Manual 2.0, 2017: 422-423). دیوان بین‌المللی دادگستری در سال ۱۹۹۶ در نظر مشورتی خود راجع به سلاح‌های

---

۱. مادهٔ ۱۳ کنوانسیون چهارم ژنو؛ مادهٔ ۵۰ پروتکل یکم الحاقی؛ و قاعدهٔ ۵ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

هسته‌ای اعلام کرد که «اصل اساسی تفکیک در حقوق بین‌الملل بشردوستانه به‌کار می‌رود و هدف از اعمال این اصل حمایت از جمعیت و اهداف غیرنظامی است و تفاوت میان رزمنده و غیر رزمنده را مشخص می‌کند. دولت‌ها هرگز نباید جمعیت غیرنظامی را هدف قرار دهند و هرگز نباید از سلاح‌هایی استفاده کنند که قادر به تمایز بین اهداف نظامی و غیرنظامی نیستند» (ICJ, 1996: Paras. 226-257). البته شایان ذکر است چنانکه در قاعدهٔ ۹۶ راهنمای تالین ۲ بیان شده است، «افراد زیر ممکن است هدف حملات سایبری قرار گیرند: الف) اعضای نیروهای مسلح؛ ب) اعضای گروه‌های مسلح سازمان‌یافته؛ ج) غیرنظامیان، درصورتی‌که و تا زمانی که در مخاصمات به‌طور مستقیم شرکت کنند؛ و (د) در یک مخاصمهٔ مسلحانهٔ بین‌المللی، شرکت‌کنندگان در «مخاصمهٔ مسلحانهٔ بین‌المللی»[1] (Tallinn Manual 2.0, 2017: 425).[2]

همچنین از سوی دیگر باید گفت برخی از طبقات افراد، با عنایت به ویژگی‌های خاصی که از حیث جنسیت، سن، حرفه، تابعیت و غیره دارند، از حمایت‌های خاص نیز برخوردارند. یکی از این طبقات، مجروحان، بیماران و معلولان هستند. افراد غیرنظامی که براثر یا در جریان درگیری‌های مسلحانه، اعم از بین‌المللی و غیربین‌المللی مجروح، بیمار یا معلول می‌شوند، باید مورد احترام و حمایت خاص قرار گیرند.[3] طرف‌های درگیری باید اقدامات لازم را جهت جست‌وجوی بیماران، مجروحان و معلولان و درمان و مراقبت از آنان معمول دارند.[4] واحدهای بهداری غیرنظامی، از جمله بیمارستان‌هایی که بیماران، مجروحان و معلولان در آن‌ها بستری هستند و وسایل حمل‌ونقل آنان مصونیت دارند.[5] آزادی عبور محمولات دارویی و لوازم پزشکی مورد نیاز مجروحان، بیماران و معلولان و اشیای لازم برای مراسم مذهبی باید تضمین شود. حمله علیه آنها ممنوع است و جنایت جنگی محسوب می‌شود.[6] باید احترام و حمایت نسبت به کارکنان بهداری و مذهبی غیرنظامی که در خدمت مجروحان، بیماران و معلولان

---

1. Participants in a Levée en Masse

۲. این قاعده از مادهٔ ۵۱ (۳) پروتکل یکم الحاقی و مادهٔ ۱۳ (۳) پروتکل الحاقی دوم استخراج شده است. این قاعده به‌عنوان حقوق بین‌الملل عرفی در هر دو نوع جنگ مسلحانهٔ بین‌المللی و غیربین‌المللی شناخته می‌شود.

۳. مادهٔ ۱۶ کنوانسیون چهارم ژنو؛ مادهٔ ۱۰ پروتکل یکم الحاقی؛ مادهٔ ۳ مشترک کنوانسیون‌های چهارگانهٔ ژنو؛ مادهٔ ۷ پروتکل دوم الحاقی؛ و قاعدهٔ ۱۳۸ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

۴. مواد ۱۶ و ۳۸ کنوانسیون چهارم ژنو؛ مادهٔ ۱۰ پروتکل یکم الحاقی؛ مادهٔ ۳ مشترک کنوانسیون‌های چهارگانهٔ ژنو و مواد ۸-۷ پروتکل دوم الحاقی

۵. مواد ۱۸-۱۹، ۲۱-۲۲ کنوانسیون چهارم ژنو؛ مادهٔ ۱۲ پروتکل یکم الحاقی؛ مادهٔ ۱۱ پروتکل دوم الحاقی؛ و قاعدهٔ ۲۸-۲۹ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

۶. قاعدهٔ ۳۰ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه و مادهٔ ۸ اساسنامهٔ دیوان کیفری بین‌المللی

غیرنظامی‌اند، معمول داشت[۱]؛ حمله علیه آنها ممنوع است و جنایت جنگی محسوب می‌شود.[۲] چنین حملاتی در مقام اقدامات تلافی‌جویانه نیز منع شده است.[۳] همچنین افراد غیرنظامی تعهد به احترام نسبت به مجروحان، بیماران و معلولان و ممنوعیت ارتکاب هرگونه عمل خشونت‌بار علیه آنان دارند[۴] و حتی از سویی مجروحان، بیماران و معلولان نمی‌توانند در هیچ شرایطی از تمام یا بخشی از حقوق بشردوستانه‌ای که به آنان داده شده است، صرف‌نظر کنند.[۵] علاوه بر این، کارکنان بهداری به‌دلیل مأموریت حساسی که ایفا می‌کنند از تضمینات بسیار قوی برخوردارند. هدف از این تضمینات که در واقع متضمن امتیازاتی برای آنهاست، تأمین آزادی عمل ایشان است. در نتیجه حق اعراض از آن را ندارند، زیرا چنین امتیازهایی همراه با وظایف است (ضیایی بیگدلی، ۱۴۰۰ب: ۱۸۳).

