Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/mtlj.2023.388893.1182

From the Blue of Sea to the Dark Web: Cyber Operations in Some Maritime Zones and International Straits in the Light of Tallinn Manual 2.0

Shahram Zarneshan[1], Reyhaneh Zandi[2*], Mousa Karami[3]

[1] Associate Professor, Department of Public and International Law, Faculty of Law and Political Science, Allameh Tabataba'i University, Tehran, Iran.

[2] Ph. D. Candidate in Public International Law, Faculty of Law, University of Qom and University Lecturer, Qom, Iran

[3.] Ph. D. Candidate in Public International Law, Faculty of Law, University of Qom and University Lecturer, Qom, Iran

Article Info

Original Article

Received:
7-3-2023
Accepted:
1-07-2023

Keywords:
Cyber Operations
Archipelagic Waters
Contiguous Zone
Exclusive Economic Zone
International Strait
Tallinn Manual 2.0

Abstract

The increasing connection of states' main functions to the interconnected nature of cyberspace exposes them to a new spectrum of threats. The international community is aware of the increase in cyber threats and is trying to develop the existing international law to regulate cyber operations. Employing a descriptive-analytic method and using library and internet sources, the present article aims at examining the conditions and requirements of cyber operations in three maritime zones, namely the archipelago waters, the contiguous zone and the exclusive economic zone and also international straits in the light of Tallinn Manual 0.2. It seems that Tallinn Manual 0.2 can be useful both in explaining the rules of international law related to cyber operations, especially in the field of cyber operations in different maritime areas, and in reducing the existing normative gap in this field. However, it is undeniable that there are still many areas of disagreement and lack of clarity, even among the experts who prepared the Tallinn Manual. It appears that the international legal framework governing piracy, even despite its shortcomings, can provide a basis for creating a similar regime to ensure international cyber security. Since countries' economic and political future is increasingly intertwined, achieving international consensus on issues such as the legal regime governing harmful cyber-attacks and operations is essential for global security and economic prosperity.

***Corresponding author**
e-mail: r.z.judge94@gmail.com

How to Cite:
Zarneshan, S., Zandi, R., & Karami, M. (2023). From the Blue of Sea to the Dark, WebCyber Operations in Some Maritime Zones and International Straits in the Light of Tallinn Manual 2.0. *Modern Technologies Law*, *4*(8), 149-168.

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

حقوق فناوری‌های نوین، ۱۴۰۲، ٤(۸) https://www.mtlj.usc.ac.ir

حقوق فناوری‌های نوین

http://doi.org/10.22133/mtlj.2023.388893.1182

از آبی دریا تا شبکهٔ سیاه: عملیات‌های سایبری در برخی مناطق دریایی و تنگه‌های بین‌المللی در پرتو دستورالعمل تالین

شهرام زرنشان[۱]، ریحانه زندی[۲*]، موسی کرمی[۳]

[۱] دانشیار گروه حقوق عمومی و بین‌الملل، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران

[۲] دانشجوی دکتری حقوق بین‌الملل عمومی، دانشکدهٔ حقوق دانشگاه قم و مدرس دانشگاه، قم، ایران

[۳] دانشجوی دکتری حقوق بین‌الملل عمومی، دانشکدهٔ حقوق و مدرس دانشگاه، دانشگاه قم، قم، ایران

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۲/۱۶

تاریخ پذیرش:
۱۴۰۲/۰۴/۱۲

واژگان کلیدی:
عملیات سایبری
آب‌های مجمع‌الجزایری
منطقهٔ مجاور
منطقهٔ انحصاراً اقتصادی
تنگهٔ بین‌المللی
دستورالعمل تالین ۲

چکیده

پیوند فزایندهٔ کارکردهای اصلی دولت‌ها با سرشت به‌هم‌پیوستهٔ فضای سایبر، کشورها را در معرض طیفی نوین از تهدیدها قرار می‌دهد. جامعهٔ بین‌المللی از افزایش تهدیدهای سایبری آگاه است و می‌کوشد حقوق بین‌الملل موجود را برای تنظیم عملیات‌های سایبری گسترش دهد. هدف از مقالهٔ حاضر این است که با استفاده از روش توصیفی ـ تحلیلی و بهره‌گیری از منابع کتابخانه‌ای و اینترنتی، شرایط و الزامات عملیات‌های سایبری را در سه منطقهٔ دریایی آب‌های مجمع‌الجزایری، منطقهٔ مجاور و منطقهٔ انحصاراً اقتصادی و نیز تنگه‌های بین‌المللی در پرتو دستورالعمل تالین ۲ دربارهٔ حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری بررسی کند. به‌نظر می‌رسد دستورالعمل تالین ۲ در تبیین قواعد حقوق بین‌الملل مربوط به عملیات سایبری، به‌ویژه در زمینهٔ عملیات‌های سایبری در مناطق مختلف دریایی سودمند است و در کاهش خلأ هنجاری موجود در این حوزه به‌کار آید. بااین‌حال، نمی‌توان انکار کرد که در میان کارشناسانی که دستورالعمل¬ را نوشته¬اند، همچنان زمینه‌های اختلاف نظر و ابهام وجود دارد. چنین می‌نماید که چارچوب حقوقی بین‌المللی حاکم بر دزدی دریایی و به‌ویژه اصل صلاحیت جهانی در پیگرد و مجازات مرتکبان، به‌رغم کاستی‌های آن، مبنای ایجاد رژیمی مشابه را به‌منظور تأمین امنیت سایبری بین‌المللی فراهم می‌آورد. ازآنجاکه آیندهٔ اقتصادی و سیاسی کشورها هرچه بیشتر درهم‌تنیده می‌شود، دستیابی به اجماع بین‌المللی دربارهٔ موضوعاتی مانند نظام حقوقی حاکم بر حملات و عملیات‌های سایبری آسیب‌زا، برای امنیت جهانی و رفاه اقتصادی ضروری است.

***نویسندهٔ مسئول**

رایانامه: r.z.judge94@gmail.com

نحوهٔ استناددهی:

زرنشان، شهرام، زندی، ریحانه، و کرمی، موسی (۱۴۰۲). از آبی دریا تا شبکهٔ سیاه، عملیات‌های سایبری در برخی مناطق دریایی و تنگه‌های بین‌المللی در پرتو دستورالعمل تالین. حقوق فناوری‌های نوین، ۴(۸)، ۱۴۹-۱۶۸.

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

شاپای الکترونیکی: ۳۸۳٦-۲۷۸۳

مقدمه

عملیات‌های سایبری، که به‌منزلهٔ «به‌کارگیری قابلیت‌های سایبری برای دستیابی به اهداف در/ ازطریق فضای سایبر» (Tallinn Manual 2.0, 2017, p. 564) تعریف شده‌اند، از جمله موضوعات و مسائل نوینِ عرصهٔ روابط و حقوق بین‌الملل هستند و موازین حاکم بر آن‌ها، به‌نسبت حوزه‌های سنتی این شاخه از حقوق، روشنی و گستردگی کمتری دارند. در واقع، «ویژگی‌های منحصربه‌فرد فضای سایبر، مسائل حقوقی خاصی را پدید آورده‌اند که پیش‌تر به آنان پرداخته نشده است» (Ziolkowski, 2013, p. 621). اگر به گفتهٔ اندیشمندان، «در روابط بین‌المللی مناطقی وجود دارد که حقوق به آن‌ها نفوذ نکرده است» و می‌توان آن‌ها را حفره‌های سیاه جامعهٔ جهانی دانست (شمیلیه-ژانرو، ١٣٨٢، ص ۴)، بی‌گمان فعالیت‌های مربوط به فضای سایبر و عملیات‌های سایبری یکی از حوزه‌هایی است که اگرچه به‌سبب پیوند آن‌ها با جوامع داخلی و بین‌المللی، حقوق و به‌ویژه حقوق بین‌الملل ناگزیر در آن‌ها رسوخ کرده است، اما حفره‌های موجود در این عرصه، خودنمایی برجسته‌ای دارند. بر این پایه، تلاش دولت‌ها و سازمان‌های بین‌المللی در راستای تبیین و توسعهٔ مبانی و منابع حقوقی در این زمینه از بایسته‌های انکارناشدنی به‌شمار می‌رود. در واقع، حقوق بین‌الملل برای فرزندِ زمانهٔ خویش بودن نیازمند پرکردن نبودها و کمبودهای خود ازجمله در حوزهٔ عملیات‌های سایبری است.

درنتیجه یکی از تلاش‌های انجام‌شده برای جبران و کاهش این نبودها و کمبودها بود که به دعوت مرکز عالی پدافند مشترک سایبری ناتو[1] در شهر تالین[2] کشور استونی، دستورالعمل تالین ٢ دربارهٔ حقوق بین‌الملل قابل اعمال بر عملیات سایبری[3] (زین‌پس دستورالعمل) به‌دست گروهی از کارشناسان بین‌المللی تدوین و در سال ٢٠١٧ منتشر شد که هم‌اکنون «فراگیرترین راهنمایِ چگونگیِ اعمال حقوق بین‌الملل بر عملیات‌های سایبری» (Ertan et al., 2020, p. v) خوانده می‌شود. دستورالعمل، که مطالب جدیدی را به دستورالعمل تالین دربارهٔ حقوق بین‌الملل قابل اِعمال بر نبردهای سایبری[4] ٢٠١٣ افزوده و اندکی نیز دستورالعمل پیشین را اصلاح کرده است (Schmitt, 2017, p. 42)، به بیان قواعد قابل اعمال بر عملیات‌های سایبری در شاخه‌های گوناگون حقوق بین‌الملل عمومی پرداخته و ازجمله در فصل هشتم از بخش دوم، از بخش‌های چهارگانه خود، به بحث پیوند عملیات‌های سایبری با حقوق بین‌الملل دریاها و مناطق گوناگون دریایی ورود داشته است (Tallinn Manual 2.0, 2017, pp. 232-258)، امری که حکایت از رسوخ روزافزون فضای سایبر در لایه‌های گوناگون حقوق بین‌الملل دارد. بی‌سبب نیست که کشورها عملیات‌های سایبری را «بخش جدایی‌ناپذیر روابط بین‌الملل» شمرده و از خطر عملیات‌های سایبری فرامرزیِ آسیب‌زا برای صلح و ثبات بین‌المللی سخن گفته‌اند (The Federal Government of Germany, March 2021, p. 1). دراین‌میان، بخشی از مشکل اعمال قوانین بین‌المللی در فضای سایبر ناشی از فقدان قوانین یا استانداردهای خاص است؛ برای مثال وقتی صحبت از صلح و امنیت بین‌المللی می‌شود، هیچ معاهدهٔ سایبری خاصی وجود ندارد و کنوانسیون‌های اندکی که از بعدی محدود به جرایم سایبری می‌پردازند، مانند کنوانسیون بوداپست و (اگر زمانی لازم‌الاجرا شود) کنوانسیون اتحادیهٔ آفریقا، طبق تعریف مطرح‌شده در نخستین بندهای مفاد خود، فقط رفتار بازیگران غیردولتی با حمایت برخی از دولت ـ ملت‌ها را هدف قرار می‌دهند؛ بنابراین قوانین بین‌المللی برای دستیابی به امتیاز کاربرد در فضای سایبری به برقراری ارتباط با معاهدات چندجانبهٔ کلی‌تر (مانند بسیاری از اسناد حقوق بشری) یا حقوق بین‌الملل عرفی نیازمندند.

