Legal Research, Vol 28, Issue 112, 2025: 1-22 Print ISSN: 1024-0772 Online ISSN: 3060-5911

Journal of Legal Research
https://lawresearchmagazine.sbu.ac.ir/

Orginal Article

Assaults on Critical Infrastructure and International Law

Ebrahim Beigzadeh[1]

Highlights

- Assaults (attack or disruption) on Critical Infrastructure, whether carried out in peacetime or during armed conflict, can seriously endanger the lives of civilians.
- Sometimes, governments also attack on critical infrastructure of neighboring countries by carrying out construction within their own territory.
- Some of assaults include the implementation of the Gap project by Türkiye and the construction of dams on the Harirud River and Helmand River by Afghanistan which has caused extensive damage to the infrastructure of Syria, Iraq, and Iran.

ABSTRACT

Introduction

Although assaults on critical infrastructure are not a new phenomenon, their occurrence has seen a significant rise in recent years. They might be deliberate, manifested as military attacks or intentional disruption, or unintentional, in the form of natural or technical disasters. In either case, they lead to catastrophic consequences, in particular for civilians, and in some situations may amount to international crimes such as forced displacement or even the deprivation of lives. Given these grave consequences, the current study addresses the main question of whether international law already contains rules prohibiting attacks on critical infrastructure or not**.** Since such attacks may take place during both armed conflict and peacetime, relevant international regulations must be examined in both contexts. It is also to be noted that, along with physical assaults, cyber operations can similarly target critical infrastructures.

Methods

To answer this question, the first issue to consider is whether international law provides a definition of critical infrastructure. The research hypothesis is that, despite the absence of a treaty-based definition, a customary one may be inferred from states practice and the positions of international organizations. Moreover, the prohibition of attacks on critical infrastructures in armed conflicts is confirmed by the principles of international humanitarian law—specifically the *principle of distinction*. This prohibition, though somewhat implicit, is also relevant in peacetime, since such acts may entail violations of the right to life, a fundamental human right.

Results and Discussions

The findings of the study confirm the research hypothesis that a customary definition of critical infrastructure can be identified under international law, and that attacks on such infrastructure are, in fact, prohibited during armed conflict and in times of peace. The international community has recently started

How to Cite: Beigzadeh, Ebrahim,"Assaults on Critical Infrastructure and International Law", Legal Research, Vol. 28, No. 112, 2025, pp:1-22.

DOI: https://doi.org/10.48308/jlr.2025.241688.2965 Received: 27/09/2025-Accepted: 30/09/2025

1. Professor of International Law, Faculty of Law, Shahid Beheshti University, Tehran, Iran
Corresponding Author Email: ebeigzadeh55@gmail.com

taking action to reinforce this prohibition by recognizing attacks on critical infrastructure as international crimes (specifically, war crimes), though this recognition is currently confined to armed conflict. In this regard, reference is to be made to the two arrest warrants issued by the International Criminal Court (ICC) against the Russian military authorities for their actions during the war against Ukraine. These warrants were issued as a result of the attacks on Ukraine's critical infrastructures, which the ICC recognized as constituting war crimes. Although this represents an initial step, limited to the prosecution of attacks on critical infrastructures in armed conflicts, it should be regarded as a positive development, demonstrating that the international community has finally taken appropriate measures to uphold justice and address impunity.

Conclusion

Nevertheless, while the definition of critical infrastructure and the rules prohibiting attacks on it are reasonably clear, international law provides no explicit regulation concerning state construction projects that cause severe disruption to the critical infrastructure of neighboring states. For instance, Turkey's construction of more than twenty dams and nineteen hydroelectric plants on the Tigris and Euphrates Rivers has significantly impaired the infrastructure of Syria, Iraq, and even Iran. According to the treaties concluded between Turkey and Syria on the one hand, and Turkey and Iraq on the other, a specific volume of water is required to flow into these two countries (i.e., Syria and Iraq). However, due to Turkey's activities, the actual amount of water entering their territories has reportedly been reduced to one-tenth of the agreed quantity. It appears that the construction projects undertaken by Turkey have served multiple purposes simultaneously. Indeed, Turkey has not only sought to render the neighboring countries dependent upon it for access to freshwater resources and thereby establish a form of regional hegemony, but has also aimed to disperse opposing Kurdish populations by submerging their villages and residential areas. Furthermore, as a result of these projects, many areas have been inundated by the lakes formed behind the dams. These submerged regions were once the sites of great ancient civilizations and contain archaeological artifacts far older than those of the Ottoman era. By constructing these dams, Turkey has, in effect, contributed to the destruction of these relics, seemingly in an attempt to assert that the Ottoman civilization represents the earliest and most significant civilization in the region. Similarly, Afghanistan's dam projects on the Helmand and Harirud Rivers have seriously disrupted infrastructure in Iran's Sistan and Baluchestan and Khorasan Razavi provinces. By constructing a dam on the Hirmand River and preventing the flow of water into Iran- contrary to the provisions of the 1972 treaty between Iran and Afghanistan- Afghanistan has caused the drying up of the Hamun region of Iran, which lies downstream of the river. These actions have resulted in the displacement and forced migration of thousands of Iranian citizens, residing in that area. Additionally, the construction of a dam on the Harirud River by Afghanistan has severely disrupted the drinking water supply infrastructure of the city of Mashhad in Iran. These situations call for further research into how international law might address such state activities—beyond the mere requirement of consultation—in order to prevent serious harm to neighboring states' critical infrastructure.

KeyWords: Critical Infrastructure; Armed Conflicts; Individual International Criminal Responsibility.

فصلنامه تحقیقات حقوقی
https://lawresearchmagazine.sbu.ac.ir/

مقاله علمی-پژوهشی

تعرض به زیرساخت‌های حیاتی و حقوق بین‌الملل

ابراهیم بیگ‌زاده[1]

نکات برجسته

- تعرض (حمله یا اختلال) به زیرساخت‌های حیاتی که هم در زمان صلح و هم در هنگام مخاصمات مسلحانه انجام می‌شود، می‌تواند حیات مردم غیرنظامی را با خطر جدی مواجه کند.
- گاهی دولت‌ها با انجام ساخت و سازهایی درون سرزمین خود به زیرساخت‌های حیاتی کشورهای همجوار نیز تعرض می‌نمایند.
- از جمله تعرض‌ها، اجرای طرح گاپ توسط ترکیه و ساخت سد روی رودخانه‌های هریرود و هیرمند توسط افغانستان است که خسارات فراوانی را به زیرساخت‌های کشورهای سوریه، عراق و ایران وارد کرده‌است.

چکیده

تعرض (حمله یا اختلال) به زیرساخت‌های حیاتی که به‌شدت روبه افزونی گذاشته است، می‌تواند ارادی یا غیرارادی باشد. تعرض به آنها آثار مخربی به‌ویژه برای غیرنظامیان دارد و ممکن است منجر به ارتکاب جنایت‌های بین‌المللی یا حتی سلب حیات آنان گردد. این تحقیق به‌دنبال پاسخ به این سؤال اصلی است که آیا حقوق بین‌الملل قواعدی برای ممنوعیت تعرض به این زیرساخت‌ها دارد؟ تعرض ارادی به زیرساخت‌های حیاتی هم در مخاصمات مسلحانه و هم در زمان صلح رخ می‌دهد؛ لذا مقررات بین‌المللی در هر دو حالت بررسی می‌شوند؛ ضمن آنکه در حال حاضر تعرض به زیرساخت‌های حیاتی از فضای سایبری نیز انجام می‌شود. برای پاسخ به سؤال اصلی باید تعریفی از زیرساخت حیاتی ارائه نمود. فرضیه بر آن است که می‌توان به یک تعریف عرفی از زیرساخت‌های حیاتی و همچنین ممنوعیت تعرض به آنها در مخاصمات مسلحانه و در زمان صلح دست یافت. تحقیق حاضر با بهره‌گیری از روش دگماتیک و تحلیلی، صحت فرضیه فوق را تأیید می‌کند. تضمین عدم رعایت ممنوعیت تعرض به زیرساخت‌های حیاتی هم واکنش جامعه بین‌المللی است که اخیراً در قالب لحاظ نمودن آن به‌عنوان جنایت جنگی بروز نموده است. اگرچه تعریف و ممنوعیت تعرض به زیرساخت‌های حیاتی در حقوق بین‌الملل تقریباً روشن است، اما نمی‌توان قواعد شفافی را درمورد اقدام‌های دولت‌هایی یافت که با ساخت‌وسازهای خود سبب ایجاد اختلال شدید در زیرساخت‌های حیاتی دولت‌های هم‌جوار خود می‌شوند.

کلید واژگان: زیرساخت حیاتی، مخاصمات مسلحانه، مسئولیت کیفری بین المللی فردی.

استناد به این مقاله: بیگ‌زاده، ابراهیم، «تعرض به زیرساخت‌های حیاتی و حقوق بین‌الملل»، فصلنامه تحقیقات حقوقی، دوره ۲۸، شماره ۱۱۲، دی ۱۴۰۴، صص:۱-۲۲.

DOI: https://doi.org/10.48308/jlr.2025.241688.2965 تاریخ دریافت: ۱۴۰۴/۰۷/۰۵ - تاریخ پذیرش: ۱۴۰۴/۰۷/۰۸

۱. استاد حقوق بین‌الملل، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران
ایمیل نویسنده مسئول: ebeigzadeh55@gmail.com

مقدمه

تعرض (حمله یا اختلال) به زیر ساخت‌های حیاتی[۱] پدیده جدیدی نیست.[۲] باوجود این، این نوع تعرض در عصر حاضر چه در زمان صلح و چه در هنگامه مخاصمات مسلحانه ابعاد گسترده‌ای به خود گرفته است. اگرچه تخریب یا اختلال در زیرساخت‌های حیاتی گاهی می‌توانند ناشی از بلایای طبیعی و غیرارادی یا فنی باشند،[۳] تخریب یا اختلال در آنها اغلب به‌صورت ارادی انجام می‌شوند.

تخریب یا اختلال در زیر ساخت‌های حیاتی نه‌فقط موجب آسیب به آنها می‌شود، بلکه آنچه مهم می‌نماید سبب می‌شود خدماتی که به‌طور عمده برای غیرنظامیان جنبه حیاتی دارند، دچار آسیب شده، از بین بروند یا حداقل برای مدت کم‌وبیش قابل‌توجهی از دسترس خارج شوند. امروزه باید بر تخریب یا اختلال در زیرساخت‌های حیاتی از طریق فضای فیزیکی، تخریب یا ایجاد اختلال در آنها از طریق اقدام‌های تروریستی و حملات سایبری را نیز افزود که هر روز در حال گسترش بیشتری هستند.[۴و۵] برای نمونه حملات تروریستی بر ضد خط لوله گازی زیر دریایی نورد استریم در سال ۲۰۲۲ است که منجر به خسارات فراوانی گردید. همچنین می‌توان به وارد کردن بدافزار استاکس نت[۶] در نیروگاه اتمی نطنز ایران ازسوی آمریکا و رژیم اشغالگر اسرائیل اشاره کرد که خسارات سنگینی به سانتریفیوژها این نیروگاه وارد نمود. نکته جالب آنکه این حمله فقط محدود به نیروگاه نطنز باقی نماند، بلکه در سراسر جهان پخش و موجب آلوده شدن صدها هزار دستگاه رایانه شد.[۷] بالاخره از باب نمونه می‌توان به خراب‌کاری در خطوط گازرسانی ایران توسط رژیم اشغالگر اسرائیل اشاره کرد که سبب بروز مشکلات فراوان ازجمله برق‌رسانی به مردم گردیده است.[۸] با توجه به خطرات جدی که

---

۱. برای اصطلاح زیرساخت حیاتی در زبان انگلیسی اغلب عبارت Critical Infrastructure و در زبان فرانسوی عبارت Infrastructure Essentielle یا Infrastructure Critique یا Infrastructure Vitale استفاده می شود. با توجه به اهمیت زیرساخت ها در زندگانی و حیات به‌ویژه غیرنظامیان در این مقاله از اصطلاح «زیرساخت حیاتی» استفاده شده است.

۲. برخی معتقدند که تعرض به زیرساخت‌های حیاتی به دوران عهد عتیق بازمی‌گردد. برای مطالعه بیشتر رجوع شود به
Newbill C. M.“ Defining Critical Infrastructures for a global application”, *Indiana Journal for a Global Studies*, Volume 26, Issue 2, 2019, P 765; cite par : Bannelier, Karine, “Le droit International face a la destruction ou la perturbation des infrastructures essentielles des Etats”, *Annuaire Français de Droit International (A.F.D.I),* Volume LXIX, 2023, P 229 l.

۳. نمونه بارز بلایای طبیعی که منجر به تخریب زیرساخت های حیاتی گردیدند، می‌توان به سونامی سال ۲۰۱۱ در ژاپن اشاره نمود که منجر به تخریب نیروگاه اتمی فوکوشیما شد.
درخصوص بلایای فنی و تکنولوژیکی بارزترین نمونه انفجار نیروگاه اتمی چرنوبیل در سال ۱۹۸۶ در شوروی سابق است.
در این مقاله توجه و تأکید بر تعرض عمدی و ارادی به زیرساخت‌های حیاتی است.

