Scientific Journal of Political Law Approaches

Scientific J. Pol. L. App., 2(2) (2025) 1-18
DOI: 10.22084/qjpla.2025.30423.1012

Bu-Ali Sina University

International Telecommunication Law in the Perspective of the Tallinn Manual 2.0

Kian Biglarbeigi[1], Sattar Azizi[2*]

[1] Ph.D. Student in International Law, Faculty of Law and Political Science, Tehran University, Tehran, Iran.
[2] Professor, Department of Law, Faculty of Humanities, Bu-Ali Sina University, Hamedan, Iran.

ABSTRACT: Cyberspace has become an essential aspect of the telecommunication industry due to the increasing reliance on digital infrastructure and the exponential growth of data traffic. However, with the emergence of technologies such as 5G, the Internet of Things (IoT), and cloud computing, the attack surface of these infrastructures has expanded, introducing new challenges and vulnerabilities that necessitate complex security protocols. On the other hand, the lack of treaty documents and customary international law in the realm of cyberspace is highly noticeable. It should be noted, however, that the absence of specific rules does not imply that states are free to conduct cyber operations without restrictions. Although existing customary and treaty laws do not explicitly regulate cyber operations, through interpretative tools, existing rules can be extended to include cyber operations. Thus, in the absence of global consensus on the application of international rules to cyber operations and the lack of uniform practices among states, the Tallinn Manual 2.0 is recognized as one of the significant efforts toward regulating cyberspace. This document examines the international law applicable to cyber operations and seeks to provide a legal framework for managing the challenges in this domain. In its eleventh chapter, the manual addresses international telecommunication law through four rules, offering related observations and considerations. Therefore, this research, using a descriptive-analytical method and relying on library resources, seeks to examine and analyze the positions of the Tallinn Manual 2.0 regarding international telecommunication law.

Review History:

Received: Dec. 27, 2024
Revised: Feb. 03, 2025
Accepted: Feb. 14, 2025
Available Online: Mar. 19, 2025

Keywords:

Cyberspace
International Telecommunication Law
Cyber Communications
Harmful Interference
Tallinn Manual 2.0.

HOW TO CITE THIS ARTICLE

Biglarbeigi, K., Azizi, S., (2025). International Telecommunication Law in the Perspective of the Tallinn Manual 2.0, *Scientific Journal of Political Law Approaches, 2*(2), 1-18. https://doi.org/10.22084/qjpla.2025.30423.1012

Online ISSN 3092-6394

*Corresponding author's email: s.azizi@basu.ac.ir

نشریه علمی رویکردهای حقوق سیاسی

نشریه علمی رویکردهای حقوق سیاسی، دوره ۲، شماره ۲، پاییز و زمستان ۱۴۰۳، صفحات ۱ تا ۱۸
(مقاله پژوهشی)
DOI: 10.22084/qjpla.2025.30423.1012

حقوق بین‌الملل ارتباطات در نظرگاه راهنمای تالین ۲

کیان بیگلربیگی[۱]، ستار عزیزی[۲*]

۱. دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران.
۲. استاد، گروه حقوق، دانشکده علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران.

خلاصه: فضای سایبر به جنبه‌ای ضروری در صنعت ارتباطات تبدیل شده است که ناشی از وابستگی فزاینده به زیرساخت‌های دیجیتال و رشد تصاعدی ترافیک داده‌ها است. با این‌حال، با ظهور فناوری‌هایی مانند 5G، اینترنت اشیاء و رایانش ابری، سطح حمله به این زیرساخت‌ها گسترش یافته است و چالش‌ها و آسیب‌پذیری‌های جدیدی را به‌وجود آورده که نیازمند پروتکل‌های امنیتی پیچیده است. از سوی‌دیگر، خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه‌ی فضای سایبر بسیار مشهود است. البته باید خاطرنشان نمود که فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به عملیات سایبری نمایند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت درخصوص عملیات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد. از این‌رو در فقدان اجماع جهانی درباره اعمال قواعد بین‌المللی بر عملیات سایبری و کمبود رویه یکپارچه در میان دولت‌ها، راهنمای تالین ۲ به‌عنوان یکی از تلاش‌های مهم در راستای قاعده‌مندسازی فضای سایبر شناخته می‌شود. این سند، حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری را مورد بررسی قرار داده و تلاش می‌کند چارچوبی حقوقی برای مدیریت چالش‌های موجود در این حوزه ارائه دهد. این راهنما در یازدهمین فصل خود، در قالب چهار قاعده، نکات و ملاحظاتی پیرامون حقوق بین‌الملل ارتباطات بیان می‌نماید. لذا در پژوهش حاضر با استفاده از روش توصیفی–تحلیلی و بهره‌گیری از منابع کتابخانه‌ای، سعی شده است مواضع راهنمای تالین ۲ را در ارتباط با حقوق بین‌الملل ارتباطات مورد بررسی و مداقه قرار دهد.

تاریخچه داوری:
دریافت: ۱۴۰۳/۱۰/۲۷
بازنگری: ۱۴۰۳/۱۱/۱۵
پذیرش: ۱۴۰۳/۱۱/۱۶
ارائه آنلاین: ۱۴۰۳/۱۲/۲۹

کلمات کلیدی:
فضای سایبر
حقوق بین‌الملل ارتباطات
ارتباطات سایبری
تداخل مضر
راهنمای تالین ۲

۱- مقدمه

ارتباطات در زمره قلمروهایی است که توانسته است اوّلین همکاری‌های مهم بین‌المللی را ممکن سازد (بیگ‌زاده، ۱۴۰۰، ص۷۹۳) و واکنش دولت‌ها، سازمان‌ها و افراد به همه‌گیری رخداده در سال ۲۰۲۰[۱]، وابستگی حیاتی به سیستم‌های ارتباطی مبتنی بر زیرساخت‌های سایبری را برجسته کرد. بدون مزایای اتصال و ارتباطات، دولت‌ها با چالش‌های بیشتری در مدیریت مواجه می‌شدند، جوامع برای حفظ انسجام خود مشکلات بیشتری داشتند، تعداد بیشتری از شرکت‌ها فعالیت خود را به‌طور کامل متوقف می‌کردند و تجربه انزوای شخصی به‌مراتب دشوارتر می‌شد (Giles & Hartmann, 2021, p 133). بنابراین در دنیای به‌شدت متصل امروز، ارتباطات به‌عنوان ستون فقرات شبکه‌های ارتباطی جهانی عمل می‌کند، تبادل داده و اطلاعات را به‌صورت بی‌وقفه ممکن می‌سازد (Ezeigweneme et al., 2023, p 1716) و از بخش‌هایی مانند بهداشت و درمان، مالی، حمل‌ونقل و عملیات‌های دولتی پشتیبانی می‌کند. زیرساختی‌هایی که پشت این شرکت‌های ارتباطی مدرن قرار دارند، از شرکت‌های ماهواره‌ای و ارائه‌دهندگان اینترنت گرفته تا شرکت‌های تلفن، این امکان را فراهم می‌نمایند که تمام ویدئوها، صداها و متن‌ها در سرتاسر جهان ارسال شوند (Sadiku et al., 2024, p 493).

با این‌حال در دنیای امروز، مواجهه هوش مصنوعی و امنیت سایبری[۲] در بخش ارتباطات، مرز حیاتی جدیدی را در حفاظت از زیرساخت‌های حیاتی و تضمین یکپارچگی شبکه‌های ارتباطی جهانی نشان می‌دهد

۱. همه‌گیری ویروس کووید-۱۹.

* نویسنده عهده‌دار مکاتبات: s.azizi@basu.ac.ir

1. Cybersecurity
امنیت ویژگی حیاتی شبکه‌های هوشمند است. این ویژگی نشان‌دهنده میزان حفاظتی است که شبکه در برابر خطرات احتمالی از دست دادن یا آسیب فراهم می‌کند. لذا مسائل امنیتی زمانی مطرح می‌شود که شبکه‌های هوشمند به هدف تهدیدات سایبری تبدیل می‌شوند. با گسترش سریع اینترنت اشیاء، احتمال حملات مخرب به شبکه‌های هوشمند درحال افزایش است و نقض امنیت در شبکه هوشمند می‌تواند برای قابلیت اعتماد آن فاجعه‌بار باشد (Sadiku et al., 2016, p 5574). اما به‌طورکلی امنیت سایبری به مجموعه اقداماتی که برای محافظت از سیستم‌های اطلاعاتی در برابر دسترسی یا حمله غیرمجاز مربوط می‌شود، تعریف می‌گردد.

(Kaur et al., 2023, p 24)؛ چراکه این پیوستگی، زیرساخت‌های ارتباطات را درمعرض طیف گسترده‌ای از تهدیدات سایبری، از جمله نقض داده‌ها و اختلالات شبکه، قرار می‌دهد که می‌تواند پیامدهای گسترده‌ای به همراه داشته باشد (Shoetan et al., 2024, p 595). برای‌نمونه در سال ۲۰۱۰، یک شرکت ارتباطی چینی اطلاعات مسیریابی نادرست برای ۳۷ هزار شبکه رایانه‌ای ارسال کرد که باعث هدایت نادرست ترافیک اینترنت از طریق چین شد. این اقدام موجب افشای داده‌های مربوط به ۸ هزار شبکه آمریکایی، ۱۱۰۰ شبکه استرالیایی و ۲۳۰ شبکه فرانسوی گردید (Stockburger, 2016, p 560) و یا در ماه مه ۲۰۱۷، سیستم‌های داخلی شرکت ارتباطی اسپانیایی تلفونیکا[1] هدف یک حمله باج‌افزاری قرار گرفتند. مهاجمان با استفاده از نسخه‌ای از باج‌افزار[2] WannaCry، فایل‌های موجود در سیستم‌های تلفونیکا را رمزگذاری کرده و سپس برای باز کردن این فایل‌ها درخواست پرداخت پول کردند (Manukonda, 2019, p 117). هم‌چنین تأثیر اقتصادی تهدیدات سایبری یکی دیگر از معیارهای مهم برای سنجش اثربخشی اقدامات امنیت سایبری است. براساس مطالعه‌ای که توسط Herjavec در سال ۲۰۱۹ انجام شده است، هزینه‌های جرایم سایبری پیش‌بینی شده بود که به‌طور قابل‌توجهی از ۳ تریلیون دلار آمریکا در سال ۲۰۱۵ به ۱۰٫۵ تریلیون دلار آمریکا سالانه تا سال ۲۰۲۵ افزایش یابد (Twain et al., 2023, p 2). ازاین‌رو تقویت امنیت سایبری در صنعت ارتباطات بیش از هر زمان دیگری ضروری به نظر می‌رسد[3].

با وجوداین، خلأ اسناد معاهداتی و حقوق بین‌المللی عرفی در عرصه‌ی فضای سایبر بسیار مشهود است[4]. به استثنای کنوانسیون سال ۲۰۰۱ بوداپست موضوع جرایم سایبری که در چارچوب «شورای اروپا[5]» منعقد گردید[6]؛ و پروتکل الحاقی به آن[7] که صرفاً به جرایم افراد مربوط می‌شود، سند بین‌المللی مهم دیگری در حوزه‌ی عملیات سایبری موجود نیست و شاید تنها بتوان به راهنماهای تالین اشاره کرد که در سال ۲۰۱۳[8] و ۲۰۱۷[9] توسط جمعی از کارشناسان بین‌المللی در چارچوب سازمان ناتو تهیه گردیده‌اند (بیگلربیگی، ۱۴۰۲، ص ۲). از این‌رو در خلأ هنجاری و رویه واحد دولتی، راهنمای تالین ۲ به‌عنوان معتبرترین و پراستنادترین اثر در زمینه حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری، بررسی دقیقی از نحوه اعمال قواعد و مقررات بین‌المللی موجود[10] در تطابق با حوزه پیچیده و درحال تحول فضای سایبر ارائه می‌کند و می‌تواند به‌خوبی دیدگاه کارشناسان و اندیشمندان حقوقی و فنی آشنا با مسائل سایبری در مورد نحوه رفتار دولت‌ها که دست به ارتکاب عملیات سایبری می‌زنند، مبرهن نماید.

این راهنما در یازدهمین فصل خود، در قالب چهار قاعده، نکات و ملاحظاتی پیرامون حقوق بین‌الملل ارتباطات بیان می‌نماید. لذا در این نوشتار بر آن بوده‌ایم که در پرتو قواعد و شرح راهنمای تالین ۲، شرایط و الزامات حقوق بین‌الملل ارتباطات را بررسی نماییم. البته کارشناسان راهنمای تالین ۲ نتیجه‌گیری نکردند که قواعد مطرح‌شده در این فصل (فصل یازدهم) راهنمای تالین ۲ لزوماً منعکس‌کننده حقوق بین‌الملل عرفی هستند، با این‌حال تأکید داشتند که تقریباً تمامی دولت‌ها عضو نظام معاهده‌ای اتحادیه بین‌المللی ارتباطات[11]، نهاد تخصصی سازمان ملل متحد در حوزه تنظیم مقررات ارتباطات بین‌المللی، هستند. از این‌رو کارشناسان توافق داشتند که

1. Telefónica
2. Ransomware

۳. در این راستا نگرانی‌ها و درخواست‌هایی در توافق‌نامه‌های بین‌المللی مانند قطعنامه ۱۳۰ اتحادیه بین‌المللی ارتباطات وجود دارد که تهدیدات و روندهای مختلف را بیان کرده و به نیاز به تقویت بیشتر همکاری‌های بین‌المللی و توسعه سازکارهای ملی، منطقه‌ای و بین‌المللی موجود (مانند توافق‌نامه‌ها، یادداشت‌های تفاهم و غیره) اشاره می‌کند. درخواست‌های همکاری و اقدام هم‌چنین در قطعنامه‌های ۴۰ و ۵۲ مجمع جهانی استانداردسازی ارتباطات (WTSA) اتحادیه بین‌المللی ارتباطات نیز دیده می‌شود (Hill, 2015, p 4).