قلمرو دریاها، که پیش‌تر به دلیل فقدان اتصال به اینترنت و ماهیت منزوی کشتی‌ها در دریا امن تلقی می‌شد، با ورود به عصر دیجیتال شاهد افزایش خیره‌کنندهٔ نقض امنیت سایبری در فنّاوری عملیاتی است. همین امر، موجب شده است مسائل دریاها با فضای سایبر پیوند یابند و آبیِ زلالِ دریاها با شبکهٔ سیاه و ناپیدا درهم آمیزند. اگرچه برخی تحقیقات در این زمینه درحال انجام است، اما چشم‌انداز امنیت سایبری دریایی عمیقاً بررسی نشده است. به علت جایگاه برجستهٔ این دستورالعمل در سپهر حقوق بین‌الملل سایبری و نقش آن در قاعده‌گذاری بین‌المللی در فضای سایبر از یک‌سو و بایستگی انجام پژوهش‌های تخصصی دربارهٔ مسائل نوپدید در حقوق بین‌الملل کنونی از سوی دیگر، در

[1]. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)
[2]. Tallinn
[3]. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)
[4]. Tallinn Manual on the International Law Applicable to Cyber Warfare

این نوشتار برآن شده‌ایم که در پرتو قواعد و شرح دستورالعمل، شرایط و الزامات عملیات‌های سایبری در سه منطقهٔ آب‌های مجمع‌الجزایری، منطقهٔ مجاور یا نظارت، منطقهٔ انحصاراً اقتصادی و نیز تنگه‌های بین‌المللی را بررسی کنیم. در دستورالعمل، افزون بر سه منطقهٔ دریایی و آبراه بین‌المللی یادشده، به عملیات‌های سایبری در دریای سرزمینی و دریای آزاد نیز پرداخته شده است، اما به دلیل محدودیت‌های واژگانی نشریات و بایستگی ادای هرچند نسبی و حداقلی مطلب، نگارندگان در پژوهشی دیگر به آن دو پرداخته‌اند. به این منظور، در چهار گفتار جداگانه، نخست به‌اختصار موازین حقوقی بین‌المللی حاکم بر آب‌های مجمع‌الجزایری، منطقهٔ نظارت، منطقهٔ انحصاراً اقتصادی و تنگه‌های بین‌المللی را از نظر می‌گذرانیم، سپس شرایط و الزامات عملیات‌های سایبری در آن‌ها را در پرتو دستورالعمل بررسی می‌کنیم.

۱. عملیات‌های سایبری در آب‌های مجمع‌الجزایری

آب‌های مجمع‌الجزایری[1] بارزترین نماد گسترش حاکمیت دولت در دریاها و اقیانوس‌ها در کنوانسیون ۱۹۸۲ حقوق دریاهاست. در این بخش، به موازین حقوقی حاکم بر این آب‌ها و فعالیت‌های سایبری در آن‌ها خواهیم پرداخت.

۱-۱. نگاهی به موازین حقوقی حاکم بر آب‌های مجمع‌الجزایری

کنوانسیون ۱۹۸۲ و موافقت‌نامه‌های اجرایی آن و موافقت‌نامه ۱۹۹۵ ملل متحد دربارهٔ ذخایر ماهی، رژیم حقوقی جامعی را درخصوص کلیهٔ فعالیت‌های دریایی تشکیل داده‌اند. در این میان، رژیم حقوقی ناظر بر آب‌های مجمع‌الجزایری در بخش چهارم کنوانسیون ۱۹۸۲ با هدف حل مسئله‌ای پیش‌بینی شد که مدت‌ها جامعهٔ بین‌المللی را به چالش کشیده بود: آیا مجموعه‌ای از جزایر را می‌توان موجودیتی واحد در نظر گرفت و مشمول رژیمی خاص و متمایز از قوانین قابل اعمال برای توده‌های خشکی قاره‌ای و جزایر منفرد به‌شمار آورد؟ (Rothwell et al., 2015, p. 153). وضعیت کشورهای مجمع‌الجزایری از دههٔ ۱۹۲۰ مطرح شد و در آن زمان، مباحث گسترده‌ای در محافل علمی گوناگون دربارهٔ مطالعهٔ حقوق بین‌الملل درخصوص آب‌های داخلی جزیره‌ها درگرفت. همین مباحثات تاحدودی به تبیین وضعیت حقوقی کشورهای مجمع‌الجزایری کمک کرد (Gamil Aboukhewat, 2019, p. 190). کشورهای مجمع‌الجزایری، که تلاش می‌کردند کنترل خود را بر آب‌های اطراف جزایرشان گسترش دهند، همواره خواستار ایجاد سیستمی قانونی برای مجمع‌الجزایر به‌منظور حفظ منافع، ثروت دریایی و امنیت منطقه‌ای خود بوده‌اند (Gamil Aboukhewat, 2019, p. 189). همچنین کشورهای بزرگ دریایی‌ای وجود داشته‌اند که همواره خواستار حفظ آزادی دریا و ناوبری بین‌المللی بوده‌اند. اگرچه در طول زمان، مشکلات ناشی از جزایر تشکیل‌دهندهٔ مجمع‌الجزایر طی مناقشات مربوط به حاکمیت و حق بر مناطق دریایی در میان چنین دولت‌هایی عمدتاً به پایان رسید، اما بسیاری از مشکلات دیگر با وجود جزایر مجمع‌الجزایر همراه بود. اندازه‌گیری نواحی دریایی جزایر، مستلزم شرح چگونگی ترسیم خطوط پایه است که این مناطق از آن‌ها اندازه‌گیری شوند. ترسیم خطوط پایه نیز بسته به شکل کلی جزایر و این‌که آیا در مقابل نواحی ساحلی یا در ورودی خلیج‌ها در این سواحل قرار دارند یا در دریا یا اقیانوس جای گرفته‌اند، متفاوت است. باقی‌ماندن تنش‌هایی بر این پایه، تا زمانی که یک سیستم منحصربه‌فرد حقوقی تحت بخش چهارم کنوانسیون ۱۹۸۲ به تصویب رسید، نشان‌دهندهٔ توسعهٔ بخش بسیار مهمی از حقوق بین‌الملل دریاها بود.

مطابق با مادهٔ ۴۷(۱) کنوانسیون ۱۹۸۲، کشور مجمع‌الجزایری[2] کشوری است که از مجموعه یا مجموعه‌هایی از جزایر تشکیل شده است. کشورهایی مانند فیلیپین یا اندونزی از مهم‌ترین کشورهای مجمع‌الجزایری به‌شمار می‌روند. همچنین وفق بند یکم مادهٔ ۴۹، دولت مجمع‌الجزایری می‌تواند، در چارچوب محدودیت‌هایی معین، خطوط مستقیم مجمع‌الجزایری را ترسیم کند که دورترین نقاط دورترین جزایرِ مجمع‌الجزایر را به‌هم متصل می‌کنند. آب‌های میان خطوط مبدأ مجمع‌الجزایری، آب‌های مجمع‌الجزایری هستند. دریای سرزمینی[3] و منطقهٔ

---

[1]. Archipelagic Waters
[2]. Archipelagic Country
[3]. Territorial Sea

انحصاراً اقتصادی[1] از خطوط مبدأ مجمع‌الجزایری به سمت دریا اندازه‌گیری می‌شوند. یک کشور درخصوص آب‌های مجمع‌الجزایری، فضای هوایی فوقانیِ آن آب‌ها و بستر و زیربستر آن‌ها از حاکمیت برخوردار است که از نقطه‌نظر معادلات سرزمینی، در به‌رسمیت‌شناسی قلمروی دولت‌های مجمع‌الجزایری نقطهٔ عطفی به‌شمار می‌رود.

براساس مادهٔ ۵۳(۱) کنوانسیون مونته‌گوبی،[2] کشورهای مجمع‌الجزایری می‌توانند آبراه‌هایِ دریایی و مسیرهای هوایی مجمع‌الجزایریِ مناسب برای دریانوردیِ بین‌المللی پیوسته و سریع شناورها و هواپیماهای خارجی از فراز آب‌های مجمع‌الجزایری یا بر فراز آن‌ها را مشخص سازند. طبق بند دوازدهم همین ماده، اگر کشور مجمع‌الجزایری چنین مسیرهایی را مشخص نکند، شناورها و هواپیماهای خارجی می‌توانند حق عبور از آبراه‌های دریاییِ مجمع‌الجزایری را در طول مسیرهایی که به‌صورت عادی برای دریانوردی و پرواز بین‌المللی استفاده می‌شوند اِعمال کنند. طبق مادهٔ ۵۲ کنوانسیون، در آب‌های خارج از این قبیل مسیرهایِ دریاییِ مجمع‌الجزایری، یا جایی که مسیرهای دریایی مجمع‌الجزایری مشخص نشده‌اند، خط سیرهایی که معمولاً برای دریانوردی بین‌المللی به‌کار می‌روند حق عبور بی‌ضرر اعمال می‌شود. درعین‌حال، کشورهایی که مستقیماً در همسایگی دولت مجمع‌الجزایری قرار دارند قادرند ماهیگیری سنتی و سایر فعالیت‌های غیرکشتیرانی را در آب‌های مجمع‌الجزایری انجام دهند (Churchill et al., 2022, p. 187). پرواضح است که هرگونه تعرض به کشتی‌ها و خدمهٔ آن‌ها درحال عبور بی‌ضرر از آب‌های فوق، بدون دلیل موجه، مسئولیت بین‌المللی دولت مجمع‌الجزایری را درپی خواهد داشت. این نکته‌ای است که بارها نظر محاکم بین‌المللی را به خود جلب کرده و بر آن صحه گذاشته شده است؛ ازجمله دیوان بین‌المللی حقوق دریاها[3] در احکام مبتنی‌بر آزادی فوری خود در قضایای خلیج کنفورکو[4] و خلیج کامکو[5] تفسیر گسترده‌ای از مفهوم «توقیف» و آزادسازی فرمانده و خدمهٔ کشتی ارائه کرده است.

۱-۲. عملیات‌های سایبری در آب‌های مجمع‌الجزایری در دستورالعمل تالین ۲

حقوق دریاها رژیمی است تخصصی با سابقهٔ طولانی و تدوین درخور توجه در دهه‌های اخیر. کارشناسان تهیه‌کنندهٔ دستورالعمل بر این نکته اتفاق‌نظر داشتند که بخش عمده‌ای از کنوانسیون ۱۹۸۲ بازتاب حقوق بین‌الملل عرفی است و درنتیجه، به‌شدت بر آن تکیه کردند (Jensen, 2017, p. 764). کارشناسان استدلال کردند که مقررات استاندارد حقوق دریاها دربارهٔ عملیات سایبری در منطقهٔ مجاور، تنگه‌های بین‌المللی، آب‌های مجمع‌الجزایری و کابل‌های زیردریایی نیز اعمال می‌شود. در قاعدهٔ ۵۳ دستورالعمل، به عملیات‌های سایبری در آب‌های مجمع‌الجزایری پرداخته شده است. طبق این قاعده، «عملیات‌های سایبری در آب‌های مجمع‌الجزایری باید با رژیم حقوقیِ مُجری در آنجا سازگار باشند» (Tallinn Manual 2.0, 2017, p. 251). در سال‌های اخیر، تعدادی از دولت‌ها توضیحاتی را دربارهٔ چگونگی درک آن‌ها از اعمال قوانین بین‌المللی در فضای سایبر ارائه کرده‌اند. برای مثال، از ابتدای سال ۲۰۱۲، ایالات متحده به ارائهٔ دیدگاه‌های خود در سخنرانی‌ها و بیانیه‌های رسمی پرداخته است. در سال ۲۰۱۸، دادستان کل بریتانیا بیانیهٔ مهمی دربارهٔ دیدگاه‌های بریتانیا در همین رابطه ارائه کرد و در سال‌های بعد، سایر دولت‌ها (عمدتاً اروپایی) دیدگاه‌های دقیق خود را به‌منزلهٔ شاهدی بر رویهٔ عمومی دولتی[6] ارائه کرده‌اند. در همین راستا، دولت‌های شیلی و اکوادور در یادداشت‌های فوق‌العاده‌ای که در سال ۲۰۱۹ برای گزارشگر ویژهٔ کمیتهٔ حقوقی بین امریکایی ارسال کردند، بر این نکته تأکید ورزیدند که برنامه‌ریزی، انجام و اجرای عملیات سایبری باید کاملاً در تطابق با قوانین بین‌المللی عمومی و به‌ویژه حقوق بشر و حقوق بشردوستانه قرار داشته باشند؛ زیرا همهٔ حوزه‌های حقوق بین‌الملل در فضای سایبری نیز کاربرد خواهند داشت (OAS, 2019, p. 17).

