مسئولیت کیفری فردی مقامات عالی رتبه نظامی برای تجاوز سایبری و اعمال صلاحیت دیوان بین‌المللی کیفری بر آن (با تأکید بر رویکردهای رسانه‌ای)

مریم استوار[۱]، محمد پارس‌زاده[۲]

چکیده

تمامی نظام‌های عدالت کیفری جهان، مفهوم مسئولیت کیفری افراد را برای نقض هنجارهایی که انجام آنها همراه با مجازات است شناسایی کرده‌اند. بنابراین مسئولیت کیفری فردی، چه در حقوق داخلی و چه در حقوق بین‌الملل کیفری یکی از اصول کلی حقوق است. مقاله حاضر با روش توصیفی-تحلیلی در پی پاسخگویی به این سوال بوده است: «چه مقامی به‌صورت فردی مسئول تجاوز سایبری است»؟ یافته‌های پژوهش نشان می‌دهد که یک حمله شبکه‌ای رایانه‌ای را به‌سختی می‌توان به‌عنوان جرم تجاوز در زمره تجاوزات مطروحه در ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری قرار داد. اما به نظر می‌رسد با توجه به «ماهیت، شدت و گستره» آن حملات، بتوان یک حمله سایبری را به‌عنوان جرم تجاوز و نقض آشکار منشور ملل متحد در دیوان بین‌المللی کیفری مورد رسیدگی قرار داد. با توجه به شرط رهبری موجود در بند ۱ ماده ۸ مکرر اساسنامه، اشخاصی که در سلسله مراتب مختلف نظامی به‌طور موثر این حملات را انجام می‌دهند، جنگجویان سایبری هستند و بر اساس ماده ۸ مکرر اساسنامه از لحاظ کیفری مسئول نخواهند بود، اما مافوق آنها در صورتی‌که شرط لازم رهبری را دارا باشد، مسئول است. بنابراین مسئولیت کیفری فردی تنها زمانی محقق می‌شود که «شخص، در یک سمت رسمی، کنترل مؤثر خود را بر عمل سیاسی یا نظامی سایبری یک دولت اعمال و یا آن عمل را هدایت کند».

واژه‌های کلیدی: تجاوز سایبری، مسئولیت کیفری فردی، صلاحیت دیوان بین‌المللی کیفری، رسانه برون‌مرزی.

تاریخ دریافت: ۱۳۹۹/۰۳/۱۱ تاریخ پذیرش: ۱۳۹۹/۰۹/۱۵

۱. کارشناسی ارشد حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه آزاد اسلامی شیراز، شیراز، ایران. maryam_ostover5414@yahoo.com

۲. استادیار حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه آزاد اسلامی کازرون، کازرون، ایران. mparszadeh@yahoo.com

۱. مقدمه

یک حمله شبکه‌ای رایانه‌ای را به سه دلیل به‌ندرت می‌توان به‌عنوان جنایت تجاوز محسوب کرد. دلیل اول اینکه ماده ۸ مکرر اساسنامه، عمل اشخاص خصوصی را در بر نمی‌گیرد، اما اغلب طراحان این حمله را شامل می‌شود. دلیل دوم اینکه یک حمله شبکه‌ای رایانه‌ای تنها در شرایط استثنایی به‌عنوان «عمل تجاوز» در مفهوم بند ۲ ماده ۸ اساسنامه تلقی می‌شود؛ یعنی حمله‌ای که توسط نیروهای مسلح یک دولت انجام می‌شود. دلیل سوم اینکه همانگونه که در بند ۱ ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری مقرر شده است، اینگونه حملات را می‌توان به‌عنوان نقض آشکار منشور ملل متحد تلقی کرد (Ambos, 2016: 495). اولین کنفرانس بازنگری اساسنامه دیوان بین‌المللی کیفری در ۳۱ می ۲۰۱۰ در کامپالا، ماده ۸ مکرر اساسنامه که به تعریف جنایت تجاوز می‌پردازد متشکل از دو پاراگراف است که بند اول درباره تعریف جنایت تجاوز و بند دوم درباره مصادیق جنایت تجاوز است. همچنین در تعریف مزبور، چهار نوع از اَشکال مشارکت، یعنی طراحی، تدارک، آغاز و اجرای اعمال تجاوزکارانه بیان شده است. در سال ۱۹۵۵، «ژرژسل»[1] استاد برجسته حقوق بین‌الملل، پیشنهادی در مورد تعریف تجاوز به کمیسیون حقوق بین‌الملل ارائه داد که به موجب آن «تجاوز، یک جنایت علیه صلح و امنیت بشری است. این جنایت بر اثر هرگونه توسل به زور که ناقض مقررات منشور ملل متحد باشد به‌وجود می‌آید، اعم از اینکه هدفش تغییر وضعیت حقوق بین‌الملل موضوعه باشد و یا نتیجه‌اش برهم‌زدن نظم عمومی باشد» (ضیایی‌بیگدلی، ۱۳۸۰: ۲۹).

در سال ۱۹۷۰، مجمع عمومی سازمان ملل در قطعنامه معروف به «اعلامیه مربوط به اصول حقوق بین‌الملل در زمینه‌ی روابط دوستانه و همکاری میان کشورها، جنگ تجاوزکارانه را به‌عنوان جنایت علیه صلح که از نظر حقوق بین‌الملل مستوجب مسئولیت است، اعلام داشت» (همان). در رابطه با شرط رهبری موجود در بند اول ماده ۸ مکرر اساسنامه حداقل دو موضوع قابل بررسی است. ابتدا طبق این شرط باید مشخص شود که چه کسانی در حلقه رهبری در یک سمت رسمی می‌توانند به‌طور مؤثر کنترل خود را اعمال نمایند و یا عمل نظامی یا سیاسی یک دولت را هدایت کنند. دوم، ارتباط میان حلقه رهبری و روش‌های کلی مشارکت تحت ماده ۲۵ اساسنامه باید شرح داده شود. بنابراین این مقاله به‌دنبال بررسی این موضوع است که اگر یک حمله شبکه‌ای

1- George Scelle

رایانه‌ای دولت‌محور منجر به نقض آشکار منشور ملل متحد و به‌عنوان جنایت تجاوز تلقی شود، مسئول آن چه کسانی خواهند بود و مسئولیت کیفری فردی چه زمانی تحقق می‌یابد؟ آیا دیوان بین‌المللی کیفری صلاحیت رسیدگی به اینگونه حملات را دارد؟ برای دستیابی به پاسخ این پرسش‌ها از روش تحقیق توصیفی- تحلیلی استفاده می‌شود.

۲. پیشینه پژوهش

در خصوص جنایت تجاوز، صلاحیت دیوان بین‌المللی کیفری در رسیدگی به آن و مسئولیت کیفری مأموران و مقامات مافوق، مقالات متعددی نوشته شده است که برخی از آن‌ها عبارتند از: مقاله «جنایات بین‌المللی عربستان سعودی در یمن و چگونگی نقش‌آفرینی دیوان بین‌المللی کیفری» کاظمی (۱۳۹۸)، «حمله سایبری به‌مثابه جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن» اسماعیل‌زاده ملاباشی (۱۳۹۶)، «تحلیل رابطه مافوق- مادون به‌عنوان عنصر ساختاری مسئولیت کیفری مقامات مافوق در اسناد بین‌المللی و رویه قضائی» قریشی (۱۳۹۳)، «تعریف، عناصر و شروط اعمال صلاحیت دیوان کیفری بین‌المللی نسبت به جنایت تجاوز» آقایی جنت‌مکان (۱۳۹۰)، «دیوان کیفری بین‌المللی و صلاحیت رسیدگی به جنایت تجاوز» شایگان‌فرد (۱۳۸۷)، «مسئولیت کیفری ماموران عالی‌رتبه دولت‌ها در حقوق بین-الملل با تاکید بر رای دیوان بین‌المللی دادگستری بین کنگو و بلژیک» حسیبی (۱۳۸۶)، «مسئولیت ماموران مادون و مقامات مافوق در اساسنامه دادگاه بین‌المللی کیفری» میرمحمد صادقی (۱۳۸۳). نوآوری مقاله حاضر در این است‌که ابتدا آستانه تجاوز سایبری، حلقه رهبری، شرط رهبری و معیار کنترل مؤثر را شرح می‌دهد، سپس مسئولیت کیفری فردی مقامات عالی‌رتبه نظامی را برای تجاوز سایبری با ذکر رویه‌های قضائی (پرونده‌ی فاربن، پرونده‌ی کروپ و فرماندهی عالی) مورد تجزیه و تحلیل قرار می‌دهد. همچنین در این مقاله، پیشنهادهای رسانه‌ای در خصوص رویکرد شبکه‌های برون‌مرزی درباره حملات سایبری ارائه می‌شود.