۴. البته باید خاطرنشان نمود که فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقدام به عملیات سایبری نمایند و هرچند حقوق عرفی و معاهداتی موجود به‌صراحت درخصوص عملیات سایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیه اروپا و دولت‌های متعدد؛ از جمله ایالات متحد آمریکا، ایران، بریتانیا، روسیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالی این نظریه را پذیرفته‌اند (Roscini, 2014, p 19-22).

5. The Council of Europe

6. Convention on Cybercrime (Budapest Convention), Council of Europe, 23 November 2001, European Treaty Series – No. 185., Entered into Force .on 1 July 2004.

۷. این پروتکل درخصوص « لزوم جرم انگاری اقدام‌های نژادپرستانه و بیگانه هراسی که با استفاده از رایانه ارتکاب می‌یابند» است.
Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Sys. tem, 2003.

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

۹. راهنمای تالین در حقوق بین‌الملل قابل اعمال در نبردهای سایبری متعلق به بازهٔ زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در کشور استونی است که توسط مایکل اشمیت در مورد مقررات حاکم بر اقدام‌ها و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبرد ناتو در ولز بریتانی، در قالب اصل چهار پیمان ناتو، تهیه شده است. به‌رغم پیوند راهنمای تالین ۲ با ناتو، در مقدمه این راهنما تصریح شده است که قواعد بیان شده در این راهنما، دیدگاه کشورهای متبوع کارشناسان تدوین‌کننده، ناتو یا مرکز عالی پدافند مشترک سایبری ناتو (CCDCOE) نیست؛ بلکه تنها محصول مطالعه مستقل کارشناسان و متخصصان تدوین‌کننده می‌باشد.

۱۰. راهنمای تالین ۲ بازتاب‌دهنده قواعد و مقرراتی است که در زمان تدوین این راهنما وجود داشته (Lex lata)؛ نه این‌که قواعد و مقررات جدیدی به گسترده حقوق بین‌الملل بی‌افزاید و از اظهاراتی که منعکس‌کننده آن‌چه که باید باشد (Lex ferenda)، اجتناب می‌کند (Wallace & Visger, 2018, p 19).

11. International Telecommunication Union (ITU).

گنجاندن قواعد مبتنی بر معاهدات مرتبط با حوزه سایبری در این راهنما مفید خواهد بود (Tallinn Manual 2.0, 2017, p 284).

منابع معاهده‌ای حقوق بین‌الملل ارتباطات عمدتاً شامل اسناد اتحادیه بین‌المللی ارتباطات می‌شود که عبارت از اساسنامه؛ کنوانسیون؛ و دو مقررات اداری آن: مقررات رادیویی و مقررات بین‌المللی ارتباطات[۱]، می‌باشد. تحت این نظام، اتحادیه بین‌المللی ارتباطات تنها سازمان بین‌دولتی است که وظایف تخصیص جهانی باندهای فرکانسی در طیف الکترومغناطیسی برای خدمات مختلف ارتباطات بی‌سیم مانند تلفن همراه، ناوبری جی‌پی‌اس[۲] و پخش ماهواره‌ای؛ هماهنگی و ثبت تخصیص فرکانس‌ها توسط دولت‌ها در ارتباط با استفاده از این تخصیص‌ها[۳]؛ و درصورت لزوم، ثبت موقعیت‌های مداری ماهواره‌ها، چه مورد استفاده قرار گرفته باشند و چه برای استفاده آینده برنامه‌ریزی شده باشند، را انجام می‌دهد[۴]. اتحادیه بین‌المللی ارتباطات هم‌چنین استانداردسازی بین‌المللی فعالیت‌های ارتباطی را تسهیل می‌کند[۵]. قواعد دیگری که برخی از ارتباطات بین‌المللی از طریق ابزارهای سایبری را تنظیم می‌کنند، در حقوق دریاها یافت می‌شوند. از جمله این قواعد می‌توان به موارد مرتبط با کابل‌های ارتباطی زیردریایی[۶] و پخش غیرمجاز در آب‌های آزاد[۷] اشاره کرد. به همین‌ترتیب، حقوق فضا جنبه‌های خاصی از ارتباطات بین‌المللی؛ مانند تعهد به بهره‌برداری از ماهواره‌های ارتباطی با رعایت فعالیت‌های سایر دولت‌ها در فضای ماورای جو[۸]، الزام دولت‌ها به صدور مجوز و نظارت بر فعالیت‌های نهادهای غیردولتی در فضای ماورای جو[۹]، همانند مورد یک شرکت خصوصی که ماهواره ارتباطی را پرتاب و بهره‌برداری می‌کند؛ و تعیین مسئولیت جبران خسارت ناشی از ماهواره‌های ارتباطی[۱۰]، را تحت پوشش قرار می‌دهد. هم‌چنین دولت‌ها می‌توانند برای خدمات ارتباطی بین‌المللی، از جمله خدمات ارتباطات سایبری بین‌المللی، توافق‌های خاصی را منعقد کنند. وجود نظام‌های ویژه، که در مواد ۴۲ و ۴۳ اساسنامه اتحادیه بین‌المللی ارتباطات پیش‌بینی شده است، دولت‌های عضو را از تعهدات خود در قبال سایر دولت‌ها تحت اسناد اتحادیه بین‌المللی ارتباطات، مانند تعهد به خودداری از ایجاد تداخل مضر در خدمات ارتباطی دیگر کشورها[۱۱]، معاف نمی‌کند (Tallinn Manual 2.0, 2017, p 286).

با این‌حال، حقوق بین‌الملل ارتباطات چنان‌که اشاره شد، به‌طور گسترده بر اساسنامه اتحادیه بین‌المللی ارتباطات و اسناد آن تکیه دارد؛ لذا در تدوین این مقاله نیز به آن ها تکیه شده است. درنهایت، این نوشتار در قالب دو گفتار تدوین شده است؛ درگفتار نخست ابتدا به تعاریف و مفاهیم کلی در حوزه سایبر و حقوق بین‌الملل ارتباطات می‌پردازیم و سپس در گفتار دوم، حقوق بین‌الملل ارتباطات را در پرتو راهنمای تالین ۲ مورد بررسی و مداقه قرار می‌دهیم.

۲- تعاریف و مفاهیم کلی

نظر به این‌که برای بررسی حقوق بین‌الملل ارتباطات در پرتو راهنمای تالین ۲ لازم است در ابتدا نسبت به این مفاهیم شناختی وجود داشته باشد، در این گفتار به‌صورت اجمالی به بررسی کلیاتی درخصوص این مفاهیم خواهیم پرداخت.

۲- ۱- سایبر و فضای سایبر

مفهوم «سایبر» و بالتَّبع شکل‌گیری فضای سایبر به گذشته‌های بسیار دور باز نمی‌گردد. شکل‌گیری فضای سایبر را شاید بتوان به دهه ۱۹۶۰ میلادی نسبت داد؛ زمانی که طی یک پروژه تحقیقاتی در ایالات متحد آمریکا، نخستین شبکه آزمایشی ارتباطات کامپیوتری با هدف اتصال رایانه‌ها از طریق خطوط تلفن راه‌اندازی شد (Naughton, 2016, p 7). با این‌حال، واژه سایبر از لغت یونانی (کی‌برنتز[۱۲]) به معنی سکان‌دار یا راهنما مشتق

---

۱. ماده ۴ اساسنامه اتحادیه بین‌المللی ارتباطات.
شایان اشاره است، اساسنامه و کنوانسیون اتحادیه بین‌المللی ارتباطات در اجلاس تکمیلی سران مختار کشورهای عضو سال ۱۹۹۲ در ژنو تصویب شد و در اجلاس‌های سران مختار بعدی، شامل کیوتو در ۱۹۹۴، مینیاپولیس در ۱۹۹۸، مراکش در ۲۰۰۲، آنتالیا در ۲۰۰۶، گوادالاخارا در ۲۰۱۰ و بوسان در ۲۰۱۴ اصلاح گردید. مقررات رادیویی اتحادیه بین‌المللی ارتباطات در سال ۱۹۹۵ تصویب و در چندین نوبت مورد بازبینی و تصویب مجدد قرار گرفت که آخرین بار در ژنو در سال ۲۰۱۵ انجام شد. بیشتر اصلاحات سال ۲۰۱۵ از تاریخ ۱ ژانویه ۲۰۱۷ لازم‌الاجرا شدند. درحال‌حاضر، دو مقررات بین‌المللی ارتباطی لازم‌الاجرا وجود دارد: مقررات سال ۱۹۸۸ و مقررات سال ۲۰۱۲. دولت‌هایی که عضو معاهده ۲۰۱۲ نیستند، هم‌چنان ملزم به رعایت مقررات بین‌المللی ارتباطات ۱۹۸۸ هستند؛ هم‌چنین دولت‌هایی که عضو معاهده ۲۰۱۲ هستند، نسبت به دولت‌های غیرعضو آن، هم‌چنان براساس مقررات ۱۹۸۸ عمل می‌کنند.

2. GPS.

۳. در این زمینه به قاعده ۶۳ راهنمای تالین ۲ نیز مراجعه کنید.
۴. ماده ۱ (۲) (الف – ب) اساسنامه اتحادیه بین‌المللی ارتباطات.
۵. کارشناسان راهنمای تالین ۲ اشاره کردند که علاوه بر اتحادیه بین‌المللی ارتباطات، نهادهای دیگری نیز در مسائل مربوط به ارتباطات سایبری بین‌المللی نقش سازمانی و سیاست‌گذاری دارند. از جمله این نهادها می‌توان به سازمان تخصیص شماره‌های اینترنتی (IANA) و گروه مهندسی اینترنت (IETF) اشاره نمود (Tallinn Manual 2.0, 2017, p 286).
۶. قاعده ۵۴ راهنمای تالین ۲.
۷. قاعده ۴۶ راهنمای تالین ۲.
۸. بند (ب) قاعده ۵۹ راهنمای تالین ۲.
۹. بند (الف) قاعده ۶۰ راهنمای تالین ۲.
۱۰. بند (ب) قاعده ۶۰ راهنمای تالین ۲.
۱۱. قاعده ۶۳ راهنمای تالین ۲.

12. Kybernetes.

شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شده است. هم‌چنین از این واژه به‌معنا و مفهوم مطالعه پیام‌ها، به‌ویژه بررسی کنترل مؤثر در قلمرو فیزیولوژیک و مهندسی یاد می‌شود. اما به‌طورکلی، فضای سایبر در اصل یک فضا و محیطی مشابه سایر حوزه‌های رقابتی هم‌چون دریا، زمین و هوا است با یک تفاوت و آن هم این که این محیط برخلاف بقیه محیط‌ها ساخته دست بشر بوده، غیرملموس است (Libickim, 2009, p 11) و به‌طورکلی فضای سایبر منبعی برای تبادل اطلاعات تلقی می‌شود.

۲- ۲- عملیات و فعالیت سایبری

اصطلاحات «عملیات سایبری[1]» و «فعالیت سایبری[2]» مفاهیم عامی هستند و بسته به سیاق متن ممکن است معانی متفاوتی داشته باشند، ولی در این نوشتار به‌جای یکدیگر به‌کار رفته‌اند. چنان‌چه بخواهیم تعریفی یکپارچه از این دو اصطلاح ارائه دهیم، می‌توان گفت انواع مختلفی از فعالیت‌ها هستند که از فضای سایبر با هدف تأثیرگذاری بر اطلاعاتی که در قلمرو سایبری جریان دارند، استفاده می‌شوند[3]. برای‌نمونه می‌توان به حملات سایبری اشاره نمود. البته در مورد تعریف حملات سایبری هیچ‌گونه اتفاق نظری وجود ندارد و این موضوع هم‌چنان بین دولت‌ها و سازمان‌های بین‌المللی مورد اختلاف است (اصلانی، رنجبریان، ۱۳۹۴، ص ۲۷۵). با وجوداین تعریف‌هایی از آن صورت گرفته است، برای‌نمونه، در قاعده ۹۲ راهنمای تالین ۲ بدین‌گونه تعریف شده است: «حمله سایبری، عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول انتظار مرگ یا صدمه به اشخاص و یا وارد کردن خسارت به اشیا می‌رود» (Tallinn Manual 2.0, 2017, p 415).

۲- ۳- ارتباطات[4] و خدمات ارتباطی بین‌المللی[5]

«ارتباطات» به «هرگونه انتقال، ارسال یا دریافت علائم، سیگنال‌ها، نوشته‌ها، تصاویر، اصوات یا اطلاعات از هر نوع، از طریق سیستم‌های سیمی، رادیویی، نوری یا سایر سیستم‌های الکترومغناطیسی»، تعریف می‌شود[6]. در این‌راستا، کارشناسان راهنمای تالین ۲ توافق داشتند که به‌دلیل خنثی بودن نظام حقوقی اتحادیه بین‌المللی ارتباطات نسبت به فناوری، پیشرفت‌های تکنولوژیکی جدید که امکان انتقال داده‌ها از طریق رسانه‌های دیگر مانند پرتوهای گاما، اشعه ایکس[7]، یا مسیرهای فیزیکی که درحال‌حاضر به‌طور گسترده در ارتباطات استفاده نمی‌شوند، به احتمال زیاد در چارچوب این تعریف قرار می‌گیرند (Tallinn Manual 2.0, 2017, p 284). البته باید اشاره داشت، حقوق مطرح‌شده در این مقاله به ارتباطات «بین‌المللی» مربوط می‌شود. در راهنمای تالین ۲، اصطلاح «ارتباطات بین‌المللی[8]» شامل آن دسته از ارتباطاتی است که مستلزم انتقال داده‌ها از مرزهای دولتی است، هم‌چنین ارتباطاتی که از، یا، به مناطق فراسرزمینی مانند آب‌های بین‌المللی، حریم هوایی بین‌المللی و فضای ماورای جو منتقل می‌شوند (Tallinn Manual 2.0, 2017, p 285).

