Public Law Studies Quarterly, Vol. ??, No ??, ?? ??
DOI: 10.22059/JPLSQ.2022.329515.2869

Cyber international law and the development of the jurisdiction of the International Criminal Court (Emphasizing the Tallinn talks of 2017)

(Type of Paper: Research Article)

Alireza mohaghegh Harcheghan[1], Mohammad Ali Ardebily[2]*,

Ebrahim Beigzadeh[3], Mohammad Ali Mahdavi Sabet[4]

Abstract

Since the cyberspace has changed the concept of national sovereignty and political independence of countries, the international community is obliged to react against it and to protect cyber sovereignty. Thus, within the framework of the principles and rules of international law, the international community has foreseen the jurisdiction of the judiciary in accordance with the provisions of international criminal law at odds with violations of cyber sovereignty and ancillary jurisdiction has been acted with regard to governance considerations. At the first step, Tallinn's talks expanded the jurisdiction of the International Criminal Court by explaining cyber-aggression as a violation of international cyber peace and security and the need to pay attention to the principle of non-interference in the internal affairs of countries (national sovereignty). The enhancement of the authority of this institution in accordance with customary international law in line with international criminal policy (countering to impunity) is done in order to maintain and restore international cyber peace and security.

Keywords

cyber sovereignty, Cyber competence, International criminal policy, Competency development, Permanent International Criminal Court.

---

1. PhD Student in Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Email: alireza.mohaghegh.1400@gmail.com
2. Professor, Department of Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran (Corresponding Author). Email: m-Ardebili@sbu.ac.ir
3. Professor, Department of International Law, Faculty of Law, Shahid Beheshti University, Tehran, Iran.
Email: Ebrahim_Beigzadeh@sbu.ac.ir
4. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Science and Research Branch, Islamic Azad University, Tehran, Iran.
Email: ali@mahdavi.fr

Received: August 30, 2021 - Accepted: April 17, 2022

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International, which permits others to download this work, share it with others and Adapt the material for any purpose.

فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ؟؟، شمارهٔ ؟؟، ؟؟ ؟؟: ۱-۲۴
DOI: 10.22059/JPLSQ.2022.329515.2869

حقوق بین‌الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)

(نوع مقاله: علمی _ پژوهشی)

علیرضا محقق هرچقان[۱]، محمدعلی اردبیلی[۲]*، ابراهیم بیگ‌زاده[۳]، محمدعلی مهدوی ثابت[۴]

چکیده

نظر به اینکه فضای سایبر مفهوم حاکمیت ملی و استقلال سیاسی کشورها را متحول ساخته، جامعهٔ بین‌الملل در مقابل آن و در جهت صیانت از حاکمیت سایبری ملزم به واکنش شده است. ازاین‌رو جامعهٔ بین‌المللی در چارچوب اصول و قواعد حقوق بین‌الملل، صلاحیت رسیدگی قضایی وفق مقررات حاکم بر حقوق کیفری بین‌المللی را در تقابل با نقض حاکمیت سایبری پیش‌بینی کرده و با رعایت ملاحظات حاکمیتی، به اِعمال صلاحیت تکمیلی اکتفا شده است. مذاکرات تالین در گام نخست با تبیین تجاوز سایبری به‌مثابهٔ نقضِ صلح و امنیت سایبری بین‌المللی و لزوم توجه به اصل منع مداخله در امور داخلی کشورها (حاکمیت ملی) صلاحیت به رسیدگی را به دیوان کیفری بین‌المللی توسعه و تسری داد. توسعهٔ صلاحیت نهاد موصوف منبعث از حقوق بین‌الملل عرفی در راستای سیاست جنایی بین‌المللی (مقابله با بی‌کیفرمانی) به‌منظور حفظ و اعادهٔ صلح و امنیت سایبری بین‌المللی صورت می‌گیرد.

کلیدواژگان

توسعهٔ صلاحیت، حاکمیت سایبری، دیوان کیفری بین‌المللی، سیاست جنایی بین‌المللی، صلاحیت سایبری.

---

۱. دانشجوی دکتری رشتهٔ حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. Email: alireza.mohaghegh.1400@ gmail.com

۲. استاد گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران (نویسندهٔ مسئول). Email: m-Ardebili@sbu.ac.ir

۳. استاد گروه حقوق بین‌الملل، دانشکدهٔ حقوق، دانشگاه شهید بهشتی، تهران، ایران. Email: Ebrahim_Beigzadeh@sbu.ac.ir

۴. دانشیار گروه حقوق جزا و جرم‌شناسی، دانشکدهٔ حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران. Email: ali@mahdavi.fr

تاریخ دریافت: ۱۴۰۰/۰۶/۰۸ - تاریخ پذیرش: ۱۴۰۱/۰۱/۲۸

مقدمه

حقوق بین‌المللی سایبری عام به مفهوم قواعد ناظر بر «حاکمیت» و «صلاحیت» اقدامات و فعالیت‌های سایبری با پیشرفت چگونگی زیستِ ملی و فراملی در محیط‌های مجازی سایبری، تعریف‌کنندهٔ روابط نوین سیاسی بین دولت‌ها و نیز روابط بین‌المللی خواهد شد و در همین زمینه تحولات سیاست جنایی بین‌المللی به معنای نظام قانونگذاری بین‌المللی در خصوص جنایات بین‌المللی در سطح بین‌الملل را به‌طور اجتناب‌ناپذیر ضروری خواهد کرد. با همین رویکرد شاهد ظهور قطعنامه‌های متعدد سازمان ملل متحد هستیم. قطعنامه‌هایی مانند قطعنامهٔ 45/121 مجمع عمومی سازمان ملل متحد در سال 1990 میلادی و نیز قطعنامه‌های239/57 و ۵۸/۱۹۹ و همچنین قطعنامهٔ ۶۰/۱۷۷ در سال ۲۰۰۵ میلادی و در حوزهٔ معاهدات بین‌المللی از همه بارزتر کنوانسیون مبارزه با جرائم سایبری بوداپست[1] در این زمینه می‌تواند گسترهٔ حاکمیت سایبری را نیز شامل دو مفهوم حاکمیت وستفالیایی و فراوستفالیایی سازد. تکیه بر فناوری‌های سایبری، یک موهبت (فرصت) و نیز فراهم‌آورندهٔ بروز ضرر و زیان به معنای ازکارافتادگی و معدوم کردن سیستم (تهدید) است.[2] فناوری سایبری هم موجب تقویت نوآوری در استفادهٔ فناوری‌های موجود در زندگی جوامع بشری (فرصت) می‌شود و هم به‌صورت فرایندهایی که سبب ظهور نقطه‌های راهبردی آسیب‌پذیر می‌شود، می‌تواند عامل خرابکاری، بروز حملات یا جرائم سایبری (تهدید) باشد. در سال ۲۰۰۷ چند مورد خدمات الکترونیکی خصوصی و عمومی استونی، مورد تهاجم عملیات سایبری خرابکارانه قرار گرفتند (Schmitt, 2017: 5) . حملات سایبری سبب قطع توزیع خدمات[3] در سطح ملی می‌شود که این قطع توزیع، به نقل از هوچشیلد[4] مغایر با اصل تفاوت‌گذاری[5] به مفهوم تفاوت میان حقوق و تکالیف اشخاص به تناسب نقش‌های ایفایی در سطح قلمرو حاکمیتی کشورها و مترادف با اصل انصاف[6] به مفهوم ایجاد تعادل و تناسب میان حق و تکلیف در نظام‌های اجتماعی از منظر راین (۱۹۸۱)[7] است (Hochshild, 1981: 51). سلاح سایبری به ویروس‌های رایانه‌ای گفته می‌شود که در چندین مرحله رمزگذاری شده و ساختار آنها به‌گونه‌ای طراحی شده است که آنتی‌ویروس‌های معمولی قادر به شناسایی و از بین بردن آن نیستند. همچنین برنامه‌ریزی آنها به‌گونه‌ای است که یک هدف خاص را مورد حمله قرار می‌دهند (پاپسا، ۱۳۹۵: ۲۰). امتناع از ارائهٔ تعریف دقیق از نوع سلاح در سطح بین‌الملل در قالب یک سند بین‌المللی و قطعنامه توسط سازمان ملل متحد که یک تکلیف بین‌المللی را موجب شود، وسیله‌ای

1. Convention on Cybercrim- Budapest, 23 November 2001.
2. Both a boon and a bane
3. Distributed Denial of Service
4. Hochshild
5. Differentiation
6. Fair play =Equity
7. Ryan

برای فرار از مسئولیت بین‌المللی در میان دولت‌هاست (Imburgia, 2010: 160)؛ اعمال حقوق بین‌المللی عام می‌تواند همچون سایر حوزه‌ها، به‌عنوان سنگ بنایِ صلح و امنیت عمل کند.[۱] تضمین حفظ صلح، امنیت و ثبات مسئولیت‌پذیری جامعهٔ بین‌المللی، خاصه صلح و امنیت سایبری، آن زمان محقق خواهد شد که با توجه به آخرین تحولات مزبور، قانونگذاری‌هایی در جهت ایجاد مسئولیت کیفری فردی و توسعهٔ صلاحیت تکمیلی رسیدگی در دیوان کیفری بین‌المللی در چارچوب قواعد حقوق بین‌المللی و مستنبط از کنوانسیون‌های چهارگانهٔ ۱۹۴۹ و نیز پروتکل‌های الحاقی آن بر پایهٔ اصل جنایت تلقی کردن اقدامات صورت‌گرفته[۲] می‌تواند انجام گیرد. التفات به قواعد به‌کارگیری صلاحیت دیوان کیفری بین‌المللی و تأثیرگذاری آن در مواجهه با موارد نقض صلح و امنیت سایبریِ بین‌المللی و نحوهٔ رسیدگی آن مبحث حاکمیت قواعد و مقررات حقوق بین‌المللی سایبری عام و موارد نقض آن را انکارناپذیر می‌سازد. بدیهی است در رویهٔ دولتی کشورها، زمینهٔ فعالیت‌ها و اقدامات سایبری عمدتاً طبقه‌بندی‌شده (Schm itt, 2017: 3) و اظهارات معطوف به باور حقوقی[۳] کمیاب‌اند، لیکن این کمبود بدان‌معنا نیست که عملیات سایبری در خلأ هنجاری قرار دارد (Schm itt, 2017: 3). در مذاکرات «تالین» ۲۰۱۷[۴] وظیفهٔ کارگروه بین‌المللی کارشناسان منتخب، تعیین چگونگی اعمال چنین حقوقی در بافت سایبری و شناسایی ابعاد منحصر به فضای آن بود. قواعد مطروحه در این خصوص، بازتاب حقوق بین‌الملل عرفیِ اعمالی در فضای سایبری است (Schm itt, 2017: 3) و قواعد مزبور مادامی‌که به‌درستی مبین حقوق بین‌المللِ عرفی باشند، تمامی دولت‌ها را ملتزم می‌سازند.

