فصلنامه علمی راهبرد سیاسی
انتشارات دانشگاه راهبردی

راهبردهای سایبری و مسئولیت بین‌المللی دولت‌ها در نظم امنیتی غرب آسیا

مهسا اکبری[1] رضا احمدی[2]

دوره ۹، شماره ۲، پیاپی ۳۳
تابستان ۱٤۰٤

مقاله پژوهشی

تاریخ دریافت:
۱٤۰٤/۰۵/۲۵
تاریخ پذیرش:
۱٤۰٤/۰۶/۲۹
صص: ۲۸۳-۲۶۳

شاپا چاپی: ٤۵۶۵-۲۵۸۸
الکترونیکی: ۰۳۸۱-۲۷۱۷

ISC

چکیده

رشد شتابان فناوری و وابستگی فزاینده به زیرساخت‌های دیجیتال، مفهوم مسئولیت‌پذیری دولت‌ها را در فضای سایبری به یکی از مهم‌ترین چالش‌های نظم بین‌المللی معاصر بدل کرده است. نبود تعریف واحد از «تهاجم سایبری» و معیارهای روشن انتساب سبب شده دولت‌ها در مرز مبهم صلح و درگیری حرکت کنند و بدون پذیرش مسئولیت مستقیم، عملیات‌های پرهزینه‌ای انجام دهند. این پژوهش با رویکرد تبیینی ـ تحلیلی و روش کیفی تطبیقی، با تحلیل اسناد بین‌المللی، گزارش‌های امنیتی و رفتار دولت‌ها، چارچوبی سه‌لایه شامل «هنجارها و حقوق بین‌الملل»، «بازدارندگی و دفاع چندلایه» و «انتساب معتبر همراه با روایت سازی شفاف» ارائه می‌کند. یافته‌ها نشان می‌دهد که ضعف سازوکارهای حقوقی و فقدان همکاری اطلاعاتی، مشروعیت پاسخ دولت‌ها را تضعیف کرده و خطر آسیب به غیرنظامیان را افزایش می‌دهد. فقدان استانداردهای شفاف و شبکه‌های اطلاعاتی معتبر، مشروعیت پاسخ دولت‌ها را تضعیف و خطر گسترش درگیری و آسیب به غیرنظامیان را افزایش می‌دهد. در مقابل، ترکیب همکاری فنی، هنجارسازی فعال و ارتقای شفافیت می‌تواند بازدارندگی پایدار ایجاد کند. پژوهش نتیجه می‌گیرد که تقویت همکاری‌های فنی، شفافیت در انتساب و نقش‌آفرینی فعال‌تر نهادهای بین‌المللی برای افزایش پاسخ‌گویی و حمایت از غیرنظامیان ضروری است

کلیدواژه‌ها: جنگ سایبری، مسئولیت دولت‌ها، انتساب سایبری، بازدارندگی و دفاع سایبری، حقوق بین‌الملل سایبری.

۱. دکتری تخصصی مدیریت دولتی، مدیریت دولتی، دانشکده مدیریت و حسابداری،دانشگاه علامه طباطبائی، تهران، ایران
(نویسنده مسئول) akbari_mahsa@atu.ac.ir
۲. دانشجوی دکتری تخصصی مهندسی صنایع گرایش مدیریت کیفیت وبهره وری، دانشگاه صنعتی مالک اشتر، تهران، ایران

۱- مقدمه

تحول دیجیتال طی دو دهه‌ی گذشته، نظم امنیتی و سیاسی جهان را دستخوش تغییراتی بنیادین کرده است. اگر در گذشته ابزارهای اعمال قدرت در انحصار ارتش‌های کلاسیک، دیپلماسی سنتی و اقتصادهای بزرگ بود، امروز رقابت‌های ژئوپلیتیک و امنیتی در بُعدی نامرئی و بی‌مرز به‌نام «فضای سایبری» جریان دارد. عملیات‌هایی که پیش‌تر نیازمند لشکرکشی و هزینه‌های هنگفت نظامی بودند، اکنون با چند خط کد می‌توانند شبکه‌های انرژی، زیرساخت‌های مالی، ارتباطی یا خدمات عمومی را از کار بیندازند و زندگی میلیون‌ها نفر را مختل کنند (Lindsay et al., 2021: 18). این دگرگونی نه‌تنها مفهوم امنیت و قدرت را بازتعریف کرده، بلکه بنیان‌های سنتی حقوق بین‌الملل، حاکمیت ملی و حتی بازدارندگی را با چالش‌های عمیق روبه‌رو ساخته است. در این میان، یکی از مهم‌ترین مسائل در عرصه‌ی روابط بین‌الملل، تعیین حدود و مصادیق «مسئولیت دولت‌ها» در فضای سایبری است. در حالی که اصولی مانند «عدم مداخله»، «منع توسل به زور» و «مسئولیت بین‌المللی» در حقوق کلاسیک تثبیت شده‌اند، اعمال آن‌ها در فضای دیجیتال با ابهامات گسترده مواجه است. نه تعریف واحدی از «حمله‌ی سایبری» وجود دارد، نه اجماع روشنی درباره‌ی معیارهای انتساب عملیات به یک دولت. همین خلأ مفهومی سبب شده است که دولت‌ها بتوانند در «منطقه‌ی خاکستری» میان صلح و درگیری حرکت کنند و بدون پذیرش مسئولیت رسمی، عملیات‌هایی را انجام دهند که پیامدهای راهبردی و انسانی سنگینی دارند (Schmitt, 2017: 24). تحولات میدانی اخیر، اهمیت این مسئله را بیش از پیش نمایان کرده‌اند. جنگ روسیه و اوکراین نه‌تنها در عرصه‌ی نظامی بلکه در فضای سایبری نیز به یکی از پیچیده‌ترین منازعات دهه‌ی اخیر تبدیل شد. از حملات به شبکه‌ی برق اوکراین گرفته تا نفوذ به سامانه‌های دولتی و زیرساخت‌های حیاتی، این منازعه نشان داد که سایبر نه یک ابزار جانبی بلکه بخشی از «میدان نبرد چندبُعدی» است (CISA/ICS-CERT, 2016: Greenberg, 2020: 121). در غرب آسیا نیز درگیری دوازده‌روزه‌ی ایران و رژیم صهیونیستی در سال ۲۰۲۵ گواهی دیگر بر همین واقعیت بود؛ در این جنگ، عملیات‌های سایبری هم‌زمان با اقدامات نظامی و اطلاعاتی، بخشی از راهبرد کلان دو طرف برای اعمال فشار، تغییر موازنه و اثرگذاری بر افکار عمومی بودند. این تحولات به‌روشنی نشان می‌دهند که «فضای سایبری» دیگر نه عرصه‌ای حاشیه‌ای، بلکه میدان اصلی

