Strategic Studies of International Politics
https://jpir.journals.umz.ac.ir/ E-ISSN: 2717-0551
Vol. 9, No. 2, Issue. 18, Summer 2026 *** Received: 2026/03/24 Accepted: 2026/05/30
Research paper

The Prosecuting War Crimes in Cyberspace; A Comparative Study between International Humanitarian Law and the Cyber Laws of the United States and Russia

Morteza Bandari
PhD in International Relations, Islamic Azad University, Ahvaz branch, Ahvaz, Iran. (corresponding author).
Email: Dr.Mortezabandari@gmail.com 0009-0002-0354-1892
Su Qingwei
Ph.D. in International Law and Global study, Shanghai University, Shanghai, China.
Email: Qwsu@t.shu.edu.cn 0009-0004-0434-4414
Eisa Soleymani
Ph.D. in International Law and Global study, Shanghai University, Shanghai, China.
Email: Eisa_soleimany@yahoo.com 0009-0005-6925-9453
Abdolreza Alishahi
PhD in Political Science, Allameh Tabataba'i University, Tehran, Iran.
Email: Abdolrea_Alishahi@atu.ac.ir 0000-0002-4122-3118

Abstract
The expansion of modern technologies and governments' growing dependence on cyberspace have made the use of cyber tools in armed conflicts a fundamental issue in international law. Although cyber operations may produce destructive effects comparable to conventional attacks, their legal status under international humanitarian law remains ambiguous. This study examines the applicability of international humanitarian law to cyber operations and compares the legal positions of the United States and Russia. It addresses whether international humanitarian law possesses sufficient capacity to identify and prosecute war crimes committed in cyberspace. Using a descriptive-analytical method, a comparative approach, and the theory of Neo-Realism, the study argues that great-power rivalry in cyberspace obstructs the institutionalization of binding international norms. The findings indicate that existing humanitarian law can potentially encompass cyber operations; however, the absence of consensus on the definition of a cyber armed attack, inadequate attribution mechanisms, and conflicting interests among major powers hinder the establishment of international criminal responsibility. While the United States generally supports an expansive interpretation, Russia adopts a more restrictive, sovereignty-based position. Consequently, dedicated international mechanisms and stronger interstate cooperation are essential for clarifying cyber warfare norms and ensuring effective legal criminal accountability.

Keywords: Cyber Warfare, International Criminal Responsibility, Digital International Humanitarian Law, Neorealism and Great-Power Competition.

Extended Abstract

Introduction: The rapid expansion of cyberspace as an arena of state competition and military operations has transformed the legal environment of armed conflict. Cyber operations may disrupt critical infrastructure, disable military systems, compromise command networks, interfere with civilian services, or cause physical and functional damage comparable to conventional attacks. Yet the application of international humanitarian law (IHL) remains contested because existing rules were developed primarily around territorially identifiable and physically observable forms of warfare. This uncertainty becomes particularly significant when cyber operations occur during armed conflicts and potentially satisfy the material elements of war crimes. The central problem is therefore whether existing IHL and international criminal law can adequately classify, attribute, and prosecute unlawful cyber conduct. Divergent approaches among major cyber powers, especially the United States and Russia, further complicate the emergence of common standards and effective accountability mechanisms.

Research Question: Does international humanitarian law possess sufficient legal capacity to identify and prosecute war crimes committed through cyber operations during armed conflicts, and how do the legal approaches of the United States and Russia affect the prospects for international criminal responsibility?

Research Hypothesis: The study hypothesizes that IHL contains sufficiently broad principles to regulate a substantial category of cyber operations conducted during armed conflicts, including distinction, proportionality, precautions in attack, protection of civilians and civilian objects, and restrictions on methods and means of warfare. However, effective criminal responsibility remains constrained by the absence of a universally accepted definition of a cyber armed attack, difficulties in attribution, uncertainty regarding the application of existing war-crimes provisions to cyber conduct, and disagreement among major powers concerning sovereignty and international regulation. Accordingly, legal applicability is more developed than the institutional and political conditions required for effective prosecution.

Methodology and Theoretical Framework: The research employs a descriptive-analytical methodology and comparative legal approach. It examines relevant principles of IHL and international criminal law and evaluates their application to cyber operations conducted in armed conflicts. Particular attention is given to distinction, proportionality, civilian protection, indiscriminate attacks, precautions, and individual criminal responsibility. The study then compares the approaches of the United States and Russia regarding cyber operations, sovereignty, attribution, and international rule-making. The theoretical framework is grounded in neorealism, emphasizing power distribution, strategic competition, and the constraints that great-power interests impose on international institutions. From this perspective, disagreements over cyber norms are understood not only as legal or technical disputes, but also as expressions of competing security interests and contrasting conceptions of sovereignty and strategic autonomy.

Research Findings: The analysis produces several interconnected findings. First, IHL is not inherently incapable of regulating cyber operations. Its established principles can, in appropriate circumstances, apply according to the effects, targets, and context of cyber conduct. Operations intentionally directed against civilians or civilian objects, or conducted indiscriminately or without required precautions, may fall within existing humanitarian prohibitions when the necessary armed-conflict nexus and other legal conditions are satisfied. The principal challenge is therefore not the complete absence of law, but translating established rules into technologically

specific situations and determining when cyber conduct reaches the legal threshold of an attack.
Second, the concept of a cyber armed attack remains insufficiently settled. Disagreement over whether physical destruction, loss of functionality, serious economic consequences, or other forms of harm are required creates uncertainty concerning when attack-related IHL rules apply. This ambiguity is especially consequential for criminal prosecution because war-crimes liability requires sufficiently precise identification of prohibited conduct and its legal elements.
Third, attribution represents a major evidentiary obstacle. Concealed origins, proxies, third-country infrastructure, manipulated digital traces, and false-flag techniques can complicate the establishment of a reliable connection between an operation and its responsible actor. Although technical attribution and legal attribution are distinct, weaknesses in technical attribution may substantially affect the evidentiary basis of legal responsibility.
Fourth, the comparison between the United States and Russia reveals divergent legal orientations. The United States generally favors an expansive interpretation under which existing international law can govern cyber operations, while retaining significant concern for operational flexibility and national security. Russia places greater emphasis on sovereignty, non-interference, state control over the information environment, and international rules reinforcing state authority. These positions are not entirely uniform, but they reflect different priorities concerning the relationship between international regulation, sovereignty, and strategic freedom.
Fifth, great-power competition restricts rapid institutionalization of detailed and binding cyber-warfare norms. States may endorse general legal principles while resisting definitions or accountability mechanisms that could constrain strategic capabilities or expose them to politically consequential responsibility. From a neorealist perspective, this helps explain why normative development has progressed further at the level of general principles than at the level of precise definitions, attribution procedures, enforcement, and criminal accountability.
Conclusion: The study concludes that IHL possesses meaningful normative capacity to regulate cyber operations during armed conflicts and, under appropriate conditions, to encompass conduct potentially constituting war crimes. Nevertheless, applicable principles do not automatically ensure effective prosecution. The principal obstacles are unresolved legal classification, uncertainty over thresholds of harm, attribution and evidentiary difficulties, and strategic disagreement among major powers over sovereignty and binding cyber norms. The United States-Russia comparison indicates that divergent legal interpretations are embedded in broader geopolitical interests, supporting the neorealist proposition that institutional development is conditioned by power distribution. Effective accountability therefore requires normative clarification of cyber operations in armed conflict, credible procedures for technical and legal attribution, clearer elements of cyber-related war crimes, stronger mechanisms for preserving digital evidence, and sustained inter-state cooperation. Rather than replacing existing IHL, these measures can strengthen its capacity to address cyber warfare and reduce the legal uncertainty that currently limits criminal responsibility.
Keywords: Cyber Warfare, International Criminal Responsibility, Digital International Humanitarian Law, Neorealism, Great-Power Competition.

E-ISSN: 2717-0551 / University of Mazandaran / Quarterly of Strategic Studies of International Politics

10.22080/jpir.2025.30542.1496

فصلنامه علمی مطالعات راهبردی سیاست بین الملل
سال نهم، شماره دوم (پیاپی ۱۸)، تابستان ۱۴۰۵، صص. ۷-۳۴
تاریخ دریافت: ۱۴۰۵/۰۱/۰۴ ـ تاریخ پذیرش: ۱۴۰۵/۰۳/۰۹

مقاله پژوهشی

تعقیب جنایات جنگی در فضای سایبری؛ مطالعه تطبیقی میان حقوق بین‌الملل بشردوستانه و حقوق سایبری ایالات متحده و روسیه

مرتضی بندری
دکترای روابط بین‌الملل، دانشگاه آزاد اسلامی، واحد اهواز، اهواز، ایران (نویسندهٔ مسئول).
Email: Dr.Mortezabandari@gmail.com 0009-0002-0354-1892
سو کینگ‌وی
دکترای حقوق بین‌الملل و مطالعات جهانی، دانشگاه شانگهای، شانگهای، چین.
Email: Qwsu@t.shu.edu.cn 0009-0004-0434-4414
عیسی سلیمانی
دانشجوی دکتری، گروه حقوق بین‌الملل و مطالعات جهانی، دانشگاه شانگهای، شانگهای، چین.
Email: Eisa_soleimany@yahoo.com 0009-0005-6925-9453
عبدالرضا عالیشاهی
دکتری علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران.
Email: Abdolrea_Alishahi@atu.ac.ir 0000-0002-4122-3118

چکیده
گسترش فناوری‌های نوین و وابستگی روزافزون دولت‌ها به فضای مجازی، بهره‌گیری از ابزارهای سایبری در درگیری‌های مسلحانه را به مسئله‌ای اساسی در حقوق بین‌الملل تبدیل کرده است. عملیات‌های سایبری می‌توانند آثاری ویرانگر مشابه حملات متعارف داشته باشند، اما جایگاه آن‌ها در چارچوب حقوق بین‌الملل بشردوستانه همچنان مبهم است. این پژوهش با هدف تحلیل قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه بر عملیات‌های سایبری و مقایسه دیدگاه‌های حقوقی ایالات متحده و روسیه، بررسی می‌کند که آیا این حقوق ظرفیت لازم برای شناسایی و تعقیب جنایات جنگی در فضای سایبری را دارد. پژوهش با روش توصیفی ـ تحلیلی، رویکرد تطبیقی و با بهره‌گیری از نظریه رئالیسم نو انجام شده است. یافته‌ها نشان می‌دهد که قواعد موجود حقوق بشردوستانه قابلیت تفسیر برای پوشش عملیات‌های سایبری را دارند؛ بااین‌حال، نبود اجماع درباره تعریف «حمله مسلحانه سایبری»، فقدان سازوکارهای دقیق انتساب و تعارض منافع قدرت‌های بزرگ، مانع تحقق مسئولیت کیفری بین‌المللی می‌شود. در این میان، ایالات متحده از تفسیر توسعه‌گرایانه و روسیه از رویکردی محدود و مبتنی بر حاکمیت ملی حمایت می‌کند. بنابراین، ایجاد سازوکارهای بین‌المللی ویژه برای شفاف‌سازی قواعد رفتاری جنگ سایبری و تقویت همکاری دولت‌ها، برای تحقق عدالت کیفری در این حوزه ضروری است.