۳. چارچوب نظری

مفهوم مسئولیت کیفری فردی مستقیماً در پرتو حقوق بین‌الملل کیفری مطرح و موجب شد تا پس از جنگ جهانی دوم در منشورهای نورنبرگ و توکیو ظاهر شود (کچوئیان‌فینی، ۱۳۸۸: ۱۱۴۲). ماده ۷ منشور نورنبرگ مقرر می‌کرد: «موقعیت رسمی متهمان خواه روسای دولت‌ها یا

ماموران مسئول در بخش دولتی نباید آن‌ها را از مسئولیت بری کند یا باعث تخفیف مجازات آن‌ها شود» (سبحانی، ۱۳۸۹: ۴۰). ماده ۶ منشور دادگاه نظامی توکیو با تغییرات اندکی همین موضوع را تأئید کرده است. بند ۲ ماده ۷ اساسنامه دادگاه کیفری بین‌المللی برای یوگسلاوی سابق مقرر می‌دارد که «سمت رسمی هر شخص متهم، خواه به‌عنوان رئیس دولت یا حکومت یا به‌عنوان مأمور دولتیِ مسئول نباید چنین شخصی را از مسئولیت کیفری مبری کند یا باعث تخفیف مجازاتش شود» (سبحانی، ۱۳۸۹: ۴۱– ۴۰). بند ۲ ماده ۶ اساسنامه دادگاه کیفری بین‌المللی برای روآندا نیز حاوی مقررات مشابه اساسنامه دادگاه کیفری بین‌المللی برای یوگسلاوی سابق است. نهایتاً مسئولیت کیفری فردی در ماده ۲۵ اساسنامه دیوان بین‌المللی کیفری درج و اجرایی شد. بنابراین در قالب نظریه «مسئولیت کیفری بین‌المللی فردی (حقیقی)» در ارتکاب جنایات بین‌المللی با دو دسته اشخاص حقیقی مسئول مواجه هستیم. اول، نظامیانی که مستقیماً مرتکب قتل و جنایت شده‌اند و دوم، سردمدارانی که مجموعه اعمال ارتکاب‌یافته توسط نظامیان تحت امر آن‌ها، یک جنایت خاص بین‌المللی مانند نسل‌زدایی، جنایت علیه بشریت، جنایت جنگی و تجاوز را شکل می‌دهد (کاظمی، ۱۳۹۸: ۱۱۹). دسته اخیر را افرادی مانند سران، وزیر جنگ و فرماندهان و مقامات عالی‌رتبه نظامی تشکیل می‌دهند که به‌موجب اصل مسئولیت کیفری بین‌المللی فردی مستحق و متحمل مجازات کیفری هستند. در نتیجه مطابق ماده ۲۵ اساسنامه دیوان بین‌المللی کیفری، دیوان تنها درباره جرایم اشخاص حقیقی صلاحیت رسیدگی خواهد داشت (سبحانی، ۱۳۸۹: ۱۲۰).

4. آستانه تجاوز سایبری

کارگروه ویژه راجع به جنایت «تجاوز» قبل از انتخاب واژه «آشکار» دو واژه «خطرناک» و «فاحش» را بررسی کردند، اما این دو واژه پذیرفته نشد و سرانجام طرفین مذاکره کننده مصمم شدند تا واژه «آشکار» را انتخاب کنند. زیرا این واژه در حقوق بین‌الملل معنی محسوس و قابل فهمی داشت، درحالی‌که واژه‌های «خطرناک» و «فاحش» بسیار نامحسوس بودند (Miller, 2014: 236-237). در بند ۲ ماده ۴۶ عهدنامه ۱۹۶۹ وین آمده است که: «تجاوز وقتی بارز است که بر کشوری که طبق رویه معمول و حسن نیت در این مورد عمل کرده است، به طور عینی روشن باشد» (Paulus, 2010: 1121). جنایت تجاوز می‌تواند تنها توسط رهبران سیاسی و نظامی ارتکاب یابد و اعمالی که در قالب دفاع مشروع و مجوز شورای امنیت انجام

می‌شود، قابل پیگیری نیستند. بنابراین هر عمل تجاوزی منجر به جنایت تجاوز نمی‌شود، بلکه طبق تعریف باید به منزله نقض آشکار منشور ملل متحد باشد. اگر عمل مزبور توسط شورای امنیت اجازه داده شود یا بر اساس ماده ۵۱ منشور سازمان ملل متحد مجاز باشد، تنها عمل تجاوز است، ولیکن جنایت تجاوز نمی‌باشد و دو شرط نقض منشور و نقض آشکار باید رعایت شود (موسی‌زاده و فروغی‌نیا، ۱۳۹۱: ۱۵۵). بنابراین باید سه شرط در خصوص آستانه حملات شبکه‌ای رایانه‌ای بررسی شود:

«گستره» این‌گونه حملات بدین معناست که متجاوزان تا چه اندازه ابزار و تجهیزات برای طرح‌ریزی و برپایی جنگ استفاده کرده‌اند.

«شدت» یعنی آثار و نتایجی که یک حمله به بار می‌آورد و باعث کشته شدن انسان‌ها و تخریب اموال می‌گردد و سرانجام «ماهیت» تجاوز یعنی آن حمله از چنان ویژگی‌ای برخوردار است که می‌تواند منجر به نقض بارز منشور ملل متحد شود. در نتیجه هر سه عامل «ماهیت، شدت و گستره» برای نقض آشکار منشور ملل متحد ضروری هستند. تجاوز سایبری یا حمله مسلحانه، یک عمل یا مجموعه‌ای از عملیات نظامی مسلحانه است که هم شدت قابل توجهی داشته و هم نتایج آن تخریب و نابودی اساسی عناصر حیاتی دولت قربانی از جمله ساختارهای اقتصادی و امنیتی، تضعیف و از بین بردن اقتدار دولتی و استقلال سیاسی و همچنین قربانی کردن مردم و محروم ساختن دولت از دارایی‌های فیزیکی همچون قلمرو است (اصلانی، ۱۳۹۵: ۱۸۵). معیار اصلی در تعیین اینکه حمله سایبری به آستانه یک حمله مسلحانه رسیده است، تبعات و نتایج قابل پیش‌بینی آن حملات می‌باشد که منجر به ورود صدمات فیزیکی و خسارت به اموال می‌گردد. حملات سایبری به شبکه‌ها و سیستم‌های رایانه‌ای در صورت داشتن این ویژگی، مصداق تجاوز سایبری یا حمله مسلحانه هستند. تنش‌ها و زد و خوردهای مرزی که در سطح و مقیاس کوچک اتفاق می‌افتند، بیشتر به‌عنوان حوادث مرزی از آن‌ها یاد می‌شود تا حمله مسلحانه. درنتیجه آستانه تجاوز سایبری با توجه به رویکرد نتیجه‌محوری آن است (اصلانی، ۱۳۹۵: ۲۶۳). یورام دینشتاین[1] از جمله حقوق‌دانانی است که به رویکرد نتیجه‌محور بودن حملات سایبری اعتقاد دارد. به‌نظر او از دیدگاه حقوقی دلیلی ندارد که بین ابزارهای فیزیکی و الکترونیکی برای حمله، قائل به تفکیک شد. اگر اقدامات سایبری بتواند نتایج مورد نظر را ایجاد نماید، می‌تواند

1.Yoram Dinstein

حمله مسلحانه قلمداد شود. به نظر او دشواری مسئله در وسیله ارتکاب نیست (چه توپخانه دشمن باشد چه یک سرور رایانه‌ای)، بلکه در میزان و وقوع نتایج است (Dinstein, 2005: 103).

5. دستورالعمل تالین[1] ناتو در خصوص جنگ سایبری

در سال ۲۰۰۹، مرکز عالی همکاری دفاع سایبری[2] واقع در تالین استونی که در سال ۲۰۰۸ از طرف ناتو به‌عنوان قطب علمی شناخته شده بود، از گروه بین‌المللی کارشناسان مستقل جهت نگارش دستورالعملی در خصوص قانون حاکم بر جنگ سایبری دعوت به عمل آورد. دستورالعمل حقوق بین‌الملل در مورد جنگ سایبری یا دستورالعمل تالین، که از روندی کارشناس‌محور نشأت گرفته در پی سندی غیرالزام‌آور جهت بسط قواعد موجود به جنگ سایبری و همچنین تلاش جهت شفاف‌سازی بیشتر اسناد منتشره شده پیرامون اقدامات سایبری از سوی دولت‌ها و با توجه خاص به قوانین حقوق بر جنگ و حقوق در جنگ است. بنابراین دستورالعمل تالین به بررسی حقوق حاکم بر جنگ سایبری پرداخته و به‌طور کلی در برگیرنده حقوق بر جنگ، حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به‌عنوان ابزار سیاست ملی، و حقوق در جنگ، حقوق بین‌الملل تنظیم کننده رفتار درگیری‌های مسلحانه (که با عنوان حقوق جنگ، حقوق مخاصمات مسلحانه یا حقوق بین‌الملل بشردوستانه نیز شناخته می‌شود) است (صلاحی و کشفی، ۱۳۹۵: ۳۶).

