Modern Interdisciplinary Research in Law
Vol. 4, Issue 1, Spring 2024, 52-66
jmirl.apadana.ac.ir

Apadana Institute of Higher Education

A Legal Perspective on Russia's Military and Cyber Attacks on Ukraine under International Public Law

Alireza Ansari Mahyari * | Assistant Professor, Faculty of Law, Theology, and Islamic Studies, Law Department, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

Zahra Sadat Hosseini | PhD Student, Faculty of Law, Theology, and Islamic Studies, Law Department, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

Ahmad Radman | Master's Graduate, Faculty of Law, Theology, and Islamic Studies, Law Department, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

Received: 19/January/2024 Accepted: 19/May/2024 eISSN: 2783-4204 ISSN: 2783-3631

Abstract

Despite the establishment of the United Nations, military conflicts and wars have not diminished globally; rather, today we witness numerous internal and international conflicts. One significant international war is the Russia-Ukraine conflict, which erupted in 2022 over power dynamics in Eastern Europe. This study aims to analyze the Russia-Ukraine war from the perspective of international law using a descriptive-analytical method. The research findings indicate that Russia's military and cyber-attacks on Ukraine constitute a blatant violation of international law, specifically breaching Article 2(4) of the United Nations Charter, which prohibits the threat or use of force against the territorial integrity or political independence of any state. Consequently, under international law, Russia had no right to invade Ukraine's territory.

Keywords: United Nations, territorial aggression, cyber warfare, international law, Russia-Ukraine war

* Corresponding Author: alimahyari63@gmail.com

فصلنامه تحقیقات نوین میان‌رشته‌ای حقوق
دوره ۴، شماره ۱، بهار ۱۴۰۳، ۵۲-۶۶
jmirl.apadana.ac.ir

تاریخ دریافت: ۱۴۰۲/۱۰/۲۹ تاریخ پذیرش: ۱۴۰۳/۰۲/۳۰ eISSN: 2783-4204 ISSN: 2783-3631

نگاهی حقوقی به حملات نظامی و سایبری روسیه به اوکراین در پرتو حقوق بین‌الملل عمومی

علیرضا انصاری مهیاری * استادیار، دانشکده حقوق الهیات و معارف اسلامی، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

زهرا سادات حسینی دانشجوی دکتری، دانشکده حقوق الهیات و معارف اسلامی، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

احمد رادمان دانش‌آموخته کارشناسی ارشد، دانشکده حقوق الهیات و معارف اسلامی، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران.

چکیده

با وجود تأسیس سازمان ملل، جنگ و درگیری‌های نظامی نه‌تنها در دنیا کمرنگ نشده بلکه امروزه شاهد درگیری‌های متعدد داخلی و نیز بین کشورها در ابعاد بین‌المللی هستیم. یکی از این جنگ‌های مهم بین‌المللی، جنگ روسیه و اوکراین بوده که در سال ۲۰۲۲ بر سر معادلات قدرت در منطقه شرق اروپا صورت گرفت. هدف از این پژوهش با استفاده از روش توصیفی-تحلیلی، بررسی جنگ روسیه و اوکراین از منظر حقوق بین‌الملل است. یافته‌های پژوهش حاکی از آن است که حملات نظامی و سایبری روسیه به اوکراین، نقض آشکار حقوق بین‌الملل به‌خصوص نقض بند ۴ ماده ۲ منشور ملل متحد یعنی اصل منع توسل به زور علیه تمامیت ارضی یا استقلال سیاسی یک دولت است. بر این اساس و مطابق با قواعد حقوق بین‌الملل، روسیه حق تجاوز به خاک اوکراین را نداشته است.

کلیدواژه‌ها: سازمان ملل، تجاوز ارضی، جنگ سایبری، حقوق بین‌الملل، جنگ روسیه و اوکراین

* نویسندهٔ مسئول: alimahyari63@gmail.com

مقدمه

با پایان جنگ سرد، ساختاری در نظام بین‌الملل به وجود آمد که اگرچه پیچیده اما قابل مدیریت بود؛ روسیه، اتحادیه اروپا و آمریکا برای مدیریت مشکلات در چارچوب آن با یکدیگر همکاری می‌کردند، اگرچه در این مسیر پرتنش در روابط دو طرف حوادثی چون حمله ناتو به کوزوو و جنگ روسیه با گرجستان در سال ۲۰۰۸ وجود داشت که روسیه را با غرب به چالشی جدی کشاند اما با وجود همه این حوادث، همکاری میان دشمنان قدیمی شرایطی را فراهم آورده بود که دو طرف به مفاد پیمان نهایی هلسینکی احترام می‌گذاشتند. از اوایل دهه ۱۹۹۰، جنگ سایبری توسط طرفداران آن به‌عنوان یک انقلاب در امور نظامی یا یک سلاح کامل جنگی معرفی شده است. بیشتر این بحث‌ها تئوری بوده و اغلب بر روی سؤالاتی تمرکز دارند که چگونه کاربرد قابلیت‌های سایبری ممکن است از آستانه یک حمله مسلحانه برآید یا از آن فراتر رود و درنتیجه به جنگ متعارف منجر شود. بااین‌حال، تعداد کمی از مطالعات تجربی، کاربرد عملیاتی نظامی قابلیت‌های سایبری را در طول جنگ بررسی می‌کنند. در طول سال گذشته و جنگ در اوکراین، قابلیت‌های سایبری در بحبوحه یک جنگ متعارف به کار گرفته شد و به ما اجازه داد تا در مورد ماهیت بالقوه تغییر بازی قابلیت‌های سایبری هنگامی‌که به‌عنوان ابزار جنگ استفاده می‌شود، نتیجه‌گیری اولیه کنیم. ادبیات مربوط به «جنگ سایبری»، معمولاً به استفاده از قابلیت‌های سایبری برای اهداف سیاسی–استراتژیک یا حتی جنایی به‌جای اهداف عملیاتی نظامی مربوط می‌شود (Bateman, 2022, p. 12).

روایت جنگ سایبری استراتژیک در دهه ۱۹۹۰، جنگ سایبری را به‌عنوان یک جبهه نسل بعدی می‌دانست که جامعه مدرن را تهدید می‌کرد و انتظار می‌رفت که عملیات سایبری، توازن قدرت را در سیستم بین‌المللی تغییر دهد زیرا آن را برتر از نیروی متعارف می‌دانستند (Schulze & Kerttunen, 2023, p. 36). محققانی مانند مارتین سی لیبیکی خاطرنشان کردند که وقتی صحبت از اهداف جنگ می‌شود، جنگ سایبری نمی‌تواند دشمن را خلع سلاح کند و «بسیار کمتر نابود می‌کند». علاوه بر این، در غیاب نبرد فیزیکی و خشونت، جنگ سایبری نمی‌تواند به دستاوردهای سرزمینی منجر شود که هنوز هم می‌تواند یکی از اهداف اصلی اکثر جنگ‌های مدرن در نظر گرفته شود (Smeets, 2018, p. 95). یک سال پس از حمله روسیه به اوکراین، فرضیات خاصی در مورد سودمندی عملیات سایبری در زمان جنگ می‌تواند مورد آزمایش قرار گیرد. جنگنده‌های سایبری روسیه این جنگ را آغاز کردند اما در مواجهه با یک مدافع سایبری مقاوم نتوانستند به اهداف خود دست یابند. به دلیل اثرات نامشخص، احتمال سرریز، چرخه‌های توسعه بدافزار و سرعت‌های عملیاتی متفاوت، همچنان اجرای جنگ‌های سایبری متعارف مشترک دشوار است. عملیات سایبری علیه اوکراین هنوز به اثرات استراتژیک عمده‌ای در کاهش ظرفیت اوکراین برای مقاومت دست نیافته است (Watts, 2022, p. 15). از سال ۲۰۱۴، روسیه و اوکراین روابط پرتنشی داشته‌اند که درنتیجه خشونت‌ها شروع شده است. حملات سایبری علاوه بر مسئله مرزی و جنبش جدایی‌طلبانه در اوکراین، به جنبه جدایی‌ناپذیر این درگیری تبدیل شده است. در سال ۲۰۲۱، تنش بین دو کشور افزایش یافت و در اوایل سال ۲۰۲۲، حمله سایبری قابل‌توجهی به وب‌سایت دولت اوکراین رخ داد. ازآنجاکه دولت اوکراین مدعی است که روسیه مغز متفکر پشت این حمله سایبری بوده است، این موضوع اختلافات بین دو کشور را تشدید کرده است. در سال ۱۹۹۱، اوکراین استقلال خود را از اتحاد جماهیر شوروی اعلام کرد. اوکراین تا همین اواخر در مقایسه با سایر نقاط اتحاد جماهیر شوروی به قلب روسیه نزدیک‌تر بود. با وجود این، روس‌ها اوکراین را بخشی از فرهنگ خود می‌دانند. بااین‌حال، این رابطه به دور از برابری است (Priyono, 2022, p. 45). روسیه سال‌هاست که علیه اوکراین اعلان جنگ کرده است. تنش بین روسیه و اوکراین در مارس ۲۰۱۴ شعله‌ور شد، زمانی که نیروهای روسی کنترل منطقه