کلیدواژه‌ها: جنگ سایبری، مسئولیت کیفری بین‌المللی، حقوق بین‌الملل بشردوستانه دیجیتال، رئالیسم نو، رقابت قدرت‌ها.

شاپای الکترونیک: ۰۵۵۱-۲۷۱۷/ دانشگاه مازندران/ فصلنامه علمی مطالعات راهبردی سیاست بین الملل

doi 10.22080/jpir.2025.30542.1496

۱. مقدمه

در دهه‌های اخیر، گسترش فناوری‌های نوین ارتباطی و توسعه زیرساخت‌های دیجیتال، برداشت سنتی از قدرت و امنیت در نظام بین‌الملل را دگرگون ساخته است. فضای سایبری نه‌تنها به بستری برای تبادل داده‌ها، فعالیت‌های اقتصادی و مدیریت خدمات حیاتی بدل شده، بلکه به عرصه‌ای رقابتی میان دولت‌ها در حوزه‌های نظامی، اطلاعاتی و امنیتی نیز تبدیل شده است. در این میان، افزایش شمار حملات سایبری علیه زیرساخت‌های حیاتی کشورها ــ مانند شبکه‌های انرژی، سیستم‌های مالی و خدمات عمومی ــ نگرانی‌های قابل‌توجهی در خصوص پیامدهای انسانی و امنیتی این اقدامات ایجاد کرده است. همین واقعیت سبب طرح این پرسش اساسی می‌شود که آیا در صورت وقوع این حملات در بستر مخاصمات مسلحانه، می‌توان آن‌ها را مشمول قواعد حقوق بین‌الملل بشردوستانه و به‌ویژه مقررات مربوط به جنایات جنگی دانست یا خیر.

بر این اساس، مسئله اصلی پژوهش حاضر از این واقعیت سرچشمه می‌گیرد که فضای سایبری مرزهای فیزیکی و مفهومی جنگ سنتی را درهم شکسته است. عملیات‌های سایبری در برخی موارد می‌توانند پیامدهایی مشابه حملات متعارف ایجاد کنند؛ پیامدهایی که از تخریب و ازکارافتادن زیرساخت‌ها تا ایجاد اختلال گسترده در خدمات حیاتی و حتی صدمه به افراد غیرنظامی را شامل می‌شود. با این حال، انطباق این عملیات‌ها با اصول بنیادین حقوق بین‌الملل بشردوستانه ــ از جمله تمایز میان اهداف نظامی و غیرنظامی، رعایت تناسب و ضرورت نظامی ــ همچنان محل بحث است. علاوه بر این، فقدان اجماع بین‌المللی در تعریف «حمله مسلحانه سایبری» و دشواری‌های مرتبط با شناسایی، انتساب و اثبات عاملان چنین حملاتی، پیچیدگی‌های حقوقی و عملی فراوانی را در مسیر اعمال مسئولیت کیفری بین‌المللی ایجاد کرده است. بنابراین پرسش محوری پژوهش حاضر آن است که آیا حقوق بین‌الملل بشردوستانه ظرفیت لازم برای شناسایی، طبقه‌بندی و تعقیب جنایات جنگی ارتکابی در فضای سایبری را داراست.

اهمیت پژوهش حاضر از چند منظر قابل توضیح است. نخست آن‌که در شرایطی که تهدیدات سایبری نقش فزاینده‌ای در ناامنی بین‌المللی ایفا می‌کنند، تبیین جایگاه عملیات‌های سایبری در چارچوب حقوقی موجود برای پیشگیری از منازعات نوین ضروری است. دوم آن‌که خلأ مفهومی و هنجاری در حوزه جنایات جنگی سایبری، خطر تضعیف اصول بنیادین حقوق بشردوستانه و نادیده‌گرفته‌شدن موازین اخلاقی

جنگ را افزایش می‌دهد. سوم آن‌که اختلاف دیدگاه‌های قدرت‌های بزرگ بر سر معیارهای حقوقی ناظر بر رفتار سایبری دولت‌ها، احتمال بهره‌برداری ابزاری از فضای مجازی در مخاصمات را بیشتر می‌کند. در این میان، بررسی تطبیقی مواضع ایالات متحده و روسیه به‌عنوان دو قدرت سایبری برجسته با رویکردهای متفاوت نسبت به حاکمیت سایبری و تفسیر قواعد بین‌المللی می‌تواند تصویری روشن‌تر از چالش‌ها و ظرفیت‌های موجود ارائه دهد و زمینه را برای شکل‌گیری قواعد مشترک فراهم سازد.

بر این اساس، پژوهش حاضر به دنبال تحلیل واقع‌بینانه و مستدل امکان شناسایی و تعقیب جنایات جنگی در فضای سایبری در پرتو حقوق بین‌الملل بشردوستانه و با تکیه بر بررسی تطبیقی دیدگاه‌های ایالات متحده و روسیه است. سؤال اصلی پژوهش چنین مطرح می‌شود: «آیا حقوق بین‌الملل بشردوستانه ظرفیت لازم برای شناسایی و تعقیب جنایات جنگی ارتکاب‌یافته در فضای سایبری را دارد؟» به‌موازات آن، پرسش‌های فرعی شامل میزان قابلیت انطباق اصول بنیادین حقوق بشردوستانه با عملیات‌های سایبری، تفاوت رویکرد دو کشور مذکور نسبت به مفهوم و مصادیق جنایات جنگی سایبری، و مهم‌ترین چالش‌های انتساب و پیگیری بین‌المللی این جرایم است. روش تحقیق نیز توصیفی ـ تحلیلی و مبتنی بر مقایسه منابع و اسناد بین‌المللی و رویه دولت‌هاست.

۲. مبانی نظری؛ نورئالیسم

تحولات نظام بین‌الملل در قرن بیست‌ویکم نشان می‌دهد که فناوری اطلاعات و فضای سایبری به یکی از مهم‌ترین میدان‌های رقابت قدرت‌های بزرگ تبدیل شده است. در این بستر جدید، مفاهیمی چون «قدرت»، «امنیت»، «تهاجم» و حتی «جنگ» بازتعریف می‌شوند و حقوق بین‌الملل، به‌ویژه حقوق بین‌الملل بشردوستانه، با چالشی مفهومی و کاربردی مواجه می‌گردد. برای تحلیل این پدیده پیچیده، تکیه بر نظریه‌های روابط بین‌الملل ضرورتی اجتناب‌ناپذیر است، زیرا درک رفتار دولت‌ها در حوزه سایبری تنها از طریق مباحث حقوقی ممکن نیست و نیازمند تبیین‌های نظری از منطق قدرت، منافع و رقابت است.

پژوهش حاضر بر پایه نظریه رئالیسم نو[1]در روابط بین‌الملل شکل گرفته است. رئالیسم نو، که توسط «کنت والتز[2]» بنیان‌گذاری شد، نظام بین‌الملل را عرصه‌ای آنارشیک می‌داند که در آن دولت‌ها برای بقا و حفظ امنیت خود ناگزیر از رقابت قدرت

1. Neorealism
2. Kenneth Neal Waltz

هستند. در این چارچوب، قواعد و نهادهای بین‌المللی تنها تا جایی اعتبار دارند که با منافع قدرت‌های بزرگ هم‌راستا باشند. به بیان دیگر، ساختار نظام بین‌الملل، نه ارزش‌ها یا نهادها، تعیین‌کننده رفتار دولت‌هاست (Clarkson, 2025: 637-638).

با استفاده از این چارچوب، می‌توان رفتار ایالات متحده و روسیه در عرصه جنگ‌های سایبری را تحلیل کرد. ایالات متحده، به‌عنوان قدرت مسلط نظام بین‌الملل، تمایل دارد قواعد بین‌المللی را به نحوی تفسیر کند که آزادی عمل بیشتری در به‌کارگیری ابزارهای سایبری برای دفاع یا حمله داشته باشد. در مقابل، روسیه که خود را در برابر نفوذ و برتری غرب آسیب‌پذیر می‌بیند، رویکردی محافظه‌کارانه‌تر اتخاذ کرده و بر حاکمیت ملی، کنترل اطلاعات و محدودسازی تفسیر توسعه‌گرایانه حقوق بین‌الملل تأکید دارد. این دو رویکرد متضاد، ناشی از تفاوت در برداشت از تهدید، منافع و قدرت است و در نتیجه، مانعی ساختاری در مسیر شکل‌گیری اجماع جهانی بر سر قواعد الزام‌آور در حوزه جنگ سایبری ایجاد می‌کند.

از منظر رئالیسم نو، نظام بین‌الملل فاقد اقتدار مرکزی برای الزام دولت‌ها به تبعیت از قواعد است (Tabak, 2025: 26). بنابراین، حتی اگر قواعد حقوق بین‌الملل بشردوستانه قابلیت تفسیر و اعمال در فضای سایبری را داشته باشند، اجرای آن‌ها منوط به اراده دولت‌هاست؛ اراده‌ای که غالباً تابع ملاحظات قدرت و منافع ملی است. به‌عنوان مثال، ایالات متحده در برخی موارد به تفسیر موسع از مفهوم «حمله مسلحانه» تمایل دارد تا عملیات‌های سایبری تهاجمی خود را مشروع جلوه دهد، در حالی‌که روسیه با تأکید بر اصل حاکمیت، هرگونه مداخله سایبری خارجی را نقض حقوق بین‌الملل می‌داند. این اختلافات نشان می‌دهد که ساختار رقابت‌آمیز نظام بین‌الملل مانع نهادینه شدن پاسخگویی کیفری بین‌المللی در حوزه سایبری می‌شود.

