فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم شماره چهارم(پیاپی۱۲)زمستان۱۳۹۹ ،صص۲۸۹۴-۲۸۷۶

سیاست جنایی بین المللی در مقابله با جرایم سازمان یافته سایبری: رویکردها و راهبردها

احسان زررخ[۱]
قباد کاظمی[۲]
محمد جواد جعفری[۳]

تاریخ دریافت :۱۰ /۱۳۹۹/۸
تاریخ پذیرش: ۱۳۹۹/۱۲/۲۵

چکیده

جرائم سایبری در فرآیند تکوینی خویش تحولات مفهومی و مصداقی در حقوق جزای کلاسیک ایجاد نموده، به گونه ای که حتی ادبیات تخصصی خاص خود را داراست. به عنوان نمونه به جای اصطلاح مجرم در جرایم سایبری از عبارت هکر استفاده می شود و هکر به معنای مجرم سایبری است فارغ از اینکه عمل مجرمانه ارتکابی وی، واجد کدام وصف کیفری است. در راستای سیاست های جنایی بین المللی بحث درباره زمینه های و تاثیرگذاری های بین المللی در خصوص جرایم سازمان یافته سایبری مطرح می شود که بسیاری از پژوهشگران حوزه جرم شناسی سایبری این دوران را به دو مرحله پیش از کنوانسیون بوداپست ۲۰۰۱ و پس از آن تقسیم می کنند. تهدیدات سایبری چالشی برای نهادهای انتظامی در هر دو دسته کشورهای توسعه یافته و در حال توسعه است. توجه به قانون گذاری به عنوان یک بخش جدایی ناپذیر از استراتژی امنیت سایبری همانطور که قبلا اشاره شد، امنیت سایبری نقش مهمی در توسعه مداوم فن آوری اطلاعات و نیز خدمات اینترنتی بازی می کند. در همین راستا مقاله حاضر به بررسی جنبه های راهبردی مقابله با جرایم سازمان یافته سایبری در سطح کلان و رویکردهای عملی تقنینی در این حوزه می پردازد که البته با بررسی الگوها و استراتژی های مختلف مشخص می شود که یک رهیافت جامع جهانی در مقابله با این گروه از جرایم وجود ندارد.

واژگان کلیدی: سیاست جنایی، فضای سایبر، جرم سازمان یافته، سازمان ملل متحد، الگوی تقنینی

[۱] دانشجوی دکترای حقوق جزا و جرم شناسی، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران. zarrokh@ut.ac.ir
[۲] استادیار گروه حقوق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران. gh.kazemi@iauksh.ac.ir
[۳] استادیار گروه حقوق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران.dr.jafari@iauksh.ac.ir

مقدمه

شناخت جنبه های مختلف فضای سایبر و جرایم ارتکابی در آن و علی الخصوص جرایم سازمان یافته سایبری و تبیین رهیافت های تقنینی موجود در این خصوص مسئله مهم مورد بررسی در این مقاله است. به دیگر سخن در نوشتار حاضر به جنبه های مختلف چگونگی شناخت و مقابله با جرایم سازمان یافته سایبری و راهکارهای و سیاست های جنایی تقنینی بین المللی در مقابله با این دسته از جرایم خواهیم پرداخت به گونه ای که اقسام قابل انطباق این دسته از سیاست جنایی در قالب راهبردهای بین المللی مقابله با جرایم سازمان یافته سایبری مورد بررسی قرار خواهند گرفت که این موارد مهم ترین مسائل مورد بررسی در این رساله می باشند. بر همین اساس به نظر می رسد که شیوه های مرسوم در قالب سیاست جنایی تقنینی در عرصه بین المللی راهبردهای قابل اعمال و پذیرش در مقابله با جرایم سازمان یافته سایبری هستند که در قالب کلیاتی در کنوانسیون های مریدا در خصوص مقابله با فساد و کنوانسیون پالرمو در باره مبارزه با جرائم سازمان‌یافته فراملی و نیز دستورالعمل های سازمان ملل متحد، دیدگاه ها و مقرره های شورای اروپا خصوصاً کنوانسیون جرایم سایبری بوداپست مورد توجه ویژه قرار گرفته اند و روش های اجرایی مقابله با جرایم سازمان یافته سایبری با لحاظ زیرساخت های کیفری و غیر کیفری و خصوصاً در قالب راهبردها و توصیه نامه و اقدامات پیشگیرانه مردم محور در مقابله با این دسته از جرایم از اهمیت ویژه برخوردار هستند که در قالب سیاست جنایی تقنینی بین المللی در مقابله با این دسته از جرایم و در دو بخش تبیین سیاست جنایی تقنینی و نیز راهبردهای اجرایی آن مورد توجه و امعان نظر قرار گرفته و محل بحث خواهند بود.

مبحث اول) جرم سازمان یافته سایبری

در ابتدای بحث پیرامون جرم سازمان یافته سایبری این سوال مطرح می شود که آیا جرم سایبری ماهیتی مستقل از سایر جرایم دارد یا اینکه همان جرایم سنتی با شیوه‌ای مدرن است؟

در این موضوع استدلال های متفاوتی با این نگرش ارائه شده است که: "هرگونه بحث درباره جرم سایبری با مراجعه به مسائل پیچیده جرم شناسی و خصوصاً این سوال که آیا منظور از آن (جرم سایبری) ضرورت شکل جدیدی از جرم است یا مربوط به مباحث نظری جرم شناسی است، شروع می‌شود." (Majid Yar, ۲۰۰۵: ٤٠٨) در همین راستا استدلال شده است که: "جرم سایبری به صورت ساده، همان شراب کهنه است که در بطری های جدید ریخته اند." در واقع گرابوسکی با این دیدگاه فضای سایبر را وسیله‌ای نوین برای ارتکاب جرایم قدیمی می داند و به قائل به وجود جرایم جدید که به عبارتی سایبری محض[۴] باشند، نیست؛ (Grabosky. P, ۲۰۰۱: ۲۴۳) چرا که وی به فضای سایبر به عنوان وسیله‌ای در جهت ارتکاب جرایم سنتی و موجود می نگرد و به این موضوع که فضای سایبر محلی برای شکل گیری جرایم خاص خود

[۴] Pure Cybercrimes

باشد، معتقد نیست؛ در تکمیل این دیدگاه ها ادعا شده است که: "اگرچه جرم سایبری در حال گسترش است ولی بدان معنا نیست که بگوییم جرایم جدیدی به وجود آمده اند بلکه بهتر است بگوییم شیوه های جدیدی برای ارتکاب جرایم موجود به دست آمده و البته شیوه های بهتری نیز برای پی بردن به آنها ایجاد شده است." (Nisbett. C, ۲۰۰۲) در واقع، این دسته از نویسندگان که البته جزو برجسته ترین نویسندگان حقوق سایبری نیز هستند، برای جرم سایبری ماهیتی مستقل از جرایم موجود در فضای واقعی، متصور نیستند؛ چرا که اندیشه ایشان بر این اساس استوار است که نمی توان قائل به تحقق جرمی خارج از جهان واقعی بود و تمامی جرایم به نحوی با فضای مادی در ارتباطند و آثار آنها در این محیط نمود ملموس می یابد، از اینرو به فضای سایبر به عنوان متحول کننده جرایم مادی می نگرند تا شکل دهنده نسل جدیدی از جرایم؛ البته دیدگاه های آنان مبتنی بر ترسی است که از پذیرش استقلال فضای سایبر در میان بشر امروز یافت می شود، چرا که ناآگاهی از ابعاد گسترده این فضا که آن را چون سیاه چاله ای تاریک می نماید، سبب پرهیز حقوقدانان از پذیرش این فضا و بالتَبعْ جرایم ارتکابی در آن شده است و تا آنجا که ممکن است سعی در انطباق آن با فضایی دارند که در آن زندگی می کنند و از این رو در تمامی موارد با نگاه مادی و ملموس به جرایم می نگرند و سعی بر آن دارند تا این جرایم را به تَبَعِ برخی از آثار مادی آنها، از حالت سایبری و فرامادی خارج و با معیارهای مادی منطبق نمایند.