کریمه اوکراین را به دست گرفتند و شبه‌جزیره را پس از اینکه کریمه‌ها در یک همه‌پرسی مورد مناقشه محلی به فدراسیون روسیه ملحق شدند، ضمیمه کردند. از آوریل ۲۰۱۴، درگیری بین جدایی‌طلبان مورد حمایت روسیه و نیروهای نظامی اوکراین منجر به جان باختن ۱۰۳۰۰ نفر و زخمی شدن ۲۴۰۰۰ نفر شده است. از سوی دیگر، روسیه با وجود اینکه به ایجاد پایگاه‌های نظامی در امتداد مرز ادامه می‌دهد، دست داشتن در جنبش جدایی‌طلبانه در اوکراین را انکار می‌کند. درنهایت، این وضعیت اعضاء ناتو، آمریکا و اروپا را وادار کرد تا به دنبال راه‌حل دیپلماتیک بین دو کشور باشند (Baezner, 2015, p. 36).

۱- جایگاه جنگ در قواعد حقوق بین‌الملل

جنگ یک وضعیت استثنائی است و طبعاً قواعد مربوط به آن نیز به نام حقوق جنگ، قواعدی استثنائی به شمار می‌رود. حقوق جنگ شامل مجموعه اصول و قواعدی است که حاکم بر روابط میان کشورهای متخاصم با یکدیگر و یا بین کشورهای متخاصم با کشورهای بی‌طرف است. به‌محض آغاز جنگ، بدون توجه به چگونگی شروع آن، کشورهای متخاصم دیگر تابع حقوق زمان صلح نیستند بلکه از حقوق جنگ تبعیت خواهند نمود؛ چه این حقوق عرفی باشد، چه قراردادی. کشورهای ثالث (کشورهایی که در مخاصمه شرکت ندارند)، خواه حقوق جنگ را مراعات نمایند یا خیر، روابط خود را با کشورهای متخاصم تابع حقوق زمان صلح نمی‌سازند بلکه از آن پس از حقوق بی‌طرفی تبعیت می‌نمایند. قانون جنگ یا حقوق جنگ، بخشی از حقوق بین‌الملل بوده و به مجموعه پیمان‌های بین‌المللی گفته می‌شود که به شرایط آغاز جنگ و رفتار طرف‌های درگیر می‌پردازد. قانون جنگ جزء حقوق بین‌الملل است که شرایط شروع جنگ و انجام خصومت را تنظیم می‌کند. قوانین جنگ حاکمیت و ملیت، ایالت‌ها و سرزمین‌ها، اشغال و سایر شرایط حیاتی قانون را تعریف می‌کند. حقوق جنگ همواره موجب یک جدال عقیدتی بین صاحب‌نظران بوده و هست. اختلاف‌نظر در این باب بعضاً به حدی است که حتی موجودیت واقعی آن را مورد سؤال قرار می‌دهد. برخی از دانشمندان، حقوق جنگ را قبول ندارند و ضرورت وجود آن را انکار می‌کنند. این گروه در مخالفت با حقوق جنگ به دلایل مهم و اساسی استناد می‌نمایند ازجمله اینکه جنگ یک جنایت بوده و جنایت را نبایستی تحت قاعده درآورد (داعی، ۱۳۹۰، ص ۴۹)؛ برای جنایت یا باید مجازات تعیین کرد و یا از وقوع آن جلوگیری نمود؛ حقوق جنگ، حقوقی بی‌فایده و غیرمفید است زیرا همیشه اجرای آن مؤخر بر وقوع جنگ است؛ حقوق جنگ بر اساس تجربیات جنگ‌های گذشته وضع شده و در جنگ‌های آینده، به دلیل پیشرفت‌های سریع علمی و فنی صورت‌گرفته در این فاصله، غیرقابل‌اجرا است. تا زمانی که مسئولیت کیفری فرد در حقوق بین‌الملل کاملاً شناخته نشده و ضمانت اجراهای مؤثر علیه اعمال فردی ناقض حقوق جنگ به وجود نیامده است، این حقوق عملاً اثری نسبت به متخاصمانی که همواره آن را در طول مخاصمات نقض می‌کنند، نخواهد داشت (ضیایی، ۱۳۹۶، ص ۵۸). گرچه مجازات جنایتکاران جنگ دوم جهانی پس از جنگ اهمیت خاص خود را دارد اما باید آن را یک رویداد استثنائی تلقی نمود. قانون‌گذار بین‌المللی مرجحاً بایستی تمامی فعالیت خود را وقف بهتر نمودن و غنی ساختن حقوق صلح نماید تا حقوق جنگ. به رغم مخالفت‌های یادشده، توجه به ضرورت حقوق جنگ اهمیتی ویژه دارد چراکه واقعیت‌ها خود پاسخگوی مخالفت‌ها است. متأسفانه جنگ به‌طور قطعی و کامل از صحنه زندگی بین‌المللی رخت برنبسته و به‌راحتی می‌توان پذیرفت که امکان وقوع جنگ در هر لحظه، به دلیل نقض تعهدات مربوط از جانب هر یک از کشورها باقی است (سادات میدانی و محمدی، ۱۴۰۲، ص ۱۸۳۳)؛ بنابراین لازم است حداقل جریان جنگ را تابع مقررات حقوقی نمود و تا آنجا که بتوان، خطرات و خسارات ناشی از آن را محدود ساخت. از سوی دیگر، همیشه این اعتراض وجود داشته و دارد که قوانین جنگ نقض شده و خواهد شد. با وجود این، مطالعه و بررسی جنگ‌های گذشته ازجمله جنگ‌های جهانی اول

و دوم، خلاف این ادعا را به اثبات می‌رساند. در جنگ جهانی اول، حقوق جنگ تا آن حدی که ادعا شده، نقض نگردید و چنین ادعایی مسلماً از روی عدم اطلاع و آگاهی است.