نکته مهم دیگر در چهارچوب نظری، پیوند میان رئالیسم نو و کارکرد حقوق بین‌الملل بشردوستانه است. از دیدگاه رئالیست‌های ساختاری، حقوق بین‌الملل بشردوستانه، هرچند واجد ارزش اخلاقی و انسانی است، اما در عمل بازتابی از توازن قدرت میان دولت‌ها محسوب می‌شود (Polinder, 2025: 53-54). در حوزه جنگ سایبری نیز این واقعیت مشهود است. دولت‌های قدرتمند در تعیین معیارهای رفتاری و قواعد الزام‌آور نقش اصلی را دارند و کشورهای ضعیف‌تر بیشتر تابع این قواعد هستند تا تدوین‌کننده آن‌ها. در نتیجه، شکاف میان ظرفیت نظری حقوق بین‌الملل برای پوشش عملیات‌های سایبری و واقعیت اجرای آن، ریشه در منطق ساختاری نظام بین‌الملل دارد.

افزون بر این، نظریه رئالیسم نو، امکان تحلیل موانع همکاری بین‌المللی در مقابله با جنایات سایبری را نیز فراهم می‌سازد. طبق این نظریه، هر دولت از بیم سوءاستفاده احتمالی رقبا از داده‌ها و فناوری‌هایش، از شفاف‌سازی کامل یا اشتراک اطلاعات در زمینه حملات سایبری خودداری می‌کند. به همین دلیل، نهادهای بین‌المللی مانند دیوان کیفری بین‌المللی یا گروه کارشناسان دولتی سازمان ملل، اگرچه تلاش‌هایی برای تنظیم قواعد رفتار دولت‌ها در فضای مجازی انجام داده‌اند، اما فاقد ابزار الزام‌آور هستند. در واقع، رقابت ساختاری میان قدرت‌ها موجب می‌شود که قواعد حقوقی در این حوزه بیشتر جنبه توصیه‌ای داشته باشند تا الزام‌آور (Williams, 2025: 71-72).

از منظر نظری، پژوهش حاضر تلاش می‌کند تا نشان دهد که نبود اجماع جهانی در تعریف و تعقیب جنایات جنگی سایبری نه صرفاً یک خلأ حقوقی، بلکه یک پیامد ساختاری نظام بین‌الملل قدرت‌محور است. بنابراین، تحلیل حقوقی بدون درک زمینه سیاسی و ساختاری روابط بین‌الملل ناقص خواهد بود. به همین دلیل، تلفیق تحلیل حقوقی (در سطح قواعد و نهادها) با تحلیل سیاسی (در سطح منافع و قدرت) رویکرد اصلی این پژوهش را شکل می‌دهد.

در مجموع، مبنای نظری پژوهش حاضر بر این فرض استوار است که قواعد حقوق بین‌الملل بشردوستانه از نظر مفهومی قابلیت انطباق با فضای سایبری را دارند، اما در عمل، تحقق پاسخگویی کیفری برای جنایات جنگی سایبری، به دلیل منطق رقابت‌آمیز نظام بین‌الملل و نبود اجماع میان قدرت‌های بزرگ، با موانع جدی مواجه است. تنها در صورتی که ساختار همکاری‌های بین‌المللی در حوزه امنیت سایبری تقویت و توازن منافع میان بازیگران اصلی برقرار شود، می‌توان به اجرای مؤثر این قواعد امیدوار بود.

جدول ۱. چارچوب مفهومی پژوهش (طراحی: نویسندگان)

متغیر	تعریف مفهومی	تعریف عملیاتی	پیوند با نظریه
جنایات جنگی سایبری	هرگونه اقدام سایبری که در جریان مخاصمات مسلحانه منجر به نقض اصول حقوق بین‌الملل بشردوستانه (تمایز، تناسب، ضرورت نظامی) شود.	نمونه‌هایی مانند حمله به زیرساخت‌های غیرنظامی، از کار انداختن شبکه‌های پزشکی یا برق در زمان جنگ.	بازتاب ابزار جدید قدرت در نظام آنارشیک بین‌الملل.
حقوق بین‌الملل بشردوستانه	مجموعه قواعد ناظر بر محدود کردن خشونت در	اسناد ژنو ۱۹۴۹، پروتکل‌های الحاقی و تفسیرهای معاصر در	زمینه حقوقی محدودکننده رفتار

	مخاصمات مسلحانه و حمایت از غیرنظامیان.	Tallinn Manual 2.0.	دولت‌ها در جنگ‌های سایبری.
نظریه رئالیسم نو	دیدگاهی که ساختار قدرت و آنارشی بین‌المللی را عامل تعیین‌کننده رفتار دولت‌ها می‌داند.	تحلیل رقابت ایالات متحده و روسیه در حوزه سایبری.	چارچوب تبیینی اصلی پژوهش برای فهم مقاومت در برابر قواعد الزام‌آور.
مسئولیت کیفری بین‌المللی	پاسخگویی افراد یا دولت‌ها در قبال ارتکاب جنایات بین‌المللی.	بررسی امکان اعمال صلاحیت دیوان کیفری بین‌المللی بر جنایات سایبری.	متغیر وابسته که تحقق آن تحت تأثیر ساختار قدرت قرار دارد.
امنیت سایبری بین‌المللی	وضعیتی که در آن دولت‌ها از حملات سایبری مخرب مصون باشند و قواعد رفتاری مشترک داشته باشند.	همکاری در قالب سازمان ملل، گروه‌های کارشناسی و معاهدات.	نتیجه مطلوب، اما محدود به میزان همکاری قدرت‌های بزرگ.

۳. روش‌شناسی تحقیق

روش تحقیق در پژوهش حاضر از نوع توصیفی ـ تحلیلی و با رویکرد تطبیقی است. داده‌های پژوهش از طریق منابع کتابخانه‌ای، اسناد بین‌المللی، کنوانسیون‌ها، گزارش‌های رسمی و رویه دولت‌ها گردآوری شده‌اند. در تحلیل داده‌ها، ابتدا مبانی نظری و اصول حقوق بین‌الملل بشردوستانه در ارتباط با فضای سایبری بررسی می‌شود، سپس با مقایسه دیدگاه‌های ایالات متحده و روسیه، نقاط اشتراک و افتراق آن‌ها تحلیل و در نهایت ظرفیت‌های حقوقی موجود برای تعقیب جنایات جنگی سایبری ارزیابی خواهد شد.

۴. یافته ها و تجزیه‌وتحلیل داده‌ها

۴-۱. امکان شناسایی و تعقیب جنایات جنگی در فضای سایبری با تأکید بر ایالات متحده

ایالات متحده آمریکا به‌عنوان یکی از بازیگران اصلی عرصه سایبری و یکی از قدرت‌های مسلط نظام بین‌الملل، نقش مهمی در شکل‌دهی به قواعد، رویه‌ها و تفسیرهای حقوقی مربوط به جنگ‌های سایبری دارد. تحلیل رویکرد آمریکا به جنایات جنگی سایبری نیازمند بررسی سه بعد اصلی است: نخست؛ چارچوب قانونی داخلی و بین‌المللی، دوم؛ مواضع و استراتژی‌های نظامی و امنیت سایبری، و سوم؛ تفسیرهای حقوقی از اصول بنیادین حقوق بین‌الملل بشردوستانه، به‌ویژه اصول تمایز، تناسب و ضرورت نظامی.

۱-۱-۴. چارچوب قانونی و حقوقی ایالات متحده

ایالات متحده، برخلاف بسیاری از کشورها، رویکردی توسعه‌گرایانه و منعطف نسبت به حقوق بین‌الملل بشردوستانه[1]در حوزه سایبری اتخاذ کرده است. قوانین داخلی آمریکا، از جمله قانون جرایم رایانه‌ای[2]و قانون سیاست‌گذاری امنیت سایبری ملی[3]چارچوب‌های اجرایی برای مقابله با تهدیدات سایبری فراهم می‌کنند. علاوه بر این، دستورالعمل‌های اجرایی ریاست جمهوری و گزارش‌های وزارت دفاع آمریکا[4]نیز امکان شناسایی عملیات سایبری که اثرات ویرانگر مشابه حملات متعارف دارند را فراهم کرده‌اند (Dedy, 2025: 314). از منظر حقوق بین‌الملل، ایالات متحده با امضای Tallinn Manual 2.0و مستندات مرتبط، پذیرفته است که عملیات سایبری می‌تواند واجد ویژگی‌های یک «حمله مسلحانه» باشد و تحت قواعد حقوق بین‌الملل بشردوستانه قرار گیرد؛ با این حال، رویکرد آمریکا تمایل دارد تا تعاریف و دامنه کاربرد اصول حقوق بین‌الملل بشردوستانه را به گونه‌ای گسترش دهد که امکان استفاده از ابزارهای سایبری در عملیات نظامی و دفاعی افزایش یابد (Carlin & Dempsey, 2024: 128-129).

این رویکرد توسعه‌گرایانه به ایالات متحده امکان می‌دهد تا ضمن حفظ ظاهری رعایت قواعد بین‌المللی و ایجاد تصویری از احترام به نُرم‌های حقوقی، فضای کافی برای تفسیرهای حقوقی انعطاف‌پذیر و انتخابی داشته باشد. به عبارت دیگر، آمریکا می‌تواند اصول کلی حقوق بین‌الملل را به عنوان چارچوبی نمادین بپذیرد، اما در عمل، آن‌ها را به گونه‌ای تفسیر کند که با منافع امنیتی و استراتژیک خود سازگار باشد (Kosseff, 2025: 89-90).