در مقالهٔ حاضر به بررسی این موضوع خواهیم پرداخت که آیا حقوق بین‌المللی سایبری عام، با توجه به وجود دو حوزهٔ حاکمیت و صلاحیت سایبری و وجود ماهیت و حقیقت دیوان کیفری بین‌المللی در فضای سایبری قابل تحقق و تحصیل هستند یا خیر؟ در این پژوهش در قسمت اول به تبیین حاکمیت سایبری و نقض و مصادیق آن، در قسمت دوم ببه صلاحیت سایبری و انواع حقوقی و حاکمیتی آن و نیز اِعمال صلاحیت (اصل اثربخشی و آثار آن) و در قسمت سوم به سیاست جنایی بین‌المللی با دامنهٔ تغییرات موسع (تحلیل ساختاری) موجود و رِئال، همچنین با دامنهٔ تحولات مضیق (جرم‌انگارانه) مطلوب و ایده‌آل، خواهیم پرداخت.

---

۱. دامنهٔ اصلی این حوزه را می‌توان در دو موضوع قابل توصیف دانست: حقوق بر جنگ (حقوق توسل به زور Jus ad bellum) و حقوق در جنگ (حقوق بشردوستانه و یا حقوق مخاصمات مسلحانه Jus in bello).

2. Criminalisation

3. Opinio Juris

۴. دستورالعمل تالین در حقوق بین‌الملل قابل اعمال در نبردهای سایبری متعلق به بازهٔ زمانی سال‌های ۲۰۱۳ تا ۲۰۱۷ میلادی در شهر تالین در کشور استونی است که توسط مایکل اشمیت استاد حقوق بین‌الملل پیرامون مقررات حاکم بر اقدامات و عملیات سایبری با همکاری یک گروه پژوهشگر و به سفارش مرکز عالی دفاع مشترک سایبری و با راهبردی ناتو (پیمان آتلانتیک شمالی) در ولزِ بریتانیا، در قالب اصل ۴ پیمان ناتو، تهیه شده است.

حاکمیت سایبری

۱. تبیین حاکمیت سایبری

واژهٔ سایبر از لغت یونانی «کی بِر نتز»[1] به معنای سکان‌دار گرفته شده است و واژهٔ «سایبرنتیک» توسط ریاضی‌دانی به نام نوربرت وینر در سال ۱۹۴۸ استفاده شد و معنای آن «کنترل رفتارها» به‌منظور «هدایت» بود (سعیدی، ۱۳۹۷: ۱۹). همچنین از این واژه به معنا و مفهوم مطالعهٔ پیام‌ها، به‌ویژه بررسی کنترل مؤثر در قلمرو فیزیولوژیک و مهندسی یاد می‌شود (امیرپور، ۱۳۹۳: ۴۲۶).

حاکمیت، اصلی بنیادین در حقوق بین‌الملل است و محافظت از نظام بین‌المللی موجود در چارچوب تعبیر و تفسیر مدرنِ حاکمیت مفهوم پیدا می‌کند. ریشهٔ لاتین آن معانی خودفرمانی، قدرت مافوق یا قدرت غالب[2] را دارد، و در صورت اعمال این واژه در حقوق بین‌الملل نوین بر قدرت مافوق دولت دلالت دارد. حاکمیت باید به شکل منطقی توسط صاحبان واقعی و برگزیدگان ملت اعمال شود. این واقعهٔ سیاسی به مفهومی واحد و تجزیه‌ناپذیر متکی بر ارادهٔ آحاد ملت است (لوئی، ۱۳۹۳: ۲۳). با توجه به قاعدهٔ اول دستورالعمل تالین در خصوص حاکمیت، ابعاد گوناگون فضای سایبری و عملیات سایبری، فراتر از محدودهٔ اصل حاکمیت نیستند.[3]

به‌طور خاص، دولت‌ها در هرگونه زیرساخت سایبری مستقر در سرزمین خویش و فعالیت‌های مربوط به آن از حاکمیت به مفهوم استقلال برخوردارند. زیرساخت‌های سایبری در محلی دیگر استقرار دارند، لیکن دولت سرزمینی به‌صورت بالفعل یا دوفاکتو[4] یا به‌صورت قانونی یا دو یوره[5] بر آن کنترل انحصاری دارد (آهنی امینه، ۱۳۹۷: ۷۳). اگرچه اصل صلاحیت سرزمینی در درون اصل حاکمیت نهفته است، دولت‌ها می‌توانند امتیازهای حاکمیتی مانند صلاحیت را در زیرساخت‌ها و فعالیت‌های سایبری فراسوی مرزها و نیز اشخاص درگیر در آن فعالیت‌ها اعمال کنند (قواعد ۱۰ و ۱۱ مذاکرات تالین). شماری از اصول و قواعد حقوق بین‌الملل عرفی که منبعث از اصل حاکمیت‌اند عبارت‌اند از: اصول و قواعد صلاحیت (قاعدهٔ ۳ مذاکرات تالین) و تعهد به احترام به مصونیت‌های خاص دیگر دولت‌ها (قاعدهٔ ۵ مذاکرات تالین) و نیز اصل مساعی مقتضی[6] به معنا و مفهوم ممانعت کردن کشور متعرض از تجاوز به قلمرو کشور ثالث (قاعدهٔ ۶ مذاکرات تالین) که علاوه‌بر آن دیوان دادگستری بین‌المللی نیز ابراز می‌دارد: «اصل احترام به حاکمیت دولت‌ها، با اصل ممنوعیت استفاده از زور[7]

---

1. kybernet
2. Superanusorpor Potestas- Esse Suae Potestatis – Sui Juris
3. UN.GGE2015 Report.Paras 27&28(b)
4. De facto
5. De jure
6. Due Diligence
7. Unlawful use of force

منطبق با قاعدهٔ ۶۶ دستورالعمل و نیز عدم مداخله[1] وفق قاعدهٔ ۶۶ دستورالعمل و همچنین حملات مسلحانهٔ مستنبط از قاعدهٔ ۷۱ سند اخیر، پیوندی تنگاتنگ دارد» (Nicarague judgement Para 212 ;Schm itt, 2017: 12). حقوق عرفی یا معاهداتی می‌تواند اِعمال حقوق حاکمیتی دولت سرزمینی را محدود سازد. فعالیت‌های غیردولتی سایر دولت‌ها، ارکان دولت‌های دیگر، کارکنان دیپلماسی و کنسولی برخوردار از مصونیت و تعرض‌ناپذیری حاکمیتی[2]، وفق قاعدهٔ ۵ دستورالعمل تالین، نمی‌توانند اعمال صلاحیت یا اقتدار کنند. با وجود نظریات موافق و مخالف حاکمیت دولتی بر داده‌هایی که ورای مرزها نگهداری می‌شوند، مبنی بر استقلال از حاکمیت دولت بر زیرساخت‌های سایبری مزبور یا عدم استقلال آنها و تحت حاکمیت قرار داشتنشان، دولت وفق قاعدهٔ ۱۰ دستورالعمل تالین، می‌تواند در شرایط معین بر داده‌های موجود در خارج از قلمرو خود مبادرت به اِعمال «صلاحیت تجویزی»[3] کند. حاکمیت خارجی از برابری حاکمیتی کشورها نشأت می‌گیرد و دولت‌ها از نظر حقوقی مطابق با مادهٔ (۱) ۲ منشور ملل متحد با هم برابرند. هر دولتی مکلف است به شخصیت، یکپارچگی سرزمینی و استقلال سیاسی سایر دولت‌ها احترام بگذارد و با حسن‌نیت[4] به تعهدات بین‌المللی خویش وفادار باشد (Nicarague judgement- Para 202; Schm itt, 2017: 14).

۲. نقض حاکمیت سایبری

با امعان نظر به صراحت قاعدهٔ ۴ دستورالعمل تالین در خصوص نقض حاکمیت، یک دولت نباید به انجام عملیات سایبری ناقض حاکمیت دولت دیگر مبادرت ورزد. آن دسته از عملیات سایبری که از اعمال امتیازات حاکمیتی دولت دیگر ممانعت به‌عمل می‌آورند یا آنها را نادیده می‌گیرند، نقض‌کنندهٔ حاکمیت بوده و از منظر حقوق بین‌الملل ممنوع هستند. البته وفق قوانین حاکم در حقوق کیفری بین‌المللی دارای مسئولیت کیفری بین‌المللی است که این مهم مشمول اقدامات بازیگران غیردولتی نمی‌شود. در مقام استثنا آنکه مطابق قواعد ۱۵ و ۱۷ دستورالعمل تالین، اقدامات مزبور قابل انتساب به یک دولت باشند که در آن صورت نقض اصل حاکمیت در خصوص زیرساخت‌های سایبری دولتی و غیردولتی یا خصوصی را که در قلمرو دولتی استقرار دارد، مشمول می‌شود. همچنین نسبت به اِعمال غیرتوافقیِ[5] صلاحیت اجرایی در قلمرو دولتی دیگر، نقض حاکمیت آن دولت به‌شمار می‌رود.

ماهیت دقیق حقوقی و مبنای اصلی در احتساب نقض حاکمیت بر دو مبنا ارزیابی می‌شود: الف) میزان تخطی از یکپارچگی سرزمینی دولت هدف، ب) وجود یا عدم مداخله در کنترل کارکردهای ذاتاً دولتی. در مورد نخست مبتنی بر کنترل دسترسی به قلمرو حاکمیتی خویش و

1. Prohibited Intervention
3. Sovereignty immunity and inviolability
4. Prescriptive Jurisdiction
5. Bona Fide
6. Non- Consensual

در مورد دومی بر حق حاکمیتی دولتی در اِعمال کارکردهای دولتی بدون دخالت هیچ دولت دیگر در قلمرو خود ابتنا دارد. کارشناسان کارگروه حقوق بین‌الملل مذاکرات تالین در مورد اولی در سه سطح خسارت فیزیکی، فقدان عاملیت[1] به مفهوم مباشرت یا حسب مورد مشارکت مادی (غیرمجازی- سایبری) و همچنین تعدی از یکپارچگی سرزمینی، ذیل آستانهٔ فقدان عاملیت (مباشرت یا در شرایط خاص، مشارکت مادی و غیرمجازی- سایبری) قرار می‌گیرد. در مورد دوم، موارد مطروحه در قالب «منع مداخله» در نقض حاکمیت سایبری ممنوعیت می‌یابد. کارگروه اخیرالذکر، در ارزیابی ماهیت ذاتاً دولتی فعالیت‌های سایبری، مفهوم اَعمال حاکمیتی[2] را در سیاق مصونیت دولت‌ها به‌کار برده است که می‌تواند در این زمینه راهگشا باشد. حوزه‌های عملی و اجرایی این مفاهیم در سطح بین‌المللی، توجه به اقدامات پیشگیرانه و مقابلهٔ کشورها با این واقعیت است. در سال مالی ۲۰۱۷ مایکل راجرز فرمانده [3] سایبری ایالات متحده بودجه‌ای معادل ۵۰۶ میلیون دلار (حدود ۱۵۰ هزار میلیارد ریال) برای راهبرد مقاصد سایبری در کمیتهٔ فرعی نیروهای مسلح مجلس نمایندگان آمریکا تقاضا کرد (جلالی، ۱۳۹۵: ۲۰).