تأکید دستورالعمل تالین، در معنای دقیق، بر اقدامات سایبری علیه تجهیزات سایبری، به‌عنوان مثال به کارگیری اقدامات سایبری علیه زیرساخت‌های حیاتی یک دولت یا حمله سایبری با هدف سامانه‌های کنترلی و فرماندهی دشمن است. همچنین این دستورالعمل توسل و تهدید به توسل به زور را در اقدامات سایبری تعریف نموده و هردوی آنان را ممنوع دانسته است. چنین اقداماتی مغایر اصل تمامیت ارضی و استقلال سیاسی کشورها و همچنین اهداف سازمان ملل تلقی شده‌اند. تأثیرات و اندازه اقدامات سایبری به جهت اطلاق به توسل به زور و غیرقانونی خواندن آنان را باید با اقدامات غیرسایبری در سطح توسل به زور مقایسه نمود (صلاحی و کشفی، ۱۳۹۵: ۴۰). بنابراین این دستورالعمل را می‌توان نمونه‌تقریبا جامعی از جرم‌انگاری و قانون‌گذاری در پدیده سایبری در سطح بین‌الملل دانست (صلاحی و کشفی، ۱۳۹۵: ۳۶).

1. Tallinn Manual
2. Cooperative Cyber Defence Centre of Excellence

6. کنوانسیون بوداپست در خصوص جرایم سایبری

شورای اروپا- که در سال ۱۹۴۹ و با هدف ترویج و تقویت همکاری میان کشورهای عضو تشکیل شد- تا به امروز رویکرد منسجم و متمرکزی را در قبال پرداختن به موضوعات مربوط به حوزه امنیت سایبری به‌ویژه جرایم سایبری اتخاذ کرده است. شورای اروپا در گام نخست و در راستای هنجارمند نمودن مباحث مربوط به جرایم ارتکابی در فضای سایبر، اقدام به تدوین و تصویب نخستین معاهده بین‌المللی لازم‌الاجرا با عنوان «کنوانسیون جرایم سایبری» یا «کنوانسیون بوداپست» در سال ۲۰۰۱ کرد و از این طریق سیاست و خط‌مشی کیفری خود را در راستای حمایت از قربانیان جرایم سایبری اعلام نمود. از جمله جرایم سایبری مندرج در کنوانسیون مزبور می‌توان به دسترسی غیرقانونی، مداخله در سیستم و مداخله در داده‌ها اشاره کرد. شایان ذکر است که کنوانسیون مزبور جرم سایبری را با اتکاء بر ابزارهایی همچون سیستم یا شبکه رایانه‌ای توصیف می‌کند. بدین ترتیب، جرایم سایبری شامل طیف وسیع و گسترده‌ای از فعالیت‌های غیر مجاز می‌شود. قواعد کنوانسیون مذکور در واقع با تکیه بر مصادیق جرایم سایبری به‌عنوان افعال و اقدامات مجرمانه و کیفری قابل تعقیب، صرفا مرتکبین این دسته از جرایم را که اصولاً افراد هستند مورد تعقیب و پیگیری قرار می‌دهد و از این‌رو اقدامات سایبری دولت‌ها داخل در صلاحیت کنوانسیون نمی‌باشد (اصلانی، ۱۳۹۵: ۶۹).

نکته دیگر اینکه برخلاف حملات سایبری، لازم نیست که جرایم سایبری منجر به تخریب شبکه رایانه‌ای هدف شده و یا دارای اهداف امنیتی، سیاسی و ملی باشند. همچنین در حین ارتکاب حمله یا جرم سایبری در واقع نمی‌توان به سادگی تشخیص داد که آیا حمله صورت گرفته مصداق یک جرم سایبری است یا مصداق یک حمله سایبری؛ چرا که هویت و هدف عامل حمله به‌راحتی قابل تشخیص نیست و از این جهت چنین عدم‌قطعیتی در تشخیص، بر اعمال صلاحیت کنوانسیون و یا عدم اعمال آن و همچنین بر نحوه واکنش به حمله صورت گرفته به‌عنوان یک حمله سایبری یا جرم سایبری تاثیر می‌گذارد. با این اوصاف، کنوانسیون جرایم سایبری شورای اروپا نیز حدود حمله سایبری را مشخص نکرده و صرفاً به بحث جرم‌انگاری مصداقی در سطح ملی به‌عنوان جرایم کیفری قابل ارتکاب توسط افراد و نه دولت‌ها پرداخته است. وجود این کنوانسیون به هر ترتیب می‌تواند نقطه آغاز و چارچوب و مدل مناسبی برای طراحی و تدوین یک سند جامع بین‌المللی جهت غیرقانونی تلقی کردن حملات سایبری باشد (اصلانی، ۱۳۹۵: ۷۰).

7. حلقه رهبری و معیار کنترل موثر

برخلاف بند اول ماده ۸ مکرر اساسنامه که شامل یک شخص می‌شود، حلقه رهبری بیش از یک شخص را در برمی‌گیرد. یعنی گروهی از اشخاص که در یک سمت رسمی قرار دارند و تحت رهبری یک دولت، اَعمالی را انجام می‌دهند. برپا کردن جنگ‌های تجاوزکارانه نه تنها یک عمل نظامی گروهی را می‌طلبد، بلکه طراحی و برنامه‌ریزی آن عملیات‌ها باید در حلقه رهبری انجام شود. اما چه کسی متعلق به این حلقه رهبری می‌باشد که قادر است یک جنگ تجاوزکارانه را برپا کند؟ حقوق موضوعه دادگاه نورنبرگ معیار «ایجاد یا تاثیرگذاری»[1] را بیان می‌کند که بر قدرت و نفوذ مجرمان جهت ایجاد یا تاثیرگذاری بر سیاست دولت‌ها متمرکز می‌شود (Ambos, 2016: 497). این معیار توسط گروه کاری ویژه‌ی جنایت تجاوز[2]رد شد. این گروه کاری بیان کرد که معیار «ایجاد یا تاثیرگذاری» گسترده‌تر از معیار کنترل موثری است که بعداً در ماده ۸ مکرر اساسنامه اتخاذ می‌شود. معیار کنترل موثر عناصر مختلفی را در بر می‌گیرد که برای ارزیابی دقیق اشخاص متعلق به حلقه رهبری مناسب می‌باشد (Ibid: 498). در ابتدا، این معیار بر کنترل موثر ماموران دوفاکتو تاکید می‌کند و می‌تواند به‌وسیله تئوری‌های پیشرفته کنترل که در رابطه با ارتکاب غیرمستقیم و دکترین«مسئولیت سران»است، ایجاد شود. بنابراین، ماموران عالی‌رتبه نظامی باید نه‌تنها قدرت ماموران دوژوره بلکه قدرت ماموران دوفاکتو را نیز در اختیار بگیرند و بتوانند کنترل نهایی یا هدایت خود را بر اعمال نظامی یا سیاسی آنها اعمال دارند. دوم، این اشخاص باید «کنترل» یا «هدایت» خود را بر عمل نظامی یا سیاسی یک دولت اعمال کنند.

«کنترل» به وظایف نظارتی مافوق در زمینه دکترین «مسئولیت سران» (مسئولیت ترک فعل یعنی فقدان یک نظارت مناسب) مربوط است. در خصوص «هدایت»، مرتکب نقش فعال‌تری را بازی می‌کند. یعنی به‌صورت فعال، عمل تجاوز را هدایت می‌نماید. سوم، «کنترل موثر» به عمل نظامی یا سیاسی دولت مربوط می‌شود. یعنی کنترل سیاست تجاوزگرانه یا اجرای این سیاست در راستای یک برنامه نظامی، کفایت می‌کند. چهارم، معیار کنترل موثر، شخصیت‌های مهم و برجسته غیر سیاسی را مستثنی نمی‌کند حتی اگر آنها در محدوده آن استاندارد، کنترل کافی را اعمال دارند (Ibid). بنابراین اشخاصی که به حلقه رهبری تعلق داشته باشند، طبیعتاً باید کنترل موثر خود را اعمال کنند، همچنین اشخاصی که خارج از این حلقه قرار دارند ممکن است با چنین

1. Shape or Influence
2. The Special Working Group on the Crime of Aggression

کنترل موثری سروکار داشته باشند و تنها به خاطر ارتکاب جرم تجاوز متحمل مسئولیت شوند. در پرونده کروپ گروهی از اشخاص به‌دلیل ارتکاب جنایاتی علیه صلح و مشارکت در توطئه نازی‌ها متهم شناخته شده بودند؛ ولی در نهایت تبرئه همه متهمان در پرونده‌های کروپ و فاربن با توجه به جنایت‌های انجام گرفته علیه صلح مشخص می‌کند که اثبات مسئولیت شخصی افرادی که به حلقه رهبری یک رژیم جنایتکار متعلق نبودند، تا چه حد سخت و دشوار است. در پرونده فاربن تبرئه متهمان به دو دلیل صورت گرفت: اول این‌که آن‌ها تأثیر واقعی بر سیاست‌های تجاوزگرانه اعمال نکرده بودند، دوم آن‌ها از برنامه‌های تجاوزگرانه هیتلرآگاهی نداشتند. در پرونده کروپ، مسئله تقصیر شخصی اهمیت داشت، ولی این موضوع به اندازه کافی مورد بررسی قرار نگرفت (Farben case,1952). نهایتاً اثبات این‌که آیا اشخاص موجود در حلقه‌ی رهبری کنترل کافی بر سیاست تجاوزگرانه‌ای که مستلزم آگاهی لازم باشد، را اعمال می‌کنند یا خیر، بسی سخت و دشوار است.