---

1. Exclusive Economic Zone (EEZ)
2. Montego Bay
3. International Tribunal for the Law of the Sea (ITLOS)
4. International Tribunal for the Law of the Sea (ITLOS), the “Monte Confurco” Case (Seychelles v. France), Prompt Release, Judgment of 18 December 2000 (b), para. 86.
5. International Tribunal for the Law of the Sea (ITLOS) (a), the “Camouco” Case (Panama v. France), Prompt Release, Order of 27 January 2000, para. 71.
6. Opinio Juris

بنابراین به‌نظر می‌رسد که اصول حقوق بین‌الملل ناظر بر آب‌های مجمع‌الجزایری در فضای سایبر نیز از قابلیت اعمال بهره‌مند است. گواتمالا و گویان هر دو حمایت مثبت خود را از اعمال قوانین بین‌المللی ابراز کردند. بااین‌حال، هر دو اخطارهایی دربارهٔ چگونگی اعمال قانون موجود در جهان ارائه کردند. گواتمالا بدون ارائهٔ هیچ مثالی خاطرنشان کرد که ممکن است مناطقی وجود داشته باشند که «جدیدبودن فضای سایبری مانع از این برنامه شود. درعین‌حال، در همین حوزه نیز اختلاف بین نظریه و رویهٔ دولت‌ها را نمی‌توان نادیده انگاشت؛ برای مثال دولت گویان خاطرنشان کرد که «عملیات سایبری در مفاهیم سنتی نمی‌گنجد و ... درحالی‌که پذیرفته شده است که قوانین بین‌المللی باید در فضای سایبر اعمال شود، اما به سختی می‌توان اصول موجود مانند استفاده از زور را، که به‌طور سنتی متضمن برخی عناصر فیزیکی و حملات مسلحانه بوده و به‌طور سنتی به‌نوعی از سلاح دلالت می‌کند، در این زمینه قابل اعمال دانست» (OAS, 2019, p. 17).

طبق دستورالعمل، فعالیت‌های سایبریِ شناورها و هواپیماهای خارجی در مسیرهای دریاییِ مجمع‌الجزایریِ مشخص‌شده یا در نبود آن‌ها، خط سیرهایی که معمولاً برای دریانوردی بین‌المللی به‌کار می‌روند، باید در راستای طرح ادعای حق عبور از مسیرهای دریاییِ مجمع‌الجزایری توسط شناور یا هواپیمای ذی‌ربط، با رژیم عبور از مسیرهای مزبور مطابقت داشته باشند. افزون‌براین، شناورها و هواپیماهای مبادرت‌کننده به عبور از مسیرهای دریاییِ مجمع‌الجزایری می‌توانند برای تضمین ایمنی و امنیت خود و دیگر شناورها یا هواپیماهایی که همراهی می‌کنند، به فعالیت‌های سایبری دست بزنند (Tallinn Manual 2.0, 2017, p. 252). مشخصاً معنایی که از قدر متیقنِ مستتر در بیان دستورالعمل می‌توان یافت، ممنوعیت استفادهٔ خصمانه از عملیات‌های سایبری و محدودیت این قبیل اقدامات به تضمین ایمنی و امنیت شناورهای مدنظر است؛ زیرا بسیاری از دولت‌ها، اعمال حق دفاع مشروع را در مقابل چنین استفاده‌هایی برای خود محفوظ دانسته‌اند؛ از جمله می‌توان به بیانیهٔ رسمی وزارت دفاع فرانسه در این زمینه اشاره کرد (The National Institute for Defense Studies, 2018).

درعین‌حال، کارشناسانی که در تدوین دستورالعمل شرکت کردند متعهد شدند که قانون را همان‌طور که بود بیان و دستورالعملی تهیه کنند که متکی بر نظر خودشان باشد، نه دیدگاه دولت‌ها. باوجوداین، شاید در دستورالعمل، به تقابل میان عملیات‌های سایبری خطرناک از هر قسم و آثار این اقدامات با اصل حاکمیت مطلق سرزمینی و تعاقبِ تحقق مسئولیت بین‌المللی درپی اتخاذ چنین اقداماتی توجه شده است. حق حاکمیت دولت مجمع‌الجزایری بر چنین آب‌هایی، یکی از اصول مسلم در حقوق بین‌الملل دریاها به‌شمار می‌رود. حال این پرسش مطرح است که انجام عملیات‌های سایبری مضر در قلمروی آب‌های مجمع‌الجزایری را از دیدگاه دولت مجمع‌الجزایری چگونه می‌توان تحلیل کرد؟ در روابط بین دولت‌ها، حاکمیت به معنای استقلال است که حق انحصاریِ اعمال وظایف در قلمروی داخلی را در پی دارد (Akani, 2019, p. 3). بدیهی است که اصل حاکمیت در فضای سایبر نیز مانند سایر فضاها اعمال می‌شود. ممکن است مجموعه‌ای از فعالیت‌های سایبری به تأثیرات مضر درخور توجهی منجر شود که حاکمیت ارضی دولت مجمع‌الجزایری را نقض می‌کند.

از این منظر، در ارزیابی نقض احتمالی حاکمیت ارضی دولت ساحلی درنتیجهٔ انجام عملیات‌های سایبری در آب‌های مجمع‌الجزایریِ مربوط به آن، چندین عامل کلیدی باید در نظر گرفته شود: دامنه، مقیاس، تأثیر یا شدت اختلال ایجادشده، ازجمله اختلال در فعالیت‌های اقتصادی و اجتماعی، خدمات ضروری، عملکردهای ذاتاً دولتی، نظم یا امنیت عمومی باید ارزیابی شود. به‌طور کلی، فعالیت‌های سایبری که بیش از سطحی از تأثیرات ناچیز یا کم‌رنگ افزایش می‌یابند و بدون رضایت دولت مجمع‌الجزایری تأثیرات مضر بسیاری را در قلمروی تحت صلاحیت او می‌گذارند، می‌توانند به‌منزلهٔ نقض قاعدهٔ حاکمیت سرزمینیِ کشور آسیب‌دیده باشند. همچنین فعالیت‌های سایبری با تأثیرات مضر در کشور دیگر به‌منزلهٔ حضور فیزیکی در قلمروی آن کشور نیست. به‌این‌ترتیب، حاکمیت ارضی صرفاً به دلیل فعالیت‌های از راه دور که در زیرساخت سایبری واقع در قلمروی کشور دیگری یا ازطریق آن انجام شده است، نقض نمی‌شود؛ بلکه وجود منشأ چنین عملیاتی در آب‌های تحت صلاحیت دولت ساحلی یا مجمع‌الجزایری نکته‌ای تعیین‌کننده در این امر به‌شمار می‌رود. بنابراین، به‌نظر می‌رسد که اگر انباشت تأثیرات عملیات‌های سایبری، که به آستانهٔ حملهٔ مسلحانه نمی‌رسند، به آستانهٔ لازمی که موردبه‌مورد بررسی می‌شوند برسند، یا اگر هم‌زمان با عملیات مسلحانهٔ فیزیکی در قلمروی تحت صلاحیت دولت مجمع‌الجزایری انجام شوند، در چنین دسته‌ای قرار می‌گیرند. در قضیهٔ سکوهای نفتی،

دیوان بین‌المللی دادگستری رویکرد متشکل از ارزیابی این‌که آیا برخی از اقدام‌های غیرمستقیم ایالات متحده در مقابل ایران را می‌توان به‌منزلهٔ مکمل حملهٔ مسلحانهٔ این دولت به سکوهای نفتی ایران طبقه‌بندی کرد، رد نمی‌کند[1].

فعالیت‌های سایبری، که تأثیرات مضر چشمگیری در اعمال وظایف ذاتاً دولتی دارند، تخلف بین‌المللیِ منجر به طرح مسئولیت بین‌المللی دولت صاحب‌پرچم به‌شمار می‌روند. حقوق مسئولیت دولت‌ها در سراسر طیف وسیعی از حوزه‌های ماهوی حقوق بین‌الملل، ازجمله در فضای سایبر، اعمال می‌شود. اقدامات متقابل قانونی در پاسخ به اقدامات غیرقانونی سایبری بین‌المللی هم ممکن است ماهیت غیرسایبری داشته باشد و هم شامل عملیات سایبری شود. با توجه به ماهیت منحصربه‌فرد فضای سایبر، دامنهٔ دقیق برخی از جنبه‌های رویه‌ای اقدامات متقابل، مانند اطلاع‌رسانی، باید ازطریق رویهٔ دولتی تعریف شود. درصورت درخواست یک کشور آسیب‌دیده از چنین عملیاتی، می‌توان اقدام به کمک کرد؛ برای مثال زمانی که کشوری آسیب‌دیده از تخصص فنی یا قانونی لازم برای پاسخ‌دادن به اقدامات سایبری متخلفانهٔ بین‌المللی برخوردار نیست[2].

هرچند نمی‌توان انکار کرد که در سطح جهانی، هیچ اجماع جهانی میان دولت‌ها دربارهٔ اعمال قوانین بین‌المللی عمومی موجود دربارهٔ عملیات سایبری وجود ندارد، تا چه رسد به چگونگی چنین اقداماتی. از کمبود و نیز فقدان رویهٔ عمومی و رویهٔ قضایی بین‌المللی در این حوزه، می‌توان نتیجه گرفت که دولت‌ها به همان اندازه تمایلی به استناد به زبان حقوق بین‌الملل در طرح اتهامات مربوط به عملیات سایبری سایر کشورها ندارند. تاکنون برخی بازیگران غیردولتی به دنبال پرکردن این کمبود اطلاعاتی با ارائهٔ دیدگاه‌های خود دربارهٔ نحوهٔ تنظیم قوانین بین‌الملل عرفی در حوزهٔ عملیات سایبری دولت‌ها بوده‌اند که به اعتقاد نگارندگان، برجسته‌ترین آن‌ها بدون شک کمیتهٔ بین‌المللی صلیب سرخ و گروه مستقل کارشناسانی است که دستورالعمل‌های تالین را تألیف کرده‌اند. بااین‌حال، واضح است که همهٔ دولت‌ها محتوای این دستورالعمل‌ها را به‌منزلهٔ منعکس‌کنندهٔ حقوق بین‌الملل عرفی تأیید نکرده‌اند. ازاین‌رو، نیاز به مجامع اضافی را که دولت‌ها بتوانند در آن‌ها حضور داشته باشند و به ابراز نظر و جمع‌آوری اطلاعات بپردازند نمی‌توان نادیده انگاشت.

۲. عملیات‌های سایبری در منطقهٔ مجاور

منطقهٔ مجاور[3]، که کلید طلایی گسترش اختیارات دولت ساحلی بر دریای سرزمینی به‌شمار می‌رود، واسط بین دریای سرزمینی و دریای آزاد است. در ادامه، وضعیت حقوقی این منطقه از دریچهٔ حقوق بین‌الملل دریاها و با نگرش بر فعالیت‌های سایبری در این منطقه بررسی می‌شود.

۲-۱. نگاهی مختصر به موازین حقوقی حاکم بر منطقهٔ مجاور

توسعهٔ منطقهٔ مجاور برایند فرایندی است پیچیده از جمع ادعاهای گوناگون دولت‌های ساحلی. اگرچه مفهوم منطقهٔ مجاور به قانون گشت‌زنی[4] بریتانیای کبیر در سدهٔ هجدهم میلادی برمی‌گردد، اما قواعد مربوط به آن تا سال ۱۹۵۸ مورد توافق کشورها قرار نگرفته بود (تاناکا، ۱۳۹۵، ص ۲۰۳). «سواحل مجاور» به معنای سواحل واقع در دو طرف مرز زمینی بین دو کشور مجاور است. دولت‌ها ممکن است تحت کنوانسیون ۱۹۸۲، سواحل مجاور داشته باشند؛ حتی اگر مرز زمینی مشترکی نداشته باشند. بند ۱ مادهٔ ۱۲ کنوانسیون دریای سرزمینی و منطقهٔ مجاور مقرر می‌دارد در مواردی که سواحل دو کشور مقابل یا مجاور یکدیگر باشند، هیچ‌یک حق ندارند دریای سرزمینی خود را فراتر از خط میانی گسترش دهند. بند ۱ مادهٔ ۱۴ کنوانسیون دریای سرزمینی همچنین مقرر می‌دارد که مرز دریای سرزمینی بین دو کشور مجاور با توافق بین آن‌ها تعیین می‌شود. درصورت نبود چنین توافقی، مگر در موردی که خط مرزی دیگری با شرایط خاص توجیه‌پذیر باشد، این مرز با استفاده از اصل فاصله از نزدیک‌ترین نقاط در خط مبدأ، که وسعت دریای سرزمینی هر کشور از آن اندازه‌گیری می‌شود، ترسیم خواهد شد (IILSS, 2022). بنابراین، تحدید حدود عبارت است از فرایندی که شامل تقسیم مناطق دریایی در شرایطی است که دو (یا چند) دولت ادعاهای رقابت دارند.