۲- تبیین تجاوز ارضی در نظام بین‌الملل

اولین معاهداتی که در آن‌ها تجاوز تعریف و اعمال تشکیل‌دهنده آن برشمرده شده، معاهدات معروف به معاهدات لندن یا پیمان‌های عدم تجاوز است که در سال ۱۹۳۳ میان اتحاد جماهیر شوروی و برخی کشورهای دیگر منعقد شد. مجمع عمومی سازمان ملل متحد پس از سال‌ها تلاش در سال ۱۹۷۴ قطعنامه شماره ۳۳۱۴ را با عنوان قطعنامه تعریف تجاوز به تصویب رسانید. طبق ماده ۱ این قطعنامه، تجاوز عبارت است از کاربرد نیروی مسلح به‌وسیله یک کشور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشور دیگر یا کاربرد آن از دیگر راه‌های مغایر با منشور ملل متحد، به‌گونه‌ای که در این تعریف آمده است (موسی‌زاده، ۱۳۹۶، ص ۲۳). طبق ماده ۲ قطعنامه، پیشی گرفتن یک کشور در کاربرد نیروی مسلح مغایر با منشور نشانه اولیه اقدامی تجاوزکارانه به شمار خواهد آمد؛ گرچه شورای امنیت طبق منشور می‌تواند نتیجه بگیرد که احراز وقوع تجاوز با توجه به دیگر شرایط مرتبط ازجمله کافی نبودن شدت اقدامات به‌عمل‌آمده یا نتایج آن‌ها قابل توجیه نیست. جنایت تجاوز ارضی، جنایتی علیه صلح بین‌الملل است و درنتیجه موجب مسئولیت بین‌المللی شده و هرگونه تصرف ارضی یا امتیاز ویژه ناشی از آن، قانونی نیست. تعیین مسئول یا متجاوز بر اساس ماده ۳۹ منشور ملل متحد با شورای امنیت است. تجاوز فقط تجاوز مسلحانه را در بر می‌گیرد و شامل مواردی مثل تهاجم و تجاوز اقتصادی، سایبری، فرهنگی و نظایر آن نمی‌شود. با توجه به بند ۱ ماده ۸ مکرر، رفتار فیزیکی لازم برای تحقق جنایت تجاوز شامل یکی از چهار فعل مثبت طراحی، آماده‌سازی، آغاز یا اجرای یک عمل تجاوزکارانه از نوع اعمال مذکور در بند ۲ ماده ۸ است (زمانی و همکاران، ۱۳۹۶، ص ۱۱۵).

۳- حمله نظامی روسیه به اوکراین

۳-۱- بررسی حمله نظامی

در سال ۲۰۲۲ میلادی، کشور اوکراین مورد حمله نظامی روسیه قرار گرفت. در این حملات، سرتاسر خاک اوکراین مورد حملات موشکی روسیه واقع شد و نیروهای زمینی روسیه نیز از جهت‌های مختلف به خاک این کشور حمله کردند. با این حملات مشخص است که روسیه بند ۴ ماده ۲ منشور را که توسل به زور را ممنوع می‌داند، نقض نموده و در مقیاس وسیعی مبادرت به توسل به زور نموده است. رئیس‌جمهور روسیه در ارتباط با حملات خود به اوکراین به ۳ دلیل اشاره نمود و بیان داشت که مطابق با این دلایل، عمل او توسل به زور نبوده است؛ دلیل اولش آن است که به ماده ۵۱ منشور سازمان ملل متحد استناد کرده است که برای دفاع از کشور خودش در برابر نوعی تهدید که از جانب اوکراین امکان ایجاد دارد، مبادرت به جنگ نموده است و درواقع در مقام دفاع مشروع بوده درحالی‌که این دلیل بی‌پایه‌ای است چراکه حمله پیش‌دستانه در مقام دفاع مشروع شرایطی دارد که یکی از این شرایط قریب‌الوقوع بودن حمله است (عزیزی، ۱۳۹۴، ص ۶۳). دلیل دوم آن است که برای دفاع مشروع دسته‌جمعی جمهوری‌های دونتسک و لوهانسک، به خاک این کشور حمله کرده است. این استدلال در صورتی صحیح است که ثابت شود اوکراین به این دو کشور حمله کرده است و حتی اگر به‌صورت فرضی این استدلال صحیح باشد، شروط ضرورت و تناسب (به‌عنوان شروط اصلی دفاع مشروع) رعایت نشده و شدت حمله به اوکراین وسیع‌تر است. دلیل سوم آن است که روسیه به علت جلوگیری از نسل‌کشی روس‌ها در شرق به اوکراین حمله کرده است و به مداخله بشردوستانه استناد نموده است. نکته‌ای که وجود دارد این است که از نظر بسیاری از حقوقدانان بین‌المللی، مداخله بشردوستانه به‌عنوان استثنائی برای

توسل به زور رد می‌شود؛ بنابراین، با توجه به آنچه گفته شد، عمل روسیه توسل به زور بوده و بند ۴ ماده ۲ منشور ملل متحد را نقض نموده است. به همین علت از طرف بسیاری از کشورهای جهان مورد تحریم قرار گرفته است (CyberPeace Institute, 2022).

۱-۱-۳- منافع روسیه در اوکراین

با فروپاشی اتحادیه جماهیر شوروی در سال ۱۹۹۱ میلادی، اوکراین نیز مانند سایر کشورها استقلال خود را بازیافت و به کشوری مستقل تبدیل شد. کشور اوکراین بعد از جنگ جهانی دوم، برای روسیه کشوری باارزش تلقی می‌شد چراکه پس از فروپاشی اتحاد جماهیر شوروی، روسیه به کشوری ضعیف تبدیل شد و سعی داشت تا با کنترل اوکراین به قدرت سابق خود بازگردد (Bebler, 2015). اهمیت اوکراین از این جهت بود که این کشور در زمان شوروی، مقر بسیاری از سلاح‌های هسته‌ای شوروی بوده و یکی از قدرتمندترین کشورهای اتحادیه به شمار می‌رفته است و بخش بزرگی از اتباع این کشور را روس‌ها تشکیل می‌دادند. در سال ۲۰۰۴، آمریکا و اروپا در این کشور نفوذ پیدا کردند و همین امر باعث از بین رفتن نفوذ روسیه در این کشور شد. در سال ۲۰۱۴ نیز انقلابی دیگر در اوکراین صورت گرفت و روسیه دوباره شکست خورد و نهایتاً در اقدامی غیرقابل‌پیش‌بینی، شبه‌جزیره کریمه در اوکراین را به خاک خود اضافه نمود (Gertz, 2021).

۲-۱-۳- نقش شبه‌جزیره کریمه در جنگ روسیه و اوکراین

بعد از جنگ جهانی دوم، برای نخستین بار یکی از قدرت‌های برتر اروپایی موفق شد بخشی از کشوری را با وجود مخالفت شدید به خاک خود اضافه نماید. به دنبال آسیب‌پذیری داخلی اوکراین و از هم پاشیدن انسجام درونی کشور و گسل عمیق در میان شهروندان اوکراین، زمینه‌های این الحاق ایجاد گردید. به دیدگاه عده‌ای، اوکراین برای چندین سده بخشی از سرزمین روسیه بوده و به همان علت رهبران روسیه خود را محق می‌دانستند که در ارتباط با اوکراین تصمیم‌گیری کنند (Rice, 2022, p. 74). علت اینکه شبه‌جزیره کریمه به روسیه ملحق شد، این بود که رهبران روسیه معتقد بودند که این ناحیه به علت اهمیت ژئوپولیتیک خود، به قدرت و اقتدار این کشور کمک خواهد نمود. به همین جهت، به دنبال ضعیف شدن اوکراین و شکاف ایجادشده بین مردم این کشور، روسیه توانست بر این منطقه تسلط پیدا کند (Greenberg, 2022, p. 52).

تصویر ۱. کشور اوکراین و مناطق الحاق‌شده به روسیه (مناطق مشخص‌شده با رنگ قرمز) (Priyono, 2022)

۲-۳- حملات سایبری

تحلیلگران سیاسی متعارف خاطرنشان می‌کنند که رویارویی نظامی روسیه و اوکراین، در صورت وقوع می‌تواند عواقب سایبری خود را داشته باشد. متخصصان سایبری می‌دانند که پشت همه این‌ها یک جنگ سایبری است که نبردهای آن از قبل آغاز شده و قربانیان آن از سال ۲۰۱۴ چندین برابر شده است. اوکراین از زمانی که مسکو، کریمه را در سال ۲۰۱۴ ضمیمه کرد، تحت حملات سایبری مداوم هکرهای روسی تحت حمایت کرملین قرار گرفته است. جاسوسی سایبری، هک کردن شبکه‌ها، پایگاه‌های اطلاعاتی و سرورها، اختلال در تأسیسات انرژی و ارتباطات، انتشار شایعات و اطلاعات نادرست به بخشی از درگیری بین روسیه و اوکراین تبدیل شده است (Mohee, 2022, p. 40). در ادامه، ابتدا پیشینه جنگ سایبری و سپس، جنگ سایبری بین اوکراین و روسیه بررسی می‌گردد.