این دیدگاه ها که در خصوص کلیت جرم سایبری و جرم سازمان یافته سایبری وجود دارند، در واقع نشأت گرفته از برداشت های متفاوت حقوقدانان از ماهیت جرایم سایبری است که به مهم ترین علل آن اشاره شد، هرچند که در حال حاضر بحث از وجود یا عدم وجود جرایم سایبری محض تا حدودی مشکل می نمایند، لکن به نظر می رسد پس از این همه بحث و جدل که میان حقوقدانان روی داده است، دیگر مجال پرداختن به مسائل وجودی و عدمی این جرایم از میان رفته باشد و می بایست قائل به وجود جرم سایبری محض باشیم، هرچند که این تعارضات در نام‌گذاری جرایم این حوزه نیز به چشم می خورند و البته به نوعی می توان آنها را نشأت گرفته از پذیرش صریح و یا ضمنی این جرایم دانست چرا که ممکن است فردی درباره "جرم سایبری (Cybercrime)، جرم مجازی (Virtual crime)، جرم رایانه ای (Computer crime)، جرم فناوری (Technology crime)، جرم دیجیتالی (Digital crime)، جرم فناوری اطلاعات (IT crime)، جرم شبکه (NET crime)، جرم اینترنتی (Internet crime) و جرم الکترونیکی (E-crime) صحبت به میان آورد" (Rob Mc Cusker, ۲۰۰٦: ۲۵۸) حال آنکه تمامی آنها از یک واقعیت، حقایق گوناگونی را بسته به توان خویش درک می کنند و در واقع همان مثال فیل در کلام مولانا است که در تاریکی هرکس قسمتی از بدن فیل را لمس می کرد و آن را ملاک قرار می داد در حالی که همه آنها در مجموع یک چیز که همانا فیل باشد را لمس کرده اند، که این مثال کاملاً بر دیدگاه های مطروحه در خصوص جرم سایبری ساری و جاری است. با این وصف به نظر نگارنده بهترین اصطلاح برای این دسته از جرایم، اصطلاح جرایم مجازی است که تمامی اَشکال

جرایم خارج از جهان واقعی را پوشش می دهد و محدودیت هایی که بر سایر تعاریف و عناوین بار می شود بر این عنوان قابل تسری نیست. با این وجود بنابر ابتلاء موجود به بررسی جرم سازمان یافته سایبری پرداخته ایم.

با این تفاسیر جرایم سایبر با پیشوند سازمان یافته منجر به استنباط جرم سازمان یافته سنتی می شوند، لکن به مجرمان عادی که از فضای سایبر به شیوه سازمان یافته استفاده می کنند باز می گردد. بر همین منوال به نظر می رسد که برخورد با گروه های مجرمان سایبر درست به منزله آن است که آنها به لحاظ اندازه، پیچیدگی، ساختار و زمان، درست معادل همتایان سنتی خویش که جنبه مجازی ندارند، هستند و این امر به گروه‌های مجرمان سایبری اجازه می دهد که مشابه تحول و توسعه سازمانی‌ای را داشته باشند که گروه های جرایم سازمان یافته سنتی از خودشان نشان می دهند.

حال به این سوال می رسیم که آیا جرم سایبری به وسیله گروه های سازمان یافته سنتی واقع می شود یا صرفاً به شیوه سازمان یافته در محیط آن لاین ارتکاب می یابد؟

به هرحال به نظر می رسد که جرم سایبری وقتی سازمان یافته است که عامل آن در راه رسیدن به نمونه یک هکر تنها اولیه متوقف شده باشد، چرا که بدل شدن به یک هکر برجسته هدف غایی تمامی طبقات هکر[۵] است و اگر در این مسیر با شکست روبرو شوند، به سوی گروه های منزوی هکرها گرایش یابد.[۶] با این وصف اگر فعالیت غیرقانونی توأم با هماهنگی، تنها عامل جرم سازمان

---

[۵] **هولینگر (Holinger) بر مبنای درجه‌بندی پیشرفت، از مبتدی تا نخبهٔ فنی جرایم رایانه‌ای، هکرها را به سه دسته تقسیم کرد: دزدان،(Pirates) مرورگران (Browsers) و رخنه‌گران (Crackers) دزدان، هکرهایی هستند که کمترین تبحر فنی دارند و فعالیت‌هایشان به نقض حق نشر از طریق دزدی نرم‌افزار محدود می‌شود.**

مرورگران افرادی با تبحر فنی متوسط هستند که به طور غیرمجاز به فایل‌های سایرین دسترسی می‌یابند، اما معمولاً به فایل‌ها آسیب نمی‌زنند یا کپی نمی‌کنند. رخنه‌گران که چیره‌دست‌ترین هکرها هستند، از توانایی فنی‌شان برای کپی کردن فایل‌ها یا صدمه‌زدن به برنامه‌ها و سیستم‌ها سوءاستفاده می‌کنند. شرکت مک‌آفی (McAfee) هکرها را به دو دستهٔ کلاه سفید (White Hat) و کلاه سیاه (Black Hat) تقسیم می‌کند.

Fitch, Cynthia (۲۰۰۳), "Crime and Punishment: The Psychology of Hacking in New Millenium",retrieved from: http://www.giac.org /practical/GSEC/Cynthia_Fitch_GSEC.pdf

کلاه سفیدها به یافتن منفذ شبکه‌های امنیتی برای شرکت‌های امنیتی گرایش دارند و بنابراین در بهبود خدمات رایانه‌ای سودمند برای کاربران شرکت می‌کنند. کلاه سیاه‌ها، هکرهای مغرضی که از مهارتشان سوءاستفاده می‌کنند. (زررخ، ۱۳۸۸: ۴۲۳)

[۶] هکرهای تنهای اولیه، در واقع پیشتازان هک هستند که به نوعی سمبل هکرهای فعلی اند که از جمله آنها می توان به مایک میتنیک اشاره نمود.

یافته به حساب آید، در آن صورت به نظر می رسد که هر شکلی از رفتار مجرمانه که مستلزم درجاتی از برنامه ریزی باشد، نوعی جرم سازمان یافته به حساب می آید. (Ibid: ۲۵۹) البته همانطور که مشخص است و پیشتر نیز عنوان کردیم، شرایط جرم سازمان یافته سایبری تنها داشتن میزانی از سازمان یافتگی نیست و می بایست، علاوه بر این مورد موارد دیگری را نیز مشاهده نمود تا بتوان بحث از جرم سازمان یافته سایبری را مطرح نمود.

شایان ذکر است که به نظر برخی با توجه به اینکه اطلاعات موجود در خصوص رابطه جرم سازمان یافته و جرم سایبری بسیار محدود است امکان تحلیل های عمیق در حال حاضر امکان پذیر نیست و این دیدگاه منطبق بر نظری است که شورای اروپا عنوان کرده است که: "داده ها و اطلاعات درباره ارتباط میان جرم سازمان یافته و جرم سایبری هنوز ناچیز است و به ما اجازه نمی دهد که بتوانیم تجزیه و تحلیل مطمئنی از آن داشته باشیم." (Council of Europe:۲۰۰٤)

با وجود این دیدگاه ها به نظر می رسد که همچنان نگرشی عمیق تر در خصوص جرایم سازمان یافته سایبری می بایست مطمح نظر قرار گیرد. چه آنکه اداره اطلاعات مرکزی آمریکا (FBI) در گزارش خود درباره یکی از گروه های جرم سازمان یافته سایبری بیان داشته است که: کاردل پلانت[۷] درست مانند مافیای ایتالیا خود را قاعده‌مند و سازماندهی نموده است. (McMillan, R, ۲۰۰۶) البته این تحلیل مبتنی بر ویژگی قاعده‌مندی است و از این حیث به نظر می رسد که این عامل به تنهایی نمی تواند معیاری برای سازمان یافتگی جرایم باشد.