---

1. ICJ (International Court of Justice), Oil Platforms (lslamic Republic oflran v. United States of America), Decision of the Court, 6 November 2003, para. 64
2. "International Law applicable in cyberspace" in Canada (2022) Available Online at: www.international.gc.ca, (Last visited: 2023)
3. Contigous Zone
4. Hovering Act

دولت ساحلی در منطقهٔ مجاور، می‌تواند کنترل لازم برای جلوگیری از نقض قوانین و مقررات گمرکی، مالی، مهاجرتی یا بهداشتی خود در قلمرو یا دریای سرزمینی را اعمال و نقض قوانین و مقرراتی را، که در قلمرو یا سرزمین آن انجام می‌شود، مجازات کند. بنابراین، برای مثال دولت ساحلی می‌تواند اقداماتی را برای جلوگیری یا تنظیم فعالیت‌های امنیتی تا ۲۴ مایل دریایی انجام دهد؛ به این دلیل که درحال انجام عملیات گمرکی برای جلوگیری از انتقال سلاح به آب‌ها یا درحقیقت بنادر خود است. به‌علاوه، به‌منظور کنترل قاچاق اشیای باستانی و تاریخی یافت‌شده در دریا، دولت ساحلی ممکن است بر این باور باشد که برداشتن چنین اشیائی از بستر دریای منطقهٔ مجاور بدون رضایت آن غیرقانونی است (NOAA, 2022) و تدابیری را در این زمینه اتخاذ کند.

برخی معتقدند ازآنجاکه کنوانسیون ۱۹۸۲ حقوق دریاها مفهوم منطقهٔ انحصاراً اقتصادی را ابداع کرده است، منطقهٔ مجاور و اعمال کنترل در آن چندان حائز اهمیت نبوده است؛ زیرا مادهٔ ۳۳ کنوانسیون مونته‌گوبی لازم‌الإتباع بوده و عملاً منطقهٔ مجاور کاملاً در محدودهٔ منطقهٔ انحصاراً اقتصادی قرار خواهد گرفت (Aquilina, 2014, p. 165). هرچند با توجه به حساسیت‌های موجود در نگرش دول ساحلی به ماهیت و حدود آب‌ها و منابع واقع در منطقهٔ مجاور، طرح این ادعا چندان صحیح به‌نظر نمی‌رسد. وانگهی، از این واقعیت نمی‌توان چشم‌پوشی کرد که دامنهٔ حاکمیت دولت ساحلی هرچه از ساحل به سمت دریا برویم، کمتر می‌شود و به همین علت است که در آب‌های داخلی و دریای سرزمینی، حاکمیت مطلق، در منطقهٔ مجاور حاکمیت نسبی و در دو منطقهٔ انحصاراً اقتصادی و فلات قاره، حقوق حاکمه برقرار است که اصولاً اقتصادی است.

۲-۲. عملیات‌های سایبری در منطقهٔ مجاور در دستورالعمل تالین ۲

به جرئت می‌توان گفت با استثنائات معدودی (به‌ویژه کنوانسیون بوداپست دربارهٔ جرایم سایبری و کنوانسیون اتحادیهٔ افریقا دربارهٔ امنیت سایبری و حفاظت از داده‌های شخصی که هنوز لازم‌الاجراست)، حقوق بین‌الملل برای تنظیم فضای سایبر از قواعد متناسبی بهره‌مند نیست. این درحالی است که این فنّاوری هم جدید و هم پویاست (Hollis, 2021, p. 2) و به همین دلیل است که این ترس محسوس همواره در میان دولت‌های ساحلی و به‌ویژه در منطقهٔ مجاور وجود داشته است که فضای سایبر محیطی است که در آن تهاجم به‌نسبت دفاع برتری دارد و این امر ـ همراه با عواملی مانند مشکلات انتساب، ضعف فرماندهی و کنترل و فقدان آستانه‌های معنی‌دار یا خطوط قرمز قابل تعیین ـ خطرات واقعی و سهوی را برای امنیت و حفاظت از اجرای قوانین دولت ساحلی در منطقهٔ مجاور ایجاد می‌کند (Borghard & Lonergan, 2019, p. 123). از نظر فنی، مشکل انتساب توانایی دولت‌ها را برای استفاده از قوانین بین‌المللی پیچیده می‌کند. دولت‌ها ممکن است بدانند که قربانی حملهٔ سایبری شده‌اند، اما نتوانند تشخیص دهند که آیا مرتکب آن یک دولت است (یا بازیگری که می‌تواند به آن دولت منتسب شود). بدون توانایی فنیِ نسبت‌دادن یک عملیات سایبری به دولتی ثالث، دولت قربانی قادر به استناد به قوانین بین‌المللی نخواهد بود. از نظر سیاسی، برخی از مشکلات ناشی از شفافیت داخلی دولت‌ها هستند. اگرچه برخی از کشورها مدت‌هاست با مسائل امنیت سایبری سروکار دارند، برای سایر دولت‌ها این مسائل هنوز نسبتاً جدید و ناشناخته‌اند.

دستورالعمل در قاعدهٔ ۵۱ خود، به بحث استفاده از ابزارهای سایبری برای پیشگیری از نقض قوانین دولت ساحلی از منطقهٔ مجاور یا در آن ورود کرده است. براساس این قاعده، «در رابطه با شناورهای مستقر در منطقهٔ مجاور دولت ساحلی، آن دولت می‌تواند به‌منظور پیشگیری از یا مقابله با نقض قوانین مالی، مهاجرتی، بهداشتی یا گمرگی در سرزمین یا دریای سرزمینی خویش و ازجمله نقض‌های ارتکاب‌یافته از طریق سایبری، از ابزارهای سایبری استفاده نماید» (Tallinn Manual 2.0, 2017, p. 248). شاید بتوان با استناد به نظر دیوان بین‌المللی دادگستری در قضیهٔ اعمال نظامی و شبه‌نظامی در نیکاراگوئه یا علیه آن[1]، نظر گروه کارشناسان را در این حوزه تأیید کرد. براساس مادهٔ ۵۱ منشور سازمان

[1]. ICJ (International Court of Justice), Military and Paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), judgment, ICJ Reports 1986, para. 194 & 282

ملل متحد، کشوری که مورد حملهٔ مسلحانه قرار می‌گیرد، حق دارد از دفاع مشروع فردی یا جمعی استفاده کند؛ بنابراین به‌نظر می‌رسد دفاع مشروع در پاسخ به حملهٔ انجام‌شده در فضای سایبر شامل ابزارهای دیجیتالِ متعارف با رعایت اصول ضرورت و تناسب است.

پیرو دستورالعمل، اگر شناوری که چه ازطریق ابزارهای سایبری و چه به دیگر طرق، قوانین مالی، مهاجرتی، بهداشتی و گمرکی را نقض کرده است در منطقهٔ مجاور حاضر شود، دولت ساحلی می‌تواند پیش از عزیمت شناور ذی‌ربط از آنجا، مانع از حرکت آن شود (یا درصورتی که مطابق حقوق بین‌الملل صورت پذیرد، به تعقیب فوری[1] مبادرت ورزد (که در مادهٔ ١١١ کنوانسیون مونته‌گوبی به آن پرداخته شده است) و شناور مزبور را برای تحقیق و تعقیب به بندر بازگرداند، دولت ساحلی می‌تواند به‌منزلهٔ بخشی از عملیاتِ ممانعت از حرکت، از ابزارهای سایبری استفاده کند. اقتدار دیگری که دربارهٔ مسائل مالی، مهاجرتی، بهداشتی و گمرکی در منطقهٔ مجاور به دولت ساحلی اعطا شده، صلاحیت پیشگیری است که مبنای قانونی آن، مادهٔ (الف)(١)٣٣ کنوانسیون ١٩٨٢ است. این اقتدار به دولت ساحلی اجازه می‌دهد که برای اخطاردادن و پیشگیری از نقضِ مقررات مالی، مهاجرتی، بهداشتی و گمرکی توسط شناورِ حاضر در منطقهٔ مجاور، که منطقاً مظنون به ارتکاب در قلمرو یا دریای سرزمینی دولت ذیربط است، از ابزارهای سایبری استفاده کند (Tallinn Manual 2, 2017, p. 248). رویهٔ عمومی دولت‌ها نیز تاحدی با این بیان هماهنگی دارد. برای مثال، بولیوی به‌صراحت اعلام می‌کند که هم ممنوعیت استفاده از زور و هم حق ذاتی دفاع از خود در پاسخ به حمله‌ای مسلحانه ممکن است ازطریق ابزارهای سایبری انجام شود (OAS, 2019, p. 20).

واقعیت آن است که اینترنت و فضای سایبر چالش‌های قانونی را مشابه آنچه در حفظ نظم در استفاده از اقیانوس‌های جهان با آن مواجه بوده‌ایم ایجاد می‌کند. کنوانسیون ١٩٨٢، که رسالت برپایی نظم در دریاها و اقیانوس‌های جهان را برعهده دارد، براساس این باور عمیق لازم‌الاجرا شد که همهٔ مشکلات فضای اقیانوس‌ها ارتباط نزدیکی با هم دارند و باید به‌طور کلی مدنظر قرار گیرند (Dunbnr, 1999, p. 627). اینترنت فضایی است که در سطح جهانی به‌اشتراک گذاشته می‌شود؛ بنابراین پیامدهای اقدامات انجام‌شده به‌دست یک کاربر اینترنتی در یک حوزهٔ جغرافیایی ممکن است به خلق آثاری در سطح جهانی منجر شود. درنتیجه، چالش‌های قانونی ناشی از تهاجم سایبری بسیار فراتر از دیدگاه سهل‌انگارانه و پردازش مختصر و چه‌بسا شتاب‌زدهٔ دستورالعمل دربارهٔ وضعیت فعالیت‌های سایبری در آب‌های مجاور بوده و از بسیاری جهات، مشابه مشکلات ناشی از دزدی دریایی و سایر فعالیت‌های مجرمانه در دریاهای آزاد است (Stahl, 2007, p. 267). مادهٔ ١٠٥ کنوانسیون مونته‌گوبی مقرر می‌دارد: «در دریای آزاد یا در هر مکان دیگری خارج از صلاحیت هر کشوری، هر دولتی می‌تواند کشتی یا هواپیمای دزدان دریایی را توقیف کند.»

به‌نظر می‌رسد که به‌رغم تفاوت در معنا، تأثیر شنیع دو جرم مقایسه‌شده و تأثیر آن‌ها در امنیت بین‌المللی، به طرزی جدی با یکدیگر متشابه است. صرف‌نظر از کاستی‌های موجود و چالش‌های مطروحه در مسیر استفاده از اصل صلاحیت جهانی در مقابله با دزدی دریایی، نمی‌توان انکار کرد که تاکنون استفاده از این رژیم حقوقی در مقابله با جرم مذکور، آثار مطلوب و البته بازدارنده‌ای را از خود برجای گذارده است. با توجه به مسائل و دشواری‌های موجود در مسیر مقابله با حملات و فعالیت‌های مضر سایبری علیه یک کشور در مناطق خاصی از قلمروی تحت صلاحیت یا موضوع حقوق حاکمهٔ آن دولت، استفاده از رژیم حقوقی مشابه، یعنی اعمال اصل صلاحیت جهانی در مقابله با مرتکبان چنین اعمالی که بی‌شک دولت قربانی حملات به‌راحتی قادر به دستگیری و محاکمهٔ آنان نخواهند بود، موقعیت مقبول و مناسبی، حتی اگر نه کافی، برای مقابله با ارتکاب این جرم بین‌المللی و ایجاد بازدارندگی در قبال آن فراهم خواهد کرد. بنابراین با قائل‌شدن چنین ماهیتی برای جرائم و فعالیت‌های نابه‌جای سایبری که بر امنیت دولت ساحلی تأثیرگذار است و یا اجرای صحیح قوانین دولت صاحب صلاحیت در آب‌های مجاور، شاید بتوان سیستمی از واکنش سریع، همه‌جانبه و بازدارنده، مشابه نوع برخورد با پدیدهٔ دزدی دریایی، را در برخورد با چنین اقداماتی در حقوق بین‌الملل دریاها تعبیه و اجرا کرد.

[1]. Hot Pursuit

۳. منطقهٔ انحصاراً اقتصادی و عملیات‌های سایبری

شاید بتوان شناسایی منطقهٔ انحصاراً اقتصادی در کنوانسیون ۱۹۸۲ را نتیجهٔ تلاش‌ها و پافشاری‌های کشورهای رهاشده از یوغ استعمار برای دستیابی به استقلال اقتصادی درپی استقلال سیاسی دانست که در دهه‌های هفتاد و هشتاد میلادی، برای احقاق حقوق ازدست‌رفتهٔ خود از چنگال قدرت‌های سیاسی و دریایی، به سازمان ملل متحد یورش بردند. در این بخش نیز، همانند دو بخش پیشین، نخست نگاهی به موازین حاکم بر این منطقه می‌افکنیم و سپس عملیات‌های سایبری در آن را از دریچهٔ دستورالعمل تالین نظاره‌گر می‌شویم.