جرائم سایبری

فضای سایبری به طرق مختلف با عناوین «قلمرو جهانی»[4] یا «قلمرو پنجم»[5] که فاقد جسمانیت بوده و واجد ماهیتی مجازی است، توصیف شده است (Schmitt, 2017: 12). هرچند فعالیت‌های سایبری ممکن است چندین مرز را بپیمایند یا در آب‌های بین‌المللی یا فضای هوایی بین‌المللی ماورای جو وقوع یابند، لیکن مرتکبان این فعالیت‌ها و اقدامات سایبری در حقیقت افراد یا نهادهایی هستند که تحت «حاکمیت یک یا چند دولت» بوده‌اند (Schmitt, 2017: 14). به بیان بهتر جنایت واقع‌شده فاقد جنبهٔ خصوصی و غیردولتی و در نتیجه حکومتی و امری حاکمیتی است. رابطهٔ میان جرائم سایبری و حملات سایبری، رابطهٔ عموم و خصوص من وجه است (آهنی امینه، ۱۳۹۷: ۲۷). جرائم سایبری به اقداماتی اطلاق می‌شود که در سامانه‌ها و شبکه‌های رایانه‌ای، با دامنه‌های درگیری کم‌شدت از حیث تخریب‌های مادی و فیزیکی علیه اشخاص و اموال کشور مورد تجاوز سایبری قرار گرفته (هیبلزگری، ۱۳۸۹: ۶۹)، مخاطراتی ایجاد می‌کند که فرایند حاکم را مختل، تضعیف یا تخریب کنند و از انواع خاصی مانند بحران‌سازهای سایبری شامل ویروس‌ها، پالس‌های الکترومغناطیسی و بمب‌های منطقی (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۵: ۲۵۰)،

---

1. Loss of functionality
2. Acta Jure Imperii
3. U.S.Cyber Command
4. Global domain
5. Fifth domain

جاسوسی سایبری، هک سیاسی در قالب ظهور هکتیویسم بـه مفهـوم اسـتفادهٔ غیرقـانونی از ابزارهای سایبری برای رسیدن به مقاصد سیاسی برای اعمال نافرمانی مدنی (جلالـی، ۱۳۹۵: ۱۴)، سابوتاژها یا خرابکاری سایبری یا جرائم بیولوژیکی سایبری، فیشینگ و جعل سایبری و نیز جاسوسی سایبری با قصدهای کاملاً متمایز نظیر منافع نظامی، صـنعتی، سیاسـی و فنـی تشکیل می‌شود (Dashora, 2011: 251). ویژگی اختلال، تخریب گسـترده و ممانعـت‌کننـدهٔ کارکردهای سیستم عمومی از شاخصه‌های بارز این جـرائم اسـت (Kesan & Hayes, 2012: 445). سرقت و ربایش‌های سایبری که در کمتر از یک میلیاردم ثانیـه از قـاره‌ای نسـبت بـه سرمایه‌های بانکی رخ می‌دهد (Hanagan, 2000: 83) و جنایت واقـع‌شـده در عرصـهٔ سـایبر ماهیت دولتی و حکومتی دارد. اگرچه توسـط بـازیگران غیردولتـی صـورت گیـرد، امـا دارای قابلیت انتساب به دولت متبوع خواهد بود و به لحاظ تشخیص دشوارِ مرتکب، جرائم سایبری را «جرائم کور» می‌نامند (Miller, 2014: 227-229). جرائم سایبری را باید واقعیت ملموس و مشهودی دانست و به‌علت همه‌گیری زمینه‌ها و بسـترهای جـرم‌زا در دهکـدهٔ جهـانی مـا بـا اپیدمی و جهانی شدن بزهکاری و جنایت بین‌المللی روبه‌رو هستیم. بنابراین موفقیت سیاست جنایی جامعهٔ ملل در کنترل و مهار جنایات بین‌المللی سایبری بود که خود مستلزم مطالعـه و شناسایی عوامل و مؤلفه‌های مشابه بسترساز جنایت است (ترنس دی، ۱۳۹۲: ۱۵). جـرائم موصوف در زمرهٔ جرائم فرصت‌مدار برای مرتکب از حیث عدم دستگیری و امکان فرار و رهایی از دست نهاد تعقیب در سطح ملی و بین‌المللی بوده و در صورت ارتکاب، مرتکـب بـا حـداقل ریسک همراه است (kesan, 2012: 454). این جرائم در زمان انتشار و ارتکاب، دارای آسیب و بروز ضرررسانی اولیهٔ اجتماعی سریع، در اذهان مردم داخـل قلمـرو سـرزمینی و نیـز ایجـاد آسیب‌های فضای فیزیکی و کارکردی ثانویهٔ کُند، نسبت به تجهیزات و زیرساخت‌های موجود در قلمرو حاکمیتی کشور مورد تعرض واقع‌شده هستند (عاملی، ۱۳۹۰: ۴۴). در گونه‌شناسی کلینارد[1] و کوئینی[2] در سال ۱۹۷۳ از پنج زمینهٔ در حال توسعه و طبقه‌بنـدی سیسـتم‌هـای رفتاری بزهکار و نه سیستم رفتاری آنها، جرائم سـایبری جـزء رفتارهـای مجرمانـهٔ عرفـی – سیاسی تلقی شده است و از دیدگاه آلبانس در سال ۱۹۹۵، جرائم سایبری را باید جزء جرائم قاعده‌مند، شغلی (Dashora , 2011: 311) و به‌تبع دولتی و حکومتی دانست.

۱. جنایت تجاوز

جنایات بین‌المللی مصرح در پیش‌نویس اساسنامهٔ رُم بـا دو منشـأ «عرفـی» منبعـث از حقـوق بین‌المللی عرفی که به‌صورت «حکمـی» نظیـر جنایـت تجـاوز، جنایـت بـین‌المللـی محسـوب

1. Clinard
2. Quinney

می‌شود و نیز «قراردادی» که با خاستگاه معاهدات بین‌المللی، نظیر تروریسم یا جنایت علیه کارکنان سازمان ملل متحد پا به عرصهٔ وجود می‌گذارند، البته با همت و تلاش کشورهای عضو عدم تعهد، جنایت تجاوز را مشمول جنایات بین‌المللی عرفی قرار داد (آل‌حبیب و بیگ‌زاده، ۱۳۸۲: ۳۶). جنایات بین‌المللی در اثر تخطی یا ناهماهنگی میان ارزش‌های ثبوتی (ارزش‌هایی که به اثبات نیاز ندارند و در زمان[1] و مکان ثابت‌اند، مانند قواعد آمره[2]) و ارزش‌های اثباتی (ارزش‌هایی مانند صلح و امنیت که مطلق، تغییرناپذیر و نیازمند اثبات‌اند) که موجِد قواعد بنیادین نظم عمومی بین‌المللی هستند، می‌شوند و اَعلی مِثال این قواعد در بروز صلح و امنیت خواهد بود (آل‌حبیب و بیگ‌زاده، ۱۳۸۲: ۶۲). در سال ۱۹۳۳ در اَروشای اوگاندا برای تشکیل دولت همراه با تقسیم قدرت، با درخواست رادیویی از هوتوهای روآندایی، نسل‌کشی توتسی‌های بینوا را درخواست کردند که شاید بتوان از آن به‌عنوان اولین جنایت نسل‌کشی و نیز جنایت علیه صلح و امنیت یاد کرد (جَرد دایموند، ۱۴۰۰: ۳۹۱)، اما رسیدگی به جنایت علیه صلح و امنیت در قالب جنایت تجاوز، دستخوش دوری از عدالت کیفری و گریبانگیرِ روابط، تعاملات، مقاصد و مطامع سیاسی طیِ طریق کرد (Clark, 2010: 663)، این در حالی است که جامعهٔ بین‌الملل اقدامات موصوف را مستند به بند ۱ قطعنامهٔ ۲۶۲۵ مجمع عمومی جنگ متجاوزانه را جنایت علیه صلح و مستوجب مسئولیت کیفری بین‌المللی می‌داند (آل حبیب و میرزایی ینگجه، ۱۳۸۲: ۲۶۳). در خصوص رسیدگی به جنایت علیه صلح و امنیت بین‌المللی، با موسع نمودنِ مسئولیت کیفری، فردی که مرتکب تخلف به‌اندازهٔ جدی از قاعدهٔ ممنوعیت مندرج در مادهٔ (۴) ۲ منشور ملل متحد است، در دادگاه‌های کیفری موقت و موردی مانند یوگسلاوی و رواندا، با تبیین و توضیح انجام عمل تجاوزکارانه در قالب طرح یا توطئهٔ مشترک محاکمه می‌شود (Kai Am bos, 2010: 51) و درصورتی‌که عمل ارتکابی با قهر و غلبه توأم باشد، مطابق با بند ۴ مادهٔ ۲ منشور سازمان ملل نیز مشمول قاعدهٔ ممنوعیت توسل به زور غیرقانونی خارج از استثنائات قابل اعمال است. این ماده مطابق با مواد ۳۹ و ۵۱ منشور یا با تجویز شورای امنیت یا به‌عنوان دفاع مشروع انفرادی یا جمعی (سودمندی، ۱۳۹۴: ۳۵) که به‌وسیلهٔ قطعنامهٔ ۱۴ دسامبر ۱۹۷۴ مجمع عمومی تبیین شد، و موارد اعلامی وفق بند ۴ مادهٔ ۳ قطعنامهٔ مذکور می‌تواند در قالب تعریف تجاوز، گنجانده شود و در این باره قول و بیان مخالفی وجود ندارد و همگی بر آن متفق‌القول‌اند (Carsten Stahn & Goran Sluiter, 2010: 713) این واقعه اساسنامهٔ رم، تصویبی سال ۱۹۹۸ میلادی را نیز شامل می‌شود که در سال ۲۰۱۰ در کامپالا در روزهای ۳۱ می تا ۱۱ ژوئن به بازنگری تعریف جنایت تجاوز در قالب قطعنامهٔ ۶. RC / Res از طریق کنسانسوس (وفاق عام) تحت عنوان مادهٔ ۸ مکرر به