پذیرش درگیری گروه های مجرمانه سازمان یافته سنتی در فعالیت های جنایی سایبری، دستگاه های مجری قانون را در یک موضع ناخواسته قرار داده که مجبور شوند جرایم مجازی پیچیده تر را همچنان در چهارچوب محیط فیزیکی اجرای قانون مورد بررسی و تحقیق قرار دهند. (Rob Mc Cusker, ۲۰۰٦: ۲٦۰) در واقع برخلاف جرایم سازمان یافته قرن بیستم، جرایم سازمان یافته سایبری قرن بیست و یک، بیشتر شبیه پذیرش و سازگار نمودن جرم سنتی به فناوری جدید است تا خلق جرم جدید با ساختاری جدید. (Ibid)

مبحث دوم) سیاست جنایی سایبری

جرایم سایبری در فرآیند تکوینی خویش تحولات مفهومی و مصداقی در حقوق جزای کلاسیک ایجاد نموده، به گونه ای که حتی ادبیات تخصصی خاص خود را داراست. به عنوان نمونه به جای اصطلاح مجرم در جرایم سایبری از عبارت هکر استفاده می شود و هکر به معنای مجرم سایبری است فارغ از اینکه عمل مجرمانه ارتکابی وی، واجد کدام وصف کیفری است.

در جرم شناسی سایبری سخن از زمینه سیاست جنایی نیز وجود دارد. به عنوان مثال اگر عین عبارت سیاست جنایی جرایم سایبری را جستجو نمائیم، با عناوین محدودی مواجه خواهیم شد، لکن اگر با ادبیات تخصصی جرایم سایبری آشنا باشیم این مشکل روبرو نمی شویم چراکه در

---

[۷] یک گروه هکری سایبری Carderplanet

آمریکا و برخی کشورها از عبارت استراتژی جرایم سایبری به جای سیاست جنایی جرایم سایبری استفاده می شود. در کشورهای چین، اکوادور، برزیل و غیره از بررسی رهنمود و برنامه های IT در زمینه حقوق و... استفاده می شود و در مواردی به جای سیاست جنایی سایبری عناوینی چون برنامه ملی پیشگیری سایبری، برنامه ملی امنیت سایبری، استراتژی امنیت سایبری و... به کار برده شده است ولذا اگر با این واژگان برخورد کردیم باید در قالب سیاست جنایی تفسیر نمائیم. علت اینکه گوناگونی واژگان نیز مشخص است و آن هم بدین خاطر است که جرایم سایبری ماهیتاً فنی هستند فلذا طبیعی است که حجم زیاد ادبیات آن فنی باشد.

سیاست جنایی مشارکتی که بیانگر نقش و جایگاه مردم و نهادهای اجتماعی و غیردولتی در فرایند کیفری است، به دو گونهٔ کنشی (پیشگیرانه یا فعال) و واکنشی (پاسخگو یا منفعل) قابل تقسیم است. هدف اصلی سیاست جنایی مشارکتی کنشی یا اولیه، پیشگیری از ارتکاب جرم یا کاهش آن از طریق فرهنگ سازی در رفتارهای اجتماعی است که به آن پیشگیری اجتماعی نیز گفته می شود و بیانگر نقش مردم در کاهش ارتکاب جرم است. هدف سیاست جنایی مشارکتی واکنشی یا ثانویه، دخالت دادن مردم و نهادهای غیردولتی در فرایند کیفری، پس از وقوع جرم است. در این رویکرد، دیگر نهاد عدالت کیفری، تنها مرجع پاسخگویی و حل اختلاف نیست، بلکه از ظرفیت نهادهای مردمی و جامعوی نیز در این زمینه استمداد می شود.

بنابر موارد فوق و با توجه به اینکه یکی از چالشهای جدید حقوق کیفری مقابله با جرائم سایبری با عنایت به گستردگی و شبکه ای بودن فضای سایبر است، باید اذعان داشت مقابله با جرائم سایبری به جهت گستردگی خسارات و کثرت بزه دیدگان، فرامرزی بودن و مشکلات کشف و تعقیب مجرم و بسیاری ویژگی های دیگر تنها با یک «راهبرد جنایی مشارکتی» می تواند کارآمد و مؤثر صورت گیرد. آنچه این نظر را تقویت می کند این است که جرائم سایبری در غیاب جرائم سنتی اتفاق نمی افتند و در واقع جایگزین جرائم سنتی نمی شوند، بلکه در کنار آنها قرار می گیرند. یعنی جرائم سنتی مانند قتل، ضرب و جرح، زنا، سرقت و کلاهبرداری های سنتی کماکان اتفاق می افتند. نتیجه این است که منابع، نیروها و امکانات موجود دستگاه عدالت کیفری دچار فرسایش و کمبود می شوند و امکان مواجهه با همه این جرائم از آنها سلب می شود. برای مقابله همه جانبه و کارآمد با این جرائم، اتخاذ یک سیاست جنایی فراگیر با مشارکت گسترده جامعه مدنی، کاربران سایبر و سازمان های مردم نهاد ضروری است. در پرتو یک سیاست جنایی مشارکتی هر یک از این گروه ها باید در مراحل مختلف فرایند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و تعقیب مجرم، مرحله رسیدگی به جرم و مجازات مجرم نقش آفرینی کنند تا ضمن کاستن از بار دستگاه عدالت کیفری به مقابله هرچه گسترده تر و دقیقتر با جرم پرداخته شود. چرا که کنترل بزه به جهات مختلف فراتر از ظرفیت نهادهای رسمی عدالت کیفری است و باید به واگذاری بخشی از سازکارهای تأمین کننده امنیت و عدالت به مردم، سازمانهای مردم نهاد و نهادهای غیردولتی پرداخت یکی از نمود های سیاست جنایی مشارکتی در زمینه سایبر، کاستن از

اختیار نهادهای دولتی و نظارتی در امر فیلترینگ و تفویض حداقل قسمتی از این امر بـه برخـی از شهروندان و کاربران شریف فضای سایبر، که رویکـردی سـنجیده و ملایـم تـر نسـبت بـه مسـئله فیلترینگ دارند، می باشد. این امر موجب افزایش دقت و هوشمندی سامانه هـای فیلترکننـده بـرای اجتناب از اشتباه در فیلترینگ نیز می شود. (حاجی ده آبادی، سلیمی:۱۳۹۳ ۸۲-۸۳)

مبحث سوم) رویکردهای سیاست جنایی بین المللی در مقابله با جرایم سازمان یافته سایبری

پیش از پرداختن به موضوع بحث و تبیین های ساختاری در باب سیاست جنایی ذکر ایـن موضـوع حائز اهمیت است که دررابطه با سیاست جنایی سایبری به طور کلـی محـدودیت هـای مـرتبط بـا منابع و یافته های علمی و تخصصی وجود دارد به گونه ای که اگر عـین عبـارت سیاسـت جنـایی جرایم سایبری، جستجو شود، با عناوین محدودی روبرو می شویم، اما اگـر بـا ادبیـات تخصصـی جرایم سایبری آشنا باشیم این مشکل تا حدودی مرتفع می شـود. در آمریکـا و برخـی کشـورها از عبارت استراتژی جرایم سایبری به جای سیاست جنایی جرایم سایبر استفاده مـی شـود. در چـین، اکوادور، برزیل و برخی کشورهای دیگر از بررسی رهنمود و برنامه های فناوری اطلاعات در زمینه حقوق کیفری و... استفاده می شود. البته به ندرت در برخی کشورها چون پاراگوئـه و مقدونیـه بـه جای سیاست جنایی اصطلاحاتی چون برنامه ملی پیشگیری سایبری، برنامه ملـی امنیـت سـایبری، استراتژی امنیت سایبری و... به کار رفته است. در نتیجه اگر با این واژگـان برخـورد نمـودیم بایـد نگاهی به سیاست جنایی داشته باشیم. علت اینکه تفاوت واژگانی فوق وجود دارد نیـز مشـخص و طبیعی است. جرایم سایبری در ماهیت امر جرایم فنی هستند، طبیعی است که حجم زیاد ادبیات آن فنی باشد. شایان ذکر است جرایم سازمان یافته سایبری در ادامـه سـیر تحـول جـرایم سـایبری بـه وجود آمده اند و عام تر از آن هستند یعنی این دسته از جرایم نمونـه توسـعه یافتـه و پیچیـده تـر جراسم یابری که مضموما و مصداقا جرایم کامپیوتری هستند، مـی باشـند و از ایـن رو در بررسـی سیاست جنایی جرایم سایبری فقط به بحث کامپیوتر اکتفا نمی شود، بلکـه مخـابرات، شـیوه هـای توسعه ای و ساختارهای فناورانه نوین و فراملی هم مدنظر قرار می گیرند.