از این‌رو «خدمات ارتباطی بین‌المللی»، به‌عنوان «ارائه قابلیت ارتباطی بین دفاتر یا ایستگاه‌های ارتباطی از هر نوع که در کشورهای مختلف قرار دارند یا به آن ها تعلق دارند» تعریف می‌شود[9]. در زمینه سایبر، اصلی‌ترین خدمات ارتباطی بین‌المللی، ارائه اتصال به اینترنت است، چه از طریق ارائه‌دهندگان خدمات اینترنتی[10] و چه از طریق شرکت‌های ارتباطی دیگر مانند آن هایی که اتصال داده تلفن همراه (برای مثال، خدمات 4G) ارائه می‌دهند. به‌عنوان نمونه، سیستم‌های ناوبری ماهواره‌ای جی‌پی‌اس یا گلوناس[11] نیز به‌عنوان خدمات ارتباطی بین‌المللی شناخته می‌شوند که در زمینه سایبر اهمیت دارند. این اصطلاح هم‌چنین شامل خدماتی می‌شود که درحال توسعه، مانند دسترسی به اینترنت از هواپیماها، کشتی‌های هوایی، یا بالون‌ها، هستند (Tallinn Manual 2.0, 2017, p 285). لذا از منظر این مقاله، خدمات ارتباطی بین‌المللی در زمینه سایبر، به‌عنوان «خدمات ارتباطات سایبری بین‌المللی[12]» شناخته خواهند شد.

۳- مداقه حقوق بین‌الملل ارتباطات در چارچوب راهنمای تالین ۲

چنان‌که اشاره شد، حقوق بین‌الملل ارتباطات، عمدتاً به ارائه خدمات

1. Cyber Operations.
2. Cyber Activities.
3. Tallinn Manual 2.0, *op.cit.*, p. 564.
4. Telecommunication.
5. International Telecommunication Service.

۶. ضمیمه شماره ۱۰۱۲ اساسنامه اتحادیه بین‌المللی ارتباطات؛ ماده ۱,۳ مقررات رادیویی اتحادیه بین‌المللی ارتباطات؛ ماده ۲ مقررات ارتباطات بین‌المللی ۱۹۸۸ اتحادیه بین‌المللی ارتباطات؛ ماده ۲ (۱) مقررات ارتباطات بین‌المللی ۲۰۱۲ اتحادیه بین‌المللی ارتباطات.

۷. محدوده فعلی طیف الکترومغناطیسی مورد استفاده برای خدمات ارتباطی بین‌المللی ۳۰۰۰ گیگاهرتز و کمتر، بدون احتساب پرتوهای گاما و اشعه ایکس، است (ماده ۲,۱. مقررات رادیویی اتحادیه بین‌المللی ارتباطات).

8. International Telecommunications.

۹. ضمیمه شماره ۱۰۱۱ اساسنامه اتحادیه بین‌المللی ارتباطات؛ ماده ۲,۲ مقررات ارتباطات بین‌المللی ۱۹۸۸ اتحادیه بین‌المللی ارتباطات؛ ماده ۲ (۲) مقررات ارتباطات بین‌المللی ۲۰۱۲ اتحادیه بین‌المللی ارتباطات.

10. Internet service Providers (ISP).
11. GLONASS.

ارتباطات بین‌المللی و بهره‌برداری از زیرساخت‌های ارتباطی می‌پردازد. لذا می‌توان آن را به‌عنوان یک نظام تسهیل‌گر برای ارتباطات بین‌المللی، از جمله ارتباطاتی که از طریق ابزارهای سایبری انجام می‌شوند، توصیف کرد. این حوزه هم‌چنین به مسائل جانبی مانند تعهد دولت‌ها به حفاظت از زیرساخت‌های سایبری[1] می‌پردازد (Tallinn Manual 2.0, 2017, p 284). بنابراین، ارتباطات از طریق ابزارهای سایبری، یعنی ارتباطاتی که درحال‌حاضر عمدتاً بر بستر شبکه‌های مبتنی بر آی‌پی[2] انجام می‌شوند، نیز به‌عنوان ارتباطات تلقی می‌شوند؛ زیرا این ارتباطات از طریق سیم، طیف الکترومغناطیسی یا فیبر نوری منتقل می‌شوند. به‌عنوان مثال، اشتراک‌گذاری اطلاعات محرمانه از طریق ایمیل امن، یک نوع ارتباط محسوب می‌شود. با این‌حال، اگر همان اطلاعات از طریق یک حافظه یواس‌بی[3] منتقل شود، به‌عنوان ارتباط تعریف نمی‌شود[4] (Tallinn Manual 2.0, 2017, p 284-285).

با وجوداین، گسترش فناوری‌های دیجیتال مانند 5G، اینترنت اشیا[5] و رایانش ابری[6] به‌طور قابل‌توجهی سطح حمله برای مجرمان سایبری را افزایش داده‌است. استفاده از این فناوری‌ها، درحالی‌که باعث بهبود اتصال و کارایی عملیاتی می‌شود، نقاط ضعف جدیدی را نیز معرفی می‌کند که می‌توانند توسط عوامل مخرب بهره‌برداری شوند. به‌عنوان مثال، دستگاه‌های اینترنت اشیا که اغلب دارای ویژگی‌های امنیتی محدود هستند، ممکن است به‌خطر بیفتند و به‌عنوان نقاط ورود برای انجام حملات گسترده‌تر به شبکه‌های ارتباطی مورد استفاده قرار گیرند. حمله بات‌نت[7] Mirai در سال ۲۰۱۶ که از دستگاه‌های اینترنت اشیا آسیب‌پذیر برای اجرای یک حمله بزرگ توزیع‌شده منع سرویس[8] استفاده کرد، نمونه‌ای از مقیاس و تأثیر بالقوه این نقاط ضعف است (Folorunsho et al., 2024, p 1861). لذا در ادامه این موضوع ذیل چهار بخش همانند راهنمای تالین ۲ مورد بررسی قرار می‌گیرد.

البته پیش از آن شایان اشاره است، کارشناسان راهنمای تالین ۲ به این نکته توجه داشت که نظام حقوقی اتحادیه بین‌المللی ارتباطات به ارتباطاتی که با ایمنی جان انسان‌ها و ارتباطات دولتی مرتبط هستند، اولویت می‌دهد[9]. با این‌حال، کارشناسان تصمیم گرفتند که موضوع اولویت‌بندی را در یک قاعده جداگانه در راهنمای تالین ۲ مطرح نکنند؛ زیرا توافق شد که در زمینه سایبر، چنین اولویت‌بندی از نظر عملی اهمیت چندانی ندارد و توسط رویه دولتی به‌طور گسترده حمایت نمی‌شود. با گسترش روزافزون خدمات ارتباطات سایبری بین‌المللی و افزایش پهنای باند موجود، نیاز به اولویت‌بندی انواع خاصی از ارتباطات سایبری بین‌المللی کاهش می‌یابد. با این‌حال، کارشناسان توافق داشتند که اگر شرایطی پیش آید که توانایی برقراری ارتباطات ایمنی جان یا دولتی به اولویت‌بندی آن ها بستگی داشته باشد، دولت‌ها باید به این ارتباطات اولویت دهند. به‌عنوان مثال، درصورت وقوع زلزله‌ای گسترده در منطقه مرزی، برای تضمین هماهنگی بدون مانع در امدادرسانی بین دولت‌های آسیب‌دیده، ممکن است دولت‌ها به‌منظور رعایت الزام اولویت‌بندی، اپراتورهای تلفن همراه و ارائه‌دهندگان خدمات اینترنتی را ملزم به محدود کردن ترافیک[10] مصرف‌کننده پهنای باند بالا، مانند انتقال فایل‌ها و پخش چندرسانه‌ای[11]، کنند (Tallinn Manual 2.0, 2017, p 287).

کارشناسان هم‌چنین به ماده ۳۷ اساسنامه اتحادیه بین‌المللی ارتباطات[12] که به محرمانگی ارتباطات می‌پردازد، توجه کردند[13]. کارشناسان ماده ۳۷ (۱) را به‌گونه‌ای تفسیر کردند که فرضیه‌ای به نفع محرمانگی مکاتبات بین‌المللی از طریق ابزارهای سایبری ایجاد می‌کند. با این‌حال، ماده ۳۷ (۲) به یک دولت اجازه می‌دهد درصورت مجاز بودن طبق حقوق داخلی یا بین‌المللی، چنین

---

۱. قاعده ۶۱ راهنمای تالین ۲.

2. IP.

3. USB.

۴. کارشناسان تأکید کردند که اگرچه داده‌ها تقریباً همیشه در سطح فنی درحال انتقال هستند، حتی زمانی که ذخیره شده‌اند، پردازش داده‌ها در یک واحد پردازش مرکزی (CPU) به‌معنای انتقال در چارچوب حقوق بین‌الملل ارتباطات محسوب نمی‌شود و بنابراین «مخابره» تلقی نمی‌گردد (Tallinn Manual 2.0, 2017, p 285).

5. Internet of Things (IoT).

6. Cloud Computing.

7. Botnet.

8. Distributed Denial-of-Service (DDoS) Attack.

۹. به ترتیب مواد ۴۰ و ۴۱ اساسنامه اتحادیه بین‌المللی ارتباطات. هم‌چنین به ترتیب مواد ۵ (۱) و ۵ (۲) مقررات ارتباطات بین‌المللی ۱۹۸۸ اتحادیه بین‌المللی ارتباطات؛ و مواد ۵ (۱) و ۵ (۲) مقررات ارتباطات بین‌المللی ۲۰۱۲ اتحادیه بین‌المللی ارتباطات.

۱۰. یکی از راهکارهایی که برای شناسایی و مقابله با تهدیدات این حوزه بیان می‌شود، تجزیه و تحلیل ترافیک داده‌ها با استفاده از محدودکردن‌های شدید می‌باشد. برای مطالعه بیشتر به منبع زیر مراجعه نمایید؛

Privalov, A., Lukicheva, V., Kotenko, I., & Saenko, I. (2020). Increasing the Sensitivity of the Method of Early Detection of Cyber-Attacks in Telecommunication Networks Based on Traffic Analysis by Extreme Filtering, ***Energies***, 13 (11), 2774, p 1-18.

11. Multimedia Streaming.

۱۲. ماده ۳۷ (محرمانگی ارتباطات) مقرر می‌دارد: «۱. کشورهای عضو توافق می‌کنند که تمام تدابیر ممکن، سازگار با سیستم ارتباطی مورد استفاده، را به‌منظور تضمین محرمانگی مکاتبات بین‌المللی اتخاذ کنند؛ ۲. با این‌حال، آن ها حق دارند چنین مکاتباتی را برای اطمینان از اجرای قوانین ملی خود یا اجرای کنوانسیون‌های بین‌المللی که طرف آن هستند، به مقامات صلاحیت‌دار ارائه دهند».

۱۳. شبکه‌های ارتباطاتی، به‌عنوان شریان‌های اتصال جهانی، درمعرض طیف متنوعی از تهدیدات سایبری قرار دارند که خطرات قابل‌توجهی برای یکپارچگی، دسترس‌پذیری و محرمانگی آن ها به همراه دارد (Singh, Kapoor, 2023, p 2). در این‌راستا، برای نمونه، از آن‌جاکه وظیفه ارائه‌دهندگان خدمات ارتباطی حفاظت از محرمانگی مکالمات مشتریانشان است، برای این شرکت‌ها اطمینان از جمع‌آوری، پردازش و نگهداری داده‌ها مطابق با قوانین حفظ حریم خصوصی، مانند مقررات عمومی حفاظت از داده‌ها (GDPR)، یک دغدغه اساسی محسوب می‌شود (Manukonda, 2019, p 115).

مکاتباتی را به مقامات ملی یا بین‌المللی ارائه کند. از آن‌جاکه کارشناسان توافق داشتند که ماده ۳۷ (۲) مبنای گسترده‌ای برای دولت‌ها فراهم می‌کند تا محرمانگی مکاتبات بین‌المللی را نقض کنند، نتوانستند به نتیجه قطعی در مورد میزان تأثیر این ماده بر عملیات سایبری دولت‌ها دست یابند. درخصوص محرمانگی ارتباطات، کارشناسان تأکید کردند که دولت‌ها به‌ویژه باید قانونی بودن عملیات سایبری خود را در چارچوب حقوق بین‌المللی بشر برای حفظ حریم خصوصی[1] ارزیابی کنند (Tallinn Manual 2.0, 2017, p 287).

