Modern Technologies Law

University of Science and Culture

http://doi.org//10.22133/mtlj.2025.424362.1265

Resort to Self-Defense Against Cyber Attacks by Non-State Actors in International Law

Parviz Farshasaid[1]* Mahmoud Jalali[2]

[1] Ph.D in Public International Law, Department of International law, Isfahan (Khorasgan) Branch ,Islamic Azad University, Isfahan, Iran.

[2] Associate Prof. Department of Law, University of Isfahan, Isfahan, Iran.

Article Info

Original Article

Received:
08-11-2023
Accepted:
28-09-2024

Key Words:
Cyber Attacks
Tallin Manual
Self Defence
Non- State Actors

Abstract

In the discussion of resorting to Self defenseSelf-defense against cyber attackscyber-attacks by non-State actors, at first it must be determined that for what type of cyber attackcyber-attack the right to Self defenseSelf-defense is allowed. The most appropriate and relevant definition in relation to the subject under discussion is the definition provided in Article 30 of the Tallinn Manual, because it considers a cyber attackcyber-attack as an attack that causes injury or death to persons and damage and destruction to objects. The main question of the current research is that according to the rules of international law, is it possible to resort to Self defenseSelf-defense against cyber attackscyber-attacks by non-state actors? This question has been answered by using the descriptive-analytical method, that although traditionally the procedure was based on the acceptability of Self defenseSelf-defense against States, but after the September 11 terrorist attacks, Self defenseSelf-defense against non-state actors was also recognized. Therefore, against cyber attackscyber-attacks by non-Statenon-state actors, if international law regulations are followed, Self defenseSelf-defense can be resorted to, either with cyber or non-cyber tools.

.

***Corresponding author**
e-mail: parvizfarshasaid@yahoo.com

How to Cite:
Farshasaid, P., & Jalali, M. (2025). Resort to Self-Defence against Cyber Attacks by Non-State Actors in International Law. *Modern Technologies Law*, *6*(12), 213-229.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

1. Introduction

The rise of innovative payment methods represents a transformative shift in the retail payments landscape, In international law, the term non-state actors encompass a wide range of actors at the international level, from non-governmental organizations to multinational corporations. However, in recent decades, new actors have emerged in the international community in the form of non-state actors who have pursued terrorist goals. With attacks taking place every day in cyberspace, it seems that the era of cyber warfare has arrived. Now, given the use of this new technology by states and non-state actors and attacks on states and individuals, the question arises as to whether existing international law applies in this area. It is a clear fact that the new style of warfare is not similar to the type of warfare we have had before and that the laws that currently exist belong to the type of warfare and the means of warfare of the twentieth century. When the authors of the Charter were drafting and writing it, what they had in mind when they considered the prohibition of the use of force was more in relation to the military force that had been used in World War II. For example, tanks, aircraft, and weapons such as nuclear weapons, which was the impetus for drafting and writing the. Article 51 of the Charter is an exception to the principle of non-use of force. Article 51 of the Charter of the United Nations states:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense of Members if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security. Members shall immediately report to the Security Council any measures taken in the exercise of this right of self-defense. Such measures shall in no way impair the powers and responsibilities of the Security Council under the present Charter for the maintenance and restoration of international peace and security, and the Council may take such measures as it may deem necessary.

Even in this article, the word force is not specified. The ability of cyber technologies to carry out attacks makes them unlike any other weapon in history. Cyber-attacks depend on information networks around the world, networks that states depend on for everything from entertainment to banking to space travel. As the world's dependence on information systems increases, so too does the impact and capability of cyber-attacks. Currently, due to the increase in cyber-attacks and the risk of these attacks, states are improving their information infrastructures. The ease of conducting cyber-attacks and their stealthy nature make them more attractive for certain types of warfare.

In cyberspace, attacks are also carried out by non-state actors, sometimes not affiliated with any state. This research analyzes whether states can resort to self-defense against cyberattacks by non-state actors..

2. Methodology

To regularly assess and update regulatory frameworks to address emerging challenges. The interplay between In this research, we tried to collect and gather information from the primary sources (including laws, regulations, directives, bylaws, judicial decisions, etc.) and secondary sources (such as books and articles, theses, research reports, etc.) in scientific research data centers, official and reputable websites, libraries, and similar resources.

According to the title of the article, which refers to Self-defense against cyber-attacks by non-state actors in international law, the concepts of cyber-attacks, armed attacks, and the inherent right of Self-defense have been discussed, and then the attribution of cyber-attacks has been discussed. In the following, the conditions of Self-defense are discussed, and the principles of necessity, proportionality, and Immediacy are discussed and analyzed. Then the nature of Self-defense against cyber-attacks is discussed in detail, and finally, Self-defense against cyber-attacks by non-State actors is analyzed.

3. Results and Discussion

In the discussion of Self-defense against cyber-attacks, it should be said that cyber-attacks are an emerging phenomenon that treaties or international customs has not yet been formed for them; Therefore, the matter should be analyzed within the framework of the existing rules of international law.

So, those types of cyber-attacks, which reach the threshold of an armed attack, i.e., cause damage and destruction to objects and kill and injure people, the right of Self-defense rises for states.

A related international obligation, which is breached by a cyber-attack and amounts to an armed attack, is the prohibition of the use of force and thus constitutes a violation of the UN Charter.

In this research, the issue of Self-defense against cyber-attacks by non-State actors has been discussed in detail, and it has been concluded that it is possible to resort to Self-defense against cyber-attacks by non-State actors, if Self-defense is based on the rules of international law and the principles of Self-defense such as proportionality, necessity, and immediacy are observed.

4. Conclusions and Future Research

The complexity and variety of cyber-attacks make it difficult to put them in the current legal framework. Cyber-attacks have destructive results such as killing and injuring people, destroying assets and property. Both states and non-state actors can launch cyber-attacks, targeting anything and anyone, including people, objects, and even entire societies.

Currently, the best definition of cyber-attack, which is related to the topic of discussion of this article, i.e., self-defense against cyber-attacks by non-state actors, lies in Article 30 of the Tallinn Manual. This definition includes all cyber operations that cause injury and death to persons and damage and destruction to objects .

A related international obligation that is violated by a cyber-attack and amounts to an armed attack is the prohibition of the use of force; Therefore, it is a violation of the United Nations Charter. In the discussion of self-defense against non-state actors, there are two narrow and broad views, and even the International Court of Justice has dealt with this issue with ambiguity, and the court's procedure has only been on identifying self-defense against states. However, for the first time after the terrorist attacks of Al-Qaeda in the United States on September 11, 2001 and the approval of resolutions 1373 and 1368, the right of self-defense against non-state actors was established, and the group of international experts of the Tallinn Manual also accepted the right of self-defense against non-state actors; Therefore, it can be concluded that currently, according to the issues raised, it is possible to resort to self-defense against cyber-attacks by non-state actors, if self-defense is based on the rules of international law and the principles of self-defense such as proportionality, necessity and immediacy must be observed.

حقوق فناوری‌های نوین

http://doi.org//10.22133/mtlj.2025.424362.1265

توسل به دفاع مشروع در قبال حملات سایبری عوامل غیردولتی در حقوق بین‌الملل

پرویز فرشاسعید[1]*، محمود جلالی[2]

[1] دکتری حقوق بین‌الملل عمومی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران.

[2] دانشیار گروه حقوق، دانشگاه اصفهان، اصفهان، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۸/۱۷
تاریخ پذیرش:
۱۴۰۳/۰۶/۰۷

واژگان کلیدی:
حملات سایبری
راهنمای تالین
دفاع مشروع
عوامل غیردولتی

چکیده

در بحث توسل به دفاع مشروع در قبال حملات سایبری عوامل غیردولتی، نخست باید مشخص شود که در قبال چه نوع حملهٔ سایبری حق دفاع مشروع ایجاد می‌شود. مناسب‌ترین و مرتبط‌ترین تعریف دررابطه‌با موضوع موردبحث، تعریف ارائه‌شده در مادهٔ ۳۰ راهنمای تالین است؛ زیرا حملهٔ سایبری را حمله‌ای می‌داند که باعث ایجاد جراحت یا مرگ برای اشخاص و خسارت و تخریب به اشیا می‌شود. سؤال اصلی پژوهش حاضر این است که باتوجه‌به قواعد حقوق بین‌الملل حاضر آیا امکان توسل به دفاع مشروع در قبال حملات سایبری عوامل غیردولتی وجود دارد؟ با استفاده از روش توصیفی - تحلیلی به این سؤال پاسخ داده شده است که اگرچه به‌طور سنتی رویه بر پذیرفتنی‌بودن دفاع مشروع علیه دولت‌ها بوده، اما پس از حملات تروریستی ۱۱ سپتامبر، دفاع مشروع علیه عوامل غیردولتی نیز به‌رسمیت شناخته شد؛ بنابراین در برابر حملات سایبری عوامل غیردولتی درصورت رعایت مقررات حقوق بین‌الملل می‌توان به دفاع مشروع چه با ابزار سایبری و چه غیرسایبری متوسل شد.