رقابت‌های امنیتی و ژئوپلیتیک در قرن بیست‌ویکم است .پیامدهای این روند صرفاً محدود به دولت‌ها نیست. هدف‌گیری زیرساخت‌های غیرنظامی – از سامانه‌های آب و برق گرفته تا بیمارستان‌ها و خدمات شهری – نشان داده که جنگ‌های سایبری می‌توانند زندگی روزمره‌ی مردم را مختل کنند و امنیت انسانی را در مقیاسی بی‌سابقه تهدید نمایند .(ESET, 2022: 5) علاوه‌براین، «روایت‌سازی» و جنگ اطلاعاتی به یکی از ابعاد تعیین‌کننده در مشروعیت‌بخشی عملیات سایبری تبدیل شده‌اند؛ دولت‌هایی که می‌توانند روایت مسلط را در فضای رسانه‌ای و دیپلماتیک شکل دهند، نه‌تنها در جنگ اطلاعاتی برتری می‌یابند بلکه مشروعیت اقدامات خود را نیز در سطح بین‌المللی تقویت می‌کنند .(Rid & Buchanan, 2015: 10) با وجود این تحولات، نظام حقوق بین‌الملل هنوز نتوانسته پاسخ‌های قانع‌کننده‌ای به این چالش‌ها ارائه کند. «تالین منوال ۲» اگرچه تلاش مهمی برای تطبیق قواعد سنتی با واقعیت‌های نوین بوده، اما به دلیل فقدان ضمانت اجرایی و نبود اجماع جهانی در عمل ناکافی مانده است (Tsagourias & Buchan, 2021: 59). سازمان‌های بین‌المللی نیز تاکنون نتوانسته‌اند سازوکار مؤثری برای انتساب، نظارت و پاسخ‌گویی ایجاد کنند و اغلب واکنش‌ها به عملیات‌های سایبری در حد بیانیه‌های سیاسی باقی مانده‌اند .(UNIDIR, 2024: 12) این ضعف نهادی نه‌تنها هزینه‌های نقض هنجارها را کاهش داده، بلکه خطر بی‌ثباتی و افزایش منازعات سایبری را نیز تشدید کرده است . در پرتو این شرایط، پژوهش حاضر با هدف تحلیل مسئولیت بین‌المللی دولت‌ها در جنگ‌های سایبری و بررسی ابعاد حقوقی، امنیتی و روایتی آن شکل گرفته است. پرسش محوری پژوهش چنین است: در غیاب تعریف واحد از تهاجم سایبری و نبود معیارهای شفاف انتساب، چگونه می‌توان رفتار دولت‌ها را در این حوزه ارزیابی کرد و چارچوبی برای پاسخ‌گویی و مشروعیت‌بخشی ارائه داد؟ فرضیه‌ی اصلی بر این پیش‌فرض استوار است که مسئولیت‌پذیری دولت‌ها تنها با تلفیق سه مؤلفه‌ی کلیدی یعنی هنجارسازی حقوقی، بازدارندگی چندلایه، و انتساب معتبر همراه با روایت‌سازی شفاف امکان‌پذیر است.

پژوهش حاضر با بهره‌گیری از روش تحلیل کیفی و تطبیقی، ضمن بررسی اسناد بین‌المللی، گزارش‌های امنیتی و سیاست‌های ملی، رفتار دولت‌ها را در دو مطالعه‌ی موردی اصلی – جمهوری اسلامی ایران و رژیم صهیونیستی – و در بستر تحولات گسترده‌تر بین‌المللی تحلیل می‌کند. هدف

نهایی، ارائه‌ی چارچوبی تحلیلی و راهبردی است که هم برای فهم علمی مسئله و هم برای سیاست‌گذاری عملی در سطح ملی و بین‌المللی قابل استفاده باشد.

۲ .روش پژوهش

این پژوهش از نظر هدف، تبیینی و تحلیلی و از نظر روش، کیفی و تطبیقی است. هدف اصلی آن تبیین سازوکارها و عوامل مؤثر بر مسئولیت بین‌المللی دولت‌ها در جنگ‌های سایبری و تحلیل نحوه‌ی بازنمایی و مشروعیت‌بخشی این رفتارها در سطح بین‌المللی است. با توجه به ماهیت چندوجهی موضوع، ترکیبی از روش‌های تحلیل مضمون، تحلیل تطبیقی و تحلیل روایی در مراحل مختلف تحقیق به‌کار گرفته شده است تا امکان بررسی هم‌زمان ابعاد حقوقی، سیاسی، امنیتی و ارتباطی مسئله فراهم شود.

۲-۱ .گردآوری داده‌ها

داده‌های پژوهش از طریق روش اسنادی و کتابخانه‌ای گردآوری شده‌اند. منابع مورد استفاده شامل اسناد رسمی سازمان‌های بین‌المللی (از جمله سازمان ملل متحد، گروه کارشناسان دولتی، و نهادهای تخصصی امنیت سایبری)، گزارش‌های مراکز پژوهشی و اندیشکده‌ها، مقالات علمی منتشرشده در نشریات معتبر، بیانیه‌های رسمی دولت‌ها، و تحلیل‌های منتشرشده در رسانه‌های بین‌المللی بوده‌اند. معیار انتخاب منابع، اعتبار علمی، ارتباط مستقیم با موضوع پژوهش، و روزآمدی آن‌ها بوده است. این تنوع منابع به پژوهش کمک کرده تا ابعاد حقوقی، سیاسی، فناورانه و روایتی موضوع به‌طور هم‌زمان مورد توجه قرار گیرد.

۲-۲ .روش تحلیل داده‌ها

تحلیل داده‌ها در سه مرحله انجام شده است. در مرحله‌ی نخست، از تحلیل مضمون (Thematic Analysis)برای استخراج مفاهیم کلیدی مانند «هنجارهای بین‌المللی»، «انتساب معتبر»، «بازدارندگی چندلایه» و «روایت‌سازی سیاسی» استفاده شده است. در مرحله‌ی دوم، با به‌کارگیری روش تطبیقی (Comparative Analysis) رفتار دولت‌ها در مواجهه با حملات سایبری، سیاست‌های بازدارندگی، و شیوه‌های توجیه اقدامات‌شان در سطح بین‌المللی مقایسه شده است. در مرحله‌ی سوم، پژوهش با استفاده از تحلیل روایی (Narrative Analysis) به بررسی

نحوه‌ی بازنمایی حملات سایبری در گفتمان‌های رسمی، رسانه‌ای و دیپلماتیک پرداخته و نشان داده است که چگونه روایت‌سازی بر مشروعیت یا عدم مشروعیت اقدامات سایبری تأثیر می‌گذارد.

۲-۳ .دامنه پژوهش و انتخاب موارد موردی

دامنه‌ی زمانی پژوهش سال‌های ۲۰۱۵ تا ۲۰۲۵ را دربرمی‌گیرد تا هم تحولات یک دهه‌ی اخیر و هم رخدادهای بسیار تازه مانند «جنگ دوازده‌روزه سایبری و نظامی ایران و رژیم صهیونیستی» در سال ۲۰۲۵ پوشش داده شود. انتخاب این بازه به پژوهش اجازه می‌دهد روندهای بلندمدت، تغییرات راهبردی و نقاط عطف در مسئولیت‌پذیری دولت‌ها را بررسی کند .در بخش مطالعات موردی، دو بازیگر اصلی یعنی جمهوری اسلامی ایران و رژیم صهیونیستی انتخاب شده‌اند، زیرا هر دو نقش محوری در تحولات سایبری غرب آسیا ایفا کرده‌اند و رفتار آن‌ها بازتابی از چالش‌های حقوقی و سیاسی گسترده‌تر در عرصه بین‌المللی است. علاوه‌براین، برای درک بهتر زمینه بین‌المللی، به‌طور مقایسه‌ای به تجارب ایالات متحده، روسیه و برخی کشورهای اروپایی نیز اشاره شده است.