۳- ۱- وظیفه ایجاد، نگهداری و حفاظت از زیرساخت‌های بین‌المللی ارتباطات[2]

امنیت سایبری در صنعت ارتباطات ماهواره‌ای، با توجه به نقش حیاتی ماهواره‌ها در شبکه‌های ارتباطی جهانی، از اهمیت بالایی برخوردار است. شبکه‌های ارتباطات ماهواره‌ای در برابر تهدیدات سایبری مانند نفوذ به داده‌ها، دسترسی غیرمجاز به شبکه و حملات محروم‌سازی از سرویس[3] آسیب‌پذیر هستند. این تهدیدات می‌توانند باعث اختلال در خدمات و به‌خطر افتادن اطلاعات حساس شوند. لذا امنیت سایبری یکی از دغدغه‌های مهم در شبکه‌های ارتباطات ماهواره‌ای، با توجه به آسیب‌پذیری این شبکه‌ها در برابر تهدیدات سایبری، می‌باشد (Okafor et al., 2024, p 254-255). یکی از این حوادث، حمله سایبری سال ۲۰۱۸ به یک ارائه‌دهنده خدمات ارتباطات ماهواره‌ای بود که منجر به افشای اطلاعات حساس مشتریان شد. این حادثه بر لزوم اجرای تدابیر امنیت سایبری قوی توسط اپراتورهای ماهواره‌ای برای حفاظت از شبکه‌های خود در برابر تهدیدات سایبری تأکید کرد (Okafor et al., 2024, p 260).

در این سیاق، قاعده ۶۱ راهنمای تالین ۲ بیان می‌دارد: «یک دولت باید اقداماتی را برای تضمین ایجاد زیرساخت‌های بین‌المللی ارتباطات که برای ارتباطات سریع و بدون وقفه[4] بین‌المللی ضروری است، انجام دهد. درصورتی‌که دولت به‌منظور رعایت این الزام، زیرساخت سایبری برای ارتباطات بین‌المللی ایجاد کند، موظف است آن زیرساخت را نگهداری و از آن حفاظت کند»؛ چراکه دولت‌ها عموماً سیستم‌های متعددی مانند سیستم شناسایی نفوذ[5]، سیستم جلوگیری از نفوذ[6]، دیوارآتش[7] و دستگاه‌های شکل‌دهی بسته‌های داده[8] را برای محافظت از شبکه‌ها در دسترس دارند (Adel et al., 2021, p 8)[9] و هم‌چنین گزارش‌ها نشان می‌دهد نیمی از حملات سایبری کسب‌وکارهای کوچک را هدف قرار می‌دهند، کسب‌وکارهایی که معمولاً از امنیت سایبری کافی برای محافظت از خود در برابر چنین تهدیداتی برخوردار نیستند (Adel et al., 2021, p 13).

در تشریح این قاعده باید بیان داشت، این قاعده براساس ماده ۳۸ اساسنامه اتحادیه بین‌المللی ارتباطات تدوین شده و هدف آن، ارتقای دسترسی و کیفیت خدمات ارتباطات بین‌المللی است. مفاد مرتبط ماده ۳۸ به این شرح است: ۱) دولت‌های عضو باید اقداماتی را که برای ایجاد کانال‌ها و تأسیسات لازم جهت تبادل سریع و بدون وقفه ارتباطات بین‌المللی تحت بهترین شرایط فنی ضروری است، انجام دهند؛ ۲) تا حد امکان، این کانال‌ها و تأسیسات باید با استفاده از روش‌ها و رویه‌هایی که تجربه عملیاتی نشان داده بهترین هستند، اداره شوند. آن ها باید در شرایط عملیاتی مناسب نگهداری شده و با پیشرفت‌های علمی و فنی همگام شوند؛ ۳) دولت‌های عضو باید از این کانال‌ها و تأسیسات در قلمرو خود محافظت کنند؛ ۴) هر دولت عضو باید اقداماتی را که برای نگهداری بخش‌های تحت کنترل خود از مدارهای ارتباطی بین‌المللی ضروری است، انجام دهد[10]. براین‌اساس، قاعده۶۱ راهنمای تالین ۲، سه تعهد مشخص را برای دولت‌ها تعیین می‌کند: ایجاد زیرساخت‌هایی که ارتباطات بین‌المللی سریع و بدون وقفه را تسهیل کند؛ حفاظت از آن زیرساخت‌ها؛ و نگهداری آن ها.

کارشناسان راهنمای تالین ۲ در این‌راستا توافق داشتند که تعهدات یک دولت برای حفاظت و نگهداری از زیرساخت‌های ارتباطی بین‌المللی شامل زیرساخت‌هایی نمی‌شود که دیگر برای انجام وظیفه دولت در زمینه ایجاد زیرساخت استفاده نمی‌شوند. هم‌چنین توافق داشتند که وظایف مقرر در این قاعده، تعهدات رفتاری و نه تعهدات به نتیجه هستند. تعهدات رفتاری عموماً ایجاب می‌کنند که دولت‌ها «تمام تلاش خود[11]» را از طریق روشی که انتخاب می‌کنند برای رعایت این تعهدات به‌کار گیرند. چنین

۱. قاعده ۳۵ راهنمای تالین ۲.

2. Duty to Establish, Maintain, and Safeguard International Telecommunication Infrastructure.

3. Denial-of-Service Attacks.

4. Rapid and Uninterrupted.

5. Intrusion Detection System (IDS).

6. Intrusion Prevention System (IPS).

7. Firewall.

8. Packet Shaping Devices.

۹. البته امروزه از روش‌های دیگری هم‌چون هکر اخلاقی (Ethical Hacking) نیز نام برده می‌شود. هکر اخلاقی، یک متخصص کامپیوتر و شبکه است که به‌طور نظام‌مند تلاش می‌کند که به یک سیستم کامپیوتری یا شبکه مخابراتی از طرف مالکان آن، برای پیدا کردن آسیب‌پذیری‌های امنیتی که یک هکر مخرب ممکن است بتواند از آن‌ها سوءاستفاده کند، نفوذ کند (Onyema, et. al., 2022, p 27).

۱۰. ماده ۳۸ اساسنامه اتحادیه بین‌المللی ارتباطات.

11. Best Efforts.

تعهداتی الزام نمی‌کنند که دولت‌ها حتماً در تلاش‌های خود موفق شوند[۱]. بنابراین، انجام این تعهدات مشروط‌به امکان‌پذیری در شرایط مربوط است؛ دولت‌ها ملزم به انجام وظایفی نیستند که برای آن ها غیرمنطقی باشد. در این زمینه، توانایی مالی و قابلیت فنی دولت مورد نظر به‌طور خاص اهمیت دارد (Tallinn Manual 2.0, 2017, p 288-289).

در این‌راستا، ماده ۳۸ (۱) اساسنامه اتحادیه بین‌المللی ارتباطات، تعهد کلی بر عهده دولت‌ها می‌گذارد تا از ایجاد «کانال‌ها و تأسیسات لازم برای تبادل سریع و بدون وقفه ارتباطات بین‌المللی» اطمینان حاصل کنند. کارشناسان راهنمای تالین ۲ توافق داشتند که دولت‌ها می‌توانند خود تصمیم بگیرند که آیا «کانال‌ها و تأسیسات» شامل زیرساخت‌های خاص ارتباطات سایبری بین‌المللی باشد یا نه. از آن‌جاکه این قاعده بیانگر تعهد رفتاری است، اگر دولتی انتخاب کند که این تعهد را با ایجاد ظرفیت ارتباط سایبری تحت بهترین شرایط فنی اجرا کند، تنها باید این کار را تا حد امکان‌پذیر و منطقی در شرایط مربوط انجام دهد. به‌عنوان مثال، اگر هزینه اتصال یک منطقه جغرافیایی دورافتاده به کابل فیبر نوری برای انتقال داده با سرعت بالا برای یک دولت بسیار بالا باشد، دولت می‌تواند بهترین جایگزین ممکن، مانند اتصال ماهواره‌ای کم‌هزینه‌تر، را فراهم کند. با این‌حال، تمامی کارشناسان توافق داشتند که این تعهد شامل فراهم‌سازی دستگاه‌های کاربری نهایی، مانند کامپیوترها و تلفن‌های هوشمند، نمی‌شود. به‌طورعملی، کارشناسان اشاره کردند که اطمینان از ایجاد زیرساخت سایبری که اتصال به اینترنت جهانی را فراهم می‌کند، روشی بسیار مؤثر برای تحقق تبادل سریع و بدون وقفه ارتباطات بین‌المللی است (Tallinn Manual 2.0, 2017, p 289).

هم‌چنین کارشناسان توافق داشتند که این قاعده، شامل زیرساخت‌های ارتباطی بین‌المللی است که هم توسط دولت‌ها و هم شرکت‌های خصوصی اداره می‌شود. بنابراین، برای اجرای تعهد ایجاد زیرساخت برای ارتباطات بین‌المللی «سریع و بدون وقفه»، دولت می‌تواند، به‌عنوان مثال، محیطی تجاری ایجاد کند که سرمایه‌گذاری شرکت‌های خصوصی در زمینه احداث کابل‌های ارتباطی و ایجاد سایر زیرساخت‌های سایبری که زیرساخت اینترنت را تشکیل می‌دهند، تشویق کند. تاجایی‌که شرکت‌های خصوصی در این حوزه فعالیت می‌کنند، دولت موظف است اطمینان حاصل کند که زیرساخت‌های سایبری که توسط آن ها اداره می‌شود نیز نگهداری و محافظت شوند (Tallinn Manual 2.0, 2017, p 289).

از سوی‌دیگر، کارشناسان راهنمای تالین ۲ توافق داشتند که تعهد به ایجاد زیرساخت‌های ارتباطات بین‌المللی ارتباط نزدیکی با ماده ۳۳ اساسنامه اتحادیه بین‌المللی ارتباطات دارد که حق عمومی برای استفاده از خدمات ارتباطات بین‌المللی را تعیین می‌کند (Tallinn Manual 2.0, 2017, p 289-290). به‌عبارت دیگر، اگر دولتی قابلیت ارتباطات بین‌المللی عمومی را فراهم کرده باشد، عموم مردم می‌توانند از حق استفاده از این خدمات برای ارتباطات بین‌المللی بهره‌مند شوند. حال زمانی که ارتباطات بین‌المللی از طریق ابزارهای سایبری انجام می‌شوند، ماده ۳۸ (۳) اساسنامه اتحادیه بین‌المللی ارتباطات دولت‌ها را موظف به «حفاظت[۲]» و مواد ۳۸ (۲) و (۴) آن‌ها را موظف به «نگهداری[۳]» از زیرساخت‌های سایبری مربوط می‌کند.

کارشناسان راهنمای تالین ۲ در این راستا اشاره کردند که وظیفه حفاظت شامل زیرساخت‌های سایبری، در قلمرو صلاحیتی دولت[۴] است[۵]، درحالی‌که تعهد به نگهداری محدود به زیرساخت‌هایی است که تحت کنترل دولت قرار دارند. اگرچه مفهوم کنترل در حقوق بین‌المللی ارتباطات تعریف نشده است، کارشناسان توافق کردند که حداقل به زیرساخت‌های سایبری که تحت کنترل انحصاری دولت است، مانند زیرساخت‌هایی که دولت مالک و بهره‌بردار آن است، اشاره دارد. برعکس، به‌طورکلی، تمام زیرساخت‌های سایبری موجود در قلمرو یک دولت تحت صلاحیت آن قرار دارند[۶] و بنابراین دولت می‌تواند از طریق تصویب قوانین و مقررات داخلی اطمینان حاصل کند که زیرساخت‌های سایبری متعلق به بخش خصوصی نیز تحت حفاظت قرار می‌گیرند. از این‌رو کارشناسان توافق کردند که وظایف حفاظت و نگهداری شامل نگهداری کلی عملیاتی و هم‌چنین تطابق با استانداردهای فنی است که اطمینان می‌دهد داده‌ها به‌طور قابل‌اعتماد و کارآمد منتقل می‌شوند. به‌عنوان مثال، یک دولت ممکن است شرایط فنی و عملیاتی را در مجوزهایی که به ارائه‌دهندگان خدمات ارتباطی صادر می‌کند، تعیین کند تا اطمینان حاصل شود که این اهداف محقق می‌شوند[۷] (Tallinn Manual 2.0, 2017, p 290).

---

۱. در این‌خصوص به بحث‌های صورت‌گرفته در قاعده ۷ راهنمای تالین ۲ درباره رعایت اصل مراقبت مقتضی و هم‌چنین به بیگلربیگی، پیشین، صص ۱۱۶ به بعد مراجعه کنید.

2. Safeguard.
3. Maintain.
4. State's Jurisdiction.

۵. قاعده ۸ راهنمای تالین ۲.
۶. قاعده ۹ راهنمای تالین ۲.
۷. در راهنمای تالین ۲ بیان شده است: «به مقدمه و بند ۲۰ دستورالعمل اتحادیه اروپا درخصوص حفظ حریم خصوصی و ارتباطات الکترونیکی توجه کنید، که از ارائه‌دهندگان خدمات ارتباطات الکترونیکی عمومی می‌خواهد تدابیر فنی و سازمانی مناسبی برای حفاظت از امنیت خدمات خود اتخاذ کنند؛ هم‌چنین به شرایطی که برای تمامی شبکه‌ها و ارائه‌دهندگان خدمات ارتباطی اعمال می‌شود: ماده ۳ (۱) (الف) نسخه تجمیعی شرایط عمومی دفتر ارتباطات (Ofcom General Conditions) (بریتانیا) (مه ۲۰۱۵) مراجعه کنید که ارائه‌دهندگان خدمات ارتباطی را ملزم می‌کند تمامی اقدامات لازم را برای حفظ عملکرد صحیح و مؤثر شبکه عمومی ارتباطات، تا حد ممکن، در تمامی زمان‌ها اتخاذ کنند».