***نویسندهٔ مسئول**

رایانامه: parvizfarshasaid@yahoo.com

نحوهٔ استناددهی:

فرشاسعید، پرویز، و جلالی، محمود (۱۴۰۴). توسل به دفاع مشروع در قبال حملات سایبری عوامل غیردولتی در حقوق بین‌الملل. حقوق فناوری‌های نوین، ۶(۱۲)، ۲۱۳-۲۲۹.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

در حقوق بین‌الملل، اصطلاح عوامل غیردولتی طیف وسیعی از کنشگران را در سطح بین‌المللی، از سازمان‌های غیردولتی گرفته تا شرکت‌های چندملیتی، دربر می‌گیرد. به‌هرحال در دهه‌های اخیر، بازیگران جدیدی در قالب عوامل غیردولتی در جامعهٔ بین‌المللی شکل گرفته‌اند که اهداف تروریستی را دنبال کرده‌اند (Jalali & Poursaeed, 2020, p. 72). با حملاتی که هر روزه در فضای سایبر انجام می‌گیرد به نظر می‌رسد که عصر جنگ‌های سایبری فرارسیده است. حال باتوجه‌به استفادهٔ دولت‌ها و عوامل غیردولتی از این فنّاوری جدید و حملات علیه کشورها و اشخاص این سؤال پیش می‌آید که آیا قوانین بین‌الملل حاضر در این حوزه کاربرد دارد؟ این حقیقت آشکار است که سبک جدید جنگ شباهتی به نوع جنگی که قبلاً داشته‌ایم ندارد و قوانینی که در حال حاضر وجود دارد متعلق به نوع جنگ و ابزارهای جنگی قرن بیستم است (Jolley, 2012, p. 1). زمانی که نویسندگان منشور درحال تدوین و نوشتن آن بودند، آنچه آن‌ها از ممنوعیت کاربرد زور در ذهن داشتند بیشتر در ارتباط با نیروی نظامی بود که در جنگ جهانی دوم استفاده شده بود. برای مثال تانک‌ها، هواپیماها و سلاح‌هایی مانند سلاح‌های هسته‌ای، که انگیزه‌ای برای تنظیم و نوشتن منشور بود (Jolley, 2012, p. 1). مادهٔ ۵۱ منشور استثنایی بر اصل کاربردنداشتن زور است. در مادهٔ ۵۱ منشور سازمان ملل متحد آمده است:

درصورت وقوع حملهٔ مسلحانه علیه یک عضو سازمان ملل متحد، تا زمانی که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین‌المللی به عمل آورد، هیچ‌یک از مقررات این منشور به حق ذاتی دفاع مشروع انفرادی یا دسته‌جمعی اعضا لطمه‌ای وارد نخواهد کرد. اعضا باید اقداماتی را که در اعمال این حق دفاع از خود به عمل می‌آورند فوراً به شورای امنیت گزارش دهند. این اقدامات به‌هیچ‌وجه در اختیارات و مسئولیتی که طبق این منشور به شورای امنیت برای حفظ و اعاده صلح و امنیت بین‌المللی واگذار شده، وارد نخواهد کرد و این شورا می‌تواند هر زمان که ضروری تشخیص دهد، اقدامات لازم را انجام دهد.

حتی در این ماده نیز عبارت زور مشخص نشده است. توانایی فنّاوری‌های سایبری برای انجام حملات آن‌ها را بی‌شباهت به هر نوع سلاح در طول تاریخ کرده است. حملات سایبری به شبکه‌های اطلاعاتی در کل جهان وابسته است، شبکه‌هایی که دولت‌ها برای هرچیزی از سرگرمی تا بانکداری و سفرهای فضایی به آن‌ها وابسته‌اند. درحقیقت همچنان که وابستگی جهان به سیستم‌های اطلاعاتی افزایش می‌یابد تأثیر و توانایی حملات سایبری نیز افزایش پیدا می‌کند. در حال حاضر، به‌دلیل افزایش حملات سایبری و خطر این حملات، دولت‌ها درحال بهبودبخشیدن زیرساخت‌های سیستم‌های اطلاعاتی‌شان هستند. سهولت انجام حملات سایبری و ماهیت پنهانی آن‌ها این حملات را برای انواع خاصی از جنگ جذاب‌تر می‌کند.

با شکل‌گیری فضای سایبری، میدان نبرد جدیدی در روابط بین‌الملل گشوده شده است که منازعهٔ میان کشورها را به فضای سایبری منتقل کرده است. در این فضا، تنها فشردن دگمه‌ای برای ایجاد تخریب گسترده در زیرساخت‌های هر کشوری کافی است و هیچ کشوری به‌رغم قدرت اقتصادی نظامی یا سیاسی آن در امان نیست (Mohammad ali poor, 2017, p. 233).

در فضای سایبری، حملاتی توسط عوامل غیردولتی نیز انجام می‌گیرد که گاهی به هیچ دولتی وابسته نیستند. این‌که آیا دولت‌ها در قبال حملات سایبری عوامل غیردولتی می‌توانند به دفاع مشروع متوسل شوند، در این تحقیق تجزیه‌وتحلیل شده است.

۱. حملات سایبری

اگرچه برای حملهٔ سایبری تعاریف متعددی ارائه شده است، تعریفی که مناسب بحث ما، یعنی دفاع مشروع در قبال حملات سایبری عوامل غیردولتی باشد، در مادهٔ ۳۰ راهنمای تالین[1] نهفته است. مادهٔ ۳۰ راهنمای تالین حملهٔ سایبری را به‌عنوان یک عملیات، خواه تهاجمی یا تدافعی که به‌طور منطقی انتظار می‌رود تا ایجاد جراحت یا مرگ برای اشخاص یا خسارت و تخریب به اشیا کند تعریف کرده است (Schmitt, 2013, rule. 30). این تعریف نسبت به تعاریف دیگری که دربارهٔ حملات سایبری ارائه شده است کامل‌تر و بیشتر بر نتیجهٔ حمله متمرکز است.

درحقیقت اگر حملهٔ سایبری باعث صدمه‌زدن به افراد یا اشیایی شود که برای بقای این افراد لازم است حق دفاع مشروع ایجاد می‌شود. اگر این دیدگاه پذیرفته شود، آنچه حق دفاع مشروع را ایجاد می‌کند واردآمدن خسارات واقعی است و نه به‌صورت لزوم وسعت و اندازهٔ حمله. در این معنا، حتی یک حمله با سطح پایین، که باعث به‌خطرانداختن مردم شود، ممکن است حق دفاع مشروع را ایجاد کند (Lieblich, 2019, p. 27).

۲. حملات مسلحانه و حق ذاتی دفاع مشروع

مفهوم حملهٔ مسلحانه محدودتر از کاربرد زور است. یک حملهٔ مسلحانه همیشه کاربرد زور را شکل می‌دهد، اما کاربرد زور همیشه به حد یک حملهٔ مسلحانه نمی‌رسد؛ بنابراین لازم است شدیدترین اشکال کاربرد زور، یعنی آن‌هایی که حمله مسلحانه را شکل می‌دهد، از اشکال ضعیف‌تر تمایز دهیم (I.C.J. Reports, 1986, para. 191). مقیاس و تأثیر حمله مهم‌ترین فاکتورها برای تعیین آستانهٔ حمله‌ای مسلحانه هستند.

نه منشور و نه هیچ معاهدهٔ دیگری مفهوم حملهٔ مسلحانه را تعریف نمی‌کنند. در بحث مفاهیم حملهٔ مسلحانه و تجاوز باید بیان کرد که این دو مفهوم یکسان نیستند، اگرچه به نظر می‌رسد بعضی از حقوق‌دانان این دو را یک مفهوم بدانند. عبارت تجاوز توسط مجمع عمومی سازمان ملل متحد به‌عنوان کاربرد زور مسلحانه توسط یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر، یا در هر روش دیگرمتناقض با منشور سازمان ملل متحد تعریف شده است (U.N.G.A. Res. 3314, 1974, article. 1).