۳ .پیشینه پژوهش

۳-۱ .چارچوب‌های حقوقی و هنجاری

مسئولیت دولت‌ها در فضای سایبری بحث مسئولیت بین‌المللی دولت‌ها در فضای سایبری از دهه‌ی ۲۰۱۰ به یکی از موضوعات محوری حقوق بین‌الملل تبدیل شده است. نقطه‌ی آغاز این مباحث را می‌توان در پروژه‌ی Tallinn Manual 2.0 دانست که کوشید اصول سنتی مانند حاکمیت، عدم مداخله و استفاده از زور را با واقعیت‌های نوین فضای مجازی انطباق دهد (Schmitt, 2017: 11–29). این سند هرچند الزام‌آور نیست، اما مبنایی برای تفسیر قواعد در مواجهه با عملیات سایبری فراهم کرده و در رویه‌ی رسمی دولت‌ها، بیانیه‌های ملی و تصمیمات سازمان‌های بین‌المللی تأثیرگذار بوده است .(UNIDIR, 2024: 3–5) بااین‌حال، بخش بزرگی از ادبیات حقوقی به خلأهای موجود اشاره می‌کند: نبود تعریف جامع از «تهاجم سایبری»، عدم اجماع درباره‌ی معیارهای «انتساب» و فقدان رویه‌ی قضایی منسجم موجب شده دولت‌ها بتوانند در «منطقه خاکستری» فعالیت کنند و مسئولیت‌پذیری را دور بزنند (Tsagourias & Buchan, 2021: 54–59). به‌علاوه، بسیاری از پژوهشگران تأکید دارند که اصول سنتی حقوق بین‌الملل

برای فضای سایبری کافی نیست و باید قواعد جدیدی متناسب با ویژگی‌های این عرصه (مانند سرعت، ناشناس‌بودن و مرزناپذیری) تدوین شود (Roscini, 2020: 112–118). در ایران نیز شماری از مطالعات به این موضوع پرداخته‌اند. برای مثال، شهبازی و آقاجانی رونقی نشان داده‌اند که قواعد موجود در زمینه‌ی مسئولیت دولت می‌تواند حتی بر عملیات «زیرآستانه‌ای» نیز اعمال شود و در چارچوب حقوق بین‌الملل قابل پیگیری باشد (شهبازی و آقاجانی رونقی، ۱٤۰۰: ۳۵). همچنین صفری و احمدی بر ضرورت بازتعریف مفهوم «تهاجم» در فضای سایبری و تطبیق آن با موازین امنیت ملی ایران تأکید کرده‌اند (صفری و احمدی، ۱٤۰۱: ۵۲). این مباحث نشان می‌دهد که پژوهش حاضر باید فراتر از توصیف هنجارها، به بررسی کارکرد واقعی آن‌ها در شرایط رقابت ژئوپلیتیکی بپردازد جایی که حقوق، سیاست و امنیت در هم تنیده می‌شوند.

۲-۳. بازدارندگی و راهبردهای سایبری در سیاست خارجی

در دهه‌ی اخیر، مفهوم بازدارندگی سایبری به‌عنوان یکی از محورهای اصلی سیاست‌گذاری امنیتی دولت‌ها مطرح شده است. برخلاف دوران جنگ سرد که بازدارندگی عمدتاً به معنای تهدید به پاسخ متقابل بود، در عصر دیجیتال، بازدارندگی شامل مجموعه‌ای از راهبردهای مکمل مانند «دفاع لایه‌ای»، «انکار دستاورد» و «هنجارسازی» نیز می‌شود (Nye, 2017: 45–47). پژوهشگران معتقدند که تلفیق این ابزارها می‌تواند احتمال موفقیت حملات سایبری را کاهش دهد و هزینه‌های مهاجم را افزایش دهد (Lindsay et al., 2021: 225–231). از منظر سیاست خارجی، جنگ سایبری دیگر صرفاً ابزاری نظامی نیست، بلکه بخشی از دیپلماسی قدرت‌های منطقه‌ای و جهانی محسوب می‌شود. به‌عنوان نمونه، ایالات متحده در «راهبرد ملی سایبری ۲۰۲۳» خود بر نقش بازدارندگی فعال و همکاری‌های چندجانبه برای افزایش مشروعیت پاسخ تأکید کرده است (White House, 2023: 14–18). در سطح منطقه‌ای نیز، اسرائیل با بهره‌گیری از توان فناورانه و همکاری اطلاعاتی با آمریکا، توانسته راهبرد سایبری خود را در چارچوب سیاست خارجی تعریف کند و آن را به ابزار اعمال فشار علیه رقبا تبدیل نماید (Maurer, 2018: 33–40). در ایران نیز سیاست‌گذاران به اهمیت بازدارندگی چندلایه واقف شده‌اند. پژوهش صفری و احمدی نشان می‌دهد که ایران ضمن توسعه‌ی دفاع بومی، بر ارتقای تاب‌آوری زیرساخت‌ها و انکارپذیری راهبردی نیز تمرکز کرده است (صفری و احمدی، ۱٤۰۱: ٦٤). بااین‌حال، چالش‌های

همکاری بین‌المللی و محدودیت در شبکه‌های اطلاعاتی همچنان مانع تحقق کامل بازدارندگی می‌شود .پیوند میان بازدارندگی و مسئولیت‌پذیری، مقدمه‌ای برای ورود به بحث مهم‌تری است: چگونگی «انتساب عملیات سایبری» و نقش آن در مشروعیت‌بخشی به پاسخ‌های دولت‌ها.

۳-۳ .انتساب عملیات، مشروعیت پاسخ و روایت‌سازی انتساب

عملیات سایبری یعنی نسبت دادن یک حمله به یک دولت خاص یکی از چالش‌برانگیزترین مباحث حقوقی و سیاسی در فضای مجازی است. پژوهش‌ها نشان می‌دهد که هیچ استاندارد واحدی برای انتساب وجود ندارد و دولت‌ها ترکیبی از شواهد فنی، تحلیل اطلاعاتی و قرائن رفتاری را به‌کار می‌برند .(Rid & Buchanan, 2015: 4–12) در عین حال، شکست در ارائه شواهد قانع‌کننده می‌تواند مشروعیت پاسخ را زیر سؤال ببرد و حتی هزینه‌های سیاسی بین‌المللی به‌دنبال داشته باشد.(Greenberg, 2020: 122–128)

ادبیات جدید همچنین بر اهمیت «روایت‌سازی» تأکید دارد: ارائه روایت منسجم و مستند از منشأ حمله و دلایل پاسخ می‌تواند حمایت متحدان را جلب کند و هزینه‌های دیپلماتیک را کاهش دهد .(Klimburg, 2017: 73–80)در این زمینه، اسرائیل از شبکه‌های اطلاعاتی گسترده و رسانه‌های جهانی برای تقویت روایت خود بهره می‌برد، در حالی که ایران بیشتر بر رسانه‌های داخلی و منطقه‌ای متکی است که دامنه‌ی اثرگذاری محدودتری دارند .(Bronk & Tikk, 2013: 45–50) این مباحث نشان می‌دهد که انتساب معتبر نه‌تنها یک ضرورت حقوقی بلکه یک ابزار راهبردی در سیاست خارجی است که می‌تواند بر میزان بازدارندگی و مشروعیت بین‌المللی تأثیر مستقیم بگذارد.

۳-٤ .مطالعات موردی و تجربه‌های غرب آسیا

تجربه‌های عملی در غرب آسیا نشان می‌دهد که نظریه‌های حقوقی و امنیتی در میدان عمل با پیچیدگی‌های جدیدی مواجه می‌شوند. یکی از برجسته‌ترین موارد، حملات سایبری روسیه علیه اوکراین از سال ۲۰۱۵ به این سو است که نشان داد انتساب معتبر بدون ائتلاف‌های اطلاعاتی و همکاری‌های بین‌المللی دشوار است .(CISA/ICS-CERT, 2016: 1) در سطح منطقه‌ای، حملات سایبری اسرائیل به زیرساخت‌های ایران از جمله حمله به بندر شهید رجایی (۲۰۲۰) — و پاسخ‌های متقابل تهران، اهمیت تفکیک اهداف نظامی و غیرنظامی را به یک مسئله‌ی هنجاری تبدیل کرده‌اند .(ESET, 2022: 5–6) مطالعات داخلی نیز به ابعاد بومی این مسئله پرداخته‌اند.

برای مثال، قرباغی و کشاورز نشان می‌دهند که خلأ در سازوکارهای بین‌المللی انتساب موجب شده ایران در اقناع جامعه بین‌المللی با چالش مواجه شود (قرباغی و کشاورز، ۱۳۹۹: ٤٨). همچنین، شهبازی و آقاجانی رونقی بیان می‌کنند که نهادینه‌سازی سازوکارهای داخلی شفاف می‌تواند مشروعیت پاسخ ایران را تقویت کند (شهبازی و آقاجانی رونقی، ١٤٠٠: ٤٥)

این مطالعات نشان می‌دهند که تحلیل مسئولیت دولت‌ها در جنگ سایبری بدون توجه به زمینه‌ی ژئوپلیتیک، روایت‌سازی و ظرفیت اطلاعاتی ناقص خواهد بود, نتیجه‌ای که مبنای چارچوب نظری این مقاله را تشکیل می‌دهد.