۳-۱. نگاهی کوتاه به موازین حقوقی حاکم بر منطقهٔ انحصاراً اقتصادی

منطقهٔ انحصاراً اقتصادی در پاسخ به نیاز جهان امروز برای توسعهٔ اقتصادی کشورهای ساحلی ایجاد شده (Sharma, 2010, p. 130) و از نوآوری‌های کنوانسیون ۱۹۸۲ به‌شمار رفته است (امیدی، ۱۳۹۴، ص۱۷۴). کنوانسیون حقوق دریاها با برقراری تعادل میان حقوق و تکالیف دولت‌های ساحلی و ثالث در منطقهٔ انحصاراً اقتصادی، رژیم حقوقی خاص و متفاوتی را بر این منطقه حاکم کرده است که درواقع بازتابانندهٔ روحی است که به ورود این نهاد در حوزهٔ حقوق بین‌الملل منجر شد: به‌رسمیت‌شناختن هرچه بیشتر حقوق حاکمیتی کشورهای ساحلی برای بهره‌برداری از منابع طبیعی، حتی فراتر از آب‌های سرزمینی. کنوانسیون ۱۹۸۲ در مواد ۵۵ و ۵۷ خود، منطقهٔ انحصاراً اقتصادی را به‌منزلهٔ منطقه‌ای در دریا تعریف کرده که یک کشور مستقل در آن از حقوق ویژه‌ای دربارهٔ اکتشاف و استفاده از منابع دریایی برخوردار است. این حقوق شامل تولید انرژی از باد و آب و همچنین استخراج نفت و گاز طبیعی است. منطقهٔ انحصاراً اقتصادی جایی است که در مجاورت دریای سرزمینی و فراتر از آن قرار دارد و می‌تواند حداکثر تا ۲۰۰ مایل دریایی از خط مبدأ گسترش یابد.

در این منطقه، کشور ساحلی از حقوقی بر منابع طبیعی برخوردار است. چنین دولتی به دلایل مربوط به حفاظت از محیط زیست، صلاحیت رسیدگی به برخی فعالیت‌ها را دارد. درعین‌حال، موظف است به حقوق کشورهای دیگر مانند آزادی دریانوردی در منطقه احترام بگذارد. تفاوت دریای سرزمینی با منطقهٔ انحصاراً اقتصادی در این است که در اولی حاکمیت کامل بر آب‌ها در اختیار دولت ساحلی قرار دارد؛ درحالی‌که ارمغان دومی برای دولت ساحلی صرفاً حقوق حاکمه‌ای است که به حقوق این دولت در زیر سطح دریا مربوط استگ ازجمله کاوش و بهره‌برداری، حفظ و مدیریت منابع طبیعی (زنده یا غیرزنده)، تولید انرژی از باد، جریان و آب، ایجاد و استفاده از جزایر مصنوعی، سازه‌ها و تأسیسات، انجام تحقیقات علمی دریایی، و حفاظت از محیط زیست دریایی.

۳-۲. عملیات‌های سایبری در منطقهٔ انحصاراً اقتصادی در دستورالعمل تالین ۲

بسیاری از پژوهشگران در این موضوع متفق‌القول هستند که ممکن است در دهه‌های اخیر، در محیط سایبر، مرز روشن بین برخی مقوله‌های حقوقی اساسی، به‌ویژه دربارهٔ عملیات سایبری نظامی، کم‌رنگ شده باشد (Mačák, 2021, p. 11). طبق قاعدهٔ شمارهٔ ۴۷ دستورالعمل، «دولتی که در منطقهٔ انحصاراً اقتصادیِ دولتی دیگر به انجام عملیات‌های سایبری دست می‌زند، باید در اِعمال حقوق و تکالیف خویش توجه مقتضی را به حقوق و تکالیفِ آن دولت در منطقهٔ ذی‌ربط مبذول دارد و عملیات‌های سایبریِ مربوطه باید برای اهداف صلح‌آمیز انجام پذیرند؛ مگر این‌که در حقوق بین‌الملل به‌گونه‌ای دیگر مقرر شده باشد». کارشناسان این دستورالعمل روشن می‌سازند که هدف از عبارت اخیر در این قاعده، تأکید بر این امر است که برای مثال، مفهوم «اهداف صلح‌آمیز» مندرج در مادهٔ ۵۸(۲) کنوانسیون حقوق دریاها، اتخاذ اقدامات متقابل و ازجمله اقدامات متقابل سایبری از منطقهٔ انحصاراً اقتصادی را ممنوع نمی‌سازد. همچنین مفهوم مزبور دولت‌ها را از انجام عملیات‌هایِ متخاصمانه علیه یکدیگر در منطقهٔ انحصاراً اقتصادی، وفق حقوق جنگ دریایی، بازنمی‌دارد. باوجوداین، عملیات‌های متخاصمانه باید به قواعد جنگ دریایی و نیز ملزومه توجه مقتضی به حقوق و تکالیف دولت ساحلی، هنگام بی‌طرفی آن دولت در مخاصمه، پایبند باشند (Tallinn Manual 2.0, 2017, pp. 240-241). واضح است که برخی از کشورها (مانند ایالات متحده، روسیه و چین) درحال حاضر ظرفیت‌های

گسترده‌ای برای دفاع در برابر عملیات سایبری دارند، ظرفیت‌هایی که آن‌ها را به ابراز دیدگاه‌های گسسته و اغلب متناقض دربارهٔ نقش نظارتی حقوق بین‌الملل سوق داده است. واقعیت آن است که در میانهٔ معادلات قدرت، بسیاری از دولت‌ها به ارائهٔ سیگنال‌های مشابه در مسائلی که قادرند با سکوت از آن جلوگیری کنند، تمایلی ندارند تا مبادا درگیر رقابت با چنین بازیگرانی شوند.

ازآنجاکه طبق کنوانسیون ۱۹۸۲، دولت‌ها می‌توانند در منطقهٔ انحصاراً اقتصادی خویش بر ایجاد و استفاده از جزایر، تأسیسات و تجهیزاتی که اهداف اقتصادی دارند، تحقیقات علمی دریایی (مادهٔ (ب)(۱)۵۶) و برخی حوادث مربوط به آلودگی ناشی از شناورها (مادهٔ ۲۱۱) اِعمال صلاحیت کنند، براساس دستورالعمل، فعالیت‌های سایبری که در تأسیساتِ تولید انرژی مستقر در منطقه‌ای انحصاراً اقتصادی مانند تأسیسات تولید برق ازطریق نیروی باد یا توربین‌هایِ مربوط به جزرومد امواج اختلال ایجاد می‌کنند، در چارچوب ظرفیت صلاحیتیِ دولت ساحلی قرار خواهند گرفت (Tallinn Manual 2.0, 2017, p. 239). افزون‌براین، بر پایهٔ مواد (۱)۵۸ و ۸۷ کنوانسیون، تمامی دولت‌ها در منطقهٔ انحصاراً اقتصادی از آزادی‌های دریای آزاد در زمینهٔ کشتی‌رانی و پرواز بر فراز منطقه و کارگذاری کابل‌ها و لوله‌ها و نیز هر استفادهٔ مشروع از نظر بین‌المللی از دریا دربارهٔ این آزادی‌ها برخوردارند؛ برای مثال هواپیماها و شناورها می‌توانند در زمان حضور در منطقهٔ انحصاراً اقتصادی دولتی دیگر، برای اهداف دریانوردی و ارتباطی، بر قابلیت‌های سایبری تکیه کنند و دولت‌ها، مادامی که توجه مقتضی را به حقوق و تکالیف دولت ساحلی در منطقهٔ انحصاراً اقتصادی مبذول دارند، در کارگذاریِ کابل‌های ارتباطیِ زیردریایی در بستر منطقهٔ انحصاراً اقتصادی دولت دیگر یا اعطای اجازهٔ این کار به شرکت‌هایی که بر آن‌ها اعمال صلاحیت می‌کنند آزادند (Tallinn Manual 2.0, 2017, p. 239). به‌نظر می‌رسد، همان‌گونه که ممانعت از آزادی‌های به‌رسمیت شناخته‌شدهٔ دولت ثالث در منطقهٔ انحصاراً اقتصادی، موجبات مسئولیت بین‌المللی دولت ساحلی را فراهم می‌سازد، ممانعت از اعمال حقوق حاکمهٔ دولت ساحلی در منطقهٔ انحصاراً اقتصادی نیز به طرح مسئولیت بین‌المللی دولت خاطی منجر خواهد شد[1]. در همین راستا و با وحدت ملاک گرفتن از گزارهٔ فوق، استفادهٔ افراطی از ابزارهای سایبری، که به هر نحو به ممانعت از اعمال حقوق حاکمهٔ دولت ساحلی منجر شود، نتایج مشابهی را برای دولت طرف مقابل به همراه خواهد داشت.

همچنین طبق دستورالعمل، شناورها و هواپیماها با هر تابعیتی که باشند، مشروط بر این‌که به‌گونه‌ای ناروا از حقوق حاکمه برشمرده‌شدهٔ دولت ساحلی در آنجا تخطی کنند یا به‌طریقی دیگر حقوق او را نقض نکنند، در منطقهٔ انحصاراً اقتصادی از آزادی‌های موجود در دریای آزاد برخوردارند. این کارشناسان خاطرنشان کردند که کنوانسیون از اشاره به منفعت امنیتی در منطقهٔ انحصاراً اقتصادی غافل مانده و درواقع توجه مقتضی را فقط دربارهٔ «حقوق و تکالیف» دولت ساحلی و نه منافع او در مفهومی کلی‌تر لازم دانسته است. براین‌اساس، فعالیت‌های نظامی نظیر پرواز بر فراز منطقه با هواپیماهای جنگی، مانور مشترک دریایی، تمرینات نظامی، پایش، فعالیت‌های پیمایشی، شناسایی و گردآوری اطلاعات و آزمایش و شلیک تسلیحات، مشروط به توجه مقتضی به حقوق دول ساحلی مجازند (Tallinn Manual 2.0, 2017, p. 240). این درحالی است که به موازات فعالیت‌های نظامی، بخش جهانی دریانوردی، به‌ویژه در حوزهٔ کشتی‌رانی تجاری و تحقیقاتی، امروزه به‌طور فزاینده‌ای به دیجیتالی‌شدن، یکپارچه‌سازی عملیاتی و عملکرد متکی به اتوماسیون وابسته است. در جهانی که امروز می‌شناسیم، کشتی‌سازان پیش‌رو به دنبال نوآوری با استفاده از فنّاوری‌ها و سامانه‌هایی هستند که فراتر از طراحی‌های سنتی قرار دارند تا کشتی‌هایی با کنترل از راه دور، ارتباطات و قابلیت‌های اتصال پیشرفته بسازند. پذیرش فنّاوری اطلاعات و ارتباطات در صنعت کشتی‌رانی، قطعاً با انفجار خطرات موجود و معرفی خطرات جدید، به‌ویژه در آب‌های انحصاراً اقتصادی، همراه خواهد بود.

[1]. ICJ (International Court of Justice), Territorial and Maritime Dispute (Nicaragua v. Colombia), Application- Instituting Proccedings, 6 December 2001, para. 4

طبق دستورالعمل اروپایی[1]، کشتی‌های سایبری ازجمله حیاتی‌ترین زیرساخت‌هایی هستند که به‌شدت به خدمات دیجیتال متکی‌اند؛ درحالی‌که اختلال مخرب در عملیات آن‌ها ممکن است به آسیب مالی و زیست‌محیطی یا حتی به‌خطرانداختن ایمنی انسان منجر شود. همچنین تشخیص و برد رادیویی (رادار) سیستمی حیاتی برای کشتی‌های مدرن است؛ زیرا اطلاعات ارزشمندی دربارهٔ محیط اطراف کشتی فراهم می‌کند و اشیای فیزیکی را با استفاده از امواج رادیویی، برای مثال امواج مایکروویو در طیف الکترومغناطیسی تشخیص می‌دهد. اکثر کشتی‌ها و شناورهای مدرن، که عمدتاً برای پیمایش مسیرهای طولانی و عبور از مناطق انحصاراً اقتصادی و آب‌های آزاد استفاده می‌شوند، به پایانه‌هایی با دهانهٔ بسیار کوچک به‌منظور اطمینان از سرعت بالای انتقال داده در طول عملیات دریایی مجهزند که به‌منزلهٔ ایستگاه زمینی ماهواره برای ارسال و دریافت داده‌ها عمل می‌کنند. صنعت حمل‌ونقل مدرن همچنین شاهد افزایش تقاضا برای سیستم‌های نظارت تصویری هوشمند خودکار به‌منظور نظارت بر عملیات حمل‌ونقل، به‌ویژه در مناطق ذخیره‌سازی بزرگ، ژنراتورها و کشتی‌های بزرگ حامل محموله‌های باارزش تجاری است. اخیراً چندین مورد جرایم سایبری در خلال فعالیت‌های تحقیقاتی و تجاری در آب‌های انحصاراً اقتصادی علیه کشتی‌های ثبت‌شده در دولت ساحلی یا متعلق به دولت‌های ثالث گزارش شده؛ درحالی‌که موارد دیگر ناشناخته مانده است؛ زیرا مالکان کشتی به دلیل بیم از لطمهٔ احتمالی به شهرت شرکت‌های کشتی‌سازی خود، حاضر نیستند آن‌ها را گزارش کنند (Akpan et.al, 2022, pp. 127-128).