البته شایان ذکر است این واحدها درصورتی‌که خارج از وظایف انسان دوستانه‌شان برای ارتکاب اعمال مضر به حال دشمن به‌کار گرفته شوند، حمایت خود را از دست می‌دهند[۶]، در غیر این صورت حمله علیه واحدهای بهداری ممنوع است و جنایت جنگی تلقی می‌شود.[۷] بنابراین، هنگامی‌که سربازان دشمن به‌علت جراحت از حالت رزم خارج می‌شوند، هدف نظامی تحقق یافته است و ضرورت نظامی جای خود را به ندای انسانیت می‌دهد که ایجاب می‌کند به درمان آنان بپردازیم (راجرز و مالرب، ۱۳۸۷: ۱۱۵) و به‌طور کلی مگر در صورت اثبات خلاف آن، حملات سایبری به زیرساخت‌های بهداشتی در زمان مخاصمات، ناقض اصل عدم حمله به غیرنظامیان خواهد بود.

از سوی دیگر، حملات سایبری به زیرساخت‌های بهداشتی در زمان مخاصمات، ناقض اصل عدم حمله به اهداف غیرنظامی خواهد بود. تفکیک میان هدف‌های نظامی و غیرنظامی به‌عنوان یکی از اصول حقوق بشردوستانه در هدایت درگیری‌های مسلحانه نقش بسیار اساسی دارد؛ چراکه هدف‌های نظامی به‌طور معمول می‌توانند مورد تهاجم و تخریب قرار گیرند، درحالی‌که هدف‌های غیرنظامی، اعم از افراد و اموال غیرنظامی، مصون از هرگونه تهاجم و تخریب هستند (ضیایی بیگدلی، ۱۴۰۰الف: ۷۹–۸۰). اموال غیرنظامی اموالی هستند که هدف نظامی محسوب نمی‌شوند.[۸] ممنوعیت حمله به اهداف غیرنظامی

---

۱. مادهٔ ۲۰ کنوانسیون چهارم ژنو؛ مادهٔ ۱۵ پروتکل یکم الحاقی؛ مادهٔ ۳ مشترک کنوانسیون‌های چهارگانه ژنو؛ مادهٔ ۹ پروتکل دوم الحاقی؛ و قواعد ۲۵ و ۲۷ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

۲. قاعدهٔ ۳۰ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه و مادهٔ ۸ اساسنامهٔ دیوان کیفری بین‌المللی

۳. بند ۶ مادهٔ ۵۱، بند ۴ مادهٔ ۵۴، بند ۲ مادهٔ ۵۵، بند ۴ مادهٔ ۵۶ پروتکل یکم الحاقی

۴. مادهٔ ۱۷ پروتکل یکم الحاقی

۵. مادهٔ ۷ کنوانسیون چهارم ژنو

۶. مادهٔ ۱۹ کنوانسیون چهارم ژنو؛ و قواعد ۲۸–۲۹ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

۷. مادهٔ ۲۳ کنوانسیون چهارم ژنو

۸. مادهٔ ۵۲ پروتکل یکم الحاقی؛ و قاعدهٔ ۹ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

به‌طور تاریخی از اعلامیه سن‌پترزبورگ در سال ۱۸۶۸ ناشی می‌شود که مقرر می‌کرد «تنها هدف مشروع که دولت‌ها باید در طول جنگ به دنبال آن باشند، تضعیف نیروهای نظامی دشمن است» (Saint Petersburg Declaration, 1868: preamble). این قاعده از آن زمان در مادهٔ ۵۲ (۱) پروتکل یکم الحاقی تدوین شده و در جنگ‌های مسلحانهٔ بین‌المللی و غیربین‌المللی به‌عنوان حقوق بین‌الملل عرفی اعمال می‌شود. مطابق مادهٔ ۵۲ پروتکل یکم الحاقی، «در مورد اموال، هدف‌های نظامی محدود به اموالی هستند که از نظر ماهیت، محل استقرار، نحوهٔ استفاده، سهم مؤثری در عملیات نظامی دارند و انهدام کامل یا بخشی از آنها، تصرف یا از کار انداختن آنها در شرایط زمانی موجود یک مزیت نظامی محسوب می‌گردد». قاعدهٔ ۹۹ راهنمای تالین ۲ در این خصوص بیان می‌دارد: «اهداف غیرنظامی نباید هدف حملات سایبری قرار گیرند. زیرساخت‌های سایبری تنها در صورتی می‌توانند هدف حمله قرار گیرند که به‌عنوان هدف نظامی شناخته شوند» (Tallinn Manual 2.0, 2017: 434-435). بر این اماکن، اصل برخورداری از احترام و حمایت بنیادین[۱]، ممنوعیت تصرف، تخریب یا انهدام، مگر انهدام آنها به‌دلیل یک ضرورت قطعی نظامی[۲] ناشی از درگیری مسلحانه باشد، حاکم است.[۳]