۱-۲-۳- بررسی جنگ سایبری

از اواسط دهه ۲۰۰۰، جنگ سایبری به‌عنوان یک قابلیت مستقل که اثراتی مستقل از درگیری جنبشی ایجاد کند، تلقی نمی‌شود بلکه بیشتر به‌عنوان تمجید از قابلیت‌های متعارف است. به عبارت دیگر، عملیات سایبری زمانی که به‌صورت مشترک و ترکیبی مورد استفاده قرار می‌گیرد، می‌تواند به‌عنوان یک نیرومند/چند انبردست برای قابلیت‌های معمولی عمل کند. در اینجا، عملیات سایبری در جنگ لزوماً با تأثیرات استراتژیک آن‌ها سنجیده نمی‌شود بلکه بیشتر به‌عنوان یک قابلیت ضد نیرویی تلقی می‌شود که می‌تواند علیه ارتش‌های دشمن هدایت گردد. یکی از این نمونه‌ها، بدافزار ایکس ایجینت است که به تجهیزات هدف‌گیری که آتش توپخانه را هدایت می‌کنند، نفوذ می‌کند و سپس، موقعیت جغرافیایی مواضع توپخانه را به نیروهای دشمن نشت می‌دهدو در ادامه، آتش ضد باتری را هدایت می‌کند. در این مفهوم‌سازی از قابلیت‌های سایبری، استفاده از وسایل سایبری به‌خوبی با ایده‌آل‌های جنگ مانور و فلج کردن دشمن با حملات جراحی یا طب سوزنی مطابقت دارد (Nardelli et al., 2022, p. 35). مطالعات نشان می‌دهد که سخت‌افزار نظامی دارای آسیب‌پذیری‌های فراوانی است که می‌توان از آن‌ها در تئوری عملیات سایبری بهره‌برداری کرد. در عمل، عملیاتی کردن این امر دشوار است. مطالعه نادیا کوستیوک و یوری‌ام در مورد استفاده از حملات انکار سرویس توزیع‌شده و عملیات نظامی جنبشی در سوریه (۲۰۱۳) و شرق اوکراین (۲۰۱۴) نشان می‌دهد که زمان‌بندی اغلب در عملیات مشترک خاموش است. حملات متعارف و عملیات سایبری مخرب دارای زمان‌های برنامه‌ریزی متفاوت و سرعت‌های عملیاتی متفاوتی هستند که دستیابی به اثرات مشترک را دشوار می‌کند. برای مثال، بدافزار دارای چرخه حیاتی است؛ ابتدا باید توسعه داده شود، آزمایش شود و سپس به سمت زیرساخت‌های سایبری و اطلاعاتی دشمن حمله شود تا اثراتی ایجاد کند تا زمانی که کشف و کاهش یابد. این موضوع نیازمند یک بازه زمانی چندماهه است. در اصل، یک به‌روزرسانی نرم‌افزار یا تغییر در پیکربندی‌ها از جانب مدافع، پتانسیل این را دارد که اثر بدافزار را از بین ببرد (Frisby, 2022, p. 63).

بدافزارها بسیار بیشتر از گلوله‌ها به هدف اختصاص دارند. درنهایت، برای همگام‌سازی اثرات آن با عملیات زمینی، بدافزار ممکن است به اتصالات فرمان و کنترل زنده به دنیای خارج نیاز داشته باشد که ممکن است در یک محیط جنگی که از تداخل جنگ الکترونیک فعال استفاده می‌کند، غیرممکن باشد؛ بنابراین، یک عملیات سایبری ممکن است در مراحل اولیه جنگ به‌عنوان یک نوع حمله اول مفید به کار گرفته شود اما هرچه این خصومت‌ها بیشتر طول بکشد، حفظ انبارهای عملیاتی بدافزارهای کاربردی و دسترسی سیستم‌های متخاصم به درب پشتی اصلی سخت‌تر می‌شود. علاوه بر این، هماهنگ کردن مانورها بین نیروهای متعارف و سایبری دشوار است. اول، اهداف متضاد یک مسئله هستند: بازیگران اطلاعات‌محور دسترسی طولانی‌مدت پنهانی به یک سیستم را ترجیح می‌دهند. جاسوسی

سایبری یا عملیات مبتنی بر حضور بر اختلالات کوتاه‌مدت سیستم‌ها (به اصطلاح عملیات اثر سایبری) که احتمالاً منجر به کشف درب پشتی استفاده‌شده و درنتیجه سوزاندن قابلیت می‌شود. دوم، جغرافیای میدان‌های نبرد دیجیتال و متعارف به‌ندرت همسو می‌شوند. ایالات‌متحده این موضوع را با عملیات سمفونی درخشان درحالی‌که زیرساخت دیجیتال داعش را هدف قرار داد، آموخت. داعش در ده‌ها کشور به خدمات دیجیتال متکی بود و حذف/تسخیر این دارایی‌ها از طریق عملیات سایبری باید با متحدان و کشورهای شخص ثالث هماهنگ شود. علاوه بر این، داعش ثابت کرد که در زمینه حملات سایبری مقاوم بوده و به‌سرعت زیرساخت ناتوان خود را بازسازی می‌کند. عملیات سمفونی درخشان نشان داد که تعامل سایبری نه موقت بلکه مستمر، مؤثرتر است و سودمندی عملیات سایبری در جنگ، کمتر در تأثیرات مخرب آن‌ها بوده و بیشتر در جمع‌آوری اطلاعات و قابلیت‌های روانی آن‌ها نهفته است. اگر دشمنی ترس داشته باشد که شبکه آن‌ها به خطر بیفتد و کسی به آن‌ها گوش دهد، به ابزارهای ارتباطی دیگر روی می‌آورد و درنتیجه برنامه‌ریزی عملیاتی خود را کند و پیچیده می‌کند (Neuman, 2022, p. 65). اریکا دی. بورگ هارد و شاون دبلیو لونرگان به این نتیجه رسیدند که یکی دیگر از کاربردهای عملیات سایبری در جنگ ممکن است توانایی آن‌ها برای هدف قرار دادن سیستم‌های لجستیکی باشد زیرا این سیستم‌ها اغلب غیرنظامی و امنیت کمتری نسبت به سیستم‌های نظامی دارند. بااین‌حال، بسیاری به این نتیجه می‌رسند که قابلیت‌های سایبری برای عملکردهای اطلاعاتی و شناسایی بهترین کارایی را دارند و جایگزین سلاح‌های معمولی نمی‌شوند. در بسیاری از موارد، خنثی کردن یک هدف با حملات هوایی یا آتش توپخانه، به‌جای عملیات سایبری، سریع‌تر، ساده‌تر، کم‌هزینه‌تر و مؤثرتر است. علاوه بر این، کاربرد اصلی عملیات سایبری، سرقت یا دست‌کاری اطلاعات برای اهداف سیاسی، اقتصادی یا حتی جنایی است. تأثیر این عملیات بر موازنه قوا در این روایت دو گونه است؛ اول می‌توان از آن‌ها برای تأثیرگذاری بر گفتمان و فرآیندهای سیاسی استفاده کرد. به‌عنوان‌مثال، تضعیف دموکراسی‌های غربی در زمان صلح. دوم اینکه آن‌ها می‌توانند به مهاجمان اجازه دهند تا دستاوردهای استراتژیک را در قالب جاسوسی سایبری طولانی‌مدت به دست آورند، همان‌طور که در مدل چینی یا کره شمالی از سایبری-دولتی دیده می‌شود. این قرائت از عملیات سایبری به‌شدت از دو گرایش الهام گرفته شده است؛ اولاً طبق قوانین بین‌المللی، اکثر عملیات سایبری معیارهای قانونی استفاده از زور یا حمله مسلحانه را برآورده نمی‌کنند و نمی‌توان از آن‌ها برای توجیه حمله بر اساس بند دفاع مشروع ماده ۵۱ منشور ملل متحد استفاده کرد. در بسیاری از موارد، عملیات سایبری عمداً به‌گونه‌ای طراحی شده‌اند که به زیرآستانه جنگ سقوط کنند و خطر تشدید انتقام‌جویی مسلحانه یا خشونت‌آمیز را به همراه نداشته باشند؛ به‌ویژه جنگ. به‌طور مشابه، مدافع نیز ممکن است علاقه‌ای به عدم تشدید واکنش خود به چنین فعالیتی داشته باشد. ثانیاً، روایات هنجاری فعالیت سایبری پیرامونی با استفاده از چنین قابلیت‌هایی توسط روسیه از زمان الحاق کریمه در سال ۲۰۱۴ و تا تلاش‌های این کشور برای مداخله در انتخابات ریاست جمهوری ایالات‌متحده در سال ۲۰۱۶ شکل گرفته است (O'Neill, 2022, p. 10).