۱-۷. پرونده فاربن[1]

در فاربن، ۲۴ نفر از اعضای هیئت مدیره برای طرح‌ریزی، آماده‌سازی، آغاز و برپایی جنگ‌های تجاوزکارانه و همچنین به دلیل مشارکت در یک طرح مشترک یا توطئه و ارتکاب جنایت علیه صلح متهم شناخته شدند. تولید انبوه لاستیک مصنوعی، گازولین، فلزات سبک، مواد منفجره و سلاح‌های شیمیایی برای برنامه‌های تجاوزکارانه نازی‌ها کاری خطرناک و حساس بود. قاضی هربرت[2] بیان کرد که «فاربن به طور گسترده زمینه تولید مواد خام را ایجاد کرده و اگر این کار انجام نمی‌شد، دادگاه نمی‌توانست به طور جدی چنین سیاستمدارانی را به برپایی جنگ تجاوزکارانه متهم سازد» (Farben case,1952: para 1216). با این حال، دادگاه نظامی نورنبرگ همه متهمان را تبرئه کرد (Ibid: para 1206- 1209). دادگاه از یک طرف به طور صریح میان برپایی جنگ تجاوزکارانه و طرح‌ریزی، آماده‌سازی یا آغاز جنگ تمایز قائل شده بود. از طرفی دیگر نتوانست متهمان را به برپایی جنگ تجاوزکارانه محکوم کند زیرا آنها به‌عنوان مجری، نه یک رهبر، در اجرای طرح‌های توطئه‌آمیز نازی‌ها مشارکت داشتند. به عبارت دیگر،

1. Farbencase
2. Herbert

متهمان، در حکومت داخلی نه جزء مقامات برجسته و عالی‌رتبه و نه از افسران نظامی رده بالای دولتی بودند (Heller, 2007: 483).

۲-۷. پرونده کروپ[1]

در این پرونده، ۱۲ مقام عالی‌رتبه کارخانه کروپ به دلیل ارتکاب جنایت علیه صلح و مشارکت در یک طرح مشترک یا توطئه محکوم شده بودند (Krupp case,1952: para 391). کروپ یک کارخانه سازنده توپخانه، زره‌های جنگی، تانک‌ها و زیردریایی‌های آلمان در طول جنگ جهانی دوم و یکی از مهمترین مشارکت‌کنندگان در جنگ آلمان بود (Ibid: para 404). علیرغم این موضوع، دادگاه نظامی نورنبرگ حکم تبرئه متهمان این جنایت را در پرونده «پیگرد قانونی»[2] صادر کرد. دادگاه سوالی را مطرح کرد: «آیا می‌توان متهمان را به‌دلیل انجام جنایت‌هایی که قبل از اول سپتامبر ۱۹۳۹ صورت گرفته بود و اینکه آگاهانه در توطئه نازی‌ها جهت برپایی جنگ تجاوزکارانه مشارکت داشته و به پیشبرد جنگ و تهاجم کمک کرده‌اند، محکوم کرد»؟ (Ibid). دادگاه اظهار داشت که «متهمان، شهروندان خصوصی و غیرجنگجو بودند و هیچ‌یک از آن‌ها از سیاستی که دولتشان را به‌سمت یک جنگ تجاوزکارانه پیش می‌بُرد اطلاعی نداشته و در اجرای آن توطئه مشارکت نداشته‌اند، همچنین هیچ‌کدام کنترلی بر جنگ تجاوزکارانه یا بر نیروهای مسلح اعمال نکرده‌اند» (Ibid: para 449). با این حال متهمان به‌دلیل عدم آگاهی از برنامه‌های تجاوزکارانه نازی‌ها تبرئه شدند و نه به‌دلیل مستثنی کردن آن‌ها از ارتکاب جنایت به‌عنوان یک موضوع حقوقی در سِمت بازیگران خصوصی اقتصادی.

۸. شرط رهبری و مسئولیت کیفری فردی مقامات عالی‌رتبه نظامی

ماده ۲۵ اساسنامه دیوان بین‌المللی کیفری یک ماده اساسی در بررسی روش‌های مشارکت است. بر این اساس می‌توان گفت که مشارکت برای اشخاصی به‌کار می‌رود که در یک سِمت رسمی به‌طور موثر کنترل خود را بر عمل نظامی یا سیاسی یک دولت اعمال می‌کنند و یا آن عمل را هدایت می‌نمایند. این اشخاص باید اساساً به حلقه‌ی رهبری تعلق داشته باشند. بنابراین آن‌ها از لحاظ کیفری ممکن است با توجه به بند ۳ ماده ۲۵ اساسنامه مسئول شناخته شوند (,Ambos

1. Krupp case
4. Prosecution

2016: 502). حال اگر میان ارتکاب جرم و مشارکت در جرم تمایز وجود داشته باشد، باید گفت که جرم تجاوز باید براساس مرتکبان اصلی آن جرم تعیین شود، نه با توجه به شرکای جرم. به عبارت دیگر، شرط رهبری نه شامل اشخاصی می‌شود که متعلق به تراز رهبری نیستند و از مسئولیت معافند و نه شرکای جرم با وجود اعمال کنترل کافی. اشخاص متعلق به حلقه‌رهبری با اعمال کنترل موثر کاملاً مشمول بند ۳ ماده ۲۵ اساسنامه دیوان بین‌المللی کیفری هستند. این بدان معناست که در پیرامون حلقه رهبری، تفاوت کلاسیک میان ارتکاب جرم و مشارکت در جرم وجود دارد. ممکن است مرتکبان اصلی جرمدر یک سمت رسمی با شرکای خود همکاری داشته باشند و یا آن‌ها با تسلط بر زیردستان خود به‌طور غیرمستقیم جرمی را مرتکب شده و یا آن اشخاص را به انجام جرم، تحریک و ترغیب نمایند. در هر صورت مسئولیت کیفری مرتکبان اصلی جرم محرز است (Ibid).

مسئولیت کیفری فردی برای جرم تجاوز شامل عنصر مادی و عنصر روانی است. بنابراین اشخاص موجود در حلقه رهبری که در برنامه‌های یک جنگ تجاوزگرانه مشارکت دارند، در صورتی که اعمالشان برخلاف قواعد حقوق بین‌الملل و از روی آگاهی و قصد باشد، مسئولیت کیفری آن‌ها محرز خواهد بود. قطعنامه ۱۹۷۴ مجمع عمومی سازمان ملل متحد نمونه‌های خاصی از اعمال تجاوز را فهرست‌بندی و تعریف تجاوز را به‌صورت جدی دنبال کرد. بند ۲ ماده ۵ قطعنامه مقرر می‌دارد که «یک جنگ تجاوزگرانه جنایت علیه صلح بین‌المللی است و منجر به مسئولیت بین‌المللی می‌شود» (Hajdin, 2015: 21). ماده ۱ قطعنامه یک تعریف کلی از تجاوز را ارائه می‌دهد: «تجاوز عبارت است از استفاده از نیروهای مسلح یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر یا در هر حالت دیگری که با منشور سازمان ملل متحد ناسازگار باشد[1]». ماده ۳ قطعنامه همچنین فهرستی از اعمال تجاوزکارانه را تهیه می‌کند که شامل «تهاجم یا حمله، بمباران سرزمین دولت دیگر، محاصره بنادر یا سواحل یک دولت توسط نیروهای مسلح دولت دیگر» است[2]. هر یک از این اعمال صرفنظر از اعلام جنگ، باید مطابق با قطعنامه ۳۳۱۴ مجمع عمومی به‌عنوان یک عمل تجاوز تعیین شوند. پایه و اساس قطعنامه ۱۹۷۴، منشور ملل متحد است که چارچوب تعریف عمل تجاوز را ایجاد می‌کند. فهرست

1. Art 1 of the "Definition of Aggression" ,annexed to the 1974 Resolution
2. Art 3 of the "Definition of Aggression" ,annexed to the 1974 Resolution

ذکر شده در ماده ۳ قطعنامه در هدایت شورای امنیت برای تصمیم‌گیری در خصوص استفاده نادرست از زور که منجر به اعمال تجاوزکارانه می‌شود، به‌کار گرفته شده است.