۴. برای مطالعه بیشتر درمورد اقدام‌های تروریستی برای تخریب یا اختلال در زیرساخت‌های حیاتی رجوع شود به:
ONU, Bureau de Lutte Contrele Terrorisme. “La protection des infrastructures critiques contre les attaques terrorists, Recueil de bonne pratique”, 176 Pages.

۵. گزارش منتشره از سوی آژانس بین‌المللی انرژی (Agence International d’Energie) اعلام کرده است که میانگین حملات سایبری بر ضد شبکه‌های برق در دنیا در هر هفته بین سال‌های ۲۰۲۰ تا ۲۰۲۲ به بیش از دو برابر افزایش یافته است؛ به طوری که در سال ۲۰۲۲ حدود ۱۱۰۱ حمله هفتگی به ثبت رسیده است.
Casanovas M. and Aloys gheim. “Cybersecurity –is the power System logging behind? ” *IEA*, In: Jack.V, “Europe’s grid is under a Cyberattack deluge, industry warns”, *Politico*, 2023, Cite Par: Bannelier, Op. Cit., P 227.

6. Stuxnet

7. Bannelier, Op.Cit.

۸. رجوع شود به اظهارات وزیر نیرو در مجلس شورای اسلامی به تاریخ ۱۱ شهریور ۱۴۰۴ در پاسخ به سؤال نمایندگان در مورد علل خاموشی‌ها و قطع برق.

در اثر تخریب یا ایجاد اختلال در زیر ساخت‌های حیاتی به‌ویژه برای مردم غیرنظامی ایجاد می‌شوند، سؤالی که مطرح می‌شود این است که اولاً چه زیرساخت‌هایی «حیاتی» محسوب می‌شوند و آیا معیارهایی برای شناسایی آنها وجود دارند؟ ثانیاً موضع حقوق بین‌الملل در قبال تعرض به زیرساخت‌های حیاتی در هنگامه مخاصمات مسلحانه و در زمان صلح چیست؟ فرضیه اصلی در این نوشتار آن است که باوجود نبود یک تعریف معاهداتی جهان‌شمول، می‌توان به‌لحاظ عرفی معیارهایی استخراج نمود که تا حدودی امکان تعریف زیرساخت‌های حیاتی را مشخص می‌کنند؛ ضمن آنکه مقررات حقوق بین‌الملل این امکان را می‌دهد که بتوان حمله به زیرساخت‌های حیاتی را ممنوع اعلام کرد؛ ممنوعیتی که عدم رعایت آن مسئولیت کیفری فردی به‌همراه خواهد داشت.

بنابراین در این نوشتار سعی بر آن است که ابتدا تعریفی از زیرساخت حیاتی باتوجه‌به معیارهای مستخرج از عرف ارائه شود، سپس ممنوعیت تعرض به آنها در هنگامه مخاصمات مسلحانه و در زمان صلح مورد واکاوی قرار گیرد و سرانجام ضمانت اجرای عدم رعایت ممنوعیت تعرض به این زیرساخت‌ها بررسی شود.

۱. تعریف زیرساخت حیاتی

برای حفظ امنیت و تاب‌آوری[1] زیر ساخت‌های حیاتی در قبال حمله یا ایجاد اختلال، نیاز است که ابتدا تعریفی از آنها ارائه شود. این تعریف به‌ویژه از لحاظ حقوقی حائز اهمیت است؛ زیرا امکان می‌دهد سهل‌تر بتوان تعرض به آنها را شناسایی و به‌عنوان نقض قواعد حقوق بین‌الملل مطرح نمود. بررسی‌ها نشان می‌دهند که دولت‌ها از پذیرش یک تعریف معاهداتی جهان‌شمول طفره می‌روند؛ پدیده‌ای که سبب می‌شود تا باتوجه‌به عرف روشن کرد که آیا می‌توان به یک تعریف عرفی از زیرساخت‌های حیاتی دست یافت؟

۱.۱. نبود تعریف معاهداتی جهان‌شمول از زیرساخت‌های حیاتی

مطالعات نشان می‌دهند که کنسانسوسی در سطح جهانی برای تعریف زیرساخت حیاتی در یک معاهده بین‌المللی فراگیر (جهان‌شمول) وجود ندارد. علل متعددی وجود دارند که مانع پذیرش تعریفی از این زیرساخت‌ها در یک سند فراگیر می‌شوند: اولاً دولت‌ها می‌خواهند اولویت و اقتدار خود را در تعیین آنها از دست ندهند؛[2] ثانیاً این اعتقاد راسخ را نیز دارند که تعریفی از زیرساخت‌های حیاتی و تعیین مصادیق آنها موجب می‌شود که آن زیر ساخت‌ها به‌راحتی آماج حملات، خراب‌کاری یا اخلالگری قرار گیرند، یا آنکه زیرساخت‌هایی که در یک سند مشخص نشده‌اند، «حیاتی» محسوب نشده، مورد تعرض قرار گیرند. ضمن آنکه این علت هم مطرح می‌شود که این زیرساخت‌ها از کشوری به کشور دیگر و از زمانی به زمان دیگر متفاوت و متغیرند. اگرچه برخی مجامع بین‌المللی در مصوبه‌های خود در قلمروهای خاصی به‌ویژه درخصوص امنیت سایبری به زیرساخت‌های حیاتی هم گوشه چشمی انداخته‌اند،[3] این مصوبه‌ها باوجود اشاره به‌ضرورت حفاظت از

---

1. Resilience
2. Bannelier, Op.Cit., P 229.
3. رجوع شود به:

قطعنامه ۵۸/۱۹۹ مجمع عمومی سازمان ملل متحد مورخ ۲۳ دسامبر ۲۰۰۳ تحت عنوان «ایجاد یک فرهنگ جهانی امنیت سایبری و حفاظت از زیرساخت‌های حیاتی اطلاعاتی». S/RES/58/199

– قطعنامه ۲۳۴۱ شورای امنیت مورخ ۱۳ فوریه ۲۰۱۷ درخصوص «حفاظت از زیرساخت های حیاتی در مقابل حملات تروریستی».

همان‌طور که ملاحظه می‌شود در این مصوبه‌ها قلمروهای خاصی مورد توجه قرار گرفته‌اند.

زیرساخت‌های حیاتی، تعریف جهان‌شمولی از آنها ارائه نمی‌کنند. در ضمن دولت‌ها پاسخ مساعدی حتی به فراخوان‌های بین‌المللی برای تعریف زیرساخت‌های حیاتی حتی در قلمروهای خاص هم نداده‌اند.[۱] اگرچه در سطوح منطقه‌ای و آن‌هم اغلب در قلمروهای خاص تلاش‌هایی برای ارائه تعریفی از زیرساخت‌های حیاتی شده است،[۲] خلأ یک تعریف معاهداتی جهان‌شمول همچنان تداوم دارد. در چنین وضعیتی است که باید به سراغ حقوق عرفی به‌ویژه مقررات و عملکرد دولت‌ها رفت و دید که آیا می‌توان به تعریفی از زیرساخت‌های حیاتی دست یافت؟

۱.۲. تعریف عرفی زیرساخت‌های حیاتی

نیک می‌دانیم که برای دستیابی به عرف بین‌الملل یکی از متداول‌ترین شیوه‌ها رجوع به رویه دولت‌هاست که در قالب قوانین و مقررات و عملکرد آنها قابل شناسایی است. بنابراین باید به عملکرد دولت‌ها برای دستیابی به تعریفی از زیرساخت‌های حیاتی پرداخت؛ ضمن آنکه در این نوشتار به رویه برخی از سازمان‌های با صلاحیت خاص و سازمان‌های منطقه‌ای نیز توجه شده است. از اولین کشورهایی که در زمینه تعیین زیرساخت‌های حیاتی گام برداشته است، می‌توان به ایالات متحد آمریکا اشاره نمود. این کشور با ایجاد کمیسیونی برای حمایت و حفاظت از زیرساخت‌های حیاتی[۳] در سال ۱۹۹۶ کار را در این زمینه آغاز نمود.[۴] آمریکا همچنین برای حفاظت از زیرساخت‌های حیاتی خود در برابر حملات سایبری قانونی در ۱۵ مارس ۲۰۲۲ توسط رئیس‌جمهور، جو بایدن، منتشر نمود که بخش y آن به حملات سایبری بر ضد زیرساخت‌های حیاتی آمریکا اختصاص یافته است. طبق این مقرره جدید، کلیه نهادهای آمریکایی مرتبط با زیرساخت‌های حیاتی کشور مکلف‌اند حملات سایبری را بدون فوت وقت به «نهاد امنیت سایبری»[۵] اطلاع دهند؛ تکلیفی که برای آن ضمانت اجرا هم لحاظ شده است.[۶] از منظر مقررات آمریکا، زیرساخت حیاتی شامل «کلیه سیستم‌ها و اموال اعم از مادی و مجازی می‌شود که اختلال یا تخریب هریک از آنها روی امنیت اقتصاد ملی، امنیت سلامت عمومی یا ایمنی یا مجموعه آنها اثر می‌گذارد».[۷]

---

۱. در این مورد برای مثال می‌توان به فراخوان پاریس در نوامبر ۲۰۲۳ اشاره نمود.

Appel de Paris pour la confiance et la securite dans le Cyberspace. “protecting critical Infrastructures against Systemic harms: A path forward to overcome national discrepancies?” November 2023.

۲. در این مورد می توان به کارهای اتحادیه اروپا و اتحادیه آفریقا اشاره نمود که در همین مقاله به آنها توجه خواهد شد.

3. Commission on critical Infrastructures protections, “Defense critical infrastructures programme”, 1996.

4. Policy Directive 21 (Critical infrastructures security and resilience), 2013.

5. Cybersecurity and Infrastructures Security Agency (C I S A).

6. Consolidated Appropriations Act, 2022, HR, 2471, March 15, 2022.

طبق این قانون کلیه نهادهای دولتی، دفاتر، شرکت ها، عاملان و کاربران زیرساخت های حیاتی باید ظرف ۲۴ ساعت از زمان اطلاع از حمله سایبری به زیرساخت ها، مراتب را به آژانس امنیت سایبری زیرساخت ها اطلاع دهند. عدم رعایت این مقرره موجب جریمه‌هایی می‌شود که می‌تواند از ۰.۵٪ (نیم درصد) درآمد ناخالص سال قبل آن شرکت برای هر روز نقض که تداوم یابد لحاظ شود. برای شرکت‌هایی که همچنان از اطلاع‌رسانی امتناع کنند، مجوز فدرال آنها هم لغو می‌شود.

۷. رجوع شود به:

Critical Foundations protecting America’s Infrastructures, ‘’The Report of President’s Commission on Critical Infrastructure Protection’’, October 1997, 192 pages.

اگرچه این تعریف کوتاه می نماید، اشاره آن به سیستم‌ها و اموال مادی و مجازی امکان لحاظ نمودن زیرساخت‌های حیاتی زیادی را می‌دهد. به همین دلیل هم بر اساس این تعریف، آژانس امنیت سایبری و امنیت زیرساخت ها شانزده زیرساخت حیاتی را مشخص نموده است.

رجوع شود به

Haataja, S. I. “Cyber operations against critical infrastructures under norms of responsibility state behaviour and international Law, International”, *Journal of Law and Information Technology*, Volume 30, 2022, PP 2126-427, cite par: Bannelier, Op.Cit., P 230.

در ایران هم به زیرساخت‌های حیاتی توجه شده‌است. حمایت و حفاظت از این زیرساخت‌ها به‌طور عمده و دقیق در مقررات مرتبط با سازمان پدافند غیرعامل مورد توجه قرار گرفته است. ابتدا قانون ایجاد سازمان پدافند غیرعامل[۱] است که در آن یکی از اهداف مورد نظر "مقاوم سازی زیرساخت‌های حیاتی و حساس و مهم کشور است". در راستای تحقق این هدف تبصره ۳ همین قانون کلیه دستگاه‌های موضوع این قانون را مکلف نموده‌است که در طرح تملک سرمایه‌ای خود اعتبارات لازم را برای پیشگیری و مقابله با تهدیدات زیرساخت‌های حیاتی، حساس و مهم خود تخصیص دهند. البته اسناد دیگری هم وجود دارند که به زیرساخت‌های حیاتی کشور توجه نموده‌اند[۲] که در میان آنها اساس‌نامه سازمان پدافند غیرعامل[۳] و به‌ویژه مصوبه‌های کمیته دائمی[۴] آن بسیار حائز اهمیت‌اند.

اساسنامه این سازمان در ماده ۲ (بند ۸) فقط به زیرساخت‌های با اهمیت اشاره‌کرده، آنها را شامل «زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت» تقسیم نموده است. مع‌هذا این مقرره تعریفی از زیرساخت ارائه نمی‌کند. این تعریف را می‌توان در مصوبه کمیته دائمی سازمان یافت که طبق آن «زیرساخت به مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند، اطلاق می‌گردد».[۵]

در چارچوب بررسی مقررات داخلی کشورها درخصوص زیرساخت‌های حیاتی می‌توان برای مثال به مقررات کشور فرانسه نیز اشاره نمود. در این کشور و در چارچوب مراقبت از منافع حیاتی، بخشنامه‌ای در سال ۲۰۰۲ تصویب شده است که طبق ماده ۲ بند ۵ آن برای تضمین عملکرد مناسب «زیرساخت‌های حیاتی در برابر فعالیت‌های تروریستی، امنیت اقتصادی، مقابله با بلایای طبیعی و تکنولوژیکی» از وزارت اقتصاد خواسته شده است تا با هماهنگی سایر نهادهای مرتبط تدابیر ضروری قانونی و اداری را ارائه نماید.[۶] این کشور سپس در ۲۳ فوریه ۲۰۰۶ با تصویب فرمانی زیرساخت‌های با اهمیت حیاتی (اعم از عمومی و خصوصی) را که کارکردشان به‌سختی قابل جایگزینی است، شامل زیرساخت‌های مرتبط

---

۱. قانون سازمان پدافند غیرعامل در ۲۹ مرداد ۱۴۰۲ در قالب یک ماده واحده و ۴ تبصره به تصویب مجلس رسید و در یکم شهریور ۱۴۰۲ مورد تأیید شورای نگهبان قرار گرفت.