علاوه بر این حمایت عام، برخی اموال از حمایت‌های خاص نیز برخوردارند. یکی از این اموال، اموال ضروری برای بقای افراد غیرنظامی است. به‌طور کلی اموالی که برای بقای افراد غیرنظامی ضروری و اجتناب‌ناپذیر است، در زمره اموال غیرنظامی محسوب می‌شود و در درگیری‌های مسلحانه، اعم از بین‌المللی یا غیربین‌المللی، نباید مورد تعرض قرار بگیرد (ضیایی بیگدلی، ۱۴۰۰الف: ۱۴۵). از این‌رو اموال مربوط به مواد غذایی، دارویی و بهداشتی شامل این اموال می‌شود. همچنین وسایل حمل‌ونقل بهداری نباید نه مورد حمله قرار گیرد و نه به آنها خسارت وارد شود و نه مانع از عبور آنها شد، بلکه برعکس باید آن‌ها را مورد احترام و حمایت قرار داد و در صورت تهاجم از آنها دفاع کرد. حتی کشتی‌های تجاری و تفریحی کشورهای بی‌طرف که مجروحان و بیماران جنگی را حمل می‌کنند، نباید ضبط و توقیف شوند. هواپیماهای بهداری که منحصراً جهت حمل‌ونقل مجروحان و بیماران جنگی و همچنین برای حمل کارکنان و ملزومات بهداری به‌کار می‌روند، نباید مورد حمله و تهاجم واقع شوند.[۴]

---

۱. مادهٔ ۴۸ پروتکل یکم الحاقی

۲. ضرورت نظامی یک روش یا تدبیر نظامی است که نیروهای مسلح هر طرف درگیری در پیش می‌گیرد تا بتواند طرف دیگر را مرعوب و مغلوب کند و به مقاصد نظامی خود نایل آید (ضیایی‌بیگدلی، ۱۴۰۰، الف: ۱۴۲).

۳. مادهٔ ۱۴۷ کنوانسیون چهارم ژنو؛ قواعد ۷ و۱۰ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه و مادهٔ ۱۸ اساسنامهٔ دیوان کیفری بین‌المللی

۴. مواد ۳۵–۳۷ کنوانسیون اوّل ژنو؛ مواد ۳۸–۴۰ کنوانسیون دوم ژنو؛ مواد ۲۱–۳۱ پروتکل یکم الحاقی؛ مادهٔ ۱۱ پروتکل دوم الحاقی؛ و قاعده ۲۹ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه.

۵. ۲. ۲. اصل منع ورود رنج و آلام بیهوده یا غیرضروری

یکی دیگر از اصول اساسی حقوق بشردوستانه آن است که طرف‌های یک درگیری مسلحانه، اعم از بین‌المللی یا غیربین‌المللی، اختیارات نامحدود در انتخاب وسایل و شیوه‌های نبرد ندارند. به‌عبارت بهتر، هیچ‌یک از طرف‌های درگیری نمی‌توانند از هر وسیله و روشی برای اذیت و آزار دشمن، حتی نظامیان و سرکوب و تسلیم آنان استفاده کنند (ضیایی بیگدلی، ۱۴۰۰الف: ۲۰۳). این قاعده امروزه به‌عنوان یک قاعدهٔ عرفی عام (حتی در درگیری‌های مسلحانهٔ غیربین‌المللی) به رسمیت شناخته شده است.[۱] یکی از جلوه‌های این ممنوعیت و محدودیت، قاعدهٔ منع ورود رنج و آلام بیهوده یا غیرضروری است. دیوان بین‌المللی دادگستری در این زمینه تأکید کرده است که وسایل و روش‌های جنگی که ماهیتاً به‌گونه‌ای هستند که به صدمه زائد و رنج غیرضروری منجر می‌شوند، ممنوع‌اند و این اصل یکی از اصول مهم حقوق بین‌الملل بشردوستانه است (ICJ, 1996: Para 238). بند ۲ مادهٔ ۳۵ پروتکل یکم الحاقی بیان می‌کند: «به‌کار بردن سلاح‌ها، پرتاب‌شونده‌ها و مواد و شیوه‌های جنگی از نوعی که منجر به وارد آوردن صدمات بیش‌ازحد و رنج غیرضروری می‌شود، ممنوع است». شعبه تجدیدنظر دادگاه ویژهٔ کیفری برای یوگسلاوی سابق نیز با تأیید این مسئله که این اصول در مخاصمات مسلحانهٔ داخلی هم قابل اجراست، بیان می‌دارد: «آنچه در جنگ‌های بین‌المللی غیرانسانی است و در نتیجه ممنوع شده، در جنگ‌های داخلی هم غیرقابل قبول و غیرانسانی است» (ICTY, 1999: Para 119). از آنجایی که هر حملهٔ کامپیوتری با توجه به نوع استفاده و اجرا متفاوت است، هر حمله‌ای باید جداگانه ارزیابی شود تا اطمینان حاصل شود که این تعادل حفظ شده است. از آنجایی که استفاده از یک سلاح که رنج یا صدمه مضاعف ایجاد می‌کند، نسبت به سلاح دیگری که مزیت نظامی مشابه دارد غیرقانونی است، طبقه‌بندی لزوماً شامل مقایسه‌ای میان سلاح‌های مختلف می‌شود (برادران، ۱۳۹۸: ۱۶۹). با این حال همان‌طور که کارشناسان راهنمای تالین ۲ اشاره می‌کنند تعیین اینکه آیا یک هدف، هدفی غیرنظامی است که از حمله مصون است و نه هدف نظامی، باید به‌صورت مورد به مورد انجام شود (Tallinn Manual 2.0, 2017: 435). اما به‌طور کلی از نظر نگارندگان اصولاً حمله به زیرساخت‌های بهداشتی ناقض این قاعده نیز خواهد بود.