۱-۱-۲-۳- حملات سایبری هکرهای روسی

بر اساس مقاله‌ای که توسط جو رابینسون، کارشناس حریم خصوصی داده‌ها و امنیت سایبری نوشته شده است، روسیه حملات سایبری را علیه ۱۹ کشور انجام داده که بین سال‌های ۲۰۰۹ تا ۲۰۱۹ منجر به ۷۵ حادثه شده است. ایالات‌متحده و دیگر کشورهای اروپایی، هدف اصلی این حملات بودند به‌طوری‌که اوکراین با ۹ حمله بین سال‌های ۲۰۱۷ تا ۲۰۱۹، در میان پرتکرارترین حملات روسیه در مدت کوتاهی قرار گرفته است. بر اساس آمار ارائه‌شده توسط مرکز مطالعات

استراتژیک و بین‌المللی[1] در مورد حوادث کلیدی سایبری که به سال ۲۰۰۶ بازمی‌گردد، موارد متعددی وجود داشته است که روسیه را به‌عنوان عامل حمله، متهم کرده است (Robinson, 2021, p. 60).

جدول ۲. تعداد حمله‌های سایبری در بازه زمانی سال‌های ۲۰۱۷ تا ۲۰۱۹ در برخی از کشورها (Robinson, 2021)

	منبع	هدف	تعداد حمله سایبری
۱	روسیه	ایالات‌متحده	۳۴
۲	چین	ایالات‌متحده	۲۵
۳	ایران	ایالات‌متحده	۱۳
۴	کره شمالی	کره جنوبی	۱۲
۵	**روسیه**	**اوکراین**	**۹**

تصویر ۲. نقشه برخی حمله‌های سایبری انجام‌شده در دنیا در بازه زمانی ۲۰۱۷–۲۰۱۹ م (Robinson, 2021)

قابل‌توجه‌ترین حملات سایبری روسیه علیه اوکراین در سال‌های ۲۰۱۴ و ۲۰۱۵ عبارت‌اند از:

– در سال ۲۰۱۴، مهاجمان سایبری روسی در آستانه انتخابات عمومی به سیستم شمارش آراء در اوکراین دسترسی پیدا کرده و سوابق الکترونیکی را از بین بردند و مقامات اوکراینی را مجبور به شمارش دستی آراء کردند؛

– در سال ۲۰۱۵ پس از آن، طی عملیاتی منسوب به گروهی مرتبط با اطلاعات نظامی روسیه، یک حمله سایبری باعث قطع برق برای چند ساعت در غرب اوکراین و بخشی از کی‌یف شد. این اولین خاموشی شناخته‌شده ناشی از یک حمله سایبری بود؛

– در طول سال ۲۰۱۷، حمله نات پتیا[2] رخ داد (توسط همان گروه مرتبط با اطلاعات نظامی روسیه) و موفق شد نزدیک به ۱۰ درصد از تمام سیستم‌های رایانه‌ای اوکراین را قبل از انتشار در سراسر جهان به یک بسته بدافزار آلوده کند و بر اساس تخمین ایالات‌متحده، در یکی از مخرب‌ترین حملات سایبری در تاریخ، حدود ۱۰ میلیارد دلار ضرر برای شرکت‌ها در سراسر جهان به همراه داشته باشد؛

– در ۱۵ ژانویه ۲۰۲۲، مایکروسافت، نرم‌افزار مخربی را که به‌عنوان باج‌افزاری به نام ویسپر گیت[3] پنهان شده بود، افشا کرد که ده‌ها سازمان دولتی و غیرانتفاعی و مؤسسه فناوری اطلاعات مستقر در اوکراین را هدف قرار داده بود؛

1. strategic and international studies (CSIS)
2. NotPetya
3. WhisperGate

– در ۱۹ ژانویه ۲۰۲۲، پس از اینکه مقامات کانادایی حمایت خود را از اوکراین گسترش دادند، یک حمله سایبری برخی از عملکردهای سازمان امور جهانی کانادا[1] را مختل کرد؛

– اخیراً (در اوایل فوریه ۲۰۲۲) مایکروسافت هدف قرار دادن دفاتر نظامی اوکراین و شبکه‌های دولتی توسط گروه اکتینیوم[2] را فاش کرد که گمان می‌رود با سرویس‌های امنیتی روسیه مرتبط باشد. این هدف‌گیری از اکتبر ۲۰۲۱ آغاز شده که هدف آن، جاسوسی و جمع‌آوری اطلاعات است.

از سوی دیگر، چندین گروه مرتبط با اوکراین، حملات سایبری متعددی را با تأثیر محدود با هدف قرار دادن توانایی‌ها و منافع روسیه انجام دادند که مهم‌ترین آن‌ها عبارت بودند از:

– عملیات پریکورمکا[3] در ماه می ۲۰۱۶ که شامل انتشار نرم‌افزار مخربی بود که لیست قیمت طعمه ماهیگیری را نمایش می‌داد. میزان آسیب ناشی از این نرم‌افزار مخرب به‌طورقطع مشخص نیست. عملیات "۹ مه ۲۰۱۶" که شامل ۹ هک موفقیت‌آمیز وب‌سایت‌های گروه جدایی‌طلب "جمهوری خلق دونتسک"، علاوه بر سایت‌های روسی برای تبلیغات ضد اوکراینی و سایت‌ها و شبکه‌های شرکت‌های نظامی خصوصی روسیه بود.

–هک چنل وان[4] در ژوئن ۲۰۱۶ که طی آن، سرور کانال یک روسیه توسط اتحاد سایبری اوکراین متشکل از هکرهای فالکونز فلیم[5]، ترینیتی[6] و رخ ۸۱۰[7] هک شد.

– سورکوف لیکس در اکتبر ۲۰۱۶ که طی آن، ۲۳۳۷ ایمیل و صدها فایل پیوست فاش شد که نقشه‌هایی برای تصرف کریمه و دامن زدن به ناآرامی‌های جدایی‌طلب در دونباس را فاش کرد.

– اخیراً یک گروه اوکراینی با انجام یک حمله سایبری در ۲۴ ژانویه ۲۰۲۲، عملیات سیستم راه‌آهن بلاروس را مختل کرد که هدف آن، کاهش سرعت حرکت نیروهای روسیه از طریق جمهوری بلاروس به سمت مرزهای اوکراین بود (Watling & Reynolds, 2022, p. 16).