کارشناسان راهنمای تالین ۲ هم‌چنین قانونی بودن ارائه خدمات ارتباطی توسط یک دولت در قلمرو دولت دیگر، در مواردی که چنین خدماتی وجود ندارد (مانند فراهم کردن دسترسی به اینترنت از طریق یک ماهواره ارتباطی یا از داخل یک هواپیما) بدون رضایت دولت اخیر را مورد بحث قرار دادند. کارشناسان تأکید کردند که هر مورد باید براساس ویژگی‌های خاص خود ارزیابی شود. به‌عنوان مثال، اگر هواپیما بدون مجوز در حریم هوایی ملی دولت دیگر پرواز کند، این اقدام به‌دلیل حضور بدون رضایت هواپیما در حریم هوایی آن دولت، غیرقانونی خواهد بود[۱]. با وجوداین، در مورد ارائه خدمات ارتباطی به خودی خود، اقلیتی از کارشناسان معتقد بودند که این اقدام قانونی است؛ زیرا هیچ قاعده‌ای علیه چنین فعالیتی به‌عنوان حقوق بین‌الملل عرفی تثبیت نشده است. با این‌حال، اکثریت کارشناسان بر این باور بودند که ارائه خدمات ارتباطی توسط یک دولت در قلمرو دولت دیگر بدون رضایت آن دولت غیرمجاز است؛ زیرا هر دولتی حق حاکمیتی دارد تا بخش ارتباطات خود را تنظیم کند، از جمله تعیین این‌که چه کسی خدمات ارائه دهد و چگونه این خدمات انجام شود[۲] (Tallinn Manual 2.0, 2017, p 290-291).

۳- ۲- تعلیق یا توقف ارتباطات سایبری[۳]

تا جایی‌که یک دولت بر زیرساخت‌ها و فعالیت‌های سایبری در قلمرو خود کنترل اعمال می‌کند، این کار را براساس اصل حاکمیت[۴] انجام می‌دهد. حق حاکمیتی دولت‌ها برای تنظیم ارتباطات آن ها، در دیباچه اساسنامه اتحادیه بین‌المللی ارتباطات نیز پیش‌بینی شده است. لذا طبق این قاعده، به‌رسمیت شناخته می‌شود که دولت‌ها در اعمال این حق حاکمیتی ممکن است گاهی خدمات ارتباطی سایبری بین‌المللی را تعلیق کنند یا انتقال ارتباطات سایبری را متوقف سازند. البته این حق بدون لطمه به تعهدات حقوق بین‌الملل است که ممکن است در موارد خاص دولت را از چنین اقداماتی منع کند.

در این‌راستا، قاعده ۶۲ راهنمای تالین ۲ بیان می‌دارد: «الف) یک دولت می‌تواند خدمات ارتباطی سایبری بین‌المللی را به‌طور کامل یا جزئی در قلمرو خود تعلیق کند. در این‌صورت، باید فوراً سایر دولت‌ها را از این تعلیق مطلع سازد؛ ب) یک دولت می‌تواند انتقال یک ارتباط سایبری خصوصی را که به‌نظر می‌رسد برخلاف قوانین ملی، نظم یا اخلاق عمومی آن باشد، یا برای امنیت ملی خطرناک است، متوقف کند». در توضیح باید بیان داشت، بندهای (الف) و (ب) قاعده ۶۲ راهنمای تالین ۲، بر مواد ۳۵[۵] و ۳۴ (۲)[۶] اساسنامه اتحادیه بین‌المللی ارتباطات استوار هستند که شرایط وقفه در جریان ارتباطات از سوی یک دولت را به‌عنوان استثنایی بر اصولی که تداوم ارتباطات را تضمین می‌کنند، مشخص می‌کنند[۷].

براساس این مواد، کارشناسان راهنمای تالین ۲ دو دسته از شرایط را شناسایی کردند که در آن ها تعلیق یا توقف ارتباطات قانونی است. در این ارتباط، بند (الف) اجازه تعلیق کامل یا جزئی[۸] خدمات ارتباطی بین‌المللی، از جمله خدمات ارتباطی سایبری بین‌المللی مانند ارتباطات اینترنتی، را می‌دهد[۹]. کارشناسان توافق کردند که این حق، شامل تعلیق ارتباطات ورودی، خروجی و حتی ارتباطاتی است که از قلمرو یک دولت عبور می‌کند. این حق هم‌چنین به ارتباطاتی که در کشتی‌ها یا هواپیماها[۱۰] انجام می‌شود یا از طریق ماهواره‌ها[۱۱] انتقال می‌یابد و دولت بر آن ها صلاحیت و کنترل اعمال می‌کند، تسری دارد. کارشناسان هم‌چنین اشاره کردند که دولت‌ها ممکن است براساس معاهدات یا قواعد عرفی، محدودیت‌هایی برای اعمال این حق داشته باشند[۱۲]. اختیار یک دولت برای تعلیق خدمات ارتباطی سایبری بین‌المللی با مثال انسداد ارتباطات اینترنتی و تلفن همراه بین‌المللی توسط دولت مصر در سال ۲۰۱۱ به‌دلیل ناآرامی‌های مدنی نشان داده شده است. در پی اعتراضات مردمی که از شبکه‌های اجتماعی مانند توییتر و فیس‌بوک استفاده می‌کردند، مصر به تصمیم دولت، این دسترسی‌ها را در سراسر کشور

---

۱. برای مطالعه بیشتر به قاعده ۵۵ راهنمای تالین ۲ مراجعه نمایید.

۲. مقدمه اساسنامه اتحادیه بین‌المللی ارتباطات. هم‌چنین درخصوص بازگردانی خدمات ارتباطی سایبری بین‌المللی توسط یک دولت که دولت دیگر آن را متوقف کرده است، به قاعده ۶۲ راهنمای تالین ۲ (در ادامه مقاله بحث می‌شود)؛ و درباره تعهد دولت‌ها به تصویب قوانین داخلی درخصوص خسارت به کابل‌های ارتباطی زیردریایی، به قاعده ۵۴ راهنمای تالین ۲ مراجعه کنید.

3. Suspension or Stoppage of Cyber Communications.

۴. برای مطالعه بیشتر در این خصوص به قاعده ۲ راهنمای تالین ۲ مراجعه کنید.

۵. ماده ۳۵ اساسنامه اتحادیه که درخصوص «تعلیق خدمات» می‌باشد، بیان می‌دارد: «هر دولت عضو حق دارد خدمات ارتباطی بین‌المللی را، به‌طورکلی یا فقط برای برخی ارتباطات و/یا برخی انواع مکاتبات (اعم از خروجی، ورودی یا عبوری)، تعلیق کند، مشروط‌بر این‌که فوراً چنین اقدامی را از طریق دبیرکل به سایر دولت‌های عضو اطلاع دهد».

۶. ماده ۳۴ درخصوص «توقف ارتباطات» بیان می‌دارد: «(۲) دولت‌های عضو ... حق دارند مطابق با قوانین ملی خود، هرگونه ارتباطات خصوصی را که ممکن است برای امنیت دولت خطرناک باشد یا برخلاف قوانین، نظم یا اخلاق عمومی باشد، قطع کنند».

۷. برای‌نمونه، به قاعده ۶۱ راهنمای تالین ۲ که پیش از این مورد بحث قرار گرفت، مراجعه کنید.

۸. تعلیق به‌معنای قطع موقت خدمات است. این امر هم‌چنین در ماده ۷ (۱) مقررات ارتباطات بین‌المللی ۱۹۸۸ اتحادیه بین‌المللی ارتباطات و ماده ۷ (۱) مقررات ارتباطات بین‌المللی ۲۰۱۲ اتحادیه بین‌المللی ارتباطات با اشاره به «تعلیق و ... بازگشت بعدی به شرایط عادی»، منعکس گردیده است.

۹. اگر یک دولت خدمات ارتباطی سایبری بین‌المللی را تعلیق کند، باید فوراً سایر دولت‌های عضو اتحادیه بین‌المللی ارتباطات را از این تعلیق و بازگشت خدمات از طریق دبیرکل این سازمان مطلع کند (ماده ۳۵ اساسنانه اتحادیه بین‌المللی ارتباطات؛ ماده ۷ مقررات ارتباطات بین‌المللی ۱۹۸۸ اتحادیه بین‌المللی ارتباطات؛ و ماده ۷ مقررات ارتباطات بین‌المللی ۲۰۱۲ اتحادیه بین‌المللی ارتباطات).

۱۰. مطابق قاعده ۱۰ راهنمای تالین ۲.

۱۱. طبق بند (الف) قاعده ۵۹ راهنمای تالین ۲.

۱۲. برای محدودیت‌های احتمالی درخصوص چنین تعلیق‌هایی برای دولت‌های عضو، به ماده ۵ ضمیمه ارتباطات راه دور توافقنامه عمومی تجارت خدمات (GATS) مراجعه کنید.

تعلیق کرد (Arthur, 2011). اگرچه مصر به الزام اطلاع‌رسانی به سایر دولت‌ها عمل نکرد، کارشناسان توافق داشتند که این اقدام در چارچوب حقوق بین‌الملل ارتباطات مشروع بود. البته این نتیجه‌گیری بدون پیش‌داوری نسبت به این پرسش است که آیا اقدام مصر با سایر قواعد حقوق بین‌الملل، مانند احترام به حقوق بین‌المللی بشر درخصوص آزادی بیان[۱] سازگار بوده است یا نه (Tallinn Manual 2.0, 2017, p 292-293).

علاوه بر این، کارشناسان به موانع عملی در اجرای تصمیم یک دولت برای تعلیق خدمات ارتباطی سایبری بین‌المللی توجه کردند. در مثال مصر، دسترسی به خدمات طی چند ساعت پس از قطع سراسری توسط دولت، با کمک شرکت‌هایی مانند گوگل و توییتر که راه‌حل‌های فناوری جایگزین مانند پیام صوتی و اتصالات آنالوگ ارائه دادند، به‌طور جزئی بازگردانده شد. با این‌حال، این مشکلات عملی موجب بی‌اعتبار شدن صلاحیت قانونی برای تعلیق نمی‌شوند. کارشناسان توافق کردند که بند (الف) تنها به اختیار دولت برای تعلیق خدمات ارتباطی سایبری بین‌المللی مربوط می‌شود. درخصوص قانونی بودن فعالیت‌های یک دولت دیگر برای بازگرداندن از راه دور خدمات ارتباطی در کشوری که خدمات را تعلیق کرده است، برای مثال، بازگرداندن دسترسی به اینترنت از طریق یک هواپیمای ارتفاع‌بالا، اختلاف‌نظر وجود داشت. اکثریت کارشناسان بر این نظر بودند که دولت‌ها باید حق حاکمیت دیگر دولت‌ها برای تنظیم ارتباطات، از جمله از طریق تعلیق، را رعایت کنند. بنابراین، اقداماتی که برای دور زدن تعلیق طراحی شده‌اند، مانند غصب یک وظیفه ذاتی دولتی، غیرقانونی خواهند بود[۲]. از سوی‌دیگر اقلیت کارشناسان بر این باور بودند، از آن‌جایی‌که هیچ قاعده‌ای در حقوق بین‌الملل عرفی وجود ندارد که تأمین از راه دور قابلیت‌های ارتباطی بین‌المللی برای یک دولت دیگر را ممنوع کند، این فعالیت مشروع است، مگر آن‌که در جریان این اقدام، قواعد دیگری از حقوق بین‌الملل (مانند قاعده ۵۵ راهنمای تالین ۲)[۳] نقض شوند[۴] (Tallinn Manual 2.0, 2017, p 293-294).

از سوی‌دیگر براساس بند (ب) قاعده ۶۲ راهنمای تالین ۲، یک دولت می‌تواند ارتباط سایبری خصوصی مانند پیام فوری، ایمیل یا توییتی را که مغایر با قوانین ملی، نظم یا اخلاق عمومی است یا امنیت ملی آن دولت را به‌خطر می‌اندازد، متوقف کند (در این قاعده، واژه «خصوصی[۵]» به‌معنای «غیردولتی» است)[۶]. به‌عنوان مثال، یک دولت می‌تواند سازکارهایی برای مسدود کردن و گزارش پیام‌های فوری افراد خصوصی که از طریق یک پورتال شبکه اجتماعی ارسال می‌شوند و شامل کلمات کلیدی خاصی هستند که نشان‌دهنده محتوای پورنوگرافی کودکان یا فعالیت‌های تروریستی است، ایجاد کند. همچنین مطابق این قاعده، نیازی به اطلاع‌رسانی قبلی یا بعد از متوقف کردن یک ارتباط سایبری خصوصی خاص نیست (Tallinn Manual 2.0, 2017, p 294).

در نهایت، کارشناسان راهنمای تالین ۲ تأکید کردند که اگر یک دولت حق خود را تحت بند (الف) یا (ب) اعمال کند، این اقدام بدون خدشه به حقوق بین‌الملل بشر (مطابق فصل ۶ راهنمای تالین ۲) خواهد بود. هم‌چنین کارشناسان توافق داشتند که طبق بند (الف)، دولت دریافت‌کننده نمی‌تواند خدمات ارتباطی سایبری بین‌المللی را که نمایندگی‌های دیپلماتیک یا پست‌های کنسولی به آن وابسته هستند، معلق کند؛ زیرا براساس قاعده ۴۲ راهنمای تالین ۲[۷]، باید امکان برقراری ارتباطات الکترونیکی آزاد برای این نمایندگی‌ها یا پست‌ها فراهم باشد. علاوه براین، بند (ب) به دولت اجازه نمی‌دهد ارتباطات سایبری رسمی نمایندگی‌های دیپلماتیک یا پست‌های کنسولی را متوقف کند؛ زیرا این ارتباطات «خصوصی» محسوب نمی‌شوند (Tallinn Manual 2.0, 2017, p 294).