1. Intemporel
2. Jus Cogens

اساسنامه اضافه کرد (رضایی‌نژاد، ۱۳۹۸: ۱۲۸) و با صلاحیت انحصاری رسیدگی به جنایت بین‌المللی تجاوز، با قابلیت انتساب به افراد تعریف شد. با وجود تصریح فصل هفتم منشور سازمان ملل که شورای امنیت وظیفهٔ حفظ و برقراری صلح و امنیت بین‌المللی و جلوگیری از جنایت تجاوز و احراز آن را دارد، اعضای دائم آن هیچ‌گاه تمایلی به اعطای صلاحیت به دیوان کیفری بین‌المللی ندارند (شریعت باقری، ۱۳۹۷: ۲۸-۲۷)، در مقابل کشورهای مستعمره یا تازه استقلال‌یافته همواره بر اعطای صلاحیت در خصوص رسیدگی به واقعهٔ حقوقی جنایت بین‌المللی تجاوز اصرار و تأکید دارند (Benjam in N. Schiff, 2008: 74)، البته این اصل که به‌منظور تثبیت ارادهٔ جامعهٔ بین‌المللی وفق مادهٔ ۵ اساسنامهٔ رم و بر مبنای صلاحیت رسیدگی موصوف بود، بارها به تعویق افتاد (Nadya Sada, 2013: 41). با تأکید بر این رویکرد، مجمع عمومی سازمان ملل به‌وسیلهٔ قطعنامهٔ ۳۳۱۴ سال ۱۹۷۴ میلادی مبادرت به تعریف جنایت تجاوز تحت عنوان «جدی‌ترین و خطرناک‌ترین شکل استفادهٔ غیرقانونی از زور» کرد (سودمندی، ۱۳۹۴: ۵۵) و در سال ۲۰۱۰ در کنفرانس کامپالا در این زمینه در قالب بند ۱ مادهٔ ۸ مکرر اساسنامهٔ رم، به صدور اصلاحیه مبادرت ورزید و جنایت تجاوز را به‌واسطهٔ ماهیت، شدت و گسترهٔ عمل آن تعریف کرد و در بند ۲ مادهٔ ۸ مکرر عمل تجاوزکارانه را با تکمیل عبارت «به هر روش دیگری با منشور ملل متحد در تعارض باشد» بیان کرد. توجه به نقطهٔ عطف بودن کنفرانس بازنگری کامپالا در سال ۲۰۱۷ مبنی بر توسعهٔ صلاحیت دیوان کیفری بین‌المللی در رسیدگی به جنایت تجاوز برای کشورهای عضو و عدم توسعهٔ صلاحیت مرجع اخیرالذکر برای کشورهای غیرعضو در امر موصوف در بازهٔ زمانی ماقبل سال ۲۰۱۷، ضروری خواهد بود (Murphy, 2015: 17). قطعنامهٔ ۳۳۱۴ سال ۱۹۷۴ مجمع عمومی پایه و اساس اقدامات فرماندهان و هدایت‌کنندگان و مبنای تعریف جنایت تجاوز است (Ophardt, 2010: 13). این قطعنامه با امعان نظر به بند ۲ مادهٔ ۸ مکرر اساسنامهٔ رم تجاوزات سایبری در دیوان کیفری بین‌المللی قابلیت پذیرش دارد. همچنین باید توجه داشت که مستنبط از مادهٔ ۵۱ منشور ملل متحد نوع سلاح در تجاوزات مسلحانه بی‌تأثیر و غیرمؤثر خواهد بود.

۲. آستانه در تجاوز سایبری

صرف‌نظر از اینکه در بادی امر، بیشتر کشورهای عضو خواستار «صلاحیت خودکار» برای دیوان کیفری بین‌المللی در رسیدگی به جنایت تجاوز بودند (آل‌حبیب و ارسنجانی، ۱۳۸۲: ۲۹۱)، لیکن در نهایت دیوان تصویب صریح اساسنامه با «صلاحیت تکمیلی» خویش را صالح به رسیدگی جنایات بین‌المللی اعلامی در اساسنامه می‌داند و برای قابلیت پذیرش دعوا، از

آستانهٔ شدت[1] در بند ۱ دال مادهٔ ۱۷ اساسنامهٔ دیوان یاد می‌کند (Pre-tril Cham ber , 2006: 21) و طرح مفهوم آستانهٔ شدت به‌طور خاص به سال ۱۹۹۲ برمی‌گردد (ذاکر حسین، ۱۳۹۹: ۱۹۱). در تعریف و جایگاه مفهوم آستانهٔ شدت باید گفت هر زمانی‌که وضعیت خاصی از سوی دولت‌ها، شورای امنیت یا به ابتکار دادستان دیوان کیفری بین‌المللی براساس مسئولیت محوله به او[2] شناسایی شود، دادستان مزبور باید مبنای معقولی را در امر تصمیم‌گیری در خصوص تعقیب نمودن یا عدم تعقیب اتخاذ تصمیم کند. مرحلهٔ اول براساس صلاحیت موضوعی، زمانی و شخصی به موضوع می‌پردازد؛ در این مرحله اقدام تحت عنوان قابلیت پذیرش از حیث صلاحیت تکمیلی[3] صورت می‌گیرد (کیتیچایساری، ۱۳۸۷: ۵۴). مرحلهٔ دوم از حیث داشتن شدت کافی یا آستانهٔ شدت براساس بند ۱ دال مادهٔ ۱۷ اساسنامه باید قابلیت پذیرش داشته باشد. معیارهای قابل پذیرش در آستانهٔ شدت الف) درجه و میزان جرم که در حال حاضر در خصوص جرائم سایبری و ارتکاب کمی آن انکارناپذیر است؛ ب) ماهیت جرم که در خصوص موضوع مزبور دارای وضعیت غیرسنتی و غیرعادی بوده و دارای ماهیت گستردگی در اضرار به غیر است و در حالت بین‌المللی آن می‌تواند در قالب ورود خسارات جبران‌ناپذیر متصور باشد؛ ج) شیوهٔ ارتکاب جرم که در خصوص مانحن‌فیه بدون حضور در جغرافیای جرم و در محیط امنیت عدم دستگیری مرتکب می‌تواند فرایند جرم ارتکابی را به‌طور کامل طی کند؛ د) تأثیر ارتکاب جرم که با وجود مضیق بودن رکن مادی جرائم موصوف به‌واسطهٔ گستردگی رکن معنوی و سوءنیت خاص قصد مجرمانه بسیار موسع (Schmitt, 2013: 47)، آستانهٔ تحقق جنایت تجاوز را می‌توان نقض جدی‌ترین قواعد حقوق بین‌الملل تلقی کرد. ظهور، تحقق و تعیین آستانهٔ تجاوز در مذاکرات تالین ۱ مستخرج از قانون ۱۳ را می‌توان در ارتکاب جرائم سایبری دانست که به آستانهٔ «حملهٔ مسلحانه» رسیده باشد. همچنین با توجه به تصویب کارگروه کارشناسی مطابق بند ۶ مادهٔ ۶۹ دستورالعمل تالین ۱ رسیدن به آستانهٔ «حملهٔ مسلحانه» را از مفهوم سنتی آن به فعالیت‌های مبتنی بر توسل به زور فعالان غیردولتی که تعرضاتشان می‌تواند به «تجاوز به حاکمیت کشور مجنی‌علیه تلقی شود» تسری و توسعه داد (Schmitt, 20013: 49). همچنین با عنایت و استنباط از وجود قاعدهٔ ۱۷ در دستورالعمل تالین ۲ در سال ۲۰۱۷ حقوق مسئولیت بین‌المللی، به‌صورت عینی، بر وجود وقایع، اعمال می‌شود. عملیات سایبری یک بازیگر غیردولتی، درصورتی‌که یک دولت به‌صورت واقعی بر آن رفتار خاص بازیگر غیردولتیِ ذی‌ربط «کنترل مؤثر» داشته باشد، به آن دولت قابل انتساب است. شدت عملیات سایبری هدایت‌شده علیه دولت مجنیٌ‌علیه، ملاحظه‌ای حائز اهمیت و مرتبط است و عملیات سایبری

1. Gravity threshold
2. Ex officio
3. Complementarity Jurisdiction

با سطح و آستانهٔ پایین که صرفاً موجب اختلال شود، به اثبات و مستندسازی نیاز دارد (Schmitt, 2017: 82-89). باید خاطرنشان کرد که در جنایت تجاوز به‌وقوع‌پیوسته، فرد مرتکب باید از اوضاع و احوال شرایط پیش‌آمده که به نقض آشکار صلح و امنیت بین‌المللی منجر شده است، علم و عمد داشته باشد که با این توضیح انتساب جزایی، منجز و مضیق خواهد بود. در مورد نقض صلح و امنیت سایبری که بروز آن به‌وسیلهٔ ارتکاب حملات یا جرائم سایبری رخ می‌دهد، مسئولیت کیفری فردی منحصر به فرماندهان با کنترل مؤثر تحت سیاست حاکمه و متخذه از سوی دولت متخاصم خواهد بود. مستند به مادهٔ ۹ مکرر اساسنامهٔ رم استقرار مسئولیت با صدور دستور حمله یا ارتکاب جرائم سایبری محقق می‌شود و اطلاعات و اِشراف فنی و تخصصی حاکم بر فناوری‌های سایبری ضرورت ندارد (Ambos, 2016: 503-504). البته براساس بند «ب» مادهٔ ۲۸ اساسنامهٔ رم نیز در جریان جنگ‌های سایبری، فرماندهان نظامی و غیرنظامی که دستور انجام عملیات سایبری را صادر می‌کنند، متهم به ارتکاب جنایت جنگی می‌شوند و مسئولیت کیفری فردی نیز بر آنها تحمیل می‌شود. با توجه به گسترش فضای سایبری در حوزهٔ عملیات و اقدامات بین‌المللی دولت‌ها و حکومت‌ها در مقام ورود اتهام به کشور متخاصم یا در مقام دفاع مشروع، استنباط‌های خود را تفسیر می‌کنند و گسترش می‌دهند (Dunlap Jr, 2011: 83). نقش مؤثر و انکارناپذیر بازیگران غیردولتی در مذاکرات تالین، خاصه در سال ۲۰۱۷ میلادی شناسایی تصریح شد. در قلمرو صلح و امنیت، صلح و امنیت بین‌المللی، در وضعیت فعلی عرصهٔ بین‌الملل در زمینهٔ چالش‌های معاصر در حقوق بین‌المللی کیفری و از منظر جمیع دولت‌های عضو و حتی غیرعضو دیوان کیفری بین‌المللی مغفول واقع شده است (Anderson, 2010: 421). در مواد ۶ تا ۸ دستورالعمل تالین، دولت‌ها را در نقض تعهدات بین‌المللی در اقدامات سایبری مسئول دانسته و همچنین این اقدامات را تعریف کرده است. با وجود این اقدامات سایبری از درون کشور را بدون کنترل مؤثر آن دولت از مقولهٔ مسئولیت مستثنا دانسته است (Schmitt, 2013: 40). قابلیت پذیرش دعوا در دیوان کیفری بین‌المللی را می‌توان اعمال صلاحیت تکمیلی بودن صلاحیت آن و تقدم دادگاه‌های ملی در رسیدگی به جنایاتی مانند تجاوز سایبری در اساسنامهٔ رم به‌صورت بالقوه دانست (Delmas-Marty, 2006: 3) و توجه به «مکانیزم ماشه» در راستای بیان توانمندی دادستان در خصوص دادرسی یک موضوع، به‌منظور اعمال صلاحیت در مقام «فعال‌سازی صلاحیت خفتهٔ دیوان کیفری بین‌المللی»[1] ضروری است (ذاکر حسین، ۱۳۹۹: ۸۲).