مادهٔ ۳ قطعنامه تعریف تجاوز مجمع عمومی مواردی از اعمال تجاوز را برمی‌شمارد. این اعمال شامل حملات، بمباران‌ها، شلیک‌های مرزگذر و محاصره هستند (U.N.G.A. Res. 3314, 1974, article. 3). این موارد ذکرشده فهرستی کامل نیست و شورای امنیت ممکن است موارد دیگری را نیز به‌منزلهٔ اعمال تجاوز به‌شمار آورد (U.N.G.A. Res. 3314,1974, article. 4). فقط درنتیجهٔ یک حملهٔ مسلحانه حق دفاع مشروع وجود دارد و این یک استثنا در برابر ممنوعیت کاربرد زور است.

در بحث دفاع مشروع در برابر حملات سایبری نیز گفتنی است که حملات سایبری پدیده‌ای نوظهور است که هنوز قاعدهٔ حقوقی معتبری در قالب معاهدات یا عرف بین‌المللی درخصوص آن شکل نگرفته است؛ ازاین‌رو موضوع باید در چهارچوب قواعد موجود حقوق بین‌الملل تحلیل شود و از طرفی، به اذعان کارشناسان و داده‌های موجود ایجاد اختلال و آسیب در شبکه‌های اطلاعاتی و سیستم‌های الکترونیکی نیروگاه‌های برق و تولید انرژی سیستم‌های حمل‌ونقل هوایی و مانند آن آثار زیان‌بار در تخریب زیرساخت‌های حساس داشته و حتی قابلیت تلفات جانی دارد و در سطوح بالاتر ممکن است منافع ملی و حیاتی دولت را در معرض خطر جدی قرار دهد (Namdar & Qasemi, 2018, p. 228)؛ بنابراین آن دسته از حملات سایبری، که به آستانهٔ حمله‌ای مسلحانه می‌رسند، یعنی موجب واردآمدن خسارت و تخریب به اشیا و کشته و زخمی‌شدن افراد می‌شوند، در قبال آن‌ها حق دفاع مشروع برای دولت‌ها ایجاد می‌شود.

---

۱. راهنمای تالین دربارهٔ حقوق بین‌الملل قابل‌اعمال دربارهٔ جنگ سایبر است که از سال ۲۰۰۸ تا ۲۰۱۲ توسط یک گروه از متخصصان بین‌المللی نوشته شد و در سال ۲۰۱۳ منتشر شد.

۳. انتساب حملات سایبری

در بحث حملات سایبری، این حقیقت روشن است که به‌علت وابسته‌شدن گستردهٔ تمامی امورات بشر به فضای سایبر و اینترنت، خطر حملات سایبری صلح و امنیت بین‌المللی را بیش‌ازپیش تهدید می‌کند (Farshasaid,P,& Jalali, 2022, p. 17). ویژگی‌های فضای سایبر، به‌ویژه وابستگی متقابل زیرساخت‌های سایبری، یکپارچگی شبکهٔ عمومی و جهانی اینترنت، آزادی دسترسی به آن برای همگان و فاقد مرز بودن، رعایت حقوق بی‌طرفی و ردیابی موارد نقض بی‌طرفی و شناسایی مرتکبان را دشوار می‌سازد (Shaygan, 2016, p. 354).

تعهد بین‌المللی مرتبط، که ازطریق یک حملهٔ سایبری نقض می‌شود و به حد حمله‌ای مسلحانه می‌رسد، ممنوعیت کاربرد زور است و بنابراین نقض منشور سازمان ملل متحد به‌حساب می‌آید. اگرچه نقض‌های دیگر مثل نقض‌های حقوق بین‌الملل بشردوستانه نیز می‌تواند به اعمال متخلفانهٔ بین‌المللی منتج شود؛ بنابراین هدف دفاع مشروع فقط زمانی قانونی است که حمله منتسب به یک دولت باشد.

انتساب حملات سایبری مشکل است؛ زیرا اولاً اغلب روش‌های ماهرانه‌ای برای پنهان‌کردن هویت حمله‌کننده استفاده می‌شود؛ ثانیاً حملات سایبری می‌توانند ازطریق رایانه‌هایی از قسمت‌های مختلفی ازجهان انجام گیرند؛ ثالثاً حملات سایبری می‌توانند در یک چشم به هم زدن اتفاق بیفتند. حادثهٔ تالین[1] نمونه‌ای از پیچیدگی انتساب را نشان می‌دهد؛ چون حدود ۸۵۰۰۰ رایانه از سراسر جهان برای انجام حملات استفاده شد.

برای درک بهتر و عمیق‌تر بحث انتساب حملات سایبری نیاز است به کنکاش در تعدادی از پرونده‌های حقوقی بپردازیم. برای مثال در قضیهٔ نسل‌کشی بوسنی، دیوان دادگستری بین‌المللی بیان کرد ادعاهایی که علیه دولت‌های درگیر به‌خاطر اتهامات سنگین وجود دارد نیازمند مدارک کامل است. اینکه استاندارد یکسانی برای انتساب چنین اعمالی استفاده می‌شود (I.C.J Reports, 2007, para. 209).

دولت‌ها مسئولیت دارند اقدامات مناسبی برای حفاظت از حقوق دولت‌های دیگر انجام دهند. در قضیهٔ کانال کورفو (انگلستان علیه آلبانی)، دیوان بین‌المللی دادگستری این‌گونه نظر داد:

این وظیفه و تکلیف هر دولتی است که به‌طور آگاهانه اجازه ندهد قلمروش برای اعمالی که مغایر حقوق دیگر کشورهاست استفاده شود (I.C.J Reports, 1949, p. 22). بعدها در قضیهٔ نیکاراگوئه، دیوان تأکید کرد که بین دولت‌های مستقل، احترام به حاکمیت سرزمینی یک اصل اساسی روابط بین‌الملل است (I.C.J Reports, 1986, para. 22). گروه کارشناسان بین‌المللی سایبری نیز در مادهٔ ۵ راهنمای تالین دراین‌باره بر این نظرند که دولت‌ها اجازه ندارند در قلمروشان اجازهٔ استفاده از تأسیساتشان را برای اعمال منع‌شده علیه دولت‌های دیگر بدهند (Schmitt, 2013, rule. 5).

همچنین این گروه بر این نظر بودند که اگر عملیات سایبری ازطریق زیرساخت‌های سایبری یک دولت انجام شود، چنین عملیاتی دلیل مشارکت آن دولت درآنها نیست(Schmitt, 2013, rule. 8)؛ بنابراین علی‌رغم تلاش‌های گروه متخصصان بین‌المللی برای شفاف‌سازی بحث انتساب حملات سایبری، معضل انتساب حملات سایبری همچنان در حوزهٔ سایبر باقی می‌ماند.

یکی از مهم‌ترین اهداف در ورای انتساب حملات سایبری، شناسایی عامل حملهٔ سایبری به‌منظور هدایت دفاع مشروع علیه حمله‌کنندهٔ واقعی است. حق دفاع مشروع به‌طور سنتی نیاز به انتساب کامل دارد و اجازهٔ دفاع مشروع بدون انتساب حوزهٔ دفاع مشروع را گسترده خواهد کرد. همچنین آن موقعیت‌های تنش‌های جزئی را به جنگ تمام‌عیار سایبری بین دولتها تبدیل می‌کند که براساس چهارچوب حقوقی امروز قادر نبوده‌اند تا درچنین فعالیت‌هایی مشارکت کنند. سوءاستفاده از حق دفاع مشروع توسط دولت‌ها برای دلایل سیاسی ممکن است رخ دهد. این سوءاستفاده مخالف هدف کاهش کاربرد زور در روابط بین‌المللی است.

---

۱ . در اوایل بهار سال ۲۰۰۷ کشور استونی مورد حمله سایبری قرار گرفت. حملات سایبری علیه آژانس‌های دولتی و کمپانی‌های خصوصی مانند ایستگاه‌های رسانه‌ای و بانک‌ها همراه شد. اساساً این حملات به شکل انکار سرویس توزیع شده بودند و تقریباً سه هفته طول کشیدند. هرچند که دولت روسیه دخالت خود را در ارتکاب این حملات رد کرد و هرگز انتساب قطعی این مسئله به فدراسیون روسیه محرز نشد، اما دولت استونی اعلام کرد که دولت روسیه مسئول اصلی این حملات است.