از منظر رئالیسم نو، چنین استراتژی‌ای نه تنها یک ابزار دیپلماتیک برای حفظ مشروعیت بین‌المللی به حساب می‌آید، بلکه نوعی حفظ برتری قدرت و آزادی عمل در نظام آنارشیک بین‌الملل نیز محسوب می‌شود.از طرفی، در نظام بین‌المللی که فاقد اقتدار مرکزی است، دولت‌ها مسئولیت حفاظت از منافع خود را دارند و محدودیت‌های بیرونی چندانی بر رفتار آن‌ها اعمال نمی‌شود. در این چارچوب، ایالات متحده با حفظ ظاهر رعایت قواعد بین‌المللی، قادر است اقدامات سایبری تهاجمی و دفاعی خود را با درجه بالایی از انعطاف عملیاتی اجرا کند. به عبارت دیگر، این رویکرد امکان می‌دهد

1. International Humanitarian Law (IHL)
2. Computer Fraud and Abuse Act, CFAA
3. National Cybersecurity Policy Acts
4. DoD

که کشور از یک سو تصویر قانون‌مدار و مسئول ارائه دهد و از سوی دیگر، از ظرفیت کامل قدرت فناورانه و نظامی خود برای اهداف امنیتی و ژئوپلیتیکی بهره‌برداری کند. این ترکیب ظاهر قانونی و آزادی عمل واقعی، نمونه‌ای از استراتژی‌ای است که رئالیسم نو آن را پیش‌بینی می‌کند. دولت‌های بزرگ، به ویژه قدرت‌های هژمونیک، در پی حداکثرسازی امنیت و نفوذ خود هستند، حتی اگر این امر مستلزم تفسیر خلاقانه یا محدود قوانین بین‌المللی باشد. به این ترتیب، رویکرد توسعه‌گرایانه آمریکا در زمینه عملیات سایبری، هم مشروعیت بین‌المللی را حفظ می‌کند و هم تضمین می‌کند که در عرصه واقعی سیاست بین‌الملل، برتری و آزادی عمل آن به حداقل محدودیت‌ها محدود شود.

۲-۱-۴. استراتژی و مواضع نظامی سایبری

مواضع نظامی و امنیتی آمریکا نشان می‌دهد که سیاست سایبری این کشور بر بازدارندگی، آماده‌سازی پیشگیرانه و توانایی پاسخ متناسب تمرکز دارد. سند Cybersecurity Strategy 2023وزارت دفاع آمریکا، بر ضرورت توسعه قابلیت‌های حمله و دفاع سایبری همزمان با احترام به قواعد حقوق بین‌الملل بشردوستانه تأکید می‌کند (Trahan, 2025: 3).

به عبارت دیگر، ایالات متحده اصول تمایز، تناسب و ضرورت نظامی را در چارچوب نظریه «نقش مسئولیت متناسب[1]» برای عملیات سایبری تبیین کرده است. به عنوان مثال، در حملات سایبری مرتبط با مخاصمات اوکراین-روسیه ۲۰۲۲–۲۰۲۴، آمریکا ضمن پشتیبانی از زیرساخت‌های دفاعی اوکراین، اقداماتی انجام داد که از نظر حقوقی در چارچوب حقوق بین‌الملل بشردوستانه قابل توجیه دانسته شد، زیرا هدف اصلی عملیات، مراکز نظامی و شبکه‌های دفاعی روسیه بود و خسارت به غیرنظامیان محدود بود. این نمونه نشان‌دهنده توانایی آمریکا در استفاده از تفسیر موسع حقوقی برای مشروعیت‌بخشی به عملیات سایبری است (Biggio, 2025: 256-257).

۳-۱-۴. تحلیل اصول بنیادین حقوق بین‌الملل بشردوستانه

الف) اصل تمایز: رویکرد ایالات متحده در حوزه عملیات سایبری مبتنی بر این اصل است که حتی در محیط‌های پیچیده و دیجیتال نیز امکان تمایز دقیق میان اهداف نظامی و غیرنظامی وجود دارد (Orr, 2024: 477). به عبارت دیگر، آمریکا تلاش می‌کند حملات خود را طوری طراحی کند که صرفاً زیرساخت‌ها و سامانه‌های مرتبط با

1. Proportionality Responsibility

فعالیت‌های نظامی یا اهداف مشروع را هدف قرار دهند و از آسیب غیرضروری به شهروندان یا زیرساخت‌های غیرنظامی جلوگیری شود. فناوری‌های پیشرفته، از جمله هوش مصنوعی و تحلیل داده‌های کلان، به آمریکا این توانایی را می‌دهند که عملیات سایبری را با دقت بالا برنامه‌ریزی و اجرا کند و بر اساس اطلاعات بلادرنگ، مسیر حمله را اصلاح نماید (Coble, 2025: 303).

از منظر رئالیسم نو، این رویکرد نه‌تنها ابزاری برای حفظ مشروعیت بین‌المللی به شمار می‌رود، بلکه در عمل به ایالات متحده امکان می‌دهد مزیت عملیاتی و آزادی عمل در فضای آنارشیک بین‌الملل را حفظ کند. با تکیه بر فناوری و تحلیل دقیق، آمریکا قادر است کارآمدی قدرت سایبری خود را حداکثر کرده و در عین حال، به‌طور ظاهری خود را پایبند به اصول حقوق بین‌الملل بشردوستانه نشان دهد. این ترکیب از دقت عملیاتی و مشروعیت نمادین، نمونه‌ای بارز از رویکرد توسعه‌گرایانه آمریکا در مواجهه با چالش‌های نوظهور امنیت سایبری است.

ب) اصل تناسب: ایالات متحده، این اصل را غالباً به‌صورت «ارزیابی ریسک و پیامد[1]» تفسیر می‌کند. به این معنا که میزان خسارت به غیرنظامیان و زیرساخت‌های غیرنظامی باید متناسب با منافع و اهداف نظامی عملیات باشد. در عمل، این رویکرد اجازه می‌دهد که تصمیم‌گیرندگان آمریکایی با در نظر گرفتن احتمال آسیب و نتایج عملیاتی، ارزیابی کنند که آیا اجرای یک حمله خاص قابل توجیه است یا خیر (Bobenrieth, 2025: 66-67).

با این حال، در حوزه سایبری، اجرای اصل تناسب با چالش‌های منحصر به فردی مواجه است. عدم شفافیت در هدف‌گیری، اثرات غیرمستقیم و پیچیدگی‌های زنجیره‌ای زیرساخت‌های دیجیتال، باعث می‌شود که تخمین دقیق خسارت به غیرنظامیان و زیرساخت‌های غیرنظامی دشوار و غالباً به‌صورت انعطاف‌پذیر قضاوت شود. به عبارت دیگر، فناوری سایبری می‌تواند پیامدهای غیرمستقیم و غیرقابل پیش‌بینی ایجاد کند که در چارچوب سنتی حقوق بین‌الملل بشردوستانه، سنجش آن‌ها دشوار است (Efrony, 2024: 12-13).

از منظر رئالیسم نو، این تفسیر انعطاف‌پذیر به ایالات متحده اجازه می‌دهد در فضای آنارشیک بین‌الملل هم آزادی عمل خود را حفظ کرده و هم ظاهراً به اصول حقوق بین‌الملل بشردوستانه پایبند باشد. این رویکرد، نمونه‌ای از استراتژی

1. Risk- and Consequence-Based Assessment

توسعه‌گرایانه آمریکا است که ترکیبی از مشروعیت نمادین و حداکثرسازی توان عملیاتی را فراهم می‌کند و در عین حال، مدیریت ریسک عملیات سایبری را ممکن می‌سازد.

ج) اصل ضرورت نظامی: ایالات متحده این اصل را به‌صورت وسیع و پویا تفسیر می‌کند، به‌گونه‌ای که استفاده از عملیات سایبری را نه تنها به عنوان یک اقدام دفاعی محدود، بلکه به عنوان ابزاری پیشگیرانه و حتی بازدارنده مشروع می‌داند. به عبارت دیگر، هر عملیات سایبری که هدف آن ارتقای امنیت ملی و کاهش تهدیدهای موجود باشد، می‌تواند با استناد به اصل ضرورت توجیه شود (Lee, 2024: 5).

این تفسیر انعطاف‌پذیر، چارچوبی فراهم می‌آورد که به آمریکا اجازه می‌دهد در فضای آنارشیک بین‌الملل، آزادی عمل عملیاتی گسترده‌ای داشته باشد، بدون اینکه ظاهراً تعهدات خود به حقوق بین‌الملل بشردوستانه را زیر پا بگذارد. در عمل، این بدان معناست که عملیات سایبری می‌تواند به شکل پیشگیرانه، بازدارنده یا حتی محدود تهاجمی طراحی شود، مادامی که استدلال امنیت ملی و کاهش تهدیدها معتبر باشد (Joshi, 2025: 193). از منظر رئالیسم نو، این رویکرد نشان‌دهنده ترکیبی از حفظ مشروعیت بین‌المللی به صورت نمادین و حداکثرسازی توان عملیاتی و آزادی عمل واقعی است؛ یعنی ایالات متحده با بهره‌گیری از تفسیر گسترده اصل ضرورت، می‌تواند هم برتری سایبری خود را حفظ کند و هم انعطاف عملیاتی لازم برای مقابله با تهدیدهای پیچیده و نوظهور را داشته باشد.

تفسیر آمریکا از سه اصل بنیادین حقوق بین‌الملل بشردوستانه تمایز، تناسب و ضرورت نشان‌دهنده انعطاف حقوقی و رویکرد توسعه‌گرایانه در حوزه عملیات سایبری است. این رویکرد به ایالات متحده اجازه می‌دهد تا ظاهراً به اصول حقوق بین‌الملل بشردوستانه احترام بگذارد و خود را پایبند به چارچوب‌های قانونی بین‌المللی نشان دهد، در حالی که در عمل، آزادی عمل گسترده‌ای برای طراحی و اجرای عملیات سایبری حفظ می‌شود. در نتیجه، این استراتژی نه تنها مشروعیت نمادین بین‌المللی را برای آمریکا فراهم می‌کند، بلکه هیچ محدودیت جدی بر توانمندی عملیاتی و قدرت نظامی سایبری کشور اعمال نمی‌کند. از منظر رئالیسم نو، چنین ترکیبی نمونه‌ای از توسعه‌گرایی استراتژیک است: آمریکا هم برتری و امنیت خود را در فضای آنارشیک بین‌الملل حفظ می‌کند و هم چارچوب قانونی بین‌المللی را به نحوی انعطاف‌پذیر به کار می‌گیرد تا اقدامات خود را مشروع جلوه دهد.