1. Activation of Dormant Jurisdiction in the International Criminal Court

صلاحیت سایبری

۱. صلاحیت‌های حقوقی

۱. ۱. صلاحیت تقنینی: اعمال صلاحیت توسط حکومت‌ها منبعث از حقوق بین‌الملل و ناشی از اصل برابری دولت‌ها و تبلور حاکمیت به معنای «حق انحصاری صلاحیت» است (Anthony Aust, 2010: 108). صلاحیت حقوقی در صلاحیت حوزهٔ تقنین، اجرا و امر قضا، ظهور پیدا می‌کند. گسترهٔ صلاحیت تقنینی در حاکمیت سایبری، منوط به تحدید اصول حاکم در حقوق بین‌الملل است و خود به دو بخش سیاست اجرایی (قانونگذاری غیرکیفری) و سیاست جنایی (قانونگذاری کیفری) تقسیم می‌شود، و در عرصهٔ بین‌المللی به معنای وضع قوانین و مقررات حاکم بر اشخاص، اموال و موقعیت‌هاست. در آن اصل بر «حق اعمال صلاحیت» است و عدم اعمال حق موصوف، نیاز به اثبات دارد.

۱. ۲. صلاحیت قضایی: استطاعت و لیاقتی را که قانونگذار به مراجع رسیدگی‌کننده در امور دعاوی مطروحه اعطا می‌کند، به صلاحیت قضایی تعریف می‌کنند، و در بادی امر صلاحیت تعیین صلاحیت، توسط مرجع رسیدگی‌کننده است که در صورت انکار ضرورت صدور قرار عدم صلاحیت انکارناپذیر است. توجه به اعمال صلاحیت قضایی و بروز صلاحیت ترافعی[1] و تشخیص و تعیین ارتباطات موضوع رسیدگی و محکمه در جرائم سایبری تحت عنوان ناشناخته بودنِ تابعی مرتکب ضروری است (شکیب‌نژاد، ۱۳۹۶: ۱۰۰-۹۷). اصول حاکم بر صلاحیت قضایی و کیفری، حدود و ثغور اقدامات در دامنهٔ این صلاحیت را تعیین می‌کند. از مهم‌ترین آنها می‌توان به الف) اصل سرزمینی[2] و تمرکز بر سرزمینی بودن جنایت، ب) اصل آثار و توابع[3] با عدم تمرکز سرزمینی بودن جنایت و توجه به تأثیر اساسی و مهم آن، ج) اصل حمایت[4] که علی‌رغم ارتکاب جنایت توسط بیگانه و خارج از قلمرو کشور است، به لحاظ اقدام علیه امنیت قابل پیگیرد است، د) اصل تبعی بودن شخصیت فردی[5] بر پایهٔ بزه‌دیده که از اتباع کشور است، اگرچه مرتکب جنایت اتباع بیگانه بوده است، اشاره کرد (آل‌حبیب و ابراهیمی، ۱۳۸۲: ۳۷۰).

۱. ۳. صلاحیت اجرایی: اختیار حاکمیت در اجرا و الزام اشخاص مسئول در مقررات وضع شده است که می‌تواند دارای ماهیت‌های قضایی (اجرای احکام و شکلی) یا اجرایی، اداری و غیرقضایی باشد. نمونهٔ بارز این صلاحیت را در راهنمای «دستورالعمل تالین در حقوق

---

1. Adijudicatory Jurisdiction
2. Territorial Principle
5. Effects Principle
4. Protective Principle
5. Passive Personality Principle

بین‌الملل قابل اعمال در نبردهای سایبری»[1] در شهر تالین در استونی می‌بینیم. این راهنما توسط مایکل اشمیت استاد حقوق بین‌الملل در خصوص مقررات حاکم بر اقدامات و عملیات سایبری است که توسط پژوهشگران مرکز عالی دفاع مشترک سایبری و به راهبردی ناتو (پیمان آتلانتیک شمالی) در ولزِ بریتانیا در قالب اصل ۴ پیمان ناتو، تهیه شده است. البته باید اذعان کرد که توانمندی‌ها و طرح‌های سایبری ناتو به لحاظ فقد ادلهٔ اثبات و عدم عنصرشناسی کافی و وافی، همچنین میسر نبودن انتساب جزایی در اقدامات و عملیات سایبری هنوز مراحل تکمیلی خود را سپری نکرده است (آهنی امینه، ۱۳۹۷: ۴۰).

۲. صلاحیت‌های حاکمیتی

۲. ۱. صلاحیت سرزمینی: ظهور و بروز این صلاحیت از منظر «تحقق رکن مادی جرم» که از آن به «صلاحیت سرزمینی ذهنی» و نیز «مکان تحقق حصول نتیجهٔ جرم» که نوعاً می‌تواند از مکان بروز رکن مادی جرم متفاوت باشد و دو جزء فعل مجرمانه و نتیجهٔ مجرمانه، دارای قلمرو و حاکمیت مستقل باشند و از آن به «صلاحیت سرزمینی عینی» یاد می‌شود، بررسی می‌شود. شناسایی محل حضور کاربر، به لحاظ مکان به فعلیت رسیدن قصد مجرمانه در ارتکاب سایبری، قابل اتکاترین وضعیت اِعمال صلاحیت سرزمینی است (Xingan, 2004: 32). صلاحیت موصوف در فضای سایبری، در قالب سه دستهٔ مکان سِرور، مکان حضور کاربر و مکان ارائه‌دهندهٔ خدمات اینترنت ISP مطرح می‌شود (شکیب‌نژاد، ۱۳۹۶: ۱۱۵).[2]

۲. ۲. صلاحیت شخصی: هنگامی‌که اِعمال صلاحیت دادگاه بر پایهٔ تابعیت مرتکب و مجنی‌علیه قرار گیرد، این نوع صلاحیت موضوعیت پیدا می‌کند (رضایی‌نژاد، ۱۳۹۸: ۵۵). مسئولیت کیفری فردی هم منبعث و مؤید همین صلاحیت است که صرف‌نظر از هر موقعیت سیاسی و اجتماعی مرتکب، تحت عنوان صلاحیت شخصی یا موردی (میر محمدصادقی، ۱۳۹۵: ۵۶) باید پاسخگوی اقدامات خویش باشد. صلاحیت مبتنی بر تابعیت با دو وضعیت فعال یا مرتکب‌محور و نیز منفعل یا مجنی‌علیه‌محور، در دادگاه منشأ اثر می‌گردد (میرمحمدصادقی، ۱۳۹۵: ۶۵-۵۹).

۲. ۳. صلاحیت واقعی: با وجود صلاحیت سرزمینی و جرم‌انگاری در محل ارتکاب جرائم سایبری، حکومت‌ها دارای «حق اعمال صلاحیت»[3] برای تبعهٔ خارجی مرتکب اخلال در امنیتِ خارج از قلمرو خویش هستند که این امر صرف‌نظر از عدم جرم‌انگاری کشور

---

1. Tallinn manuul on International Law applicable to Cyber Warfares.

۲. در نظام Comman Law اصالت با صلاحیت سرزمینی و در نظام Roman-German اصالت با صلاحیت شخصی است.

3. The right Exercise of Jurisdiction = Exercise of competence.

محل ارتکاب جرم مزبور خواهد بود. جرائم ارتکابی در محیط سایبری به لحاظ نبود عناصر مادی و خارجی، موجبات گسترش تمایل کشورها در مورد شمول قرار دادن اقدامات سایبری، تحت عنوان صلاحیت واقعی را فراهم آورده است (Colangelo, 2005: 540). این صلاحیت به لحاظ تفوق و برتری بر اصالت دادن به حاکمیت کشور موصوف به صلاحیت حمایتی نیز معروف است (Inazumi, 2005: 25).

۲. ۴. صلاحیت جهانی: وجود جرائم علیه جامعهٔ بین‌الملل[1] و مجوز اعطایی از سوی حقوق بین‌الملل عرفی موجب شده تا صرف‌نظر از تابعیت مرتکبان و مجنی‌علیهم ناشی از ارتکاب این جرائم، صلاحیت جهانی پا به عرصهٔ وجود نهاده و با این تأسیس، موجبات جلوگیری از نقض امنیت و صلح بین‌المللی فراهم شده باشد (Schabas, 2011: 340) با همین رویکرد است که می‌توان برای دیوان کیفری بین‌المللی در رسیدگی به معاونت در جنایات بین‌المللی که از طریق اقدامات سایبری توسط کاربران صورت گرفته است، «صلاحیت عام در صلاحیت جهانی» را منظور کنیم. صلاحیت جهانی از دو منظر الف) اعمال صلاحیت جهانی به‌صورت الزامی یا اختیاری و ب) اعمال صلاحیت اصحاب دعوا به‌صورت اقدام از سوی دولت محل حضور متهم یا به‌صورت اقدام از سوی درخواست‌کنندهٔ استرداد، دارای محملِ قانونی و ماهیتِ حقوقی است. در خصوص اِعمال صلاحیت جهانی و وجود چهار نوع صلاحیت جهانی اولیهٔ الزامی و اختیاری و نیز صلاحیت ثانویهٔ الزامی و اختیاری با دو اثر حقوقی اِعمال صلاحیت جهانی نسبی دولت اقدام‌کننده و ضرورت شناسایی مطلق نسبت به سایر دولت‌ها یاد کرد و از میان انواع صلاحیت جهانی، دیوان کیفری بین‌المللی، «صلاحیتِ جهانی ثانویهٔ اختیاری»[2] به مفهوم اختیار اعمال صلاحیت از سوی دولت درخواست‌کننده استرداد را به خود اختصاص داده است (حکیمی‌ها، ۱۳۹۵: ۲۱-۱۹).