۴. شرایط توسل به دفاع مشروع

اصل ممنوعیت توسل به‌زور به‌منزلهٔ یکی از اصول بنیادین جامعهٔ بین‌المللی بر روابط دولت‌ها حاکم است و به‌موجب منشور سازمان ملل متحد، آن‌ها مکلف شده‌اند ضمن خودداری از توسل به‌زور و حتی تهدید به توسل به‌زور، اختلافات خود را ازطریق روش‌های مسالمت‌آمیز حل‌وفصل کنند. بدین‌ترتیب، دفاع مشروع درحکم مهم‌ترین استثنا بر اصل ممنوعیت توسل به‌زور پذیرفته شده است؛ لذا مطلوب آن است که واژهٔ زور در بند ۴ مادهٔ ۲ منشور حداقل آن‌چنان موسع تفسیر شود که هر استفادهٔ مهمی از زور ممنوع تلقی شود و در همین راستا، از استثنا مذکور در مادهٔ ۵۱ تفسیری مضیق و دقیق به عمل آوریم.

به همین خاطر، توسل به دفاع مشروع باید هرچه محدودتر و تحت شرایط و ضوابط خاصی صورت پذیرد تا امکان سوءاستفاده از آن محدودتر شود. روند روبه‌رشد تحول و پیشرفت روزافزون فنّاوری اطلاعات و کاربرد گستردهٔ آن در عرصهٔ فضای مجازی و استفاده از ابزار و تجهیزات سخت‌افزاری و نرم‌افزاری مرتبط بر روش‌ها و فنون نبردها تأثیر داشته و شکل خاصی از جنگ را پدید آورده است. الزام نیروهای مسلح کشورها به بهره‌برداری از آخرین دستاوردهای فنّاوری را امری حیاتی کرده است؛ ازاین‌رو، شناخت صحیح و ورود به موقع در عرصه‌های نوین دفاعی همواره یکی از دغدغه‌های طراحان و بازیگران حوزهٔ راهبرد و دفاع است (بختیاری، ۱۳۹۳، ص ۴۷). در ادامه، شرایط توسل به دفاع مشروع بررسی می‌شود. نخستین و مهم‌ترین شرط دفاع مشروع، ارتکاب حملهٔ مسلحانه است. به دلیل این‌که حملهٔ مسلحانه قبلاً بررسی شده است، در این قسمت به سایر شرایط توسل به دفاع مشروع می‌پردازیم.

۴-۱. اصل ضرورت

یکی دیگر از شرایط اساسی توسل به قوای قاهره در قالب دفاع مشروع، ضرورت است؛ یعنی هیچ‌گونه جایگزین دیگری جز استفاده از زور در مقابل زور وجود نداشته باشد. اگرچه متن مادهٔ ۵۱ منشور سازمان ملل متحد در این مورد، که وجود حالت ضرورت شرط استفاده از حق دفاع مشروع محسوب می‌شود، صراحتی ندارد؛ لیکن با اطمینان می‌توان گفت که به‌موجب مقررات مادهٔ مزبور، وجود حالت ضرورت شرط اساسی و لازم برای استفاده از حق دفاع مشروع است؛ زیرا اولاً ارتباط مادهٔ ۵۱ با حقوق بین‌الملل عرفی مسلم است و بر همین اساس، شرایطی که در گذشته به‌موجب حقوق بین‌الملل عرفی برای اعمال حق دفاع مشروع وجود داشته، ازجمله ضرورت، اکنون نیز وجود دارد. ثانیاً چون مادهٔ ۵۱ منشور استفاده از حق دفاع مشروع را درصورت وقوع حملهٔ مسلحانه تا موقعی که سازمان ملل متحد اقدام لازم را برای تأمین صلح اتخاذ نکند اجازه می‌دهد؛ درحقیقت برای استفاده از دفاع مشروع، شرط ضرورت در حملهٔ مسلحانه‌ای به وقوع می‌پیوندد که کشوری مورد تهاجم نظامی قرار گیرد و سازمان ملل متحد اقدامی به عمل نیاورد؛ در این حالت، ارکان ضرورت و فوریت خودبه‌خود تحقق می‌یابد. دربارهٔ شرط ضرورت، دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه این نظر را داد:

برای مثال منشور سازمان ملل هیچ‌گونه قانون خاصی دربر ندارد؛ درحالی‌که دفاع مشروع تنها اقداماتی را ضمانت می‌کند که متناسب با حمله مسلحانه هستند و برای پاسخ‌دادن به آن ضروری‌اند. قانونی که در حقوق بین‌الملل عرفی به‌درستی جا افتاده است (I.C.J. Reports 1986, p. 176).

ملزومهٔ ضرورت در بحث دفاع مشروع به این معناست که دفاع باید به‌طورجدی ضروری باشد؛ بنابراین هیچ گزینهٔ مؤثر دیگری نباید هنگام کاربرد زور در دسترس باشد.

در حوزهٔ سایبری بحث ضرورت برای این مطرح می‌شود که وقتی دولتی مورد حملهٔ سایبری قرار بگیرد و این حمله به حد کاربرد زور برسد، دولت قربانی برای دفع آن بتواند به دفاع مشروع بپردازد؛ البته اقدامات دربردارندهٔ زور ممکن است با اقدامات بدون کاربرد زور مانند دیپلماسی، تحریم‌های اقتصادی یا اجرای قانون ترکیب شوند (Tallin Manual, 2013, rule. 14, para. 2).

کلید تجزیه‌وتحلیل ضرورت در فحوای سایبر، بودن یا نبودن اقداماتی است که به سطح کاربرد زور نمی‌رسند. اگر دفاع سایبری انفعالی مانند دیوار آتش بتواند به طور مؤثر و کافی یک حملهٔ مسلحانه را خنثی کند، اقدامات دیگر، خواه سایبری یا غیرسایبری، که به سطح کاربرد زور می‌رسد، مجاز نیست؛ یعنی اگر عملیات سایبری انفعالی که به سطح کاربرد زور نمی‌رسند برای جلوگیری یا دفع حملهٔ مسلحانه‌ای مناسب باشد، کاربرد زور سایبری یا غیرسایبری به‌وسیلهٔ مقولهٔ ضرورت منع خواهد بود. اگر اقداماتی که به حد کاربرد زور نمی‌رسد، به‌تنهایی نتواند یک حملهٔ مسلحانه را دفع و از حملات متعاقب بعدی جلوگیری کند، عملیات سایبری یا غیرسایبری براساس حق دفاع مشروع مجاز هستند (Tallin Manual, 2013, rule. 14, para. 3).

۴-۲. اصل تناسب

اصل دیگری که هنگام توسل به دفاع مشروع باید رعایت شود اصل تناسب است. براساس این اصل، وسایل و حد دفاع مشروع باید با شدت حملهٔ مسلحانه متناسب باشد. برای تعیین این‌که آیا دفاع مشروع متناسب است، نیاز است با حمله مقایسه شود. به همین ترتیب، تلفات و خسارات ایجادشده از کاربرد زور در دفاع مشروع باید با خسارات ایجادشده از حمله متناسب باشد.

به‌طور خلاصه، منظور از تناسب در دفاع مشروع آن است که کشور مورد تهاجم، فقط می‌تواند به اعمالی دست بزند که برای دفع حمله ضرورت داشته و در همان حد متوقف شود. اگرچه اصل تناسب به‌صراحت در مادهٔ ۵۱ منشور سازمان ملل متحد منعکس نشده است، اما تردیدی نیست که امروزه در حقوق بین‌الملل عرفی جایگاه مستحکمی دارد.

دیوان بین‌المللی دادگستری نیز در «قضیهٔ سکوهای نفتی» بر وجود اصل تناسب به‌عنوان یکی از شرایط مهم در توسل به دفاع مشروع تأکید می‌کند و صراحتاً اعلام می‌دارد که حملات آمریکا به سکوهای نفتی ایران با حوادثی که وقوعشان بهانهٔ حمله به سکوها شده، هیچ تناسبی نداشته است (I.C.J Reports, 2003, para. 77).