بند ۱ ماده ۸ مکرر اساسنامه در تبیین عنصر مادی مقرر می‌دارد: «جنایت تجاوز یعنی برنامه‌ریزی، آمادگی، شروع یا اجرای یک عمل تجاوزکارانه». اعمال تجاوزکارانه نیز اعمالی هستند که در قسمت دوم بند ۲ ماده ۸ مکرر احصا شده‌اند. بنابراین می‌توان گفت که عنصر مادی جنایت تجاوز عبارت است از: «برنامه‌ریزی، آماده‌سازی، شروع یا اجرای یکی از اقدامات دارای کیفیات تجاوزکارانه». در ماده مذکور، شروع به اجرای هریک از اقدامات دارای کیفیات تجاوزکارانه نیز برای تحقق جنایت تجاوز کافی دانسته شده است. بنابراین تمام مصادیق مذکور در بند یک و دو ماده ۸ مکرر از نوع فعل مثبت مادی هستند (آقایی جنت‌مکان، ۱۳۹۰: ۱۷۳-۱۷۲). مسئولیت کیفری فردی در تعریف قطعنامه ۱۹۷۴ در خصوص تجاوز گنجانده نشده است. در ابتدا قطعنامه به سمت مسئولیت دولت‌ها متمایل شده بود ولی هیچ عاملی در خصوص عنصر معنوی جرم تجاوز در تعریف وجود نداشت. بنابراین نمی‌توان این تعریف را اساس تعیین مسئولیت کیفری فردی در رابطه با جرم تجاوز دانست (Hajdin, 2015: 22).

در دوره قبل از کنفرانس کامپالا، رای دادگاه نظامی بین‌المللی یک منشا اساسی در رابطه با مسئولیت کیفری فردی برای جرم تجاوز بود. این دادگاه اعلام کرد که عنصر روانی به‌همراه عنصر مادی بخش اساسی جرم تجاوز را تشکیل می‌دهند. کریانگساک کیتی چایساری[1] تصریح کرد که عنصر معنوی جرم تجاوز شامل قصد و آگاهی از عمل تجاوز است (Kittichaiseree, 2001: 221). او پرونده «فرماندهی عالی[2]» را به‌منظور اثبات دیدگاهش بیان کرد. دیوان نظامی آمریکا بیان داشت که «اشخاصی که به ارتکاب جرم تجاوز متهم شده‌اند، باید از جنگ تجاوزگرانه که در شرف وقوع است آگاهی داشته و یا اینکه اگر جنگی قرار است آغاز شود بتوان آن را یک جنگ تجاوزگرانه محسوب کرد. به‌علاوه آن اشخاص بعد از کسب آگاهی باید در یک موقعیت رسمی با ایجاد یا تاثیرگذاری بر سیاست تجاوزگرانه یک دولت باعث شروع و برپایی جنگ شوند که در این صورت می‌توان آن‌ها را از لحاظ کیفری مسئول دانست و یا ممکن است مانع از اجرا یا خنثی‌سازی چنین سیاست تجاوزگرانه‌ای شوند که عمل آن‌ها با توجه به چنین سیاستی فقدان قصد کیفری می‌باشد» (High Command case,1950).

1. KriangsakKittichaiseree
2. HighCommandCase

ماده ۳۰ اساسنامه دیوان بین‌المللی کیفری جز در موارد استثنایی، قصد و علم را همراه با عنصر مادی جرم ضروری می‌داند. بنابراین برای ارتکاب جنایت تجاوز و اقدامات تجاوزگرانه وجود قصد و آگاهی از این اعمال ضروری است. همچنین بند ۴ از عناصر جنایت تجاوز از ضمیمه‌ی دوم اصلاحات عناصر جرائم ماده ۸ مکرر، به وجود آگاهی از اقدامات تجاوزکارانه اشاره کرده: «مرتکب از شرایط و اوضاع و احوال واقعی که مغایرت چنین استفاده‌ای از یک نیروی مسلح را با منشور ملل متحد مسلم می‌دارد، آگاهی داشته باشد» (آقایی جنت‌مکان، ۱۳۹۰: ۱۷۳).

تاکید بر این موضوع حائز اهمیت است که وقوع عمل تجاوزگرانه به‌صورت اتوماتیک منجر به مسئولیت کیفری اشخاصی که در اینگونه اعمال مشارکت دارند، نمی‌شود (Ambos, 2011: 482). حداقل وجود سه شرط برای تحقق چنین مسئولیتی لازم و ضروری است. در ابتدا ضابطه‌های ماهیت، شدت و گستره‌عمل تجاوزگرانه باید تا حدی باشد که بتوان آن را نقض آشکار منشور ملل متحد دانست. دوم معیار «کنترل یا هدایت» مؤثر باید توسط فرماندهان و مقامات عالی‌رتبه نظامی یک دولت اعمال شود. نهایتاً برای تحقق مسئولیت کیفری باید مشارکت و دخالت آن اشخاص در طرح‌ریزی، آماده‌سازی، آغاز یا اجرای عمل تجاوزکارانه به اثبات رسیده باشد (Sayapin, 2014: 257). درحالی‌که عمل تجاوزگرانه در قطعنامه مجمع عمومی تعریف شده بود ولی حداقل دو نوآوری در بند ۱ ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری وجود داشت (Ambos, 2011: 466-467). اول این‌که برای تحت تعقیب قرار دادن متهمان به دلیل ارتکاب جرم تجاوز، باید آستانه‌ای با توجه به ماهیت، شدت و گستره عمل تجاوز مشخص شود تا بتوان عمل تجاوز را نقض آشکار منشور ملل متحد تلقی کرد. نوآوری دوم این بود که جرم تجاوز باید تنها به‌وسیله اشخاصی انجام شود که در یک موقعیت رسمی کنترل خود را بر سیاست دولت اعمال و یا آن را هدایت می‌کنند که در این صورت موجبات مسئولیت کیفری آن‌ها فراهم می‌شود. با توجه به رای دادگاه‌های نورنبرگ و توکیو، قضات معتقد بودند که افسران رده‌پایین دولتی را نباید مسئول جرم تجاوز تلقی کرد. زیرا آن‌ها فاقد عنصر معنوی جرم هستند (Heller, 2007: 478).

در نتیجه، سربازان عادی را نمی‌توان مسئول جرم تجاوز دانست (Gillet, 2013: 860). یعنی آن‌ها در اکثر پرونده‌ها با توجه به موقعیتشان از قصد و نیت تجاوزگرانه فرماندهان عالی‌رتبه خود آگاهی نداشتند. در قرن نوزدهم، سرباز، ابزاری مثل سایر آلات جنگی محسوب می‌شد،

بنابراین وظیفه‌ای جز اطاعت کامل از اوامر مافوق نداشت. اپنهایم[1] در کتاب خود تحت عنوان «حقوق بین‌الملل»، که برای اولین بار در سال ۱۹۰۶ چاپ شد، گفت که تنها فرماندهان به‌دلیل نقض مقررات جنگی مسئولیت کیفری دارند و سربازان، چون چاره‌ای جز اطاعت ندارند، مسئولیتی نیز در این باره نخواهند داشت (میرمحمد صادقی، ۱۳۸۳: ۲۰۴). بنابراین معمولاً تنها افسران و مقامات عالی‌رتبه از برنامه‌های تجاوزگرانه یک دولت آگاهی دارند و می‌توانند مسئول آن اعمال باشند.

در خصوص تجاوز سایبری یا حملات مسلحانه که توسط یک دولت هدایت می‌شود، مسئولیت کیفری فردی به اشخاصی که در یک سمت رسمی متعلق به حلقه رهبری هستند و هدایت و کنترل موثر خود را بر سیاست تجاوزگرانه دولت اعمال می‌دارند، تعلق می‌گیرد و مسئولیت کیفری آنها محرز است. ولی ممکن است آن‌ها در مورد یک حمله شبکه‌ای رایانه‌ای هیچ اطلاعی نداشته باشند و یا آگاهی ناچیزی داشته باشند و هدایت آن‌ها در حد صادر کردن یک دستور جهت برپا کردن یک حمله شبکه‌ای رایانه‌ای باشد، همچنین این امکان وجود دارد که آن‌ها نتوانند به درستی آن حمله را به دلیل فقدان قابلیت‌های فنی، تحت هدایت و نظارت قرار دهند (Ambos, 2016: 503). شخصی که در یک سمت رسمی دستور انجام یک عمل تجاوزگرانه را صادر و به‌طور موثر کنترل خود را بر آن عمل اعمال می‌کند، لازم نیست تا از جزئیات تکنیکی ابزار و وسایل مورد استفاده جهت اجرای دستوراتش، اطلاع داشته باشد. کافی است که فقط اطمینان حاصل کند که فرمان و دستورش تمام و کمال اجرا خواهد شد و نتایج زیان‌باری برای اهداف مورد نظرش خواهد داشت (Ibid: 504). یک مقام عالی‌رتبه ممکن است حتی نگران و دلواپس انجام آن اقدام تجاوزگرانه هم نباشد، بدین معنی که از انجام چنین حمله‌ای توسط زیردستان خود مطمئن است. از طرفی ممکن است حتی اتخاذ تصمیم در خصوص صادر کردن دستور حمله به هدف مورد نظر و به بارآوردن خسارات گسترده با هر وسیله ممکن را به زیردستان خود محول کند. بنابراین مسئولیت کیفری فردی مقامات عالی‌رتبه بستگی به ابزار مورداستفاده جهت اجرای دستورات یا آگاهی از جزئیات به‌کارگیری آن ابزار با توجه به پیامدهای زیان‌بار آن‌ها ندارد. از طرف دیگر ارزیابی و در نظر گرفتن عنصر معنوی در حملات شبکه‌ای رایانه‌ای معمولاً دشوار و به راحتی امکان‌پذیر نیست، به‌خصوص این موضوع بیشتر در مواردی