در راستای سیاست های جنایی بین المللی بحث درباره زمینه های و تاثیرگذاری های بـین المللـی در خصوص جرایم سازمان یافته سایبری مطرح می شود که بسـیاری از پژوهشـگران حـوزه جـرم شناسی سایبری این دوران را به دو مرحله پیش از کنوانسیون بوداپست ۲۰۰۱ و پـس از آن تقسـیم می کنند و همانطور که در بیانه "هیـات قـانون گـذاری و چـارچوب هـای قـانونی[۸] کنوانسـیون و چارچوب های قانونی جرایم رایانه ای و مدارک الکترونیکی: برخی از نظرات در مورد تحولات در سال ۲۰۱۸" آمده، موازین تاثیرگذاری و نیز داده های آماری در این خصوص به شرح ذیل است:

[۸] Panel on legislation and legal frameworks

ابزارهای بین المللی موجود، مبنایی موثر برای هم کاری بین المللی در مورد جرایم رایانه ای و شواهد الکترونیکی ارائه می دهند.

- UNTOC و پروتکل آن برای هم کاری قانونی بین المللی در زمینه مبارزه با جرائم سازمان یافته از جمله جرایم رایانه ای
- کنوانسیون بوداپست درباره راهنمای توسعه قوانین داخلی و چارچوب هم کاری بین المللی
- شکاف های وجود دارند که باید از طریق قوانین داخلی برطرف شوند
- عدم توانایی عدالت کیفری اغلب باعث تاخیر در پذیرش و اعمال قانون می شود.

گزارشی از پیشرفت های خوب از سال ۲۰۱۳ تا ۲۰۱۸ در زمینه قانونگذاری با "هماهنگ سازی/ ثبات و پراکندگی کم تر:

- تقریبا نیمی از کشورهای عضو سازمان ملل در حال حاضر دارای مقررات قائم به ذات قانونی کیفری به جا در این مورد هستند.
- قوانین اساسی داخلی بیشتر با استانداردهای بین المللی مانند کنوانسیون بوداپست سازگار هستند.
- با توجه به قدرت های رویه ای باید تلاش های بیشتری انجام شود.
- قدرت ها باید با شرایط و تدابیر حفاظتی در حال محدود شدن هستند.
- مشکل اصلی بسیاری از کشورها فقدان صلاحیت کیفری لازم برای اعمال قانون در عمل هستند.
- اصلاحات بیشتر و ایجاد ظرفیت مورد نیاز است.

در سال های اخیر حدود ۹۰ درصد از کشورهای عضو سازمان ملل اصلاحات در زمینه جرایم رایانه ای و مدارک الکترونیکی را انجام داده اند یا شروع کرده اند.

اصلاحات در جریان یا در سال های اخیر					
در ژانویه ۲۰۱۸		کشوها در ژانویه ۲۰۱۳			
٪۸۳٫۱	۴۵	٪۴۶	۲۵	۵۴	تمام افریقا
٪۸۹	۳۱	٪۷۱	۲۵	۳۵	تمام امریکا
٪۸۸	۳۷	٪۸۱	۳۴	۴۲	تمام اسیا
٪۱۰۰	۴۸	٪۹۸	۴۷	۴۸	تمام اروپا
٪۸۶	۱۲	٪۸۶	۱۲	۱۴	تمام اقیانوسیه
٪۹۰	۱۷۳	٪۷۴	۱۴۳	۱۹۳	همه

کنوانسیون بوداپست، قانونگذاری را در اکثریت کشورهای عضو سازمان ملل متحد هدایت نموده و یا با الهام بخشیدن موجب آن شده است.

تا ژانویه ۲۰۱۸:

- ۷۱ کشور (۳۷ ٪ از اعضای سازمان ملل) یا عضو شده اند و یا امضا کرده اند و یا از آنها برای توافق کردن دعوت شده است.
- بیش از ۷۰ درصد از اعضای سازمان ملل به نظر می رسد که از این معاهده به عنوان راهنما یا منبع الهام استفاده کرده اند.
- کنوانسیون بوداپست به عنوان رهنمود جهانی برای قانونگذاری داخلی[۹] عمل می کند.

کنوانسیون بوداپست در حال اجرا است و تا به امروز باقی مانده است چرا که توسط کمیته کنوانسیون جرم سایبری (T-CY) و فعالیت های ظرفیت سازی مورد حمایت قرار می گیرد.

- تا ژانویه ۲۰۱۸، ۷۱ کشور عضو یا ناظر در کمیته کنوانسیون جرم سایبری(T-CY) بودند
- . ارزیابی هایT-CY برای بهبود کیفیت اجرا و به اشتراک گذاشتن روش های خوب
- دستورالعمل های راهبردی (بوت نت ها، اسپم، دزدی هویت، حملات چیپ، بدافزار، تروریسم)نشان می دهند که چگونه کنوانسیون می تواند برای رسیدگی به پدیده جدید مورد استفاده قرار گیرد و بنابراین به روز باقی بماند.
- کار بر روی یک پروتکل جدید برای ارتقا همکاری بین المللی جهت رسیدگی به مشکل مدارک در حوزه های قضایی خارجی، چندگانه یا ناشناخته (در "ابر")
- دفتر برنامه جرم سایبری شورای اروپا (C-proc) در رومانی برای فعالیت های ظرفیت سازی در سراسر جهان برای حمایت از اجرای کنوانسیون و پی گیری توصیه های T-CYوقف شده است
- چارچوبی پویا برای هم کاری

موارد مذکور در این گزارش گروه تخصصی هیات بین دولتی سازمان ملل در مورد جرم سایبری به وضوح تاثیرگذاری کنواسیون بین المللی جرایم سایبری بوداپست را در شکل گیری زیرساخت های تقنینی کشورهای مختلف آشکار می نماید که البته این مهم صرفاً جنبه هایی از آن را به اثبات می رساند و هنوز مباحث عمده و ضرورت های تقنینی بین المللی در ترسیم مقررات بین المللی واحد در برابر جرایم سازمان یافته سایبری باقی مانده است.

مبحث چهارم) سیر تکامل سیاست جنایی تقنینی سایبری

چندین سازمان بین المللی و فراملی، ماهیت ذاتی جرایم رایانه ای، محدودیت های متعاقب رویکردهای یک جانبه و نیاز به هماهنگ سازی بین المللی راه حل های فنی، قانونی و دیگر را

[۹] domestic legislation

شناسایی کرده اند. بازیگران اصلی در این زمینه، سازمان هم کاری اقتصادی و توسعه(OECD) ، شورای اروپا، اتحادیه اروپا و اخیرا – گروه ۸ و پلیس بین الملل هستند. به علاوه، سازمان ملل، WIPOو GATS نیز نقش مهمی ایفا کرده اند. این سازمان های بین المللی و فراملی به طور قابل توجهی به هماهنگ سازی قانون جزا و همچنین قانون مدنی و اجرایی در همه نواحی فوق الذکر مربوط به اصلاحات قانون جزایی مرتبط با کامپیوتر، کمک کرده اند. اولین تحقیق جامع در رابطه با مشکلات قانون کیفری مربوط به جرایم مربوط به کامپیوتر در سطح بین المللی توسط کشورهای OECD آغاز شده است. در سال ۱۹۸۳ گروهی از متخصصان توصیه کردند که کشورهای OECD دعوت برای در تلاش برای دستیابی به هماهنگ سازی قانون جرایم رایانه ای اروپا قبول کنند. بنابراین، از سال ۱۹۸۳ تا ۱۹۸۵ مطالعه ای در مورد امکان هماهنگی بین المللی قوانین جنایی برای رسیدگی به جرایم مربوط به کامپیوتر انجام داد.