۵. ۲. ۳. اصل تناسب

مقصود از قاعدهٔ تناسب، سازش دادن امتیازات عملی ناشی از یک حمله با ضرورت‌های نظامی است. این قاعده مبتنی بر این اصل مسلم است که حمله نباید موجب آسیب رساندن به افراد و اموال غیرنظامی در حدی شود که در مقایسه با امتیاز نظامی مورد انتظار، بیش از اندازه باشد (ممتاز و شایگان، ۱۳۹۷: ۹۳).

---

۱. قاعدهٔ ۷۰ از مجموعه قواعد عرفی حقوق بین‌الملل بشردوستانه

این قاعده، بر اساس بند ۵ (ب) مادهٔ ۵۱ و بند ۲ (۳) مادهٔ ۵۷ پروتکل الحاقی اول تدوین شده است. این اصل اغلب به‌عنوان «قاعدهٔ تناسب»[1] شناخته می‌شود، اگرچه از منظر فنی و حقوقی، موضوع آن «بیش‌ازحد بودن»[2] است نه تناسب. این اصل به‌طور کلی به‌عنوان بخشی از حقوق بین‌الملل عرفی پذیرفته شده و در درگیری‌های مسلحانهٔ بین‌المللی و غیربین‌المللی قابل اعمال است (Tallinn Manual 2.0, 2017: 471).

از این‌رو این اصل در قاعدهٔ ۱۱۳ راهنمای تالین ۲ بدین‌گونه تعریف شده است: «حملهٔ سایبری که احتمال می‌رود به تلفات تصادفی در میان غیرنظامیان، جراحت به غیرنظامیان، خسارت به اموال غیرنظامی، یا ترکیبی از این موارد منجر شود و این خسارات در مقایسه با مزیت نظامی عینی و مستقیمی که انتظار می‌رود حاصل شود، بیش‌ازحد باشد، ممنوع است». بنابراین، این قاعده به وضعیت‌هایی می‌پردازد که در آنها به غیرنظامیان یا اموال غیرنظامی به‌طور تصادفی آسیب وارد می‌شود؛ به این معنا که آنها هدف اصلی حمله نیستند. مرگ یا جراحت غیرنظامیان و آسیب یا تخریب اموال غیرنظامی که به‌طور تصادفی رخ می‌دهد، اغلب «خسارت جانبی»[3] نامیده می‌شود. از این‌رو همان‌طور که این قاعده به‌روشنی بیان می‌دارد، صرف اینکه غیرنظامیان یا اموال غیرنظامی در جریان حملهٔ سایبری به یک هدف نظامی مشروع متحمل آسیب شوند، به‌خودی‌خود[4] آن حمله را غیرقانونی نمی‌سازد، بلکه قانونی بودن چنین حمله‌ای که به خسارت جانبی منجر می‌شود، به نسبت میان آسیبی بستگی دارد که مهاجم می‌تواند به‌طور منطقی انتظار داشته باشد به‌طور تصادفی به غیرنظامیان و اموال آنها وارد شود و مزیت نظامی‌ای که مهاجم پیش‌بینی می‌کند در نتیجهٔ آن حمله به‌دست آورد. به‌عنوان مثالی از نحوهٔ اجرای این قاعده، مورد حملهٔ سایبری به سامانهٔ موقعیت‌یاب جهانی[5] را در نظر بگیرید. این سامانه کاربرد دوگانه دارد، بنابراین هدف مشروع نظامی محسوب می‌شود. با این حال، محروم ساختن کاربران غیرنظامی از اطلاعات حیاتی مانند داده‌های ناوبری احتمالاً به آسیب‌هایی نظیر خسارت به کشتی‌های تجاری و هواپیماهای غیرنظامی منجر می‌شود که برای هدایت خود به سامانهٔ موقعیت‌یاب جهانی وابسته‌اند. اگر آسیبی که به‌طور منطقی انتظار می‌رود در نتیجهٔ چنین حمله‌ای به غیرنظامیان وارد شود، در مقایسه با مزیت نظامی پیش‌بینی‌شده از آن عملیات بیش‌ازحد باشد، آن عملیات ممنوع خواهد بود[6] (Tallinn Manual 2.0, 2017: 471-472). بنابراین، به‌نظر می‌رسد که حمله به زیرساخت‌های بهداشت و

1. Proportionality
2. Excessiveness
3. Collateral Damage
4. *per se*
5. GPS

۶. مادهٔ ۸ (۲) (ب) (۴) اساسنامهٔ رم

درمان، در اغلب موارد، با اصل تناسب در حقوق مخاصمات مسلحانه ناسازگار باشد، چراکه میزان آسیب و رنج انسانی ناشی از چنین حملاتی، در مقایسه با مزیت نظامی احتمالی حاصل از آنها، به‌مراتب بیشتر است. از این‌رو این‌گونه حملات، به موجب حقوق بین‌الملل بشردوستانه، اصولاً ممنوع تلقی می‌شوند.