۲. ۵. صلاحیت تجویزی: ماهیت صلاحیت ممکن است سرزمینی[3] (قاعدهٔ ۹ دستورالعمل) یا فراسرزمینی[4] (قاعدهٔ ۱۰ دستورالعمل) باشد. دامنهٔ قابلیت اعمال صلاحیت سرزمینی بر فعالیت‌های سایبری و اشخاص دخیل در آنها از صلاحیت مبتنی بر اصل سرزمینی متمایز است. از جمله به‌نوعی صلاحیت اعمالی یعنی ماهیت تجویزی، اجرایی و قضایی صلاحیت ذی‌ربط بستگی دارد. صلاحیت تجویزی بر اشخاص دخیل در فعالیت‌های سایبری در فراسوی مرزها، زیرساخت سایبری مستقر در خارج از کشور یا عمل مرتبط با فضای سایبری که در خارج از قلمرو یک دولت وقوع می‌یابد. وجود مبانی گوناگون برای صلاحیت تجویزی می‌تواند به صلاحیت همزمان دو یا چند کشور بر فعالیت سایبری واحد

1. Delicta Juris Gentium
2. Optional secondary universal jurisdiction.
3. Territorial
4. Extraterritorial

بینجامد. صلاحیت سرزمینی ذهنی[1] مطابق بند «ب» قاعدهٔ ۹ دستورالعمل با تأکید بر فعالیت‌های سایبری ملی و نیز صلاحیت سرزمینی عینی[2] با اشعار بر فعالیت‌های سایبری فراملی از مشتقات صلاحیت سرزمینی است و نوع اولی آن تحت صلاحیت تام (تجویزی، اجرایی و قضایی) دولت نخستین قرار دارد، بدین‌دلیل که از قلمرو آن دولت نشأت گرفته است (Schmitt, 2017: 52-54). بدیهی است که در خصوص صلاحیت فراسرزمینی مستخرج از قاعدهٔ ۱۰ دستورالعمل، نوع صلاحیت تجویزی فراسرزمینی خواهد بود که می‌تواند نسبت به اتباع کشور، یا تجهیزات دارای تابعیت آن کشور و همچنین نسبت به اتباع خارجی به‌منظور تضعیف کشور مزبور و در نهایت براساس اصل صلاحیت جهانی موجب شکل‌گیری «جنایت سایبری» به موجب حقوق بین‌الملل شده باشد.

۳. اِعمال صلاحیت

۳. ۱. اصل اثربخشی: دیوان کیفری بین‌المللی هم در خصوص دارا بودن صلاحیت و هم نسبت به قابل پذیرش بودن موضوع مطروحه وفق بند ۱ مادهٔ ۱۹ اساسنامه باید احراز حاصل کرده و تصمیم‌گیری کند. لیکن با توجه به بند «ج» قاعدهٔ ۹ دستورالعمل تالین بیان‌کنندهٔ دکترینِ فعالیت سایبری دارای اثرگذاری اساسی در قلمرو خود است. براساس این اصل، اعمال صلاحیت بر یک جنایت، مستلزم وقوع عنصر سازندهٔ آن جنایت در قلمرو دولت یا برخی دیگر از پیوندهای سرزمینی است (Libman V. 1985: para74)، با این حال اصل موصوف، البته منوط به شماری شروط برای حفاظت در مقابل توسعهٔ نامحدود آن، به‌صورت فرایندهای مورد پذیرش قرار می‌گیرد و تمام کارشناسان کارگروه بین‌المللی بر اینکه این اصل، بازتاب حقوق بین‌الملل عرفی سایبری است، متفق‌القول بودند. اصل مزبور در عرصهٔ سایبری اهمیت خاصی دارد و علاوه‌بر یک عملیات سایبری واحد می‌تواند موجب بروز آثاری در کشورهای متعدد شود. در چنین مواردی، آستانهٔ اِعمال بی‌قیدوشرط صلاحیت، تا اندازه‌ای فراتر از مصادیق مطرح در شِق الف (زیرساخت سایبری و اشخاص در فعالیت‌های سایبری) و همچنین شِق ب (فعالیت‌های سایبری نشأت‌گرفته یا تکمیل‌شده در قلمرو خویش) است. اگر دولتی در زمینهٔ فعالیت‌های سایبری با فضای سایبر و اشخاص دخیل در آن مبادرت به اِعمال صلاحیتِ مبتنی بر آثار کند، باید این عمل را به شیوه‌ای معقول و با توجه مقتضی به منافع دیگر دولت‌ها صورت دهد. شرایط به رسمیت شناخته‌شده در این زمینه از این قرارند: دولتی که مبادرت به تصویب قوانین مبتنی بر آثار می‌کند، منفعت و علقه‌ای

1. Subjective Territorial Jurisdiction
2. objective Territorial juridiction

واضح و از نظر بین‌المللی پذیرفته‌شده در این عمل داشته باشد؛ آثاری که دولت مترصد تنظیم آنهاست باید به اندازهٔ کافی، مستقیم و قصدشده[1] یا پیش‌بینی‌پذیر[2] باشند. آن آثار باید به اندازهٔ کافی برای تعمیم قانون دولت به اتباع خارجیِ خارج از قلمرو او و به همان اندازه اساسی باشند. در اساسنامهٔ رم وفق مادهٔ ۹ بررسی عناصر تشکیل‌دهندهٔ جنایت واقع‌شده صورت می‌گیرد. با استخراج اصول عمومی حقوق بین‌الملل، مستند به بند ۳ مادهٔ ۲۱ اساسنامهٔ رُم که نباید متناقض با حقوق بشر شناخته‌شده بین‌المللی باشد، باید قصد اصلی و صریح آن در تفسیر قلمرو صلاحیت، باید همواره با تحدید اختیارات دیوان همراه باشد. لیکن در مقام عمل به استناد فصل هفتم منشور ملل متحد و حسب نقض صلح و امنیت (سایبری) باید حیطهٔ صلاحیت رسیدگی دیوان کیفری بین‌المللی را توسعه داد (آل‌حبیب و ارسنجانی، ۱۳۸۲: ۲۹۷).

۳. ۲. آثار اثربخشی: اِعمال صلاحیت مبتنی بر آثار، به‌واسطهٔ نداشتن پیوندی معنادار یا دولتی که درصدد اِعمال چنین صلاحیتی (صلاحیت سرزمینی) است، موجب تعدی ناروا که در حقوق بین‌الملل از آن به جنایت یاد می‌شود، در منافع سایر دولت‌ها یا اتباع خارجی نشود (Akehurst, 2008: 221). در نتیجه، تصویب قانون بر مبنای دکترین اثرگذاری، در راستای حمایت از یک دولت در برابر آثار اساسی عملیات سایبری انجام‌گرفته در خارج از قلمرو او، و مادامی‌که منافع مشروع سایر دولت‌ها به‌گونه‌ای ناروا مورد تخطئه قرار نگیرد، مجاز خواهد بود (Schmitt, 2017: 64). اِعمال هر نوع صلاحیت، بر مبانی اصل صلاحیت سرزمینی مشروط به محدودیت‌های معینی است که در حقوق بین‌الملل در زمینهٔ اختیارات صلاحیتی مقرر شده‌اند؛ البته باید توجه کرد که مصونیت و تعرض‌ناپذیری حاکمیتی[3]، موضوع قاعدهٔ شمارهٔ ۵ دستورالعمل تالین و همچنین مصونیت دولت‌ها از اِعمال صلاحیت موضوع قاعدهٔ شمارهٔ ۱۲، از جمله محدودیت‌هایی است که به‌صورت عام‌الشمول شناسایی شده است.[4] مستنبط از قاعدهٔ ۸ دستورالعمل تالین، یک دولت با لحاظ محدودیت‌های مصرح در حقوق بین‌الملل می‌تواند به اِعمال صلاحیت سرزمینی و فراسرزمینی بر فعالیت‌های سایبری مبادرت ورزد. صلاحیت به اهلیت و اختیار دولت‌ها برای تنظیم و سامان بخشیدن به اشخاص، اشیا و رفتار وفق حقوق داخلی خود، در چارچوب محدودیت‌های تحمیلی توسط حقوق بین‌الملل دلالت دارد (The Draft Convention On Research in Internationnal Law of the Harvard Law Scool, 1935)[5]

---

1. Intended
2. Predictable
3. Immunnity of states from the exercise of jurisdiction
4. see: Qppenheim' International Law, at 458 – shaw's International Law , at 478
5. 29AM.J,int'1/435&466)andalso:Restatment Third, 1984,at19;Oppenheim's International Law ,at 465; shaw's International Law , at 469

سیاست جنایی بین‌المللی

جنایات بین‌المللی عرفی ریشه در حقوق بین‌الملل عرفی دارد و نیز جنایات بین‌المللی معاهده‌ای و قراردادی با انعقاد معاهدات بین‌المللی، پا به عرصهٔ بین‌المللی می‌گذارند (ریاحی، ۱۳۹۲: ۲۹). گسترش و ایجاد شبکه‌های جدید، بر پیچیدگی روش ارتکاب و تغییر نوع ارعاب و اخلال در نظم بین‌المللی و متعاقب آن نوع جدیدی از واکنش جامعهٔ بین‌المللی را موجب شده است (زینالی، ۱۳۹۴: ۲۷). مطابق تعریف فن لیست[1] از سیاست جنایی، سازماندهی عقلایی مبارزه علیه جنایات رخداده [ملی و بین‌المللی] بر پایهٔ داده‌های دانشِ علوم کیفری و جرم‌شناسی است (حسینی، ۱۳۹۷: ۲۵).

۱. سیاست جنایی موسع (تحلیل ساختاری)[2]

بروز سیاست جنایی بین‌المللی با صدور قطعنامه‌های سازمان ملل متحد مانند الف) قطعنامهٔ ۴۵/۱۲۱[3]، با موضوع تشویق دولت‌ها به تقنین جرائم سایبری و صدور دستورالعمل در زمینهٔ جلوگیری و کنترل جرائم سایبری[4]، ب) قطعنامهٔ ۵۵/۶۳[5] با موضوع مقابله با سوءاستفادهٔ جزایی از فناوری‌های اطلاعاتی از دولت‌ها، گام‌های ضروری برای مقابله با جرائم سایبری در سطح «منطقه‌ای» و «بین‌المللی» را خواست؛ ج) قطعنامهٔ ۵۶/۱۲۱[6] با موضوع مقابله با سوءاستفادهٔ جزایی از فناوری‌های ارتباطی و ضرورت همکاری میان دولت‌ها و سازمان ملل را تصویب کرد؛ د) قطعنامه‌های ۵۷/۲۳۹ و نیز ۵۸/۱۹۹[7] با تأکید بر ضرورت همکاری بین‌المللی، قطعنامهٔ اولی با موضوع ایجاد فرهنگ جهانی امنیت سایبری و قطعنامهٔ دومی با موضوع حفاظت از زیرساخت‌های حیاتیِ ارتباطی؛ ه) قطعنامهٔ ۶۰/۱۷۷ با اشاره به ابعاد فرامرزی جرائم سایبری، بر لزوم ایجاد همکاری از طریق توسعهٔ مشارکت با بخش خصوصی تأکید دارد؛ و) قطعنامهٔ ۶۴/۲۱۱[8] با موضوع درخواست ایجاد کنوانسیون بین‌المللی در زمینهٔ جرائم سایبری و درخواست تهیهٔ کنوانسیون‌های منطقه‌ای و مقابله با جرائم سایبری (شکیب‌نژاد، ۱۳۹۶: ۱۴۵-۱۴۳).

---

1. Franz Von Listzt

حقوقدان آلمانی‌الاصل از بنیانگذاران اتحادیهٔ بین‌المللی و حقوق بین‌المللی کیفری که در سال ۱۸۸۹ میلادی می‌زیسته است.

2. Analyse Structurell

۳. مصوب سازمان ملل در ۱۴ دسامبر ۱۹۹۰ میلادی.