این مطالعه به گزارش سال ۱۹۸۶، در ارتباط با جرایم مرتبط با کامپیوتر انجامید: تحلیل سیاست حقوقی که قوانین و پیشنهادها موجود برای اصلاح را مورد بررسی قرار داده و یک فهرست حداقلی از سو استفاده هایی را که کشورها باید به موجب قانون جزا جرم انگاری شوند، مورد بررسی قرار داد. از سال ۱۹۸۵ تا ۱۹۸۹ کمیته منتخب متخصصان جرایم مربوط به کامپیوتر شورای اروپا درباره مسائل مطرح شده توسط جرایم رایانه ای و توصیه که در ۱۳ سپتامبر ۱۹۸۹ به تصویب رسیده بود، بحث و تبادل نظر کردند. این توصیه بر اهمیت واکنش مناسب و سریع به چالش جدید جرایم رایانه ای تاکید کرد. در دستورالعمل مجالس ملی برای بررسی افزایش قوانین آن ها، پیشنهاد حداقل فهرستی از نامزدهای مورد نیاز برای چنین جرایمی به تصویب رسید و توسط اجماع بین المللی مورد پی گرد قانونی قرار گرفت و همچنین یک "فهرست اختیاری" که جرائم برجسته در اجماع بین المللی را توصیف می کند، قابل حصول استدر سال ۱۹۹۰ کنگره سازمان ملل متحد در زمینه پیش گیری از جنایت و رفتار متخلفان، مشکلات قانونی جرایم رایانه ای را مورد بررسی قرار داد. قطعنامه از کشورهای عضو خواست تا تلاش های خود را برای مبارزه با جرایم مرتبط با کامپیوتر با مدرنیزه کردن قوانین ملی خود، بهبود تدابیر امنیتی و ترویج توسعه چارچوب جامع بین المللی رهنمودها و استانداردها برای پی گیری این جنایات در آینده تشدید کنند.

دو سال بعد، شورای کشورهای OECD و ۲۴ عضو از کشورهای عضو آن توصیه هایی برای شورای امنیت سیستم های اطلاعاتی به تصویب رساندند که هدف از آن ارائه یک چارچوب امنیتی جدید برای بخش های دولتی و خصوصی است. دستورالعمل هایی برای امنیت سیستم های اطلاعاتی به توصیه ضمیمه شد این چارچوب شامل قوانین رفتاری، قوانین و اقدامات فنی می شود.

آن ها بر اجرای حداقل استانداردها برای امنیت سیستم های اطلاعاتی تمرکز دارند. با این حال، این رهنمودها درخواست می کند که کشورهای عضو سیستم کیفری مناسب، اجرایی از دیگر

مجازات ها برای سو استفاده و سو استعمال از سیستم های اطلاعاتی ایجاد کنند. در سال ۱۹۹۵ سازمان ملل متحد، مانوئل سازمان ملل متحد در زمینه پیش گیری و کنترل جرم مرتبط با کامپیوتر را منتشر کرد این مانوئل، پدیده جرایم مربوط به کامپیوتر، قانون جزایی اساسی، حفاظت از حریم خصوصی، قانون رویه ای، و نیازها و راه های هم کاری بین المللی را مورد مطالعه قرار داد. در همان سال، پلیس بین الملل اولین کنفرانس خود را در مورد جرم کامپیوتری سازماندهی کرد. این کنفرانس تایید کرد که سطح بالایی از نگرانی در جامعه انتظامی در مورد انتشار جرم کامپیوتری وجود دارد. بعدا، پلیس بین الملل چندین کنفرانس را در همان زمینه برگزار کرد. در همان سال، شورای اروپا توصیه هایی شماره آر ۹۵ از کمیته وزرا به کشورهای عضو، در مورد اجبار اصولی که باید دولت ها و مقامات تحقیق آن ها در حوزه فن آوری اطلاعات را هدایت کند، تصویب کرد. برخی از این اصول جستجو و توقیف ، تعهد به هم کاری با تحقیق، استفاده از رمزنگاری و هم کاری بین المللی را پوشش می دهند.

در ۲۴ آوریل ۱۹۹۷، کمیسیون اروپا قطعنامه ای را در مورد "ارتباط کمیسیون اروپا بر روی محتوای غیرقانونی[۱۰] و زیان آور بر روی اینترنت تصویب کرد که از ابتکارات انجام شده توسط کمیسیون و تاکید بر نیاز به هم کاری بین المللی در حوزه های مختلف حمایت کرد یک سال بعد، کمیسیون اروپا گزارشی در مورد جرم مرتبط با کامپیوتر ارائه داد که برای آن قرارداد امضا شده بود. چند سال بعد، شورای خبره در زمینه جنایت در فضای سایبری این تکلیف را قلبا پذیرفت و یک پیش نویس کنوانسیون را در مورد جرم سایبری آماده نمود. آماده سازی این کنوانسیون یک فرآیند طولانی بود؛ چهار سال و بیست و هفت پیش نویس را پیش از آخرین نسخه مورخ ۲۵ مه ۲۰۰۱ به کمیته اروپا در پنجاهمین جلسه جامع که در ۱۸-۲۲ ژوئن ۲۰۰۱ برگزار شد تحویل داده شد. فصل دوم این کنوانسیون حاوی مفادی است که مربوط به موضوعات مورد نظر در این ماده هستند. این فصل به دو بخش تقسیم شده است: بخش ۱ با قانون جزایی اساسی سر و کار دارد، بخش ۲ با قانون رویه ای سر و کار دارد. با توجه به یادداشت تفاهم مربوط به کنوانسیون پیش نویس، بخش ۱ به دنبال بهبود وسیله ای برای پیش گیری و سرکوب جرم یا جرم های مرتبط با کامپیوتر از طریق ایجاد حداقل استاندارد برای جرم مرتبط است. کشورهای عضو کنوانسیون موافقت خواهند کرد که چنین اقداماتی را تصویب کنند و اقدامات دیگری را که ممکن است برای ایجاد فعالیت های ویژه جرایم رایانه ای تحت قانون داخلی خود لازم باشد، اتخاذ نمایند. طبق بخش ۱ از فصل ۲ کنوانسیون، این فعالیت ها عبارتند از: (۱) جرایم در برابر قابلیت اعتماد، یکپارچگی و در دسترس بودن داده ها و سیستم ها؛ (۲)جرایم مربوط به کامپیوتر؛ (۴)جرایم مربوط به تخطی از قوانین کپی رایت و حقوق مرتبط (۵)مقررات مربوط به تحمیل کمک و معاونت شرکت. از طرف آن ها، جی ۸ در ماه مه سال ۲۰۰۰ یک کنفرانس سایبری برای بحث در مورد

[۱۰] Illegal content

چگونگی مقابله با جرایم رایانه ای برگزار کرد. این کنفرانس ۳۰۰ قاضی، پلیس، دیپلمات ها و رهبران تجاری کشورهایG ۸ را گرد هم آورد. پیش نویس یک دستور کار برای نشست بعدی که قرار بود در ماه جولای برگزار شود را پیش نویس کرد. در نشست جولای ۲۰۰۰، G۸ بیانیه ای صادر کرد که در بخش مربوطه اعلام شد که رویکردی هماهنگ با جرائم فن آوری پیشرفته مانند جرایم رایانه ای که می تواند امنیت جامعه اطلاعاتی جهانی را به شدت تهدید کند، دارد. در این اطلاعیه آمده است که رویکردG ۸ در مورد این موضوعات در یک سند همراه با منشور اوکیناوا در زمینه جامعه اطلاعاتی جهانی تنظیم شده است.