در نهایت باید گفت اگرچه در نظام حقوق بشردوستانه نفوذ در سیستم‌های رایانه‌ای ممنوع نیست، با وجود این، استفاده از آن برای انجام حملات بدون رعایت اصل تفکیک یا وارد کردن تلفات انسانی و مادی بدون رعایت اصل تناسب و بدون وجود ضرورت‌های نظامی باید ممنوع لحاظ شود. به دیگر سخن، باید ابتدا بررسی کرد که آیا استفاده از فناوری سایبری در چارچوب مخاصمات مسلحانه مغایر و ناقض قواعد عام و خاص حقوق بشردوستانه ناظر بر وسایل و شیوه‌های جنگی است یا نه؟ و اگر پاسخ منفی باشد باید به این نکته توجه کرد که آیا استفاده از چنین فناوری‌ای در برخی اوضاع و احوال می‌تواند به نقض «شرط مارتنس»[1] یعنی «اصول بشردوستانه و اقتضائات وجدان جمعی منجر شود؟ شرطی که دیوان بین‌المللی دادگستری آن را «بیان حقوق عرفی» و لازم‌الاجرا دانسته است؛ ضمن آنکه وسیلهٔ مؤثری برای مقابله با تحول سریع فناوری‌های نظامی است (بیگ‌زاده، ۱۴۰۱: ۱۵۲۲۵-۱۵۲۶).

۶. نتیجه

از آنجایی که ممکن است در فضای سایبر شناسایی پیام‌دهنده و محل ارسال پیام قابل شناسایی نباشد، بنابراین امکان سوءاستفاده از آن و حملات سایبری وجود دارد. امروزه متأسفانه بخش بهداشت و درمان به‌دلیل اهمیت و مزایای اقتصادی که دارد، به گزینه‌ای آسیب‌پذیر و در عین حال جذاب برای حملات سایبری تبدیل شده است. این حملات هم در زمان صلح و هم در زمان مخاصمات امکان‌پذیرند. چنانکه به‌تفصیل بیان شد، در زمان صلح، این حملات می‌تواند ناقض حق حیات، حق بر سلامتی و حق بر برابری و عدم تبعیض در حوزهٔ سلامتی باشد و مسئولیت بین‌المللی حمله‌کننده را فراهم سازد. از سوی دیگر، اگر نفوذ در سیستم رایانه‌ای به ورود جراحت و مرگ افراد یا خسارت به اموال منجر شود، در آن صورت می‌توان آن را «حمله» در مفهوم حقوق بشردوستانه لحاظ کرد. به دیگر سخن، برای تعیین «آستانه» مخاصمهٔ مسلحانه در حمله‌های سایبری باید به گستره و آثار آن توجه داشت و با لحاظ کردن آنها می‌توان حملهٔ سایبری را «توسل به زور» دانست. با توجه به این مسئله، انجام این حملات در زمان مخاصمات، اصولاً ناقض اصل تفکیک، ممنوعیت حمله به غیرنظامیان و اهداف غیرنظامی، قاعدهٔ منع ورود رنج و آلام بیهوده یا غیرضروری و اصل تناسب خواهد بود که ارتکاب آنها جنایت جنگی محسوب می‌شود.

با توجه به اهمیت این بخش و نوع اطلاعات کاربری موجود در سیستم‌های اطلاعات بهداشتی، این

1. Martens Clause

بخش باید بر امنیت سایبری تأکید بیشتری داشته باشد. برای بیماران، ارائه‌دهندگان خدمات و هکرهای هویتی، سوابق بهداشتی و داده‌های پزشکی بسیار باارزش‌اند. برآورد شده است که ارزش داده‌های بهداشتی ده تا چهل برابر بیشتر از اطلاعات کارت اعتباری یا بانکی است[1]، زیرا اگر اطلاعات کارت اعتباری یا بانکی به خطر بیفتد، می‌توان آنها را تغییر داد، اما سوابق یا داده‌های بهداشتی که می‌توانند به یک فرد خاص مرتبط شوند، تغییرپذیر نیستند. از این‌رو باید در صورت وقوع یک حملهٔ سایبری، تحقیق کامل در خصوص حادثه در راستای شناسایی نوع حملهٔ سایبری، شناسایی دستگاه‌های آسیب‌دیده، بررسی نقاط ورود و آسیب‌پذیری‌ها و هشدار و همکاری نزدیک با مقامات صورت گیرد. باید از کارشناسان امنیت سایبری برای اطمینان از رعایت پروتکل‌های امنیتی و تقویت آنها بهره‌مند شد. علاوه بر این، بیمارستان‌ها باید به شبکه‌های اطلاعاتی منطقه‌ای یا ملی بپیوندند و تمام تهدیدات سایبری را بشناسند. مدیران ارشد باید از تمام خطرهایی که با استفاده از فناوری اطلاعات با آنها مواجه‌اند، آگاه باشند و یاد بگیرند که چگونه آنها را کاهش دهند. همچنین در مواجهه با درخواست‌های باج‌گیرانه، توصیه نمی‌شود که قربانیان به‌سرعت باج موردنظر مهاجمان باج‌افزار را پرداخت کنند؛ چراکه هیچ‌گونه تضمینی وجود ندارد که حمله تکرار نشود یا مهاجمان مجدداً به اطلاعات دسترسی پیدا نکنند. در صورت وقوع حملهٔ باج‌افزاری، توصیه می‌شود به‌سرعت با نهادهای مسئول اجرای قانون تماس گرفته شده و راهنمایی‌های لازم از آنان دریافت شود. افزون بر این، پشتیبان‌گیری منظم از داده‌ها در فضای ابری می‌تواند فرآیند بازسازی شبکه‌ها را تسهیل کند. ضروری است که برنامه‌ریزی برای بازیابی در شرایط بحرانی، پیش از بروز تهدیدات سایبری صورت گیرد.