۴-۱-۴. سازوکارهای نظارتی و پاسخگویی

ایالات متحده، به منظور حفظ حاکمیت و امنیت ملی خود، رویکردی محتاطانه نسبت به ایجاد و پذیرش سازوکارهای بین‌المللی الزام‌آور در حوزه عملیات سایبری اتخاذ کرده است. این کشور عمدتاً به جای تعهدات حقوقی سختگیرانه، از سازوکارهای خودتنظیمی، چارچوب‌های داخلی و همکاری‌های محدود با نهادهای بین‌المللی بهره می‌گیرد. چنین رویکردی، امکان پاسخگویی بین‌المللی مستقیم و محدودیت عملیاتی بر اقدامات سایبری آمریکا را به حداقل می‌رساند و در عین حال، تصویری از همکاری و رعایت نُرم‌های بین‌المللی ارائه می‌دهد (Sarkar & Shukla, 2025: 86-87). این سیاست کاملاً با پیش‌بینی‌های رئالیسم نو همخوانی دارد؛ طبق این دیدگاه، قدرت‌های بزرگ، به‌ویژه آمریکا، از هر سازوکار الزام‌آور بین‌المللی که ممکن است آزادی عمل نظامی یا سایبری آن‌ها را محدود کند، اجتناب می‌کنند. در فضای آنارشیک بین‌الملل، دولت‌ها مسئول اصلی حفاظت از منافع خود هستند و سازوکارهای بین‌المللی تنها زمانی مورد پذیرش قرار می‌گیرند که با منافع استراتژیک آن‌ها تداخل نداشته باشند. بنابراین، رویکرد محتاطانه آمریکا نمونه‌ای از حفظ برتری قدرت و انعطاف عملیاتی است، در حالی که به طور ظاهری همچنان از همکاری و رعایت نُرم‌های بین‌المللی سخن گفته می‌شود (Lin, 2025: 107-108).

به طور کلی، تحلیل رویکرد ایالات متحده نسبت به حقوق بین‌الملل بشردوستانه در فضای سایبری نشان می‌دهد که این کشور از یک استراتژی توسعه‌گرایانه و انعطاف‌پذیر بهره می‌برد. این رویکرد به آمریکا اجازه می‌دهد تا هم ظاهراً به نُرم‌های بین‌المللی پایبند باشد و هم آزادی عمل گسترده‌ای برای عملیات سایبری تهاجمی و دفاعی حفظ کند. از طرفی، اصول بنیادین حقوق بین‌الملل بشردوستانه تمایز، تناسب و ضرورت نظامی توسط آمریکا به شکل وسیع و پویا تفسیر می‌شوند. این تفسیر انعطاف‌پذیر، امکان مشروعیت‌بخشی به اقدامات سایبری، از جمله حملات دقیق و پیشگیرانه، را فراهم می‌کند و در عین حال به کشور اجازه می‌دهد تا توان عملیاتی و آزادی عمل نظامی خود را محدود نکند. همچنین، استراتژی ملی سایبری ایالات متحده، بر بازدارندگی، پیشگیری و پاسخ متناسب متمرکز است. نمونه‌های عملی این رویکرد، از جمله حمایت سایبری و اطلاعاتی آمریکا از اوکراین، نشان‌دهنده مشروعیت عملیاتی این سیاست‌ها در مواجهه با تهدیدهای پیچیده و نوظهور است. نهایتاً آنکه در سطح بین‌المللی، آمریکا رویکرد محتاطانه‌ای نسبت به سازوکارهای الزام‌آور دارد و عمدتاً بر چارچوب‌های داخلی و همکاری محدود با نهادهای بین‌المللی متکی است.

این سیاست باعث می‌شود که پاسخگویی بین‌المللی مستقیم به عملیات سایبری کشور محدود شود و در عین حال، ایالات متحده بتواند برتری و امنیت سایبری خود را حفظ کند. به طور کلی، توانایی آمریکا در اجرای عملیات سایبری مطابق با اصول حقوق بین‌الملل بشردوستانه، همزمان با حفظ آزادی عمل و قدرت نظامی، ناشی از ترکیبی از قدرت نظامی، فناوری پیشرفته و تفسیر توسعه‌گرایانه حقوق بین‌الملل است. این ترکیب نمونه‌ای بارز از استراتژی‌ای است که هم مشروعیت بین‌المللی را حفظ می‌کند و هم توان عملیاتی را به حداکثر می‌رساند.

۲-۴. امکان شناسایی و تعقیب جنایات جنگی در فضای سایبری با تأکید بر روسیه

روسیه، به عنوان یکی دیگر از بازیگران اصلی عرصه سایبری جهانی و قدرت نظامی بزرگ، رویکردی محافظه‌کارانه و مبتنی بر حاکمیت ملی نسبت به جنایات جنگی سایبری دارد. این رویکرد برخلاف سیاست توسعه‌گرایانه ایالات متحده، بر محدودیت‌های قانونی داخلی، حفظ کنترل بر اطلاعات و مقاومت در برابر نهادینه‌سازی قواعد الزام‌آور بین‌المللی تمرکز دارد. تحلیل رویکرد روسیه نیازمند بررسی سه بعد اصلی است: نخست؛ چارچوب حقوقی داخلی و نگرش نسبت به حقوق بین‌الملل بشردوستانه، دوم؛ استراتژی نظامی و امنیت سایبری، و سوم؛ تفسیر اصول بنیادین حقوق بین‌الملل بشردوستانه در فضای سایبری.

۱-۲-۴. چارچوب قانونی و حقوقی روسیه

روسیه قوانین داخلی گسترده‌ای در زمینه امنیت سایبری و کنترل فضای مجازی دارد، از جمله قانون فدرال «درباره اطلاعات، فناوری اطلاعات و حفاظت از اطلاعات» (۲۰۲۰) و قانون جرایم سایبری (۲۰۲۲). این قوانین تأکید دارند که هرگونه عملیات سایبری باید در چارچوب حاکمیت ملی انجام شود و دولت‌های خارجی حق مداخله در فضای اطلاعاتی روسیه را ندارند (Tokarev, 2024: 674-675). در حوزه حقوق بین‌الملل، روسیه موضع محدودکننده‌ای اتخاذ کرده است. این کشور با استناد به اصل حاکمیت ملی و عدم مداخله در امور داخلی کشورها، به سختی قواعد حقوق بین‌الملل بشردوستانه را به عملیات سایبری تعمیم می‌دهد. به بیان دیگر، اگرچه روسیه به طور کلی عضویت یا احترام به قوانین بین‌المللی را اعلام می‌کند، اما تفسیر محدود از تعاریف حمله مسلحانه سایبری و جنایات جنگی باعث می‌شود بیشتر عملیات‌های سایبری در

قلمرو داخلی یا در چارچوب سیاست‌های دفاعی مشروعیت یابند (Sambaluk, 2024: 37).

این رویکرد محدودکننده با نظریه رئالیسم نو سازگار است؛ روسیه با توجه به موقعیت خود در رقابت قدرت‌های بزرگ، از هرگونه هنجارسازی بین‌المللی که ممکن است آزادی عمل و ابزارهای دفاعی و تهاجمی آن را محدود کند، اجتناب می‌کند. در عین حال، این سیاست، فضای همکاری بین‌المللی را محدود کرده و موجب اختلاف در تفسیر اصول حقوق بین‌الملل بشردوستانه می‌شود.

۲-۲-۴. استراتژی نظامی و امنیت سایبری

استراتژی ملی سایبری روسیه، همانند مواضع حقوقی و قانونی این کشور، بر حفظ حاکمیت ملی، امنیت کشور و کنترل اطلاعات متمرکز است. اسناد رسمی، از جمله «راهبرد ملی امنیت سایبری روسیه ۲۰۲۳» و گزارش‌های وزارت دفاع، بر تقویت قابلیت‌های دفاعی و توسعه توانمندی‌های حمله محدود سایبری تأکید دارند. به عبارت دیگر، روسیه تلاش می‌کند فضای سایبری را به عنوان یک حوزه حیاتی برای حفاظت از منافع ملی و امنیت داخلی مدیریت کند و در عین حال، توانایی مقابله و پاسخ به تهدیدات خارجی را حفظ نماید (Mel'nik, 2024: 19).

هرچند اجرای عملیات تهاجمی سایبری در این چارچوب ممکن است، اما چنین اقداماتی باید به گونه‌ای طراحی شوند که از نظر حقوقی و سیاسی داخلی توجیه داشته باشند و همزمان از برخورد با محدودیت‌ها و نُرم‌های بین‌المللی پرهیز شود. این محدودیت‌ها، ناشی از ضرورت حفظ مشروعیت داخلی و جلوگیری از تشدید تنش‌های بین‌المللی است، زیرا آسیب مستقیم به غیرنظامیان یا نقض آشکار حقوق بین‌الملل می‌تواند پیامدهای سیاسی و اقتصادی جدی برای روسیه به همراه داشته باشد (Tsakanyan, 2025: 7-8).

نمونه عملی این رویکرد را می‌توان در جنگ اوکراین مشاهده کرد. روسیه در این جنگ از عملیات سایبری برای دستیابی به اهداف نظامی و راهبردی استفاده کرده است، اما تلاش کرده است که این عملیات به زیرساخت‌های نظامی، مراکز دولتی و سیستم‌های حیاتی محدود شود و از آسیب مستقیم به غیرنظامیان و زیرساخت‌های غیرنظامی اجتناب گردد. این نمونه نشان می‌دهد که روسیه در عمل، رویکرد محدودکننده، کنترل‌شده و مبتنی بر حاکمیت ملی را دنبال می‌کند، به گونه‌ای که هم با قوانین داخلی و هم با منافع امنیتی و دفاعی کشور هماهنگ باشد (Yakovleva, 2024: 387).

به طور کلی، استراتژی سایبری روسیه ترکیبی است از تقویت توانمندی‌های دفاعی، حفظ مشروعیت داخلی و محدود کردن مواجهه با فشارهای بین‌المللی. این رویکرد نشان می‌دهد که روسیه، برخلاف قدرت‌های بزرگ با استراتژی توسعه‌گرایانه مانند ایالات متحده، بیشتر بر کنترل و مدیریت محتاطانه فضای سایبری تمرکز دارد تا اطمینان حاصل کند که عملیات آن در چارچوب حاکمیت ملی و امنیت داخلی قابل توجیه است و در عین حال، اثرگذاری عملیاتی خود را محدود به اهداف مشخص نظامی و دولتی نگه می‌دارد.