۲-۱-۲-۳- بررسی اثر روابط سیاسی اوکراین و ایالات‌متحده آمریکا بر حملات سایبری روسیه

بر اساس بیانیه معاون وزیر خارجه اوکراین در امور امنیت ملی و دفاع، عاملان حمله سایبری موسوم به یو. ان. سی ۱۱۵۱[8] علیه اوکراین با اطلاعات بلاروس ارتباط دارند. یو. ان. سی ۱۱۵۱، یک سازمان جاسوسی سایبری مرتبط با خدمات ویژه بلاروس است. به گفته فرمانده پلیس سایبری اوکراین، این گروه سابقه هدف قرار دادن لیتوانی، لتونی، لهستان و اوکراین و همچنین، انتشار روایت‌های انتقادی از موضع ناتو در اروپا را دارد. ویروس خطرناکی که برای رمزگذاری برخی از سیستم‌های دولتی استفاده می‌شود، بسیار شبیه بدافزار مورد استفاده باند هکر (ای. تی. پی ۲۹[9]) بوده که در هک کردن کمیته ملی دموکرات‌ها قبل از انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۱۶ نقش داشته است. این سازمان با سازمان‌های اطلاعاتی ویژه روسیه مرتبط است و هدف آن، انجام جاسوسی سایبری با جذب و بهره‌برداری از افراد داخلی است. پس از حمله سایبری، پیام‌هایی به سه زبان اوکراینی، روسی و لهستانی در وب‌سایت اوکراینی گذاشته شد. آن‌ها به والهینیا[10] و شرق گالیسیا[11] اشاره داشتند، جایی که ارتش شورشی اوکراین در لهستان

1. global affairs canada GAC
2. Actinium
3. Prikormka
4. Channel One
5. FalconsFlame
6. Trinity
7. Rukh810
8. UNC1151
9. ATP-29
10. Volhynia
11. Galicia

تحت اشغال نازی‌ها[1] اعدام‌های دسته‌جمعی انجام داد. این مورد هنوز هم منبع اختلاف بین لهستان و اوکراین است (Sanger, 2022, p. 18). دنیای سایبری دارای عنصر ناشناس بودن است. غم‌انگیزترین حمله سایبری تاریخ در سال ۲۰۰۷ در استونی رخ داد، زمانی که یک سری حملات سایبری گسترده علیه وب‌سایت‌های دولتی استونی ازجمله بانک‌ها، پارلمان، روزنامه‌ها و صداوسیما در ۲۷ آوریل ۲۰۰۷ در پاسخ به مناقشه این کشور با روسیه در مورد جابه‌جایی سرباز برنزی تالین در گورستان‌های جنگی تالین و همچنین، یک بنای تاریخی تدفین‌شده در دوران شوروی رخ داد. دولت استونی مشتاق بود که انگشت اتهام را به‌سوی کرملین بگیرد و کرملین را به همدستی مستقیم در اعتصاب در آن زمان متهم کند. بااین‌حال، وقتی وزیر دفاع استونی اظهار داشت که هیچ مدرکی دال بر ارتباط این حمله سایبری با کرملین ندارد، ثابت شد که اتهامات کاملاً واقعی نیستند. روسیه این ادعاها را «بی‌اساس» اعلام کرد و نه متخصصان ناتو و نه متخصصان کمیسیون اروپا نتوانستند شواهدی دال بر دخالت رسمی دولت روسیه به دست آورند. بهترین کاری که می‌توان انجام داد، همان‌طور که استونی پس از حمله از آن حمایت کرد، بهبود حفاظت از امنیت سایبری و مدیریت حوادث است (Windrem, 2016, p. 24)؛ بنابراین، درحالی‌که بر اساس این تحلیل نتیجه می‌گیریم که ارتباطی بین حملات سایبری در اوکراین و جنگ بین روسیه و اوکراین وجود دارد، عاملان این حملات باید از نظر قانونی تأیید شوند. ازآنجاکه این کار ناکارآمد است، سرمایه‌گذاری روی یک دفاع سایبری قوی و انعطاف‌پذیری سایبری قابل اعتماد به‌جای تمرکز تمام تلاش‌ها بر روی یافتن عامل واقعی، ترجیح داده می‌شود (Zoria, 2022, p. 23).

۴- نگاه سازمان ملل متحد به جنگ روسیه و اوکراین

تحولات اوکراین در سال ۲۰۱۳ که آثار آن تا به امروز نیز تداوم دارد، یکی از جدیدترین تحولاتی است که آثار متعددی بر نظام‌های منطقه‌ای و بین‌المللی داشته است. تحولات اوکراین در سال ۲۰۱۳ میلادی را نیز که همراه با ناآرامی‌های متعدد در این کشور و خارج شدن شبه‌جزیره کریمه از حاکمیت اوکراین شد، می‌توان ازجمله رخدادهای بین‌المللی دانست که آثار متعددی از لحاظ سیاسی، اقتصادی و اجتماعی در معادلات بین‌المللی به وجود آورده است. پیامدهای تحولات اوکراین از جنبه‌های گوناگون قابل ارزیابی است؛ چنانکه هم می‌توان به آثار این تحولات بر ترتیبات منطقه‌ای توجه کرد و هم می‌توان آثار این تحولات را از دید کلان‌تر، یعنی نظام بین‌المللی و همچنین دیدگاه و مواضع سازمان‌های بین‌المللی و حقوق بشری مورد بررسی و ارزیابی قرار داد (وثوقی و همکاران، ۱۳۹۸، ص ۲۳).

۴-۱- نگاه حقوق بشری

مجمع عمومی سازمان ملل متحد در روز چهارشنبه ۲ مارس ۲۰۲۱ در یک نشست فوق‌العاده به قطعنامه‌ای رأی داد که تهاجم روسیه به اوکراین را محکوم می‌کرد. این قطعنامه به شکل قاطعانه از تجاوز روسیه به تمامیت ارضی اوکراین و نقض بند ۴ ماده ۲ منشور سازمان ملل متحد ابراز تأسف کرده و از روسیه می‌خواهد فوراً و به‌طور کامل و بدون قید و شرط نیروهایش را از داخل مرزهای به رسمیت شناخته‌شده اوکراین خارج کند (The Institute for Economics & Peace Briefing Series, 2021). بااین‌حال، رأی یکپارچه اعضاء و اظهارات دفاتر نمایندگی کشورها نشان می‌دهد که نگرانی‌ها از نقض آشکار تمامیت ارضی یک کشور عضو سازمان ملل باعث بروز نگرانی‌های فراگیر شده است (Mearsheimer, 2014, 16). درگیری ارضی میان روسیه و اوکراین در سال ۲۰۱۴ نیز بالا گرفته بود؛ زمانی

1. UPA

که نیروهای روسی، شبه‌جزیره کریمه را اشغال و آن را ضمیمه خاک خود کردند. در آن هنگام، مجمع عمومی سازمان ملل متحد در ۲۷ مارس ۲۰۱۴ با تصویب قطعنامه‌ای از روسیه خواست تا به‌طور کامل، در اسرع وقت و بدون قید و شرط از شبه‌جزیره کریمه اوکراین خارج شود (European Parliamentary Research, 2022).

۲-۴- قطعنامه شورای امنیت سازمان ملل در محکومیت حملات به اوکراین ۲۲ فوریه ۲۰۲۲

جلسه شورای امنیت سازمان ملل برای رأی‌گیری در مورد پیش‌نویس قطعنامه در مورد اوکراین در حالی توسط آمریکا و آلبانی مطرح گردید که نماینده آمریکا بیان نمود: روسیه جنگ با اوکراین را انتخاب و قوانین بین‌المللی را نقض کرده است. ما بر حاکمیت و تمامیت ارضی اوکراین تأکید می‌کنیم و از روسیه می‌خواهیم فوراً نیروهای خود را از اوکراین خارج کند. نماینده آلبانی در شورای امنیت نیز گفت: باید با اوکراین اعلام همبستگی کنیم. نماینده انگلیس در شورای امنیت تأکید کرد: باید برای نجات نسل‌های آینده از جنگ، تلاش کنیم. قطعنامه‌ای که امروز به آن رأی می‌دهیم، پیام حمایت از مردم اوکراین است. نماینده برزیل در شورای امنیت نیز گفت: برای حل بحران اوکراین باید فرصت‌های گفتگو را فراهم کنیم. ما دوباره درخواست خود برای توقف درگیری‌ها در اوکراین را اعلام می‌کنیم. نماینده هند در شورای امنیت گفت: ما خواستار پایان دادن به خصومت‌ها و بازگشت زبان گفتگو هستیم. نماینده چین در شورای امنیت گفت: به‌جای محکومیت باید تدابیری برای رفع بحران اندیشید. امنیت یک کشور را نمی‌توان به هزینه کشورهای دیگر ساخت. نگرانی‌های امنیتی روسیه باید در نظر گرفته شده و به آن رسیدگی شود. نماینده روسیه در شورای امنیت گفت: از کشورهایی که از پیش‌نویس قطعنامه درباره اوکراین حمایت نکردند، تشکر می‌کنیم. پیش‌نویس قطعنامه درباره اوکراین متعادل نبود. مقامات کی‌یف، جنگی را علیه شهروندان شرق اوکراین به راه انداختند. ملی‌گرایان اوکراین مرتکب جنایت علیه بی‌گناهان شدند. ارتش روسیه در عملیات خود غیرنظامیان را هدف قرار نمی‌دهد. نماینده اوکراین در شورای امنیت تأکید کرد: پیش‌نویس قطعنامه از روسیه خواست تا خصومت در اوکراین را متوقف کند. تضمین‌های روسیه تحریک‌آمیز است. دبیر کل سازمان ملل هم گفت: جامعه بین‌الملل باید برای توقف جنگ متحد شود. سپس، سفیر آمریکا در شورای امنیت گفت: با وجود وتوی روسیه، به شکل متحد پشت اوکراین و مردم آن هستیم. نماینده انگلیس هم در شورای امنیت از وتوی پیش‌نویس قطعنامه درباره اوکراین انتقاد کرد. نماینده نروژ در شورای امنیت گفت: ما به پیش‌نویس رأی مثبت دادیم و از وتوی روسیه متأسفیم. نماینده ایرلند در شورای امنیت نیز گفت: روسیه حمله بی‌دلیلی به اوکراین انجام داده است. نماینده فرانسه در شورای امنیت هم استفاده روسیه از حق وتو را محکوم کرد (Lieven, 2022, p. 36).

نتیجه‌گیری

جامعه بین‌المللی برای محقق شدن یک بستر مطلوب برای زندگی انسان‌ها باید تلاش‌های خود را برای جلوگیری از وقوع جنگ و درگیری میان کشورها بیشتر کند. این موضوع محقق نمی‌شود مگر با محو و از بین بردن زمینه‌ها و دلایل ایجاد اختلافات و پیش‌بینی سازوکارهای مناسب و عادلانه برای حل‌وفصل نمودن مسالمت‌آمیز این جنگ‌ها و درگیری‌ها و در انتها، انجام اقدامات قاطع و عملی برای مجازات متجاوزان و جنایتکاران جنگی، همانند دادگاه نورنبرگ که برای جنایتکاران و سران دولت‌های مغلوب جنگ برگزار شد. حوزه دریای سیاه به علت مداخلات روسیه در گرجستان و اوکراین به نقطه اشغال بدل شده است. این موضوع نه‌تنها برای امنیت اروپا بلکه برای امنیت دریای مدیترانه نیز دارای پیامدهایی است. جنگ روسیه و اوکراین از سال ۲۰۱۴ میلادی به علت وجود اختلاف بر سر مناطق کریمه و حوادث سیاسی داخلی کشور اوکراین شروع شد و در سال ۲۰۲۲ با حمله نظامی مستقیم روسیه به خاک

اوکراین شدت یافت. در این جنگ، جنایت‌های جنگی متعددی توسط نظامیان روسی توسط منابع بین‌المللی گزارش شده که توسط دولت وقت روسیه پذیرفته نشده است. در شرایط جنگ بین روسیه و اوکراین، حمله سایبری در اوکراین برای روسیه بسیار مفید است. روسیه که در حال حاضر تحت فشار زیادی از سوی ایالات‌متحده و ناتو بر سر موضوع مرز اوکراین است، صرف‌نظر از اینکه آیا این حمله علیه روسیه انجام شده است یا خیر، دستور دولت یا نه بازیگران غیردولتی یا هر کسی که به نمایندگی از کشورها یا گروه‌های خاصی اقدام می‌کند، می‌تواند از فضای سایبری سوءاستفاده کند که برای امنیت جهانی بسیار مضر است زیرا می‌تواند توسط اشخاص ثالث برای افزایش تنش بین کشورها استفاده شود. ردیابی بازیکنانی که حملات سایبری انجام می‌دهند، دشوار است زیرا اکثر افرادی که قربانی این حملات هستند، نمی‌خواهند در مورد آن صحبت کنند زیرا اعتبار امنیتی یک کشور یا سازمان را به خطر می‌اندازد. علاوه بر این، تحقیق در مورد آگاهی امنیتی کاربران موردنیاز است زیرا در تئوری زنجیره امنیتی، ضعیف‌ترین قسمت زنجیره متعلق به انسان است. به‌طورکلی، حملات سایبری اوکراین، ابتدایی بوده و تأثیر محدودی داشتند. اوکراین از فقدان تخصص در زمینه امنیت سایبری، مقررات ضعیف، ظرفیت پاسخگویی محدود و عدم هماهنگی بین آژانس‌های مختلف رنج می‌برد که همگی کاستی‌هایی هستند که کی‌یف در تلاش برای رفع آن است. در طرف دیگر، خرس روسی قرار دارد که مملو از منابع مالی و انسانی بسیار سازمان‌یافته، کارآمد و مراکز تحقیقاتی پیشرفته امنیت سایبری است. توانایی‌های سایبری روسیه در زمینه دفاع و بازدارندگی بسیار پیشرفته است و همیشه قادر به نظارت و پاسخگویی به حملات سایبری، شناسایی شکاف‌های موجود در سیستم‌های دشمن و برنامه‌ریزی حملات مؤثر و دردناکی است که خسارات سنگینی به دشمن وارد می‌کند. مقامات اوکراینی به‌طور کامل از قابلیت‌های سایبری روسیه آگاه هستند و به همین دلیل برای توسعه توانایی‌های خود در زمینه دفاع و امنیت سایبری وارد مسابقه‌ای با زمان شده‌اند که طی آن، هماهنگی با آژانس‌های مرتبط با امنیت سایبری برای آموزش نظارت و پاسخ به این‌گونه حملات انجام می‌شود. یکی از اولویت‌های این آژانس، افزایش آگاهی اپراتورهای زیرساخت‌های حیاتی و ارتباط آن‌ها با مراکز اطلاعات سایبری است تا حملات به‌سرعت قابل رصد، تجزیه‌وتحلیل و پاسخ به آن‌ها باشد. تحلیلگران سیاسی متعارف خاطرنشان می‌کنند که یک رویارویی نظامی روسیه و اوکراین، در صورت وقوع می‌تواند عواقب سایبری خود را داشته باشد. متخصصان سایبری می‌دانند که پشت همه این‌ها یک جنگ سایبری قرار دارد که نبردهای آن از قبل آغاز شده و قربانیان آن از سال ۲۰۱۴ چندین برابر شده است. اوکراین از زمانی که مسکو کریمه را در سال ۲۰۱۴ ضمیمه کرد، تحت حملات سایبری مداوم هکرهای روسی تحت حمایت کرملین قرار گرفته است. جاسوسی سایبری، هک کردن شبکه‌ها، پایگاه‌های اطلاعاتی و سرورها، اختلال در تأسیسات انرژی و ارتباطات، انتشار شایعات و اطلاعات نادرست به بخشی از درگیری بین روسیه و اوکراین تبدیل شده است.