۲. طبق ماده ۵ تصویب‌نامه کمیته دائمی سازمان پدافند غیرعامل مورخ ۱۴۰۲/۰۸/۰۱، اسناد بالادستی و مرتبط با زیرساخت‌ها شامل:

– فرامین رهبری و تدابیر و مصوبات رهبری.

– سیاست‌های کلی نظام در موضوع پدافند غیرعامل و آمایش سرزمین.

– قانون احکام دائمی برنامه‌های توسعه کشور (ماده ۵۶).

– قانون پنج‌ساله ششم توسعه ج–ا– ایران (ماده ۱۰۶ بند پ).

– ماده ۲۹ قانون پنج‌ساله توسعه اقتصادی، اجتماعی و فرهنگی مصوب ۱۴ اسفند ماه ۱۳۹۵.

– سیاست‌های کلی برنامه پنج‌ساله توسعه ج–ا– ایران بند ۲۴.

– ماده ۵ قانون مدیریت خدمات کشوری مصوب ۸ مهر ماه ۱۳۸۶.

– طرح راهبردی حفاظت از زیرساخت‌های کشور مصوب ۲۰ مهر ماه ۱۴۰۱ کمیته دائمی سازمان پدافند غیرعامل.

– آیین‌نامه اجرایی ماده ۳۴ قانون احکام دائمی برنامه‌های توسعه کشور مصوب ۵ اسفند ماه ۱۴۰۰.

۳. اساسنامه سازمان پدافند غیرعامل در ۳۰ ماده و ۲۲ تبصره در تاریخ اول مرداد ۱۴۰۳ به تصویب رهبری رسیده، از تاریخ ۱۹ دی ماه ۱۴۰۳ (تاریخ ابلاغ) لازم‌الاجرا شده است. تفسیر اساسنامه سازمان برعهده ستاد کل نیروهای مسلح ایران است.

۴. سازمان پدافند غیرعامل شامل یک کمیته دائمی، رئیس سازمان (به‌عنوان دبیر نیز هست)، کارگروه پدافند غیرعامل دستگاه‌های اجرایی و استان‌های کشور است.

۵. رجوع شود به «فرماندهی کل قوا» کمیته دائمی پدافند غیرعامل کشور به شماره ۱۶۰/۱/۲۹۲۲ مورخ اول آبان ماه ۱۴۰۲ در سایت مرکز پژوهش‌های مجلس، تاریخ رجوع شانزدهم مرداد ۱۴۰۴.

6. Para 2.5 du Circulaire du 14 Fevrier 2002 relative a la defense economique, J O R F, N○70 du 23 Mars 2002, Texte No10

با تولید و توزیع مایحتاج و ارائه خدمات ضروری برای رفع نیازهای اساسی مردم، اجرای اقتدارات و اختیارات دولت، حفظ عملکرد اقتصاد، حفظ قدرت دفاعی، امنیت ملت یا دارنده خطرات شدید برای مردم در نظر گرفته است.[۱] سرانجام فرانسه در ۲۳ مه ۲۰۱۸ در فرمانی را درمورد حفظ امنیت شبکه‌ها و سیستم‌های اطلاعاتی تصویب نموده است. این فرمان در ۳۳ ماده و یک ضمیمه به تصویب رسیده است. در این فرمان خدمات حیاتی برای عملکرد جامعه و اقتصاد مورد توجه قرار گرفته‌اند و آن شامل انرژی، حمل‌ونقل، لجستیک، بانک، زیرساخت‌های بازارهای مالی، خدمات مالی، بیمه، نهادهای تأمین اجتماعی، استخدام و آموزش کارکنان، سلامت، تولید و توزیع آب آشامیدنی، تصفیه آب‌های غیرقابل شرب، زیرساخت‌های دیجیتالی، آموزش، نهادهای تأمین‌کننده مواد غذایی برای نهادهای جمعی همچون مراکز درمانی، مدارس و زندان‌ها می‌شود.[۲] لازم به یادآوری که اغلب کشورها در قلمرو زیرساخت‌های حیاتی خود مقرراتی دارند که پرداختن به همه آنها در این نوشتار ممکن نیست.

علاوه‌بر مقررات داخلی، می‌توان به اقدام‌های برخی از سازمان‌های جهانی با صلاحیت خاص و همچنین سازمان‌های منطقه‌ای در قلمرو تعریف از زیرساخت‌های حیاتی اشاره کرد. درخصوص سازمان‌های با صلاحیت خاص که در قلمرو زیرساخت‌های حیاتی اقدام‌هایی انجام داده‌اند، می‌توان به اینترپل و سازمان همکاری و توسعه اقتصادی اشاره نمود. اینترپل ضمن تفکیک میان زیرساخت‌های حیاتی که ارائه‌کننده خدمات حیاتی‌اند و مراکز آسیب‌پذیر[۳] از دولت‌ها می‌خواهد تا ضمن اتخاذ راهبردهای ملی برای کاهش خطرات نسبت به زیرساخت‌های حیاتی و پیش بینی مسئولیت کیفری برای مرتکبان تعرض به آنها، با یکدیگر در قلمروهای مختلف ازجمله تبادل اطلاعات، تجارب و هماهنگ کردن فعالیت‌های نهادهای ملی همکاری کنند. اینترپل همچنین از دولت‌ها می‌خواهد که برای حفاظت از زیرساخت‌های حیاتی همکاری‌های بین‌المللی در قلمروهای مختلف[۴] را تقویت کنند.[۵]

سازمان همکاری و توسعه اقتصادی در سندی، دوازده توصیه برای حفاظت از زیرساخت‌های حیاتی اطلاعاتی و کامپیوتری و ارتباطی به دولت‌های عضو کرده است. سازمان در این سند اعلام می‌دارد که زیرساخت‌های حیاتی اطلاعاتی شامل

---

1. Voir l’ articl 1 du Decret N○2006-212 du 23 Fevrier 2006 relatif a la securite des activites d’ importance vitale, cite par : Bannelier, Op. Cit., P 230.

البته باید متذکر شد که این فرمان در ۲۴ آوریل ۲۰۰۷ به‌روزرسانی شده است. طبق این فرمان حدود سیصد زیرساخت (اپراتور) حیاتی لحاظ شده اند که فهرست آنها محرمانه است. این زیرساخت‌ها دوازده بخش از فعالیت‌ها را پوشش می‌دهند که شامل فعالیت‌های غیرنظامی دولت، فعالیت‌های قضایی، فعالیت‌های نظامی دولت، مواد غذایی، ارتباطات الکترونیکی سمعی و بصری و اطلاعاتی، انرژی، فضا و تحقیقات، مالی، مدیریت آب، صنعت، سلامت، حمل‌ونقل می‌شود.

2. Decret NO 2018-384 du 23 Mai 2018 relatif a la securite des reseaux et systemes d’ information des operateurs de services essentiels et des founisseurs de service numerique, J O R F , NO 0118 du 25 Mai 2018.

آخرین به‌روزرسانی این فرمان در تاریخ ۲۶ می ۲۰۱۸ انجام شده است.

۳. طبق نظر اینترپل دولت‌ها باید میان اماکن آسیب‌پذیر مثل مراکز تجاری، پیاده‌روها (بعد از حمله تروریستی به عابران پیاده در شهر نیس فرانسه با یک خودرو، بازارها یا استادیوم‌های ورزشی با زیرساخت‌های حیاتی که ارائه‌کننده خدمات عمومی برای همگان‌اند، مانند زیرساخت‌های انرژی قائل به تفکیک شوند.

۴. قلمروهای موردنظر اینترپل به‌طور مشخص شامل بخش‌های دریایی، حمل‌ونقل هوایی، فناوری اطلاعاتی، تسلیحات کلاسیک، شیمیایی، بیولوژیکی، رادیولوژیکی و هسته‌ای می‌شود.

۵. برای مطالعه بیشتر درمورد گزارش اینترپل رجوع شود به:

INTERPOL, ‘’La protection des infrastructures critiques contre les attaques terrorists: Recueil de bonnes pratiques)), Etabli par la Direction du Comite Contre le Terrorisme et le Bureau de Lutte Contre le Terrorisme, 2018, 176 pages.

سیستم‌ها و شبکه‌های اطلاعاتی متصل به یکدیگر می‌شوند که اختلال یا تخریب آنها می‌توانند تأثیر جدی مخربی بر سلامت، امنیت، ایمنی، شکوفایی اقتصادی شهروندان، ارتقای سطح زندگی، و بر عملکرد مؤثر دولت یا اقتصاد داشته باشد.[۱] همان‌گونه که مشاهده می‌شود، تأکید این سازمان بر حفاظت از زیرساخت‌های اطلاعاتی و ارتباطی است که تخریب یا اختلال در آنها می‌توانند به‌طور عمده بر اقتصاد و امنیت شهروندان و دولت‌ها اثرگذار باشد.

در سطوح منطقه‌ای می‌توان به مقررات و اقدام‌های اتحادیه اروپا و اتحادیه آفریقا اشاره نمود. در اروپا پارلمان و شورای اتحادیه اروپا مقررات مفصلی درمورد زیرساخت‌های حیاتی وضع کرده‌اند. این سازمان ابتدا مقرراتی برای حفاظت از زیرساخت‌های حیاتی اطلاعاتی مرتبط با بخش‌هایی را وضع نمود؛[۲] آنگاه با طرح اپراتورهای «خدمات حیاتی» مسئله حفاظت از زیرساخت‌های حیاتی را به کلیه نهادهای ارائه‌کننده خدمات حیاتی اجتماعی و اقتصادی گسترش داده است. از خلال اسناد و اقدام‌های زیادی که توسط اتحادیه اروپا تصویب و انجام شده‌اند، زیرساخت‌های حیاتی به مجموعه‌ای از تأسیسات و تجهیزاتی اطلاق می‌شود که نقش بنیادین در کارکرد جامعه داشته، اختلال یا تخریب آنها امنیت ملی و منافع اقتصادی و اجتماعی دولت را شکننده و آسیب‌پذیر می‌سازد.[۳] در تعریفی دیگر که در سال ۲۰۲۲ ارائه شده است، زیرساخت حیاتی بر هر سیستم اساسی حیاتی برای تضمین کارکرد اقتصادی و اجتماعی اطلاق می‌شود که عدم دسترسی یا تخریب یک زیرساخت حیاتی می‌تواند توان نظامی یا اقتصادی، امنیت یا امکان حیات و سلامت مردم را به‌طرز فاحشی با خطر مواجه کند[۴]. در چارچوب اتحادیه آفریقا وضعیت زیرساخت‌های حیاتی در قالب "کنوانسیون امنیت سایبری و

---

۱. سازمان همکاری و توسعه اقتصادی (O C D E) از دولت‌های عضو می‌خواهد که چارچوب مؤثر و کارآمدی را برای به اجرا گذاشتن اصول راهبردی سازمان برای حفظ امنیت زیرساخت‌های حیاتی از طریق ارزیابی خطرات تهدیدکننده عوامل زیر مشخص کنند:

– اجزا و عوامل اطلاعاتی که زیرساخت‌های حیاتی اطلاعاتی بر آنها استوارند.

– زیرساخت‌های اطلاعاتی که عوامل اصلی فعالیت‌های دولتی بر آنها قرار دارند.

– زیرساخت‌های اطلاعاتی حیاتی برای اقتصاد ملی.

برای مطالعه بیشتر رجوع شود به:

O C D E, ‘’ Recommandations du Conseil sur la Protection des Infrastructures d’ Information Critique’’, *Instrument Juridique de l’ O C D E*, 2025, 7 pages.

اولین دسته از توصیه‌ها در سال ۲۰۰۹ ارائه شده. سپس این توصیه‌ها در سال ۲۰۱۹ توسعه یافتند. در این توصیه‌ها شورای سازمان از دولت‌ها می‌خواهد که برای حفظ امنیت دیجیتالی در مقابل خطرات، یک رهیافت راهبردی جهت مدیریت این خطرها تدوین و ارائه نمایند. رجوع شود به:

-O E C D / LEGAL / 0361.

-O E C D / LEGAL / 0456.

2. Les infrastructures de l’ Union Europeenne et le probleme informatique de l’ an 2000, Les trimestre 1999, 31 pages.

در این سند زیرساخت‌های مهم برای اتحادیه اروپا عبارت از زیرساخت‌های انرژی، حمل و نقل، ارتباطات، هسته‌ای، مالی و آب هستند.