٤ .چارچوب نظری و رهیافت تحلیلی

رشد پرشتاب فناوری‌های دیجیتال و گسترش فضای سایبری باعث شده روابط بین‌الملل، امنیت و حقوق بین‌الملل با تحولات بنیادینی روبه‌رو شوند. فضای سایبری نه‌تنها به‌عنوان عرصه‌ای جدید برای رقابت میان دولت‌ها مطرح است، بلکه با مفاهیم سنتی امنیت، حاکمیت و مسئولیت نیز پیوند خورده است. بر همین اساس، پژوهش حاضر برای تحلیل مسئله «مسئولیت بین‌المللی دولت‌ها در جنگ‌های سایبری» چارچوبی سه‌لایه طراحی می‌کند که از ادبیات پژوهش استخراج شده و شامل:

۱) هنجارها و قواعد حقوق بین‌الملل، ۲) بازدارندگی و راهبردهای سایبری، و ۳) انتساب عملیات و مشروعیت پاسخ می‌شود.

٤-١ .هنجارها و قواعد حقوق بین‌الملل

نخستین لایه این چارچوب بر مبنای نظریه‌های حقوق بین‌الملل عمومی شکل گرفته و فرض می‌کند که رفتار دولت‌ها در فضای سایبری را می‌توان تا حد زیادی با اصول شناخته‌شده‌ای مانند «حاکمیت»، «عدم مداخله» و «ممنوعیت توسل به زور» تبیین کرد (Schmitt, 2017: 21). بااین‌حال، ویژگی‌های خاص فضای سایبری – از جمله ناشناس‌بودن، سرعت بالا و نبود مرزهای فیزیکی – باعث شده اجرای این اصول با ابهاماتی همراه شود (Roscini, 2020: 110). در نتیجه، برخی از پژوهشگران بر ضرورت توسعه قواعد جدید یا بازتفسیر اصول موجود تأکید کرده‌اند (Tsagourias & Buchan, 2021: 59).این بخش از چارچوب نظری فرض می‌کند که میزان

انطباق دولت‌ها با هنجارهای بین‌المللی و نحوه‌ی تفسیر آن‌ها از این اصول، یکی از عوامل کلیدی در شکل‌گیری مسئولیت بین‌المللی و قضاوت جهانی درباره مشروعیت اقدامات سایبری آن‌هاست.

۴-۲ .بازدارندگی و راهبردهای سایبری

لایه دوم چارچوب، از نظریه‌های امنیت بین‌الملل و بازدارندگی اقتباس شده است. برخلاف دوران جنگ سرد که بازدارندگی عمدتاً بر تهدید به پاسخ متقابل نظامی استوار بود، در فضای سایبری مفهوم بازدارندگی چندلایه و پیچیده‌تر است و شامل راهبردهایی مانند دفاع فعال، انکار دستاورد، تاب‌آوری زیرساخت‌ها و همکاری‌های بین‌المللی می‌شود (Nye, 2017: 45 Lindsay et al., 2021:226)

این چارچوب همچنین بر نقش «حاکمیت سایبری» تأکید دارد؛ مفهومی که نشان می‌دهد دولت‌ها علاوه بر حفاظت از زیرساخت‌های ملی، به دنبال شکل‌دهی استانداردها و قواعد فنی جهانی نیز هستند تا موقعیت راهبردی خود را تقویت کنند .(Klimburg, 2017: 74) در این میان، سطح توانایی یک دولت در ایجاد بازدارندگی مؤثر می‌تواند بر میزان مسئولیت‌پذیری و پاسخگویی بین‌المللی آن نیز تأثیر بگذارد.

۴-۳ .انتساب، مشروعیت و روایت‌سازی

لایه سوم بر نظریه‌های سیاست بین‌الملل و مشروعیت مبتنی است و فرض می‌کند که «انتساب معتبر» عملیات سایبری پیش‌شرط اصلی برای مشروعیت‌بخشی به پاسخ دولت‌ها محسوب می‌شود .(Rid & Buchanan, 2015: 6)اگر دولت‌ها نتوانند شواهد کافی برای نسبت دادن حمله به یک بازیگر خاص ارائه دهند، پاسخ آن‌ها ممکن است از دید جامعه بین‌المللی نامشروع تلقی شود .(Greenberg, 2020: 127)همچنین، «روایت‌سازی» یا شکل‌دهی به ادراک عمومی درباره منشأ حمله و ضرورت پاسخ، بخش مهمی از مسئولیت‌پذیری در فضای سایبری را تشکیل می‌دهد. دولت‌هایی که توانایی بیشتری در روایت‌سازی دارند – از طریق شبکه‌های رسانه‌ای، ائتلاف‌های سیاسی و همکاری‌های اطلاعاتی – معمولاً حمایت بین‌المللی بیشتری برای اقدامات خود جلب می‌کنند .(Bronk & Tikk, 2013: 48)

با وجود تلاش‌های ارزشمند در تبیین ابعاد حقوقی، امنیتی و سیاسی جنگ‌های سایبری، مرور کلی پژوهش‌های موجود نشان می‌دهد که این حوزه هنوز در مرحله‌ی «گذار مفهومی» قرار دارد.

بسیاری از مطالعات، اگرچه از منظر نظری دقیق و مستدل هستند، اما در سطح «تحلیل‌های بخشی» باقی مانده‌اند و کمتر کوشیده‌اند تا چارچوبی تلفیقی ارائه دهند که ابعاد مختلف مسئولیت‌پذیری را در کنار یکدیگر بسنجد (Roscini, 2020; Tsagourias & Buchan, 2021). این خلأ سبب شده است که مقایسه‌ی نظام‌مند میان دولت‌ها دشوار شود و ارزیابی نهایی از مشروعیت یا مسئولیت اقدامات آن‌ها بیشتر مبتنی بر برداشت‌های سیاسی یا امنیتی باشد تا ارزیابی‌های حقوقی و هنجاری .نکته‌ی دیگر آن است که بسیاری از پژوهش‌های پیشین، مسئله‌ی «روایت‌سازی» را به‌عنوان یک مؤلفه‌ی کلیدی مسئولیت بین‌المللی نادیده گرفته‌اند. در حالی که تجربه‌ی حملات سایبری روسیه علیه اوکراین، عملیات‌های رژیم صهیونیستی در غرب آسیا و حتی حملات گسترده به زیرساخت‌های ایالات متحده نشان داده‌اند که شکل‌دهی به افکار عمومی و کنترل روایت در فضای رسانه‌ای، می‌تواند به اندازه‌ی اقدامات فنی و نظامی بر ادراک مشروعیت تأثیر بگذارد (Greenberg, 2020; Rid & Buchanan, 2015).

این بعد روایتی، که اغلب در تقاطع سیاست، امنیت و ارتباطات قرار دارد، تاکنون در پژوهش‌های دانشگاهی کمتر مورد توجه قرار گرفته و همین امر یکی از خلأهای مهم ادبیات را شکل می‌دهد .در عین حال، در سطح منطقه‌ای نیز پژوهش‌های اندکی به مطالعه‌ی تطبیقی رفتار دولت‌ها در غرب آسیا پرداخته‌اند. بیشتر مطالعات تمرکز خود را بر ایالات متحده، چین یا روسیه قرار داده‌اند و نقش بازیگران منطقه‌ای به‌ویژه ایران و رژیم صهیونیستی در شکل‌دهی به قواعد و هنجارهای سایبری کمتر مورد بررسی قرار گرفته است (صفری و احمدی، ۱٤۰۱). پژوهش حاضر با تمرکز بر این دو بازیگر و با تلفیق رویکردهای حقوقی، امنیتی و روایتی، تلاش دارد تا تصویری جامع‌تر از الگوهای مسئولیت‌پذیری در جنگ‌های سایبری ارائه دهد و شکاف‌های موجود در ادبیات را پر کند.