4. UN Manual on the Prevention and Control of Computer-Rrlated Crime, United Nations Office at Vienna, Center for Social Development and Humanitarian Affairs(1994)

۵. مصوب مجمع عمومی سازمان ملل به سال ۲۰۰۰ میلادی.

۶. مصوب مجمع عمومی سازمان ملل متحد در سال ۲۰۰۲ میلادی.

۷. تصویب‌شده توسط سازمان ملل متحد به‌ترتیب ۳۱ ژانویهٔ ۲۰۰۳ و نیز ۳۰ ژانویهٔ ۲۰۰۴.

۸. تصویب‌شده توسط سازمان ملل متحد ۳ آگوست ۲۰۰۹.

۲. سیاست جنایی مضیق (جرم‌انگاری)[1]

منشور سازمان ملل متحد نسبت به هر معاهده یا کنوانسیون به‌تصویب‌رسیده در سطح جامعهٔ بین‌الملل، در ایجاد صلاحیت نظارتی خود، بر مؤثر و کارامد بودن اصول و مفاد اسناد بین‌المللی مزبور توسط دولت‌های عضو و دولت‌های بازدارنده و ناقض اقتدار و حاکمیت‌های سرزمینی و ملی کشورها در راستای حفظ نظم و صلح و امنیت پیشتاز بوده است. دیوان دادگستری بین‌المللی نیز در برخورد با وقایع ناقض نظم و صلح و امنیت بین‌المللی دارای شیوه و روش‌هایی مانند به‌کارگیری تفسیر موسع در خصوص رسیدگی به اقدامات صورت‌گرفته در عرصهٔ بین‌الملل و توجه به اقدامات پیشگیرانه و غایت‌شناسانه و هدف‌گرا که همانا جلوگیری از وقوع اقدامات موصوف است نیز بوده است (رمضانی قوام‌آبادی، ۱۳۹۲: ۳۷)، لیکن نسبت به منشور سازمان ملل متحد در جایگاهی پایین‌تر قرار دارد و در همین زمینه به‌صورت قاطع، صریح و بلامنازع در مقولهٔ موصوف موفقیت نداشته است و عدم تدبیر قاطع در حفظ ارزش بین‌المللی مزبور، تأسیس و ایجاد سیاست جنایی بین‌المللی را انکارناپذیر نشان داده است. در سال ۲۰۰۱ میلادی پروفسور کاسپرسن[2] بازدارندگی در خصوص جرائم سایبری با رویکرد توجه به حقوق جزای ماهوی، آیین دادرسی کیفری، حقوق جزای بین‌الملل را در دستور کار خود قرار داد و آن را کنوانسیون بوداپست نامید.[3] از مهم‌ترین اهداف آن تحقیق و تعقیب، صلاحیت و رفع تعارض مثبت و منفی، معاضدت و همکاری بین‌المللی است (جلالی فراهانی، ۱۳۹۵: ۱۴-۱۲) بازدارندگی موصوف، با تعیین ضمانت اجرا، محکومیت و مجازات کردن فرد مرتکب به دور از بهانه‌های حقوقی مانند مصونیت، صورت می‌گیرد که این مهم با تأسیس دیوان کیفری بین‌المللی تحقق خواهد یافت. تعیین صلاحیت‌های لازم و اِعمال صلاحیت‌های قضایی در اجلاس کامپلا ۲۰۱۰ میلادی تکمیل شد. دادگاه موصوف با اهداف نظام‌دهی و منسجم ساختن محاکمه، و اِعمال مجازات مرتکب با وجود قانونی مدون در راستای حفظ صلح و ایجاد امنیت، اقدام کرد (میرعباسی، ۱۳۹۴: ۳۷). نهاد مسئولیت کیفری فردی راه را برای هرگونه مصونیت و فرار از پاسخگویی مرتفع و مسدود کرده و با این اقدام موجبات مبارزه با بی‌کیفرمانی و عقیم ماندن واکنش جامعهٔ بین‌المللی در برابر جنایات بین‌المللی را فراهم ساخته است.

نتیجه‌گیری

توجه به روابط نوین بین‌المللی در قالب عملیات سایبری، باب ادبیات جدیدی را در روابط بین‌المللی منبعث از حقوق بین‌المللی عرفی گشود که گسترهٔ حاکمیت سایبری را مشمول دو

1. Incrimination
2. DR. H .W. K . K aspersen
3. Implementation of Recommendation N R(89)9 on computer-related crime, Report prepared by professor DR. H .W. K. Ksaspersen (doc. CDPC(97)5 and PC-CY (97)5 , page 106)

مفهوم حاکمیت وستفالیایی و فراوستفالیایی می‌داند و نظام حق و تکلیف مدرن و پیشرفته‌ای را از مفاهیمی مانند سلاح‌های سایبری و کاربرد آنها و اِعمال حقوق بین‌المللی سایبریِ عام را ترسیم می‌کنند. بروز حملات و جرائم سایبری توسط سلاح‌های مزبور بهترین مثال سوءاستفاده از فناوری‌های روز و ابزارهای سایبری است که منشأ اخلال در نظم و امنیت سایبری بین‌المللی است. حقوق منبعث از نظام حق و تکلیف موصوف وضعیت روابط بین‌المللی را در مقام حاکمیت سایبری و اهمیت صلح و امنیت سایبری بین‌المللی بیان می‌کند و نتیجهٔ نقض آن را ظهور ضمانت‌های کیفری که فصل ممیز میان اخلاق و حقوق است، خواهند دانست. مسئولیت کیفری فردی، تأسیس حقوقی است در تحقق عدالت کیفری که فرایند رسیدگی بدون اعمال نفوذ به‌واسطهٔ مناصب و مشاغل را میسر و ممکن می‌سازد. مطابق اساسنامهٔ رم صلاحیت تحقیق، تعقیب و رسیدگی به جنایت تجاوز حتی با بروز جرائم سایبری و حملات سایبری به‌دلیل تحقق توسل به زور سایبری[1] با مجوز دستورالعمل تالین متصور است. در مذاکرات تالین ۲۰۱۷ وظیفهٔ کارگروه بین‌المللی کارشناسان منتخب، تعیین چگونگی اِعمال قواعد حقوقی در بافت سایبر و شناسایی ابعاد منحصر به فضای در آن بود. قواعد مطروحه در این خصوص، بازتاب حقوق بین‌الملل عرفی اعمالی در فضای سایبری هستند، و قواعد مزبور مادامی‌که به‌درستی مبین حقوق بین‌الملل عرفی باشند، تمامی دولت‌ها را ملتزم می‌سازند. حدود و ثغور تکالیف دولت‌ها به‌دلیل نقض فصل هفتم منشور سازمان ملل و همچنین مطابق با ضوابط مصرح در قواعد ۱۵ و ۱۷ دستورالعمل مزبور قابلیت انتساب جزایی به‌عنوان تجاوز سایبری به‌سبب نقض اصل حاکمیت سایبری و تجاوز سایبری، انکارناپذیر خواهد بود. مستنبط از بند ۲ مادهٔ ۸ مکرر اساسنامهٔ رم اصلاحی در کنفرانس کامپالا و نیز قطعنامهٔ ۳۳۱۴ احراز جنایت تجاوز به‌عنوان جدی‌ترین و خطرناک‌ترین شکل توسل به زور، تحقق آستانهٔ تجاوز سایبری با صراحت قانون ۱۲ دستورالعمل تالین، منوط به وقوع اقدامات سایبری به میزان «حملهٔ مسلحانه» خواهد بود. مداقه در صلاحیت سایبری در حوزه‌های حقوقی و حاکمیتی و انواع آنها، ذهن را متوجه اتخاذ سیاست جنایی بین‌المللی به‌عنوان واکنش بین‌المللی در قبال جنایات سایبری رخ‌داده به‌صورت موسع و موجود می‌کند که مبین تغییرات و تحولات در این خصوص و در نهایت اِعمال سیاست جنایی بین‌المللی مضیق و جرم‌انگارانه در قبال تجاوزات سایبری است که نقش بسزایی در نقض حاکمیت کشورها دارد و می‌تواند به‌عنوان مؤثرترین راه برای ایجاد صلح و امنیت سایبری مطرح شود.

1. Use of Cyber Force

منابع

۱. فارسی

الف) کتاب‌ها

۱. آل‌حبیب، اسحاق؛ بیگ‌زاده، ابراهیم (۱۳۸۲)، *دیوان کیفری بین‌المللی و جمهوری اسلامی ایران* «بررسی جنایت نسل‌کشی و جنایات بر ضد بشریت در اساسنامهٔ دیوان کیفری بین‌المللی» چ هشتم، تهران: مرکز چاپ و انتشارات وزارت امور خارجه.

۲. آهنی امینه، محمد (۱۳۹۷)، *حقوق بین‌الملل مدرن و جنگ سایبری در فضای مجازی*، چ اول، تهران: مؤسسهٔ انتشارات جهان جام جم.

۳. امیرپور، مهناز؛ بهرامیان، شفیع (۱۳۹۳)، *مبانی کلی نظریه‌های ارتباط جمعی*، چ دوم، تهران: جامعه‌شناسان.

۴. ترنس دی، میت؛ ریچارد سی، مک کرل؛ لیسوان شلی جی (۱۳۹۲)، *نیمرخ‌های جنایی*، ترجمهٔ علی نجفی توانا و ایوب میلکی، چ اول، تهران: آموزش و سنجش.

۵. حسینی، سید محمد (۱۳۹۷)، *سیاست جنایی*، چ پنجم، تهران: انتشارات دانشگاه تهران.

۶. حمزه زینالی، امیر؛ کوره‌پز، محمد (۱۳۹۴)، *بازدارندگی نوین: جرم و سیاست جنایی در عصر جهانی شدن*، چ اول، تهران: خرسندی.

۷. جلالی فراهانی، امیرحسین (۱۳۹۵)، *کنوانسیون جرائم سایبر و پروتکل الحاقی آن*، چ دوم: تهران: خرسندی.

۸. حکیمی‌ها، سعید؛ ضیائی، سید یاسر (۱۳۹۵)، *صلاحیت جهانی در رسیدگی به جرائم جنگی از منظر حقوق بین‌المللی با نگرشی بر حقوق ایران*، چ اول: تهران، مؤسسه و چاپ دانشگاه امام حسین (ع).

۹. ذاکر حسین، محمدهادی (۱۳۹۹)، *آیین پیش دادرسی دیوان کیفری بین‌المللی، دفتر نخست (فرایند گزینشگری قضایا)*، چ اول، تهران: شهر دانش.

۱۰. رضایی‌نژاد، ایرج (۱۳۹۸)، *صلاحیت دیوان کیفری بین‌المللی*، چ سوم: تهران: مجمع علمی و فرهنگی مجد.

۱۱. ریاحی، اویس (۱۳۹۲)، *دفاعیات در حقوق کیفری بین‌المللی*، چ اول، تهران: فرهنگ‌شناسی.