۳. برای مطالعه بیشتر در این مورد برای مثال رجوع شود به:

Tremblay, Monica.’’ Les infrastructures essentielles: un defi pour la securite des Etats’’, Rapport evolutif, Laboratoire d’ etude sur les politiques publiques et la mondialisation, ENAP, L’ Universite de l’ administration publique, 21 pages.

4. UE, Infrastructure Critique: L’ UE cherche a ameliorer leur securite, 28 Octobre 2022.

برای مطالعه بیشتر درمورد فعالیت‌های اتحادیه اروپا رجوع شود به:

Le Directive 2022/2554 du Parlement Europeen et du Conseil.

این دستورالعمل شامل:

-La resilience operationnelle numerique du secteur financier.

-Des mesures destinees a assurer un niveau eleve commun de cybersecurite dans l’ ensemble de l’ Union.

-Modifiant les directives 2009-2016 en ce qui concerne la resilience operationnelle numerique du secteur financier.

-La resilience des entites critiques et abrogeant la directive 2008/114/CE du Conseil.

حمایت از داده‌ها" مصوب ۲۷ ژوئن ۲۰۱۴ مورد توجه قرار گرفته است. طبق ماده یک این سند زیرساخت حیاتی فضای سایبری به آن دسته از زیرساخت‌هایی اطلاق می‌شود که برای ارائه خدمات مرتبط با امنیت عمومی، ثبات اقتصادی، امنیت ملی، ثبات بین‌المللی و برای تداوم و استقرار مجدد فضای سایبری حیاتی مورد استفاده قرار می‌گیرند و هر دولت عضو باید مقرراتی را تصویب یا تدابیری اتخاذ نماید که به نظرش برای شناسایی بخش‌های امنیت ملی و بهتر شدن اقتصادش ضروری‌اند.[۱] همان‌طور که ملاحظه می‌شود، این سند ضمن ارائه تعریف مختصری از زیرساخت حیاتی به زیرساخت‌های اطلاعاتی و آن هم فقط برای حفاظت از آنها در مقابل حملات سایبری توجه وافر نشان داده است. در همین راستا باید به فعالیت‌های «کارگروه کارشناسان دولتی مسئول بررسی پیشرفت‌های انفورماتیک و ارتباطات در چارچوب امنیت بین‌المللی» و همچنین به فراخوان پاریس اشاره نمود که چندان توأم با موفقیت نبودند.[۲و۳]

همان‌طور که ملاحظه می‌شود، اگرچه تعیین، تشخیص و در نهایت تعریف زیرساخت‌های حیاتی ناشی از ارزیابی‌هایی است که به‌صورت موردی و توسط هر دولت یا هر سازمانی انجام می‌شود، جملگی بر یک معیار اصلی اتفاق‌نظر دارند و آن «حیاتی بودن» آنهاست. به دیگر سخن زیرساخت‌هایی را می‌توان «حیاتی» محسوب نمود که تخریب یا اختلال در آنها می‌تواند حتی حیات یک جامعه را با خطر نابودی مواجه کند. بدیهی است که در این مورد ماهیت و وسیله و محیط انجام اعمالی برضد زیرساخت‌ها ملاک نیستند، بلکه ویژگی «حیاتی بودن» عملکرد زیرساخت‌هاست که باید مدنظر قرار گیرد که تعرض به آنها می‌تواند خطر جدی برای مردم یک جامعه ایجاد کند.[۴] حتی برای حیاتی محسوب کردن یک زیرساخت محل استقرار آن هم اهمیت چندانی ندارد و می‌تواند خارج از قلمرو یک سرزمین باشد، اما عملکرد آن برای حیات جامعه یا جوامعی ضروری و غیر قابل اجتناب باشد. نمونه بارز آن زیرساخت‌های ارتباطات اینترنتی است که در بسیاری از موارد از طریق فیبرهای نوری زیردریایی برقرار می‌شود که این کاملاً می‌توانند در مناطق دریایی چندین دولت یا حتی در دریای آزاد قرار داشته باشند. در ضمن باید به این نکته نیز توجه داشت که میان اغلب زیرساخت‌های حیاتی

---

[1]. Convention de l’ Union Africaine sur la cybersecurite et la protection des donnees a caractere personnel, EX.
CL/846 (XXV), 27 Juin 2014.
این کنوانسیون در ۳۸ ماده در تاریخ ۲۷ ژوئن ۲۰۱۴ در شهر مالابو (Malabo)، پایتخت کشور گینه استوایی (Guinee Equatoriale) به تصویب رسیده، از ۸ ژوئن ۲۰۲۳ لازم‌الاجرا شده است.

[2]. Groupe d’ Expert Gouvernementaux یا Group of Governmental Expert = G G E.
این کارگروه در راستای اجرای قطعنامه ۷۳/۲۶۶ مجمع عمومی سازمان ملل متحد ایجاد گردید. این نهاد متشکل از ۲۵ نفر در ظرفیت شخصی خود از سال ۲۰۱۹ فعالیت خود را آغاز نمود و گزارش نهایی خود را در سال ۲۰۲۱ به مجمع عمومی ارائه کرد. برای مطالعه گزارش این کارگروه رجوع شود به A/76/135 ۱۴مورخ جولای ۲۰۲۱ تحت عنوان:
Groupe of Gouvernmental Expert on Advancing Responsible State behaviour in cyberspace in the context of international security, General Assembly, United Nations, 26 pages.

[3]. درمورد فراخوان پاریس رجوع شود به:
Apple de Paris pour la confiance et la securite dans le cyberspace یا Paris call for Trust and security in cyberspace.
برای ملاحظه بیشتر کارهای فراخوان پاریس رجوع شود به:
-Multistakeholder participation at the UN, November 2021, 36 pages.
-Advancing International Cyber Norms: Multistakeholder Recommandations, November 2021, 48 pages.
-Working Group 5: Building a Cyberstability index, Executive Summary and Final Report, November 2021, 19 pages.
-Working Group 6 (WG) 6: Bringing concrete tools to the Paris Call Community, Report Securing I C T, Supply Chains, 2021, 43 pages.

[4]. ماهیت زیرساخت‌های حیاتی می‌تواند دولتی، عمومی یا خصوصی باشد.

وابستگی متقابل وجود دارد، به‌گونه‌ای که تخریب یا اختلال در یک زیرساخت می‌تواند به‌صورت زنجیره‌ای سبب تخریب یا اختلال در سایر زیرساخت‌های ضروری برای ارائه خدمات حیاتی گردد. برای مثال تخریب یک نیروگاه برق می‌تواند بسیاری از زیرساخت‌های حیاتی یا ارائه خدمات حیاتی را از دسترس خارج کند. از آن جمله می‌توان خارج از دسترس شدن خدمات‌درمانی، حمل و نقل، رساندن آب قابل شرب، رساندن مواد غذایی سالم، اینترنت، حمل و نقل (به‌خصوص دریایی و هوایی) اشاره نمود. اگرچه برخی از دولت‌ها با توجه به تشخیص خود دایر بر حیاتی بودن برخی زیرساخت‌ها آنها را حیاتی اعلام و معیارهایی هم برای تشخیص و تعیین آنها ارائه نموده‌اند، باوجود این، آنها نیز امکان گسترش زیرساخت‌های حیاتی را پیش‌بینی کرده‌اند.[۱] حوزه‌های مرتبط با زیرساخت‌های حیاتی را می‌توان در برخی قوانین داخلی کشورها نیز مشاهده نمود.[۲]

باتوجه‌به مطالب پیش‌گفته به نظر می‌رسد بتوان «زیرساخت حیاتی» را این‌گونه تعریف کرد: زیرساخت‌های حیاتی شامل آن دسته از تأسیسات و تجهیزات و اموال و دارایی‌هایی می‌شوند که برای تأمین، تضمین، ارائه و رفع نیازهای اساسی مردم ضروری‌اند، تخریب یا اختلال جدی در کارکرد آنها موجب ورود خسارات اغلب جبران‌ناپذیر و حتی به خطر افتادن حیات آنان می‌گردد.

همان‌گونه که مشاهده می‌شود، تلاش شده که این تعریف بر معیار «حیاتی بودن» زیرساخت‌ها که مورد قبول تمام کشورها و سازمان‌هاست، ارائه گردد.

---

۱. نمونه بارز آن کشور ایران است. کمیته دائمی سازمان پدافند غیرعامل ۱۵ حوزه را با اهمیت اعلام نموده است که شامل این حوزه‌هاست:
– انرژی، آب، کشاورزی، حمل و نقل، بهداشت و سلامت، دفاع و امنیت، صنعت، رسانه، هسته‌ای، فضا، جمعیت، حاکمیتی، خدمات ضروری و فوریتی، پولی و مالی، ارتباطات و فناوری اطلاعات می‌شوند.
رجوع شود به ماده یک مصوبه کمیته دائمی سازمان پدافند غیرعامل مورخ آبان ماه ۱۴۰۲، ص ۲.
آنگاه این سازمان با تعیین معیارهای:
– اهمیت کارکرد هر حوزه در تأمین نیازهای حیاتی مردم در شرایط اضطراری، شدت اثرگذاری بر اقتصاد و امنیت ملی و سلامت مردم، وابستگی زیرساخت‌های سایر حوزه‌ها به عملکرد آنها، شدت پیامد وقوع تهدید مبتنی بر جغرافیا و جمعیت.
هشت حوزه را با اهمیت بالا و کلیدی لحاظ نموده است که شامل:
انرژی، آب، ارتباطات و فناوری اطلاعات، حمل و نقل، بهداشت و سلامت، غذا و کشاورزی، دفاعی و امنیتی، حاکمیتی می‌شوند.
کمیته دائمی در ماده ۶ مصوبه خود تحت عنوان تهدیدات مفروض ابتدا به تهدیدات نظامی (هوایی، زمینی، دریایی، موشکی)، تهدیدات امنیتی و تروریستی (اقدامات ضد زیرساختی تروریستی)، تهدیدات سایبری زیرساختی (تهدیدات زیرساختی سایبری علیه زیرساخت‌های هوشمند) و تهدیدات از درون دشمن پایه اشاره می‌کند. این ماده سپس در تبصره خود اعلام می‌دارد: «سایر تهدیدات نوین و نو پدید با منشأ دشمن و ترکیبی از آنها با هدف تخریب و اختلال در عملکرد زیرساخت‌ها که در آینده با آن مواجه خواهیم شد» را نیز شامل می‌شود.
کمیته دائمی، پیشین ص ۶.

۲. رجوع شود به مقررات سوئیس:
-Confederation Suisse, office federal de la protection de la population (O F P P).
-La strategie nationale de protection des infrastructures critiques, 5 octobre 2023.
همچنین رجوع شود به قانون فدرال سوئیس درمورد زیرساخت‌های بازار موصوب ۱۹ ژوئن ۲۰۱۵ (به‌روز شده در اول فوریه ۲۰۲۴) که شامل ۱۶۴ ماده است.
Document de position sur les services esentiels, Juillet 2021,16 pages
آمریکا هم زیرساخت‌های حیاتی در مقابل حملات فیزیکی، سایبری، خرابکاری، تروریستی و آلودگی را شامل زیرساخت‌های زیر می‌داند:
–بخش‌های شیمیایی، تأسیسات تجاری، تولیدات حیاتی، سدها، زیرساخت‌های صنعتی و دفاعی، خدمات فوریتی، انرژی، خدمات مالی، مواد غذایی و کشاورزی، تأسیسات دولتی، درمان و سلامت عمومی، فناوری اطلاعات، مراکز و مواد و پسماندهای هسته‌ای، حمل و نقل، سیستم‌های ذخیره‌سازی آب و تصفیه‌خانه‌های فاضلاب‌ها. رجوع شود به:
-Senstar pedia ‘’Protection des Infrastructures Critiques’’, Date de reference 25 Aout 2025.

۲. تعرض به زیرساخت‌های حیاتی و حقوق بین‌الملل

بی‌تردید تعرض به زیرساخت‌های حیاتی چه در هنگامه مخاصمات مسلحانه و چه در زمان صلح نقض مقررات بین‌المللی بوده، موجب مسئولیت می‌گردد.

۲.۱. تعرض به زیرساخت‌های حیاتی در زمان مخاصمات مسلحانه

اگرچه باید در هنگامه مخاصمات مسلحانه میان زیرساخت‌های حیاتی قائل به تفکیک شد،[۱] تعرض به این زیرساخت در تقریباً کلیه مخاصمات مسلحانه یکی از اهداف اصلی متخاصمین است.[۲] تعرض به زیرساخت‌های حیاتی در مخاصمات مسلحانه می‌تواند فیزیکی بوده باشد، یعنی این زیرساخت‌ها به‌طور مستقیم مورد حملات نظامی قرار گیرند یا ممکن است این تعرض با استفاده از فضای سایبری انجام شود. البته حملات سایبری حتی اگر منجر به ورود خسارات جانی یا مالی به‌غیر نظامیان نگردند، می‌توانند نقض حاکمیت محسوب شوند.[۳] این در دستورالعمل تالین ۲ نیز مورد توجه قرار گرفته است. در این دستورالعمل حملات سایبری نقض حاکمیت محسوب می‌شود.[۴] آنچه در چارچوب مخاصمات مسلحانه (اعم از بین‌المللی و غیر بین‌المللی) می‌توان گفت این است که حقوق حاکم بر این مخاصمات حاوی قواعدی نیست که به‌صراحت به زیرساخت‌های حیاتی اشاره کند. معهذا باتوجه‌به الزامی بودن رعایت اصل تفکیک و تکلیف متخاصمین به رعایت ممنوعیت تعرض به اموال غیرنظامی، می‌توان به ضرس قاطع گفت که زیرساخت‌های حیاتی غیرنظامی[۵] نباید مورد حمله قرار گیرند.[۶] این زیرساخت‌ها هیچ‌گاه و تحت هیچ شرایطی نمی‌توانند به‌عنوان اهداف نظامی محسوب شوند و مورد حمله قرار گیرند. ممنوعیت حمله به این زیرساخت‌ها را می‌توان با توجه به ماده ۲ - ۵۲ پروتکل شماره یک سال ۱۹۷۷ منضم به کنوانسیون‌های چهارگانه ژنو سال ۱۹۴۹ و همچنین قاعده عرفی شماره ۷ تحت‌عنوان «اصل تفکیک بین اموال غیرنظامی

---

[۱]. متمایز کردن زیرساخت‌های حیاتی به غیرنظامی، نظامی و با کاربری دوگانه باید بر اساس «اصل تفکیک» که یکی از اصول بنیادین حقوق بشردوستانه است، انجام شود.