1. Oppenheim

صدق می‌کند که بعضی عواقب خاص قصد می‌شود ولی عواقب دیگری که طی آن جریانات نیز به طور عادی دور از انتظار نیست، رخ می‌دهد. حال سوالی که در این‌جا مورد توجه قرار می‌گیرد این است که آیا افراد برای عواقب قصد نشده‌ای که از حملات ناشی می‌شوند، مسئوول هستند؟ به عبارت دیگر عواقب مذکور مورد قصد حمله کنندگان نبوده‌اند ولی این‌گونه عواقب در آن حملات قابلیت پیش‌بینی را داشته‌اند. آیا شدت در این عواقب باعث آشکار بودن عمل تجاوز می‌شود؟ به‌نظر می‌رسد در این‌گونه موارد اگرچه ماهیت آن اقدام با خود عواقب وخیمی به همراه دارد ولی عنصر معنوی به طور خاص باید وجود داشته باشد (اسماعیل‌زاده ملاباشی، ۱۳۹۶: ۵۹-۶۰). نگارندگان بر این باورند که با توجه به شرط رهبری، اگر شخصی دارای یک موقعیت رسمی باشد و به‌طور موثر برنامه‌های سیاسی و نظامی دولت را کنترل و یا هدایت نماید، می‌توان او را از لحاظ کیفری مسئول دانست. اگرچه ارزیابی عنصر معنوی در حملات شبکه‌ای رایانه‌ای دشوار و به‌راحتی امکان‌پذیر نیست ولی می‌توان گفت که وجود این عنصر به همراه عنصر مادی برای تحقق مسئولیت کیفری فردی مقامات عالی‌رتبه نظامی برای انجام جرم تجاوز سایبری لازم و ضروری است. بنابراین تنها مقامات عالی‌رتبه نظامی را می‌توان شخصاً مسئول دانست. زیرا تنها آن‌ها هستند که از برنامه‌های تجاوزکارانه دولت آگاهی دارند.

9. صلاحیت دیوان بین‌المللی کیفری در رسیدگی به جرم تجاوز سایبری

دیوان بین‌المللی کیفری اولین و در حال حاضر تنها دیوان بین‌المللی است که صلاحیت رسیدگی به جرایم بین‌المللی را دارد. مطابق با اساسنامه این دیوان، صلاحیت دیوان بین‌المللی کیفری محدود به شدیدترین جرایمی که قابل انتساب به اشخاص هستند، است.به موجب ماده ۵ اساسنامه، دیوان نسبت به رسیدگی به ۴ جرم صلاحیت خواهد داشت: ۱- نسل‌کشی (کشتار جمعی)[1] ۲- جرائم علیه بشریت[2] ۳- جرائم جنگی[3] ۴- تجاوز[4]. با وجود این، اعضای شورای امنیت سازمان ملل متحد تمایلی به قراردادن جنایت تجاوز در صلاحیت دیوان بین‌المللی کیفری را نداشتند زیرا بر اساس فصل هفتم منشور ملل متحد وظیفه حفظ و برقراری صلح و امنیت

1. Genocide
2. Crimes against humanity
3. War crimes
4. Aggression

بین‌المللی و جلوگیری از تجاوز و احراز آن با شورای امنیت بود و اعضای دائم شورای امنیت تمایلی به واگذاری اختیارات خود به دیوان بین‌المللی کیفری نداشتند (اسماعیل‌زاده ملاباشی، ۱۳۹۶: ۴۷).

در کنفرانس رم، نیز پافشاری و استدلال کشورهایی نظیر جمهوری اسلامی ایران، هند و مکزیک در مخالفت با صلاحیت شورای امنیت نسبت به رسیدگی یا تشکیل دادگاه رسیدگی کننده از سوی شورای مزبور به این راه‌حل بینابینی منجر شد که صلاحیت دیوان نسبت به رسیدگی به جرم تجاوز شناسایی شود. سرانجام اعمال آن موکول به تعریف تجاوز شد (شریعت‌باقری، ۱۳۷۷: ۸۶). به منظور ایجاد تعادل بین دیدگاه‌های مختلف کشورها در مورد صلاحیت دیوان در رسیدگی به جرایم مربوط به تجاوز، نهایتاً مطابق با ماده‌ی ۵ اساسنامه رم صلاحیت رسیدگی به این جرم به دیوان واگذار گردید ولی تعریف جنایت تجاوز به آینده موکول شد (اسماعیل‌زاده ملاباشی، ۱۳۹۶: ۴۷). در کنفرانسی که در سال ۲۰۱۰ کامپالا به منظور بازنگری اساسنامه دیوان بین‌المللی کیفری تشکیل شد، اعضای شرکت کننده در کنفرانس مذکور تصمیماتی را در خصوص تعریف عمل متجاوزانه و جنایت تجاوز اتخاذ نمودند و صلاحیت رسیدگی دیوان به جرم مذکور را به طور بالقوه حتی در صورتی که شورای امنیت موضوعی را به دیوان ارجاع ننماید، در نظر گرفتند (همان: ۵۱). مطابق با ماده ۵ اساسنامه دیوان بین‌المللی کیفری مقرر شده که دیوان زمانی صلاحیت خود را در مورد جنایت تجاوز اعمال می‌کند که مقرره‌ای مطابق با مواد ۱۲۱ و ۱۲۳ اساسنامه دیوان در خصوص تعریف جنایت تجاوز تصویب شود و شرایطی که وفق آن دیوان در خصوص این جرم اعمال صلاحیت می‌کند، مشخص شود. ضمن اینکه مطابق با ماده مذکور چنین مقرره‌ای باید با مقررات مربوطه در منشور ملل متحد سازگار باشد (همان :۴۹). از یکسو مطابق مفاد صریح ماده ۲۴ منشور ملل متحد، شورای امنیت به‌عنوان مسئول اصلی حفظ صلح و امنیت بین‌المللی، در احراز وقوع عمل تجاوز دارای اولویت و تقدم است و از سوی دیگر در صورت امتناع شورای امنیت از احراز وقوع عمل تجاوز، رسیدگی دیوان کیفری به جنایت تجاوز با بن‌بست مواجه می‌شود (شایگان‌فرد، ۱۳۸۷: ۲۷۳).

بنابراین به‌منظور ایجاد راه‌حلی متعادل، که هم از یک‌سو امکان عملی برای انجام وظایف دیوان بین‌المللی کیفری در رسیدگی به جنایت تجاوز را فراهم کند و هم از سوی دیگربا مقررات منشور ملل متحد در مورد مسئولیت اولیه و اصلی شورای امنیت در حفظ صلح و امنیت بین‌المللی

هماهنگ باشد، طرح‌های متعددی[۱] در جریان کنفرانس رم و نیز در نشست‌های متعدد کمیسیون مقدماتی برای دیوان توسط نمایندگان کشورهای شرکت‌کننده، مطرح شد. در هر کدام از این طرح‌ها دیوان بین‌المللی کیفری در صورت وصول شکایت در مورد تجاوز، ابتدا به مسئولیت اولیه و اساسی شورای امنیت توجه کرده و در خصوص این‌که آیا این شورا وقوع عمل تجاوز را احراز کرده یا خیر تحقیق و تفحص خواهد نمود، سپس در صورت عدم احراز عمل تجاوز و عدم اتخاذ تصمیم در این مورد توسط شورا، دیوان کیفری باید به شورای امنیت موضوع را اطلاع داده و درخواست اتخاذ تصمیم مقتضی توسط شورا را از آن بنماید (همان).