۳-۲-۴. تحلیل اصول بنیادین حقوق بین‌الملل بشردوستانه

الف) اصل تمایز: روسیه اصل تمایز را در عملیات سایبری به شکل محدود و محافظه‌کارانه تفسیر می‌کند. طبق مواضع حقوقی و سیاست‌های رسمی، هرگونه عملیات سایبری که به اهداف غیرنظامی آسیب برساند، از نظر قوانین داخلی و استانداردهای بین‌المللی قابل توجیه نیست. این رویکرد منعکس‌کننده تمرکز روسیه بر حاکمیت ملی، امنیت داخلی و محدودیت‌های حقوقی است و نشان می‌دهد که این کشور به صورت رسمی، احترام به حقوق بین‌الملل بشردوستانه را یک اصل اساسی در فضای سایبری می‌داند (Shtodina, 2024: 115).

با این حال، در عمل، تعیین دقیق مرز بین اهداف نظامی و زیرساخت‌های غیرنظامی در فضای سایبری بسیار دشوار است. پیچیدگی شبکه‌های دیجیتال، وابستگی متقابل زیرساخت‌ها و اثرات زنجیره‌ای حملات سایبری، تعریف «هدف نظامی» و «زیرساخت غیرنظامی» را با ابهام مواجه می‌کند. این چالش عملی موجب شده که برخی عملیات روسیه با تفسیرهای متفاوت جامعه بین‌المللی مواجه شده و اختلافات حقوقی به وجود آورد (Melella et al., 2024: 4-5). بنابراین، رویکرد روسیه به اصل تمایز در فضای سایبری نشان‌دهنده ترکیبی از محافظه‌کاری حقوقی و محدودیت عملیاتی ناشی از پیچیدگی فناوری است؛ کشور تلاش می‌کند هم مشروعیت داخلی و بین‌المللی را حفظ کند و هم توان عملیاتی خود را در چارچوب اهداف نظامی محدود مدیریت نماید.

ب) اصل تناسب: روسیه اصل تناسب را در عملیات سایبری به‌صورت محافظه‌کارانه و محدودکننده ارزیابی می‌کند. مطابق با این رویکرد، میزان خسارت به غیرنظامیان باید تا حد ممکن کاهش یابد و هیچ‌گونه عملیاتی نباید اثرات غیرضروری یا گسترده بر زیرساخت‌های غیرنظامی داشته باشد. حتی زمانی که اهداف عملیات کاملاً نظامی هستند، روسیه ملاحظات داخلی و بین‌المللی را در نظر می‌گیرد و از انجام اقداماتی

که می‌تواند خسارت قابل توجه یا پیامدهای سیاسی منفی ایجاد کند، اجتناب می‌نماید (Kolodii, 2024: 652-653).

این رویکرد منعکس‌کننده تمرکز روسیه بر حاکمیت ملی، امنیت داخلی و مشروعیت حقوقی است و نشان می‌دهد که کشور تلاش دارد تا توان عملیاتی سایبری خود را در چارچوب محدودیت‌های اخلاقی و قانونی مدیریت کند. با این وجود، پیچیدگی و غیرقابل پیش‌بینی بودن اثرات عملیات سایبری، اجرای دقیق اصل تناسب را دشوار می‌کند و در برخی موارد باعث اختلاف‌نظر با جامعه بین‌المللی شده است (Grib & Kudra, 2024: 32-33). به طور کلی، تفسیر محافظه‌کارانه روسیه از اصل تناسب، نمونه‌ای از ترکیب محدودکنندگی قانونی و مدیریت محتاطانه فضای سایبری است که هدف آن حفاظت از غیرنظامیان و زیرساخت‌های حیاتی، بدون کاهش توان عملیاتی برای اهداف نظامی می‌باشد.

ج) اصل ضرورت نظامی: در تفسیر روسیه، اصل ضرورت نظامی عمدتاً به معنای دفاع از حاکمیت ملی و امنیت داخلی است و تأکید کمی بر استفاده تهاجمی فراتر از مرزهای ملی دارد. به عبارت دیگر، هرگونه عملیات سایبری باید با هدف حفاظت از منافع داخلی و کاهش تهدیدهای موجود برای کشور طراحی شود و نه صرفاً برای اعمال قدرت در خارج از قلمرو ملی (Bassett, 2024: 79).

این رویکرد باعث می‌شود که عملیات سایبری روسیه غالباً محدود به اهداف دفاعی و بازدارنده باشد و انعطاف عملیاتی آن، به ویژه در مقایسه با رویکرد توسعه‌گرایانه و گسترده آمریکا، کمتر باشد. از منظر حقوقی، این سیاست انعطاف کمی برای توجیه اقدامات پیشگیرانه یا حملات سایبری فرامرزی فراهم می‌کند و نشان‌دهنده تمرکز روسیه بر کنترل محتاطانه فضای سایبری و محدود کردن پیامدهای بین‌المللی است (Parmaar, 2024: 5). لذا، تفسیر روسیه از اصل ضرورت، نمونه‌ای از ترکیب محافظه‌کاری حقوقی و محدودیت عملیاتی مبتنی بر حاکمیت ملی است؛ یعنی کشور تلاش می‌کند هم مشروعیت داخلی و بین‌المللی را حفظ کند و هم توان دفاعی خود را به شکل کنترل‌شده و محدود به کار گیرد.

به طور کلی، رویکرد روسیه در فضای سایبری، نشان‌دهنده محافظه‌کاری حقوقی و عملی است که با تأکید بر اصل حاکمیت ملی و محدود کردن دامنه عملیات سایبری، تلاش می‌کند تعارضات حقوقی بین‌المللی را به حداقل برساند. این سیاست محدودکننده، باعث می‌شود که عملیات روسیه عمدتاً دفاعی، بازدارنده و محدود به اهداف نظامی داخلی باشد و انعطاف‌پذیری کمتری نسبت به اقدامات پیشگیرانه یا

تهاجمی فرامرزی داشته باشد. در مقابل، ایالات متحده با رویکرد توسعه‌گرایانه و انعطاف‌پذیر نسبت به حقوق بین‌الملل بشردوستانه، توانسته است آزادی عمل گسترده‌ای برای اجرای عملیات سایبری تهاجمی و دفاعی به دست آورد. این تفاوت بنیادین در تفسیر اصول حقوق بین‌الملل بشردوستانه و مدیریت فضای سایبری، زمینه را برای اختلافات حقوقی و ژئوپلیتیکی بین دو قدرت بزرگ فراهم می‌کند؛ روسیه تلاش می‌کند چارچوب محدودکننده خود را حفظ کند، در حالی که آمریکا از تفسیر وسیع خود برای حداکثرسازی قدرت عملیاتی بهره می‌برد. این تضاد میان محافظه‌کاری روسیه و توسعه‌گرایی آمریکا نشان‌دهنده دو مسیر متفاوت در مواجهه با چالش‌های حقوقی، عملیاتی و استراتژیک فضای سایبری است و پیامدهای آن برای نظم بین‌المللی و تعاملات قدرت‌های بزرگ قابل توجه است.

۴-۲-۴. سازوکارهای نظارتی و پاسخگویی

برخلاف ایالات متحده، روسیه تمایل دارد بیشتر از سازوکارهای داخلی و ملی برای مدیریت فضای سایبری استفاده کند تا اطمینان حاصل شود که عملیات سایبری تحت کنترل کامل دولت باقی بماند و تصمیم‌گیری درباره آن صرفاً در چارچوب منافع ملی و امنیت داخلی انجام شود. این کشور به ندرت به سازوکارهای الزام‌آور بین‌المللی اعتماد می‌کند و نهادهایی مانند دیوان کیفری بین‌المللی، گروه‌های کارشناسی سازمان ملل و سایر سازوکارهای جهانی، به دلیل پافشاری روسیه بر اصل حاکمیت ملی و عدم مداخله خارجی، کمتر قادر به اعمال فشار یا محدود کردن اقدامات سایبری آن هستند. به عبارت دیگر، روسیه ترجیح می‌دهد قوانین و چارچوب‌های داخلی خود را مبنای پاسخگویی و کنترل عملیات سایبری قرار دهد و از پذیرش الزامات بین‌المللی که ممکن است آزادی عمل آن را محدود کند، اجتناب (Pavlikova, 2024: 60-61).

این رویکرد با مبانی رئالیسم نو سازگار است زیرا بر اساس این دیدگاه، قدرت‌های بزرگ از هر هنجارسازی یا سازوکار بین‌المللی که ممکن است توان عملیاتی یا آزادی عمل نظامی و سایبری آن‌ها را محدود کند، دوری می‌کنند. روسیه با تمرکز بر حاکمیت و قوانین داخلی، تلاش می‌کند ضمن حفظ کنترل کامل بر فعالیت‌های سایبری خود، پیامدهای حقوقی و سیاسی ناشی از فشارهای بین‌المللی را به حداقل برساند. نتیجه عملی این رویکرد، ایجاد کاهش چشمگیر در امکان پاسخگویی کیفری بین‌المللی است. در عمل، خلأهایی در زمینه شناسایی، مستندسازی و تعقیب جرایم جنگی سایبری ایجاد می‌شود که نهادهای بین‌المللی را در اعمال استانداردهای حقوقی محدود می‌کند. این وضعیت به روسیه اجازه می‌دهد تا توان عملیاتی خود را در حوزه

سایبری حداکثر کرده و همزمان خطر پیامدهای بین‌المللی را کاهش دهد. علاوه بر این، سیاست محدود کردن سازوکارهای بین‌المللی، همخوان با استراتژی کلی روسیه در حفظ حاکمیت، امنیت ملی و کنترل اطلاعات است و نمونه‌ای از مدیریت محتاطانه و محافظه‌کارانه فضای سایبری به حساب می‌آید. بنابراین، رویکرد روسیه به سازوکارهای بین‌المللی و حقوق بین‌الملل در فضای سایبری، نشان‌دهنده ترکیب محافظه‌کاری قانونی، تمرکز بر حاکمیت ملی و مدیریت محتاطانه عملیات سایبری است؛ این سیاست، در عین حفظ کنترل داخلی و توان عملیاتی، زمینه اختلاف و رقابت با ایالات متحده و دیگر قدرت‌های بزرگ را نیز فراهم می‌کند، زیرا آزادی عمل نسبی و تفسیر توسعه‌گرایانه حقوق توسط آمریکا، با محدودیت محافظه‌کارانه روسیه در تضاد قرار می‌گیرد. به طور کلی، تحلیل رویکرد روسیه نسبت به حقوق بین‌الملل بشردوستانه در فضای سایبری نشان می‌دهد:

- روسیه رویکردی محدودکننده و مبتنی بر حاکمیت ملی در حوزه عملیات سایبری دارد؛
- اصول تمایز، تناسب و ضرورت نظامی به گونه‌ای محافظه‌کارانه تفسیر می‌شوند تا محدودیت‌ها برای فعالیت‌های داخلی و دفاعی رعایت شود؛
- استراتژی ملی سایبری روسیه بر بازدارندگی، امنیت و کنترل اطلاعات تمرکز دارد و کمتر به استفاده توسعه‌گرایانه از ابزارهای سایبری توجه دارد؛
- روسیه از سازوکارهای بین‌المللی الزام‌آور اجتناب می‌کند و بیشتر بر چارچوب‌های داخلی و منافع امنیت ملی تأکید دارد؛
- این رویکرد باعث کاهش امکان پاسخگویی بین‌المللی و ایجاد اختلاف در تعریف و تفسیر جنایات جنگی سایبری با قدرت‌های دیگر، به ویژه آمریکا، می‌شود.