[۲]. برای مثال در جنگ روسیه – اوکراین دوکشور به صورت دائمی زیرساخت‌های یکدیگر را مورد حمله قرار می‌دهند. برای نمونه می‌توان به حمله روسیه به زیرساخت‌های انرژی به ویژه نیروگاه‌های برق در شرق اوکراین در ۱۹ اوت ۲۰۲۵ یا حمله اوکراین به تعدادی از پالایشگاه های روسیه در ۲۲ اوت ۲۰۲۵ اشاره نمود. مجمع عمومی سازمان ملل قبلاً حمله روسیه به نیروگاه هسته‌ای زاپوریژیا اوکراین را در ۱۵ ژوئیه ۲۰۲۴ محکوم کرده بود. رجوع شود به A/RES/78/316:

[۳]. حاکمیت به مثابه یک قاعده بنیادین حقوق بین الملل نیز می‌تواند با حملات سایبری نقض گردد. به همین دلیل است که ایران در مذاکرات مربوط به کنوانسیون امنیت سایبری بر این نظر است که عملیات(هایی) که زیرساخت‌های حیاتی کشور اعم از عمومی یا خصوصی را آلوده می‌کنند، می‌توانند سازنده یک عمل «تجاوز» باشند. تعرض به حاکمیت فارغ از ورود خسارات در رویه قضایی بین‌المللی هم مورد توجه قرار گرفته است. برای مثال رجوع به قضیه تنگه کورفو:

C I J, '' Defroit de Corfou '', Arret du 9 Avril 1949.

دیوان در این قضیه به اتفاق آرا اعلام نمود که عملیات انگلستان در ۱۲ و ۱۳ نوامبر برای مین‌روبی از آب‌های تنگ کورفو، که تحت حاکمیت آلبانی قرار دارند، نقض حاکمیت آن کشور است.

[۴]. برای مطالعه بیشتر درمورد مقررات تالین ۲ رجوع شود به:

Schmitt M.N, *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Cambridge University Press, 2nd edition, February 2017, Particular PP. 11-29.

[۵]. این زیرساخت‌ها به‌طور عمده و نه منحصراً شامل مراکز بهداشتی و درمانی، مواد غذایی، آب آشامیدنی، تأسیسات دارای نیروی خطرناک مانند سدها، آب‌بندها، تأسیسات و مراکز اتمی و نیروگاه‌های برق می‌شوند.

[۶]. قاعده ممنوعیت تعرض به اموال غیرنظامی (اینجا زیرساخت حیاتی غیرنظامی) در مواد ۴۸ و۵۲.۲ پروتکل شماره یک سال ۱۹۷۷ تدوین شده و هیچ‌گونه شرطی هم بر آنها اعمال نشده است. ماده ۴۸ با کنسانسوس و ماده ۵۲،۲ با ۷۹ رأی مثبت و ۷ رأی ممتنع و بدون رأی مخالف به تصویب رسیده‌اند.

و اهداف نظامی استخراج کرد».[۱] بنابراین حمله به زیرساخت‌های حیاتی غیرنظامی ممنوع و نقض فاحش و شدید حقوق بشردوستانه بوده، جنایت جنگی محسوب می‌شود.[۲] به نظر می‌رسد که باتوجه‌به ممنوعیت مطلق در حمله به زیرساخت‌های حیاتی غیرنظامی، توجه به اصل «تناسب ضرورتی نداشته باشد».[۳] همچنین به نظر می‌آید که این اصل درمورد زیرساخت‌های حیاتی با کاربری دوگانه (نظامی و غیرنظامی)[۴] نیز قابل‌اجرا نباشد، زیرا چنین زیرساخت‌هایی علی‌الاصول باید غیرنظامی لحاظ شوند. البته برخی به این نظرند که درخصوص این نوع زیرساخت‌ها باید اصل تناسب را جاری دانست. طبق این نظر، اگر حمله به این نوع زیرساخت‌ها از مزیت نظامی بیشتری نسبت به خسارات وارده به آنها برخوردار است، می‌توان حمله به آنها را توجیه نمود.[۵] حاصل چنین نگرشی آن است که در مواقعی نمی‌توان حمله به زیرساخت‌های حیاتی با کاربردی مضاعف را نامشروع تلقی کرد. معهذا، ازآنجاکه اغلب زیرساخت‌های حیاتی با کاربری دوگانه در زمره زیرساخت‌هایی‌اند که باید مصون از تعرض باشند، نمی‌توان حمله به آنها را به‌عنوان اهداف مشروع نظامی تلقی نمود. به‌خصوص که متخاصمین معمولاً زیرساخت‌های حیاتی را که نیروی خطرناک مانند مراکز هسته‌ای دارند، مورد حمله قرار می‌دهند؛ حتی اگر فاقد کاربری نظامی باشند. نمونه بارز آن را می‌توان در جنگ دوازده‌روزه و حمله رژیم اشغالگر اسرائیل و آمریکا به مراکز هسته‌ای ایران مشاهده نمود[۶]. حمله به زیرساخت‌های حیاتی غیرنظامی یا با کاربری مضاعف در زمان مخاصمات مسلحانه با استفاده از هر روشی (فیزیکی یا سایبری) ممنوع است. البته برخی مانند مایکل اشمیت بر این نظرند که اگر عملیات‌های سایبری بر ضد

---

[1]. Henckaerts J. M. and Louise Doswald Beck, Customary International Humanitarian Law, Volume 1 (Rules), Cambridge University Press, 2005, PP 25 – 29.

این کتاب تحت عنوان «حقوق بین‌المللی بشردوستانه»، جلد اول، قواعد، توسط دفتر امور بین‌الملل قوه قضائیه و کمیته بین‌المللی صلیب سرخ ترجمه و با ویرایش حسین‌زاده کتایون و عسکری پوریا، توسط انتشارات مجد در سال ۱۳۹۱ (چاپ دوم) به زیور طبع آراسته شده است. برای اصل ۷ رجوع شود به فصل دوم تفکیک بین اموال غیرنظامی و اهداف نظامی، صص ۹۸ – ۹۳.

همچنین رجوع شود به کارهای O E W G و G G E به ویژه هنجار 13f و مصوبه‌های مجمع عمومی سازمان ملل متحد، قطعنامه‌های:

-A/ RES/ 70/ 237 du 20 Decembre 2015.

-A/RES/ 71/28 du 5 Decembre 2016.

-A/RES/ 73/27 du 11 Decembre 2018.

-Declaration on Responsible states behavior in Cyberspace, Lucca, 11 Avril 2017, cite par : Bannelier, Op.Cit., P 235.

[۲]. رجوع شود به ماده ۸ – ۲ – ب – ۲ اساسنامه دیوان بین المللی کیفری. البته حمله به زیرساخت‌های حیاتی در مخاصمات مسلحانه غیربین‌المللی در این اساسنامه مورد توجه قرار نگرفته است. برای مطالعه بیشتر درمورد جنایت‌های جنگی و عناصر تشکیل‌دهنده این جنایت‌ها رجوع شود به: دورمن، کنوت، ***عناصر جنایات جنگی در اساسنامه دیوان بین‌المللی کیفری***، ترجمه زهرا جعفری، زهرا محمودی و پریسا سفیدپری، تهران: مجد، ۱۳۹۳، صص ۲۲۶ – ۲۱۹.

همچنین رجوع شود به:

-Selected Basic Documents related to the International Criminal Court, International Criminal Court Publication, The Hague, 2009, PP. 229-272.

-Fernandez Julian, Pacreau Xavier, Ubeda – Saillard Muriel, *Statut de Rome de la Cour Penale International: Commentaire article par article*, 2e edition, Tome 1, PP. 627 – 685, Paris : Pedone, 2019.

[۳]. طبق اصل تناسب، باید رابطه میان خسارات وارده به اموال غیرنظامی (زیرساخت های حیاتی غیرنظامی) و مزیت های نظامی مورد توجه قرار گیرد.

[۴]. برای مثال می توان نیروگاه برقی را در نظر گرفت که هم برق شهری غیرنظامیان و هم برق نیروهای مسلح و پادگان ها و کارخانه های اسلحه سازی و..... تامین می کند.

[5]. Bannelier, Op. Cit., P 238.

[۶]. در جریان این جنگ آمریکا مراکز هسته‌ای ایران در فردو، نطنز، اصفهان و خنداب (اراک که محل استقرار تأسیسات آب سنگین بود) را مورد بمباران هوایی و موشکی قرار داد. این حملات درحالی انجام شد که کاربری نظامی این مراکز محرز و قطعی نشده و طبق اظهار مقامات نظامی آمریکا هیچ‌گونه فعالیتی از سوی ایران برای تولید تسلیحات اتمی مشاهده نشده بود.

زیرساخت‌های حیاتی به آستانه حمله مسلحانه ممنوع شده بر طبق اصل تفکیک نرسیده باشند، ممنوع نیستند. به دیگر سخن، اگر عملیات‌های سایبری به زیرساخت‌های حیاتی موجب ورود خسارات فیزیکی جدی نشوند، ممنوع نخواهند بود.[1] این تفسیر مضیق از اصل تفکیک منجر به مشروعیت بخشیدن به عملیات‌های سایبری نظامی عمدی به زیرساخت‌های حیاتی می‌شود. پدیده‌ای که نمی‌تواند قابل قبول باشد، زیرا اولاً احراز رابطه مستقیم میان اختلال در یک زیرساخت حیاتی و خسارات فیزیکی جدی به مردم غیرنظامی در اغلب حملات حداقل بسیار سخت است و علت آن هم این است که خسارات جدی ممکن است فوراً آشکار نشود و در یک بازه زمانی بعضاً طولانی هویدا شوند؛ ثانیاً بررسی گستره و میزان خسارات جدی وارده تابعی از متغیرهای متنوعی است که از جامعه‌ای به جامعه دیگر متفاوت‌اند؛ ثالثاً آثار روانی و تروماهای فردی و اجتماعی ناشی از تخریب یا اختلال زیرساخت‌های حیاتی به سهولت قابل احصا نیستند. اگر این نظر پذیرفته شود می‌تواند منجر به این شود که برای مثال حمله به یک خانه مسکونی از نظر مقررات حقوق بشردوستانه حاکم بر مخاصمات مسلحانه ممنوع است، اما حمله به زیرساخت حیاتی که تأمین‌کننده نیازهای اساسی و حیاتی بعضاً میلیون‌ها نفر است ممنوعیت ندارد. چنین تفسیری به‌هیچ‌وجه با متن و روح اصل تفکیک هماهنگی ندارد[2] و به‌راحتی می‌تواند مورد سوءاستفاده قرار گیرد. قابل پذیرش نبودن چنین تفسیری به‌خصوص در پرتو تحولات جدید علوم و فناوری و اثر آنها بر تسلیحات و شیوه‌های جنگی بیشتر نمایان می‌گردد؛ بنابراین باید به تفسیری پویا روی آورد؛ تفسیری که امروزه در رویه قضایی بین‌المللی هم پذیرفته شده است.[3] در پرتو چنین تفسیری است که می‌توان تعرض به زیرساخت‌های حیاتی اعم از غیرنظامی و با کاربری مضاعف را ممنوع دانست و آن فارغ از هرگونه ورود خسارات جانی و مالی است. اگر متخاصمین چنین ممنوعیتی را در عمل رعایت نمی‌کنند، نمی‌تواند به این برداشت منتهی شود که می‌توان آن را نادیده انگاشت، بلکه برعکس رعایت نکردن این ممنوعیت خدشه بر اصول و قواعد حاکم بر مخاصمات مسلحانه و نقض آنهاست و موجب مسئولیت بین‌المللی می‌شود.

۲.۲. تعرض به زیرساخت‌های حیاتی در زمان صلح

متداول‌ترین شکل تعرض به زیرساخت‌های حیاتی در زمان صلح ایجاد اختلال در آنها با استفاده از فضای سایبر است. البته در این مورد بین دولت‌ها اختلاف‌نظر وجود دارد. برخی برآن‌اند تا زمانی که عملکرد زیرساخت حیاتی در عملیات سایبری از بین نرفته یا کاملاً از دسترس خارج نشده است، نمی‌توان آن عملیات را اختلال در زیرساخت حیاتی لحاظ نمود. به دیگر سخن، در این دیدگاه ورود خسارت به زیرساخت است که ملاک تشخیص اینکه آیا عملیات سایبری تعرض به آن محسوب می‌شود یا نه، مورد توجه قرار می‌گیرد.