۱۲. رمضانی قوام‌آبادی، محمدحسین (۱۳۹۲)، *روش کار قاضی بین‌المللی*، چ دوم، تهران: شهر دانش.

۱۲. سعیدی، رحمان (۱۳۹۷)، *حقوق بین‌الملل ارتباطات سایبر (مجازی)*، چ اول، تهران: خجسته.

۱۳. سودمندی، عبدالمجید (۱۳۹۴)، *رسیدگی به جنایت تجاوز در دادگاه کیفری بین‌المللی*، تهران: مؤسسهٔ فرهنگی هنری انتشاراتی نگاه بینه.

۱۴. شریعت باقری، محمدجواد (۱۳۹۷)، *حقوق کیفری بین‌المللی*، چ پانزدهم، تهران: جنگل.
۱۵. شکیب‌نژاد، احسان (۱۳۹۶)، *قانونگذاری در فضای سایبر از منظر حقوق بین‌الملل*، چ اول، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.
۱۵. عاملی، سید سعیدرضا (۱۳۹۰)، *رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی*، چ اول، تهران: امیرکبیر.
۱۶. کیتیجایساری، کریانگ (۱۳۸۷)، *حقوق کیفری بین‌المللی*، ترجمهٔ حسین آقایی جنت‌مکان، چ اول: تهران: جنگل.
۱۷. لوئی، تروتابا (۱۳۹۳)، *حقوق اساسی فرانسه*، ترجمهٔ سید محسن شیخ‌الاسلام، چ سوم، تهران: کوشا مهم.
۱۸. میرعباسی، سید باقر (۱۳۹۴)، *بایسته‌های دیوان کیفری بین‌المللی در تئوری و عمل*، چ دوم: تهران: خرسندی.
۱۹. میرمحمد صادقی، حسین (۱۳۹۵)، *دادگاه کیفری بین‌المللی* چ نهم: تهران: دادگستر.

ب) مقالات

۲۰. جلالی، غلامرضا (۱۳۹۵)، «اخبار پاپسا»، *ماهنامهٔ سازمان پدافند غیرعامل غیرعامل کشور*، ش ۱۳، ص ۲۳,
۲۱. خلیلی‌پور رکن‌آبادی، علی؛ نورعلی‌وند، یاسر (۱۳۹۵)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، *فصلنامهٔ مطالعات راهبردی*، سال پانزدهم: ش ۲، ص ۲۵۰.

۲. انگلیسی

A) Books

1. Akehurst, Michael, (2008)**,** *Jurisdiction in International Law*, Published Oxford university press , 8th Edition
2. Blake D Imburgia JS (2010), *Bloodless Weapons? The need to conduct legal reviews of certain weapons and the implcations of defeining them as Weapons.* Air Force Law Rev 66
3. Clark, Roger S. (2009), *The Crime of Aggression and the International Criminal Court*, Edited by José Doria Hans-Peter Gasser M. Cherif Bassiouni, The Legal Regime of the International Criminal Court, Essays in Honor of Professor Igor Blishchenko, Martinus NIJHOFF Publisher.
4. Hanagan, Michael (2000), *" States and Capital: Globalization Past and Present in The Ends of Globalization"* , edited by D. Kalb , M. van der Land, R.Staring, B. van Steenbergen and N.Wilterdink. Published Oxford university press
5. Hochshild Jennifer (1981), *What is Fair: AMERICAN Beliefs about Distributive*

Justice. Cambridge, MA: Harvard University Press.
6. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, *Tallinn Manual on The International Law Applicable to Cyber Warfare*, Cambridge University Press.
7. Kai Ambos (2010),"*The Crime of Aggression after Kampala*." German Year Book of International Law.
8. Li Xingan (2004), *Theories and Practiccces of International Jurisdiction to Cyber Crime* , Asian and Comparative Law, Vol. 2,No. 1
9. Michael N Schmitt (2013), *Tallinn Manual on The International Law Applicable To Cyber Warfare1*. Cambridge University Press.
10. Miller, Kevin L. (2014), "The Kampala Compromised and Cyberattacks: Can There be an International Crime of *Cyber-Aggression?*" *Southern California Interdisciplinary Law Journal* 23.
11. Schabas, Willam A.; Bernaz, Nadia (2011), *Routledge Handbook of Internantional Criminal Law*, London: Taylor and Franis Group.
12. Schiff, Benjamin N.(2008), *Building the International Criminal Court*. New York: Cambridge University Press.
13. Schmitt, Michael N (2017), *Tallinn Manual on The International Law Applicable To Cyber Warfare2*. Cambridge University Press.
14. Schmitt, Michael N.(2010), *Cyber Operations in International Law: The Use of Force, Collective Security, Self Defence, and Armed Conflicts, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, Washington: National Academic Press.
15. Stahn, Carsten & Sluiter, Göran (2009), *The Emerging Practice of the International Criminal Court, Legal Aspects of International Organization.* Vol. 48. Leiden: Martinus Nijhoff Publisher.

B) Articles

16. Ambos, Kai (2016), "Individual Criminal Responsibility for Cyber Aggression" *Journal of Conflict and Security Law, Oxford University Press*, pp.495–504.
17. Anderson, Michel (2010), "Reconceptualizing Aggression". Vol 60, *Duke law Journal*, Issue 11.
18. Delmas, Marty Mireille (2006), "Interctions between National and Internation Criminal Law in the Preliminary Phasr of Trial at the I.C.C", *Journal of Internation Criminal justice*, No.4.
19. Dunlap Jr, Charles J. (2011), "Major General, USAF Retired, Perspectives for Cyber Strategists on Law for Cyberwar*", Strategic Studies Quarterly* 5(1).
20. Dashora, K.(2011),"Cyber Crime in the Society: Problems and Preventions". *Journal of Alternative Persepctive in the Social Science* , Vol.3 , No. 1.
21. Kesan, Jay P., & Carol M. Hayes (2012), "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", *Harvard Journal of Law and Technology* 25.
22. Ophardt, Jonathan A. (2010),"Cyber Warfare and the Crime of Aggression: The

Need for Individual Accountability on Tomorrow's Battlefield", *Duke Law and Technology Review*.

C) Documents

23. Libman V.(1985), *The Queen in supreme cort Judgments*. Collection 1985,Canada,2SCR. Para 74.
24. *Report to the San Francisco conference*, 9 unclo (1945) ; Declaration on Friendly , Pmble
25. *Restatment (Third),*Part IV,Mann 1984,at19;Oppenheims International Law ,at 65; shaws International Law , at 469
26. *The Draft Convention On Research in Internationnal Law of the Harvard Law Scool* , (Supp.1935) 29AM.J, int-1/435 & 466

Refrences In Persian:

A) Books

1. Al-Habib, Ishaq & Ebrahim Beigzadeh (2003), *International Criminal Court and the Islamic Republic of Iran "Investigation of Genocide and Crimes against Humanity in the Statute of the International Criminal Court" Eighth Edition*, Tehran: Ministry of Foreign Affairs Publishing Center (In Persian).
2. Ahani Amineh, Mohammad (2018), *Modern International Law and Cyber Warfare in Cyberspace*, First Edition, jJahan Jam Jam Publishing Institute (In Persian).
3. Amirpour, Mahnaz & Shafi Bahramian (2014). *General Foundations of Mass Communication Theories*, Second Edition, Tehran: Sociologists Publications (In Persian).
4. Terence Dee, Mate; Richard C., McCarl & Liswan Shelley Jay (2013), *Criminal profiles*, translated by Ali Najafi Tavana and Ayub Milki. First Edition, Tehran: Education and Measurement Publications (In Persian).
5. Hosseini, Seyed Mohammad (2018), *Criminal Policy*, Fifth Edition, Tehran: University of Tehran Press (In Persian).
6. Hamzeh Zeinali, Amir & Koorehpez, Mohammad (2015), *New Deterrence: Crime and Criminal Politics in the Age of Globalization*, First Edition, Tehran: Khorsandi Publications (In Persian).
7. Jalalia Farahani, Amir Hossein (2015), *Cybercrime Convention and its Additional Protocol*, Second Edition: Tehran, Khorsandi Publications (In Persian).
8. Hakimiha, Saeed & Ziaei, Seyed Yaser (2015), *Global Jurisdiction in War Crimes from the Perspective of International Law with a View to Iranian Law*, First Edition, Tehran: Imam Hossein University Institute and Press (In Persian).
9. Zakir Hussein, Mohammad Hadi (2020), "*Pre-Trial Procedure of the International Criminal Court*, First Office (Case Selection Process)", First Edition, Tehran: Shahr-e-Danesh Institute for Legal Studies and Research Publications (In Persian).
10. Rezainejad, Iraj. (2019), *Jurisdiction of the International Criminal Court*, Third Edition: Tehran: Majd Scientific and Cultural Association Publications (In Persian).
11. Riahi, Oveys (2013), *Defense in International Criminal Law*, First Edition, Tehran: Farhang Shenasi Publications (In Persian).
12. Ramezani Ghavamabadi, Mohammad Hossein (2013), *The Method of Working for an International Judge*, Second Edition, Tehran: Shahr-e-Danesh Institute for Legal Studies and Research (In Persian).
13. Saeedi, Rahman (2018), *International Law of Cyber Communications (Virtual)*, First Edition, Tehran: Khojasteh Publications (In Persian).
14. Soodmandi, Abdolmajid (2014), Investigation of the crime of aggression in the International Criminal Court, Tehran: Negah Bineh Publishing House (In Persian).
15. Shariat Baqeri, Mohammad Javad (2018), *International Criminal Law*, Fifteenth Edition, Tehran: Jangal Publications (In Persian).
16. Shakibnejad, Ehsan (2017), *Legislation in Cyberspace from the Perspective of*

International Law, First Edition: Danesh Shahr Institute for Legal Studies and Research (In Persian).
17. Ameli, Seyed Saeed Reza (2011), *Judicial approach to harms, crimes and laws and policies of cyberspace*, first edition, Tehran: Amirkabir Publications (In Persian).
18. Kitijaysari, Kriang (2008), International Criminal Law, translated by Hossein Aghaei Janatmakan, first edition: Tehran, Jangal Publications (In Persian).
19. Louis, Trotaba (2014), *French constitutional law*, Translated by Seyyed Mohsen Sheikha-ol-Islam, third edition: Tehran, Koosha Mohm Publications (In Persian).
20. Mir Abbasi, Seyed Baqer (2015), Requirements of the International Criminal Court in Theory and Practice, Second Edition, Tehran: Khorsandi Publications.
21. Mir Mohammad Sadeghi, Hossein (2015), *International Criminal Court Ninth Edition*, Tehran: Dadgostar Publishing House (In Persian).

B) Articles

22. Jalali, Gholamreza (2016), "Papsa News", the monthly magazine of the country's inactive passive defense organization: No. 13 (In Persian).
23. Khalilipour Roknabadi, Ali & Noor Alivand, Yaser (2015), "Cyber Threats and Its Impact on National Security", *Strategic Studies Quarterly*, Year 15: Issue 2 (In Persian).