گفتار اول) ضرورت های شناختی در تبیین سیاست جنایی تقنینی سایبری

تهدیدات سایبری چالشی برای نهادهای انتظامی در هر دو دسته کشورهای توسعه یافته و در حال توسعه است. از آنجا که ICT ها به سرعت تکامل می یابند، به خصوص در کشورهای در حال توسعه، ایجاد و اجرای یک استراتژی موثر مبارزه با جرایم رایانه ای به عنوان بخشی از استراتژی ملی ضروری است. توجه به قانون گذاری به عنوان یک بخش جدایی ناپذیر از استراتژی امنیت سایبری همانطور که قبلا اشاره شد، امنیت سایبری نقش مهمی در توسعه مداوم فن آوری اطلاعات و نیز خدمات اینترنتی بازی می کند. ساخت اینترنت امن تر (و حفاظت از کاربران اینترنت) برای توسعه خدمات جدید و نیز سیاست دولت امری اساسی شده است. استراتژی های امنیت سایبری - برای مثال، توسعه سیستم های حفاظت فنی یا آموزش کاربران برای جلوگیری از تبدیل آن ها به قربانیان جرم سایبری – می تواند به کاهش خطر جرایم رایانه ای کمک کند. یک استراتژی مبارزه با جرایم رایانه ای باید یک عنصر کامل از یک استراتژی امنیت سایبری باشد. دستور کار امنیت سایبری جهانیITU، به عنوان چارچوب جهانی برای گفتگو و هم کاری بین المللی برای هماهنگ کردن واکنش بین المللی به چالش های رو به رشد امنیت سایبری و افزایش اعتماد و امنیت در جامعه اطلاعاتی، بر روی کار، موجود ابتکارات و مشارکت موجود با هدف پیشنهاد استراتژی های جهانی برای رسیدگی به این چالش ها ساخته شده است. همه اقدامات مورد نیاز در پنج ستون دستور کار امنیت سایبری جهانی مربوط به هر استراتژی امنیت سایبری هستند. علاوه بر این، توانایی مبارزه موثر علیه جرایم رایانه ای به اقداماتی نیاز دارد که باید در تمام پنج ستون انجام شود.

۱) پیاده سازی استراتژی های موجود

یک احتمال این است که استراتژی های مبارزه با جرایم رایانه ای توسعه یافته در کشورهای در حال توسعه را می توان معرفی کرد که مزایای کاهش هزینه و زمان برای توسعه را ارایه می دهد. اجرای استراتژی های موجود می تواند کشورهای در حال توسعه را قادر سازد تا از بینش و تجربه موجود بهره مند شوند. اجرای یک استراتژی مبارزه با جرم سایبری موجود، تعدادی از مشکلات را به همراه دارد. اگرچه هم کشورهای در حال توسعه و هم در حال توسعه با چالش های مشابهی رو به رو هستند، راه حل های بهینه که ممکن است اتخاذ شوند بستگی به منابع و قابلیت های هر

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم، شماره چهارم (پیاپی ۱۲)، زمستان ۱۳۹۹

کشور دارد. کشورهای صنعتی ممکن است بتوانند امنیت سایبری را به روش های مختلف و انعطاف پذیر ارتقا دهند، به عنوان مثال با تمرکز بر مسائل مربوط به حفاظت فنی فشرده.

مسائل دیگری نیز وجود دارند که باید توسط کشورهای در حال توسعه اتخاذ شوند که استراتژی های مبارزه با جرایم رایانه ای موجود را می پذیرند. آن ها شامل سازگاری با سیستم های قانونی مربوطه، وضعیت اقدامات حمایتی (به عنوان مثال آموزش و پرورش جامعه)، میزان حمایت از خود در جایگاه و میزان حمایت بخش خصوصی (به عنوان مثال از طریق مشارکت خصوصی عمومی).

۲) تفاوت های منطقه ای

با توجه به ماهیت بین المللی جرایم رایانه ای، هماهنگی قوانین و تکنیک های ملی در مبارزه با جرایم رایانه ای بسیار حیاتی است. با این حال، هماهنگ سازی باید در حیطه ظرفیت و توانایی منطقه ای نظر گرفته شود پاهمیت جنبه های منطقه ای در اجرای استراتژی های مبارزه با جرایم رایانه ای با این واقعیت که بسیاری از استانداردهای قانونی و فنی که در میان کشورهای صنعتی به توافق رسیده اند و جنبه های مختلف مهم برای کشورهای در حال توسعه را شامل نمی شود، مورد تاکید قرار گرفته است. بنابراین، عوامل منطقه ای و تفاوت ها باید در اجرای آن ها در جای دیگر گنجانده شوند.

۳) ارتباط مسائل جرایم رایانه ای در ستون های امنیت سایبری

دستور کار امنیت سایبری جهانی هفت هدف اصلی استراتژیک دارد که در پنج حوزه کاری ساخته شده است: ۱) اقدامات قانونی و رویه ای ۲) مقررات فناورانه و رویه ای ۳) ساختارهای سازمانی ۴) ظرفیت سازی ۵) همکاری بین المللی.

همانطور که در بالا اشاره شد، مسایل مربوط به جرایم رایانه ای نقش مهمی در هر پنج ستون در دستور کار امنیت سایبری جهانی ایفا می کنند. در بین این حوزه های کاری، "اقدامات قانونی" بر روی چگونگی رسیدگی به چالش های قانونی مطرح شده توسط فعالیت های جنایی بر روی شبکه های ICT در یک روش سازگار بین المللی متمرکز است.

گفتار دوم) تبیین یک سیاست جنایی سایبری به عنوان نقطه شروع

قوانین درحال توسعه برای جرم انگاری رفتار خاص یا معرفی ابزارهای تحقیقاتی برای اکثر کشورها یک فرآیند نسبتا غیر معمول است. روند عادی برای معرفی یک سیاست اولویت دارد. یک سیاست قابل مقایسه با یک استراتژی است که ابزارهای مختلف مورد استفاده برای رسیدگی به این مساله را تعریف می کند. بر خلاف استراتژی کلی تر جرایم رایانه ای که ممکن است به ذینفعان مختلف رسیدگی کند، نقش سیاست، تعیین پاسخ عمومی دولت به یک مساله خاص است. این واکنش لزوما به قانون محدود نمی شود چون دولت ها ابزارهای مختلفی دارند که می توانند برای رسیدن به اهداف سیاست استفاده شوند. و حتی اگر این تصمیم گرفته شود که نیاز به اجرای

قانون وجود دارد، لزوما نیازی به تمرکز بر قانون جزایی نیست، بلکه می تواند شامل قوانینی نیز باشد که بر پیش گیری از جرم متمرکز هستند. در این رابطه، توسعه یک سیاست، دولت را قادر می سازد تا به طور جامع واکنش دولت به یک مشکل را تعریف کند. همانطور که مبارزه علیه جرایم رایانه ای نمیتواند تنها ی تواند محدود به معرفی قانون باشد، بلکه شامل استراتژی های مختلفی با مقررات مختلف است، این سیاست می تواند تضمین کند که این مقررات متفاوت باعث بروز اختلاف نمی شوند. در رویکردهای مختلفی برای هماهنگی قوانین جرایم رایانه ای اولویت کمی به تنها ایجاد قوانین در چارچوب قانونی ملی داده شده بلکه ان رابه یک سیاست موجود، یا توسعه چنین سیاستی برای اولین بارشامل میکند.در نتیجه برخی از کشورها که صرفا قوانین مبارزه با جرایم رایانه ای را بدون ایجاد استراتژی مبارزه با جرایم سایبری و همچنین سیاست هایی در سطح دولتی معرفی کردند با مشکلات جدی مواجه شدند. آن ها عمدتا ناشی از فقدان تدابیر پیش گیری از جرم و هم پوشانی میان تدابیر مختلف بودند.