اگر شورای امنیت وقوع عمل تجاوز را احراز کند، دیوان کیفری با توجه به احراز وقوع عمل تجاوز، شروع به رسیدگیمی‌کند. ولی اگر دیوان احراز نماید که حمله صورت گرفته تجاوز نبوده و یا اهمیت آن در حدی نبوده که احراز عمل تجاوز را توجیه کند، در آن صورت دیوان نمی‌تواند به شکایت مربوطه رسیدگی کند، چرا که ارتکاب جنایت تجاوز مستلزم وقوع قبلی عمل تجاوز است. حال اگر شورای امنیت نتوانست هیچ تصمیمی در خصوص وقوع یا عدم وقوع عمل تجاوز اتخاذ کند، در آن صورت خود دیوان مجاز خواهد بود به شکایت مطروحه مبنی بر ارتکاب جنایت تجاوز رسیدگی کند. بنابراین اقدام دیوان در رسیدگی به جنایت تجاوز پس از اطمینان از عدم امکان اتخاذ تصمیم توسط شورای امنیت، کاملا در راستای منشور و اهداف ملل متحد است (شایگان فرد، ۱۳۸۷ :۲۷۵). در ماده ۱۵ مکرر قطعنامه کنفرانس بازنگری، شرایط اعمال صلاحیت دیوان بر جنایت تجاوز مطرح شده است که عمده ترین ویژگی‌های آن شامل موارد زیر است: ۱- اعمال صلاحیت دیوان در اثر ارجاع وضعیت توسط یک دولت عضو. ۲- عدم صلاحیت دیوان نسبت به دولت‌های عضو که از پذیرش صلاحیت دیوان انصراف داده‌اند. ۳- اعمال صلاحیت دیوان نسبت به دولت‌های غیرعضو. دیوان در صورتی می‌تواند صلاحیت خود را بر جنایت تجاوز اعمال نماید که حداقل یکی از دولت‌هایی که در قلمرو آن، فعل یا ترک فعل مورد نظر روی داده باشد و یا دولتی که شخص مورد تحقیق یا تعقیب، تبعه آن است، عضو اساسنامه‌ی دیوان باشد یا صلاحیت دیوان را بر طبق بند ۳ ماده ۱۲ اساسنامه پذیرفته باشد (موسی‌زاده و فروغی‌نیا، ۱۳۹۱: ۱۵۸).

۱- از مهم‌ترین آن‌ها می‌توان به طرح کامرون در جریان کنفرانس رم، طرح مشترک یونان- پرتغال در جریان مباحث کمیسیون مقدماتی و طرح کلمبیا اشاره کرد.

در رابطه با انصراف دولت‌های عضو از صلاحیت دیوان در بند ۴ ماده ۱۵ مکرر آمده است: «دادگاه مطابق ماده ۱۲ اساسنامه، زمانی بر جنایت تجاوز اعمال صلاحیت می‌کند که عمل تجاوز ارتکابی به‌وسیله دولت عضو اساسنامه انجام شده باشد مگر این‌که آن دولت قبلا اعلامیه‌ای مبنی بر عدم پذیرش صلاحیت نزد دبیرخانه دیوان سپرده باشد (موسی‌زاده و فروغی‌نیا، ۱۳۹۱: ۱۵۹– ۱۵۸). درباره‌ی صلاحیت دیوان و وضعیت کناره‌گیری چند حالت قابل تصور است: حالت اول جنایات تجاوزکارانه‌ای که در زمان عضویت دولت و قبل از نافذ شدن کناره‌گیری، تحقیق یا تعقیب نسبت به آن‌ها شروع شده است. با توجه به بند ۲ ماده ۱۲۷ اساسنامه، کناره‌گیری به هیچ‌وجه آسیبی به ادامه رسیدگی به موضوع که توسط دیوان تحت بررسی بوده است، نخواهد رساند و لذا دیوان به رسیدگی خود ادامه می‌دهد. حال اگر در حین کناره‌گیری جنایات تجاوزکارانه‌ای در حال ارتکاب باشد و در رابطه با آن‌ها هیچ‌گونه رسیدگی آغاز نشده باشد، طبق ماده ۷۰ کنوانسیون وین در مورد حقوق معاهدات، دیوان حق آغاز رسیدگی بعد از کناره‌گیری را دارد . با این حال، کناره‌گیری تأثیری در اعمال صلاحیت دیوان به‌موجب ارجاع شورای امنیت یا پذیرش موردی دیوان توسط کشور مورد نظر ندارد (موسی‌زاده و فروغی‌نیا، ۱۳۹۱: ۱۶۰– ۱۵۹).

در ارتباط با دولت‌های غیرعضو اساسنامه دیوان، در بند ۵ قطعنامه آمده است: «در ارتباط با دولتی که عضو اساسنامه نیست، دادگاه بر جنایت تجاوزکارانه ارتکابی از طرف افراد متبوع یا در سرزمین دولت مزبور اعمال صلاحیت نخواهد کرد»(همان). نگارندگان در خصوص اعمال صلاحیت دیوان بر تجاوز سایبری معتقدند که دیوان باید قبلا وقوع عمل تجاوز توسط مقامات عالی‌رتبه نظامی را احراز کرده باشد و در این مورد باید آستانه تجاوز را مد نظر قرار داد. بدین صورت که اگر تبعات و آثار اینگونه حملات، ورود خسارت و صدمات فیزیکی نظیر تخریب سیستم‌ها و شبکه‌های رایانه‌ای در سطح گسترده باشد، می‌توان گفت که این حملات به آستانه‌ی تجاوز یا یک حمله مسلحانه رسیده است. به عبارت دیگر اگر ماهیت، شدت و گستره این‌گونه حملات در حدی باشد که منجر به تخریب و ازهم گسیختگی زیرساخت‌های ملی و حساس یک دولت شود و خسارات قابل توجهی را در سطح وسیعی به بار آورد، می‌توان آن حمله را نقض آشکار منشور ملل متحد دانست و به‌عنوان تجاوز در دیوان بین‌المللی کیفری مورد رسیدگی قرار داد.

10. نتیجه‌گیری

حملات شبکه‌ای رایانه‌ای که در آستانه تجاوز سایبری قرار می‌گیرند، می‌توانند منجر به نقض آشکار منشور ملل متحد شوند و درصورتیکه مقامات عالی‌رتبه نظامی در یک حلقه رهبری به طور موثر کنترل خود را بر اعمال سیاسی یا نظامی دولت اِعمال و یا آن اَعمال را هدایت کنند، مسئولیت کیفری آن‌ها محرز خواهد بود. برای تحقق مسئولیت کیفری فردی باید هم عنصر مادی و هم عنصر معنوی جرم وجود داشته باشد. یعنی مقامات عالی‌رتبه نظامی هم باید در برنامه‌ریزی، آماده‌سازی، شروع یا اجرای اقدامات تجاوزکارانه مشارکت داشته باشند و هم از اجرای آن اقدامات مطلع باشند. ولی ممکن است آن‌ها در مورد این حملات اطلاعات فنی و تکنیکی نداشته باشند و هدایت و رهبری آن‌ها ممکن است صرفاً شامل صدور فرمان برای راه انداختن و آغاز یک حمله‌ی سایبری باشد، و آن‌ها به‌دلیل فقدان قابلیت‌های فنی در این‌گونه حملات قادر به نظارت صحیح و درست نباشند، با این حال با توجه به ماده ۸ مکرر اساسنامه رم، به نظر می‌رسد یک مقام عالی‌رتبه که در موقعیت صدور دستور برای انجام اقدامی تجاوزکارانه است و به‌طور موثر بر آن اقدام کنترل دارد، لازم نیست که اطلاعات جزئی از حمله و ابزاری که توسط آن، حمله صورت می‌گیرد، داشته باشد. همین حد کفایت می‌کند که فقط اطمینان حاصل کند فرمان و دستورش تمام و کمال اجرا خواهد شد و نتایج زیان‌باری برای اهداف مورد نظرش خواهد داشت. با توجه به بند ۳ ماده ۲۵ اساسنامه می‌توان گفت که جرم تجاوز براساس مرتکبان اصلی جرم (مقامات و فرماندهان عالی‌رتبه نظامی) مشخص می‌شود نه با توجه به شرکای جرم (افسران رده‌پایین و سربازان عادی). بنابراین، در یک سیاست تجاوزکارانه، مسئولیت کیفری فردی مرتکبان اصلی جرم محرز است. دیوان در صورتی صلاحیت رسیدگی به جنایت تجاوز را دارد که قبلا وقوع آن جنایت را احراز کرده باشد. یعنی با توجه به ماهیت، شدت و گستره جنایت تجاوز که منجر به ورود خسارت و صدمات فیزیکی به زیرساخت‌های حساس و شبکه‌های رایانه‌ای یک دولت در سطح گسترده‌ای شده، می‌تواند به آن مساله رسیدگی کند.

۱۱. پیشنهادهای رسانه‌ای

۱) مهم‌ترین حملات سایبری که به‌طور خاص اهداف دولتی را هدف گرفته و بیشترین نمود و بازتاب خبری و رسانه‌ای داشته و علاوه بر این، بیشترین چالش حقوقی را از منظر حقوق بین‌الملل در پی داشته‌اند شامل حملات زیر هستند که شبکه‌های برون‌مرزی با پرداخت

جامع و بررسی کامل این حملات، می‌توانند ورود دیوان بین‌المللی کیفری در رسیدگی به اینگونه حملات را به یک مطالبه افکار عمومی جهان تبدیل کنند.