٤-٤ .چارچوب تحلیلی پیشنهادی

برآیند این سه لایه نشان می‌دهد که مسئولیت بین‌المللی دولت‌ها در فضای سایبری نه‌تنها تابع قواعد حقوقی، بلکه نتیجه‌ی تعامل پیچیده میان هنجارها، بازدارندگی و انتساب است. از این منظر، هر دولت برای مدیریت مسئولیت خود باید سه گام اصلی را دنبال کند

۱. همسوسازی اقدامات سایبری با اصول و هنجارهای بین‌المللی؛

۲. توسعه راهبردهای بازدارندگی چندلایه برای کاهش انگیزه و توان مهاجمان؛

۳. ایجاد سازوکارهای انتساب معتبر و روایت‌سازی مؤثر برای مشروعیت‌بخشی به پاسخ‌ها. این چارچوب مبنای تحلیل در بخش‌های بعدی مقاله را فراهم می‌کند و امکان بررسی سیاست‌ها و اقدامات دولت‌ها را در سطحی فراتر از توصیف صرف فراهم می‌سازد.

در پرتو مباحث نظری و پژوهش‌های مروری که تاکنون بررسی شد، می‌توان دریافت که مسئله‌ی مسئولیت‌پذیری دولت‌ها در جنگ‌های سایبری از منظرهای گوناگون مورد توجه قرار گرفته است. با این حال، برای دستیابی به درکی نظام‌مندتر و روشن‌تر از مسیر تحول این حوزه، لازم است مطالعات پیشین به‌صورت ساختارمند و مقایسه‌پذیر بازنمایی شوند. از این‌رو، در جدول زیر مهم‌ترین پژوهش‌های انجام‌شده در حوزه‌ی مسئولیت بین‌المللی دولت‌ها در فضای سایبری با تمرکز بر ابعاد حقوقی، امنیتی، هنجاری و روایتی گردآوری شده‌اند. این جدول، ضمن نشان‌دادن روندهای اصلی تحقیق، روش‌های به‌کاررفته و یافته‌های کلیدی، دلالت‌های هر مطالعه برای پژوهش حاضر را نیز مشخص می‌کند و مبنایی تحلیلی برای تدوین چارچوب مفهومی در بخش بعدی فراهم می‌آورد.

۵-٤ دلالت‌های پژوهش‌های پیشین

برای تحقیق حاضر مرور نظام‌مند مطالعات پیشین نشان می‌دهد که ادبیات موجود درباره‌ی مسئولیت دولت‌ها در جنگ‌های سایبری، علی‌رغم رشد قابل‌توجه در دهه‌ی اخیر، هنوز دارای کاستی‌های نظری و تحلیلی مهمی است. نخست آن‌که بخش عمده‌ای از پژوهش‌ها، همان‌طور که در آثار Schmitt (2017) ، Tsagouriasو Buchan (2021) و Delerue (2020) دیده می‌شود، همچنان بر تفسیر و بسط اصول کلاسیک حقوق بین‌الملل متمرکز هستند و کمتر به چگونگی انطباق آن‌ها با پویایی‌های خاص فضای سایبری پرداخته‌اند. در نتیجه، هنوز چارچوبی واحد و مورد اجماع برای تعریف مفاهیمی چون «تهاجم سایبری»، «مداخله» و «مسئولیت بین‌المللی» وجود ندارد و همین خلأ، راه را برای اقدامات خاکستری و زیرآستانه‌ای باز گذاشته است .دوم آن‌که، همان‌طور که مطالعات Rid و Buchanan (2015) ، Maurerو (2018) Zetter (2014)نشان می‌دهند، مسئله‌ی «انتساب» همچنان یکی از چالش‌های اساسی در تعیین مسئولیت دولت‌هاست. فقدان معیارهای فنی و حقوقی مشترک برای انتساب باعث شده است که دولت‌ها بتوانند با استفاده از بازیگران نیابتی، عملیات‌های مخفی و سازوکارهای انکارپذیری، از

مسئولیت حقوقی بگریزند. این مسئله به‌ویژه در شرایطی که واکنش‌های بین‌المللی مبتنی بر اجماع سیاسی است، اهمیت بیشتری می‌یابد .سوم، ادبیات بازدارندگی سایبری که توسط Nye (2017)، Lindsayو همکاران (۲۰۲۱) و Smeets (2022) توسعه یافته، نشان می‌دهد که راهبردهای سنتی بازدارندگی در فضای دیجیتال ناکافی هستند. بازدارندگی مؤثر در این فضا نه‌تنها نیازمند تهدید به مجازات بلکه مستلزم ترکیب دفاع چندلایه، تاب‌آوری زیرساختی، همکاری‌های اطلاعاتی و هماهنگی میان‌بخشی است. این موضوع در سیاست‌گذاری امنیت ملی اهمیت زیادی دارد و خلأ آن می‌تواند پیامدهای گسترده‌ای برای ثبات بین‌المللی به‌همراه داشته باشد .چهارم، بعد «روایت‌سازی» که در پژوهش‌های Greenberg (2020) و Shackelford (2014) مورد توجه قرار گرفته، در بسیاری از مطالعات دیگر مغفول مانده است. کنترل روایت‌ها، اقناع افکار عمومی و مشروعیت‌بخشی به پاسخ‌ها، به‌ویژه در شرایطی که خطوط نبرد سایبری از دید عموم پنهان هستند، به اندازه‌ی خودِ عملیات اهمیت دارد. کشورهایی که توانایی مدیریت روایت را دارند، معمولاً در جلب حمایت بین‌المللی و مشروعیت‌بخشی به اقداماتشان موفق‌ترند .در نهایت، بخش قابل توجهی از ادبیات به بازیگران بزرگ بین‌المللی (ایالات متحده، روسیه، چین و اتحادیه اروپا) اختصاص دارد و پژوهش‌های اندکی به بررسی رفتار دولت‌های منطقه‌ای، به‌ویژه در غرب آسیا، پرداخته‌اند (صفری و احمدی، ۱٤۰۱). همین خلأ پژوهشی یکی از مهم‌ترین انگیزه‌های تحقیق حاضر است که می‌کوشد با مطالعه تطبیقی بازیگران منطقه‌ای و تحلیل تلفیقی ابعاد حقوقی، امنیتی و روایتی، درک جامع‌تری از مسئولیت دولت‌ها در جنگ‌های سایبری ارائه کند.