۱) مسئولیت دولت

این سیاست سازگاری توانایی ها برای یک موضوع درون دولت را ممکن می سازد. همپوشانی بین وزارتخانه های مختلف هیچ چیز غیر عادی نیست – با توجه به جرایم رایانه ای که به کرات اتفاق می افتد چون این یک موضوع میان رشته ای است.

جنبه های مربوط به مبارزه علیه جرایم رایانه ای ممکن است مربوط به دستور وزارت دادگستری، وزارت ارتباطات یا وزارت امنیت ملی برای نام تنها سه مورد باشد. در فرآیند توسعه یک سیاست، نقش نهاده ای مختلف دولتی درگیر می تواند تعریف شود. برای مثال، این موضوع در پیش نویس سیاست مدلPAC۴ ICB۸۹۳ برای جرم سایبری بیان شده است.

در این زمینه مهم است که مسئولیت های سهامداران مختلف به وضوح تعریف نشده باشد این موضوع به خصوص به این دلیل مرتبط است که جرم سایبری یک موضوع بخش متقاطع است که ممکن است مربوط به احکام نهاده ای مختلف مانند دادستان عمومی، وزارت ارتباطات و غیره باشد.

۲) مدل های سیاست جنایی سایبری

همانطور که در بالا اشاره شد، می توان از سیاست برای تعریف اجزای مختلف رویکرد استفاده کرد. این می تواند از تقویت ظرفیت های سازمانی (به عنوان مثال پلیس و تعقیب) به اصلاحات عینی قانون (مانند معرفی قوانین پیشرفته تر)باشد. این موضوع دیگری است که در پیش نویس سیاست مدل PAC ۴ ICB برای جرم سایبری بیان شده است:

پرداختن به چالش های چند بعدی مبارزه، نیازمند رویکردی جامع است که باید شامل سیاست های کلی، قانونگذاری، آموزش و آگاهی، افزایش ظرفیت، تحقیق و نیز رویکردهای تکنیکی باشد. به طور ایده آل سیاست باید برای هماهنگ کردن فعالیت های مختلف مورد استفاده قرار گیرد – حتی اگر آن ها توسط وزارتخانه های مختلف و نهاده ای دولتی اجرا شوند. این حقیقت که

سیاست ها به طور کلی نیازمند تایید کابینه هستند به همین دلیل نه تنها شناسایی نهاده ای مختلف دولتی و وزارتخانه های دخیل در رابطه با موضوع را ممکن می سازد، بلکه هماهنگی فعالیت های آن ها را نیز ممکن می سازد.

این سیاست نه تنها نهادهای دولتی درگیر بلکه ذی نفعان را نیز شناسایی می کند. برای مثال، ممکن است برای توسعه راهنمایی با توجه به دخالت بخش خصوصی لازم باشد. مساله ذی نفعان که باید درگیر شود و به ان پرداخته شود، برای مثال، در پیش نویس سیاست مدل ICB ۸۹۶PAC۴ برای جرم سایبری بیان شده است:

افزون بر آن، چنین رویکردی باید شامل ذی نفعان مختلفی نظیر دولت، وزارتخانه ها و ادارات دولتی، بخش های خصوصی، مدارس و دانشگاه ها، رهبران عرفی، جامعه، قضات، گمرکات، دادستان ها، وکلا، جامعه مدنی و سازمان های غیردولتی باشد.

۳) شناسایی معیارها

همانطور که در ادامه تاکید شد، اهمیت هماهنگ سازی قانون به عنوان یک اولویت کلیدی توسط سازمان های منطقه ای مختلف شناسایی می شود. اما نیاز به هماهنگ سازی محدود به قانون نیست – شامل مسائلی مانند استراتژی و آموزش متخصصان می شود. سیاست می تواند برای شناسایی مناطقی مورد استفاده قرار گیرد که در آن هماهنگی باید انجام شود و استانداردهای منطقه ای و / یا بین المللی را تعریف کند که باید اجرا شوند. اهمیت هماهنگ سازی برای مثال در سیاست مدل پیش نویسICB ۸۹۹PAC۴ برای جرم سایبری بیان شده است. با توجه به ابعاد جهانی جرم سایبری و نیز نیاز به حفاظت از کاربران اینترنت در منطقه از تبدیل شدن به قربانی جرم سایبری، اقداماتی برای افزایش توانایی مبارزه با جرم سایبری باید اولویت بالایی داشته باشد. استراتژی ها و به خصوص قانونگذاری که برای رسیدگی به چالش های جرم سایبری توسعه یافته است باید در یک طرف با استانداردهای بین المللی باشد و از طرف دیگر، نشان دهنده یگانگی حوزه باشد.

یک مثال دیگر، سیاست جنایی مدل HIPCAR در جرم سایبری است.

مقرراتی وجود دارند که رایج ترین استانداردهای پذیرفته شده بین المللی جرم سایبری و همچنین جرایمی است که منافع خاص برای منطقه دارند (مانند اسپم) برای اطمینان از توانایی هم کاری با سازمان های مجری قانون از کشورها در منطقه و نیز خارج از منطقه، این قانون باید با استانداردهای بین المللی و بهترین تجارب و نیز (حداکثر تا حد ممکن) با استانداردهای منطقه ای موجود و بهترین تجارب سازگار باشد.

۴) تعریف موضوعات کلیدی برای قانونگذاری

سیاست می تواند برای تعریف حوزه های کلیدی که باید توسط قانون مورد بررسی قرار گیرند، مورد استفاده قرار گیرد. این امر می تواند شامل فهرستی از جرایمی باشد که باید پوشش داده

شوند. سطح جزییات می تواند به جزییات قانونی که باید در قانون جرایم رایانه ای گنجانده شوند، کاهش یابد.

یک نمونه، تاثیر سیاست جنایی مدل HIPCAR بر روی جرم سایبری است.

باید یک تدارک برای تولید تعمدی و غیر قانونی، فروش و اقدامات مرتبط با پورنـوگرافی کـودک، وجود داشته باشد.

به خصوص در این زمینه، استانداردهای بین المللی باید در نظر گرفته شوند. این قانون باید عـلاوه بر جرم انگاری پورنوگرافی کودکان و دسترسی به وب سایت های پورنوگرافی به کودکان، پوشـش داده شود. معافیت که نهادهای انتظامی را قادر می سازد تـا تحقیقـات را انجـام دهنـد بایـد مـورد استفاده قرار گیرند.

۵) تغییر، بروزرسانی و اصلاحات در تعریف چارچوب های قانونی

وارد کردن قوانین جرایم رایانه ای یک کار ساده نیست چون مناطق مختلفی هستند که بـه مقـررات نیاز دارند. علاوه بر قانون جزا و قانون رویه ای، قوانین جرایم رایانه ای ممکن است شامل مسـائل مربوط به همکاری بین المللی، شواهد الکترونیکی و مسیولیت یک عرضه کننده خـدمات اینترنتـی (ISP)باشد. در اکثر کشورها چنین قانونی ممکن است وجود داشته باشـد – اغلـب در چـارچوب های قانونی متفاوت. مفاد مربوط به جرایم رایانه ای لزوما باید در یک قانون واحد اجرا شـوند. بـا توجه به ساختارهای موجود، ممکن است لازم باشد بخـش هـای مختلـف قانونگـذاری را بـه روز رسانی کنیم (مانند اصلاح قانون شواهد برای اطمینان از اینکه قابل اجرا با توجه به مقبولیت مدارک الکترونیکی در جریان دادرسی جنایی) یا از بین بردن مفاد قانون قدیمی تر (بـرای مثـال در قـانون ارتباطات) در فرآیند معرفی قوانین جدید است.

این رویکرد اجرای قانون جرایم رایانه ای به وسیله فرآینـد احتـرام بـه سـاختارهای موجـود قطعـا چالش برانگیزتر از اجرای یک استاندارد منطقه ای یا بهترین کلمه عمل بین المللی است که در یک قطعه مستقل از قانون عمل می کند. اما با توجه به این واقعیت که این روند سفارشی کـردن اجـازه حفظ سنت قانونی ملی را می دهد، بسیاری از کشورها از چنین رویکردی بهره می برنـد. سیاسـت می تواند برای تعریف اجزای مختلف مورد استفاده قرار گیرد که باید با هم ادغام شـوند و قـوانین موجود را شناسایی کنند که به به روز رسانی ها نیاز دارند.