---

۱. برای مطالعهٔ بیشتر ر.ک:

Cyberpolicy. (n.d.). Why Medical Records are 10 Times More Valuable Than Credit Card Info. Retrieved May 23, 2025 from https://www.cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info; Humer, C.; & Finkle, J. (2014). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved May 23, 2025 from https://www.reuters.com/article/technology/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I/; Zabel, L. (2014). The Value of Personal Medical Information: Protecting Against Data Breaches. *National Association of Healthcare Access Management (naham).* Retrieved May 23, 2025 from https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information

منابع

۱. فارسی

الف) کتاب‌ها

۱. بـرادران، نـازنین (۱۳۹۸). جنـگ *سـایبری از منظـر حقـوق بین‌الملـل*. چ اول، تهـران: مؤسسـهٔ مطالعـات و پژوهش‌های حقوقی شهر دانش.

۲. بیگ‌زاده، ابراهیم (۱۴۰۱). *حقوق بین‌الملل. جلد دوم: روابط تابعان*. چ اول. تهران: میزان.

۳. راجرز، آنتونی پ.و.؛ مالرب، پل (۱۳۸۷). *قواعد کاربری حقوق مخاصمات مسلحانه*. ترجمهٔ کمیتـهٔ ملـی حقـوق بشردوستانه، تهران: امیرکبیر.

۴. ضیایی بیگدلی، محمدرضا (۱۴۰۰الف). *حقوق بین‌الملل بشردوستانه*. چ پنجم. تهران: انتشارات گنج دانـش، بـا همکاری کمیتهٔ بین‌المللی صلیب سرخ.

۵. ضیایی بیگدلی، محمدرضا (۱۴۰۰ب). *حقوق جنگ: حقوق بین‌الملـل مخاصـمات مسـلحانه*. چ هفـتم، تهـران: انتشارات دانشگاه علامه طباطبایی.

۶. قاری سیدفاطمی، سیدمحمد (۱۳۹۹). *حقوق بشر معاصر. دفتر دوم: جستارهایی تحلیلی در حق‌هـا و آزادی‌هـا*. تهران: نگاه معاصر.

۷. ممتاز، جمشید؛ شایگان، فریده (۱۳۹۷). *حقوق بین‌الملل بشردوستانه در برابر چالش‌های مخاصـمات مسـلحانهٔ عصر حاضر*. چ دوم، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.

ب) مقالات

۸. اصلانی، جبار؛ رنجبریان، امیرحسین (۱۳۹۴). بررسی تطبیقی و تحلیل تعریف حملهٔ سایبری از منظر دکتـرین، رویهٔ کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل. *فصلنامهٔ تحقیقات حقوقی دانشگاه شهید بهشـتی*، ۱۸ (۷۱)، ۲۵۷-۲۷۸.

۹. شاملو، باقر؛ حسینی، مهدی (۱۴۰۳). عنصر زمینه‌ای جنایات جنگی سایبری ناشی از رایاجنگ‌های مختل‌کننده در پرتو سند مقررات تالین. *فصلنامهٔ مطالعات حقوق تطبیقی*، ۱۵ (۲)، ۶۰۱-۶۳۶.

۱۰. شایگان، فریده؛ صفوی‌کوهساره، سیدحامد (۱۳۹۷). عملیات سایبری به‌مثابهٔ توسل به زور. *فصلنامهٔ مطالعات حقوق عمومی*، ۴۸ (۲)، ۴۱۹-۴۴۱.

۱۱. شهبازی، آرامش؛ آقاجانی‌رونقی، آیدا (۱۳۹۹). جاسوسی سایبری در حقوق بین‌الملل: مسئلهٔ انتساب مسـئولیت بین‌المللی به دولت در هاله‌ای از ابهام. *فصلنامهٔ مطالعات حقوق عمومی*، ۵۰ (۴)، ۱۴۸۷-۱۵۰۳.

۱۲. صلح‌چی، سارا؛ بیگلربیگی، کیان؛ عزیزی، سـتار (۱۴۰۳). سـوگیری هـوش مصـنوعی علیـه زنـان در حـوزهٔ سلامت. *مجلهٔ علمی پژوهشی حقوق پزشکی*، ۱۸ (۵۹)، ۲۳۵-۲۱۷.

۱۳. محقق‌هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم؛ مهـدوی ثابـت، محمـدعلی (۱۴۰۲). حقـوق

بین‌الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی). *فصلنامهٔ مطالعات حقوق عمومی*، ۵۳ (۳)، ۱۵۳۷-۱۵۵۹.

۱۴. محقق‌هرچقان، علیرضا؛ اردبیلی، محمدعلی؛ بیگ‌زاده، ابراهیم؛ مهدوی ثابت، محمدعلی (۱۴۰۱). اثربخشی دستورالعمل تالین ۲۰۱۷ میلادی بر صلاحیت دیوان کیفری بین‌المللی در ایجاد صلح و امنیت سایبری بین‌المللی. *فصلنامهٔ آموزه‌های حقوق کیفری*، ۱۹ (۲۳)، ۲۶۹-۲۹۶.