۳- ۳- تداخل مضر[۸]

قاعده ۶۳ راهنمای تالین ۲ مقرر می‌دارد: «استفاده یک دولت از ایستگاه‌های رادیویی نباید به‌گونه‌ای باشد که تداخل مضر با استفاده‌های محافظت‌شده دیگر دولت‌ها از فرکانس‌های رادیویی برای ارتباطات یا خدمات سایبری بی‌سیم ایجاد کند». در توضیح باید اذعان نمود، ممنوعیت تداخل مضر یک دولت با ارتباطات و خدمات سایبری بی‌سیم دولت دیگر براساس ماده ۴۵ (۱) اساسنامه اتحادیه بین‌المللی ارتباطات است. این ماده مقرر می‌دارد: «تمام ایستگاه‌ها، صرف‌نظر از هدفشان، باید به‌گونه‌ای تأسیس و بهره‌برداری شوند که تداخل مضر با خدمات یا ارتباطات رادیویی دیگر دولت‌های عضو ایجاد نکنند». البته شایان اشاره است، «تداخل مضر» به‌معنای تداخلی است که «عملکرد یک خدمت ناوبری رادیویی را به‌خطر

---

۱. قاعده ۳۵ راهنمای تالین ۲.
۲. مقدمه اساسنامه اتحادیه بین‌المللی ارتباطات.
مطابق قاعده ۴ راهنمای تالین ۲.
۳. قاعده ۵۵ راهنمای تالین ۲ (کنترل هواپیماهای انجام‌دهنده عملیات سایبری در حریم هوایی ملی) مقرر می‌دارد: «یک دولت می‌تواند عملیات هواپیماها، از جمله آن‌هایی که عملیات سایبری انجام می‌دهند، را در حریم هوایی ملی خود تنظیم کند».
۴. درخصوص تأمین خدمات ارتباطی به دولتی که این خدمات در آن موجود نیستند، به قاعده ۶۱ راهنمای تالین ۲ که پیشتر در این مقاله بررسی شد، مراجعه شود.

5. Private.
۶. ضمیمه‌های شماره ۱۰۱۴-۱۰۱۵ اساسنامه اتحادیه بین‌المللی ارتباطات.
۷. قاعده ۴۲ راهنمای تالین ۲ (آزادی ارتباطات) مقرر می‌دارد: «دولت پذیرنده موظف است ارتباطات سایبری آزاد یک مأموریت دیپلماتیک یا پست کنسولی را برای همه مقاصد رسمی اجازه داده و از آن محافظت کند».
8. Harmful Interference.

می‌اندازد یا به‌طور جدی کیفیت، انسجام یا استمرار یک خدمت ارتباط رادیویی که مطابق با مقررات رادیویی عمل می‌کند را مختل می‌کند[1]» (Tallinn Manual 2.0, 2017, p 296). لذا در چارچوب این مقاله، تداخل مضر به‌معنای کاهش جدی، انسداد یا قطع ارتباطات یا خدمات سایبری است که بر پایه طیف الکترومغناطیسی عمل می‌کنند.

در این راستا، ارتباطات و خدمات سایبری بی‌سیم از طریق امواج رادیویی، یعنی بر روی بخش خاصی از طیف الکترومغناطیسی، انجام می‌شوند[2]. خدمات سایبری بی‌سیم، برای‌نمونه، شامل مواردی مانند داده‌های تلفن همراه، دسترسی به وای‌فای[3]، جی‌پی‌اس و اتصال به اینترنت از طریق ماهواره‌های ارتباطی هستند. در ارتباط با اشاره به «ایستگاه‌های رادیویی» در این قاعده، کارشناسان راهنمای تالین ۲ توافق کردند که با وجود اشاره ماده ۴۵ (۱) اساسنامه اتحادیه بین‌المللی ارتباطات به «تمام ایستگاه‌ها»، این ماده صرفاً مربوطبه ایستگاه‌های رادیویی است. این نتیجه‌گیری کارشناسان براساس این واقعیت است که ماده ۴۵ در فصل هفتم اساسنامه اتحادیه بین‌المللی ارتباطات، تحت عنوان «مقررات ویژه برای رادیو»[4]، قرار دارد. البته همان‌طور که در قاعده ۶۴ راهنمای تالین ۲ بیان شده است (در ادامه مقاله بررسی می‌شود)، ممنوعیت تداخل مضر در این قاعده شامل ایستگاه‌های رادیویی نظامی که برای اهداف نظامی استفاده می‌شوند، نمی‌شود. البته شایان اشاره است، در راهنمای تالین ۲ اصطلاح «ایستگاه‌ها[5]» به هر ایستگاه رادیویی ارسال‌کننده اشاره دارد، چه در زمین باشد و چه در فضا، که سیگنال‌های فرکانس رادیویی را در طیف الکترومغناطیسی ارسال کرده و می‌تواند باعث تداخل مضر در خدمات یا ارتباطات بی‌سیم سایر دولت‌ها شود[6]. نمونه‌های مرتبط با سایبر، شامل ایستگاه‌های زمینی ماهواره‌ای که سیگنال‌ها را به ماهواره‌های ارتباطی ارسال می‌کنند، ماهواره‌های ارتباطی که داده‌ها را به زمین ارسال می‌کنند، آنتن‌های انتقال تلفن همراه و دکل‌های ارائه‌دهندگان خدمات اینترنت بی‌سیم[7] هستند (Tallinn Manual 2.0, 2017, p 295).

علاوه بر این، کارشناسان راهنمای تالین ۲ توافق کردند که این قاعده به‌طور انحصاری به تداخلی اعمال می‌شود که توسط یک دولت در استفاده دولت دیگر از فرکانس‌هایی که ارتباطات یا خدمات سایبری را ممکن می‌سازند، صرف‌نظر از این‌که این ارتباطات یا خدمات در کجا صورت می‌گیرند، از جمله در فضای ماورای جو، ایجاد می‌شود. هدف این قاعده تضمین آزادی دولت‌ها از تداخل مضر توسط سایر دولت‌ها در استفاده صحیح هماهنگ‌شده و ثبت‌شده آن ها در ثبت فرکانس بین‌المللی اصلی[8] از فرکانس‌های رادیویی طیف الکترومغناطیسی است. تداخل موردنظر می‌تواند عمدی یا غیرعمدی باشد. با این‌حال، حفاظت از تداخل مضر مشروط به این است که دولت، استفاده از فرکانس‌های خاص را با ثبت رسمی آن ها طبق مفاد مربوط مقررات رادیویی اتحادیه بین‌المللی ارتباطات به رسمیت شناخته باشد. موردی را در نظر بگیرید که دولت (الف) یک شبکه ارتباطات بی‌سیم جدید را برای فعالیت انحصاری در قلمرو خود مجوز می‌دهد و از زیرساخت سایبری موجود در آن‌جا استفاده می‌کند. دولت (الف) نه فرکانس‌های جدید استفاده‌شده را در ثبت فرکانس بین‌المللی اصلی ثبت کرده و نه الزام هماهنگی استفاده از فرکانس‌های اپراتور خود را با دولت‌های همسایه (ب) و (ج) انجام داده‌است. دولت‌های (ب) و (ج) پیش‌تر مجوز فعالیت یک شبکه مشابه را مطابق با الزامات اتحادیه بین‌المللی ارتباطات صادر کرده و حقوق استفاده و شناسایی بین‌المللی برای آن فرکانس‌ها را به‌دست آورده‌اند. اپراتور جدید دولت (الف) شبکه خود را فعال می‌کند و تداخل مضر برای اپراتورهای دولت‌های (ب) و (ج) ایجاد می‌شود. لذا دولت (الف) در این مورد، مرتکب نقض این قاعده شده است (Tallinn Manual 2.0, 2017, p 296-297).

علاوه بر این، برای نمونه، یک مهاجم سایبری ممکن است تلاش کند کیفیت خدمات در دسترس کاربران شبکه را با پر کردن کانال‌های ارتباطی با حجم زیادی از ترافیک جعلی کاهش دهد. حمله محروم‌سازی از سرویس به شبکه بی‌سیمی که برای کنترل عملیات یک کارخانه استفاده می‌شود (برای مثال، حمله اختلال[9]) ممکن است منجر به تعطیلی آن شود. تسلط بر یک مرکز تبادل ارتباطی می‌تواند به مهاجم سایبری این امکان را بدهد که با تماس‌های جعلی، وزارت دفاع دشمن را به شدت تحت فشار قرار دهد و استفاده کارکنان از تلفن‌ها برای انجام کارهایشان را غیرممکن کند. هم‌چنین حمله محروم‌سازی از سرویس ممکن است برای جلوگیری از استفاده دشمن

---

۱. ضمیمه شماره ۱۰۰۳ اساسنامه اتحادیه بین‌المللی ارتباطات؛ ماده ۱،۱۶۹مقررات رادیویی اتحادیه بین‌المللی ارتباطات.

از دیدگاه فنی، تداخل زیان‌بار زمانی رخ می‌دهد که دو یا چند موج الکترومغناطیسی با طول‌موج و دامنه یکسان، اما با فازهای مختلف، به‌صورت جزئی یا کامل با یکدیگر هم‌پوشانی داشته باشند و درنتیجه، یکدیگر را تضعیف یا خنثی کنند.

۲. امواج رادیویی، «امواج الکترومغناطیسی با فرکانس‌های به‌طور دلخواه کمتر از ۳۰۰۰ گیگاهرتز هستند که در فضا بدون راهنمای مصنوعی انتشار می‌یابند» (ماده ۱،۵ مقررات رادیویی اتحادیه بین‌المللی ارتباطات.

3. Wi-Fi.

4. Special Provisions for Radio.

5. Stations.

۶. ایستگاه [رادیویی] در مقررات رادیویی اتحادیه بین‌المللی ارتباطات به‌عنوان «یک یا چند فرستنده یا گیرنده یا ترکیبی از فرستنده‌ها و گیرنده‌ها، شامل تجهیزات جانبی لازم در یک مکان مشخص برای ارائه خدمات رادیو–ارتباطی یا خدمات رادیو–نجومی» تعریف شده است (ماده ۱،۶۱ مقررات رادیویی اتحادیه بین‌المللی ارتباطات). در بسیاری موارد، مقررات رادیویی اتحادیه بین‌المللی ارتباطات به‌طور خاص به «ایستگاه‌های فرستنده» (transmitting stations) اشاره می‌کند.

7. Wireless Internet Service Providers (so-called ‘WISPs’).

8. Master International Frequency Register (MIFR).

9. Jamming.

از یک سیستم ارتباطی به‌کار رود و او را مجبور کند به روش‌های ارتباطی کمتر امن روی بیاورد که در برابر بهره‌برداری سایبری آسیب‌پذیر باشد (Lin, 2010, p 70).

لذا با توجه به ایجاد عمدی تداخل مضر، کارشناسان راهنمای تالین ۲ اشاره کردند که دولت‌ها به‌طور منظم فعالیت‌هایی را انجام می‌دهند که گاه به‌عنوان عملیات جنگ الکترونیکی یا به‌سادگی «اختلال[۱]» نامیده می‌شود. در زمان صلح، دولت‌ها اقدام به عملیات اختلال برای مسدودسازی پخش رادیو، تلویزیون و ماهواره به‌دلایل ایدئولوژیک یا سیاسی کرده‌اند. به‌عنوان مثال، کارشناسان به اختلال کوبا در پخش رادیو مارتی[۲] از ایالات متحد اشاره می‌نمایند. لذا کارشناسان توافق کردند، مگر این‌که اختلال در زمان صلح توسط یک ایستگاه رادیویی نظامی[۳] انجام شود یا به‌طور کامل در قلمرو آن دولت صورت گیرد و تأثیر بگذارد، این اقدام معمولاً نقض این قاعده به شمار می‌رود. با این‌حال، کارشناسان هم‌چنین توافق داشتند که اختلال فرامرزی برای جلوگیری از نقض هنجارهای قاعده آمره[۴]، مانند پخش‌های رادیویی که نسل‌کشی رواندا در سال ۱۹۹۴ را تحریک کردند، قانونی است[۵]. درنهایت، کارشناسان یادآور شدند که اختلال در شرایط خاصی می‌تواند به‌عنوان یک اقدام متقابل[۶] قانونی مجاز باشد. از طرف دیگر در جریان یک مخاصمه مسلحانه، جواز انجام اختلال تحت شمول قواعد حقوق مخاصمات مسلحانه[۷] به‌عنوان حقوق خاص[۸] تعیین می‌شود. برای مثال، اختلال عمدی در سیستم‌های راداری دفاع هوایی دشمن یا سیستم‌های ناوبری جی‌پی‌اس به‌منظور حمایت از حمله هوایی به یک هدف نظامی[۹] قابل بررسی است. اگر این اختلال احتمالاً منجر به تلفات جانبی غیرنظامیان یا آسیب به اموال غیرنظامی شود، این خسارات باید به‌عنوان خسارت جانبی در تحلیل تناسب[۱۰] و الزامات احتیاط در حمله[۱۱] مورد توجه قرار گیرد. هم‌چنین عملیات ایجاد تداخل عمدی مضر ممکن است نقض سایر قواعد حقوق بین‌الملل باشد. به‌ویژه، مقررات مربوط به محدودیت‌های اعمال‌شده بر کشتی‌ها در عبور بی‌ضرر[۱۲] و هواپیماها و کشتی‌ها در عبور از آبراه‌های ترانزیتی[۱۳] و مجمع‌الجزایری[۱۴] ممکن است مرتبط باشد[۱۵] (Tallinn Manual 2.0, 2017, p 297-298).