۳-۴. امکان شناسایی و تعقیب جنایات جنگی در فضای سایبری؛ مطالعه تطبیقی ایالات متحده و روسیه

با توجه به نقش فزاینده فضای سایبری به‌عنوان میدان جدید رقابت قدرت‌های بزرگ، تحلیل تطبیقی رویکردهای ایالات متحده و روسیه در حوزه شناسایی و تعقیب جنایات جنگی سایبری، هم از منظر حقوقی و هم از منظر عملی اهمیت ویژه‌ای دارد. در این بخش، تفاوت‌ها و همگرایی‌های دو کشور بررسی شده و آثار آن‌ها بر مسئولیت کیفری بین‌المللی و شکل‌گیری هنجارهای رفتاری در نظام بین‌الملل تبیین می‌گردد.

۱-۳-۴. تفاوت‌های بنیادین رویکرد آمریکا و روسیه

الف) مبانی حقوقی و نحوه تفسیر حقوق بین‌الملل بشردوستانه: ایالات متحده رویکردی توسعه‌گرا اتخاذ می‌کند و می‌کوشد اصول حقوق بین‌الملل بشردوستانه را با شرایط نوظهور فضای سایبری منطبق سازد. تفسیر اصولی چون تمایز، تناسب و ضرورت نظامی در آمریکا انعطاف‌پذیر بوده و زمینه مشروعیت‌بخشی به دامنه وسیع‌تری از عملیات سایبری را فراهم می‌کند. روسیه در نقطه مقابل، تفسیری محافظه‌کارانه و مبتنی بر اصل حاکمیت ملی ارائه می‌دهد. از منظر روسیه، کاربرد حقوق بین‌الملل بشردوستانه در فضای سایبری باید محدود بماند و عملیات سایبری عمدتاً در چهارچوب دفاع و بازدارندگی تعریف می‌شود. این دو نگرش، دو منطق متفاوت از نسبت میان قدرت و حقوق بین‌الملل را بازتاب می‌دهند به این صورت که آمریکا به‌دنبال افزایش آزادی عمل، و روسیه در پی تحکیم کنترل و امنیت ملی است.

ب) چارچوب قانونی داخلی و تعامل با قواعد بین‌المللی: ایالات متحده با تکیه بر قوانینی مانندCFAA ، اسناد سیاست‌گذاری امنیت سایبری و تفسیرهای مکتب تالین بستر گسترده‌تری برای اجرای عملیات سایبری فراهم می‌آورد. این کشور عموماً از سازوکارهای الزام‌آور بین‌المللی فاصله می‌گیرد و ترجیح می‌دهد نقش‌آفرینی خود را از طریق رژیم‌های همکاری غیرالزام‌آور پیش ببرد. روسیه نیز اگرچه از چارچوب قانونی داخلی گسترده‌ای برخوردار است، اما این ساختار بیشتر تأکید بر کنترل دولتی و صیانت از حاکمیت دارد. مشابه آمریکا، مسکو نیز از سازوکارهای الزام‌آور بین‌المللی فاصله می‌گیرد اما با هدف محدودسازی مداخلات خارجی و نه گسترش آزادی عمل فرامرزی. در نتیجه، اگرچه هر دو کشور چارچوب قانونی داخلی دارند، هدف‌گذاری‌ها متفاوت است: آمریکا به‌دنبال ظرفیت‌سازی برای عملیات فرامرزی و روسیه به‌دنبال تثبیت محدودیت‌های کنترلی. این تفاوت موجب تشتت در تعریف «حمله مسلحانه سایبری» و تفسیر مسئولیت کیفری بین‌المللی می‌شود.

ج) جهت‌گیری‌های نظامی و امنیت سایبری: ایالات متحده سیاست سایبری خود را بر بازدارندگی فعال، عملیات پیش‌دستانه و پاسخ متناسب بنا کرده است. ترکیب توان تهاجمی و دفاعی، همراه با تفسیر انعطاف‌پذیر اصول حقوق بشردوستانه، امکان اقدام سایبری گسترده‌تری را فراهم می‌سازد. روسیه به‌طور سنتی بر امنیت ملی، کنترل داخلی و بازدارندگی محدود تمرکز دارد. عملیات تهاجمی سایبری این کشور بیشتر به حوزه‌های داخلی و نظامی محدود است و انعطاف‌پذیری کمتری نسبت به

آمریکا دارد. این اختلافات بازتاب‌دهنده تفاوت در درک تهدیدات، منافع ملی و برداشت آن‌ها از جایگاه خود در نظم بین‌الملل است.

۲-۳-۴. نقاط اشتراک آمریکا و روسیه

با وجود تفاوت‌های عمیق، دو کشور در چند محور همگرایی دارند.

الف) پایبندی به اصول بنیادین حقوق بین‌الملل بشردوستانه: هر دو کشور اصولی همچون تمایز، تناسب و ضرورت نظامی را پذیرفته‌اند؛ هرچند حدود و قلمرو این اصول را متفاوت تفسیر می‌کنند.

ب) اولویت‌دهی به امنیت ملی: صرف‌نظر از تفاوت رویکرد، عملیات سایبری در هر دو کشور در راستای حفظ منافع ملی و تقویت قدرت نظامی طراحی می‌شود.

ج) پرهیز از سازوکارهای الزام‌آور بین‌المللی: هر دو قدرت از پذیرش قواعدی که ممکن است آزادی عمل سایبری آن‌ها را محدود کند، احتراز می‌کنند.

د) اتکا به فناوری‌های پیشرفته برای ارزیابی اهداف: استفاده از ابزارهای پیچیده تحلیل داده و شناسایی اهداف، عنصر مشترک هر دو قدرت در برنامه‌ریزی عملیات سایبری است.

این اشتراکات نشان می‌دهد که حتی در چارچوب رقابت قدرت‌ها، منطق رئالیستی در حوزه سایبری بر تفسیرهای حقوقی غلبه دارد.

۳-۳-۴. پیامدهای حقوقی و عملی

الف) اختلاف در تعریف جنایات جنگی سایبری: تنوع در تفسیر اصول حقوق بین‌الملل بشردوستانه و نبود تعریف یکپارچه از «حمله مسلحانه سایبری» موجب ابهام در تحقق مسئولیت کیفری بین‌المللی شده است.

ب) تعامل میان انعطاف‌پذیری آمریکا و محدودیت روسیه: رویکرد توسعه‌گرا و آزادی عمل گسترده آمریکا در مقابل رویه محدودکننده روسیه می‌تواند زمینه‌ساز تنش‌های حقوقی و سیاسی در سطح جهانی شود.

ج) پایداری خلأهای نهادی: عدم تمایل دو کشور به پذیرش نهادهای الزام‌آور موجب می‌شود نهادهای بین‌المللی مانند دیوان کیفری بین‌المللی توان محدودی در اعمال مسئولیت‌پذیری سایبری داشته باشند.

د) پیامدهای امنیتی برای نظام بین‌الملل: رقابت، عدم شفافیت و نبود قواعد الزام‌آور، ریسک وقوع حملات سایبری غیرمنتسب و پراکنده را افزایش می‌دهد و ثبات امنیتی جهانی را تهدید می‌کند.

در یک نگاه تطبیقی، می‌توان گفت که جنایات جنگی در فضای سایبری از نظر اصول حقوق بین‌الملل بشردوستانه قابل شناسایی‌اند، اما تحقق مسئولیت کیفری بین‌المللی آن‌ها با موانع جدی مواجه است. تفاوت رویکرد آمریکا و روسیه که ترکیبی از منافع ملی، ملاحظات امنیتی و برداشت‌های متفاوت از حقوق بین‌الملل است به شکاف‌های حقوقی و نهادی در سطح بین‌المللی دامن می‌زند. این وضعیت خود نشان‌دهنده ضرورت توسعه سازوکارهای شفاف، تقویت همکاری‌های چندجانبه و حرکت به‌سوی تنظیم‌گری بین‌المللی منسجم در حوزه سایبری است.

۵. نتیجه‌گیری و پیشنهاد

پژوهش حاضر نشان داد که فضای سایبری به‌عنوان عرصه‌ای نوظهور در مخاصمات مسلحانه، چالش‌های جدی و متفاوتی برای حقوق بین‌الملل بشردوستانه و نظام پاسخگویی کیفری بین‌المللی ایجاد کرده است. ماهیت غیرمادی، فرامرزی و متغیر این فضا، آن را از جنگ‌های سنتی متمایز می‌کند و سبب می‌شود اعمال قواعد کلاسیک حقوق بشردوستانه، هرچند از نظر نظری ممکن، در عمل با محدودیت‌های قابل توجهی روبه‌رو باشد. این محدودیت‌ها تنها ناشی از فناوری یا خلأهای حقوقی نیستند، بلکه در بستر ساختار سیاسی و رقابت قدرت‌ها ریشه دارند.

تحلیل تطبیقی رویکرد ایالات متحده و روسیه نشان می‌دهد که منطق قدرت، نه صرفاً قواعد حقوقی، تعیین‌کننده رفتار دولت‌ها در حوزه جنگ سایبری است. آمریکا با تفسیری توسعه‌گرایانه از اصول حقوق بین‌الملل بشردوستانه، درصدد افزایش آزادی عمل برای انجام عملیات دفاعی و تهاجمی است و تفسیر حقوقی را ابزاری برای مشروعیت‌بخشی به اقدامات خود در نظام آنارشیک می‌داند. در مقابل، روسیه بر محدودسازی و حفظ حاکمیت ملی تأکید دارد و دامنه اجرای عملی قواعد حقوق بشردوستانه را به‌نحوی تنظیم می‌کند که امنیت داخلی و کنترل ملی اولویت یابد. این تضاد رویکردها نشان می‌دهد که اجرای مؤثر حقوق بشردوستانه در حوزه سایبری تنها در شرایط اجماع یا همکاری میان قدرت‌های بزرگ امکان‌پذیر است.