بحث تناسب در حوزهٔ سایبری به این مسئله می‌پردازد که چه مقدار زور، ازجمله از نوع سایبری، نیاز است اگر کاربرد زور لازم باشد. این مقولهٔ مقیاس، حد، طول و شدت پاسخ دفاعی را تا آن حدی محدود می‌کند که به وضعیتی که باعث ایجاد حق دفاع مشروع شده پاسخ دهد. تناسب، اندازهٔ زور استفاده‌شده در حملهٔ مسلحانه را محدود نمی‌کند؛ زیرا میزان زور لازم برای دفاعی موفقیت‌آمیز به موقعیت وابسته است. برای دفع یا شکست‌دادن یک حملهٔ آنی، ممکن است مقدار زیاد یا کم زور لازم باشد. به‌علاوه، نیازی نیست تا نوع زور برای دفاع مشابه زوری باشد که در حملهٔ مسلحانه استفاده شده است؛ بنابراین ممکن است در برابر حملات مسلحانه، که به‌وسیلهٔ ابزار غیرسایبری انجام می‌گیرد، با نوع سایبری پاسخ داد و بالعکس، در برابر حملات مسلحانهٔ سایبری با ابزار غیرسایبری به دفاع مشروع پرداخت (Tallin Manual, 2013, rule. 14, para. 6).

۴-۳. اصل فوریت

براساس اصل فوریت، دفاع مشروع نباید به‌مدت طولانی بعد از حمله انجام شود؛ بلکه باید در یک دورهٔ زمانی منطقی بعد از آن‌که حمله صورت گرفت انجام پذیرد. طبق این شرط، دفاع مشروع باید بلافاصله پس از وقوع حمله آغاز شود. فوریت به دورهٔ بعد از انجام حملهٔ مسلحانه اشاره دارد که دولت قربانی ممکن است اقدام به دفاع مشروع کند. عواملی مانند تقریب زمانی بین حمله و پاسخ، دورهٔ لازم برای شناسایی حمله‌کننده و دورهٔ موردنیاز برای آماده‌کردن یک پاسخ در این ملاحظه مرتبط هستند (Tallin Manual, 2013, rule. 15, para. 9).

چالش مهمی که در بحث فوریت در دفاع مشروع در حوزهٔ سایبری ایجاد می‌شود نحوهٔ دفاع در برابر حملات سایبری است که پیوسته و در فاصلهٔ زمانی کوتاهی یکی پس از دیگری ارتکاب می‌یابد. برای مثال، یک حملهٔ سایبری ممکن است با موجی از عملیات سایبری علیه دولت قربانی انجام گیرد. اگر دولت قربانی نتیجه‌گیری کند که عملیات سایبری بیشتری احتمال دارد ادامه یابد، ممکن است آن عملیات را

سلسله‌عملیاتی سایبری در نظر گیرد و به انجام دفاع مشروع، براساس حملات سایبری انجام‌گرفته، ادامه دهد (Tallin Manual, 2013, rule. 15, para. 9).

۵. بررسی ماهیت دفاع مشروع در برابر حملات سایبری

حملات سایبری و آمادگی‌هایی که اکنون برخی کشورها کسب کرده‌اند نشان می‌دهد که رقابت برای فائق‌آمدن در حملات و دفاع سایبری آغاز شده است (Rezaei & Jalali, 2018, p. 71). دولتی که هدف عملیات سایبری در سطح حملهٔ مسلحانه قرار می‌گیرد، می‌تواند به حق ذاتی خود برای دفاع مشروع متوسل شود. تعیین اینکه یک عملیات سایبری مصداق حملهٔ مسلحانه باشد، به میزان و پیامدهای آن بستگی دارد (Tallin Manual, 2013, rule. 13).

کارشناسان اعتقاد دارند که عبارت «حملهٔ مسلحانه» نباید با کاربرد زور موجود در مادهٔ ۱۱ راهنمای تالین مساوی در نظر گرفته شود (Tallin Manual, 2013, rule. 13). دیوان بین‌المللی دادگستری نیز بیان کرده است که هر کاربرد زوری به سطح حملهٔ مسلحانه نمی‌رسد (I.C.J. Reports, 1986, pp. 191-195) و تنها وقتی که به سطح حملهٔ مسلحانه برسد، دولت‌ها حق توسل به دفاع مشروع دارند. یکی از مقوله‌های اصلی برای طبقه‌بندی یک حمله به‌عنوان حملهٔ مسلحانه، شدت آن است (Tallin Manual, rule. 13, para. 5-6)؛ بنابراین بعضی موارد به‌آسانی می‌تواند به‌عنوان حملات مسلحانه طبقه‌بندی شود، مانند آن‌هایی که منجر به واردشدن صدمه به اشخاص و اموال منجر می‌شود.

متخصصان راهنمای تالین دربارهٔ اینکه اعمال جمع‌آوری اطلاعات سایبری و اختلال جزئی خدمات اینترنتی غیرضروری به سطح حملات مسلحانه نمی‌رسد، نظر یکسانی داشتند (Tallin Manual, 2013, rule. 13, para. 6). متخصصان معتقدند اگر دولتی هدف حملات سایبری متعددی قرار گیرد که هریک به‌تنهایی در حد حملهٔ مسلحانه نباشند، اما مجموعاً تأثیر مخربی داشته باشند، تعیین‌کنندهٔ آن است که آیا این حملات با هدفی واحد انجام شده‌اند و آیا درمجموع، آستانهٔ لازم برای «مقیاس و تأثیرات» را برآورده می‌کنند (Tallin Manual, 2013, rule. 13, para. 8).

در ملاحظه با مواردی از حملات که به حد جراحت، مرگ و نابودی نمی‌رسند، اما مختل‌کننده هستند، متخصصان نتوانستند به اجماعی برسند؛ برای نمونه، حملهٔ سایبری به بازار سهام نیویورک باعث سقوط آن شد. بعضی از متخصصان نمی‌خواستند آن را حملهٔ مسلحانه در نظر گیرند؛ زیرا آن مورد، ضرر و زیان مالی بود و بعضی دیگر عقیده داشتند که به‌خاطر شدت نتایج، این حمله باید حملهٔ مسلحانه در نظر گرفته شود (Tallin Manual, rule. 13, para. 9). در تعیین اینکه آیا یک حملهٔ سایبری حملهٔ مسلحانه به‌حساب می‌آید یا نه، متخصصان پیش‌بینی‌پذیربودن تأثیرات را پیشنهاد داده‌اند. برای مثال، اگر حملهٔ سایبری یک ایستگاه تصفیهٔ آب را هدف قرار دهد، آلودگی آب و بیماری نتیجهٔ قابل پیش‌بینی است (Tallin Manual, 2013, rule. 13, para. 10). اکثریت متخصصان راهنمای تالین هم‌نظر بودند که قصد اولیهٔ حمله تعیین نمی‌کند که آیا یک عملیات مسلحانه است یا نه. برای مثال عملیات جاسوسی، که منتج به خسارات شدید شود، ممکن است به دفاع مشروع منجر شود. همچنین متخصصان راهنمای تالین عقیده داشتند که یک دولت ثالث هنگامی حق دفاع مشروع دارد که تحت‌تأثیر حملاتی قرار گیرد که بین دو دولت متخاصم ردوبدل می‌شود (Tallin Manual, 2013, rule. 13, para. 12).

هنگامی که یک عملیات حملهٔ مسلحانه ارزیابی می‌شود، مسئلهٔ دفاع مشروع مطرح می‌شود. هرگونه دفاع مشروع باید ضروری و متناسب باشد (Tallin Manual, 2013, rule. 13, para. 14) و حق دفاع مشروع زمانی ایجاد می‌شود که حمله آنی باشد (Tallin Manual, 2013, rule. 13, para. 15). به‌علاوه، نیازی نیست نوع و روش دفاع مشروعی که انجام می‌گیرد یکسان باشند. دولت‌ها ممکن است در مقابل حملات با سلاح‌های نظامی، با حملات سایبری پاسخ دهند و بالعکس، در مقابل حملات سایبری متوسل به سلاح‌های نظامی شوند تاجایی‌که اصول حاکم بر دفاع مشروع رعایت شود (Tallin Manual, 2013, rule. 14, para. 5).

مسئلهٔ مشروعیت حملات سایبری بیشتر در پرتو بند ۴ مادهٔ ۲ منشور سازمان ملل متحد ارزیابی می‌شود و درنتیجه، حملات سایبری که به ایجاد آثار فیزیکی منجر شده‌اند با نقض بند ۴ مادهٔ ۲ منشور، توسل به‌زور غیرقانونی محسوب شده و درصورتی‌که به آستانهٔ لازم برای یک حملهٔ مسلحانه رسیده باشند، در مقابل برای دولت قربانی حق دفاع مشروع از خود، طبق مادهٔ ۵۱ منشور ایجاد می‌شود (Baradaran et al, 2017, p. 262). در طول تاریخ، کاربرد زور با استفاده از سلاح‌های سنتی، که به حد حملهٔ مسلحانه رسیده است، به‌وسیلهٔ سلاح‌های سنتی پاسخ داده شده است. با توسعهٔ سریع فنّاوری نظامی، این مطابق با موقعیت فعلی نیست. سؤالی که در اینجا مطرح می‌شود این است که اگر یک حمله با استفاده از فنّاوری‌های جدید اتفاق بیفتد، آیا دولتی می‌تواند با استفاده از سلاح‌های سنتی اقدام به دفاع مشروع کند؟ برعکس، اگر حمله‌ای با استفاده از سلاح‌های سنتی صورت گیرد، آیا دفاع مشروع می‌تواند از فناوری‌های جدید استفاده کند؟ در تفسیر راهنمای تالین، گروه کارشناسان بین‌المللی به این سؤال پاسخ داده‌اند. آن‌ها معتقدند حق دفاع مشروع دولت‌ها، شامل حملات با سلاح‌های سنتی و غیرسنتی می‌شود و این‌که هیچ نیازی نیست که حملهٔ انجام‌شده و دفاع مشروع در برابر آن از یک نوع باشد (Tallin Manual, 2013, rule. 14, para. 5).

اگرچه سلاح‌های هسته‌ای در مقایسه با فنّاوری‌های سایبری در ماهیت مانند سلاح‌های سنتی هستند، نظر دیوان بین‌المللی دادگستری در نظریهٔ مشورتی ۱۹۹۶ دربارهٔ سلاح‌های هسته‌ای با فناوری سایبری مرتبط است؛ زیرا هم جنگ‌های هسته‌ای و هم سایبری، فنّاوری نظامی غیرسنتی را به کار می‌گیرند. در این رأی، دیوان بیان کرد که کاربرد سلاح‌های هسته‌ای در دفاع مشروع تحت هیچ شرایطی مستثنی نیست، اما آن می‌تواند از نظر حقوق بین‌الملل قانونی باشد اگر استفاده از آن متناسب باشد و همچنین ملزومات حقوق بین‌الملل بشردوستانه را رعایت کند (I.C.J Reports, 1996, para. 42). از حملات سایبری در پاسخ به یک حملهٔ مسلحانه می‌توان استفاده کرد وقتی که شرط تناسب رعایت شود و این دفاع مطابق حقوق بین‌الملل بشردوستانه انجام شود. همچنین دفاع مشروع می‌تواند هم شامل اقدامات دفاعی با استفاده از سلاح‌های سنتی و هم با استفاده از فنّاوری جدید، یعنی فناوری سایبری باشد، تاجایی‌که چنین دفاع مشروعی با حمله انجام‌شده تناسب داشته باشد.

به نظر می‌رسد که توافق کارشناسان در بحث دفاع مشروع روی مسئلهٔ تناسب باشد تا نوع کاربرد زوری که به‌وسیلهٔ ابزار سنتی یا فنّاوری جدید، یعنی فنّاوری سایبری انجام می‌گیرد. در بحث دفاع مشروع در برابر یک حملهٔ سایبری ممکن است با ابزار سنتی پاسخ داده شود و برعکس، در برابر یک حملهٔ مسلحانه با استفاده از سلاح‌های سنتی ممکن است نوع دفاع مشروع با استفاده از ابزار سایبری انجام گیرد.

۶. دفاع مشروع در قبال حملات سایبری عوامل غیر دولتی

ظهور بازیگران غیردولتی که دست به عملیات تروریستی مهیب می‌زنند و نیز دغدغه‌های حقوق بشری جامعهٔ بین‌المللی، بخشی از ساختار سنتی حقوق بین‌الملل، به‌ویژه قلمرو اصل عدم مداخله و اطلاق اصل ممنوعیت توسل به‌زور را رفته‌رفته متحول و شکل‌های تازه‌ای از حملهٔ مسلحانه و متقابلاً دفاع مشروع را مطرح کرده است (Mohebbi & Shafiei, 2017, p. 109).

در حقوق بین‌الملل توسل به‌زور منع شده است؛ مگر اینکه برای دفاع مشروع یا با مجوز شورای امنیت صورت گیرد. در بند ۴ مادهٔ ۲ منشور سازمان ملل متحد، عبارت «کلیهٔ اعضا» به‌کار رفته است؛ یعنی بند ۴ مادهٔ ۲ منشور سازمان ملل متحد روابط بین‌المللی را بین دولت‌های عضو دربر می‌گیرد و به چیز دیگری اشاره نکرده است. همچنین مادهٔ ۵۱ منشور سازمان ملل متحد فقط روی اتفاقات یک حملهٔ مسلحانه، بدون هیچ اشاره‌ای به منبع چنین حمله‌ای، تمرکز می‌کند. این اختلاف دو ماده می‌تواند به دو روش فهمیده شود: ازیک‌طرف، بند ۴ مادهٔ ۲ و مادهٔ ۵۱ به هم مرتبط هستند و یک حملهٔ مسلحانه یک استثنای ممنوعیت کاربرد زور است؛ بنابراین با یک دیدگاه مضیق، حق توسل به‌زور فقط هنگامی به کار می‌رود که حمله‌کننده یک دولت است؛ چون بند ۴ مادهٔ ۲ از نظر لغوی چنان بیان می‌کند.

همچنین در رأی مشورتی دیوان دربارهٔ دیوار حائل، دیوان بین‌المللی دادگستری رأی داد که: «مادهٔ ۵۱ منشور، بنابراین وجود یک حق ذاتی دفاع مشروع در هنگام حملهٔ مسلحانه به‌وسیلهٔ یک دولت علیه دولت دیگر را شناسایی می‌کند، اگرچه اسرائیل ادعا نمی‌کند که حملات علیه آن به یک دولت خارجی نسبت داده می‌شود» (I.C.J Reports, 2004, p. 139).

سپس یک سال بعد در قضیهٔ فعالیت‌های مسلحانه، دیوان نتیجه گرفت که حملات قضیه قابل‌انتساب به جمهوری دموکراتیک کنگو نیست و بنابراین، دیوان دریافت که شرایط حقوقی و واقعی برای اعمال حق دفاع مشروع توسط اوگاندا علیه جمهوری دموکراتیک کنگو وجود ندارد (I.C.J Reports, 2005, para.1.47).

این حقیقت که دیوان بین‌المللی دادگستری دربارهٔ دفاع مشروع بسیار با ابهام برخورد کرده و این موضوع بسیار جنجالی را شفاف نکرده است، حتی ازطریق قضات خودش بسیار مورد انتقاد قرار گرفته است. در یک نظر جداگانه، قاضی کویجمن[1] بیان کرد که عقیدهٔ او این است که حملات مسلحانه به‌طور مطمئن می‌تواند توسط عوامل غیردولتی انجام شود که منشور اجازهٔ دفاع مشروع در برابر چنین حمله‌ای را نمی‌دهد و بنابراین، نپذیرفتن حق دفاع مشروع دولت مورد حمله قرارگرفته غیرمنطقی است (I.C.J Reports, 2005, para. 30).

اندکی بعد از حملات تروریستی به‌وسیلهٔ القاعده در ایالات متحده در ۱۱ سپتامبر ۲۰۰۱، شورای امنیت قطعنامه‌های ۱۳۶۸[2] و ۱۳۷۳[3] را تصویب کرد که حق دفاع مشروع در برابر عوامل غیردولتی شناسایی تأیید شد (UNSC Resolution 1368, 2001). این قطعنامه‌ها جنجالی بودند و این اولین‌بار بود که دولت‌ها به‌طور رسمی حق دفاع مشروع را در ارتباط با حملات عوامل غیردولتی برقرار کردند. قبلاً مفهوم دفاع مشروع علیه عوامل غیردولتی برای بسیاری از دولت‌ها و مفسران پذیرفته نبود.

مسئله حملات سایبری، که به حد یک حمله مسلحانه می‌رسد و ازطریق عوامل غیردولتی انجام می‌شود، بدون امکان انتساب آن اقدامات به یک دولت در بین گروه کارشناسان بین‌المللی بحث شده است. همچنین با اشاره به قطعنامه‌های قبلی از طرف شورای امنیت و عملکرد دولت‌ها، اکثریت گروه کارشناسان بین‌المللی عقیده داشتند که حق دفاع مشروع علیه عوامل غیردولتی برقرار شده است (Tallin Manual, 2013, rule. 13, para.s. 16-17). براساس تفسیر کارشناسان بین‌المللی از آرای قضایی دیوان بین‌المللی دادگستری، به نظر نمی‌رسد دیوان آماده باشد تا همین دیدگاه را بپذیرد (Tallin Manual, 2013, rule. 13, para. 17). به‌علاوه گروه متخصصان بین‌المللی دربارهٔ اینکه آیا دفاع مشروع علیه عوامل غیردولتی در قلمرو یک دولت بدون اجازهٔ آن دولت قانونی است توافق نداشتند، اما گروه تأیید کرد که به هنگام توسل به دفاع مشروع علیه عوامل غیردولتی، باید به اصل حاکمیت سرزمینی آن دولت ملاحظه زیادی بشود. علی‌رغم این، گروه متخصصان بین‌المللی به هیچ‌گونه شفاف‌سازی یا تحلیل عمیق‌تر موضوع توسل به دفاع مشروع علیه عوامل غیردولتی نپرداختند.

موقعیت‌هایی که وقتی دفاع مشروع علیه دولتی که عوامل غیردولتی در قلمرو آن فعالیت می‌کنند صورت می‌گیرد و وقتی که دفاع مشروع علیه خود عوامل غیردولتی انجام می‌گیرد باید از همدیگر تمیز داده شوند. این نتیجه می تواند گرفته شود که کاربرد زور علیه دولت دیگر بدون انتساب حملات انجام‌شده به دولت براساس منشور سازمان ملل متحد منع شده است. در واقع، چنین کاربرد زوری حاکمیت آن دولت و تمامیت ارضی آن را نقض خواهد کرد، اما رضایت یک دولت به انجام عملیات در قلمرو آن دولت موجب قانونی‌بودن آن عملیات خواهد شد. سؤال دیگری که مطرح می‌شود این است که آیا دفاع مشروع علیه عوامل غیردولتی در خاک یک کشور دیگر، که به آن حمله رضایت نداده است، قانونی است؟ برای مثال، ایالات متحدهٔ آمریکا علیه دولت اسلامی عراق و شام هم در عراق و هم در سوریه اقدام به کاربرد زور کرده است. حملات هوایی آمریکا در عراق در آگوست ۲۰۱۴ بعد از اینکه دولت عراق از این کشور درخواست کرد شروع شد و بنابراین براساس منشور سازمان ملل

1. Judge Kooijmans

۲. قطعنامهٔ ۱۳۶۸ شورای امنیت سازمان ملل متحد که در تاریخ ۱۲ سپتامبر ۲۰۰۱ تصویب شد، سندی بین‌المللی دربارهٔ تهدید صلح و امنیت بین‌المللی ناشی از اقدامات تروریستی است. این قطعنامه طی نشست ۴۳۷۰ام با ۱۵ رأی موافق، ۰ مخالف و ۰ ممتنع تصویب شد.

۳. قطعنامهٔ ۱۳۷۳ شورای امنیت سازمان ملل متحد، که در تاریخ ۲۸ سپتامبر ۲۰۰۱ تصویب شد، نیز سندی بین‌المللی دربارهٔ تهدید صلح و امنیت بین‌المللی ناشی از اقدامات تروریستی است. این قطعنامه طی نشست ۴۳۸۵ام با ۱۵ رأی موافق، ۰ مخالف و ۰ ممتنع تصویب شد.

متحد به‌عنوان دفاع مشروع دسته‌جمعی مطابق مادهٔ ۵۱ مجاز است (Hakimi, 2015, p. 20). در مقایسه، دولت سوریه به ایالات متحدهٔ آمریکا دربارهٔ کاربرد زور در قلمروش علیه دولت اسلامی عراق و شام اجازه نداده است و با وجود مخالفت دولت سوریه، ایالات متحده در سپتامبر ۲۰۱۴ حملات خود علیه دولت اسلامی را در این کشور آغاز کرد (Hakimi, 2015, p. 21). در قطعنامهٔ ۲۱۷۰[1]، شورای امنیت از دولت‌ها خواست تا اقدامات مختلفی به‌منظور سرکوب دولت اسلامی اتخاذ کنند، اما کاربرد زور را تجویز نکرد (UNSC resolution 2170, 2014). دولت اسلامی نه‌تنها به کاربرد زور با استفاده از سلاح‌ها و تجهیزات جنگی متوسل شد، بلکه همچنین هکرها را استخدام کرد. در ابتدای سال ۲۰۱۵ یک گروه، که خودش را خلافت سایبری نامید، حساب‌های توییتر و یوتیوب فرماندهی نظامی مرکزی ایالات متحدهٔ آمریکا را هک کرد و اظهارات تهدیدآمیزی منتشر کرد. با مشاهدهٔ اعمال وحشیانه‌ای که دولت اسلامی در عراق و سوریه انجام داده است، تهدید عوامل غیردولتی که ممکن است در فضای سایبری ایجاد شود نباید دست‌کم گرفته شود.

نظر دیگری که در این مورد وجود دارد این است که دولت‌ها باید اطمینان حاصل کنند که قلمرو آن‌ها برای صدمه‌زدن علیه دولت دیگری استفاده نشود (I.C.J. Reports, 1949, p. 22). اگر یک گروه غیردولتی از سرزمین دولتی حملاتی را علیه دولت دیگر انجام دهد، حق دولت زیان‌دیده برای توسل به دفاع مشروع وجود دارد. دولت زیان‌دیده باید از دولت دیگر بخواهد تا از سرزمین خود مراقبت کند. اگر دولت مربوطه تمایل نداشته باشد یا قادر نباشد از حملات بیشتر جلوگیری کند، دولت قربانی ممکن است علیه گروه غیردولتی اقدام به دفاع مشروع کند، اما باید در نقض حاکمیت سرزمینی، حدود و ماهیت عملیات خود را به مواردی محدود کند که به‌طورجدی برای دفاع در برابر آن گروه ضروری است.

امروزه عوامل غیردولتی عملیاتی انجام می‌دهند که به حد حملهٔ مسلحانه‌ای می‌رسند که قبلاً توسط دولت‌ها انجام می‌شد و درواقع غیرمنطقی به نظر می‌رسد که دفاع مشروع نباید یک روش قانونی پاسخ‌دادن به چنین رفتاری باشد و به نظر می‌رسد که منشور سازمان ملل نیز این را منع نمی‌کند. اگر دولتی بخواهد علیه عوامل غیردولتی، که از داخل کشور دیگری حملاتی را علیه آن دولت انجام داده‌اند اقدام به دفاع مشروع کند، باید ملاحظه شود تا پاسخ به حملات علیه عوامل غیردولتی باشد و نه دولتی که عوامل غیردولتی از خاک آن برای هدایت حملات خود استفاده کرده‌اند. هنگامی که کاربرد زور در دفاع مشروع علیه عوامل غیردولتی انجام می‌گیرد، اصول حاکمیت دولت و تمامیت ارضی اهمیت بسزایی دارد؛ اگرچه در بحث دفاع مشروع در برابر حملات سایبری باید بیان کرد که به‌طور طبیعی بین بمباران در قلمرو یک دولت دیگر و نابودی سیستم‌های رایانه‌ای تفاوت وجود دارد، این آشکار است که در حوزهٔ سایبر یک مزیت است؛ زیرا دولت‌های خارجی به این‌گونه عملیات علیه عوامل غیردولتی در سرزمینشان بهتر رضایت می‌دهند و دامنهٔ این نوع از عملیات با سلاح‌های کلاسیک نظامی کمتر است و متفاوت از سبک سنتی دفاع مشروع علیه عوامل غیردولتی است.

نتیجه‌گیری

پیچیدگی و تنوع حملات سایبری قراردادن آن‌ها را در چهارچوب حقوقی فعلی مشکل می‌کند. حملات سایبری نتایج مخربی مانند کشتن و زخمی‌کردن افراد، تخریب دارایی و اموال دارند. هم دولت‌ها و هم عوامل غیردولتی می‌توانند حملات سایبری را انجام دهند و هر چیز و هر کسی را ازجمله افراد، اشیا و حتی کل جوامع هدف قرار دهند. در حال حاضر، بهترین تعریف از حملهٔ سایبری، که مرتبط با موضوع بحث این مقاله، یعنی دفاع مشروع در قبال حملات سایبری عوامل غیردولتی باشد، در مادهٔ ۳۰ راهنمای تالین نهفته است. این تعریف همهٔ عملیات‌های سایبری را دربر می‌گیرد که باعث ایجاد جراحت و مرگ برای اشخاص و خسارت و تخریب به اشیا می‌شود.

تعهد بین‌المللی مرتبط که توسط یک حملهٔ سایبری نقض می‌شود و به حد حملهٔ مسلحانه می‌رسد، ممنوعیت کاربرد زور است؛ بنابراین نقض منشور سازمان ملل متحد به حساب می‌آید. در بحث دفاع مشروع علیه عوامل غیردولتی، دو دیدگاه مضیق و موسع وجود دارد و حتی

۱. قطعنامه ۲۱۷۰ از گروه‌های داعش و جبهة النصره، افراد و دیگر نهادها و گروه‌های وابسته به القاعده می‌خواست به فوریت سلاح‌های خود را زمین گذارند.

دیوان بین‌المللی دادگستری نیز با این قضیه با ابهام برخورد کرده است و رویهٔ دیوان تنها بر شناسایی دفاع مشروع علیه دولت‌ها بوده است، اما اولین‌بار پس از حملات تروریستی القاعده در ایالات متحده در ۱۱ سپتامبر ۲۰۰۱ و تصویب قطعنامه‌های ۱۳۷۳ و ۱۳۶۸، حق دفاع مشروع علیه عوامل غیردولتی برقرار شد و گروه کارشناسان بین‌المللی راهنمای تالین نیز حق دفاع مشروع علیه عوامل غیردولتی را پذیرفته‌اند؛ بنابراین می‌توان نتیجه گرفت که در حال حاضر، با توجه به مواردی که مطرح شد، امکان توسل به دفاع مشروع در قبال حملات سایبری عوامل غیردولتی وجود دارد، اگر دفاع مشروع براساس قواعد حقوق بین‌الملل صورت گیرد و اصول دفاع مشروع مانند تناسب، ضرورت و فوریت رعایت شود.

منابع

بختیاری، ایرج (۱۳۹۳). تبیین نقش جنگ سایبری در جنگ‌های آینده .علوم و فنون نظامی، ۱۰(۲۸)، ۴۷-۷۴. لینک

برادران، نازنین، حبیبی، همایون، زمانی، سید قاسم و هنجی، سیدعلی (۱۳۹۶). کاربرد اصل عدم مداخله در امور داخلی دولت‌ها در حملات سایبری. پژوهش‌های سیاسی و بین‌المللی، ۸(۳۳)، ۲۴۱-۲۶۷. لینک

جلالی، محمود و پورسعید، فرزانه (۱۳۹۹). ظهور عوامل غیردولتی تروریستی: تعهدات بین‌المللی و چالش نظارت بر سلاح‌های کشتار جمعی. مطالعات حقوقی شیراز، ۱۲(۱)۳۵-۷۴. https://doi.org/10.22099/JLS.2020.33069.3372

رضایی، مسعود ، وجلالی ، محمود (۱۳۹۷). جنگ سایبری و توسعه حقوق بین‌الملل منع توسل به زور. فصلنامه مطالعات حقوق عمومی، ۴۸(۳)، ۶۹۷-۷۱۳. https://doi.org/10.22059/jplsq.2018.217523.1365

فرشاسعید، پرویز، و جلالی، محمود (۱۴۰۱). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی در حقوق بین‌الملل. فصلنامه حقوق فناوری‌های نوین، ۳(۶)، ۱۷۳-۱۸۴. https://doi.org/10.22133/mtlj.2023.367059.1136

محبی، محسن و شفیعی، ایمان (۱۳۹۶). تحول مفهوم دفاع مشروع: حقوق بین‌الملل و بازیگران غیردولتی. فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی، (۸۱)، ۸۹-۱۱۳. https://doi.org/10.22034/JLR.2018.120863.1134

محمدعلی‌پور، فریده (۱۳۹۶). حملات سایبری و چالش‌های جدید اصل منع استفاده از زور در روابط بین‌الملل. سیاست جهانی، ۶(۳)، ۲۳۳-۲۵۷. https://doi.org/10.22124/WP.2017.2696

نامدار، سعید و قاسمی، غلامعلی (۱۳۹۷). بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران. مطالعات حقوقی دانشگاه شیراز، ۱۰(۱)، ۱۹۹-۲۳۵. https://doi.org/10.22099/JLS.2018.23191.2178

Hakimi, M. (2015). Defensive force against non-state actors: The state of play. *International Law Studies*, *1*, 1-31. Link

International Court of Justice (I.C.J Reports). (2004). Legal consequences of the construction of a wall in the occupied Palestinian territory. Advisory Opinion of 9 July 2004. Link

International Court of Justice. (1949). The Corfu Channel Case (United Kingdom v. Albania) (Merits). Judgment of 9 April 1949. I.C.J. Reports 1949. Link

International Court of Justice. (1986). Military and para.military activities in and against Nicaragua (Nicaragua v. United States of America) (Merits). Judgment of 27 June 1986, para. 202. I.C.J. Reports 1986. Link

International Court of Justice. (1996). Legality of the threat or use of nuclear weapons. Advisory Opinion of 8 July 1996, para. 42. Link

International Court of Justice. (2003). Oil platforms (Islamic Republic of Iran v. United States of America). Judgment of 6 November 2003. Link

International Court of Justice. (2007). Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). Judgment of 26 February 2007. Link

Jolley, J. D. (2012). Article 2 (4) and cyber warfare: How do old Rule.s control the brave new world? *Available at SSRN 2128301*. http://dx.doi.org/10.2139/ssrn.2128301

Lieblich, E. (2019). Self-Defence against Non-State Actors and the Myth of the Innocent State. *Global Rights*. Link

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

United Nations Security Council (UNSC Resolution). (2001). *Resolution 1368*. UN Doc. S/RES/1368. Link

United Nations Security Council (UNSC Resolution). (2014). *Resolution 2170*. UN Doc. S/RES/2170. Link

UNSC Resolution 1368, UN Doc S/RES/1368 12 September 2001. Link

Urbina Escobar, T. (2023). Estratégias de autodefesa contra ciberataques de atores não-estatais. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, *18*(2), 61-72. https://doi.org/10.18359/ries.6639

[In persian]

Bakhtiari, I. (2014). Explaining the Role of Cyber Warfare in Future Wars. *Military Science and Technology*, *10*(28), 47-74. Link

Baradaran, N., Habibi, H., Zamani, S., & Henji, S. (2017). Application of the principle of non-interference in the internal affairs of states in cyberattacks. *Public Law Studies Quarterly*, *8*(33), 241-267. Link

Farshasaid, P., & Jalali, M. (2022). International responsibility of states for cyberattacks of non-state actors. *Contemporary Legal Studies Journal*, *3*(6), 148-173. https://doi.org/10.22133/mtlj.2023.367059.1136

Jalali, M., & Poorsaied, F. (2020). Emergence of terrorist non-state actors: International obligations and the challenge of supervision over the weapons of mass destruction. *Public Law Studies Quarterly*, *10*(1), 35-74. https://doi.org/10.22099/JLS.2020.33069.3372

Mohammad Ali Poor, F. (2018). Cyberattacks and new challenges to the principle of prohibition of the use of force in international relations. *Legal Studies Quarterly*, *6*(3), 233-257. https://doi.org/10.22124/WP.2017.2696

Mohebbi, M., & Shafiee, I. (2018). The evolution of the concept of self-defense: International law and non-state actors. *Defense Policy Quarterly*, *21*(81), 89-113. https://doi.org/10.22034/JLR.2018.120863

Namdar, S., & Gasemi, G. (2018). Analyzing the concept of self-defense in light of cyberattack (With an emphasis on Stuxnet attack on Iran's nuclear facilities). *Public Law Studies Quarterly*, *10*(1), 199-235. https://doi.org/10.22099/JLS.2018.23191.2178

Rezaei, M., & Jalali, M. (2018). Cyber war and development of international law of non-use of force in cyberspace. *Journal of Legal Justice*, *48*(3), 697-713. https://doi.org/10.22059/jplsq.2018.217523.1365