ج) پایان‌نامه

۱۵. بیگلربیگی، کیان (۱۴۰۲). حملات سایبری و نقض اصل عدم مداخله. *پایان‌نامهٔ کارشناسی ارشد حقوق بین‌الملل*. به راهنمایی ابراهیم بیگ‌زاده. تهران: دانشگاه شهید بهشتی، دانشکدهٔ حقوق، تاریخ دفاع ۱۴۰۲/۰۶/۱۹.

۲. انگلیسی

A) Books

1. Clemente, D. (2013). *Cyber Security and Global Interdependence: What Is Critical?*. London: Chatham House.
2. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
3. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. (2017). *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation*, Cambridge University Press.
4. Lehto, M. (2022). *Cyber-Attacks Against Critical Infrastructure*. In book: Lehto, M.; & Neittaanmäki, P. (Eds.), Cyber Security: Critical Infrastructure Protection. Springer. Computational Methods in Applied Sciences, Vol. 56, 3-42.
5. Liivoja, R.; & McCormack, T. (2013). *Law in Virtual Battlespace: The Tallinn Manual and the jus in bello*. Vol. 15. Yearbook of International Humanitarian Law,
6. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
7. Taubman, C.; Hart, A.; Hertelendy, A.; Tin, D.; Hata, R.; & Ciottone, G.R. (2023). *Reviewing the Health Care Impacts of Attacks on Critical Infrastructure*. In book: Prehospital and Disaster Medicine, Vol. 38, No. 5, Cambridge University Press, 660-667.

B) Articles

8. Adebukola, A., Navya, A., Jordan, F., Jenifer, N., & Richard D., B. (2022). Cyber Security as a Threat to Health Care. *Journal of Technology and Systems,* 4 (1), 32 – 64.
9. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1), 1-10.

10. Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. *BMC Medical Informatics and Decision Making,* 24, 133, 1-15.
11. Chon, A., Dave, C., & Ronald, R. S. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, 62(4), 539-548.
12. Hartlev M. (2013). Equal Access to Healthcare on a Non-Discriminatory Basis-Reality or Aspiration. *European Journal of Health Law*, 20(4), 343-346.
13. Kulkarni, V. P. (2025). Cybercrime in healthcare: Legal frameworks for prevention and enforcement. *International Journal of Law*, 11(4), 30-35.
14. Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: an economic perspective. *Economics and Business Review*, 5(19), No. 2, 24-47.
15. Nandy, M., & Dubey, A.. (2024). Public Health Care Cybersecurity Challenges and Solutions for Cyber-Attacks on Critical Health Infrastructure. South Eastern European Journal of Public Health, 322–326.
16. Nelson, C.J., Soisson, E.T., Li, P.C., Lester-Coll, N.H., Gagne, H., Deeley, M.A., Anker, C.J., Ann Roy, A., & Wallace, H.J. (2022). Impact of and Response to Cyberattacks in Radiation Oncology. *Advances in Radiation Oncology*, 7 (5), 1-7.
17. Orzechowski, M., Nowak, M., Bielińska, K., Chowaniec, A., Doričić, R., Ramšak, M., Muzur, A., Zupanič-Slavec, Z., & Florian, S.. (2020). Social diversity and access to healthcare in Europe: how does European Union's legislation prevent from discrimination in healthcare?. *BMC Public Health*, 20, 1399, 1-10.
18. Schwendimann, F. (2011). The legal framework of humanitarian access in armed conflict. *International Review of the Red Cross*, 93(884), 993-1008.
19. Yustina, EW., & Kusumaningrum, AE. (2019). The Principle of Non-Discrimination in Health Services in the Perspective of Government Responsibility.*Untag law review (ULREV)*, 3(2), 188-198.

C) Thesis

20. Valo, J. (2014). Cyber Attacks and the Use of Force in International Law. *Master's Thesis*. Supervisor: LL.D. Jarna Petman. Helsinki: University of Helsinki, Faculty of Law, January 2014.

D) Cases

21. ICJ. (1986). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Judgment. Retrieved November 16, 2024 from https://www.icj-cij.org/case/70
22. ICJ. (1996). Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. Retrieved November 16, 2024 from https://www.icj-cij.org/case/95
23. ICTY. (1999). The Tadić case (IT-94-1-A), Appeals Chamber, Judgment, 15 July 1999. Retrieved November 19, 2024 from https://www.icty.org/en/case/tadic

E) Conventions & Documents

24. Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System. (2003). Retrieved November 17, 2024 from https://rm.coe.int/168008160f
25. Constitution of the World Health Organization (1946). Retrieved September 12, 2024