- انفجار لوله‌های انتقال گاز طبیعی شوروی سابق در دوران جنگ سرد (۱۹۸۲)
- حملات موسوم به «moonlight maze» که در یک بازه زمانی دو ساله (۲۰۰۰–۱۹۹۸) با هدف بررسی دقیق سیستم‌های رایانه‌ای پنتاگون، ناسا، وزارت انرژی و سایر بخش‌های خصوصی صورت گرفت که منجر به سرقت ده‌ها هزار فایل اطلاعاتی شد.
- حمله سال ۱۹۹۹ به شبکه تلفن یوگسلاوی سابق توسط ناتو در اثنای مخاصمات مسلحانه کوزوو.
- حادثه‌ی ۲۰۰۱ « هاینان»[1] که منجر به ورود ۲ میلیارد دلار خسارت مالی به آمریکا و آلوده کردن بالغ بر ۶۰۰۰ رایانه در این کشور شد.
- حملات سایبری گسترده علیه دولت‌های غربی و رایانه‌های صنعتی موسوم به «تیتان رین»[2].
- حملات سایبری به استونی (۲۰۰۷) و حملات سایبری به گرجستان (۲۰۰۸).
- حملات سایبری متعدد به جمهوری اسلامی ایران (۲۰۱۲–۲۰۰۶) که مهم‌ترین آن حملات، حمله کرم استاکس‌نت به تاسیسات هسته‌ای نطنز بود.

۲) در خصوص راهکارهای حقوقی برای مقابله با تهدیدات موجود در فضای سایبر، اهمیت دارد شبکه‌های برون‌مرزی در قالب‌های مختلف و تأثیرگذار برنامه‌سازی کنند.

۳) تهیه‌ی یک برنامه گفت‌وگوی ویژه خبری پیرامون حملات سایبری به سایت‌های برخی نهادهای دولتی کشور و بحث کارشناسی در مورد آن، به‌ویژه بر اساس کنوانسیون بوداپست و دستورالعمل تالین.

۴) چون حملات سایبری به‌مثابه حملات مسلحانه یا تجاوز سایبری، یکی از شیوه‌های نوین تخاصم در صحنه بین‌المللی است و منجر به ایجاد تلفات گسترده و خسارات وسیع می‌شود، لذا پیشنهاد می‌شود که رسانه‌های برون‌مرزی به‌ویژه شبکه پرس‌تی‌وی برنامه‌های مستند و کارشناس‌محور در این زمینه تهیه کنند و با استفاده از حقوق‌دانان داخلی و بین‌المللی بر لزوم ورود دیوان بین‌المللی کیفری برای پیگیری کیفری عاملان این حملات در ذیل جنایات بین‌المللی از جمله جنایت تجاوز تأکید نماید.

---

1. Hinan
2. Titan Rain

منابع و مأخذ

آقایی جنت‌مکان، حسین (۱۳۹۰)، «تعریف، عناصر و شروط اعمال صلاحیت دیوان بین‌المللی کیفری نسبت‌به جنایت تجاوز (با نگاهی به موافقتنامه کامپالا)»، **مجله حقوقی بین‌المللی، نشریه مرکزامورحقوقی بین‌المللی ریاست جمهوری**، سال ۲۸، شماره ۴۴، صص ۱۸۴-۱۶۳.

اسماعیل‌زاده‌ملاباشی، پرستو (۱۳۹۶)، «حمله سایبری به‌مثابه جنایت تجاوز و بررسی صلاحیت دیوان بین‌المللی کیفری در رسیدگی به آن»، **مجله پژوهش‌های حقوق جزاوجرم‌شناسی: شهردانش**، سال پنجم، شماره ۱۰، صص ۶۵-۴۳.

اصلانی، جبار (۱۳۹۵)، «حملات سایبری در چارچوب نظام مسئولیت بین‌المللی»، رساله دکترا، **دانشگاه تهران، دانشکده حقوق وعلوم سیاسی**.

سبحانی، مهین (۱۳۸۹)، «تاملی بر مصونیت کیفری مقام‌های عالی‌رتبه دولتی در جرایم بین‌المللی»، **پژوهشنامه حقوقی**، سال اول، شماره دوم، صص ۵۵-۳۱.

شایگان‌فرد، مجید (۱۳۸۷)، «دیوان بین‌المللی کیفری و صلاحیت رسیدگی به جنایت تجاوز»، **فصلنامه حقوق، مجله دانشکده حقوق وعلوم سیاسی**، دوره ۳۸، شماره ۴، صص ۲۷۹-۲۵۵.

شریعت‌باقری، محمدجواد (۱۳۷۷)، «نگاهی به اساسنامه دیوان بین‌المللی کیفری»، **پژوهشگاه علوم انسانی و مطالعات فرهنگی**،شماره ۱۲، صص ۱۰۹-۷۸.

صلاحی، سهراب و کشفی، مهدی (۱۳۹۵)، «جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین»، **مطالعات قدرت نرم**، شماره ۱۴، صص ۴۶-۲۸.

ضیایی‌بیگدلی، محمدرضا (۱۳۸۰)، **حقوق جنگ (حقوق بین‌الملل مخاصمات مسلحانه)**، چاپ دوم، انتشارات دانشگاه علامه طباطبایی.

حسیبی، آذین (۱۳۸۶)، « مسئولیت کیفری ماموران عالی‌رتبه‌ی دولت‌ها در حقوق بین‌الملل با تاکید بر رای دیوان بین‌المللی دادگستری بین کنگو و بلژیک»، **مجله‌ی کانون وکلا**، شماره‌ی ۱۹۶ و ۱۹۷، صص ۴۹-۲۴.

قریشی، سیدرسول (۱۳۹۳)، « تحلیل رابطه مافوق-مادون به عنوان عنصر ساختاری مسئولیت کیفری مقامات مافوق در اسناد بین‌المللی و رویه قضایی»، **فصلنامه علمی مطالعات بین‌المللی پلیس**، دوره ۵، شماره ۲۰، صص ۸۶-۵۹.

کاظمی، احمد (۱۳۹۸)، «جنایات بین‌المللی عربستان سعودی در یمن و چگونگی نقش‌آفرینی دیوان بین‌المللی کیفری (با تاکید بر رسالت رسانه‌های برون‌مرزی)»، **پژوهشنامه رسانه بین‌الملل**، سال چهارم، شماره چهارم، صص۱۵۰-۱۱۵.

کچوئیان فینی، جواد (۱۳۸۸)، «تحول مفهوم مصونیت سران دولت‌ها در حقوق بین‌الملل کیفری»، **فصلنامه سیاست خارجی**، سال ۲۳، شماره ۴، صص ۱۱۶۴-۱۱۳۸.

موسی‌زاده، رضا و فروغی‌نیا، حسین (۱۳۹۱)، «تعریف جنایت تجاوز در پرتو قطعنامه کنفرانس بازنگری اساسنامه دیوان بین‌المللی کیفری در کامپالا (ژوئن ۲۰۱۱)»، **فصلنامه راهبرد**، سال ۲۱، شماره ۶۳، صص ۱۷۳-۱۴۱.

میرمحمد صادقی، حسین (۱۳۸۳)، «مسئولیت ماموران مادون و مقامات مافوق در اساسنامه دادگاه کیفری بین‌المللی»، **مجله تحقیقات حقوقی**، شماره ۳۹، صص ۲۱۹-۲۰۳.

Ambos, Kai (2016), "Individual Criminal Responsibility for Cyber Aggression", **Journal of Conflict & Security Law**, Vol .21, No. 3, pp 495-504.

Ambos,Kai (2011), **the crime of Aggression after Kampala**, 53 German Yearbook of International Law.

Dinstein, Yoram (2005), **War**, **Aggression and Self-defense**, Cambridge University press, 4th Ed.

Gillett, Mathew (2013),"The Anatomy of and International Crime: Aggression at the International Criminal Court", **International Criminal Law Review**, Vol .13, No. 4, pp.829-864.

Hajdin, Nikola (2015),"Individual Criminal Responsibility for the Crime of Aggression: Tracking down the leaders of a state", **Faculty of Law lund University**, Master Thesis.

Heller, Kevin Jon (2007), "Retreat from Nuremberg: The Leadership Requirement in the Crime of Aggression", **the European Journal of International Law**, Vol. 18 No.3, pp. 477-497.

Kittichaiseree, Kriangsac (2011), **International Criminal Law**, Oxford: Oxford university Press.

Miller, Kevin L (2014),"The Kampala Compromise and Cyberattacks: Can there be an International Crime of Cyber-ggression?",**Southern California Interdisciplinary Law Journal** , Vol. 23, pp. 217-260.

Paulus, Andreas (2010), "Second Thoughts on The Crime of Aggression", **The European Journal of International Law**, Vol.20, No.4, pp. 1117-1128.

Sayapin, Sergey (2014), **The Crime of Aggression in International Criminal Law: Historical Development,Comparative Analysis and Present State,** The Hague: T.M.C. Asser Press.

US v von leeb et al case (**HighCommandcase**) (1950), Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law No 10 (TWC).

US v Krupp Von Bohlen und Halbach et al case (**Krupp Judgment**), Military Tribunal III, (1952)TWC.

US v Krauch et al cace, Military Tribunal VI (**Farben Judgment**), (1952) TWC.