از سوی‌دیگر، اساسنامه اتحادیه بین‌المللی ارتباطات بیان می‌کند که «فرکانس‌های رادیویی و هرگونه مدارهای مرتبط منابع طبیعی محدودی هستند و باید به‌صورت منطقی، کارآمد و اقتصادی مورد استفاده قرار گیرند تا کشورها یا گروه‌های کشورها بتوانند دسترسی عادلانه‌ای به این مدارها و فرکانس‌ها داشته باشند[۱۶]». با توجه به این‌که استفاده از این منابع محدود توسط کشورها به‌طور قابل‌توجهی افزایش یافته است، به‌ویژه با ظهور و گسترش فعالیت‌های سایبری بی‌سیم، احتمال تداخل مضر غیرعمدی نیز افزایش یافته است. بنابراین، برنامه‌ریزی و هماهنگی استفاده از این منابع در سطح بین‌المللی از اهمیت حیاتی برخوردار است. در این‌راستا، اتحادیه بین‌المللی ارتباطات نقش هماهنگ‌کننده‌ای برای کشورهای عضو در مدیریت طیف الکترومغناطیسی به‌عنوان یک منبع مشترک و مدارهای زمینی مرتبط ایفا می‌کند[۱۷]. برای این‌که کشورها بتوانند شناسایی بین‌المللی فرکانس‌ها و مدارهای زمینی مرتبطی که استفاده می‌کنند را دریافت کرده و از حفاظت ناشی از آن در برابر تداخل مضر بهره‌مند شوند، باید استفاده آن ها مطابق با نظام هماهنگی و ثبت اتحادیه بین‌المللی ارتباطات یا هرگونه ترتیبات ویژه مطابق با ماده ۴۲ اساسنامه اتحادیه بین‌المللی ارتباطات باشد[۱۸]. در این‌راستا کارشناسان راهنمای تالین ۲

---

۱. اختلال (جَمینگ) با هدف مسدودسازی فعالیت‌های خاص، از جمله فعالیت‌های سایبری، معمولاً براساس محتوای آن ها انجام می‌شود (Tallinn Manual 2.0, 2017, p 297).

2. Radio Marti.

۳. قاعده ۶۴ راهنمای تالین ۲.

4. Jus Cogens.

۵. در این‌خصوص مراجعه کنید به؛
The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, Case No. ICTR-99-52-T, judgment and sentence, paras. 949–953, 970–974 (3 December2003).

۶. قاعده ۲۰ راهنمای تالین ۲.

۷. بخش چهارم راهنمای تالین ۲.

8. Lex Specialis.

۹. قاعده ۱۰۰ راهنمای تالین ۲.

۱۰. قاعده ۱۱۳ راهنمای تالین ۲.

۱۱. قواعد ۱۱۴–۱۲۰ راهنمای تالین ۲.

۱۲. قاعده ۴۸ راهنمای تالین ۲.

۱۳. قاعده ۵۲ راهنمای تالین ۲.

۱۴. قاعده ۵۳ راهنمای تالین ۲.

۱۵. هم‌چنین، به محدودیت‌های مربوط به پرواز هواپیماها بر فراز حریم هوایی ملی یک کشور دیگر (قاعده ۵۵ راهنمای تالین ۲) توجه شود.

۱۶. ماده ۴۴ (۲) اساسنامه اتحادیه بین‌المللی ارتباطات.

۱۷. مدیریت طیف فرکانسی با کنوانسیون بین‌المللی تلگراف بی‌سیم ۱۹۲۷ آغاز شد. اتحادیه بین‌المللی ارتباطات نیز از اواخر دهه ۱۹۵۰ شروع به تنظیم موقعیت‌های مداری کرد.

۱۸. مواد ۸ و ۱۱ مقررات رادیویی اتحادیه بین‌المللی ارتباطات. باید اشاره داشت، مقررات رادیویی اتحادیه بین‌المللی ارتباطات چارچوب بین‌المللی برای اعلام و ثبت استفاده از فرکانس‌های الکترومغناطیسی و مدارها را تعیین می‌کند. براساس این مقررات، استفاده از فرکانس‌های الکترومغناطیسی و مدارها در ثبت فرکانس بین‌المللی اصلی (MIFR) یا در یک برنامه توافق‌شده برای استفاده از فرکانس‌ها ثبت می‌شود. شایان ذکر است که استفاده‌های نظامی از منابع طیف و مدار، به‌صورت شفاف در ثبت فرکانس بین‌المللی اصلی ثبت نمی‌شوند، بلکه به‌طور کلی به‌عنوان استفاده‌های دولتی یا «غیراختصاص‌یافته» در قلمرو یک دولت تعیین می‌شوند. این امر با قاعده ۶۴ راهنمای تالین ۲ مطابقت دارد. راهنمای تالین ۲ برای نمونه‌هایی از استفاده نظامی از طیف الکترومغناطیسی به منبع زیر اشاره می‌نماید.

United States Department of Defense, JP 6-01, Joint Electromagnetic Spectrum Management Operations, 2012.

نتیجه گرفتند که نظام اتحادیه بین‌المللی ارتباطات درخصوص استفاده از طیف الکترومغناطیسی و مدارهای زمینی مرتبط، به‌خوبی تثبیت شده و در مورد استفاده از آن ها برای فعالیت‌های سایبری نیز قابل اعمال است[۱] (Tallinn Manual 2.0, 2017, p 295-296).

۳- ۴- معافیت ایستگاه‌های رادیویی نظامی[۲]

عملیات سایبری تا حد زیادی از زیرساخت اینترنت استفاده می‌کنند. در چنین شرایطی، اینترنت به‌طور هم‌زمان برای مقاصد غیرنظامی و نظامی استفاده می‌شود که آن را به یک شیء دوگانه‌کاربرد[۳] تبدیل می‌کند. بنابراین، همان طورکه در مورد هر شیء دوگانه‌کاربرد وجود دارد، اینترنت (یعنی زیرساخت شبکه‌ای که از آن تشکیل شده است) ممکن است به‌عنوان یک هدف نظامی در نظر گرفته شود (Woltag, 2015, p 6).

از این‌رو، افزایش تعداد موارد اختلال در شبکه‌های اطلاعاتی و ارتباطی به‌دلیل حملات سایبری، ضرورت حفاظت از آن ها در برابر این نوع حملات را مشخص می‌کند. به‌ویژه، مسئله افزایش امنیت سایبری در شرایط اجرای عملیات توسط نیروهای نظامی بسیار حائز اهمیت است. به‌واسطه درگیری‌های مسلحانه در شرق اوکراین، بی‌ثباتی نظامی- سیاسی در خاورمیانه و رقابت برای نفوذ بر جریان‌های مالی و انرژی جهان، بی‌ثباتی نظامی- سیاسی جهانی شدت یافته است. این وضعیت، به‌دلیل افزایش تعداد دستگاه‌های ارتباطی در شبکه‌های اطلاعاتی و مخابراتی و هم‌چنین افزایش تعداد حملات احتمالی که می‌توانند برای مختل کردن عملکرد این شبکه‌ها استفاده شوند، رخ داده‌است (Sova, 2022, p 25). لذا شایسته است که اپراتورهای فنی باید نوع حمله بعدی، شدت آن و منابع اضافی برای کمک به دفاع، علاوه‌بر افزایش پیشگیری از حملات سایبری علیه دولت، ارتش، زیرساخت‌های حیاتی و غیرنظامیان کشور را پیش‌بینی کنند (Vaseshta et al., 2014, p 6).

با این‌حال، ماده ۴۸ (۱) اساسنامه اتحادیه بین‌المللی ارتباطات بیان می‌دارد: «کشورهای عضو درخصوص ایستگاه‌های رادیویی نظامی خود از آزادی کامل برخوردار هستند» و در قاعده ۶۴ راهنمای تالین ۲ نیز بیان شده است: «یک دولت در چارچوب حقوق بین‌الملل ارتباطات، درخصوص ایستگاه‌های رادیویی نظامی از آزادی کامل برخوردار است».

کارشناسان راهنمای تالین ۲ توافق داشتند که این مقرره، منعکس‌کننده رویه دیرینه دولت‌ها درخصوص حاکمیت بر ارتباطات بین‌المللی از راه دور است. در این زمینه، آن ها خاطرنشان کردند که معافیتی مشابه در کنوانسیون تلگراف بین‌المللی ۱۹۰۶ اتحادیه تلگراف بین‌المللی[۴] (پیشروی اتحادیه بین‌المللی ارتباطات) نیز گنجانده شده بود[۵]. این استثناء در نسخه‌های بعدی کنوانسیون‌های هر دو اتحادیه حفظ شده است[۶] (Tallinn Manual 2.0, 2017, p 298).

در این راستا باید بیان داشت، اگرچه کنوانسیون اتحادیه بین‌المللی ارتباطات تعریفی از «ایستگاه رادیویی[۷]» ارائه نمی‌دهد، کارشناسان راهنمای تالین ۲ توافق داشتند که این اصطلاح شامل تجهیزاتی است که امکان انتقال بی‌سیم داده‌ها از طریق امواج رادیویی را فراهم می‌کنند (البته درصورتی‌که این ایستگاه‌ها یا دیگر ایستگاه‌های رادیویی دارای ماهیت «نظامی[۸]» باشند، این قاعده اعمال می‌شود). هم‌چنین درباره دامنه اصطلاح «ایستگاه‌های رادیویی نظامی[۹]»، کارشناسان توافق کردند که ایستگاهی که منحصراً برای اهداف نظامی به‌کار می‌رود، مانند یک ماهواره ارتباطی نظامی، مشمول این قاعده است. کارشناسان هم‌چنین متفق‌القول بودند که این اصطلاح شامل ایستگاه‌های رادیویی نظامی مورد استفاده توسط نیروهای چندملیتی، از جمله نیروهای صلح‌بان، نیز می‌شود. درنهایت، برخی ایستگاه‌های غیرنظامی که صرفاً برای اهداف نظامی استفاده می‌شوند، مانند یک ماهواره شناسایی که توسط یک سازمان اطلاعاتی غیرنظامی برای جمع‌آوری اطلاعات نظامی به‌کار گرفته می‌شود، ممکن است تحت شمول این قاعده قرار گیرند. با این‌حال، به‌طورکلی، ایستگاه‌هایی که برای مقاصد دولتی استفاده می‌شوند، مشمول تعریف ایستگاه‌های رادیویی نظامی نمی‌شوند[۱۰] (Tallinn Manual 2.0, 2017, p 299).

علاوه براین، کارشناسان توافق داشتند که این قاعده شامل ایستگاه‌های رادیویی غیرنظامی که نظامیان به همراه کاربران غیرنظامی از آن‌ها استفاده می‌کنند (ایستگاه‌های به‌اصطلاح «دومنظوره») نمی‌شود[۱۱]. نمونه برجسته این

---

۱. چنین هماهنگی فنی از اواسط قرن بیستم به‌طور مستمر در میان دولت‌ها در سطوح دوجانبه، چندجانبه و جهانی انجام شده است.

2. Exemption of Military Radio Installations.

3. Dual-Use.

4. International Telegraph Union.

۵. ماده ۲۱ کنوانسیون بین‌المللی رادیوتلگراف ۱۹۰۶.

۶. ماده ۳۹ کنوانسیون بین‌المللی ارتباطات ۱۹۳۲؛ ماده ۳۸ کنوانسیون ارتباطات ۱۹۷۳؛ ماده ۴۸ اساسنامه اتحادیه بین‌المللی ارتباطات.

7. Radio Installation.

8. Military.

9. Military Radio Installations.

۱۰. راهنمای تالین ۲ به منبع زیر با این مضمون اشاره می‌نماید: «ماده ۴۸ به «تأسیسات رادیویی نظامی» اشاره دارد و نه به ایستگاه‌هایی که به‌طور کلی برای مقاصد دولتی استفاده می‌شوند».

Circular Letter from François Rancy, Director, Radiocommunication Bureau, to Administrations of Member States of the ITU, CR/389, 26 January 2016.

۱۱. ماده ۴۸ (۳) اساسنامه اتحادیه بین‌المللی ارتباطات.

مورد، سیستم ناوبری جی‌پی‌اس است که توسط وزارت دفاع ایالات متحد آمریکا اداره می‌شود، اما هم به مقاصد غیرنظامی و هم نظامی خدمت می‌کند. کارشناسان هم‌چنین توافق کردند که این قاعده شامل ایستگاه‌های رادیویی نظامی یک دولت که خدماتی مانند اتصال به اینترنت بی‌سیم را منحصراً به عموم مردم ارائه می‌دهند، نمی‌شود (Tallinn Manual 2.0, 2017, p 299).

از سوی‌دیگر، استثنای ایستگاه‌های نظامی از حقوق بین‌الملل ارتباطات در ماده ۴۸ (۱) اساسنامه اتحادیه بین‌المللی ارتباطات، به‌عنوان «آزادی کامل[1]» توصیف شده است. کارشناسان راهنمای تالین ۲ توافق داشتند که این آزادی به این معناست که، برای مثال، یک دولت ملزم نیست تخصیص فرکانس یک ماهواره ارتباطی نظامی در مدار زمین ثابت را طبق مقررات رادیویی اتحادیه بین‌المللی ارتباطات ثبت کند[2]، امری که در شرایط عادی الزامی است[3]. درواقع، از آن‌جا که یک ماهواره ارتباطی نظامی احتمالاً برای انتقال اطلاعات حساس و طبقه‌بندی‌شده به‌کار گرفته می‌شود، افشای فرکانس‌هایی که این ماهواره استفاده می‌کند، رهگیری این داده‌ها توسط سایر دولت‌ها را تسهیل می‌کند. هم‌چنین کارشناسان تأیید کردند که ماده ۴۸ (۲) اساسنامه اتحادیه بین‌المللی ارتباطات دولت‌ها را ملزم می‌کند تا «تا حد امکان» مقررات اداری اتحادیه بین‌المللی ارتباطات (یعنی مقررات رادیویی و مقررات بین‌المللی ارتباطات) را رعایت کنند. بنابراین، برای مثال، اگر دولتی یک ماهواره ارتباطی نظامی را به‌کار گیرد و فرکانس‌های مورد استفاده آن را ثبت نکرده باشد، آن دولت باید تا حد امکان از ایجاد تداخل مضر با استفاده هماهنگ و ثبت‌شده سایر دولت‌ها از همان فرکانس‌ها خودداری کند (Tallinn Manual 2.0, 2017, p 299-300). البته ایستگاه‌های رادیویی نظامی که از خاک دولت دیگری فعالیت می‌کنند، مشمول رضایت دولت پذیرنده هستند[4].