منابع

زمانی، مسعود، و نیکوئی، مجید. (۱۳۹۶). مشروعیت مداخله نظامی کشور ثالث بر اساس دعوت کشور میزبان: بررسی تحلیلی مداخلات نظامی در مالی، اوکراین، سوریه و یمن. *فصلنامه پژوهش حقوق عمومی*، ۱۸(۵۴)، ۲۸۹-۳۱۷.

عزیزی، ستار. (۱۳۹۴). بررسی مشروعیت جدایی یک‌جانبه کریمه از اوکراین: تحلیل رویه و عملکرد دولت‌ها. *فصلنامه پژوهش‌های حقوق تطبیقی*، ۱۹(۱)، ۹۵-۱۱۶.

موسی‌زاده، رضا. (۱۳۹۶). *بایسته‌های حقوق بین‌الملل عمومی* (چاپ ۲۳). تهران: انتشارات میزان.

وثوقی، سعید، صفری، عسگر، و مرادی‌فر، سعیده. (۱۳۹۸). تحولات اوکراین و تأثیر آن بر نظام بین‌الملل. *فصلنامه راهبرد*، ۲۹(۹۶)، ۱۴-۳۶.

Baezner, M. (2018). *Cyber and Information warfare in the Ukrainian conflict* (No. 1, pp. 1-56). ETH Zurich.
BBC. (2022). *Ukraine cyber-attack: Russia to blame for hack, says Kyiv*. https://www.bbc.com/news/world-europe-59992531
Bebler, A. (2015). Crimea and the Russian-Ukrainian conflict. *Romanian Journal of European Affairs*, *15*, 35.
Council of Europe, Commissioner for Human Rights. (2022). Memorandum on the human rights consequences of the war in Ukraine.
CyberPeace Institute. (2022). Ukraine conflict: Cyber-attacks, frequently asked questions. https://cyberpeaceinstitute.org/news/ukraine-conflict-cyberattacks-frequently-asked-questions/.
European Parliamentary Research. (2022). Latest analyses of Russia's war on Ukraine. (European Parliamentary Research Service), PE 212. 525, 1-7.
European Parliamentary Research. (2022). Russia's war on Ukraine in international law and human rights bodies: Bringing institutions back in. (European Parliamentary Research Service), PE 639. 322, 1-12.
European Parliamentary Research. (2022). Russia's war on Ukraine: Investigating and prosecuting international crimes. (European Parliamentary Research Service), PE 733. 525, 1-12.
European Parliamentary Research. (2022). Topical Digest: Russia's war on Ukraine: Background. (European Parliamentary Research Service), PE 325. 657, 1-15.
Food and Agriculture Organization of United Nations. (2022). Ukraine: Note on the impact of the war on food security in Ukraine.
Foreign Affairs Institute. (2022). Geopolitics of the war in Ukraine. 1-77.
Frisby, J. (2020). *Cyber security Exposure Index (CEI)*. https://passwordmanagers.co/cybersecurity-exposure-index/#global
Galeotti, M., & Bowen, A. S. (2018). Putin's Empire of the Mind. *Foreign Policy*, (206), 16.
Ghent Institute for International and European Studies. (2022). Gies Occasional paper: The War in Ukraine. *Gies Occasional Paper*, 1-70.
Gierczak, B. (2020). The Russo-Ukrainian Conflict. *Manhattan College*.
Greenberg, A. (2022). Russia's new cyberwarfare in Ukraine is fast, dirty, and relentless. *Wired*.
Human Rights Declaration. (1948).
Human Rights Monitoring Mission in Ukraine. (2022).
Karaganov, S. (2016). Russia, Europe, and New Challenges. *Russia in Global Affairs*, 19-30.
Lieven, A. (2022). *Ukraine and Russia: A fraternal rivalry*. Washington, D.C: United States Institute of Peace.
Martz, C. (2022). Russian war crimes against Ukraine: The breach of international humanitarian law by the Russian federation. *SSRN Electronic Journal.*
Mearsheimer, J. J. (2014). Why the Ukraine crisis is the West's fault: the liberal delusions that provoked Putin. *Foreign Affairs*, *93*, 77.
Mohee. A. (2022). Cyber war: The hidden side of the Russian-Ukrainian crisis. *The Institute for Arab Research and Studies*.
Neuman, S. (2022). *Ukraine is hit by a massive cyberattack that targeted government websites*. https://www.npr.org/2022/01/14/1073001754/ukraine-cyber-attack-government-websites-russia
O'Neill, P. (2022). *How a Russian cyberwar in Ukraine could ripple out globally*. https://www.technologyreview.com/2022/01/21/1043980/how-a-russian-cyberwar-in-ukraine-could-ripple-out-globally/.
Pikulicka-Wilczewska, A., Sakwa, R. (2016). Ukraine and Russia: People, politics, propaganda and perspectives. *E-International Relations*, 1-280.
Press Release. (2022). Bache let urges respect for international humanitarian law amid growing evidence of war crimes in Ukraine.
Priyono, U. (2022). Cyber Warfare as Part of Russia and Ukraine Conflict. *Jurnal Diplomasi Pertahanan*, *8*(2), 44-59.
Prohorovs, A. (2022). Russia's war in Ukraine: Consequences for European countries' businesses and economies. *Journal of risk and financial management*, *15*(7), 295.
Rice, D. (2022). The Untold Story of the Battle for Kyiv. *Small Wars Journal*, *31*.
Robinson, J. (2021). *Cyber warfare statistics: A decade of geopolitical attacks*. https://www.privacyaffairs.com/geopolitical-attacks

Sanger, D. E. (2022). Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks. *International New York Times*, NA-NA.
Schulze, M., & Kerttunen, M. (2023). *Cyber operations in Russia's war against Ukraine: Uses, limitations, and lessons learned so far* (No. 23/2023). SWP Comment.
Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12*(3), 90-113.
The Institute for Economics & Peace Briefing Series. (2021). Ukraine Russia Crisis: Terrorism Briefing.
United Nations Charter. (1948).
United Nations High Commissioner for Human Rights. (2022). New report by UN Human Rights shows the shocking toll of the war in Ukraine.
United Nations Human Rights. (2022). New report by UN Human Rights shows the shocking toll of the war in Ukraine.
United Nations. (2022). Brief No. 1: Global Impact of war in Ukraine on food, energy and finance systems. 1-22.
Watling, J., & Reynolds, N. (2022). Operation Z: The Death Throes of an Imperial Delusion.
Watling, J., & Reynolds, N. (2022). Ukraine at War Paving the Road from Survival to Victory. *Royal United Services Institute for Defense and Security Studies*, 1-25.
Watling, W., & Reynolds, N. (2022). *Ukraine at war: Paving the road from survival to victory. royal united services institute*. https://static.rusi.org/special-report-202207-ukraine-final-web.pdf
Watts, C. (2022). *Preparing for a Russian cyber offensive against Ukraine this winter*. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/
Windrem, R. (2016). *Timeline: Ten years of russian cyber attacks on other nations*. https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111
Zoria, Y. (2022). *Ukrainian official sites under massive cyberattack with a Russian trace*. https://euromaidanpress.com/2022/01/14/ukraine-under-massive-cyberattack-with-a-russian-trace/

استناد به این مقاله: انصاری مهیاری، علیرضا، حسینی، زهرا سادات، و رادمان، احمد. (۱۴۰۳). نگاهی حقوقی به حملات نظامی و سایبری روسیه به اوکراین در پرتو حقوق بین‌الملل عمومی. *فصلنامه تحقیقات نوین میان‌رشته‌ای حقوق*، ۴(۱)، ۵۲-۶۶.