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال سوم، شماره چهارم (پیاپی ۱۲)، زمستان ۱۳۹۹

نتیجه گیری

در راستای تبیین یک ساختار تقنینی جامع در مقابله با جرایم سازمان یافته سایبری در عرصه بین المللی و مطابق آنچه فوقاً معروض گردید ساختار مبنایی بین المللی متقنی در این خصوص وجود ندارد و رهیافت های ابرازی در این باب جملگی مبتنی بر یک سلسله فرآیندهای محدود منطقه ای یا کلیات عام بین المللی است که در آنها به نحود اختصاصی به ارائه راهکارهایی جهت ترسیم یک سازوکار جهانی پرداخته نشده است.

در عرصه بین المللی تبیین ساختار تقنینی واحد در جهت سوق دادن کشورها و دولت ها به همراهی در جهت پیروی از یک مدل واحد جهانی با عنایت به تفاوت های ساختاری، ایدئولوژیک، اجتماعی، سیاسی، مذهبی، فکری و اقتصادی همواره مواجه با ایرادات جدی بوده است و شیوه های اجرایی واحدی را نمی توان در این خصوص بر کشورها تحمیل نمود چه آنکه برخی دولت ها با لحاظ ساختارهای داخلی خویش و با بهانه های حفظ استقلال و حاکمیت ملی خویش از تن دادن به یک نظام تقنینی جامع بین المللی خودداری می ورزند چه آنکه در مواردی همانطور که پیشتر گفته شد برخی اشکال جرایم سازمان یافته سایبری با حمایت های دولت ها و علیه منافع دول دیگر به وقوع می پیوندد و بر این اساس پیروی از یک ساختار تقنینی واحد در جرم انگاری و مقابله با این دسته از جرایم چندان مقبول دولت ها نیست و حتی مغایر منافع و اقدامات ایشان و محدود کننده آنهاست. در چنین شرایطی گرایش دولت ها به پیروی از چنین احکام و مقررات محدود کننده ای مواجه با مقابله و معارضه جدی است که نافی منافع آنهاست و چون پذیرش این موازین بین المللی موجب پذیرش متفرعات آن و محدودیات ها مجازات های پیش بینی شده در مقابله با این دسته از جرایم می شود لذا در مسیر نیل به یک سیاست جنایی تقنینی بین المللی همواره با کارشکنی هایی مواجه شده ایم.

با این تفاسیر بر خی مقرره های عام و احکام تقنینی منطقه ای خصوصاً رهیافت های و رهنمودهای تقنینی منبعث از کنوانسیون جرایم سایبری اتحادیه اروپا مشهور به کنوانسیون بوداپست و به تعبیری ترسیم زیرساخت های آن به عنوان یک الگو و نمونه تقنینی در ترسیم سیاست های تقنینی سایبری بسیاری از کشورها و از جمله کشور ما موثر بوده است لکن تمام این موارد صرفاً در باب مقابله با جرایم معمول سایبری و نه جرایم سازمان یافته سایبری مطرح شده اند و در بسیاری موارد مواجه با خلاءهای متعدد قانونی می باشیم که منبعث از ضعف مقررات اجرایی متحدالشکل در مقابله با این دسته از جرایم هستند و نهایتاً از موازین عام مورد اشاره در برخی کنوانسیون های بین المللی مقابله با جرایم سازمان یافته به معنای عام چون پالرمو و مریدا اشاره می شود و از مقرره های آنها با لحاظ محدودیت های پیش بینی شده از حیث موضوع و صلاحیت احکام کلی مقابله با جرایم سامان یافته سایبری استفاده می شود؛ که این موارد جملگی موید ضرورت توجه به تبیین یک نظام تقنینی جامع بین المللی در مقابله با این دسته از جرایم با لحاظ شیوع و گسترش و اثرگذاری روزافزون آنهاست.

منابع

۱. پور قهرمان بابک، ***سیاست جنایی ایران در قبال جرایم رایانه ای در پرتو اسناد بین المللی***، رساله دکتری، دانشگاه آزاد اسلامی واحد خوراسگان، به راهنمایی دکتر قدرت الله خسروشاهی، ۱۳۹۲

۲. جلالی قراهانی، امیر حسین، ***کنوانسیون جرایم سایبری و پروتکل الحاقی آن***، چ اول، تهران، خرسندی، ۱۳۸۹.

۳. حاجی ده آبادی، احمد، سلیمی ، احسان، ***اصول جرم انگاری در فضای سایبر(با رویکردی انتقادی به قانون جرائم رایانه ای)***، مجلس و راهبرد سال بیست و یکم زمستان، شماره ۸۰، ۱۳۹۳.

٤. زررخ، احسان، ***جرم مخابراتی***، مجله حقوقی دادگستری، شماره ۶۹، ۱۳۸۹.

٥. زررخ، احسان؛ ***جرم شناسی فضای مجازی***، به راهنمایی دکتر علی‌حسین نجفی ابرندآبادی، رساله کارشناسی ارشد؛ ۱۳۸۹ ش.

٦. کاظمی، قباد، ***حقوق کیفری عمومی و تحولات ناشی از جرایم سازمان یافته***، نشر جنگل جاودانه، تهران، ۱۳۹۷.

۷. Brenner, w.s, Organized Cybercrime-How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina Journal of Law & Technology, Volume ٤, Issue ١: Fall ٢٠٠٢

۸. Council for Security Cooperation Asia and Pacific, ٢٠٠٤, 'Cybercrime and its Effects on the Asia Pacific Region: Report of the Transnational Crime Working Group', August ٤, at http//www.police.govt.nz/events/٢٠٠١/ecrimeforum/cybercrime_and_its_effects.html.

۹. Council of Europe (٢٠٠٤). Organised crime situation report: Focus on the threat of cybercrime.Europol (٢٠٠٦). Organised Crime Threat Assessment.

۱۰. Csonka, P. ٢٠٠٥, 'The council of Europe Convention on Cybercrime: A Response to the challenge of the New Age?', in R. Broadhurst and P. Grabosky, eds. CyberCrime: The Challenge in Asia, University of Hong Press.

۱۱. cyber law simplified; indianinformation technology Act (٢٠١٥)

۱۲. Esposito, G. ٢٠٠٤ 'The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument?', in Broadhurst, R. Ed, Proceedings of the ٢nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong.

۱۳. Global alliance on Transnational Organised Crime, Hong Kong Police: Printing Department HKSAR.

۱۴. Grabosky, P. and R. Broadhurst ٢٠٠٥, 'The Future of Cyber-Crime in Asia', in R. Broadhurst and P. Grabosky, eds. Cyber-Crime: The Challenge in Asia, University of Hong Press.

۱۵.Korean Institute of Criminology, ۲۰۰۵, ‘Workshop ٦ ‘Measures to Combat Computer-related Crime’, ۱۱th UN Congress on Crime Prevention, Bangkok, April ۲۲-۲۳, ۲۰۰۵ with UN Office Drugs and Crime.

۱۶.Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from ۱۰ to ۱۳ April ۲۰۱۷

۱۷.Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, ۱۹ April ۲۰۱۰

۱۸.The Commission on Crime Prevention and Criminal Justice, Resolution ۲۲/۷, Strengthening international cooperation to combat cybercrime

۱۹.The Commission on Crime Prevention and Criminal Justice, Resolution ۲۲/۸,Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime

۲۰.UNODC Comprehensive Study on Cybercrime, February ۲۰۱۳.

۲۱.US-China bilateral agreement,۲۰۱۱ Council of Europe ۲۰۰۱ Convention of Cyber Crime, Asia-Pacific Economic Cooperation (APEC) Cyber Security Strategy of ۲۰۰۲ et al.