٤- نتیجه‌گیری

با پیشرفت سریع فناوری و افزایش وابستگی به زیرساخت‌های دیجیتال در بخش ارتباطات، این حوزه با تهدیدات سایبری و آسیب‌پذیری‌های متعددی مواجه است. این تهدیدات شامل نقض داده‌ها، حملات محروم‌سازی از خدمات، دسترسی غیرمجاز، آلودگی به بدافزارها و غیره هستند که همگی می‌توانند خدمات حیاتی را مختل کنند. ادغام فناوری‌هایی هم‌چون 5G، اینترنت اشیاء و رایانش ابری نیز به گسترش سطح حملات منجر شده و چالش‌های امنیتی جدیدی را مطرح می‌کند که به اجرای پروتکل‌های امنیتی پیچیده نیاز دارند.

با این‌حال همان‌طور که در مقاله به تفصیل مورد مداقه قرار گرفت؛ نخست، دولت‌ها باید اقداماتی را برای تضمین ایجاد زیرساخت‌های بین‌المللی ارتباطات که برای ارتباطات سریع و بدون وقفه بین‌المللی ضروری است، انجام دهند. در صورتی‌که دولت‌ها به‌منظور رعایت این الزام، زیرساخت سایبری برای ارتباطات بین‌المللی ایجاد کند، هم‌چنین موظف‌اند آن زیرساخت را نگهداری و از آن حفاظت کنند؛ دوم، دولت‌ها می‌توانند خدمات ارتباطی سایبری بین‌المللی را به‌طور کامل یا جزئی در قلمرو خود تعلیق کنند. در این‌صورت، باید فوراً سایر دولت‌ها را از این تعلیق مطلع سازد. هم‌چنین دولت‌ها می‌تواند انتقال یک ارتباط سایبری خصوصی را که به‌نظر می‌رسد برخلاف قوانین ملی، نظم یا اخلاق عمومی آن باشد، یا برای امنیت ملی خطرناک است، متوقف کند. البته تمام این اقدامات باید در شرایطی باشد که سایر قواعد حقوق بین‌الملل، برای نمونه حریم خصوصی در چارچوب قواعد حقوق بشر، نقض نگردد؛ سوم، استفاده دولت‌ها از ایستگاه‌های رادیویی نباید به‌گونه‌ای باشد که تداخل مضر با استفاده‌های محافظت‌شده دیگر دولت‌ها از فرکانس‌های رادیویی برای ارتباطات یا خدمات سایبری بی‌سیم ایجاد کند؛ و در نهایت، دولت‌ها در چارچوب حقوق بین‌الملل ارتباطات، درخصوص ایستگاه‌های رادیویی نظامی از آزادی کامل برخوردار می‌باشند. البته برخورداری از این حق، مستلزم بررسی مورد به مورد می‌باشد تا دولت‌ها با نحوه استعمالشان از این حق، در پی سوءاستفاده از آن و ایجاد تداخل مضر برای سایر دولت‌ها برنیایند.

در پایان شایان اشاره است، در راستای اجرای تدابیر مؤثر برای مقابله با این تهدیدات، نیاز به یک استراتژی جامع وجود دارد که شامل مدیریت اصولی، تأمین منابع مالی کافی و بازنگری مستمر در شیوه‌های امنیت سایبری باشد و شرکت‌های مخابراتی نیز با جدیدترین تحولات تهدیدات سایبری و روندها آشنا شوند تا بتوانند پروتکل‌های امنیتی خود را به‌طور مناسب تنظیم و به‌روزرسانی کنند.

---

1. Entire Freedom.

۲. مدار زمینی ماهواره، مسیر حرکت ماهواره در اطراف زمین است که تحت تأثیر نیروی جاذبه قرار دارد. مدار زمین‌ثابت، جایی‌که اکثر ماهواره‌های ارتباطی در آن قرار می‌گیرند، در فاصله‌ی ۳۵,۷۸۶ کیلومتری از زمین و دقیقاً بالای خط استوا قرار دارد. از آن‌جا که ماهواره‌ای که در این مدار قرار گرفته با همان سرعت و در همان جهت چرخش زمین حرکت می‌کند، نسبت به یک نقطه‌ی مشخص روی زمین ثابت باقی می‌ماند.

۳. از جمله ماده ۸ مقررات رادیویی اتحادیه بین‌المللی ارتباطات.

۴. قاعده ۲ راهنمای تالین ۲.

منابع

[۱] اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹۴). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی، ۱۸ (۷۱)، ۲۵۷-۲۷۸.

[۲]بیگ‌زاده، ابراهیم (۱۴۰۰). حقوق سازمان‌های بین‌المللی. چاپ هشتم. تهران: انتشارات مجد.

[۳] بیگلربیگی، کیان (۱۴۰۲). حملات سایبری و نقض اصل عدم مداخله. پایان‌نامه کارشناسی ارشد حقوق بین‌الملل. به راهنمایی ابراهیم بیگ‌زاده. تهران: دانشگاه شهید بهشتی، دانشکده حقوق، تاریخ دفاع ۱۴۰۲/۰۶/۱۹..

[4] Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System, (2003). Retrieved November 17, 2024 from https://rm.coe.int/168008160f

[5] Adel, A., Sarwar, D. & Hosseinian-Far, A. (2021). Transformation of Cybersecurity Posture in IT Telecommunication: A Case Study of a Telecom Operator, In book: Cybersecurity, Privacy and Freedom Protection in the Connected World, Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London.

[6] Arthur, Charles. (2011). Egypt blocks social media websites in attempted clampdown on unrest, The Guardian. Retrieved January 12, 2025 from https://www.theguardian.com/world/2011/jan/26/egypt-blocks-social-media-websites

[7] Circular Letter from François Rancy, Director, Radiocommunication Bureau, to Administrations of Member States of the ITU, (2016). CR/389. Retrieved January 14, 2025 from https://www.itu.int/en/ITU-R/conferences/RRB/Documents/ai%204_1_compendium%20to%20be%20published%20as%20special%20topics_English.docx

[8] Consolidated Version of General Conditions Office of Communications (UK) (‘Ofcom General Conditions’) (2015). Retrieved January 12, 2025 from https://www.ofcom.org.uk/siteassets/resources/documents/phones-telecoms-and-internet/information-for-industry/general-authorisationregime/consolidated_version_of_general_conditions_as_at_28_may_20151.pdf?v=335358

[9] Convention on Cybercrime (Budapest Convention), (2001). Council of Europe, European Treaty Series – No. 185., Entered into Force on 1 July 2004. Retrieved November 17, 2024 from https://rm.coe.int/1680081561

[10] Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009). Retrieved January 12, 2025 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

[11] Ezeigweneme, C.A., Umoh, A.A., Ilojianya, V.I., & Oluwatoyin, A. (2023). “Telecom project management: Lessons learned and best practices: A review from Africa to the USA”, World Journal of Advanced Research and Reviews, 20(03), pp. 1713–1730.

[12] Folorunsho, S. O., Adenekan, O. A., Ezeigweneme, C., Somadina, I. C., & Okeleke, P. T. (2024). “Ensuring Cybersecurity in telecommunications: Strategies to protect digital infrastructure and sensitive data”, Computer Science & IT Research Journal, 5(8), pp. 1855-1883.

[13] General Agreement on Trade in Services, Annex on Telecommunications. (1994). Retrieved January 12, 2025 from https://www.wto.org/english/docs_e/legal_e/26-gats.pdf

[14] Giles, K., & Hartmann, K. (2021). “Adversary Targeting of Civilian Telecommunications Infrastructure”, 13th International Conference on Cyber Conflict (CyCon), pp. 133-150.

[15] Hill, R. (2015). Dealing with Cyber Security Threats: International Cooperation, ITU and WCIT, in Maybaum, M., Osula, A.M, and Lindström L. (Eds.), Proceedings of the7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015, NATO CCDCOE Publications.

[16] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence. (2017). Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation, Cambridge University Press.

[17] International Radiotelegraph Convention. (1906). Retrieved January 13, 2025 from https://www.itu.int/en/history/Pages/RadioConferences.aspx?conf=4.36

[18] International Radiotelegraph Convention. (1927). Retrieved January 13, 2025 from https://history.state.gov/historicaldocuments/frus1927v01/d235

[19] International Telecommunication Convention. (1932). Retrieved January 13, 2025 from https://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=4.5

[20] International Telecommunication Convention. (1973). Retrieved January 13, 2025 from https://treaties.un.org/pages/showDetails.aspx?objid=08000002800e18c9

[21] ITU Constitution, Annex, No. 1012. Retrieved January 12, 2025 from https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf

[22] ITU Constitution. Retrieved January 12, 2025 from https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf

[23] ITU International Telecommunication Regulations. (1988). Retrieved January 12, 2025 from https://www.itu.int/dms_pub/itu-t/oth/3f/01/t3f010000010001pdfe.pdf

[24] ITU International Telecommunication Regulations. (2012). Retrieved January 12, 2025 from https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

[25] ITU Radio Regulations. (2024). Retrieved January 12, 2025 from https://www.itu.int/pub/R-REG-RR

[26] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). "Artificial intelligence for cybersecurity: Literature review and future research directions". Information Fusion, 97(101804), pp . 1-29.

[27] Lin, H. S. (2010). "Offensive Cyber Operations and the Use of Force", Journal of National Security Law & Policy, 4(63), pp. 63-86.

[28] Manukonda, K. R. R. (2019). "Cyber Attack on Telecommunications Company", European Journal of Advances in Engineering and Technology, 6(12), pp.113-120.

[29] Naughton, J. (2016). "The evolution of the Internet: from military experiment to General Purpose Technology", Journal of Cyber Policy, (1), pp. 5-28.

[30] Okafor, E. S., Akinrinola, O., Usman, F. O., Amoo, O. O., & Ochuba, N. A. (2024). "Cybersecurity analytics in protecting satellite telecommunications networks: a conceptual development of current trends, challenges, and strategic responses", International Journal of Applied Research in Social Sciences, 6(3), pp. 254-266.

[31] Oleg, S. (2022). "Analysis of conditions and factors affecting cyber security in the special purpose information and telecommunication system", Technology audit and production reserves, 4 (2/66), pp. 25 - 28.

[32] Privalov, A., Lukicheva, V., Kotenko, I., & Saenko, I. (2020). "Increasing the Sensitivity of the Method of Early Detection of Cyber-Attacks in Telecommunication Networks Based on Traffic Analysis by Extreme Filtering", Energies, 13(11), 2774, pp. 1-18

[33] Roscini, M. (2014). Cyber Operations and the Use of Force in International Law. Oxford University Press.

[34] Sadiku, M. N. O., Adekunte, P. A., & Sadiku. J. O. (2024). "Cybersecurity in Telecommunications", International Journal of Trend in Scientific Research and Development, 8(6), pp. 493-502.

[35] Sadiku, M. N. O., Tembely, M., & Musa, S. M. (2016). "Smart grid cybersecurity", Journal of Multidisciplinary Engineering Science and Technology, 3(9), pp.5574-5576.

[36] Shoetan, P. A., Amoo, O. O., Okafor, E. S., & Olorunfemi, O. L. (2024). "Synthesizing Ai's impact on cybersecurity in telecommunications: a conceptual framework", Computer Science & IT Research Journal, 5(3), pp. 594-605.

[37] Singh, K., Kapoor, R. (2023). "Robotic

Process Automation and Security Operations in Telecommunications: Addressing Cyber Threats and Vulnerabilities", MZ Computing Journal, 4(1). pp. 1-7.

[38] Stockburger, P. Z. (2016). "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum", American University International Law Review, 31(4), pp. 544-591.

[39] The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, Case No. ICTR-99-52-T, judgment and sentence, (2003). Retrieved January 12, 2025 from https://www.refworld.org/jurisprudence/caselaw/ictr/2003/en/91852

[40] Twain, M. W., Morrison, J. L. & Scott, W. F. (2023). "Assessing the Effectiveness of Cybersecurity Measures in the United States Telecommunications Industry: A Comprehensive Analysis", Journal of Marketing and Communication, 6(1), pp. 1-10.

[41] United States Department of Defense, JP 6-01, Joint Electromagnetic Spectrum Management Operations,)2012(. Retrieved January 13, 2025 from https://www.govinfo.gov/content/pkg/GOVPUB-D5-PURL-gpo29176/pdf/GOVPUB-D5-PURL-gpo29176.pdf

[42] Vaseashta, A., Susmann, F., & Braman, E. (2014). Cyber Security and Resiliency Policy Framework, IOS Press.

[43] Wallace, W., & Visger, M. (2018). " Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community", Journal of Law & Cyber Warfare, 6(2), pp. 3-55.

[44] Woltag, J. C. (2015). Cyber Warfare, Max Planck Encyclopedias of International Law.