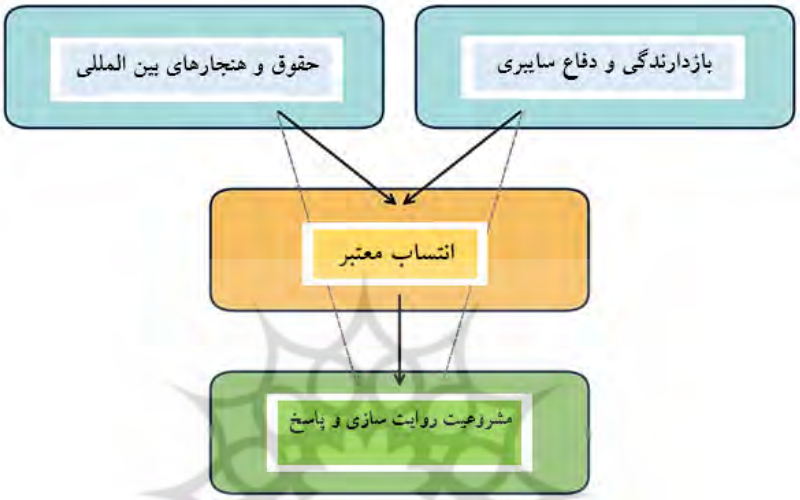
۵. چارچوب مفهومی پژوهش

برآیند مرور ادبیات و تحلیل یافته‌های پژوهش‌های پیشین نشان می‌دهد که مسئولیت‌پذیری دولت‌ها در جنگ‌های سایبری را نمی‌توان تنها از یک بُعد مورد بررسی قرار داد. پیچیدگی ذاتی این حوزه، ماهیت چندسطحی تهدیدات و تنوع ابزارهای مورد استفاده دولت‌ها ایجاب می‌کند که چارچوبی تلفیقی برای تحلیل شکل گیرد. در این پژوهش، چارچوب مفهومی پیشنهادی بر سه بُعد مکمل و در عین حال درهم‌تنیده استوار است:

- هنجارها و حقوق بین‌الملل :این بُعد پایه‌ی تحلیلی پژوهش را تشکیل می‌دهد. اصول سنتی چون حاکمیت، عدم مداخله، توسل به زور و مسئولیت بین‌المللی باید در بستر فضای سایبری بازتعریف شوند. فقدان تعریف واحد از «تهاجم سایبری» یا «دخالت» و نبود قواعد الزام‌آور سبب شده دولت‌ها بتوانند با بهره‌گیری از خلأهای حقوقی اقدامات خود را توجیه کنند. در نتیجه، تدوین هنجارهای روشن و به‌روزرسانی قواعد عرفی و قراردادی برای پاسخ‌گویی به واقعیت‌های سایبری امری ضروری است.
- بازدارندگی و دفاع چندلایه :بررسی تجربیات نشان می‌دهد که بازدارندگی سایبری صرفاً از مسیر تهدید به مجازات قابل تحقق نیست، بلکه باید با سازوکارهایی چون انکار دستاورد، دفاع فعال، تاب‌آوری زیرساختی و همکاری‌های بین‌المللی تکمیل شود. این لایه نقش واسط میان قواعد حقوقی و عمل‌گرایی امنیتی دارد و به دولت‌ها امکان می‌دهد علاوه بر کاهش آسیب‌پذیری، ظرفیت واکنش مؤثر و مشروع را افزایش دهند
- انتساب معتبر و روایت‌سازی :مسئولیت‌پذیری بدون شناسایی عامل حمله بی‌معناست. انتساب معتبر مستلزم تلفیق شواهد فنی، اطلاعاتی و دیپلماتیک و ارائه‌ی آن در قالب روایتی منسجم است. روایت‌سازی نه‌تنها ابزاری برای اقناع جامعه بین‌المللی است، بلکه در مشروعیت‌بخشی به پاسخ‌ها، جلوگیری از تشدید تنش‌ها و شکل‌دهی به هنجارهای آینده نقش حیاتی ایفا می‌کند. کنترل روایت و مدیریت افکار عمومی در این بُعد از اهمیت ویژه‌ای برخوردار است .این سه بُعد در تعامل با یکدیگر چارچوبی را می‌سازند که می‌تواند مبنای تحلیل مسئولیت دولت‌ها در جنگ‌های سایبری قرار گیرد. هنجارها و قواعد حقوقی زمینه‌ی هنجاری را فراهم می‌کنند، بازدارندگی و دفاع چندلایه ابزارهای عملیاتی برای پیشگیری و پاسخ‌گویی را ارائه می‌دهند، و انتساب معتبر همراه با روایت‌سازی تضمین می‌کند که اقدامات دولت‌ها از مشروعیت و پذیرش بین‌المللی برخوردار باشند.

در راستای تبیین چارچوب مفهومی پژوهش و برای شفاف‌سازی روابط میان سه مؤلفه‌ی اصلی تحلیل، شکل زیر طراحی شده است. این نمودار نشان می‌دهد که چگونه سه لایه‌ی «هنجارها و حقوق بین‌الملل»، «بازدارندگی و دفاع چندلایه» و «انتساب معتبر همراه با روایت‌سازی» در تعامل با یکدیگر، فرآیند ارزیابی مسئولیت بین‌المللی دولت‌ها در جنگ‌های سایبری را شکل می‌دهند. همچنین فلش‌های

بازگشتی بیانگر این نکته‌اند که نتایج حاصل از انتساب و روایت‌سازی می‌توانند بر شکل‌گیری هنجارهای جدید و بازتعریف قواعد حقوقی نیز اثرگذار باشند. این مدل به‌طور خلاصه مسیر منطقی پژوهش را از مبانی نظری تا پیامدهای سیاستی ترسیم می‌کند.



شکل ۱. چارچوب مفهومی پژوهش درباره مسئولیت بین‌المللی دولت‌ها در فضای سایبری

این چارچوب نشان می‌دهد که هنجارها و حقوق بین‌الملل در تعامل با بازدارندگی و دفاع سایبری، زمینه‌ساز انتساب معتبر هستند و در نهایت به ارزیابی مسئولیت بین‌المللی و تدوین پاسخ‌های سیاستی منجر می‌شوند.

۱-۵ پیوند چارچوب مفهومی با پژوهش حاضر

چارچوب مفهومی ارائه‌شده در این پژوهش نه‌تنها یک مدل تحلیلی برای بررسی رفتار دولت‌ها در فضای سایبری محسوب می‌شود، بلکه نقشه‌ای راهبردی برای فهم چگونگی شکل‌گیری مسئولیت بین‌المللی آن‌ها نیز فراهم می‌کند. سه بُعد «هنجارها و حقوق بین‌الملل»، «بازدارندگی و دفاع چندلایه» و «انتساب و روایت‌سازی» در تعامل با یکدیگر یک زنجیره‌ی تحلیلی را تشکیل می‌دهند که از مبانی نظری آغاز شده و به پیامدهای عملی و راهبردی ختم می‌شود. این چارچوب به ما اجازه می‌دهد تا رفتار دولت‌ها را نه‌فقط در سطح حقوقی یا امنیتی، بلکه در بستر سیاسی و ارتباطی گسترده‌تری نیز ارزیابی کنیم .بر این اساس، در بخش‌های بعدی مقاله تلاش خواهد شد تا با بهره‌گیری از این

چارچوب سه‌لایه، رفتار دولت‌ها در محیط سایبری مورد تحلیل تطبیقی قرار گیرد و نشان داده شود که چگونه شکاف‌های هنجاری، ضعف‌های ساختاری در بازدارندگی، و ناکامی در انتساب معتبر می‌توانند به تشدید تنش‌ها، گسترش دامنه‌ی درگیری‌ها و آسیب‌پذیری زیرساخت‌های حیاتی منجر شوند. این پیوند تحلیلی همچنین بستر مناسبی برای ارزیابی مسئولیت‌پذیری دولت‌های مختلف و ارائه‌ی پیشنهادهای سیاستی فراهم می‌سازد.

٦ .بحث و تحلیل یافته‌ها

تحلیل یافته‌های این پژوهش نشان می‌دهد که مسئولیت‌پذیری دولت‌ها در جنگ‌های سایبری صرفاً نتیجه‌ی پذیرش یا عدم‌پذیرش قواعد حقوق بین‌الملل نیست، بلکه محصولی چندبُعدی از تعامل میان هنجارها، راهبردهای امنیتی، ظرفیت‌های فنی، و توان روایت‌سازی سیاسی است. بررسی روندهای دهه‌ی اخیر در غرب آسیا نیز نشان می‌دهد که این ابعاد در عمل به‌شکل‌های متفاوتی در رفتار دولت‌ها نمود پیدا می‌کنند و بر ادراک جامعه‌ی بین‌المللی از مشروعیت اقدامات سایبری آن‌ها اثر می‌گذارند.