همچنین، پژوهش حاضر نشان داد که فرآیند پاسخگویی کیفری بین‌المللی در حوزه جنایات جنگی سایبری تابع سه متغیر کلیدی است: نخست، ساختار آنارشیک نظام بین‌الملل که موجب مقاومت قدرت‌ها در برابر قواعد الزام‌آور می‌شود؛ دوم، تفاوت رویکرد دولت‌ها در تفسیر اصول حقوق بشردوستانه که از توسعه‌گرایی تا محدودکنندگی متغیر است و خلأهای عملی در انتساب و تعقیب مسئولیت ایجاد می‌کند؛ و سوم، ضعف نهادها و سازوکارهای بین‌المللی که ابزار کافی برای اعمال فشار

یا تضمین اجرای قواعد ندارند. این عوامل نشان می‌دهند که محدودیت‌های موجود در شناسایی و تعقیب جنایات جنگی سایبری بیشتر ناشی از رقابت سیاسی و منافع قدرت‌هاست تا نقص قواعد حقوقی. عدم اجماع میان قدرت‌های بزرگ موجب تداوم شرایطی می‌شود که در آن امکان سوءاستفاده از عرصه سایبری افزایش می‌یابد و زیرساخت‌های حیاتی غیرنظامی در معرض تهدید قرار می‌گیرند. در غیاب مکانیسم‌های همکاری و سازوکارهای شفاف، حملات سایبری می‌توانند پیامدهای انسانی، امنیتی و اقتصادی گسترده داشته باشند. همچنین یافته‌ها نشان داد که نظریه رئالیسم نو ابزار مفیدی برای فهم رفتار دولت‌ها در زمینه جنایات جنگی سایبری است؛ زیرا توضیح می‌دهد که قواعد بین‌المللی تا زمانی مؤثرند که با منافع قدرت‌های بزرگ سازگار باشند. این دیدگاه علت محدود شدن نقش عملی حقوق بشردوستانه در فضای سایبری را روشن می‌سازد و نشان می‌دهد که تحلیل حقوقی باید همراه با تحلیل سیاسی باشد.

در نهایت، پژوهش تأکید می‌کند که فضای سایبری خارج از حوزه حقوق بین‌الملل نیست، اما موفقیت در اجرای مسئولیت کیفری بین‌المللی در این عرصه نیازمند همگرایی میان حقوق، سیاست و فناوری است. تعامل پیچیده این عوامل تعیین می‌کند که عدالت بین‌المللی در حوزه جنگ سایبری تا چه اندازه قابل تحقق باشد. بر اساس نتایج پژوهش، چند توصیه کلیدی برای سیاست‌گذاری قابل استخراج است:

۱- طراحی یک رژیم حکمرانی سایبری بین‌المللی با قواعد الزام‌آور و قابل اجرا: ایجاد یک رژیم واحد و شفاف می‌تواند پراکندگی تفاسیر حقوقی را کاهش داده و استانداردهای مشترک رفتاری را در منازعات سایبری تثبیت کند. چنین رژیمی باید شامل سازوکارهای نظارت، اجرا و تنبیه باشد تا از تبدیل‌شدن قواعد به صرف توصیه‌های غیرالزام‌آور جلوگیری شود؛

۲. ایجاد مجمع راهبردی قدرت‌های سایبری برای مدیریت رقابت و افزایش همکاری امنیتی: برقراری یک چارچوب گفت‌وگوی نهادی میان قدرت‌های بزرگ (مانند آمریکا، روسیه، چین و اتحادیه اروپا) می‌تواند از تشدید رقابت ساختاری جلوگیری کرده و فضای لازم برای شناسایی، انتساب و پاسخ هماهنگ به حملات سایبری را فراهم سازد. این مجمع باید سازوکاری برای حل‌وفصل اختلافات و مدیریت بحران‌های سایبری نیز داشته باشد؛

۳. سرمایه‌گذاری در یکپارچه‌سازی ابزارهای فنی انتساب با سازوکارهای حقوقی قابل اتکا: توانمندسازی ظرفیت‌های فنی مانند تحلیل‌های مبتنی بر هوش مصنوعی،

ردگیری زنجیره حملات و تقویت زیرساخت‌های دیجیتال باید همزمان با توسعه چارچوب‌های حقوقی دقیق برای ارزیابی شواهد انجام شود. این هم‌افزایی، امکان انتساب معتبر و جلوگیری از ادعاهای ساختگی یا سیاسی‌شده را افزایش می‌دهد؛

۴- همسوسازی قوانین ملی سایبری با استانداردهای بین‌الملل بشردوستانه و ایجاد انطباق عملیاتی: کشورها باید قوانین داخلی خود درباره حملات سایبری، امنیت دیجیتال و دفاع سایبری را به‌گونه‌ای تنظیم کنند که با اصول بنیادین حقوق بشردوستانه مانند تمایز، تناسب و احتیاط سازگار باشد. این هماهنگی، اجرای قواعد بین‌المللی در سطح ملی را تسهیل کرده و از ایجاد نقاط خلأ حقوقی جلوگیری می‌کند؛

۵- تقویت ظرفیت‌سازی جهانی و انتقال دانش برای کاهش نابرابری سایبری میان دولت‌ها: اختلاف فنی و حقوقی میان کشورها، نظم سایبری را شکننده می‌کند و زمینه سوءاستفاده را برای بازیگران قدرتمند فراهم می‌آورد. ظرفیت‌سازی مشترک در حوزه آموزش، فناوری و استانداردسازی، انسجام ساختار امنیت سایبری جهانی را افزایش می‌دهد و مانع از شکل‌گیری مناطق خارج از کنترل می‌شود.

فهرست منابع

- Bassett, L. (2024). Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare. Journal of Transnational Law, (8), 76-94.
- Biggio, G. (2025). Regulating non-kinetic effects of cyber operations: the ‘Loss of Battlefield’ paradigm. Journal of Conflict & Security Law, 30(2), 241- 278.
- Bobenrieth, E. (2025). US military legal doctrine and the emerging wartime cyber environment. International Review of the Red Cross, 38(3), 57-80.
- Carlin, J., & Dempsey, J. (2024). Cybersecurity Law Fundamentals. NewYork: Columbia University Press.
- Clarkson, J. (2025). The Rousseauian roots of neorealism. Journal of Review of International Studies, 48(1), 629-650.
- Coble, K. (2025). A US perspective on special operations and the law of armed conflict. International Review of the Red Cross, 38(4), 289-311.
- Dedy, M. (2025). The evolution of cyber law: Protecting privacy and security in the digital age. Journal of Information Systems Engineering and Management, 10(5), 307-332.

- Efrony, D. (2024). Enhancing accountability in cyberspace through a three-pillar model. U.S. Naval War College International Law Studies, 24(1), 1-27.
- Grib, V. G., & Kudra, A. S. (2024). On Some Problems of Ownership of Rights to the Results of the Work of Artificial Intelligence Systems (Russia & foreign countries). Eurasian Law Journal, 194(7), 23-48.
- Joshi, A. (2025). Key US cyber law expires, and other cybersecurity news. World Economic Forum. Berkeley: University of California Press.
- Kolodii, R. (2024). Unpacking Russia's Cyber-Incident Response. Journal of Security Studies, 33(4), 640-669.
- Kosseff, J. (2025). Cybersecurity Law (4th ed.). New Jersey: John Wiley & Sons.
- Lee, J. (2024). Autonomous weapons, war crimes, and accountability. North Carolina Journal of International Law, 18(2), 1-25.
- Lin, L. S. (2025). Organisational challenges in US law enforcement's response to AI-driven cybercrime and deepfake fraud. Laws, 14(4), 98-124.
- Mel'nik, S. S. (2024). Legal regulation of cyber-extremism and cyber-terrorism: challenges and opportunities. Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 1, 187-210.
- Melella, C., Ferazza, F., and Mersinas, K. (2024). Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies. Journal of Applied Cybersecurity & Internet Governance, 14(2), 1-21.
- Orr, Z. R. (2024). Addressing unlawful cyber operations in armed conflict through human rights bodies instead of the International Criminal Court. Journal of Transnational Law, (57), 468-492.
- Parmaar, S. (2024). The Cyberwar Between Russia and Ukraine: Impacts and Implications. Journal of Global Law Review, 28(1), 1-19.
- Pavlikova, M. P. (2024). Russian Active Measures in Cyberspace through the Lens of Security Sectors. Politicke Vedy, 25(4), 50-76.
- Polinder, S. (2025). Towards A New Christian Political Realism: The Amsterdam School of Philosophy and the Role of Religion in International Relations. London: Routledge.
- Sambaluk, N. M. (2024). Weaponizing Cyberspace: Inside Russia's Hostile Activities. London: Bloomsbury Academic.
- Sarkar, G., & Shukla, S. (2025). Cyber slavery infrastructures: A socio-technical study of forced criminality in transnational cybercrime. New Jersey: Princeton University Press.
- Shtodina, D. D. (2025). United Nations Convention against Cybercrime, 2024 – the Outcome of "Cyber Compromise"? Moscow Journal of International Law, 1(4), 110-124 .
- Tabak, M. (2025). Realism in International Relations: The Making of a Disarrayed Tradition. London: Palgrave Macmillan.

- Tokarev, A. M. (2024). Legal regulation of deepfake technologies in the Russian Federation. Eurasian Law Journal, 26(4), 663-689.
- Trahan, J. (2025). Cyber operations and the crime of aggression. Case Western Reserve. Journal of International Law, 22(3), 1-23.
- Tsakanyan, V. (2025). Russia’s Escalating Digital Iron Curtain: New Data Laws and Their Geopolitical Fallout. Center for Cyber Diplomacy and International Security. Oxford Journal of Legal Studies, 36(1), 1-23.
- Williams, M. J., Hutto, J. W., & Dogra, A. P. (2025). Realism; In Understanding International Security: Theory and Practice. London: Cambridge University Press.
- Yakovleva, A. V. (2024). Cybersecurity and its Legal Regulation (Foreign and Russian Experience). Journal of Sociopolitical Sciences, 11(4), 381-403.