در مقابل، اکثر کشورها از جمله فرانسه برآن‌اند که اختلال ناشی از عملیات سایبری که موجب ورود خسارات هم نشود، نقض حقوق بین‌الملل محسوب می‌گردد. در واقع نظر آنان بر این گزاره استوار است که حاکمیت چه به‌مثابه اصل لحاظ گردد که قواعد منع توسل به‌زور و عدم مداخله در امور داخلی از آن ناشی می‌شوند، و چه خود به‌مثابه قاعده لحاظ شود و هرگونه عملیات سایبری آنها را نقض کند، موجب مسئولیت بین‌المللی می‌گردد. در این میان، موضع ایران جالب می‌نماید. ایران بر این نظر است که هرگونه عملیات سایبری در مواقعی که مستلزم نفوذ غیرمجاز به زیرساخت‌ها (اعم از

---

[1]. Schmitt, Op. Cit., P 240.

[2]. Bannelier, Op. Cit., P 0.

[3]. برای مثال رجوع شود به تفسیر تکاملی دیوان بین‌المللی دادگستری در اختلاف کاستاریکا – نیکاراگوئه:

C. I. J.''Differend relative a des droits de navigation et des droits connex (Costarica C. Nicaragua), Arret du 13 Juillet 2009.

دولتی یا خصوصی)، که تحت کنترل دولت دیگرند، باشد، می‌تواند نقض حاکمیت دولت هدف تلقی شود.[۱] این نگرش کاملاً مبتنی‌بر لحاظ کردن حاکمیت به‌مثابه «قاعده» است. با چنین نگرشی هرگونه نفوذ سایبری در زیرساخت‌ها از جمله زیرساخت‌های انتخاباتی برای تغییر نتیجه انتخابات می‌تواند نماد بارز نقض قاعده منع مداخله در امور داخلی باشد.[۲] همان‌طور که قبلاً اشاره شد، آنچه باید به‌عنوان تعرض به زیرساخت ملاک قرار گیرد، نه ماهیت و نه شیوه و نه محل استقرار اخلالگران است، بلکه باید عملکرد زیرساخت حیاتی ملاک قرار گیرد. به دیگر سخن، اگر در اثر عملیات سایبری، اختلالی در عملکرد زیرساخت‌های حیاتی ایجاد شود، آن عملیات باید به‌عنوان تعرض به زیرساخت‌ها و نقض حاکمیت دولت هدف لحاظ گردد و آن فارغ از خسارات وارده یا خارج نمودن آنها از دسترس است. در غیر این صورت حداقل کلیه عملیات‌های سایبری که خسارات فیزیکی ظاهری و فوری ایجاد نکنند، «ممکن است» مشروع تلقی شوند؛ پدیده‌ای که موجب خسران زیاد به‌ویژه به غیرنظامیان می‌شود.

۳. قربانیان تعرض به زیرساخت‌های حیاتی و ضمانت اجرای عدم رعایت تعرض به این زیرساخت‌ها

تعرض به زیرساخت‌های حیاتی نه فقط منجر به ورود خسارات به تأسیسات و اجزای آنها می‌گردد، بلکه موجب ورود زیان و حتی سلب حیات از اشخاص حقیقی می‌شود؛[۳] پدیده‌ای که موجب مسئولیت بین‌المللی مدنی و کیفری می‌گردد. تا این اواخر، مسئولیت کیفری مرتکبان تعرض به زیرساخت‌های حیاتی، که می‌تواند خود منشأ بسیاری از جنایت‌های بین‌المللی دیگر گردد،[۴] مورد توجه جامعه بین‌المللی نبود. تا اینکه از اوایل سال ۲۰۲۴ با ورود دیوان بین‌المللی کیفری و طرح مسئولیت بین‌المللی کیفری تخریب‌کنندگان زیرساخت‌های حیاتی، گامی در جهت زدودن بی کیفر مانی این جنایتکاران برداشته شده است.[۵]

۳.۱. قربانیان تعرض به زیرساخت‌های حیاتی

بی‌تردید اولین قربانیان تعرض به زیرساخت‌های حیاتی غیرنظامیان اعم از حقیقی و حقوقی‌اند؛ چراکه تخریب یا اختلال در کارکرد زیرساخت‌های حیاتی تأثیر مستقیم و غیرمستقیم بر زندگی و حتی حیات آنان دارد، ضمن آنکه انسجام

---

[۱]. مرکز فضای سایبری نیروهای مسلح، ماده ۲ بیانیه ستاد کل نیروهای مسلح جمهوری اسلامی ایران در قبال حقوق بین‌الملل فضای سایبری ایران، ۲۷ مرداد ۱۳۹۹ برابر ۲۷ اوت ۲۰۲۰. این بیانیه شامل یک مقدمه و چهار ماده و یک جمع‌بندی است. تاریخ رجوع به اینترنت برای این سند ۲۰ اوت ۲۰۲۵ است.

[۲]. برای نمونه می توان به ادعای برخی از سیاست‌مداران آمریکا در کنگره این کشور دائر بر مداخله روسیه در انتخابات ایالات متحد آمریکا اشاره نمود.

[۳]. تعرض به زیرساخت علاوه‌بر خسارات مستقیم می‌تواند خسارات غیرمستقیم زیادی به غیرنظامیان وارد کند. برای مطالعه بیشتر در این مورد برای مثال رجوع شود به:

I C R C, ‘’Quel sont les effects indirects des attaques contre des infrastructures energetiques?’’ Date de reference le 22 Aout 2025, 6 pages.

[۴]. تعرض به زیرساخت‌های حیاتی که منجر به نابودی یا خروج کامل آنها از دسترس می‌شود، موجب می‌گردد که غیرنظامیان منتفع از آنها مجبور به کوچ (جابه‌جایی) اجباری شوند که از مصادیق بارز جنایت بر ضد بشریت است.

[۵]. درمورد حرکت جامعه جهانی برای مبارزه با بی کیفر مانی آثار زیادی منتشر شده‌اند که برای نمونه می‌توان به این موارد اشاره کرد:

-Federation Internationale pour les Droits Humains,’’Faire foctionner la Justice: La societe civile s’ unit dans la lutte mondiale contre l’ impunite, 4.6.2024 Date de reference 22 Aout 2025.

-European Center for Constitutional and Human Rights (ECCHR),” Global Initiative Against Impunity, Making Justice work, 6 Juin 2024, Date de refrence 22 Aout 2025.

اجتماعی را با خطر جدی مواجه می‌کند. برای نمونه می‌توان به حملات رژیم اشغالگر اسرائیل به غزه بعد از ۷ اکتبر ۲۰۲۳ اشاره نمود که تقریباً تمام زیرساخت‌های حیاتی ازجمله زیرساخت‌های انرژی، مراکز درمانی (به‌ویژه بیمارستان‌ها)، صنایع غذایی و تصفیه‌خانه‌ها هستند؛ حملاتی که منجر به کشته شدن هزاران نفر از مردم غیرنظامی به‌صورت مستقیم یا غیرمستقیم در اثر از دسترس خارج شدن خدمات عمومی مانند آب آشامیدنی، مواد غذایی و دارویی شده است.[۱] علاوه‌بر انتقام‌کشی رژیم اشغالگر اسرائیل، این رژیم مصوبه‌ای برای اشغال دائمی شهر غزه نیز تصویبو اخیراً آن شهر را به‌عنوان منطقه جنگی اعلام کرده است.[۲] یکی از دلایل مهم این رژیم برای اشغال دائمی شهر غزه تسلط بر منابع انرژی عظیمی است که در این منطقه و مناطق دریایی مقابل آن وجود دارند. برای نمونه منطقه انحصاری اقتصادی غزه حاوی ۳۵ میلیارد مترمکعب گاز است که قابلیت استخراج با ظرفیت سالانه ۱/۲ میلیارد مترمکعب را برای مدت دوازده سال دارد. این میدان گازی در ۳۶ کیلومتری غرب شهر غزه قرار دارد.[۳] رژیم اشغالگر اسرائیل همچنین در راستای حملات خود بر ضد زیرساخت‌های حیاتی کشورها، در ۱۴ و ۱۵ ژوئن ۲۰۲۳ به پالایشگاه پارس جنوبی در بندر عسلویه ایران حمله کرد که به کشته شدن حداقل ۱۲۸ و مجروح گردیدن ۹۰۰ نفر انجامید.[۴] نمونه دیگر حمله به زیرساخت‌های انرژی و مخازن آب در شهرهای مختلف سودان در جریان جنگ داخلی در این کشور است. حملات به این زیرساخت‌های حیاتی منجر به محرومیت میلیون‌ها نفر مردم غیرنظامی از دسترسی به برق و آب آشامیدنی شده است.[۵] حملات به زیرساخت‌های حیاتی برای اشخاص حقوقی نیز فاجعه‌بار بوده است؛ برای مثال حملات سایبری واناکرای به زیرساخت‌های حیاتی منجر به آسیب دیدن ۲۵۰ هزار کامپیوتر در ۱۵۰ کشور جهان و خسارات هنگفت به بخش الکترونیکی شرکت‌های کشتیرانی، نیسان موتور، فوکس و حتی چندین دانشگاه در کشورهای مختلف شده است.[۶]

---

[۱]. از ۳۶ بیمارستان غزه ۲۴ بیمارستان کاملاً فعالیتشان متوقف شده است. براساس آمار یونیسف (صندوق ملل متحد برای حمایت از کودکان) تا ۱۴ اوت ۲۰۲۵ بیش از ۶۱۰۰۰ نفر در غزه کشته شده‌اند که از این تعداد ۱۸۰۰۰ کودک هستند. همچنین ۱۵۴۰۰۰ نفر مجروح شده‌اند که ۴۵۰۰۰ کودک در میان آنان دیده می‌شود. بر این تعداد باید مفقود شدن ۱۱۲۰۰ نفر را هم اضافه نمود که به نظر می‌رسد بتوان در زمره کشته‌شدگان لحاظ نمود. طبق اعلام سازمان ملل متحد، ۷۰ درصد از کشته‌شدگان زنان و کودکان هستند. طبق اعلام این سازمان در ۲۲ اوت ۲۰۲۵ غزه وارد مرحله قحطی مطلق شده و برنامه جهانی غذا اعلام کرده است که ۹۳ درصد از ساکنان این منطقه در وضعیت ناامنی غذایی جدی قرار دارند. این فاجعه انسانی که هر روز عمیق‌تر و دردناک‌تر می‌شود، درحالی همچنان ادامه دارد که دیوان بین‌المللی دادگستری در دستور موقت صادر در ۲۶ ژانویه ۲۰۲۴ در اختلاف آفریقای جنوبی علیه رژیم اشغالگر اسرائیل از این رژیم می‌خواهد که اجازه دهد خدمات اساسی (زیربنایی) و کمک‌های بشردوستانه به مردم غزه ارائه شوند. تخریب زیرساخت‌های اساسی در غزه از جمله منجر به بروز بیماری های عفونی ناشی از عدم دسترسی به مواد غذایی، آب آشامیدنی و مراکز بهداشتی و درمانی شده است.

[۲]. رجوع شود به مصوبه کابینه امنیتی رژیم اشغالگر اسرائیل در ۱۷ اوت ۲۰۲۵. شبکه خبری الجزیره اعلام کرد که ایال زمیر، رئیس ستاد ارتش اسرائیل، طرح اشغال شهر غزه را تصویب کرده است.

[3]. Guillaum Jean – Sebastien.''Du gaze en Palestine'', Conflits, Revue de Geopolitique, 14 Novembre 2023.

[4]. Politique France International,''Pour l' Iran, la frappe d' Israel sur ce site gazier est un gros coup dur'', 15. Mai. 2023, Date de reference 24 Aout 2025.

[5]. C I C R, *Soudan: Les attaques contre des infrastructures civiles essentielles se multiplient sur fond d' escalade des combats*, Communique de Presse, 25 Janvier 2025, Date de reference 24 Aout 2025.

[۶]. اغلب دولت‌ها به رغم تعهد خود دائر بر جرم‌انگاری نقض حقوق بشردوستانه (به ویژه کنوانسیون‌های چهارگانه ۱۹۴۹ ژنو) هنوز اهتمامی به خرج نداده، این تعهد را اجرا نکرده‌اند. نمونه بارز آن ایران است. علی‌رغم تلاشی که شد و لایحه‌ای در رابطه با «جنایات جنگی، علیه بشریت، نسل‌کشی و تعدیات نژادی» به مجلس ششم تقدیم شد. مجلس در ۲۹ اردیبهشت ۱۳۸۱ کلیه مقررات مرتبط با جنایت‌های جنگی را حذف نمود. سایر جنایت‌ها هم در پی ابهام‌های مطروح ازسوی شورای نگهبان (به‌ویژه درمورد جنایت نسل‌کشی) به سرانجامی نرسید. تلاش دیگری هم در معاونت آموزشی و توسعه قوه قضائیه انجام شد که آن نیز به نتیجه‌ای نینجامید. نویسنده این مقاله خود از نزدیک شاهد این وقایع بود. به همین دلیل هنوز نقض کنوانسیون چهارگانه ۱۹۴۹ ژنو، که دولت ایران از قبل از انقلاب به آنها پیوسته است، در مقررات داخلی جرم‌انگاری و مجازاتی برای نقض آنها پیش‌بینی نشده است.

همان‌طور که ملاحظه می‌شود، تخریب یا اختلال در زیرساخت‌های حیاتی موجب ورود خسارات جانی و مالی فراوانی می‌شود. خساراتی که علی‌الاصول موجب مسئولیت بین‌المللی مدنی و کیفری می‌شوند. در حرکت اخیر جامعه بین‌المللی به‌سوی شناخت مسئولیت کیفری بین‌المللی فردی، این مسئله به‌عنوان ضمانت اجرای عدم رعایت ممنوعیت حمله به زیرساخت‌های حیاتی مورد توجه قرار می‌گیرد.

۳.۲. ضمانت اجرای عدم رعایت ممنوعیت تعرض به زیر ساخت‌های حیاتی

علی‌رغم اعتراض برخی از نهادهای غیردولتی مانند کمیته بین‌المللی صلیب سرخ در تعرض به زیرساخت‌های حیاتی در زمان مخاصمات مسلحانه، دولت‌ها چندان تمایلی به توقف حملات خود به این زیرساخت‌ها و برخورد با مرتکبان آنها نداشتند.[۱] بنابراین طراحان و حمله‌کنندگان از هرگونه کیفری در امان بودند. به دیگر سخن، بی‌کیفرمانی آنانی که با تخریب یا اختلال در زیرساخت‌های حیاتی، زندگی میلیون‌ها انسان بی‌گناه را حتی با خطر نابودی مواجه می‌کردند، تداوم داشت. مبارزه با این بی‌کیفرمانی سرانجام با حرکت دیوان بین‌المللی کیفری از سال ۲۰۲۴ آغاز شده است. دیوان بین‌المللی کیفری با صدور قرارهای بازداشت مبارزه با بی‌کیفرمانی مرتکبان تخریب زیرساخت‌های حیاتی را آغاز نموده است. این دیوان دو سری قرار بازداشت در سرزمین اوکراین در خلال جنگ روسیه علیه آن کشور صادر کرده است.

قرار اول در ۵ مارس سال ۲۰۲۴ به درخواست دادستان دیوان[۲] توسط شعبه ۲ پیش دادرسی (مقدماتی) دیوان بین‌المللی کیفری ضد دو تن از افسران عالی‌رتبه نیروهای مسلح فدراسیون روسیه صادر گردید.[۳] شعبه ۲ پیش دادرسی قرار خود را به‌اتهام ارتکاب جنایت‌های جنگی و جنایت‌های بر ضد بشریت در سرزمین اوکراین صادر کرده است. قرار دوم شعبه ۲ پیش‌دادرسی در تاریخ ۲۴ ژوئن ۲۰۲۴ در چارچوب «وضعیت در اوکراین» ضد دو تن از مقامات ارشد نظامی ارتش روسیه صادر شده است.[۴] شعبه ۲ پیش‌دادرسی در هر دو سری قرار بازداشت صادره، اتهام جنایت‌های جنگی را در قالب

---

[1]. Declaration du Procureur de la Cour P*é*nale Internationale (C P I), Khan Karim, Communique de presse du 2 Fevrier 2024.

البته اولین درخواست دادستان در ۲۸ فوریه ۲۰۲۲ برای شروع تحقیقات در اوکراین تحت عنوان «وضعیت در اوکراین» ارائه شد که با آن موافقت گردید. اولین قرار بازداشتی هم که شعبه ۲ پیش‌دادرسی در ۲۷ مارس ۲۰۲۳ صادر کرد که درمورد ولادیمیر ولادیمیروویچ پوتین Vlademir (Vlademirovich Poutin) رئیس‌جمهور فدراسیون روسیه و ماریا الکسیونا ایووا – بلوا Maria Alekseievna Ivova – Belova) (کمیسر حقوق کودکان در دفتر رئیس‌جمهور فدراسیون روسیه به اتهام ارتکاب جنایت کوچ (جابه‌جایی) غیرقانونی مردم و ارتکاب جنایت جنگی (کوچاندن اجباری اوکراینی‌ها به‌ویژه کودکان از سرزمین‌های اشغالی اوکراین به‌سوی روسیه است.

[۲]. قرار ۵ مارس ۲۰۲۴ بر ضد سرگئی ایوانویچ کوبیلاش (Sergei Ivanovich Kobylash) ژنرال ارتش و فرمانده نیروی هوایی و مسئول نیروی هوافضا روسیه و ویکتور نیکولایویچ سکولوف (Viktor Nikolayvich Sokolov) دریادار و فرمانده ناوگان دریایی روسیه در دریای سیاه در لحظه ارتکاب این جنایت‌ها بوده اند.

[۳]. اگرچه متن این قرار بازداشت محرمانه است، درمورد کلیات آن و نام متهمان رجوع شود به:

Situation en Ukraine: Les Juges de la C P I delivrent des mandats d’ arret contre Sergei Ivanovich Kobylash et Viktor Nikolayvich Sokolov, Communique de presse du 5 Mars 2025, Site official de la C P I, Date de reference le 25 Aout 2025.

[۴]. قرار بازداشت ۲۴ ژوئن ۲۰۲۴ شعبه ۲ پیش دادرسی بر ضد سرگی کوژوجتوویچ شوآگی (Sergi Kuzhugetovich Shoigu) وزیر دفاع فدراسیون روسیه و والری واسیلیویچ گرامیسوف (Valery Vasilyevich Geramisov) رئیس ستاد ارتش و معاون اول وزیر دفاع فدراسیون روسیه در هنگام ارتکاب این جنایت ها بوده‌اند.

حمله به اموال غیر نظامی[۱] و وارد کردن خسارات شدید به غیرنظامیان و اموال غیر نظامی[۲] به‌شکل پیش‌بینی‌شده در اساسنامه دیوان بین‌المللی کیفری مطرح کرده است. به نظر شعبه دلایل معقول و قابل قبولی برای اثبات مسئولیت کیفری آنان برای این موارد وجود دارند:

- ارتکاب جنایت‌های پیش‌گفته به‌صورت مشترک یا به‌وسیله اشخاص دیگر[۳]،
- صدور دستور ارتکاب این جنایت‌ها[۴]،
- عدم توانایی در اعمال کنترل مناسب بر نیروهای تحت امر خود[۵].

آنچه در این دو قرار جلب توجه می‌کند (که مرتبط با موضوع این نوشتار نیز است) اینکه شعبه پیش دادرسی بر آن است که دلایل معقول و قابل‌قبولی برای اطمینان یافتن از اینکه متهمان مسئولیت شلیک موشک توسط نیروهای مسلح روسیه ضد چندین زیرساخت‌های الکتریکی اوکراین در ۱۰ اکتبر ۲۰۲۲ و ۹ مارس ۲۰۲۳ برعهده دارند، وجود دارند. شعبه ۲ پیش‌دادرسی همچنین اعلام می‌دارد دلایل متقنی وجود دارند که میزان خسارات ناشی از این حملات به زیرساخت‌های الکتریکی اوکراین بیش از مزیت‌های نظامی موردنظر آنان است.

شعبه برای اینکه مستدلاً بیان کند رفتار متهمان منجر به ورود آسیب و خسارات جانی و مالی به غیرنظامیان شده است، به رعایت نکردن «اصل تفکیک» میان اموال غیرنظامی و اهداف نظامی توجه کرده که موجب وارد شدن خسارات فراوان جانی و مالی به اقشار آسیب‌پذیر به‌ویژه سالمندان، زنان و کودکان شده است.[۶و۷] این حرکت ازسوی دیوان بین‌المللی کیفری را باید به فال نیک گرفت که حمله به زیرساخت‌های حیاتی در مخاصمات مسلحانه قطعاً مسئولیت کیفری فردی به‌همراه دارد؛ پدیده‌ای که حتماً باید به‌عنوان یکی دیگر از جنایت‌های ارتکابی سران رژیم اشغالگر اسرائیل در مخاصمات

---

۱. حمله به اموال غیرنظامی موضوع ماده ۸ (۲) (b) (ii) اساسنامه دیوان بین‌المللی کیفری است.

۲. ورود خسارات شدید به غیرنظامیان موضوع ماده ۸ (۲) (b) (iv) اساسنامه دیوان بین‌المللی کیفری است.

۳. ارتکاب جنایت‌ها در قالب اعمال مشترک یا به وسیله اشخاص دیگر موضوع ماده ۲۵ (۳) (a) اساسنامه دیوان بین‌المللی کیفری است.

۴. صدور دستور برای ارتکاب جنایت های اتهامی موضوع ماده ۲۵ (۳) (b) اساسنامه دیوان بین المللی کیفری است.

۵. عدم اعمال کنترل بر نیروهای تحت امر موضوع ماده ۲۸ اساسنامه دیوان بین‌المللی کیفری است. مواد اساسنامه دیوان بین‌المللی کیفری رجوع شود به:

Selected basic documents related to the International Criminal Court, Op. Cit., PP 9 – 76, en particulier PP 12 – 22 – 23 – 24.

۶. البته شعبه ارتکاب جنایت‌های ضد بشریت از سوی متهمان در قالب ارتکاب «اعمال غیرانسانی» را نیز مطرح کرده است. اعمال غیرانسانی عمدی که هدفشان وارد کردن درد و رنج یا لطمه بر تمامت جسمی یا به سلامت جسمی و روحی افراد بوده است. این جنایت موضوع ماده ۷ (۱) (k) اساسنامه دیوان بین‌المللی کیفری است. شعبه در احراز اینکه این جنایت‌ها در قالب یک سیاست (به‌صورت سازمان‌یافته) ارتکاب یافته‌اند، به برگزاری کمپین‌های برگزارشده در روسیه اشاره می‌کند و اعلام می‌دارد که وارد کردن خسارات جانی و مالی در واقع یک سیاست (سازمان‌یافته) بوده است.

۷. در مجموع تابه‌حال شش قرار بازداشت ضد مقامات فدراسیون روسیه صادر شده‌اند. البته باید خاطرنشان کرد که اوکراین نیز به تعدادی از زیرساخت‌های روسیه ازجمله چندین پالایشگاه حمله کرده که منتهی به تخریب آنها شده است، ولی تابه‌حال دیوان بین‌المللی کیفری اقدامی درمورد مقامات نظامی اوکراین انجام نداده است. چند دلیل وجود دارد: اول آنکه روسیه عضو اساسنامه دیوان بین‌المللی کیفری نیست؛ درحالی‌که اوکراین بعد از دو بار پذیرش موردی صلاحیت دیوان به استناد بند ۳ ماده ۱۲ اساسنامه، سرانجام اساسنامه این رکن را در ۲۴ اکتبر ۲۰۲۴ تصویب نمود. این سند از اول ژانویه ۲۰۲۵ برای این کشور لازم‌الاجرا شده است؛ نکته دوم اینکه هیچ دولتی تخریب زیرساخت‌های حیاتی روسیه توسط اوکراین را به دیوان بین المللی کیفری در قالب جنایت‌های جنگی ارجاع نداده است؛ درحالی‌که حملات روسیه به زیرساخت‌های حیاتی اوکراین به عنوان جنایت‌های جنگی از سوی ۴۳ کشور در قالب «وضعیت در اوکراین» به دیوان بین‌المللی کیفری ارجاع داده شده است. دادستان دیوان هم با توجه به اسناد، شواهد و مدارک موجود در این ارجاعات خواستار شروع تحقیقات علیه روسیه گردید که در نهایت منجر به صدور قرارهای بازداشت ضد مقامات سیاسی و نظامی آن کشور شده است.

مسلحانه خود در غزه، کرانه باختری رود اردن، سوریه پس از سقوط بشار اسد[۱] و در ایران مطرح نمود.[۲] البته احراز مسئولیت کیفری موجب مسئولیت مدنی مرتکبان این‌گونه حملات یا دولت متبوع آنها نیز خواهد شد.

نتیجه‌گیری

همان‌طور که ملاحظه شد، از منظر مقررات بین‌المللی ابهام‌های زیادی درخصوص تعریف و حفاظت از زیرساخت‌های حیاتی وجود ندارند. حفاظت از این زیرساخت‌ها بالاخص در مخاصمات مسلحانه با پذیرش تفسیر موسع از اصل تفکیک میان اموال غیرنظامی و اهداف نظامی و برخورد کیفری بین‌المللی با مرتکبان تعرض به آنها از قوت بیشتری هم برخوردار شده است.

باوجود این، خطر تعرض به زیرساخت‌های حیاتی به‌ویژه در زمان صلح هنوز به‌طور کامل برطرف نشده‌اند. دو نمونه از تعرض به زیرساخت‌های حیاتی در زمان صلح جلب توجه می‌کنند: نمونه اول آنکه دولت‌ها گاهی به بهانه‌های مختلف به‌ویژه امنیتی به‌صورت ارادی مبادرت به ایجاد اختلال در زیرساخت‌های حیاتی خود می‌کنند. این‌گونه اختلال‌ها در زیرساخت‌های ارتباطی مانند اینترنت، جی‌پی‌اس، شبکه‌های اجتماعی و حتی خطوط تلفنی بیشتر قابل مشاهده‌اند. اقدام دولت‌ها در ایجاد این‌گونه اختلال‌ها در زیرساخت‌های حیاتی بدون تردید توأم با خسارات هنگفتی است که به مردم غیرنظامی تحت صلاحیتشان وارد می‌شوند. برای نمونه می‌توان به ادعای شرکت اسنپ اشاره نمود. براساس اعلام این شرکت قطع جی‌پی‌اس توسط وزارت ارتباطات (قطع جی‌پی‌اس توسط وزیر آن وزارتخانه پذیرفته شده است) بعد از جنگ ۱۲روزه سبب ورود یک میلیارد دلار خسارت به آن شرکت شده است. ضمن آنکه قطع جی‌پی‌اس خطرات جدی برای صنعت حمل و نقل به‌ویژه کشتیرانی و هوانوردی ایجاد می‌کند.

نمونه دوم این است که تعرض به زیرساخت‌های حیاتی در مواردی ناشی از ساخت‌وسازها در کشورهای هم‌جوار رخ می‌دهد. برای مورد دوم می‌توان به دو طرح اشاره نمود: اوّلین مورد اجرای طرح «گاپ» توسط ترکیه است. این کشور با ساخت بیست و دو سد و نوزده نیروگاه برق آبی بر روی رودخانه‌های دجله و فرات، بسیاری از زیرساخت‌های حیاتی سوریه و عراق را با خطر جدی و حتی نابودی مواجه کرده است. این درحالی است که ترکیه در قالب معاهداتی که با این دو کشور دارد، متعهد است که تعرض به میزان دبی آبی که در هر ثانیه وارد این کشورها می‌شود، نکند. همین ساخت‌وسازها را ترکیه درمورد ارمنستان در قالب طرح داپ، که ساخت سد بر روی رودخانه ارس است، انجام داده است.[۳] طرح دوم ساخت سد روی رودخانه هریرود توسط افغانستان است که اخیراً انجام شده، به اختلال جدی در زیرساخت مرتبط با آب آشامیدنی شهر مشهد در ایران انجامیده است. این کشور قبلاً نیز با ساخت بند کمال خان و همچنین منحرف کردن آب رودخانه هیرمند، مانع استفاده ایران از حقابه خود طبق معاهده ۱۳۵۱ شده است. این اقدام موجب از

---

۱. رژیم اشغالگر اسرائیل بعد از سقوط رژیم بشار اسد بسیاری از زیرساخت‌های حیاتی سوریه اعم از نظامی و غیرنظامی را به بهانه اینکه ممکن است آنها در آینده بر ضد اسرائیل مورد استفاده قرار گیرند، بمباران و نابود کرده است.

۲. رژیم اشغالگر اسرائیل علاوه‌بر تخریب تعدادی از زیرساخت های حیاتی ایران در زمان جنگ ۱۲روزه، به برخی از زیرساخت‌های حیاتی در قبل و بعد از جنگ ۱۲روزه نیز حمله کرده و سبب تخریب یا آسیب شدید به آنها شده است.

۳. این اقدام ترکیه نه فقط با تعهدات دوجانبه آن کشور با سوریه و عراق مغایرت دارد، بلکه در تعارض با کنوانسیون‌های «بهره‌برداری از آبراهه‌های غیرقابل کشتیرانی»، رامسر در مورد تالاب‌ها، مقابله با بیابان‌زایی، اسپو، آرهوس و اعلامیه استکهلم است که بسیاری از مقررات این اسناد از ویژگی عرفی برخوردار شده، برای تمام کشورها لازم‌الاتباع‌اند. ترکیه با این اقدام لطمات شدید به زیرساخت‌های حیاتی کشورهای سوریه و عراق و ارمنستان و تا حدودی جمهوری آذربایجان وارد کرده، آنها را با بحران‌های محیط زیستی، اقتصادی، اجتماعی، انسانی و امنیتی مواجه کرده است. آثار این بحران‌ها گریبانگیر کشور ایران هم در غرب و شمال غرب می‌شوند.

میان رفتن زیرساخت‌های حیاتی کشاورزی و آب آشامیدنی در بخشی از استان سیستان و بلوچستان ایران شده، سبب کوچ (جابه‌جایی) اجباری صدهزار نفر از ساکنان آن منطقه شده است.[1] اگرچه این ساخت‌وسازها و اختلال‌های ناشی از آنها به‌ظاهر به قصد تعرض به زیرساخت‌های حیاتی دولت‌های هم‌جوار انجام نشده‌اند؛ اما این‌گونه عملکردها در واقع تعرض به زیرساخت‌های ارائه‌کننده خدمات حیاتی به مردم غیرنظامی در کشورهای آسیب‌دیده و در نتیجه وارد نمودن خسارات اغلب جبران‌ناپذیر به آنان است.

اگرچه ممکن است بتوان به برخی از اصول و قواعد بین‌المللی برای برخورد با این‌گونه تعرض‌ها استناد نمود، اما ایجاد ممنوعیت برای این‌گونه اقدام‌ها برای حفاظت از زیرساخت‌های حیاتی به‌سهولت ممکن نیست؛ پدیده‌ای که خود نیاز به تأمل و مطالعه بیشتر و یافتن قواعد حقوقی الزام‌آور و نه مشورتی دارد، که می‌تواند موضوع تحقیق دیگری قرار گیرد.

منابع

کتاب

۱. آقایی، کامران، ***مکتب‌های تفسیری در حقوق بر بنیاد هرمنوتیک حقوقی***، تهران: میزان، ۱۳۸۸.

۲. بیگ‌زاده، ابراهیم، ***حقوق بین‌الملل***، جلد ۲ (روابط تابعان)، تهران: میزان، چاپ دوم، ۱۴۰۲.

۳. دورمن، کنوت، ***عناصر جنایات جنگی در اساسنامه دیوان بین‌المللی کیفری***، ترجمه زهرا جعفری، زهرا محمودی و پریسا سفیدپری، تهران: مجد، ۱۳۹۳.

۴. زمانی، سید قاسم و نادر ساعد (به اهتمام و ویرایش)، ***حقوق بشردوستانه در مخاصمات مسلحانه***، تهران: شهر دانش، ۱۳۸۷.

۵. کرافورد، جیمز، ***حقوق مسئولیت بین‌المللی (قواعد عمومی)***، ترجمه ابراهیم گل، علیرضا کریمی و سیامک کریمی، تهران: سنگلج قلم، ۱۳۹۵.

References

Books

1. Agha’ei, Kamran, *Interpretive Schools in Law Based on Legal Hermeneutics*, Tehran: Mizan, 2009. (In Persian)
2. Beigzadeh, Ebrahim, *International Law*, Volume 2 (Relations Between Subjects), Tehran: Mizan, Second Edition, 2023. (In Persian)
3. Benoit, Dupont. *Essential Infrastructure*, University of Montreal Press, Montreal. (In French)
4. Chachra, Deb, *How Infrastructure Works: Inside the Systems That Shape Our World* Transworld Digital, 2023.
5. Crawford, James, *International Liability Law,* Translated by: Ebrahim Gol, Alireza Karimi and Siamak Karimi, Tehran: Sangelaj Ghalam, 2016. (In Persian)
6. De Frouvill, Olivier et Anne-Laure Chaumette. *International Criminal Law: Sources, Incriminations, Responsibility*, Paris: Pedon, 2012. (In French)
7. De Sereville, Etienne. *Cybersecurity of Critical Infrastructure: Applying and Implementing the NIS 2 Directive*, Dunod, 2025. (In French)

[1]. باید گفت که علی‌رغم چندین دور مذاکرات با حکومت طالبان در افغانستان نه فقط مشکلات ناشی از نقض تعهدات افغانستان در چارچوب معاهده ۱۳۵۱ درمورد رودخانه هیرمند حل نشده‌اند، مشکل ناشی از اقدام اخیر افغانستان، یعنی ساخت سد بر رودخانه مرزی هریرود (این رودخانه در بخشی از مرز دو کشور که یک صد و چهار کیلومتر طول دارد، در جریان است و سپس وارد کشور ترکمنستان می‌شود)، بر آنها افزوده شده است.

8. Dörmann, Knut, *Elements of War Crimes In Statute of International Court of Justice,* Translated by: Zahra Ja'fari, Zahra Mahmoudi and Parisa Sefid-Pari, Tehran: Majd, 2014. (In Persian)
9. Guarnieri, Franck; Luciano Morabito and Robert Benoit, *Reducing the Vulnerability of Critical Infrastructure*, Paris : Tec et Doc, 2009. (In French)
10. Henckaerts J. M. and Louise Doswald Beck, *Customary International Humanitarian Law*, Volume 1 (Rules), Cambridge University Press, 2005.
11. Schmitt M. N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Second Edition, 2017.
12. Selected Basic Documents Related to the International Criminal Court, International Criminal Court Publication, *The Hague*, 2009.
13. Zamani, Sayyed Ghasem and Nader Sa'ed (eds.), *Humanitarian Law in Armed Conficts,* Tehran: Shahr-e-Danesh, 2008. (In Persian)

Articles

14. "Security Considerations for Critical Infrastructure", *Canadian Centre for Cyber Security,* 2025, Available at : https://www.cyber.gc.ca/fr/orientation/considerations-en-matiere-de-securite-pour-les-infrastructures-essentielles-itsap10100 (In French)
15. Aramis, "Access to Essential Infrastructure and Resources", 2025. (In French)
16. Bannelier, Karine, "International Law in the Face of the Destruction or Disruption of Essential State Infrastructure", *French Yearbook of International Law (A.F.D.I)*, Volume LXIX, 2023 .(In French)
17. Casanovas M. and Aloys gheim. "Cybersecurity –Is the Power System Logging Behind? " *IEA,* In: Jack.V, "Europe's Grid Is under a Cyberattack Deluge, Industry Warns", *Politico*, 2023.
18. Commission on Critical Infrastructures Protections, "Defense critical infrastructures programme", 1996.
19. Critical Foundations protecting America's Infrastructures, "The Report of President's Commission on Critical Infrastructure Protection", October 1997.
20. De Felice, Fabio; Ilaria Baffo and Antonella Petrillo. "Critical Infrastructures Overview: Past, Present and Future'', *MDPI,* 2022.
21. European Center for Constitutional and Human Rights (ECCHR)," Global Initiative Against Impunity, *Making Justice work*, 2024. (In French)
22. European Parliament. "New Rules to Protect Critical EU Infrastructure", 2022, Available at: https://www.europarl.europa.eu/news/fr/pressroom/20221118IPR55705/de-nouvelles-regles-pour-proteger-les-infrastructures-critiques-de-l-ue
23. Fernandez Julian, Pacreau Xavier, Ubeda – Saillard Muriel, *Rome Statute of the International Criminal Court: Article-by-Article Commentary*, Second Edition, Volume 1, Paris: Pedone, 2019.
24. France International Politics, "For Iran, Israel's strike on this Gas Site Is a Major Blow," May 15, 2023. (In French)
25. Gallagher. "Risk of Cyber Contagion and Protection of Critical Infrastructure'', 2025. (In French)
26. Group of Governmental Expert on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, *General Assembly*, United Nations. (In French)
27. Guillaume Jean – Sebastien. "Gase in Palestine", Conflicts, *Geopolitical Review*, 2023. (In French)
28. Haataja, S. I. "Cyber Operations against Critical Infrastructures under Norms of Responsibility State Behaviour and International Law, International", *Journal of Law and Information Technology*, Volume 30, 2022.
29. ICRC, "Sudan: Attacks against Essential Civilian Infrastructure are Increasing Amid Escalating Fighting", *Press Release*, January 25, 2025. (In French)
30. ICRC, "What are the Indirect Effects of Ettacks against Energy Infrastructure?", 2025. (In French)
31. International Federation for Human Rights, "Making Justice Work: Civil Society Unites in the Global Fight Against Impunity", 2025. (In French)

32. INTERPOL, “Protecting Critical Infrastructure against Terrorist Attacks: A Collection of Good Practices)”, *The Directorate of the Counter Terrorism Committee and the Counter Terrorism Office*, 2018. (In French)
33. Newbill C. M. “ Defining Critical Infrastructures for a Global Application”, *Indiana Journal for a Global Studies*, Volume 26, Issue 2, 2019.
34. OECD, “Council Recommendations on the Protection of Critical Information Infrastructure”, *OECD Legal Instrument*, 2025. (In French)
35. Paris Call for Trust and Security in Cyberspace. “Protecting Critical Infrastructures against Systemic Harms: A Path Forward to Overcome National Discrepancies?” November 2023. (In French)
36. Situation in Ukraine: ICC Judges Issue Arrest Warrants against Sergei Ivanovich Kobylash and Viktor Nikolayvich Sokolov, Press release of 5 March 2025, Official website of the ICC, Reference date 25 August 2025. (In French)
37. Sonesson T. R; Jonas Johasson and Alexander Cedergen. “Governance and Interdependencies of Critical Infrastructures: Exploring Mechanisms for Cross Sector Resilience”, Google Scholar, 2021.
38. The Infrastructures of the European Union and the Computer Problem of the Year 2000, Quarter 1999. (In French)
39. Tremblay, Monica. “Essential Infrastructure: A Challenge for State Security”, Evolving Report, Laboratory for the Study of Public Policies and Globalization, *ENAP, The University of Public Administration.* (In French)
40. UN, Office of Counter-Terrorism. “Protecting Critical Infrastructure Against Terrorist Attacks: A Collection of Good Practices”. (In French)