٦-١ .تنوع راهبردی در مواجهه با جنگ‌های سایبری

بررسی بازیگران فعال در غرب آسیا نشان می‌دهد که دولت‌ها برای پیشبرد اهداف خود در فضای سایبری از راهبردهای متفاوتی بهره می‌برند. برخی کشورها مانند ایالات متحده و بریتانیا، بر شفافیت نسبی و انتشار اسناد رسمی انتساب تأکید دارند و تلاش می‌کنند با همراه‌سازی متحدان، مشروعیت پاسخ خود را افزایش دهند .(White House, 2023: 14) در مقابل، برخی دولت‌ها راهبردی مبتنی بر ابهام راهبردی اتخاذ می‌کنند تا ضمن بهره‌برداری از مزایای عملیات سایبری، از پذیرش مسئولیت رسمی آن بگریزند. این رویکرد به‌ویژه در میان بازیگران منطقه‌ای همچون رژیم صهیونیستی مشاهده می‌شود که در بسیاری از موارد عملیات خود را نه انکار کرده و نه رسماً بر عهده گرفته است .(Greenberg, 2020: 124) در نقطه‌ی مقابل، کشورهایی مانند ایران که در معرض حملات مکرر قرار دارند، تمرکز خود را بر بازدارندگی تدافعی و تقویت تاب‌آوری زیرساخت‌ها قرار داده‌اند (صفری و احمدی، ١٤٠١: ٩٣). این راهبرد، هرچند از منظر حقوقی قابل دفاع‌تر است، اما به

دلیل محدودیت در ائتلاف‌سازی اطلاعاتی و ضعف در روایت‌سازی بین‌المللی، معمولاً در جلب حمایت جهانی کمتر موفق بوده است .(Rid & Buchanan, 2015: 10)

۲-٦. مسئولیت‌پذیری در میدان عمل

از قواعد تا کنش مقایسه رفتار بازیگران اصلی نشان می‌دهد که در عمل، مسئولیت‌پذیری سایبری تابعی از سه عامل کلیدی است :۱. انطباق با هنجارهای حقوق بین‌الملل: دولت‌هایی که عملیات سایبری خود را در چارچوب اصولی چون عدم مداخله و تناسب توجیه می‌کنند، از مشروعیت بین‌المللی بیشتری برخوردارند. با این حال، نبود تعریف دقیق از «حمله سایبری» و نبود اجماع درباره‌ی آستانه‌ی استفاده از زور، فضای تفسیر را برای دولت‌ها باز گذاشته است (Schmitt, 2017: 23).

۲. توانایی در انتساب معتبر: کشورهایی که می‌توانند شواهد فنی و اطلاعاتی را به‌طور قانع‌کننده‌ای ارائه دهند، از پشتیبانی دیپلماتیک بیشتری برخوردار می‌شوند. تجربه حملات علیه زیرساخت‌های اوکراین در سال‌های اخیر نشان داد که حتی در حضور شواهد فنی، اجماع سیاسی شرط ضروری برای انتساب معتبر است .(CISA/ICS-CERT, 2016: 2)

۳. روایت‌سازی و مشروعیت‌بخشی سیاسی: توانایی در شکل‌دهی به افکار عمومی جهانی، چه از طریق رسانه‌ها و چه از طریق بیانیه‌های رسمی، نقشی تعیین‌کننده در ارزیابی مشروعیت اقدامات دارد. رژیم صهیونیستی با بهره‌گیری از شبکه‌های رسانه‌ای بین‌المللی و حمایت متحدان غربی، اغلب در روایت‌سازی موفق‌تر بوده است .(Bronk & Tikk, 2013: 84)

۳-٦ .پیامدهای انسانی و ضرورت نظارت بین‌المللی

یکی از یافته‌های مهم این پژوهش آن است که تداوم منازعات سایبری بدون چارچوب نظارتی مؤثر، نه‌تنها امنیت دولتی بلکه امنیت انسانی را نیز تهدید می‌کند. نمونه‌هایی چون تلاش برای نفوذ به سامانه‌های آب شهری (ESET, 2022: 5) یا حمله به بندر شهید رجایی (قرباغی و کشاورز، ۱۳۹۹: ٤٥) نشان می‌دهد که مرز میان اهداف نظامی و غیرنظامی به‌طور فزاینده‌ای در حال محو شدن است. این روند با اصول بنیادین حقوق بین‌الملل بشردوستانه از جمله «تفکیک» و «تناسب» در تعارض است و ضرورت نقش‌آفرینی فعال‌تر نهادهای بین‌المللی را برجسته می‌کند .نکته‌ی قابل توجه این است که حتی در حضور قواعد حقوقی موجود، سازوکارهای اجرایی و نظارتی کافی برای تضمین

پاسخ‌گویی دولت‌ها وجود ندارد. شورای امنیت سازمان ملل تاکنون هیچ قطع‌نامه الزام‌آوری در زمینه‌ی عملیات سایبری تصویب نکرده و اغلب اقدامات به بیانیه‌های سیاسی غیرالزام‌آور محدود مانده‌اند (UNIDIR, 2024: 12). این ضعف نهادی باعث شده که دولت‌ها احساس کنند هزینه‌ی تخطی از هنجارها بسیار پایین است.

٦-٤ .مسیرهای پیش‌رو:

از بازدارندگی تا هنجارسازی برآیند تحلیل‌ها نشان می‌دهد که بدون ایجاد سازوکارهای مشترک انتساب و پاسخ‌گویی، رقابت سایبری به‌سوی بی‌ثباتی فزاینده پیش خواهد رفت. راهکارهای پیشنهادی شامل موارد زیر است :توسعه‌ی رژیم‌های بین‌المللی برای تعریف دقیق‌تر «تهاجم سایبری» و تعیین آستانه‌های حقوقی آن .تقویت همکاری‌های فنی و اطلاعاتی میان کشورها برای ارتقای توان انتساب و جلوگیری از انکارپذیری.

افزایش نقش سازمان‌های بین‌المللی در نظارت بر رعایت اصول بشردوستانه در فضای سایبری . طراحی سازوکارهایی برای پاسخ‌گویی سیاسی و حقوقی به دولت‌هایی که عملیات سایبری را علیه زیرساخت‌های غیرنظامی اجرا می‌کنند.

۷ .نتیجه‌گیری و دلالت‌های سیاستی تحلیل انجام‌شده

در این پژوهش نشان می‌دهد که مسئله‌ی «مسئولیت بین‌المللی دولت‌ها در جنگ‌های سایبری» در حال تبدیل شدن به یکی از اصلی‌ترین چالش‌های نظم جهانی معاصر است. جنگ سایبری دیگر نه پدیده‌ای حاشیه‌ای، بلکه ابزاری مرکزی در راهبردهای امنیت ملی، رقابت ژئوپلیتیکی و حتی سیاست خارجی کشورهاست. در چنین شرایطی، چارچوب‌های سنتی حقوق بین‌الملل که بر مبنای جنگ‌های متعارف و تهدیدات فیزیکی بنا شده‌اند ــ پاسخ‌گوی پیچیدگی‌های فضای دیجیتال نیستند و همین خلأ، فضای خاکستری بزرگی برای کنش دولت‌ها ایجاد کرده است.

۷-۱ .بازتعریف مسئولیت در عصر دیجیتال

یافته‌های پژوهش نشان می‌دهد که مسئولیت‌پذیری در فضای سایبری را نمی‌توان صرفاً به پایبندی به قواعد حقوقی تقلیل داد. بلکه باید آن را فرآیندی چندلایه دانست که از هنجارسازی، بازدارندگی، انتساب معتبر، و روایت‌سازی مشروع تشکیل شده است. دولت‌ها با ترکیب این عناصر

می‌توانند هم امنیت خود را تضمین کنند و هم مشروعیت اقدامات‌شان را در سطح بین‌المللی افزایش دهند. برعکس، فقدان یکی از این عناصر می‌تواند حتی عملیات دفاعی را از دید جامعه جهانی غیرقانونی یا نامشروع جلوه دهد.