کشتی‌های جنگی و هواپیماهای نظامیِ دارای قابلیت‌های مرتبط با عملیات‌های سایبری، در دریانوردی و فعالیت درخلال منطقهٔ انحصاراً اقتصادی و از آن آزادند (Tallinn Manual 2.0, 2017, p. 240). بااین‌حال، شماری از کارشناسان دستورالعمل قائل به این بودند که برخی از فعالیت‌های نظامی و ازجمله فعالیت‌های توأمان با کارکردهای اطلاعاتی و عملیات‌های سایبری، بدون رضایت دولت ساحلی نباید در منطقهٔ انحصاراً اقتصادی انجام شوند. آنان ابراز داشتند که مادهٔ ۵۸(۳) کنوانسیون حقوق دریاها، بر لزوم بذلِ توجه مقتضی به حقوق و تکالیف دولت ساحلی، که ایشان آن را مشتمل بر امنیت می‌دانند، تأکید می‌ورزد. همچنین به باور بیشینهٔ کارشناسان، فعالیت‌های نظامی نوعاً تأثیری در بهره‌مندی از حقوقِ حاکمه و صلاحیتِ محدودی که دولت ساحلی در منطقهٔ انحصاراً اقتصادی از آن‌ها برخوردار است برجای نمی‌گذارد. باوجوداین، کلیهٔ کارشناسان توافق داشتند که تحقیقات علمی دریایی برای «منفعت کل بشریت» ازجمله تحقیقاتی که ازطریق نیروهای نظامی انجام می‌شوند، مستلزم کسب رضایت‌اند (Tallinn Manual 2.0, 2017, p. 240). با توجه به حقوق حاکمهٔ به‌رسمیت شناخته‌شده برای دولت ساحلی در این مناطق و برقراری مسئولیت اصلی حفظ نظم و امنیت در چنین مناطقی برعهدهٔ دولت اخیر، چنین استدلالی را می‌توان منطقی ارزیابی کرد.

کارشناسان در زمان تدوین دستورالعمل به این نتیجه رسیدند که «یک نکتهٔ خاص در زمینهٔ سایبری، آزادی ناوبری در دریای آزاد و استقرار کابل‌های زیردریایی است. در این راستا، «حق بازدید»[2] را دربارهٔ فعالیت‌های سایبری تأیید کردند (Tallinn Manual 2.0, 2017, p. 236). دربارهٔ کابل‌های زیردریایی، کارشناسان نتوانستند درمورد اعمال صلاحیت قضایی «بین دولت ساحلی و دولتی که کابل ارتباطی زیردریایی را در فلات قاره کشور ساحلی یا در منطقهٔ انحصاراً اقتصادی آن می‌گذارد» به توافق برسند. اگرچه موافقت کردند که آسیب‌رساندن به کابل‌های ارتباطی زیردریایی نقض قوانین بین‌المللی است، این امر را نیز پذیرفتند که می‌توان از چنین کابل‌هایی برای جمع‌آوری و انتقال داده‌ها استفاده کرد (Tallinn Manual 2.0, 2017, p. 257). این دستورالعمل، در ضمن مباحث خود به مناطقی اشاره می‌کند که در آن‌ها حقوق دریاها دربارهٔ عملیات سایبری وضعیت ناپایدار دارد، مانند نیاز دولت‌ها به یافتن روشی برای جرم‌انگاری آسیب عمدی یا سهوی به کابل‌های ارتباطی زیردریایی در زیر دریاهای آزاد (Borghard, 2019, p. 140).

با توجه به حجم وسیعی از داده‌هایی که ازطریق کابل‌های ارتباطی زیردریایی عبور می‌کنند و توانایی فزاینده کشورها برای دسترسی به آن‌ها، بی‌شک ناحیهٔ انحصاراً اقتصادی منطقه‌ای است که رویهٔ دولت‌ها در آن ادامه خواهد یافت و جایگاه تعیین‌کنندهٔ خود را با قدرت حفظ خواهد

[1]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).

[2]. Right to visit

کرد. در همین راستا و به‌منظور یکپارچه‌سازی رویهٔ دولت‌ها و تضمین امنیت سایبری در حوزهٔ مدنظر از این رهگذر، شاید بهترین گزینهٔ موجود بر روی میز جامعهٔ جهانی، تلاش برای تدوین و تصویب سندی الزام‌آور و عام‌الشمول در این حوزه در سطح بین‌المللی باشد. برهمین‌اساس، اگر ادعا کنیم که چنین موضوعی برای قرارگیری در دستور کار کمیسیون حقوق بین‌الملل اهمیت و حساسیت فراوانی دارد سخنی به‌گزاف نگفته‌ایم.

۴. تنگه‌های بین‌المللی و عملیات‌های سایبری

در این بخش، نخست به‌اختصار به موازین حاکم بر تنگه‌های بین‌المللی نظر می‌افکنیم و سپس رویکرد دستورالعمل در قبال عملیات‌های سایبری در این بخش از دریاها و اقیانوس‌ها را بررسی می‌کنیم.

۴-۱. نگاهی کوتاه به موازین حقوقی حاکم بر تنگه‌های بین‌المللی

تنگه‌های بین‌المللی[1] به علت نقش‌های گوناگونِ اقتصادی، ارتباطی، نظامی و سیاسی (Ajorloo & Turk, 2015, p. 75) در حقوق بین‌الملل دریاها و مسائل امنیتی و پدافندی کشورها اهمیت بسزایی دارند. در این میان، تنگه‌های راهبردی به‌خاطر ارزش‌های چندسویهٔ خود، در موازنهٔ قدرت منطقه‌ای و جهانی نقش مؤثری دارند و دولت‌ها و قدرت‌های حاکم بر تنگه از آن به‌منزلهٔ ابزاری در سیاست خارجی خود بهره می‌گیرند (حافظ‌نیا و ربیعی، ۱۳۹۴، ص ۳) و در مقابل، چالش‌آفرین نیز هستند. برای نمونه، مسئلهٔ عبور از تنگه‌های بین‌المللی و به‌طور خاص تنگهٔ هرمز، به‌سبب اهمیت ژئوپلتیکی و ژئواستراتژیکی آن برای ایران در منطقهٔ بسیار واجد اهمیت خلیج‌فارس (مجتهدزاده، ۱۳۸۸، صص ۳۱-۳۳) و نیز وابستگی تقریباً کامل این کشور به آن، به‌ویژه از نظر اقتصادی (حافظ‌نیا و میرزایی‌تبار، ۱۳۹۲، ص ۹۱)، یکی از تردیدهای حقوقی و سیاسی ایران برای تصویب کنوانسیون مونته‌گوبی بوده که در سال‌های اخیر موجب بروز تنش‌هایی شده است (Lott & Kawagishi, 2022, p. 123). حاکمیت در تنگه‌های بین‌المللی، همچون قلمروهای دیگر دریایی، در گذشته تابع توان نظامی کشورهای ساحلی و توافق‌های دوجانبهٔ بین‌المللی بود (عسگری و قادری حاجت، ۱۴۰۰، ص ۱۱۴)، ولی امروزه حقوق بین‌الملل درحکم شاخهٔ حقوقیِ منظم روابط بین‌الملل، قواعد و موازینی را برای آن‌ها وضع کرده و موضوع تنگه‌ها، در گفتمان‌های اصلی حقوق بین‌الملل، که به بیش از سه سده پیش و زمان هوگو گروسیوس در سدهٔ هفدهم بازمی‌گردد، مطرح بوده است (Oral, 2019, p. 163).

تنگه‌های بین‌المللی، که برخلاف کانال‌ها یا ترعه‌های بین‌المللی، ساختهٔ دست انسان هستند (Spanier, 2023, p. 118)، راه‌هایی آبی شمرده می‌شوند که از حیث جغرافیایی به‌دست بشر حفر نشده‌اند، بلکه به‌صورت طبیعی به‌وجود آمده‌اند و دو دریا را به‌هم متصل می‌کنند. این دست آبراه‌ها، اگر قابلیت دریانوردی داشته و طبق حقوق بین‌الملل، وصف «بین‌المللی» پیدا کرده باشند، تنگهٔ بین‌المللی محسوب می‌شوند؛ حتی اگر تمامی طول تنگه در قلمرو یک کشور قرار گرفته باشد. طبق تعریف کنوانسیون ۱۹۸۲، حقوق دریاها، تنگه‌های بین‌المللی عبارت‌اند از تنگه‌هایی که در خدمت دریانوردی بین‌المللی هستند و بخشی از دریای آزاد یا منطقهٔ انحصاراً اقتصادی را به بخش دیگری از دریای آزاد یا منطقهٔ انحصاراً اقتصادی یا دریای سرزمینی یک کشور را به بخشی از دریای آزاد یا منطقهٔ انحصاراً اقتصادی کشور دیگر متصل و مرتبط می‌کنند (مواد ۳۷ و ۴۵). نظام حقوقی عام یا مشترک تنگه‌های بین‌المللی، از یک‌سو مشتمل بر قواعد عرفی عام و از سوی دیگر، شامل دو معاهدهٔ عام بین‌المللی، یعنی عهدنامهٔ ۱۹۵۸ ژنو دربارهٔ دریای سرزمینی و منطقهٔ مجاور و عهدنامهٔ ۱۹۸۲ حقوق دریاهاست؛ البته گفتنی است که بخش اعظمی از قواعد معاهداتی یادشده، به‌ویژه مقررات دریای سرزمینی، به‌رغم اندک‌بودن آن، تدوین قواعد عرفی است (ضیایی بیگدلی، ۱۴۰۱، صص ۳۲۶-۳۲۷). افزون‌براین، برخی تنگه‌های بین‌المللی مشمول معاهدات تاریخی ویژه‌ای هستند که از مهم‌ترین آن‌ها تنگه‌های بسفر و داردانل ترکیه را می‌توان نام برد که مسائل مربوط به آن‌ها، به‌ویژه پس از درگیری‌های چند سال اخیر در اوکراین و به‌طور خاص از سال ۲۰۱۴ به این‌سو، اهمیتی افزون‌تر یافته است (Yücel, 2019, p. 214).

[1]. International straits

در کنوانسیون ۱۹۵۸[1]، تنگه‌ها صرفاً مشمول رژیم عبور بی‌ضرر می‌شدند، اما در کنوانسیون ۱۹۸۲، با توجه به گسترش عرض دریای سرزمینی و مشمول‌شدن پهنهٔ آبی ده‌ها تنگهٔ بین‌المللی در چارچوب دریای سرزمینی و همچنین به‌سبب جلب نظر قدرت‌های بزرگ دریایی، برخی تنگه‌های بین‌المللی مشمول رژیم عبور ترانزیت[2] شدند (امیدی، ۱۳۹۴، ص ۱۹۲) که رژیم عبوری آزادتر از عبور بی‌ضرر در عرف بین‌المللی و کنوانسیون ۱۹۵۸ ژنو است (Caligiuri, 2020, p. 1). سنجهٔ تعیین این‌که تنگه‌ای تابع عبور ترانزیت است یا خیر، جغرافیایی است و نه کارکردی. در این زمینه، کاربرد تاریخی یا حجم رفت‌وآمد از تنگه نیز تعیین‌کننده نیست؛ بلکه اگر بتوان تنگه‌ای را برای دریانوردی بین‌المللی میان یک منطقه از دریای آزاد یا منطقهٔ انحصاراً اقتصادی با دیگر منطقهٔ دریای آزاد یا منطقهٔ انحصاراً اقتصادی به‌کار گرفت، رژیم ترانزیت اعمال می‌شود که مبنای آن، مادهٔ ۳۷ کنوانسیون ۱۹۸۲ است (Office of the Staff Judge Advocate, 2021, p. 41). به‌نظر می‌رسد تعبیهٔ این رژیم در کنوانسیون مونته‌گوبی برای برخی تنگه‌هایی که به‌منظور دریانوردی بین‌المللی به‌کار می‌روند، برایند چیرگی اصلِ بنیادین آزادی دریانوردی برای جامعهٔ بین‌المللی بر اصل حاکمیت دولت‌های مجاور آن‌هاست.

گفتنی است که تفاوت عبور ترانزیت با عبور بی‌ضرر این است که در عبور ترانزیت، هواپیماهای خارجی برای عبور بر فراز تنگه‌ها نیاز به کسب اجازهٔ قبلی از کشور ساحلی ندارند و زیردریایی‌ها ملزم نیستند به روی سطح آب آمده و پرچم خود را نشان دهند. درعوض، زیردریایی‌ها، کشتی‌ها و هواپیماهای خارجی موظف‌اند سریع و پیوسته از قعر، سطح و فراز تنگه عبور کنند و از ارتکاب هر عملی که به تهدید یا استفاده از زور علیه حاکمیت، تمامیت ارضی و استقلال سیاسی دولت مجاور تنگه منجر شود، خودداری کنند. دولت ساحلی می‌تواند برای امنیت عبور از تنگه، مسیرهای دریایی خاصی را تعریف کند؛ به شرط آن که به تصویب «سازمان بین‌المللی ذی‌صلاح» برسد. دولت ساحلی موظف است خطرات احتمالی عبور از تنگه را به اطلاع کشتی‌های عبوری برساند. بر این مورد در رأی دیوان بین‌المللی دادگستری در قضیهٔ کانال کورفو[3] تأکید شد (امیدی، ۱۳۹۴، صص۱۹۲ و ۱۹۵-۱۹۶)، موضوعی که نخستین دعوی مطرح‌شده در دیوان لاهه است و این خود نشان‌دهندهٔ جایگاه برجستهٔ مسائل حقوق دریاها در سپهر حقوق و روابط بین‌الملل است.

۴-۲. عملیات‌های سایبری در تنگه‌های بین‌المللی در دستورالعمل تالین ۲

به گفتهٔ پژوهشگران، مسئلهٔ عبور از تنگه‌های بین‌المللی از سدهٔ هفدهم به این‌سو، همواره محل مناقشه بوده (Rusli, 2012, p. 110) و به این علت هم در روابط و حقوق بین‌الملل اهمیت بسزایی داشته است. به همین سبب است که قاعدهٔ ۵۲ دستورالعمل، موضوع عملیات‌های سایبری در تنگه‌های بین‌المللی را به بحث گذاشته و بیان کرده است: «عملیات‌های سایبری در تنگه‌ای که برای دریانوردی بین‌المللی به‌کار می‌رود، باید با حقِ عبور ترانزیت سازگار باشند» (Tallinn Manual 2.0, 2017, p. 249). این قاعده، بر قسمت دوم از بخش سوم کنوانسیون حقوق دریاها استوار است که کارشناسان دستورالعمل، درخصوص انعکاس حقوق بین‌الملل عرفی‌بودن آن همدل بودند. ماده‌ی ۳۴ کنوانسیون مونته‌گوبی اشعار دارد که تنگه‌های استفاده‌شده برای دریانوردی بین‌المللی یا همان تنگه‌های بین‌المللی، مسیرهای موجود در دریای سرزمینی یک دولت یا دریاهای سرزمینیِ متداخل دو یا چند دولت هستند که یک ناحیه از دریای آزاد یا منطقه‌ی انحصاراً اقتصادی را به ناحیه‌ای دیگر از دریای آزاد یا منطقه‌ی انحصاراً اقتصادی متصل می‌سازند و برای دریانوردی بین‌المللی به‌کار می‌روند. بستر و آب‌هایِ موجود در یک تنگه‌ی بین‌المللی مشمول صلاحیت دولت یا دولت‌های مجاور هستند و آن دولت‌ها، مشروط به رعایت حق عبور ترانزیتی که شناورها و هواپیماهای سایر کشورها از آن برخوردارند، عموماً از حقوق مجری در دریای سرزمینی بهره‌مند و در مقابل در آنجا مسئول‌اند (Tallinn Manual 2.0, 2017, p. 249). در واقع، این وضعیت با عبور بی‌ضرر دریای سرزمینی تفاوت دارد و رفت‌وآمد شناورها و هواپیماها را کمتر کنترل می‌کند و شبیه عبور از دریای آزاد هم نیست (چرچیل و لو، ۱۴۰۰، ص ۱۵۲). با توجه به مصونیت حاکمیتی کشتی‌های جنگی آستانه‌ای که یک کشور ساحلی می‌تواند کشتی

[1]. 1958 Geneva Convention on the Territorial Sea and the Contiguous Zone
[2]. Transit passage
[3]. Corfu Channel Case

جنگی را مجبور به خروج از تنگه‌ی بین‌المللی کند مشخص نیست. به‌علاوه، کشورهای ساحلی نمی‌توانند ترانزیت را ممنوع یا حقوق عبور بی‌ضرر کشتی‌های دارای انرژی هسته‌ای را مختل کنند.

کارشناسان دستورالعمل به این امر اشاره می‌کنند که حق عبور ترانزیت در طول تنگه، یعنی از خط ساحلی یکی از دولت‌های مجاور تنگه تا خط ساحلی دولت مجاور دیگر[1] و کرانه‌های آن وجود دارد. براساس مواد ۳۸(۲) و (الف)۳۹(۱) کنوانسیون مونته‌گوبی، عبور از تنگه با شناورها و هواپیماها باید پیوسته و سریع باشد و بدون تأخیر صورت پذیرد. چنان‌که در بخش پیشین نیز اشاره شد، برخلاف عبور بی‌ضرر، دولت یا دولت‌های ساحلی نمی‌توانند عبور ترانزیت را تعلیق کنند. به‌علاوه، طبق مادهٔ (ج)۳۹(۱) کنوانسیون ۱۹۸۲ حقوق دریاها، شناورها و هواپیماها می‌توانند «در حالت عادی» به عبور مبادرت ورزند؛ یعنی زیردریایی‌ها می‌توانند به صورت غوطه‌ور در آب حرکت و هواپیماها اجازه دارند بر فراز تنگه پرواز کنند. پیرو دستورالعمل، که از مادهٔ ۳۹ کنوانسیون مونته‌گوبی الهام گرفته است، شناورها و هواپیماهای حاضر در تنگه، درصورت مبادرت به فعالیت‌های سایبریِ مغایر با رژیم عبور ترانزیت، نمی‌توانند مدعی حق ذی‌ربط شوند. برای مثال، گردآوری اطلاعات هوابردِ ارتباطات سایبری از دولت مجاور با رژیم عبور ترانزیت مغایرت دارد؛ زیرا ازطریق ابزارهایِ سایبری، درحال ارسال تبلیغات ضددولتی به کشور مربوطه است (Tallinn Manual 2.0, 2017, p. 250). در واقع، این مقرره، از منافع دولت ساحلی در برابر آزادی افسارگسیخته‌ی کشتی‌ها و هواپیماهای درحال عبور از تنگه حفاظت می‌کند (چرچیل و لو، ۱۴۰۰، ص ۱۵۵).

طبق دستورالعمل، شناورها و هواپیماهای مبادرت‌کننده به عبور ترانزیت برای تضمین ایمنی و امنیت خویش و شناورها یا هواپیماهایی که همراهی می‌کنند می‌توانند به فعالیت‌های سایبریِ ضروری دست بزنند. عملیات‌های نظامیِ خصمانه ازجمله عملیات‌های سایبری، درصورت انجام درحین عبور ترانزیت از تنگه‌ای بی‌طرف در خلال مخاصمه‌ای مسلحانه، مجاز نیستند (Tallinn Manual 2.0, 2017, p. 250)، امری که در حقوق بی‌طرفی و بایستگی خودداری از نقض آن به‌دست طرف‌های یک درگیری مسلحانهٔ بین‌المللی ریشه دارد (کولب و هاید، ۱۳۹۴، صص ۴۳۷-۴۳۱). همچنین گفتنی است که برپایهٔ دستورالعمل، به پیروی از مادهٔ ۴۲(۱) کنوانسیون مونته‌گوبی، شناورها یا هواپیماهای مبادرت‌کننده به عبور ترانزیت، جز قوانین و مقررات مرتبط با ایمنی دریانوردی، تنظیم آلودگی، فعالیت‌های ماهیگیری و امور مالی، مهاجرتی، بهداشتی و گمرکی، مشمول قوانین و مقررات دولتِ مجاور تنگه نیستند. ممکن است چنین قوانین و مقرراتی مثلاً فعالیت‌های سایبریِ انجام‌شده برای ارسال دستورالعمل‌های ایمنی دریانوردی یا انتظام‌بخشی به رفت‌وآمد ازطریق تنگه‌ها را مطمح نظر قرار دهند. کلیه‌ی شناورها و هواپیماها باید درحین عبور ترانزیت، آن‌ها را رعایت کنند (Tallinn Manual 2.0, 2017, p. 250).

مطابق نظر کارشناسان دستورالعمل، هرچند امکان دارد شناورها و هواپیماهای بهره‌مند از مصونیت حاکمیتی در حین عبور ترانزیت به فعالیت‌های سایبری ناقض قوانین و مقررات دولت ساحلی مبادرت جویند، ولی دولت ساحلی نمی‌تواند مدعی صلاحیت اجرایی بر آن‌ها باشد. دولت ساحلی ازجمله با ابتنای بر مواد ۳۴ و ۳۸(۳) کنوانسیون حقوق دریاها، اقتدار «الزام» شناورِ واجد مصونیت حاکمیتی به توقف فعالیت مجرمانه و ترک تنگه را در اختیار دارد. افزون‌براین، مبتنی‌بر مادهٔ ۴۲(۵) کنوانسیون، دولت صاحب‌پرچمِ هواپیما یا شناورِ دارای مصونیت حاکمیتی، بابت هر زیان یا خسارت، واجد مسئولیت بین‌المللی است که از رعایت‌نکردن قوانین و مقررات دولت ساحلی ناشی می‌شود. دولت صاحب‌پرچم، درصورتی‌که فعالیت ذی‌ربط موجب شکل‌گیری یک عمل متخلفانه بین‌المللی شود نیز مسئولیت دارد (Tallinn Manual 2.0, 2017, pp. 250-251). گفتنی است که مسئله‌ی انتساب مسئولیت بین‌المللی در فضای سایبر و عملیات‌های سایبری، یکی از مسائل حقوق بین‌الملل کنونی در رویارویی با دنیای کمترشناخته‌شده‌ی سایبری است (Costa & Ben, 2016, pp. 141-142).

دستورالعمل به بحث عملیات‌های سایبری در تنگه‌های خاص بین‌المللی نیز اشاره می‌کند. دربارهٔ سایر تنگه‌ها نیز رژیم‌هایی وجود دارند که واجد مجموعه‌ای متفاوت از تعهدات هستند. مانند تنگه‌ای که درخصوص آن یک رژیمِ معاهداتیِ خاص اِعمال می‌شود؛ همچون تنگه‌های کشور ترکیه که رژیم حقوقی آن‌ها در کنوانسیون مونترو[2] مقرر شده است. به باور کارشناسان، امکان دارد این قبیل رژیم‌های اختصاصی، عبور

[1]. Shoreline-to-shoreline
[2] Montreux Convention

کشتی‌های جنگی و بایسته‌های مرتبط با فعالیت‌های سایبری را تحت‌الشعاع قرار دهند و باید به‌صورت موردبه‌مورد تجزیه و تحلیل شوند. مثال دیگر تنگه‌هایی هستند که برای دریانوردی بین‌المللی میان دریای آزاد یا منطقه‌ای انحصاراً اقتصادی و دریای سرزمینی کشوری دیگری به‌کار می‌روند. در این تنگه‌ها، رژیم تعلیق‌ناپذیر عبور بی‌ضرر اِعمال می‌شود و قواعد و موازین مرتبط با این نوع عبور بر آن پیاده می‌شود (Tallinn Manual 2.0, 2017, p. 251).

نتیجه‌گیری

در سدهٔ بیست‌ویکم، دات‌کام‌ها، بیت‌ها و بایت‌ها به اندازهٔ گلوله‌ها و بمب‌ها تهدیدکننده هستند. در جهانی که امروز می‌شناسیم، اینترنت از وسیله‌ای ارتباطی به فنّاوری توانمندی که تقریباً همهٔ جنبه‌های فعالیت‌های انسانی را تسهیل می‌کند گسترش یافته است. دریاها نه‌فقط همیشه منبع اصلی تغذیه برای زندگی بوده‌اند، بلکه از زمان ثبت تاریخ، در مسیر تجارت و بازرگانی، ماجراجویی و اکتشاف نیز حرکت کرده‌اند. در سراسر تاریخ بشر، دریاها از یک‌سو مردم را از هم دور نگه داشته‌اند و از سوی دیگر به هم نزدیک کرده‌اند. در این پژوهش، به الزامات و شرایط حاکم بر عملیات‌های سایبری در سه منطقهٔ دریاییِ آب‌های مجمع‌الجزایری، منطقهٔ نظارت یا مجاور، منطقهٔ انحصاراً اقتصادی و نیز تنگه‌های بین‌المللی از چشم‌انداز دستورالعمل تالین ٢ پرداخته شد و تلاش شد که چگونگی اعمال حقوق بین‌الملل موجود بر عملیات سایبری روشن شود. اگرچه این دستورالعمل سندی است غیرالزام‌آور، گروه کارشناسان بین‌المللی تدوین‌کنندهٔ آن مدعی شدند که منعکس‌کنندهٔ قواعد جهان‌شمولی بوده که در حوزهٔ عملیات سایبری از قابلیت اعمال برخوردار است؛ اگرچه چنین ادعایی به‌دلیل نقش مسلط چند دولت غربی در روند تهیهٔ پیش‌نویس و غفلت از عملکرد «دولت‌های آسیب‌دیده» در عملیات سایبری محل تردید است.

هرچند بسیاری از اندیشمندان بر این باورند که دستورالعمل کلیت رویهٔ دولتی را، که باید در شکل‌گیری حقوق بین‌الملل عرفی عامل تعیین‌کننده باشد، نادیده می‌گیرد و بیشترین تأثیر خود را از دول عضو سازمان ناتو می‌پذیرد، ماهیت جامع، تجزیه‌وتحلیل آگاهانه و نتیجه‌گیری و ادغام نظریات برخی از دولت‌ها، همگی ویژگی‌هایی هستند که این دستورالعمل و سلف آن را به یکی از ارزشمندترین مراجع و نقاط عزیمت برای بحث دربارهٔ حقوق بین‌الملل قابل اعمال در عملیات سایبری تبدیل کرده است. درعین‌حال، نمی‌توان انکار کرد که هنوز بسیاری از زمینه‌های اختلاف نظر و ابهام، حتی در میان کارشناسانی که دستورالعمل‌های دوگانهٔ تالین را نوشته‌اند، وجود دارد. همچنین این مشکل درخور توجه است که بسیاری از دولت‌ها دربارهٔ عملیات‌های سایبری در مناطق دریایی به‌طور علنی صحبت یا عمل نکرده‌اند و از این طریق، ایجاد عرف بین‌المللی را بیش‌ازپیش با کندی همراه کرده‌اند. موضوع این پژوهش حوزه‌ای رو به رشد در حقوق بین‌الملل است که در آن نیاز زیادی به بینش و درک برای ایجاد رویکردهای جدید دربارهٔ مشکلات موجود وجود دارد. بااین‌حال، تا زمانی که فقط تابعان فعال حقوق بین‌الملل مسیر دقیق حرکت حقوق بین‌الملل را در حوزهٔ عملیات‌های سایبری مشخص کنند، تالین ٢ نقطهٔ شروع مناسبی برای حرکت رو به جلو در حقوق مربوط به عملیات‌های سایبری به‌ویژه در دریاها خواهد بود.

تشبیه تهدیدات سایبری به چیزی شبیه به نگرانی‌هایی که به همکاری در توسعهٔ حقوق بین‌المللی دریایی منجر شد، نقطهٔ شروع مفیدی برای تحلیل و توسعهٔ واکنشی بین‌المللی است که در پرداختن معنادار به امنیت سایبری جهانی ضروری به‌نظر می‌رسد. در این زمینه، به‌نظر می‌رسد چارچوب حقوقی بین‌المللی حاکم بر دزدی دریایی، حتی با وجود کاستی‌های آن، مبنایی را برای ایجاد رژیمی مشابه به‌منظور تأمین امنیت سایبری بین‌المللی فراهم می‌کند. بدون توافق بین‌المللی، که طیف تجاوز سایبری را تعریف می‌کند، نوعی صلاحیت جهانی را بر مرتکبان اعطا می‌کند و یک سازمان بین‌المللی متمرکز بر سیاست امنیت سایبری تأسیس می‌کند، تهدید امنیت بین‌المللی ناشی از عملیات‌های سایبری همچنان افزایشی خواهد بود. برای این منظور، وجود یک دادگاه یا مرجع بین‌المللی جرایم سایبری به تشویق همکاری در توسعهٔ هنجارهای بین‌المللی مربوط به جرایم سایبری کمک می‌کند؛ درحالی‌که به کشورها اجازه می‌دهد سطحی از خودمختاری را در توسعه و اجرای سیاست‌های امنیت سایبری داخلی حفظ کنند. حتی تشکیل شعبه‌ای مستقل و تخصصی در همین حوزه، در زیرمجموعهٔ دیوان بین‌المللی حقوق دریاها (ایتلوس)، که تاکنون در اثبات توانایی و کارکرد مؤثر خود عملکرد موفقی داشته است، در این حوزه راهگشا خواهد بود.

منابع

امیدی، علی (۱۳۹۴). حقوق بین‌الملل: از نظریه تا عمل، تهران: میزان.

تاناکا، یوشیفومی (۱۳۹۵). حقوق بین‌الملل دریاها، ترجمهٔ آرمین طلعت، تهران: شهر دانش.

چرچیل، رابین و لو، آلن (۱٤۰۰). حقوق بین‌الملل دریاها، ترجمهٔ بهمن آقایی، تهران: گنج دانش.

حافظ‌نیا، محمدرضا و ربیعی، حسین (۱۳۹٤). خلیج فارس و نقش استراتژیک تنگهٔ هرمز، تهران: سمت.

حافظ‌نیا، محمدرضا و میرزایی‌تبار، میثم (۱۳۹۲). بررسی بازتاب‌های انسداد احتمالی تنگهٔ هرمز، تهران: جهاد دانشگاهی واحد تهران.

شمیلیه-ژانرو، مونیک (۱۳۸۲). بشریت و حاکمیت‌ها: سیری در حقوق بین‌الملل، ترجمهٔ مرتضی کلانتریان، تهران: آگه.

ضیایی بیگدلی، محمدرضا (۱٤۰۱). حقوق بین‌الملل عمومی، تهران: گنج دانش.

عسگری، سهراب و قادری حاجت، مصطفی (۱۴۰۰). «جایگاه ژئوپلتیکی تنگه هرمز در راهبرد دفاع دریایی ایران». مطالعات بنیادین و کاربردی جهان اسلام، ۳(۷)، ۱۱۳-۱۴۶.

کولب، رابرت و هاید، ریچارد (۱۳۹۴). درآمدی بر حقوق مخاصمات مسلحانه، ترجمهٔ حسام‌الدین لسانی، تهران: مجد.

مجتهدزاده، پیروز (۱۳۸۸). خلیج فارس: کشورها و مرزها، تهران: عطایی.

Akani, N. (2019). The Concept of Sovereignty in International Law and Relations. Available Online at: https://www.researchgate.net, (Last visited: 2023).

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123-138.

Aquilina, Kevin (2014). 2 Territorial Sea and the Contiguous Zone, *the IMLI Manual on International Maritime Law*. Volume I, 2014.

Borghard, E. D., & Lonergan, S. W. (2019). Cyber operations as imperfect tools of escalation. *Strategic Studies Quarterly*, *13*(3), 122-145.

Caligiuri, A. (2020). Clarifying Freedom of Navigation through Straits Used for International Navigation: A Study on the Major Straits in Asia. *Questions in International Law, Zoom In*, Vol. 76, pp. 1-4.

Churchill, R., Lowe, V., & Sander, A. (2022). The law of the sea. In *The law of the sea*. Manchester University Press.

Costa, F. G. D., & Benn, V. L. H. (2016). The Challenges of Attribution of Internationally Wrongful Acts in The Cyberspace: A Critical Analysis of Control Tests and the Standard of Proof in International Courts. *Revista do CEPEJ*, (19), Special Issue, pp. 122-146.

Dunbar, B. H. (1999). "Recent Developments in the International Law of the Sea". *International Lawyer*, *33*(2), pp. 627-636.

Ertan, A., Floyd, K. H., Pernik, P., & Stevens, T. (Eds.). (2020). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. CCDCOE.

Gamil Aboukhewat, M. (2019). The Legal Status of Archipelagos in the International Law of the Sea. *Economics, Law and Policy, 2*(2), 189-204.

Hollis, D. (2021). A brief primer on international law and cyberspace. *Carnegie Endowment for International Peace, dostupno na: https://carnegieendowment. org/2021/06/14/briefprimer-oninternational-law-and-cyberspace-pub-84763, приступљено, 15*, 2022.

IILSS-International institute for Law of the Sea Studies (2021). LAW OF THE SEA. Available Online at: http://iilss.net, (Last visited 2023).

Jafar Ajorloo, M., & Turk, R. (2014). The strategic importance of the strait of Tiran in the conflict in South West Asia. *Geopolitics Quarterly*, *10*(36), 70-92.

Jensen, E. (2017). The Tallinn Manuul 2.0: Highlights and Insights, *Georgetown Journal of International Law48*, pp. 735-778.

Lott, A., & Kawagishi, S. (2022). The legal regime of the Strait of Hormuz and attacks against oil tankers: law of the sea and law on the use of force perspectives. *Ocean Development & International Law*, *53*(2-3), 123-146.

Mačák, Kubo. (2021). "Unblurring the Lines: Military Cyber Operations and international Law", *Journal of Cyber Policy, Vol. 6, No.3*, pp. 411-428.

NOAA (National Oceanic and Atmospheric Administration) (2022). Maritime Zones and Boundaries, Available Online at: www.noaa.gov, (Last visited: 2023).

O.P. Sharma, (2010). The Exclusive Economic Zone. *Oxford Academic*, pp. 130–167.

OAS- Inter-American Juridical Committee (2019). *International Law and State Cyber Operations, Department of International Law of the Secretariat for Legal Affairs*, pp. 1-34.

Office of the Staff Judge Advocate (2021). International Straits. *International Law Studies, 97*, pp. 39-44.

Oral, N. (2019). Navigating the Ocans: Old and New Challenges for the Law of the Sea for Straits Used for International Navigation. *Ecology Law Quarterly*, *46*(1), pp. 163-190.

Rothwell, D. R., Elferink, O., Scott, K. N., & Stephens, T. (2015). *The Oxford Handbook of the Law of the Sea*, Oxford Handbooks in Law.

Rusli, M. H. B. M.(2012). A Historical Overview of the Legal Status of Straits Used for International Navigation Under International Law. *AALCO Journal of International Law*, *1*(2), pp. 103-131.

Schmitt, M. N. (2017). Peacetime cyber responses and wartime cyber operations under international law: An analytical vade mecum. *Harv. Nat'l Sec. J.*, 8, 239.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Spanier, B. (2023). Freedom of Navigation in the Suez Canal and the Channels: Law of the Sea. In *The Suez Canal: Past Lessons and Future Challenges* (pp. 117-133). Cham: Springer International Publishing.

Stahl, W. M. (2011). The uncharted waters of cyberspace: applying the principles of international maritime law to the problem of cybersecurity. *Ga. J. Int'l & Comp. L.*, *40*, 247.

The German Federal Government of Germany (March 2021). On the Application of International Law in Cyberspace. *Position Paper, German Federal Foreign Office and the German Federal Ministry of Defence in cooperation with the German Federal Ministry of the Interior*, Building and Community. Available at: https://www.auswaertiges, (Last visited: 2023).

Yücel, K. (2019). *The Legal Regime of the Turkish Straits: Regulation of the Montreux Convention and its Importance on the International Relations after the Conflict of Ukraine* (Doctoral dissertation, Johann Wolfgang Goethe-Universität Frankfurt am Main).

Ziolkowski, K. (2013). *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy*. Tallinn: NATO CCD COE Publications.