from https://treaties.un.org/doc/Treaties/1948/04/19480407%2010-51%20PM/Ch_IX_01p.pdf
26. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. (1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949?activeTab=1949GCs-APs-and-commentaries
27. Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. (1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gcii-1949?activeTab=1949GCs-APs-and-commentaries
28. Convention (III) relative to the Treatment of Prisoners of War. (1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949?activeTab=1949GCs-APs-and-commentaries
29. Convention (IV) relative to the Protection of Civilian Persons in Time of War. (1949). Geneva, 12 August 1949. Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949
30. Convention on Cybercrime (Budapest Convention). (2001). Council of Europe. European Treaty Series – No. 185., Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https://rm.coe.int/1680081561
31. Customary international humanitarian law (IHL). (2005). Retrieved November 19, 2024 from https://ihl-databases.icrc.org/en/customary-ihl
32. Draft articles on Responsibility of States for Internationally Wrongful Acts. (2001). Retrieved November 19, 2024 from https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
33. European Convention on Human Rights. (1950). Retrieved September 12, 2024 from https://www.echr.coe.int/documents/d/echr/convention_ENG
34. Human Rights Committee. (1984). General Comment No 14. Retrieved November 17, 2024 from https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/Health/GC14.pdf
35. ICRC. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, official working document of the 31st International Conference of the Red Cross and Red Crescent, 28 November–1 December 2011, Doc. 31IC/11/5.1.2. Retrieved November 19, 2024 from http://www.rulac.org/assets/downloads/2011_Contemporary_Challenges_report.pdf
36. International Covenant on Civil and Political Rights. (1966). Retrieved September 12, 2024 from https://www.ohchr.org/sites/default/files/ccpr.pdf
37. International Covenant on Economic, Social and Cultural Rights. (1966). Retrieved September 12, 2024 from https://www.ohchr.org/sites/default/files/cescr.pdf
38. International Health Regulations (2005). Retrieved May 23, 2025 from https://iris.who.int/bitstream/handle/10665/246107/9789241580496-eng.pdf
39. OHCHR. (2011). International legal protection of human rights in armed conflict. New York: United Nations. Retrieved November 17, 2024 from https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf

40. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1). (1977). Retrieved November 14, 2024 from https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf
41. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II). (1977). Retrieved November 14, 2024 from https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf
42. Resolution 2341. (2017). Adopted by the Security Council at its 7882nd meeting on 13 February 2017. Retrieved November 15, 2024 from https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf
43. Rome Statute of the International Criminal Court. (1998). Retrieved November 19, 2024 from https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf
44. Saint Petersburg Declaration. (1868). Retrieved November 16, 2024 from https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868
45. United Nations Charter. (1945). Retrieved September 12, 2024 from https://www.un.org/en/about-us/un-charter/full-text
46. United nations office of Counter-Terrorism; United nations security council Counter-Terrorism Committee Executive Directorate (CTED); INTERPOL. (2022) The Protection of Critical Infrastructure Against Terrorist Attacks, Compendium of Good Practices 2022 Update. Retrieved November 16, 2024 from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf
47. Universal Declaration of Human Rights. (1948). Retrieved September 12, 2024 from https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

F) Websites

48. Aydogan, M. (2024). Ransomware attacks on hospitals are 'issues of life and death,' warns WHO chief. *Anadolu Ajansi*. Retrieved November 10, 2024 from https://www.aa.com.tr/en/world/ransomware-attacks-on-hospitals-are-issues-of-life-and-death-warns-who-chief/3388792
49. Cimpanu, C. (2018). CenturyLink outage takes down several 911 emergency services across the US. *ZDNET*. Retrieved November 12, 2024 from https://www.zdnet.com/article/centurylink-outage-takes-down-several-911-emergency-services-across-the-us/
50. Council of Europe. (n.d). What are human rights?. *Council of Europe*. Retrieved June 6, 2025 from https://www.coe.int/en/web/portal/what-are-human-rights
51. Cyberpolicy. (n.d.). Why Medical Records are 10 Times More Valuable Than Credit Card Info. *Cyberpolicy*. Retrieved May 23, 2025 from https://www.cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info
52. Fortinet. (n.d). "Types Of Cyber Attacks". *Fortinet*. Retrieved May 20, 2025 from https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

53. Humer, C.; & Finkle, J. (2014). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved May 23, 2025 from https://www.reuters.com/article/technology/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I/;
54. ICRC. (n.d). Human Rights applicable in armed conflicts. *casebook.icrc*. Retrieved May 20, 2025 from https://casebook.icrc.org/a_to_z/glossary/human-rights-applicable-armed-conflicts
55. Kumar, N. (2024). How Many IoT Devices Are There (2025-2030 Data). *Demandsage*. Retrieved May 20, 2025 from https://www.demandsage.com/number-of-iot-devices/
56. Martin, G.; Martin, P.; Hankin, C.; Darzi, A.; & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ*. Retrieved November 20, 2024 from https://www.bmj.com/content/358/bmj.j3179
57. OHCHR. (2023). Special Rapporteur on the Right to Health Says Digital Innovation Has Strengthened the Right to Health for Some, but Warns it Could Enable Violations and Undermine this Right. *OHCR*. Retrieved November 5, 2023 from https://www.ohchr.org/en/news/2023/06/special-rapporteur-right-health-says-digital-innovation-has-strengthened-right-health.
58. OHCHR. (n.d). What are human rights?. *United Nations*. Retrieved June 6, 2025 from https://www.ohchr.org/en/what-are-human-rights#:~:text=Human%20rights%20are%20rights%20we,of%20international%20human%20rights%20law
59. Rojas, R.; McGee, J.; Lee. E.; & Cavendish, S. (2020). When Nashville Bombing Hit a Telecom Hub, the Ripples Reached Far Beyond. *New York Times*. Retrieved June 5, 2023 from https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html
60. The United Nations Office at Geneva. (2024). Cyberattacks on healthcare: A global threat that can't be ignored. *UNGENEVA*. Retrieved November 10, 2024 from https://www.ungeneva.org/en/news-media/news/2024/11/100103/cyberattacks-healthcare-global-threat-cant-be-ignored
61. Zabel, L. (2014). The Value of Personal Medical Information: Protecting Against Data Breaches. *National Association of Healthcare Access Management (naham).* Retrieved May 23, 2025 from https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information