۷-۲ .پیامدهای انسانی و ضرورت پاسخ‌گویی

مهم‌ترین یافته‌ی این پژوهش آن است که نبود سازوکارهای پاسخ‌گویی مؤثر، نه‌تنها امنیت ملی بلکه امنیت انسانی را نیز تهدید می‌کند. درگیری‌های اخیر، از جمله جنگ دوازده‌روزه ایران و رژیم صهیونیستی در سال ۲۰۲۵ و حملات مکرر علیه زیرساخت‌های حیاتی اوکراین و سایر کشورها، نشان داده‌اند که فضای سایبری به بستری برای هدف‌گیری غیرنظامیان و ایجاد فشار روانی بر جوامع تبدیل شده است. این روند نه‌تنها با اصول بنیادین حقوق بشردوستانه در تضاد است، بلکه خطر «نظامی‌سازی کامل فضای مجازی» را افزایش می‌دهد.

۷-۳ .دلالت‌های سیاستی برای دولت‌ها و نهادهای بین‌المللی

با توجه به یافته‌های این پژوهش، چند دلالت کلیدی برای سیاست‌گذاران قابل طرح است .1 : تعریف دقیق‌تر تهاجم سایبری و استانداردهای انتساب: جامعه بین‌المللی باید در قالب معاهدات یا توافق‌نامه‌های چندجانبه، تعاریف روشن‌تری از «تهاجم سایبری» و آستانه‌های حقوقی آن ارائه کند تا فضای تفسیری برای سوءاستفاده کاهش یابد .2 .ایجاد رژیم‌های چندجانبه پاسخ‌گویی: نهادهایی همچون شورای امنیت یا مجمع عمومی سازمان ملل می‌توانند سازوکارهایی برای بررسی و قضاوت درباره‌ی حملات سایبری ایجاد کنند و ضمانت‌های اجرایی مشخصی برای تخلفات در نظر بگیرند . .3توسعه‌ی همکاری‌های اطلاعاتی و فنی: همکاری میان دولت‌ها و شرکت‌های فناوری برای شناسایی و انتساب حملات سایبری می‌تواند نقش مهمی در کاهش انکارپذیری و افزایش مسئولیت‌پذیری ایفا کند .4 .تقویت سازوکارهای حمایت از غیرنظامیان: نهادهای بین‌المللی باید معیارهای مشخصی برای حمایت از زیرساخت‌های حیاتی غیرنظامی و پاسخ به تخلفات مربوط به آن تدوین کنند .5 .سرمایه‌گذاری در روایت‌سازی و دیپلماسی سایبری: کشورهای در حال توسعه به‌ویژه باید ظرفیت‌های خود را در حوزه روایت‌سازی تقویت کنند تا بتوانند در عرصه افکار عمومی جهانی از مشروعیت اقدامات دفاعی خود دفاع کنند.

جمع‌بندی نهایی

پژوهش حاضر نشان داد که جنگ‌های سایبری عرصه‌ای مبهم و چندوجهی هستند که در آن مرز میان صلح و درگیری، دفاع و تهاجم، و حتی نظامی و غیرنظامی به‌سادگی قابل تشخیص نیست. در چنین محیطی، مسئولیت‌پذیری دولت‌ها نه‌تنها یک تعهد حقوقی بلکه یک ضرورت راهبردی است که بر مشروعیت سیاسی، امنیت ملی و ثبات نظم بین‌الملل تأثیر مستقیم دارد. بدون چارچوب‌های شفاف، همکاری‌های چندجانبه و سازوکارهای معتبر انتساب، فضای سایبری به بستری برای بی‌قانونی، بی‌پاسخ‌گویی و تشدید بحران‌های جهانی تبدیل خواهد شد.

فهرست منابع

ر ضایی، علی(۱٤۰۲). تحلیل تطبیقی دکترین بازدارندگی سایبری در ایران و رژیم صهیونیستی، امنیت ملی، ۳٤(۱)، ۲۵–٥٤.

شهبازی، سید محمد؛ آقاجانی رونقی، امیر(۱٤۰۰). مسئولیت دولت‌ها در قبال عملیات سایبری فراملی: از حقوق عرفی تا رویه بین‌المللی، مطالعات حقوقی بین‌المللی، ٥۱(۲)، ٤٥–۷۳.

صفری، احمد؛ احمدی، نسرین(۱٤۰۱). سیاست دفاع سایبری جمهوری اسلامی ایران: چالش‌ها و چشم‌اندازها»، مطالعات راهبردی، ۲۹(۳)، ۱۱۲–۱۳٥.

قره‌باغی، مهدی؛ کشاورز، سارا(۱۳۹۹). حملات سایبری و مسئولیت بین‌المللی دولت‌ها: مطالعه موردی ایران، سیاست جهانی، ۲٦(٤)، ۸۸–۱۱۰.

مو سوی، ر ضا(۱۳۹٦). حقوق بین‌الملل و چالش‌های جنگ سایبری، تهران: انتشارات دانشگاه علامه طباطبایی.

Bronk, C., & Tikk, E. (۲۰۱۳). The Cyber Attack on Saudi Aramco. Survival, ٥٥(۲), ۸۱–۹۶.

CISA / ICS-CERT. (۲۰۱۶). IR-ALERT-H-۱۶-۰٥۶-۰۱: Cyber-Attack Against Ukrainian Critical Infrastructure. U.S. Department of Homeland Security.

Delerue, F. (۲۰۲۰). Cyber Operations and International Law. Cambridge University Press.

ENISA. (۲۰۲۳). ENISA Threat Landscape ۲۰۲۳. European Union Agency for Cybersecurity.

ESET Research. (۲۰۲۲). INDUSTROYER۲: New Sandworm Malware Targeting Ukraine's Energy Sector. ESET White Paper.

Greenberg, A. (۲۰۲۰). Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (۲۰۱۲). The Law of Cyber-Attack. California Law Review, ۱۰۰(۴), ۸۱۷–۸۸٥.

Healey, J. (Ed.). (۲۰۱۳). A Fierce Domain: Conflict in Cyberspace, ۱۹۸۶–۲۰۱۲. Washington, DC: Atlantic Council.

Klimburg, A. (۲۰۱۷). The Darkening Web: The War for Cyberspace. New York: Penguin Press.

Lindsay, J. R., Smeets, M., & Vu, A. (۲۰۲۱). Routledge Handbook of Cybersecurity. London: Routledge.

Maurer, T. (۲۰۱۸). Cyber Mercenaries: The State, Hackers, and Power. Cambridge: Cambridge University Press.

Nye, J. S. (۲۰۱۷). Deterrence and Dissuasion in Cyberspace. International Security, ۴۱(۳), ۴۴–۷۱.
Rid, T., & Buchanan, B. (۲۰۱۵). Attributing Cyber Attacks. Journal of Strategic Studies, ۳۸(۱–۲), ۴–۳۷.
Roscini, M. (۲۰۲۰). Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press.
Schmitt, M. N. (Ed.). (۲۰۱۷). Tallinn Manual ۲ on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.
Shackelford, S. J. (۲۰۱۴). Managing Cyber Attacks in International Law, Business, and Relations: In Search of a Common Language. Cambridge: Cambridge University Press.
The White House. (۲۰۲۳). National Cybersecurity Strategy. Washington, DC.
Tsagourias, N., & Buchan, R. (Eds.). (۲۰۲۱). Research Handbook on International Law and Cyberspace (۲nd ed.). Cheltenham: Edward Elgar.
UN GGE. (۲۰۲۱). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/۱۳۵/۷۶). United Nations.
UN OEWG. (۲۰۲۱). Final Report of the Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (A/۸۱۶/۷۵). United Nations.
UNIDIR. (۲۰۲۴). Norms, Rules, and Principles for Responsible State Behaviour in Cyberspace. Geneva: United Nations Institute for Disarmament Research.
Zetter, K. (۲۰۱۴). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown.