Journal iranian political sociology

Vol. 4, No.3, fall2022

https://dx.doi.org/10.30510/psi.2022.299725.2131

National and Transnational Legislative Strategies to Combat Organized Cybercrime

Abstract

The evolution of cyberspace in recent years and its pervasive expansion and the tremendous impact this environment has on human life in a way that minimizes the boundary between real-world and cyber-life. The need to pay for new aspects of cyberspace has become inevitable. The evolution of cybercrime and the spread of organized cyber crime groups apart from its various forms make it increasingly necessary to address legal strategies to tackle this transnational criminal phenomenon. In other words, given the limitation of the scope of organized cybercrime and the interference of international organizations and governments with this type of criminal phenomenon, identifying national and transnational legislative measures and strategies against it is particularly important; It can be tackled by other cyber-attackers. Therefore, in the present study, by analyzing the strategies of the United Nations and the Council of Europe, as well as the legislative policies of some governments in the fight against organized cybercrime, and in addition to examining the legal policy of our country against such crimes, it has provided an analysis and analysis of existing strategies. It was determined, therefore, that in order to fully address and prevent organized cybercrime, we need to develop legal criminal policy and take advantage of the practices and actions of other international actors as described in this article to address the gaps and shortcomings of criminal polic to let's get rid of our legacies

Keywords: Criminal Policy, Organized Cybercrime, International Legal System, Cybercrime Law, Islamic Penal Code, Preliminary Study.

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره سوم (پیاپی۱۵)پاییز ۱۴۰۰،صص۳۱۰ -۲۷۸

https://dx.doi.org/10.30510/psi.2022.299725.2131

راهبردهای تقنینی ملی و فراملی در مقابله با جرایم سازمان یافته سایبری

احسان زررخ[۱]

قباد کاظمی[۲]

محمد جواد جعفری[۳]

تاریخ دریافت: ۱۴۰۰/۰۵/۲۲

تاریخ پذیرش: ۱۴۰۰/۰۸/۱۶

چکیده

سیر تحولات فضای سایبر در سالهای اخیر و گسترش لجام گسیخته آن و تأثیرات شگرف این محیط بر زندگی انسان به گونه‌ای که مرز میان زندگی در جهان واقعی و سایبری را به حداقل رسانده است ضرورت پرداخت به جنبه‌های نوین فضای سایبری را اجتناب‌ناپذیر نموده است. تحولات جرایم سایبری و گسترش گروه‌های جرم سازمان یافته سایبری سوای اشکال مختلف آن، پرداختن به راهبردهای تقنینی مقابله با این پدیده مجرمانه فراملی را بیش از پیش ضرروی می‌نماید. به دیگر سخن با توجه به عدم محدودیت قلمرو وقوع جرایم سازمان یافته سایبری و تقابل سازمان‌های بین‌المللی و دولت‌ها با این قسم از پدیده مجرمانه بازشناسی اقدامات و راهبردهای تقنینی ملی و فراملی در برابر آن از اهمیت ویژه برخوردار می‌باشد تا بر اساس آن بتوان با بهره‌گیری از شیوه‌های مقابله سایر کنشگران فضای سایبر با این گونه از جرایم مقابله نمود. بنابراین در پژوهش حاضر با بررسی راهبردهای سازمان ملل متحد و شورای اروپا و نیز سیاست‌های تقنینی برخی دولت‌ها در مقابله با جرایم سازمان یافته سایبری و النهایه بررسی سیاست تقنینی کشورمان در مقابله با این گونه از جرایم به تبیین و تحلیل راهبردهای موجود پرداخته که بر آن اساس مشخص گردید در راستای مقابله جامع و مانع با جرایم سازمان یافته سایبری نیازمند توسعه سیاست جنایی تقنینی و بهره‌گیری از شیوه‌های و اقدامات سایر کنشگران بین‌المللی، به شرح مندرج در این مقاله در صدد هستیم تا با روش تفسیری-کیفی و با مطالعه میدانی بتوان خلاءها و کاستی‌های سیاست جنایی تقنینی خویش را برطرف نمائیم.

واژگان کلیدی: جرایم سازمان یافته سایبری، سیاست جنایی، قانون جرایم رایانه‌ای، قانون مجازات اسلامی، نظام حقوقی بین‌المللی،مطالعه تطبیقی.

[۱] دانشجوی دوره دکتری،گروه حقوق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه،ایران.

[۲] استاد حقوق جزا و جرم شناسی ، گروه حقوق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه،ایران(نویسنده مسئول) آدرس ایمیل: gh.kazemi@iauksh.ac.ir

[۳] گروه حقوق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران.

مقدمه

جرایم سایبری سالهاست به موضوعی حائز اهمیت در میان ملت‌ها و دولت‌ها بدل شده است که این مهم در کنار توسعه روزافزون فضای سایبر و گسترش حضور اشخاص اعم از حقیقی و حقوقی در این فضا و به تعبیری وابستگی روبه رشد زندگی واقعی به فعالیت‌های فضای سایبری زمینه‌های گسترش جنبه‌های مثبت و منفی این محیط را نیز سبب شده است به‌گونه‌ای که در کنار افزایش تأثیرات مثبت بر زندگی مردم، جنبه‌های منفی و بزهکارانه نیز توسعه یافته است که در این راستا و با توجه به منافع مالی سرشار و ساختار خاص فضای سایبر و همچنین سامانه‌های حفاظتی در برابر مجرمان سایبری و نیز حضور مؤثر دولت‌ها در قالب پلیس‌های سایبری در این محیط زمینه‌های توسعه جرایم سازمان یافته سایبری را فراهم آورده است که البته این شیوه اقدامات مجرمانه نیز در دو دسته کلی نمود پیدا کرده که شیوه اول فعالیت‌های گروه‌های جرم سازمان یافته سایبری فضای واقعی در فضای سایبر است و شیوه دوم فعالیت گروه‌های جرم سازمان یافته سایبری که در فضای سایبر شکل گرفته اند و نمودی در فضای واقعی ندارند و غالباً منطبق با ساختارهای سنتی گروه‌های جرم سازمان یافته در فضای واقعی و سلسله مراتب و ارکان خاص آنها نمی‌باشند لکن در اجرای اقدامات مجرمانه خویش به‌صورت سازمان یافته و منسجم فعالیت می‌نمایند. این در حالی است که توسعه تراکنش‌های مالی هنگفت در فضای سایبر و نیز شکل‌گیری پول‌های مجازی چون بیت کوئین و نیز توسعه زیرساخت‌های مجرمانه فضای سایبر در قالب شبکه تاریک[4] فعالیت‌های جنایی سازمان یافته در فضای سیابر را گسترش داده است. البته در خصوصاً وجود جنبه‌های مختلف جرایم سازمان یافته و بحث‌های ثبوتی و اثباتی آن و به تعبیری امکان سنجی تحقق جرایم سازمان یافته سایبری مباحث مختلفی مطرح شده است که خارج از موضوع این پژوهش می‌باشد چراکه در این نوشتار به دنبال تبیین سیاست جنایی در مقابله با جرایم سازمان یافته سایبری و تبیین شیوه‌های متخذه از سوی کشورها و سازمان‌های بین‌المللی در مقابله با این دسته از جرایم هستیم.

۱) امکان سنجی وقوع جرایم سازمان یافته سایبری

بحث پیرامون وقوع جرایم سازمان یافته سایبری مدت‌هاست که آغاز شده و صاحب‌نظران بسیاری در این خصوص به نگارش مقالات علمی همت گمارده‌اند[5] و در آنها به بیان دیدگاه‌های خویش در این خصوص پرداخته‌اند؛ این دیدگاه‌ها را می‌توان در سه دسته کلی طبقه‌بندی نمود که در این قسمت به بررسی و تبیین آنها خواهیم پرداخت و عبارتند از:
۱. سازمان یافتگی مطلق جرایم سایبری؛ ۲. عدم سازمان یافتگی جرایم سایبری؛ ۳. سازمان یافته بودن برخی از جرایم سایبری.

۱-۱) سازمان یافتگی مطلق جرایم سایبری

در رابطه با جرایم سایبری دیدگاه‌های متفاوتی عنوان شده است، عده‌ای ابراز داشته‌اند که این جرایم مطلقاً سازمان یافته هستند و پذیرش جرم سایبری سازمان نیافته برای ایشان قابل تصور نیست. به دیگر سخن این گروه با توجه به نوع و ماهیت جرایم سایبری امکان انجام آنها را به وسیله یک نفر قابل تحقق نمی‌دانند و معتقدند که انجام جرایم سایبری

[4] Dark Web

[5] اهم این منابع در فهرست مآخذ انتهایی مورد اشاره قرار گرفته‌اند.

نیازمند حدی از سازمان یافتگی است. در همین راستا ادعا شده است که "جرایم موجود سایبری ملاحظاتی را برای ما به وجود می‌آورند که سازمان یافته بودن یکی از جنبه‌های جرم در بُعد مجازی و جنبه عمده آن است." (Nisbett, C, 2002) در تأیید این نظر بیان گردیده که جرایم سایبری که در شبکه جهانی اینترنت به وقوع می‌پیوندند نیازمند یک کار تیمی و سازمان یافته هستند؛ مانند ایجاد سایت‌های مستهجن که با توجه به ساختار آنها و نیاز مبرم به تهیه محتویات غیرمجاز، بارگذاری، تنظیم ترافیک سایت و... از عهده یک نفر خارج می‌باشند؛ مثال بارز در این خصوص دیدگاهی است که واحد جرایم سازمان یافته سایبری سپاه پاسداران انقلاب اسلامی[۶] در متلاشی ساختن سایت‌های مستهجن مطرح کرده بود. این نیرو پس از دستگیری عوامل این سایت‌ها دریافته بود که ساختار غالب این سایت‌ها مبتنی بر کار تیمی و به تعبیر این واحد، سازمان یافته و با برنامه‌ریزی قبلی بوده است. البته نکته ظریفی در این میان وجود دارد که در غالب این سایت‌ها فعالیت اولیه گاهاً از سوی یک نفر صورت می‌پذیرد و سپس از طریق عضوگیری و تشکیل فضای مشارکت و ارائه امکانات به اعضاء آنها را در تأمین محتویات سایت دخالت می‌دهند؛ از این‌رو اداره این قبیل سایت‌ها صرفاً مبتنی بر مشارکت‌های جمعی است بدون آن‌که لزوماً هماهنگی و ارتباط طبقاتی میان اعضاء وجود داشته باشد و به تعبیری فاقد ویژگی‌های جرایم سازمان یافته است. از طرفی در جرایم سایبری نیز امکان ارتکاب جرم به‌صورت انفرادی و بدون مشارکت با دیگر افراد و به تعبیری سازمان دادن یک گروه تبهکار، قابل تصور است؛ نمونه بارز در این خصوص اقدامات مارک میتنیک در ورود به سایت‌های مختلف و تخلیه اطلاعات آنهاست(زررخ، ۱۳۸۸: ٤٣٧) با این وصف به نظر می‌رسد که دیدگاه‌های ارائه شده در خصوص اطلاق انطباق وصف سازمان یافتگی بر جرایم سایبری فاقد وجاهت علمی است و نمی‌توان به‌طور مطلق جرایم سایبری را سازمان یافته دانست.

۲-۱) عدم سازمان یافتگی جرایم سایبری

در مقابل دیدگاه پیش گفته که مطلقاً جرایم سایبری را سازمان یافته تلقی می‌کردند، دیدگاه دیگری مطرح گردید که با توجه به ساختار فضای سایبر امکان سازمان یافتگی را در جرایم سایبری ناممکن می‌دانست. در همین راستا استدلال شده است که: "صرف نوع و طبیعت فضای سایبر با سلسله مراتب نمی‌خواند، فضای سایبر یک شبکه است و یا درست‌تر بگوییم شبکه‌ای از شبکه‌هاست؛ شبکه‌ها عریض، پراکنده، متحرک و توسعه یافته هستند، لکن سلسله مراتب‌ها که در گروه‌های جرم سازمان یافته یکی از ارکان اساسی می‌باشند عمودی، متمرکز، محکم و ثابت هستند." (Nisbett, C, 2002)

علاوه بر این عنوان شده است که "ویژگی‌های فضای سایبر-که بی‌ثباتی، فقدان قید و بند تجربی، محیط منتشر شده، متحرک و باز می‌باشد-نشان می‌دهد که ساختارهای سلسله مراتبی نه تنها در آن، مورد نیاز نیستند بلکه اقتضایی هم در فعالیت‌های مرتبط با فضای سایبر ندارند." (Brenner, 2002:39)

این دیدگاه‌ها به‌گونه‌ای مطرح شده‌اند که ساختار افقی فضای سایبر را دلیلی بر عدم امکان تحقق جرایم سازمان یافته می‌دانند، چرا که از منظر ایشان در فضای سایبر امکان طراحی یک ساختار سلسه مراتبی غیرهمسطح وجود ندارد. این

---

[۶] جهت اطلاعات بیشتر در این خصوص به آدرس اینترنتی www.gerdab.ir رجوع نمائید.

ایراد عنوان می‌شود که در نظامات الکترونیکی دولتی در فضای سایبر که در قالب دولت‌های الکترونیکی مطرح می‌شوند، ساختار سلسله مراتبی ترسیم گردیده و در این نظامات تبعیت میان سلسله مراتب اداری وجود دارد؛ به دیگر سخن رابطه رئیس و مرئوسی وجود داشته و افراد در سطوح مختلف مکلف به تبعیت از طرف بالادستی خود هستند. با این حال، آیا می‌توان این ساختار سلسه مراتبی دولتی را با ساختار سلسله مراتبی موجود در گروه‌های جرم سازمان یافته منطبق دانست و از آن وحدت ملاک گرفت؟ به نظر چنین امری خلط مبحث است و نمی‌توان این دو را با یکدیگر مقایسه نمود، چرا که در نظام سلسله مراتبی اداری که در دولت‌های الکترونیک نیز مطرح هستند، نوعی نظام افقی با محدودیت‌های دسترسی وجود دارد و نه نام سلسله مراتبی و در این ساختار تمامی ارکان در کنار یکدیگر قرار دارند و تنها سطوح دسترسی و تأیید اقدامات در آنها پیش‌بینی شده است. به عبارت دیگر در روشی که به اتوماسیون اداری معروف است، مقام بالادستی می‌تواند اقدامات افراد پائین دستی را مورد نظارت قرار داده و آنها را تأیید یا اصلاح کند و از سویی حدود دسترسی‌ها نیز به فراخور میزکار (کارتابل) آنهاست و حتی در این سیستم نیز محدودیت‌هایی وجود دارد و یک ساختار سلسله مراتبی به معنای آنچه در گروه‌های جرم سازمان یافته مدنظر است، وجود ندارد. به‌عنوان مثال در دسترسی‌های معمول اداری در بسیاری موارد حتی ریاست آن اداره دولتی به کارتابل اداره حراست یا امورمالی احاطه ندارد و نمی‌تواند در آن بخش‌ها وارد شود و تنها می‌تواند به تأیید یا رد اقدامات آنها آن هم پس از طی مراحل و تشریفات اداری اقدام کند. این در حالی است که در نظامات سلسله مراتبی گروه‌های جرم سازمان یافته رئیس گروه مجرمانه احاطه کامل بر تمامی عناصر تحت سیطره خود دارد.

به نظر می‌رسد که این ایراد را نمی‌توان وارد دانست و باید قائل به آن شد که ساختار فضای سایبر پذیرای ساختاری سلسله مراتبی نیست، چرا که این محیط از گروه‌های همکار[۷] سلول مانند تشکیل شده است و در آن امکان برقراری روابط سلسه وار قابل تصور نیست و از این‌رو ساختار سلسله مراتبی در گروه‌های مجرمانه نیز محقق نمی‌شود و اعضای این گروه‌ها در فضای سایبر به مانند آنچه که در فضای واقعی مطرح است، در طول یکدیدگر قرار نمی‌گیرند، هرچند که نوعی از روابط رئیس و مرئوسی در میان آنها دیده می‌شود. لازم به ذکر است که ساختار نوین حاکم بر گروه‌های جرم سازمان یافته اصولاً با خصیصه سلسله مراتبی انطباق ندارد و اکنون این گروه‌ها و حتی گروه‌های موجود در فضای واقعی در حال خروج از قواعد ناظر بر سلسله مراتبی و عمودی بودن و گرایش به سمت ساختارهای افقی و هم رده هستند. این ویژگی با توجه به امکان ریاست موازی، عاملی در جهت تداوم فعالیت‌های گروه در زمان از میان رفتن رؤسای اصلی است. در هر حال ترسیم ساختار سلسله مراتبی بر مبنای گروه‌های جرم سازمان یافته موجود در زمان ارائه آن نظریات بوده و همچون بسیاری از تقسیم‌بندی‌های عقلی، حسب شناخت حاصله از جرم سازمان یافته بوده و امری نیست که نتوان خلاف آن را اثبات کرد. بنابراین گروه‌های مجرمانه سازمان یافته سایبری با شکلی جدید و بدون ساختار عمودی در فضای مجازی حضور دارند و از این حیث این دیدگاه نیز قابل پذیرش نیست.

---

[۷] (Grew) گروهی که با یکدیگر کار می کنند.

اما ایراد دیگری که مطرح شده، آن است که حسب اطلاعات موجود در خصوص فضای سایبر و مجرمان سایبری، جرم سایبری یک جرم غیر سازمان یافته است و گروه‌های مجرمان در آن نقشی ایفا نمی‌کنند، (Ibid) چرا که تا مدت ها این‌گونه تصور می‌شد که جرایم سایبری تنها از سوی هکرها که غالباً افرادی منزوی و گوشه‌گیر هستند و علاقه‌ای به حضور در گروه‌های مختلف و از جمله گروه‌های مجرمان سازمان یافته ندارد، ارتکاب یافته است. زیرا ایشان به لحاظ خصوصیات شخصیتی خاص خود، خلقیات دنباله‌رو ندارند و دستورپذیر نمی‌باشند، از ای‌نرو توانایی حضور در گروه‌های مجرمان سازمان یافته، که نیازمند فرمانبرداری از شخص دیگری به عنوان رئیس است، را ندارند. (زررخ، ۱۳۸۸: ٤٢٥)

البته این استدلال ناشی از مقدمات و پیش فرض‌هایی است که نادرستی آنها اثبات گردیده و اکنون مشخص شده است که مجرمان سایبری افرادی منزوی و گوشه‌گیر نیستند و در پاره‌ای موارد مجرمان سایبری افراد کاملاً اجتماعی و برونگرا هستند. از این‌رو این نتیجه نیز صحیح به نظر نمی‌رسد، چرا که از مقدمات ناصحیحی بدست آمده است.

۳-۱) سازمان یافته بودن برخی از جرایم سایبری

بنابرآنچه که در بالا مطرح نمودیم، دو نظریه مطلق‌گرا در باب جرم سازمان یافته سایبری که نفیاً و اثباتاً به اظهارنظر در خصوص این نوع از جرایم می‌پردازند، فاقد جنبه علمی لازم هستند. با این وصف به نظریه دیگری می‌رسیم و آن سازمان یافته بودن برخی از جرایم سایبری است. در این دیدگاه جرایم سایبر به فراخور گروه‌هایی که آنها را انجام می‌دهند به دو دسته قابل تقسیم‌اند: ۱. جرایم سازمان یافته سایبری ارتکابی به‌وسیله گروه‌های جرم سازمان یافته فضای واقعی؛ ۲. جرایم سازمان یافته سایبری ارتکابی به وسیله گروه‌های جرم سازمان یافته خاص فضای سایبر.

۱-۳-۱) جرایم سازمان یافته سایبریِ ارتکابی به وسیله گروه‌هایِ جرم سازمان یافته فضای واقعی

پس از بحث پیرامون این موضوع که جرم سازمان یافته سایبری وجود دارد و این مهم واقعیتی انکارناپذیر است. در این قسمت به بررسی حضور گروه‌های جرم سازمان یافته سنتی در فضای سایبر می‌پردازیم. در خصوص حضور این گروه‌های در فضای سایبر، این نظر وجود دارد که: "گروه‌های جرایم سازمان یافته سنتی درخلال فعالیت‌هایشان در جهان واقعی تحول پیدا کرده‌اند و حال به جهت ورود انسان‌ها به فضای سایبر، گروه‌های جرم سازمان یافته سنتی نیز به دنبال سایرین به این محیط قدم نهاده‌اند."(Brenner, 2002:24)

بر مبنای این دیدگاه که تا حدود زیادی منبعث از نظریه جرم شناسانه انتقال فضاست مفاهیم جرم، مجرم و بزه‌دیده از فضای واقعی به فضای سایبر منتقل شده‌اند، اما تغییر فضا و وجود شرایط خاص حاکم بر فضای سایبر موجب شکل‌گیری جرایم، مجرمان و بزه‌دیدگان خاص این فضا شده است که تا حدودی با همتایان فضای واقعی خویش متفاوت‌اند. (زررخ، ۱۳۸۹: ۱۱۸-۱۱۷)[۸]

---

[۸] جهت آگاهی از فرضیات این نظریه و استدلال‌های آن ر.ک به: زررخ، احسان؛ *جرم‌شناسی فضای مجازی*، رساله کارشناسی ارشد، ۱۳۸۹، صص ۱۱۸-۱۱۷.

در همین راستاست که استدلال شده است "جرم سازمان یافته کاملاً برای بهره‌گیری از فضای سایبر مناسب است." (Olson, J. L, 2004) چرا که تأکید این نظر بیشتر بر نوآوری، سازگاری‌های اطلاعاتی-عملیاتی و فرار از شناسایی فضای سایبر است که به ابزاری مطمئن برای تسهیل فعالیت‌های گروه‌های جرم سازمانه سایبری بدل شده است. از این‌رو "انتقال جرایم سازمان یافته از محیط فیزیکی به محیط مجازی امری کاملاً بدیهی است، به این سبب که گروه‌های جرم سازمان یافته همیشه صنایع ویژه‌ای را به‌عنوان هدف اعمال نفوذ ناروای خود انتخاب می‌کنند و در این بین فضای سایبر و گسترش تجارت الکترونیک، که یک سلسله هدف‌های جدید را برای رخنه کردن و اعمال نفوذ فراهم نموده‌اند؛ بهترین گزینه هستند." (Williams, P., 2001:25) مثال بارزی که در زمینه فعالیت گروه‌های سازمان یافته سنتی در فضای سایبر می‌توان مطرح نمود، اقدام مافیای سیسیل در سرقت بودجه ۴۰۰ میلیون دلاری تخصیص یافته از سوی اتحادیه اروپا برای اجرای طرح‌های داخلی سیسیل بود. (Williams, 2001:23) به هرحال، این خود شاهدی از فعالیت‌های بزرگترین سازمان جنایی دنیای واقعی در فضای سایبر است.

از مطالب مشروحه فوق این‌چنین استفاده می‌شود که حضور گروه‌های جرم سازمان یافته در فضای سایبر به دو شکل اصلی تحقق یافته است؛ نخست انجام اقدامات خرابکارانه سازمان یافته در فضای سایبر و دوم استفاده از توانمندی‌های فضای سایبر جهت تسهیل اقدامات مجرمانه در فضای واقعی.

البته به نظر می‌رسد که شیوه دوم کاربردهای بیشتری داشته است و درحال حاضر مهم‌ترین کاربرد فضای سایبر برای گروه‌های جرم سازمان یافته فضای واقعی، کاربرد تسهیل کنندگی است.

نمونه بارز این موضوع در اقدامات تروریستی نمود می‌یابد، هرچند که برخی بر این باورند که تروریسم جزو جرایم سازمان یافته نیست و برخی آن را سازمان یافته می‌دانند، اما باید اظهار داشت که تروریسم ذوجنبتین است و هم می‌توان به‌عنوان جرم سازمان یافته و هم جرم عادی بدان اشاره نمود.[۹] از این‌رو با توجه به این‌که جنبه سازمان یافته تروریسم نیز قابل تصور است و به وقوع پیوسته است، در ادامه به بررسی این دسته از جرایم سازمان یافته سایبری می‌پردازیم، چرا که در بسیاری موارد این گروه‌ها از فضای سایبر به‌عنوان وسیله ارتباطی اطلاع‌رسانی استفاده می‌کنند.

این بهره‌مندی نیز به دو شیوه عمده صورت می‌گیرد: نخست) استفاده از سیستم‌های اطلاع‌رسانی موجود در فضای سایبر به منظور ارتباط میان خود و نیروهای وابسته به خود؛ دوم) استفاده از امکانات اطلاع‌رسانی و انتشاراتی فضای سایبر. چرا که یکی از ویژگی‌های بارز اقدامات تروریستی رسانه‌ای بودن است (جلالی فراهانی، ۱۳۸۵: ۸۹) که امروزه فضای سایبر به‌عنوان رسانهٔ رسانه‌ها آن را به خوبی پوشش می‌دهد و زمینه‌های چنین امری را فراهم می‌کند. این رویکرد در اقدامات گروه‌های تروریستی چون القاعده بسیار نمود یافته و این گروه بسیاری از تصاویر اقدامات تروریستی و اطلاعیه‌های خود را از طریق پایگاه اطلاع‌رسانی خویش در فضای سایبر منتشر می‌کند.

با این وصف فضای سایبر به‌طور خاص و بنابر ویژگی‌هایی که دارد، محیط بسیار مناسبی برای فعالیت‌های تروریستی سازمان یافته است، چرا که:

---

[۹] برای مطالعه نظرات بیشتر در این خصوص ر.ک: محمدابراهیم شمس ناتری، درآمدی بر درک جرم سازمان یافته و مظاهرفرا ملی آن، قابل دسترس در: http://www.alqaza.com/far/index.php?option=com_content&view=article&id=۲۱۶۷---------۱:

۱. بدون مرز بودن فضای سایبر: ماهیت فرامرزی فضای سایبر، آن هم به‌گونه‌ای که هیچ یک از موانع و مرزهای موجود در دنیای فیزیکی در آن ملاحظه نگردد، یک ویژگی اساسی محسوب می‌شود و مزایای بی‌شماری از آن نشأت می‌گیرد.

۲. کاهش هزینهٔ جرم: فضای سایبر هزینهٔ جرم را به‌طور قابل ملاحظه‌ای کاهش داده است. به هنگام محاسبهٔ هزینهٔ جرم دو مؤلفه مورد توجه قرار می‌گیرد: نخست) نتیجه‌ای که عاید می‌شود؛ دوم) احتمال دستگیری و مجازات. مسئلهٔ هزینهٔ جرم برای تروریستها اهمیت بسیار و حتی حیاتی دارد. زیرا جرائمی که مرتکب می‌شوند، مجازاتهای بسیار سنگینی دارند و عملاً امکان رهایی از آنها وجود ندارد. لذا ماهیت فرامرزی فضای سایبر فرصت بسیار مغتنمی برای آنهاست که با وجود دستیابی به اهداف مخرب پیش‌بینی شده، امکان به دام افتادن آنها به حداقل ممکن می‌رسد.

۳. امکان وارد آوردن خسارات مالی، بدون آسیبهای جسمی: اکثر اقدامات تروریستی در دنیای فیزیکی، با آسیب‌دیدگی افراد همراه است که این خود چندان با هدف جلب افکار عمومی و همنواسازی آنها با اهداف تروریستی سازگاری ندارد. زیرا اصولاً آسیبهای جانی، به ویژه اگر با مرگ همراه باشد، حساسیتها و واکنشهای زیادی را برمی‌انگیزد، لذا بدیهی است با وجود انواع اطلاعات ارزشمند مالی و دولتی در فضای سایبر، این فرصت بی‌نظیر ارتکاب جرم، برای تروریستها فراهم شده است.

٤. تأمین راحت امکانات و عوامل مورد نیاز برای اقدامات تروریستی: ماهیت اقدامات تروریستی فیزیکی به گونه‌ای است که برای ارتکاب آنها باید به ابزارهایی متوسل شد که تأمین آنها با مشکلات زیادی همراه است، مانند انواع مواد منفجره. همچنین به دلیل خطرناک بودن این اقدامات و احتمال بالای دستگیری و مجازات، کمتر کسی حاضر می‌شود آن را به انجام برساند. اما فضای سایبر تمامی ابزارهای مورد نیاز برای انواع اقدامات تروریستی سایبری را به‌صورت روزآمد در اختیار همگان قرار داده و البته نحوهٔ به‌کارگیری آنها تا حدی ساده شده که با کمترین مهارت و تجربه می‌توان از آنها استفاده کرد.

۵. انعکاس جهانی موفقیت، مکتوم ماندن شکستها: شاید فناوری اطلاعات و ارتباطات الکترونیکی تنها ابزاری باشد که جهانیان همگی به‌صورت مشترک از آن استفاده می‌کنند. لذا هرگونه اختلال در آن به خوبی انعکاس جهانی دارد و به راحتی اعتبار یک کشور یا مجموعهٔ خاصی در فضای سایبر لکه‌دار می‌شود. به همین دلیل، از آنجا که تروریستها به دنبال انعکاس جهانی اقداماتشان هستند، این فضا می‌تواند بهترین گزینه باشد. با این حال، تا عملی در این فضا مشاهده یا آثار و نتایج آن لمس نگردد، کسی از وقوع آن آگاهی نمی‌یابد، لذا چنانچه این‌گونه اقدامات با شکست مواجه شود و به نتیجهٔ مورد نظر نرسد، عملاً به میزان قدرت و اعتبار تروریستها لطمه‌ای وارد نمی‌شود.

٦. امکان هماهنگی لحظه‌ای در سراسر جهان با ضریب اطمینان بالا: یکی از ابزارهای مورد نیاز و حیاتی تروریستها، وسایل ارتباطی پیشرفته است تا بتوانند در کوتاه‌ترین زمان و با کمترین مشکل از وضعیت یکدیگر آگاه شوند. فضای سایبر این امکان را برای آنها فراهم آورده و آنها می‌توانند با بهره‌گیری از انواع ابزارهای ارتباطات الکترونیکی، مانند پست الکترونیکی، محیط‌های گپ (Chat) و... به شکل مکتوب، صوتی و ویدیویی و به‌صورت زنده با یکدیگر ارتباط داشته باشند. البته مزیت برجستهٔ این ابزارها که امکان به‌کارگیری بهینه را برای گروه‌های تروریستی فراهم می‌آورد،

امکان رمزنگاری (Cryptography) محتوای ارتباطات الکترونیکی با ابزارهای بسیار پیشرفته است که احتمال رمزگشایی (Decryption) آنها را بسیار ضعیف می‌گرداند. به این ترتیب، آنها می‌توانند بدون دغدغه از دستیابی مجریان قانون به محتوای نامفهوم ارتباطاتشان، به راحتی به هماهنگی امور بپردازند. همچنین شیوه‌های نوین استگانوگرافی (Steganography) به تروریستها امکان می‌دهد در لوای پیام های مشروع و غیرمشکوک، اطلاعات راجع به اقدامات تروریستی‌شان را مبادله کنند.

۷. امکان جذب حامیان از سراسر جهان: جلب حمایت جامعه مخاطبان موردنظر و حتی عضوگیری از میان آنها، از جمله اقدامات حیاتی گروه‌های تروریستی محسوب می‌شود. حال با توجه به اینکه فضای سایبر امکانات رسانه‌ای بسیار گسترده‌تر با تأثیرگذاری بسیار بیشتر را با هزینهٔ بسیار ناچیز نسبت به امکانات رسانه‌ای دنیای فیزیکی در اختیار همگان قرار داده است، تروریستها نیز با بهره‌گیری از آنها و ساخت انواع برنامه‌های تبلیغاتی چندرسانه‌ای (Multimedia) به جلب حامی و جذب نیرو می‌پردازند.(همان، ۱۳۸۵: ۹۵-۹۱)

این فعالیت‌ها که اکثراً نشأت گرفته از گروه‌های جرم سازمان یافته فضای واقعی هستند که در فضای سایبر فعالیت می‌کنند، خود مهم‌ترین دلیل بر وجود و فعالیت‌های گروه‌های جرم سازمان یافته سنتی در فضای سایبر هستند؛ گروه‌هایی که در مقام تروریسم سایبری سازمان یافته یا به ارتکاب جرم در فضای سایبر می‌پردازند و یا از ویژگی‌های این محیط به منظور ارتکاب جرایم خود در فضای واقعی بهره می‌گیرند.

۲-۳-۱) جرایم سازمان یافته سایبریِ ارتکابی به‌وسیله گروه‌هایِ جرم سازمان یافته خاص فضای سایبر

خصوصیات منحصربه فرد فضای سایبر منجر شده است تا ضرورت بررسی گروه‌های سازمان یافته خاص فضای سایبر به واقعیتی خدشه ناپذیر بدل شود. چرا که برخی از قواعد راجع به جرم سازمان یافته در فضای واقعی با آنچه در خصوص جرم سازمان یافته سایبری مطرح می‌شود تفاوت دارند. در این میان سه ویژگی قدرت مرکزی، استمرار و توسل به خشونت که در رابطه با جرایم سازمان یافته جهان واقعی مطرح شده‌اند در جرایم سازمان یافته سایبری جایگاهی ندارند.[۱۰] در همین راستا برخی این‌گونه استدلال نموده‌اند که "تشکیلات جنایی آنلاین کمتر بر گرایش به ساختارهای سازمانی طبقه‌بندی شده تأکید دارند و در همان حال بر ساختار زمینه‌ای جنبی و وسیع‌تر تأکید می‌کنند. دلیلی ندارد که تشکیلات جنایی آنلاین در عضوگیری و عملکرد به وسیله مرزهای ملی و محلی و یا تفاوت‌های فرهنگی محدود شوند، زیرا مجرمان سایبری فرهنگی را که از مرزها و قلمرو ملی فراتر رفته است منتشر کرده‌اند. بنابراین درست در مقابل تشکیلات طبقه‌بندی شده، ثابت، محکم و اغلب محلی که فاصله زیادی از ویژگی‌های گروه‌های جنایی منطقه‌ای و حتی جهانی دارند، قرار خواهند داشت." (Brenner, 2002:45)

---

[۱۰] هرچند که به نظر می‌رسد امروزه برخی اوصاف مطروحه در مورد جرایم سایبری همچون وصف استمرار یافتگی در رابطه با جرایم سازمان یافته حتی در جهان مادی و فیزیکی نیز، کاربردی نداشته باشد و گروه‌های جرم سازمان یافته‌ای هستند که در برهه زمانی خاصی برای ارتکاب یک نوع خاص از جرایم ایجاد شده‌اند و پس از مدتی نیز منحل شده‌اند.

در تأئید این دیدگاه که گروه‌های جرم سازمان یافته از ویژگی خشونت که در گروه‌های سازمان یافته سنتی وجود دارد، تبعیت نمی‌کنند، شورای اروپا چنین اظهارنظر کرده است: "جرم سایبری مستلزم نظارت کمتر بر قلمرو جغرافیایی، خشونت و ارعاب کمتر، تماس‌های شخصی و سرانجام ارتباط کمتر و به‌طور خلاصه نیاز کمتری به تشکیلات رسمی وجود دارد." (Council of Europe, 2005)

در تأیید این نکته، لازم به ذکر است که ساختارهای تشکیلاتی و استمرار گروه‌های سازمان یافته دستخوش تغییر شده‌اند و از این‌رو برخی بدین سان اظهارنظر کرده‌اند که: "این ائتلاف‌ها (گروه‌های سازمان یافته سایبری) به نظر ترکیبی از پیشگامان جرم سایبری و گروه‌های فرصت‌طلب با ساختارهای بی‌ثبات و پراکنده (فاقد سلسله مراتب) می‌باشند که دنباله‌رو روش جاری گروه‌های روسی جرم سازمان یافته در محیط واقعی هستند، بدین صورت که به منظور ارتکاب جرم خاصی تبانی می‌کنند و پس از انجام آن منحل می‌شوند." (Brenner, 2002:47)

در دنباله همین نظرات برخی با تکیه بر ویژگی‌های اصیل فضای سایبر و مجرمان سایبری به اثبات وجود گروه‌های سازمان یافته خاص فضای سایبر می‌پردازند و استدلال نموده‌اند که "عناصر درون جرم سایبری و جرم سازمان یافته آنها را تشویق می‌کنند که در هم ادغام شوند. هکرها از نظر سنتی افراد مجرد و ضد اجتماعی بودند که بدون هیچ نوع سودا و تمنای مالی و مادی عمل می‌کردند. حال آن‌که انگیزه‌های آنها از سمت کنجکاوی محض به سوی حملات منفعت طلبانه سوق یافته است و اکنون هکرها اغلب با یکدیگر کار می‌کنند."(Olson, 2004: 15)

با این وصف ذکر این نکته ضروری است که گروه‌های جرم سازمان یافته سایبری در واقع منبعث از خرده فرهنگ‌های مجرمانه موجود در فضای سایبر هستند، چرا که به هرحال فضای سایبر خود مبتنی بر فرهنگ‌های خاص خویش است. مهم‌ترین این خرده فرهنگ‌ها، خرده فرهنگ‌های هکری هستند که در خود گرایش‌های بزهکارانه را نهادینه کرده‌اند؛ هرچند تعداد زیادی از این گروه‌های اقدام به انتشار مرامنامه‌های هکری مختلف نموده‌اند و در آن به گونه‌ای سخن گفته شده که گویی هکرها به یک سری ارزش‌های والای بشری اعتقاد دارند. (زررخ، ۱۳۸۸: ٤٥٣) اما در عمل رفتارهای این گروه‌های موجبات ایراد خسارت به دارایی‌های محترم افراد را فراهم می‌آورد. به گونه‌ای که به‌عنوان مثال سرقت نرم‌افزارها ارزشمند اشخاص حقیقی یا حقوقی از سوی این گروه‌ها و در دسترس عموم قرار دادن آنها موجبات ورود ضرر به ایشان را فراهم می‌کند که خود امری مذموم است. با این تفاسیر و با توجه به جایگاه و اهمیت خرده فرهنگ‌های هکری در شکل‌گیری گروه‌های جرم سازمان یافته فضای سایبری، به نظر می‌رسد که شناخت این خرده فرهنگ‌ها در شناخت جنبه‌های مختلف این گروه‌ها از جایگاه والایی برخوردار باشد، چرا که سنگ بنای بسیاری از گروه‌های جرم سازمان یافته سایبری را خرده فرهنگ‌های هکری موجود در فضای سایبر بنا نهاده‌اند.

علاوه بر این در خصوص تشابه ساختار جرایم سازمان یافته و سایبری، که هر دو به‌طور مخفی و به تعبیر وی زیرزمینی هستند این‌گونه اظهارنظر شده که "بسیاری از صفات مشخصه‌ای که از لحاظ سنتی به جرم سازمان یافته منتسب می‌گردد به هکرها و مجرمان سایبری نیز قابل انتساب است. این تطابق مهارت و انگیزه نوعی پیوند طبیعی بین دو شبکه زیرزمینی را ایجاد کرده است که خود بیانگر نسل جدیدی از جرایم سایبری، یا به تعبیری جرایم سازمان یافته سایبری هستند." (Olson, 2004: 16)

این دیدگاه‌ها، به نظر منطبق با واقعیت فضای سایبر هستند، چرا که بسیاری از مجرمان سایبری به نوعی دچار دگردیسی شده‌اند و با انگیزه‌های مادی به فعالیت‌های خویش می‌نگرند و توانمندی‌های خود را به مثابه ابزاری در راستای کسب منافع مالی می‌دانند. (زررخ، ۱۳۸۹: ۱۱۳)

با این حال پیشرفت‌های دفاعی که در سال‌های اخیر روی داده و توانایی مقابله با هکرها را در میان اعضای جامعه مجازی افزایش داده و به نوعی دولت‌ها نیز به این عرصه بی‌دفاع وارد شده‌اند، همین امر و نیز افزایش آگاهی‌های مردم در خصوص فضای سایبر منجر به دشواری ارتکاب جرایم سایبری شده و سبب گرایش هکرها به روش‌های نوین بزهکاری شده است که در این بین ساختار سازمان‌های جنایی الگوی قابل قبولی را برای این افراد فراهم نمود و با توجه لزوم گرایش به کار گروهی در ارتکاب جرایم سایبری، گرایش به ایجاد سازمان‌های جنایی سایبری افزایش یافته است؛ در همین حال انواع جرایم سایبری خود بر نحوه ارتکاب آنها تأثیر گذاشته است، و برخی به فراخور موضوع خویش با شیوه ارتکاب سازمان یافته هم‌خوانی بیشتری دارند.

این مباحث درحالی مطرح می‌شوند که به عقیده دایره مبارزه با جرایم سازمان یافته مهم در پادشاهی انگلستان[۱۱] "در سال ۲۰۰۶ جرایم سازمان یافته تغییر یافته‌اند و جرم سازمان یافته سایبری در معنای واقعی آن از این سال آغاز شده است." (SOCA, 2006:23)

با این مبانی به نظر می‌رسد که گروه‌های جرم سازمان یافته خاص فضای سایبری واقعیتی انکار ناپذیرند و نمی‌توان وجود و اهمیت این گروه‌های مجرمانه را منکر شد. بنابراین می‌بایست به بررسی دقیق و هدفمند این گروه‌ها پرداخت تا بتوان راهکارهایی برای مقابله با شکل‌گیری و فعالیت آنها ترسیم نمود. در این بین شناخت ویژگی‌های گروه‌های جرم سازمان یافته سایبری مهم‌ترین رکن این بررسی را تشکیل می‌دهد. به نظر می‌رسد که مهم‌ترین ویژگی‌های گروه‌های جرم سازمان یافته خاص فضای سایبر را باید موارد مشروحه ذیل دانست:

۱. سیال هستند و اعضایشان را غالباً تغییر می‌دهند.
۲. برای انجام طرح مجرمانه‌ای به‌صورت جداگانه شکل می‌گیرند و منحل می‌شوند.
۳. از افراد عادی که خطرات زیادی را با دریافت مبالغ اندک می‌پذیرند، تشکیل شده‌اند.
۴. خط مشی‌های مجرمانه را با نگاهی کودکانه می‌نگرند.
۵. غالباً میان گردانندگان اصلی و اعضای عملیاتی ارتباط حضوری وجود ندارد.[۱۲]

به نظر می‌رسد که این ویژگی‌ها ریشه در ویژگی نخستین این گروه‌ها یا همان سیال بودنشان دارد، به‌طوری تغییر مداوم افراد نیز از همین مسئله نشأت می‌گیرد و به تبع بهترین گزینه استفاده از افراد آماتور است؛ هرچند که ممکن است این افراد در کار خود که همانا انجام امور رایانه‌ای است خبره باشند، لکن یک تبهکار حرفه‌ای آموزش دیده، نیستند. همین ضعف دیدگاه‌ها سبب شده تا ایشان نگرشی به اصطلاح کودکانه به امور مجرمانه‌ای که مرتکب می‌شوند داشته باشند،

[11] Serious Organized Crime Agency of The United Kingdom

[۱۲] جهت کسب اطلاعات بیشتر در خصوص این تقسیم‌بندی به آدرس ذیل مراجعه فرمائید:

http://www.dc214.org/notes/june_2005

بنابراین اعمال ارتکابی در اندیشه اکثریت این مجرمان به نوعی شوخی و سرگرمی می‌نماید. در غالب این گروه‌ها نیز افرادی که عنصر مادی جرایم را مرتکب می‌شوند با افرادی که گرداننده واقعی این گروه‌ها هستند ارتباط بی‌واسطه ندارد و از این‌رو شناختی هم از آنان ندارند، لذا نیروهای پلیس را در یافتن گردانندگان اصلی این جرایم با مشکل مواجه ساخته است.

البته این ویژگی‌ها را تنها باید در میان گروه‌های جرم سازمان یافته غیردولتی جستجو نمود و برخی از این ویژگی‌ها در خصوص گروه‌های جرم سازمان یافته سایبری دولتی جایگاهی ندارند. امروزه بحث از جرم سازمان یافته دولتی در میان گروهی از جرم شناسان مطرح شده است و این دیدگاه را در جرایم سایبری می‌توان با قوت بیشتری مشاهده نمود. اهمیت این اعمال تا بدان جاست که در سال جاری میلادی در دولت آمریکا واحدی برای مقابله با این تهدیدات ایجاد شده است. بحث ارتش سایبری[۱۳] که امروزه در منازعات بین‌المللی مطرح و کشورهای چین، آمریکا و روسیه بزرگترین آنها را دارند، در واقع یکی از مهم‌ترین شاخه‌های جرم سازمان یافته سایبری است. چه آن‌که این گروه‌ها که از آنها با نام ارتش سایبری یاد می‌شود، کاری جز ارتکاب جرایم در فضای سایبر به‌صورت سازمان یافته و مختل کردن و نابود ساختن داده‌های زیرساخت های کشور دیگر ندارند. هرچند که در برخی موارد بحث دفاع از حریم داده‌های مجازی یک کشور را نیز به آنها محول می‌کنند، لکن این اعمال به شیوه‌ای کاملاً سازمان یافته از سوی آنها صورت می‌گیرد.

درگیری میان روسیه و گرجستان، پیش از آنکه در فضای واقعی جنگی رخ دهد، نیروهای سایبری روسیه تمامی شبکه بانکی و دولتی گرجستان را مختل کردند و اولین ضربه را بر پیکر این کشور وارد آوردند. (زررخ، ۱۳۸۹: ۸۷)

سوالی که مطرح می‌شود آن است که تمامی اجزای مورد نیاز جرم سازمان یافته سایبری در این اعمال متصور است و دولت‌ها در آنها نقش حامی و گرداننده اصلی را بازی می‌کنند. البته لازم به ذکر است که علاوه بر این روش شیوه رایج دیگری نیز وجود دارد که در آن دولت‌ها با آموزش و تجهیز افراد در کشورهای مختلف، آنها را به ارتکاب جرایم سایبری مطابق خواست خودشان ترغیب می‌کنند؛ این دیدگاه در نظریه گروه مبارزه با جرایم سازمان یافته سایبری سپاه پاسداران انقلاب اسلامی مطرح شده است.[۱۴]

به گونه‌ای که ارتکاب برخی جرایم از سوی افراد خاص در کشور مقصد و با حمایت کشورهای متخاصم صورت می‌گیرد و این امر مصداق بارز جرم سازمان یافته شبه دولتی است و به تعبیری می‌توان آن را از مصادیق جنگ نرم برشمرد. به نظر می‌رسد این دیدگاه خالی از قوت نیست و هیچ نامی جز جرم سازمان یافته سایبری نمی‌توان بر آن نهاد، که در آن محوریت با یک دولت خاص است.

۲) راهبردهای تقنینی بین‌المللی در برابر جرایم سازمان یافته سایبری

---

[13] Cyber Army

[۱۴] برای مشاهده نظر این واحد به آدرس اینترنتی آن به نشانی www.gerdab.ir مراجعه کنید. البته باید باید اذعان داشت که این گروه که در سپاه پاسداران انقلاب اسلامی ایجاد شده و خود را متولی مبارزه با جرایم سازمان یافته سایبری می‌داند، بر مبنای ضوابط قانونی ایجاد نشده و از این حیث تشکیل و فعالیت آن و همچنین اظهارنظرش محل سؤال است. چرا که دامنه فعالیت این گروه در حیطه وظایف پلیس سایبری است.

نظام بین‌المللی متشکل از دولت‌ها و سازمان‌های مختلف که نقش آفرینان عرصه حقوق بین‌الملل کیفری نیز هستند دیدگاه‌ها و رویه‌های مختلفی در برابر جرایم سازمان یافته سایبری وجود دارد که منبعث از ساختارهای حاکمیتی و منافع ایشان است که بر همین اساس و با توجه به ساختار فراملی جرایم سازمان یافته سایبری ناگزیر بخش عمده راهبردهای مقابله با این گونه از جرایم در پروتو اقدامات بین‌المللی و شناخت شیوه های مرسوم برخی کشورهای جهان در این حوزه است.

چندین سازمان بین‌المللی و فراملی، ماهیت ذاتی جرایم رایانه‌ای، محدودیت‌های متعاقب رویکردهای یک جانبه و نیاز به هماهنگ سازی بین‌المللی راه‌حل‌های فنی، قانونی و غیره را شناسایی کرده‌اند. (GOODMAN and BRENNER, 2000, 165) بازیگران اصلی در این زمینه، سازمان هم کاری اقتصادی و توسعه(OECD) ، شورای اروپا، اتحادیه اروپا و اخیراً گروه جی۸ و پلیس بین‌الملل هستند و به علاوه، سازمان ملل، WIPO و GATS نیز نقش مهمی ایفا کرده‌اند. این سازمان‌های بین‌المللی و فراملی به‌طور قابل توجهی به هماهنگ‌سازی قانون جزا و همچنین قانون مدنی و اجرایی در همه نواحی فوق الذکر مربوط به اصلاحات قانون جزایی مرتبط با رایانه، کمک کرده‌اند. (SIEBER, 1998, 33) اولین تحقیق جامع در رابطه با مشکلات قانون کیفری مربوط به جرایم مرتبط با رایانه در سطح بین‌المللی 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 رایانه‌ای اروپا قبول کنند. بنابراین OECD از سال ۱۹۸۳ تا ۱۹۸۵ مطالعه‌ای در مورد امکان هماهنگی بین‌المللی قوانین جنایی برای رسیدگی به جرایم مربوط به رایانه انجام داد. (کتابچه راهنمای سازمان ملل متحد در خصوص پیشگیری و کنترل جرایم مرتبط با رایانه، ۱۹۹٤)

این مطالعه به گزارش سال ۱۹۸٦، در ارتباط با جرایم مرتبط با رایانه انجامید: تحلیل سیاست حقوقی که قوانین و پیشنهادها موجود برای اصلاح را مورد بررسی قرار داده و یک فهرست حداقلی از سو استفاده‌هایی را که کشورها باید به موجب قانون جزا جرم انگاری نمایند، مورد بررسی قرار داد. (همان) از سال ۱۹۸۵ تا ۱۹۸۹ کمیته منتخب متخصصان جرایم مربوط به رایانه شورای اروپا درباره مسائل مطرح شده توسط جرایم رایانه‌ای 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 رایانه‌ای تأکید کرد. در دستورالعمل مجالس ملی برای بررسی افزایش قوانین آن‌ها، پیشنهاد حداقل فهرستی از نامزدهای مورد نیاز برای چنین جرایمی به تصویب رسید و توسط اجماع بین‌المللی مورد پی‌گرد قانونی قرار گرفت و همچنین یک "فهرست اختیاری" که جرائم برجسته در اجماع بین‌المللی را توصیف می‌کند، قابل حصول است. (توصیه نامه شماره ٤ (۸۹) شورای اروپا در مورد جرایم مرتبط با رایانه، ۱۹۹۵) در سال ۱۹۹۰ کنگره سازمان ملل متحد در زمینه پیش‌گیری از جنایت و رفتار متخلفان، مشکلات قانونی جرایم رایانه‌ای را مورد بررسی قرار داد. قطعنامه از کشورهای عضو خواست تا تلاش‌های خود را برای مبارزه با جرایم مرتبط با رایانه با مدرنیزه کردن قوانین ملی خود، بهبود تدابیر امنیتی و ترویج توسعه چارچوب جامع بین‌المللی رهنمودها و استانداردها برای پی‌گیری این جنایات در آینده تشدید کنند.(هشتمین کنگره پیشگیری از جرم و رفتار با مجرمین، سند A/CONF.144/L.11 of 4، ۱۹۹۰)

دو سال بعد، شورای کشورهای OECD و ۲٤ عضو از کشورهای عضو آن توصیه‌هایی برای شورای امنیت سیستم‌های اطلاعاتی به تصویب رساندند که هدف از آن ارائه یک چارچوب امنیتی جدید برای بخش‌های دولتی و خصوصی است. دستورالعمل‌هایی برای امنیت سیستم‌های اطلاعاتی به توصیه ضمیمه شد. این چارچوب شامل قوانین رفتاری، قوانین و اقدامات فنی می‌شود. آن‌ها بر اجرای حداقل استانداردها برای امنیت سیستم‌های اطلاعاتی تمرکز دارند. با این حال، این رهنمودها درخواست می‌کند که کشورهای عضو سیستم کیفری مناسب، اجرایی از دیگر مجازات‌ها برای سوء استفاده و سوء استعمال از سیستم‌های اطلاعاتی ایجاد کنند. (توصیه نامه OECD در مورد دستورالعمل‌های مربوط به امنیت سیستم‌های اطلاعاتی، ۱۹۹۲) در سال ۱۹۹۵ سازمان ملل متحد، مانوئل سازمان ملل متحد در زمینه پیش گیری و کنترل جرم مرتبط با رایانه را منتشر کرد این مانوئل، پدیده جرایم مربوط به رایانه، قانون جزایی اساسی، حفاظت از حریم خصوصی، قانون رویه ای، و نیازها و راه های هم کاری بین‌المللی را مورد مطالعه قرار داد. در همان سال، پلیس بین‌الملل اولین کنفرانس خود را در مورد جرم رایانه‌ای سازماندهی کرد. این کنفرانس تأیید کرد که سطح بالایی از نگرانی در جامعه انتظامی در مورد انتشار جرم رایانه‌ای وجود دارد. بعدا، پلیس بین‌الملل چندین کنفرانس را در همان زمینه برگزار کرد. در آن سال، شورای اروپا توصیه های شماره R95 از کمیته وزرا به کشورهای عضو، در مورد اجبار اصولی که باید دولت‌ها و مقامات تحقیق آن‌ها در حوزه فن‌آوری 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 بین‌المللی را پوشش می‌دهند. (توصیه‌نامه پذیرفته شده شورای اروپا به شماره R95- 13 ، ۱۹۹۵)

در ۲٤ آوریل ۱۹۹۷، کمیسیون اروپا قطعنامه‌ای را در مورد "ارتباط کمیسیون اروپا بر روی محتوای غیرقانونی[15] و زیان‌آور بر روی اینترنت تصویب کرد که از ابتکارات انجام شده توسط کمیسیون و تأکید بر نیاز به همکاری بین‌المللی در حوزه‌های مختلف حمایت کرد یک سال بعد، کمیسیون اروپا گزارشی در مورد جرم مرتبط با رایانه ارائه داد که برای آن قرارداد امضا شده بود. (SIEBER, Ibid) چند سال بعد، شورای خبره در حوزه جنایت در فضای سایبری عمیقاً این تکلیف را پذیرفت و یک پیش‌نویس کنوانسیون در مورد جرم سایبری آماده نمود. آماده‌سازی این کنوانسیون یک فرآیند طولانی بود که چهار سال به طول انجامید و بیست و هفت پیش‌نویس را پیش از آخرین نسخه که در مورخ ۲۵ می ۲۰۰۱ در پنجاهمین جلسه جامع که در ۲۲–۱۸ ژوئن ۲۰۰۱ برگزار شد، به کمیته اروپا تحویل نمود. فصل دوم این کنوانسیون حاوی مفادی است که مربوط به موضوعات مورد نظر در این بحث هستند. این فصل به دو بخش تقسیم شده است: بخش ۱ با قانون جزایی ماهوی سر و کار دارد، بخش ۲ با قانون آیین دادرسی سر و کار دارد. با توجه به یادداشت تفاهم مربوط به پیش‌نویس کنوانسیون، بخش ۱ به دنبال بهبود وسیله‌ای برای پیش‌گیری و سرکوب جرم یا جرم‌های مرتبط با رایانه 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 فعالیت‌های ویژه جرایم رایانه‌ای تحت قانون داخلی خود لازم باشد، اتخاذ نمایند. طبق بخش ۱ از فصل ۲ کنوانسیون، این فعالیت‌ها عبارتند از: (۱) جرایم در برابر قابلیت اعتماد، یکپارچگی و در دسترس بودن داده‌ها و سیستم‌ها؛ (۲)جرایم مربوط به رایانه؛

[15] Illegal content

(٤)جرایم مربوط به تخطی از قوانین کپی رایت و حقوق مرتبط (٥)مقررات مربوط به تحمیل کمک و معاونت شرکت. (کمیسیون اروپایی شورا و پارلمان اروپا ایجاد جامعه اطلاعاتی امن‌تر با بهبود امنیت زیرساختهای اطلاعاتی و مبارزه با جرایم رایانه‌ای، ۲۰۰۰)

از طرف آن‌ها، جی ۸ در ماه مه سال ۲۰۰۰ یک کنفرانس سایبری برای بحث در مورد چگونگی مقابله با جرایم رایانه‌ای برگزار کرد. این کنفرانس ۳۰۰ قاضی، پلیس، دیپلمات‌ها 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. (GOODMAN and BRENNER, 2000, 173) در نشست جولای ۲۰۰۰، G۸ بیانیه ای صادر کرد که در بخش مربوطه اعلام شد که رویکردی هماهنگ با جرائم فن‌آوری پیشرفته مانند جرایم رایانه‌ای که می‌تواند امنیت جامعه اطلاعاتی جهانی را به شدت تهدید کند، دارد. در این اطلاعیه آمده است که رویکردG۸ در مورد این موضوعات در یک سند همراه با منشور اوکیناوا در زمینه جامعه اطلاعاتی جهانی تنظیم شده است.

در ژوئیه ۱۹۸۹ با اجماع گروه G ۸ برای مبارزه با پولشویی گروه ویژه اقدام مالی (FATF)[16] تعریف و سازمان‌دهی شد. گروه ویژه اقدام مالی یک سازمان بین دولتی است. هدف آن شامل تنظیم استانداردها و گسترش اجرای قوانین، تنظیم‌کننده معیارهای عملیاتی برای مبارزه با پولشویی، مقابله با تأمین مالی تروریست‌ها و دیگر تهدیدات مربوط که امنیت سیستم یکپارچه مالی دنیا را برهم بزند، است؛ بنابراین گروه ویژه اقدام مالی یک سازمان خط مش گذار (policy making) است که برای ایجاد اراده سیاسی لازم به‌منظور ورود به قوانین ملی و تنظیم قوانین در این مناطق شکل‌گرفته است.

پس از وقایع ۱۱ سپتامبر ۲۰۰۱ گروه ویژه اقدام مالی نیز به پیشنهاد امریکا تن داده و فعالیت‌های خود را توسعه دهد. پس لیست توصیه‌های گروه ویژه اقدام مالی با اضافه شدن ۸ پیشنهاد جدید برای مقابله با تأمین مالی تروریست‌ها بلندتر شد. از سمت دیگر ابداع و اجرای تکنیک‌های جدید برای تأمین مالی تروریست‌ها باعث شد گروه ویژه اقدام مالی در ژوئن سال ۲۰۰۳ اصلاحاتی در مورد توصیه‌ها انجام دهد. سرانجام در اکتبر سال ۲۰۰٤ یک توسعه دیگر نیز به این لیست اضافه شد و لیست به‌صورت ٤۰ توصیه بعلاوه ۹ توصیه دیگر تغییر یافت.

در ماده ۷ قطعنامه ١٦١٧ شورای امنیت که در سال ۲۰۰٥ صادرشده است از همه اعضای به‌شدت درخواست می‌شود که مفاد ٤۰ توصیه مقابله با پولشویی و ۹ توصیه با مقابله با تروریسم را انجام دهند. این بند قطعنامه ١٦١٧ به نیروی ویژه گزارش مالی این قدرت را می‌دهد که به‌صورت حقوقی نیز عمل کند. از نکات جالب متن توصیه‌ها وجود و تکرار مکرر کلمه باید است. این حالت زمانی برجسته می‌شود که هر کشوری حق دارد، توصیه‌ای را نپذیرد ولی وقتی کشورها با شماتت و مشکلات بانکی، مالی و تحریم‌ها روبرو می‌شوند، دیگر معنی توصیه چندان کاربردی ندارد. این نکات باعث می‌شود که FATF نه توصیه‌ای به نظر برسد و نه برنامه فنی بلکه به‌صورت یک استاندارد حقوقی دیده شود.

در ماده ۷ قطعنامه ١٦١٧ شورای امنیت که در سال ۲۰۰٥ صادرشده است از همه اعضای به‌شدت درخواست می‌شود که مفاد ٤۰ توصیه مقابله با پولشویی و ۹ توصیه با مقابله با تروریسم را انجام دهند. این بند قطعنامه ١٦١٧ به نیروی ویژه

[16] Financial Action Task Force

گزارش مالی این قدرت را می‌دهد که به‌صورت حقوقی نیز عمل کند. از نکات جالب متن توصیه‌ها وجود و تکرار مکرر کلمه باید است. این حالت زمانی برجسته می‌شود که هر کشوری حق دارد، توصیه‌ای را نپذیرد ولی وقتی کشورها با شماتت و مشکلات بانکی، مالی و تحریم‌ها روبرو می‌شوند، دیگر معنی توصیه چندان کاربردی ندارد. این نکات باعث می‌شود که FATF نه توصیه‌ای به نظر برسد و نه برنامه فنی بلکه به‌صورت یک استاندارد حقوقی دیده شود.

در توصیه ۳٦ آن آمده است: کشورها باید در کنوانسیون وین (۱۹۹۸)، کنوانسیون پالرمو (۲۰۰۰)، کنوانسیون سازمان ملل متحد علیه فساد (۲۰۰۳) و کنوانسیون مبارزه با تأمین مالی تروریسم (۱۹۹۹) نیز عضو شوند. بر این اساس عضو جدید با قبول توصیه‌های FATF ملزم به قبول مفاد ٤ کنوانسیون دیگر هم می‌شود. این کنوانسیون هرکدام بندهای خاصی دارند باعث می‌شود تصورات از گروه ویژه اقدام مالی کاملاً تغییر یابد. مثلاً در کنوانسیون وین فصل دوم ماده ۱۹ شرط، حق شرط تعیین‌شده است. حق شرط یک بیانیه یک‌جانبه از سمت قبول کننده معاهده است تا بعضی از آثار حقوقی و مقررات معاهد در مورد آن تعدیل یا بی‌اثر شود. ماده ۱۹ کنوانسیون وین می‌گوید زمانی یک کشور می‌تواند از حق شرط استفاده کند که معاهد حق شرط را ممنوع نکرده باشد. درصورتی‌که در توصیه شماره ٦ توصیه‌نامه گروه ویژه اقدام مالی حق شرط برداشته‌شده است و هیچ کشوری نمی‌تواند لایحه یا شرطی را به آن اضافه کند. مثلاً زمانی که مصر تقاضا کرد نیروهای مقاومت از لیست تروریست‌ها حذف شوند تا به عضویت FATF درآید با یک نه بزرگ روبرو شد. در کنوانسیون ۲۸ ماده‌ای مبارزه با تأمین مالی تروریسم (ICSFT) ماده ٦ کشور عضو را مجاب می‌کند تا طبق قوانین مورد نظر کنوانسیون، قانون‌گذاری کند. بدین‌وسیله هیچ راه فراری برای مقابله با تروریسم ایجاد نشود. در ماده شماره ۲ نیز تعریف مشخص و از قبل تعیین‌شده‌ای برای تروریسم ساخته و پرداخته شده که باید ملاک نظر کشورهای عضو باشد، که ممکن است مغایر تعریف آن‌ها از تروریسم یا گروه‌های مقاومت باشد.

در کنار اقدامات بین‌المللی پیش گفته و مقررات تنظمی صورت گرفته، کشورهای مختلف نیز به تصویب برخی مقررات ملی در مقابله با جرایم سازمان یافته سایبری پرداخته اند که در زیر به‌صورت نموداری به برخی از آنها اشاره شده است.

۲-۲) نمونه هایی از استراتژی های امنیت سایبری و مقابله با جرایم سازمان یافته سایبری

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم‌انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
تحت معیارهای "اجرای قانونی و انتظامی" عبارتند از: - تأمین منابع اضافی برای ادارات امنیتی و انتظامی به منظور افزایش قابلیت‌های عملیاتی تضمین ارتباط و اشتراک اطلاعات بین امنیت سایبری و تلاش‌های اجرای قانون -حصول اطمینان از اینکه چارچوب قانون کیفری و مدنی استرالیا مستحکم بوده و با تحولات همگام است -فراهم کردن قانون استرالیایی با سطح مورد نیاز دانش فنی و درک مؤثر این موارد: - هماهنگ‌سازی چارچوب قانونی استرالیا برای امنیت سایبری با دیگر حوزه‌های قضایی و بین‌المللی برای تسهیل به اشتراک‌گذاری اطلاعات و همکاری انتظامی در مرزهای جغرافیایی	اولویت‌های استراتژیک عبارتند از: -بهبود تشخیص، تحلیل، کاهش و پاسخ به تهدیدات پیشرفته سایبری، با تمرکز بر دولت، زیرساخت‌یاتی و سیستم‌های دیگر منافع ملی -تمام استرالیایی‌ها را با اطلاعات، اعتماد و ابزار عملی برای حفاظت از خود، به‌صورت آنلاین آموزش می‌دهد و قدرتمند می‌سازد. -هم کار با کسب وکار برای ترویج امنیت[17] و انعطاف‌پذیری در زیرساخت‌ها، شبکه‌ها، محصولات و خدمات - بهترین عملکرد در حفاظت از فن‌آوری اطلاعات و ارتباطات دولت را به‌عنوان مدر قرار می‌دهد.	این استراتژی توسط بخش دادستان کل تهیه شد و نشان دهنده استراتژی دولت استرالیا است -دو سازمان جدید ایجاد شده: - CERT استرالیا به عنوان نقطه هماهنگی ملی در زمینه اطلاعات امنیتی و همکاری مؤثرتر بین‌المللی -مرکز عملیات امنیتی سایبری برای شناسایی حملات پیچیده و تسهیل واکنش‌های عملیاتی	ریسک بالا برای اقتصاد استرالیا از سمت تخریب و نفوذ رایانه‌ی توسط عاملان دولتی و غیردولتی -امنیت سایبری به‌صورت زیر تعریف می‌شود: "اقدامات مربوط به محرمانه بودن، در دسترس بودن و یکپارچگی اطلاعات پردازش شده، ذخیره شده که توسط ابزارهای الکترونیکی یا مشابه منتقل می‌شوند. - هدف سیاست امنیت سایبری دولت استرالیا حفظ محیط فعال، انعطاف پذیر و قابل اعتمادی است که از امنیت ملی استرالیا پشتیبانی می‌کند و مزایای اقتصاد دیجیتال را تقویت می‌کند. -اهداف سیاست امنیت سایبری این است: - همه استرالیایی‌ها از ریسک‌های سایبری، ایمن‌سازی رایانه خود و برداشتن گام‌هایی برای حفاظت از هویت، حریم خصوصی و امور مالی خود آگاه هستند. -کسب و کارها در استرالیا ایمن هستند و اطلاعات انعطاف‌پذیر و فن‌آوری‌های ارتباطی برای حفاظت از یکپارچگی فعالیت‌های خود و هویت و حریم خصوصی مشتریان خود دارند.	استراتژی امنیت سایبری استرالیا (۲۰۰۹)

[17] Security

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم‌انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
مبارزه با جرایم رایانه‌ای یک جز تحت عنوان "کمک به کانادایی‌ها برای امنیت آنلاین" است. این معیارها عبارتند از: - پلیس مجهز برای محافظت در برابر سرقت هویت و جرایم رایانه‌ای بین‌المللی با مقامات قانونی و منابع مالی -ایجاد مرکز متمرکز ادغام یکپارچه سایبری برای پاسخ به حملات سایبری علیه دولت یا زیرساختار انتقادی - اصلاحات قانون گذاری بیشتر: -استثمار جنسی کودکان -تعمیر ISP ها برای حفظ قابلیت‌های رهگیری - تعمیر ISP ها برای ارائه اطلاعات شناسایی مشتری	-تأمین امنیت سیستم‌های دولت: -تعیین نقش‌ها و مسئولیت‌های فدرال مشخص -تقویت امنیت سیستم‌های سایبری فدرال - افزایش آگاهی‌ها در زمینه امنیت سایبری توسط دولت -مشارکت برای امن نمودن سیستم‌های سایبری حیاتی خارج از دولت فدرال -مشارکت با استانها و مناطق -همکاری با بخش خصوصی و بخش‌های زیر ساختی حیاتی - کمک به کانادایی تا به‌طور آنلاین ایمن شوند. -مبارزه با جرم سایبری حفاظت انلاین کانادایی‌ها	امنیت عمومی کانادا اجرای استراتژی را هماهنگ می‌کند: -سایر سهامداران: -مرکز واکنش سایبری کانادا (در داخل سازمان امنیت عمومی کانادا) ایجاد امنیت ارتباط در کانادا -سرویس اطلاعات امنیتی کانادا -پلیس سلطنتی کانادا -دبیرخانه هیات خزانه‌داری -امور خارجه و تجارت بین‌الملل کانادا -وزارت دفاع ملی و نیروهای کانادایی	اقتصاد کانادا به شدت وابسته به اینترنت است -حملات سایبری شامل دسترسی غیر عمدی و غیر مجاز، استفاده، دستکاری، وقفه یا تخریب (از طریق ابزارهای الکترونیکی)اطلاعات الکترونیکی و /یا زیرساخت فیزیکی و الکترونیکی مورد استفاده برای پردازش، برقراری ارتباط و /یا ذخیره اطلاعات است. قواعد اصلی: - دولت جاسوسی اینترنتی و فعالیت نظامی را تحت حمایت قرار داد. -استفاده تروریست‌ها از اینترنت -جنایت سایبری[18] توسط مجرمان سازمان یافته -تهدید در حال تحول است سه ستون برای مقابله با این چالش: -تأمین امنیت سیستم‌های دولت - مشارکت برای امن نمودن سیستم‌های سایبری حیاتی خارج از دولت فدرال. -کمک به کانادایی‌ها به‌صورت آنلاین	استراتژی امنیت سایبری کانادا (۲۰۱۰)

[18] cyber-crime

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
در چارچوب قانون‌گذاری: "جمهوری چک مراحل قانونی و رویه‌ای را بهبود خواهد بخشید تا زمینه امنیت سایبری در نهایت شامل پیش‌گیری، شناسایی، واکنش و اقدامات طراحی شده برای شناسایی و مبارزه با جرایم اینترنتی شود"	-چارچوب قانون‌گذاری -تقویت امنیت سایبری -مدیریت دولتی و فن‌آوری اطلاعات -تاسیس CERT ملی -همکاری بین‌المللی همکاری دولت، بخش خصوصی و دانشگاه -افزایش آگاهی در امنیت سایبری -معیارهای اقدامات: تحلیل ریسک و استانداردهای بین‌المللی برای حفاظت و تضمین امنیت سایبری ملی و حفظ حریم خصوصی، رعایت حریم خصوصی، حقوق اساسی و آزادی‌های اساسی، دسترسی آزاد به اطلاعات و دیگر اصول دموکراتیک. جمهوری چک بر کفایت آن‌ها با متعادل سازی نیاز به تضمین امنیت در برابر احترام به حقوق و آزادی‌های اساسی، تمرکز خواهد کرد.	پیاده‌سازی، بهره‌برداری و امنیت سیستم‌های اطلاعات و ارتباطات معتبر، وظیفه جمهوری چک و مسئولیت تمام سطوح دولت و ادارات، بخش خصوصی و عمومی است.	ICTها اثر عمده‌ای بر عملکرد جوامع پیشرفته و اقتصادهای وابسته به ICT و جوامع وابسته به ICT دارند. این استراتژی نشان دهنده یک چارچوب سازمانی است که بخشی از سیستم امنیتی جمهوری چک را تشکیل می‌دهد. سند چارچوب نشان می‌دهد که "امنیت سایبری" نیاز به ایجاد یک جامعه اطلاعاتی معتبر با پایه‌های قانونی محکم دارد، که به انتقال ایمن سایبری و پردازش اطلاعات در همه حوزه‌های فعالیت‌های انسانی متعهد است و اطمینان حاصل می‌کند که اطلاعات می‌تواند مورد استفاده قرار گیرد و آزادانه و ایمن به اشتراک گذاشته شود. اهداف عبارتند از: -"محافظت در برابر تهدیدهایی که سیستم‌های اطلاعاتی و ارتباطی و فن‌آوری‌ها (از این پس " ICTها) در معرض آنها هستند و کاهش عواقب بالقوه در صورت حمله به ICT ها. -حفظ یک محیط امن، ایمن، مقاوم و معتبر که از فرصت های موجود در عصر دیجیتال استفاده می‌کند. این استراتژی عمدتاً بر دسترسی آزادانه به خدمات، یکپارچگی داده‌ها و محرمانه بودن فضای مجازی[19] جمهوری چک تمرکز دارد و با دیگر استراتژی‌ها و مفاهیم مرتبط هماهنگ می‌شود.	پیش‌نویس استراتژی امنیت سایبری جمهوری چک - ۲۰۱۱ ۲۰۱۵

[19] Cyberspace

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
استراتژی امنیت سایبری شامل تدابیر ملی برای هدف قرار دادن جرائم اینترنتی نمی‌شود؛ چرا که وزارت دادگستری پیش از این یک سیاست جنایی را برای مبارزه با جرایم سایبری تدوین کرده است و همچنین به این دلیل که وزارت امور داخله پیش نویس اولویت های امنیت داخلی استونی تا سال ۲۰۱۵ را آماده کرده است. -با این حال، این استراتژی شامل برخی از اقدامات بین‌المللی برای: - افزایش آگاهی از جرایم رایانه‌ای و امنیت سایبری -توسعه هم کاری های بین‌المللی کنوانسیون بوداپست درباره جرم سایبری جهانی و کمک به الحاق کشورها به این کنوانسیون است	-توسعه و اجرای مقیاس بزرگ سیستم اقدامات امنیتی -حفاظت از اطلاعات حیاتی -توسعه و پیاده سازی یک سیستم معیارهای امنیتی -تقویت همکاری‌های سازمانی از جمله تشکیل شورای امنیت سایبری -صلاحیت فزاینده در امنیت سایبری - سازمان آموزش در مورد امنیت سایبری -بهبود وضعیت تحقیق و توسعه چارچوب قانونی برای حمایت از امنیت سایبری -توسعه همکاری بین‌المللی -ترویج امنیت سایبری و دفاع در سطح جهانی -ترویج کنوانسیون بوداپست درباره جرم سایبری در سطح جهانی -تخصص استونی در سازمان‌های بین‌المللی -مشارکت در کار سازمان‌های بین‌المللی -افزایش آگاهی‌ها درباره امنیت سایبری	-استراتژی توسط کمیته استراتژی امنیت سایبری به رهبری وزارت دفاع و وزارت آموزش و تحقیقات، وزارت امور اقتصادی و ارتباطات، امور داخله و امور خارجه تهیه شده - کمیته، با همکاری بخش خصوصی مسئول توسعه طرح‌های اجرایی -شورای امنیت سایبری برای نظارت بر اجرا	حملات سایبری[20] علیه جوامع اطلاعاتی پیشرفته با هدف تضعیف عملکرد سیستم‌های اطلاعاتی بخش خصوصی و دولتی تهدیدی برای امنیت بین‌المللی محسوب می‌شوند. حملات در مقیاس بزرگ در برابر استونی از سال ۲۰۰۷ و تکرار حوادث، آغاز دوره‌ای جدید است که در آن امنیت فضای مجازی یک بعد جهانی را به دست می‌آورد و حفاظت از سیستم‌های اطلاعاتی حیاتی به مسأله امنیت ملی تبدیل می‌شود. امنیت سایبری در مورد "کاهش آسیب‌پذیری فضای مجازی، پیش‌گیری از حملات سایبری در وهله اول و در صورت وقوع یک حمله، تضمین بهبود سریع عملکرد سیستم‌های اطلاعاتی" است. استراتژی امنیتی سایبری مرتبط با سیاست‌های ملی امنیت و دفاعی است، بلکه به استراتژی جامعه اطلاعاتی استونی در سال ۲۰۰۷ نیز مرتبط است.	استراتژی امنیت سایبری استونی (۲۰۰۸)

[20] Cyber-attacks

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
-مبارزه با جرایم سایبری یکی از پایگاه‌های تأمین امنیت سایبری در نظر گرفته می‌شود. -هدف چهارم به بهبود قانون‌گذاری و همکاری بین‌المللی با توجه به جرایم اینترنتی اشاره دارد. -محور ٦ به همکاری بین‌المللی علیه جرایم رایانه‌ای اشاره دارد.	هفت محور از تلاش‌ها: ۱. پیش بینی و آنالیز ۲. کشف، هشدار و واکنش ۳. بهبود و توسعه پایدار علمی، فنی، صنعتی و توانایی‌های انسان ٤. حفاظت از سیستم‌های اطلاعاتی دولت و اپراتورهای حیاتی زیرساخت ۵. قوانین را وفق دهید ٦. توسعه همکاری بین‌المللی ۷. برقراری ارتباط برای مطلع کردن و متقاعد کردن	استراتژی آماده شده توسط آژانس ملی امنیت فرانسه به دنبال یک سیستم اطلاعاتی است که به آن اجازه می‌دهد در برابر حوادث ناشی از فضای مجازی مقاومت کند در دسترس بودن ، یکپارچگی یا محرمانه بودن داده‌های ذخیره شده، پردازش شده یا منتقل شده و خدمات مرتبط با این سیستم‌ها را در کنترل گیرد"	امنیت سایبری به‌عنوان توانایی تضمین قابلیت اعتماد، یکپارچگی و در دسترس بودن سیستم‌های اطلاعاتی در برابر حوادث ناشی از فضای سایبری تعریف می‌شود: چهار هدف از این استراتژی عبارتند از: ۱. یک قدرت جهانی در حوزه دفاع سایبری ۲. تضمین آزادی در تصمیم‌گیری[21] توسط مقامات دولتی فرانسه از طریق حفاظت از اطلاعات مربوط به حاکمیت ملی (اطمینان از محرمانه بودن ارتباطات) ۳. تقویت امنیت سایبری زیرساختار ملی انتقادی ٤ .تضمین امنیت در فضای سایبری	استراتژی دفاعی و امنیتی سیستم‌های اطلاعاتی فرانسه

[21] Decision-making

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
حوزه راهبردی شماره ٦ بر روی کنترل جرم مؤثر همچنین در فضای سایبری: -تقویت قابلیت‌های نیروی انتظامی، اداره فدرال امنیت اطلاعات و بخش خصوصی نهاده‌ای مجری قانون /صنعت مشترک -پروژه حمایت از کشورهای شریک-تلاش عمده برای هماهنگ‌سازی جهانی حقوق کیفری بر پایه بررسی کنوانسیون جرایم سایبری شورای اروپا درباره نیاز به کنوانسیون‌های دیگر در سطح سازمان ملل	ده حوزه استراتژیک: ۱ .حفاظت از زیرساخت‌های اطلاعاتی مهم به‌عنوان اولویت اصلی امنیت سایبری ۲ .سیستم‌های فن‌آوری اطلاعات امن در آلمان ۳ .تقویت امنیت IT در مدیریت دولتی ٤ .مرکز واکنش سایبری جدید ملی ٥ .شورای امنیت سایبری جدید برای افزایش هم کاری بین موسسات فدرال و همچنین بین بخش دولتی[۲۲] و خصوصی ٦ .کنترل مؤثر جرم در فضای مجازی ۷ .اقدام هماهنگ مؤثر برای تضمین امنیت سایبری در اروپا و سراسر جهان ۸ .استفاده از فن‌آوری اطلاعات قابل اعتماد و قابل اتکا ۹ .توسعه شخصی	*استراتژی تهیه شده توسط وزارت داخله فدرال اجرای این استراتژی تحت کنترل کلی شورای امنیت سایبری ملی جدید متشکل از وزرای فدرال و دبیران ایالتی وزارت امور خارجه، وزارت داخله، دفاع، اقتصاد و فن‌آوری، عدالت، تحصیل و تحقیقات، نمایندگان ایالات و بخش خصوصی به عنوان اعضای مرتبط است	"امنیت سایبری" به‌عنوان وضعیتی تعریف شده است که در آن خطرات فضای مجازی جهانی به حداقل قابل قبول کاهش می‌یابد. -نیاز به تضمین قابلیت اعتماد، یکپارچگی و در دسترس بودن سیستم‌های فن‌آوری اطلاعات. -خطرات شامل عملکرد بد فن‌آوری‌های اطلاعات، شکست زیرساخت اطلاعات و یا شکست‌های.IT -خطر اصلی حملات سایبری به سوی یک یا چند سیستم فن‌آوری اطلاعات و هدف آسیب رساندن به امنیت IT است: -حملات علیه محرمانه بودن سیستم‌های فن‌آوری اطلاعات (-"جاسوسی اینترنتی-") -حملات به تمامیت و در دسترس بودن سیستم‌های فن‌آوری اطلاعات ("خرابکاری سایبری")	آلمان: راهبرد امنیتی سایبری آلمان (۲۰۱۱)

[22] Public sector

	در مراجع فدرال ۱۰ .ابزارهایی برای پاسخ به حملات سایبری			

معیارهای جرایم رایانه‌ای	اولویت های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
بخش ۳.۵ چارچوب قانونی امنیتی و اجرای قانون: -چارچوب قانونی -واحدهای جنایی سایبری -امکانات آموزشی برای نیروهای انتظامی و قضایی -همکاری بین‌المللی برای به اشتراک‌گذاری اطلاعات استراتژی مبارزه با جرایم اینترنتی/سایبری: -گزارش جنایت -کاهش بزهکاری و پیش‌گیری -قانون‌گذاری -هم‌کاری در صنعت تجارت -هم‌کاری بین‌المللی بخش ۳.٦ اشتراک گذاری[۲۳] اطلاعات و همکاری -CERT-نیروی انتظامی هم‌کاری در سطح داخلی و بین‌المللی	فرآیند فعال فعال ۳.۰: -تهدید امنیتی و مدیریت آسیب‌پذیری -تهدید و واکنش اولیه به تهدید امنیتی بهترین تجارب امنیتی، رعایت و تضمین -حمایت از زیرساخت اطلاعات -چارچوب تضمین امنیت اطلاعات -حاکمیت الکترونیک -توسعه نرم‌افزار ایمن و اپلیکیشن -مدیریت بحران امنیتی برای مقابله با حملات سایبری و تروریسم سایبری -چارچوب قانونی امنیتی و اجرای قانون -به اشتراک‌گذاری اطلاعات امنیتی و همکاری ٤.٥تکنولوژی‌های در حال فعال شدن ۵.۰ توانا کردن مردم ٦.۰ عمل مسئولانه توسط کاربر	پیش‌نویس تهیه شده توسط وزارت فن‌آوری اطلاعات، دولت هند ۱۳ نوع از سهامداران با تمرکز بر مدیریت حوادث و پاسخ فهرست شده‌اند (به عنوان مثال هیأت اطلاعات ملی، کمیته مدیریت بحران ملی، دبیرخانه شورای امنیت ملی، -CERT IN، دبیرخانه (CERT	ارتباط بخش فن‌آوری اطلاعات برای اقتصاد. هند به عنوان یک بازیگر جهانی برای تکنولوژی کلاس جهانی و خدمات کسب وکار کار -تهدید حملات و استفاده نادرست از فن‌آوری اطلاعات توسط مجرمان، تروریست‌ها یا دولت‌ها. - تهدید به حملات علیه دولت یا زیرساخت اطلاعات انتقادی -نیاز به سیستم اکو سیستم امنیتی سایبری نیاز به یک سری اطلاعات سایبری و دفاع سایبری "- امنیت سایبری فعالیت حفاظت از اطلاعات و سیستم‌های اطلاعاتی (شبکه‌ها، رایانه‌ها، پایگاه‌های داده، مراکز داده‌ها و برنامه‌های کاربردی)با تدابیر و تکنولوژی امنیتی مناسب است". اولویت‌ها: آگاهی، محیط قانونی، حفاظت، واکنش، حادثه / واکنش اضطراری، فنون امنیتی و فن‌آوری‌ها، فرهنگ امنیت سایبری، پیش‌گیری از جرم سایبری و پیگرد قانونی، حفاظت از داده‌ها	هند پیش نویس در مورد سیاست امنیت سایبری ملی (۲۰۱۱)

[23] Sharing

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی[۲۴]	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
خط عمل ۵ به‌طور خاص جنایت سایبری را مورد رسیدگی قرار می‌دهد: -مجموعه تخصصی و ثبت متخصصان از دولت، بخش خصوصی و دانشگاهیان -تمرکز بر تحقیقات بین مرزی -تمرکز بر قوانین و مقررات بین‌المللی برای جرایم اینترنتی -گروه فرمان در سطح ملی برای جرائم اولویت ایجاد خواهد شد -متخصصان کافی در کل زنجیره عدالت کیفری برای مبارزه با جرایم سایبری -نظم عمومی ایمنی -هیات بازرسی برای ببرسی عملکرد پلیس -تبدیل منابع بودجه ای برای افزایش تحقیقات و پی‌گیری جرایم اینترنتی رویکرد برنامه جرم‌سایبری: -مرکز دانش درون پلیس -تقویت سازمان پلیس و تغییر منابع -دادستان ها، قضات و قوانین تخصصی سایبری	خطوط عمل عبارتند از: ۱. ایجاد شورای امنیت سایبری و مرکز امنیت سایبری ملی ۲. آماده سازی آنالیز تهدید و ریسک ۳. افزایش انعطاف‌پذیری زیرساخت حیاتی ٤ .ظرفیت واکنش برای ایستادگی در برابر اختلالات ICTو حملات سایبری ۵ .تحقیقات و پی‌گیری جرایم اینترنتی ٦ .تحقیق و پرورش محرک	مسئولیت با یک شورای هیات امنیت سایبری جدید خواهد بود. که در آن همه احزاب مربوطه نمایش داده خواهند شد. مرکز امنیت سایبری ملی باید با احزاب دولتی و خصوصی ایجاد شود. GOVCERT.NL باید تقویت شود و در مرکز قرار گیرد هدف این استراتژی تقویت امنیت جامعه دیجیتال به منظور افزایش اعتماد به استفاده از فن‌آوری اطلاعات توسط شهروندان، جامعه تجاری و دولت است. در این راستا، دولت هلند می خواهد همکاری مؤثرتری با سایر احزاب در زمینه امنیت و قابلیت اطمینان یک جامعه رها و آزاد داشته باشد. این امر موجب تحریک اقتصاد و افزایش موفقیت و رفاه می‌شود. حفاظت قانونی خوب در حوزه دیجیتال تضمین شده است و از اخلال در اجتماع جلوگیری شده است و اگر مشکلی پیش بیاید حاصل شود اقدام کافی صورت خواهد	امنیت سایبری به گونه آزادی از خطر یا آسیب ناشی از اخلال یا خرابی یا سو استفاده از فن‌آوری اطلاعات و ارتباطات، که از محدودیت موجود بودن و قابل اعتماد بودن اطلاعات ICT، نقض محرمانه بودن اطلاعات ذخیره شده در ICTو یا آسیب به یکپارچگی آن اطلاعات، تعریف می‌شود. اقدامات لازم برای این کار: -ICT از اهمیت بنیادی برای جامعه و اقتصاد برخوردار است. -جامعه آسیب‌پذیر است (تهدیدها شامل بوتنت‌ها، حمله به زیرساخت توسط کشورهای دیگر (استاکسنت) انکار حملات خدمات است. -نیاز به هم کاری بین طرفین در جامعه دیجیتال در سطوح داخلی و بین‌المللی	استراتژی امنیت سایبری ملی هلند، ncss(۲۰۱۱)

[24] Institutional responsibility

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات[۲۵]	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
جرم سایبری به‌عنوان اقدامات تحت پوشش فصل سیزدهم سال ۲۰۰۲ (دسترسی غیرمجاز به اطلاعات، رهگیری و تداخل با داده‌ها از جمله سوء استفاده از وسایل (بخش ۸۶)، زورگیری مرتبط با رایانه، کلاهبرداری و جعل (بخش ۸۷)و کمک و معاونت، تعریف می‌شود. برخی از اقدامات کلی در این زمینه پیش‌بینی شده‌اند: -توسعه اقدامات پیشگیرانه برای پیش‌گیری و مبارزه با جرایم سایبری -مشارکت‌های خصوصی -تحقیق و توسعه برای افزایش مهارت‌ها برای کاهش جرائم اینترنتی	-ایجاد ظرفیت سازمانی برای پاسخ به جرائم اینترنتی و تهدیدات -شورای مشورتی امنیت ملی سایبری -تیم واکنش به حادثه -کاهش تهدیدات امنیتی سایبری و آسیب‌پذیری‌های امنیتی - همکاری و مشارکت بین دولت، بخش خصوصی و شهروندان -ارتقا و تقویت همکاری‌های بین‌المللی، نوآوری، توسعه مهارت‌ها و انطباق با استانداردهای امنیتی تکنیکی و عملیاتی مناسب	پیش‌نویس سیاست ایجاد شده توسط وزارت ارتباطات منتشر شده در روزنامه دولتی برای مشاوره‌های عمومی	-نیاز به رویکرد هماهنگ در مقابله با امنیت سایبری -چالش‌های قانونی برای مقابله مؤثر با جرایم اینترنتی -نیاز به افزایش همکاری بین‌المللی برای امنیت سایبری -فعالیت‌های تجاری / دولتی / جامعه مدنی مورد نیاز برای رسیدگی به جرائم اینترنتی -نیاز به استانداردهای امنیتی سایبری و پروتکل‌ها -هدف از این سیاست تاسیس محیطی است که اعتماد و اتکا به استفاده ایمن از فن‌آوری اطلاعاتی و ارتباطی را تضمین کند. -اهداف: -تسهیل ایجاد ساختارهای مرتبط در حمایت از امنیت سایبری -اطمینان از کاهش تهدیدات امنیتی سایبری و آسیب‌پذیری‌های امنیتی -هم کاری بین دولت و بخش خصوصی -ارتقا و تقویت هم کاری بین‌المللی در زمینه امنیت سایبری -ایجاد ظرفیت و ترویج فرهنگ امنیت سایبری -ارتقا انطباق با استانداردهای امنیتی تکنیکی و عملیاتی مناسب	پیش نویس سیاست امنیتی سایبری آفریقای جنوبی (۲۰۱۰)

[25] Strategic priorities and measures

معیارهای جرایم رایانه‌ای	اولویت‌های استراتژیک و اقدامات	مسئولیت سازمانی	چشم انداز / اهداف / مسایلی که باید مورد توجه قرار گیرد	کشور/ استراتژی
اغلب اقدامات مربوط به جرایم سایبری هستند. هدف ۱ قرار است از طریق ۲٤ آیتم‌های عملی از جمله موارد زیر بدست آید: – دادگاه‌ها از اختیارات موجود استفاده کنند – قابلیت جرایم اینترنتی جدید در اداره ملی جرایم در سال ۲۰۱۳ –متخصصان سایبری برای پشتیبانی از پلیس –آموزش نیروی انتظامی –منابع بیشتر برای کار با بخش خصوصی و شرکای بین‌المللی –ارتقا هم کاری بین‌المللی (کنفرانس لندن، کنوانسیون بوداپست، دستورالعمل اتحادیه اروپا) –بررسی قوانین موجود –سیستم‌های گزارش‌دهی برای شهروندان و کسب وکار کوچک –روند کلی سایبری در پلیس –اقدام علیه جرایم نفرت –اقدامات مشترک بخش خصوصی LEA\ –همکاری فرامرزی –پشتیبانی از سایت گت سیف آنلاین دات او ار جی –امنیت سایبری قوی در خدمات عمومی –به کار انداختن صنعت امنیت سایبری بریتانیا	در زیر هر یک از این چهار هدف، رویکرد و دامنه فعالیت‌ها تعریف شده است: ۱. جرم سایبری –مقابله با جرایم اینترنتی (رهبری: اداره داخله) –انجام کسب وکار در فضای مجازی امن‌تر (رهبری با BIS) ۲. محافظت و حفاظت در برابر حملات سایبری –دفاع از زیرساخت ملی (رهبری: دفتر هیأت دولت) –قابلیت حفاظت از منافع بریتانیا در فضای مجازی (رهبری:MOD) ۳. فضای مجازی باز –کمک به شکل دادن به توسعه فضای مجازی (رهبری: وزارت فرهنگ، رسانه و ورزش) –محافظت از روش زندگی‌مان (رهبری: FCO) ٤. دانش توسعه دانش (رهبری: BIS) –بهبود مهارت ها (رهبری:BIS) –توسعه توانایی (رهبری:	موسسات ویژه مسئول اقدامات مختلف از جمله: – دپارتمان کسب وکار، نوآوری و مهارت‌ها (BIS) – وزارت دفاع (MOD) – دفتر امور خارجه و کشورهای مشترک المنافع (FCO) –دانشکده فرهنگ، رسانه و ورزش	چشم‌انداز "برای بریتانیا در سال ۲۰۱۵ ، به دست آوردن ارزش اقتصادی و اجتماعی عظیم از فضای مجازی پویا، انعطاف‌پذیر و امن" است، که آن اقدامات ما، به وسیله ارزش‌های اصلی ما از آزادی، انصاف، شفافیت و حاکمیت قانون، افزایش رفاه، امنیت ملی و یک جامعه قوی، هدایت می‌شود. اهدافی که باید تا سال ۲۰۱۵ به دست آیند: ۱. انگلستان به مبارزه با جرایم سایبری می‌پردازد و به یکی از امن‌ترین مکان‌ها در جهان برای انجام کسب وکار در فضای مجازی تبدیل می‌شود. ۲. بریتانیا نسبت به حملات سایبری، انعطاف‌پذیری بیشتری دارد و در حمایت از منافع ما در فضای سایبری تواناتر است. ۳. بریتانیا به شکل دادن یک فضای مجازی آزاد، باثبات و پر جنب و جوش کمک کرده است که مردم بریتانیا می‌توانند به‌طور ایمن از آن استفاده کنند و ان جوامع آزاد پشتیبانی می‌کند. ٤. بریتانیا باید دانش، مهارت‌ها و توانمندی را داشته باشد که بتواند از همه اهداف امنیت سایبری ما پشتیبانی کند.	استراتژی امنیتی سایبری بریتانیا (۲۰۱۱)

-آگاهی در بین کسب و کارها	دفتر کابینه)		مرکز اینترنت[۲۶] برای اقتصاد و جامعه. حملات سایبری تهدیدهای درجه اول است که بر رونق، زیرساختار کلیدی، مکان‌های کار و خانه تأثیر می‌گذارد. تهدیدها توسط مجرمان، ایالت‌ها، تروریست‌ها، هکرهای فعال‌ها.	

۳- راهبردهای تقنینی ایران در مقابله با جرایم سازمان یافته سایبری

مطالب پیش گفته در باب جرم سازمان یافته سایبری و امکان‌سنجی آن با بررسی فرضیه‌های مختلف در این خصوص به یک نتیجه واحد رسید و آن اینکه جرم سازمان یافته سایبری شاخه‌ای از جرایم سایبری است که با ویژگی‌های خاص خود وجود دارد و توسط دو گروه مجرمان سازمان یافته فضای واقعی و مجرمان سازمان یافته سایبری ارتکاب می‌یابد. شناخت ارکان و عناصر این جرم مبانی ساختاری و ماهوی آن را در دیدگاه حقوق‌دانان بین‌المللی تا حدودی تبیین نمود و نیز اقدامات برخی کشورها و سازمان‌های بین‌المللی درمقابله با آن هم مطرح گردید و حال راهبرد تقنینی نظام کیفری ایران را در این خصوص مورد بررسی قرار می‌دهیم.

با عنایت به اینکه مهم‌ترین مقرره قانونی در این خصوص قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون مجازات اسلامی مصوب ۱۳۹۲ می‌باشد، از این مستندات قانونی برای تبیین جایگاه قانونی جرایم سازمان یافته سایبری در نظام حقوقی ایران بهره می‌گیریم.

۱-۲) قانون جرایم رایانه‌ای

با بررسی قوانین موضوعه ایران در موارد خاصی با واکنش‌هایی نسبت به جرم سازمان یافته مواجه می‌شویم. چرا که در غالب موارد صرفاً ارتکاب جرم به‌صورت دسته جمعی مورد اشاره مقنن قرار گرفته است و بحثی از جرم سازمان یافته با ویژگی‌های خاص آن به میان نیامده است. در قوانین موضوعه فعلی تنها مواد ١٤ و ٢٦ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به موضوع سازمان یافتگی اشاره نموده‌اند و آن را مورد بحث قرار داده‌اند. البته این دو ماده نیز صرفاً از باب کیفیات مشدده و افزایش مجازات مرتکبین جرایم رایانه‌ای مورد اشاره قرار گرفته‌اند.

[26] Internet central

در تبصره ۳ ماده ١٤ آمده است که: "چنانچه مرتکب اعمال مذکور در این ماده[۲۷] را حرفهٔ خود قرار داده باشد یا به‌طور سازمان یافته مرتکب شود چنانچه مفسد فی‌الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد."

در واقع این تبصره صرف سازمان یافته بودن را از مصادیق علل مشدده و موجب تشدید مجازات دانسته است. مقرره بعدی بند (د) ماده ٢٦ این قانون است که در آن نیز سازمان یافتگی به‌طور عام و در تمامی جرایم سایبری از علل مشدده به حساب آمده است. این بند اشعار می‌دارد: "جرم به‌صورت سازمان یافته ارتکاب یافته باشد."

نکته حائز اهمیت آن است که در هیچ کدام از این دو مقرره قانونی سازمان یافتگی تعریف نشده و به چگونگی و کیفیت جرم سازمان یافته سایبری نیز اشاره نشده است. در واقع صرفاً به‌عنوان یک وجه نامعلوم از جرم سایبری ذکر شده و مشخص نیست، قضات چه مصادیقی را باید برای سازمان یافته بودن یک عمل مناط اعتبار قرار دهند؟ آیا باید به تعریف و ویژگی‌های مندرج در نظریه جرم‌شناسان و به تعبیری دکترین حقوقی استناد نمایند؟ این ابهام با توجه به اهمیت این وصف در مجازات تعیینی خود عاملی سرنوشت‌ساز در تصمیم نهایی در خصوص متهم است چرا که به حکم ماده ١٤ همان قانون اگر وجه سازمان یافتگی احراز شود امکان صدور حکم به مجازات محاربه وجود دارد و حال آنکه اگر این وصف احراز نشود حداکثر مجازات دو سال حبس یا چهل میلیون ریال جزای نقدی خواهد بود که تفاوت شدت مجازات‌ها اهمیت این موضوع را به خوبی آشکار می‌نماید.

۲-۲) قانون مجازات اسلامی مصوب ۱۳۹۲

در قانون مجازات اسلامی مصوب ۱۳۹۲ به‌طور عام در ماده ۱۳۰ در خصوص سازمان یافتگی اظهارنظر شده است و در تبصره ۲ آن با تعریف گروه مجرمانه و تبیین اوصافی چون انسجام نسبی، تشکیل شدن از حداقل ۳ نفر، قصد ارتکاب جرم پیش یا پس از تشکیل اظهارنظر شده است هرچند که این موارد نیز کلی و مجمل هستند و در باب تبیین مفاهیم فوق الاشاره و تعیین ساختار قانونی مترتب بر عنصر مادی و ساختاری جرم سازمان یافته اظهارنظری نشده است و کلیت سردستگی و تعریفی مجمل از گروه مجرمانه ارائه شده است نه گروه مجرمانه سازمان یافته که در عنوان فصل چهارم از بخش سوم این قانون ذکر شده است فلذا با توجه به اصول حاکم بر تفسیر قوانین جزایی امکان توسعه تعریف گروه مجرمانه به گروه مجرمانه سازمان یافته محل ایراد است و از سویی با توجه به موازین قانونی، فقهی و اصولی چنین امری نیز میسر نمی‌باشد. به دیگر سخن با توجه به شرایط ۱۰ گانه مطروحه در خصوص گروه‌های جرم سازمان یافته که در ابتدای این نوشتار نیز بدان اشاره گردید به هیچ عنوان نمی‌توان شرایط حقوقی حاکم و ناظر بر گروه‌های جرم سازمان یافته سایبری را از تعریف مطروحه از سوی مقنن در تبصره ۲ ماده ۱۳۰ قانون مجازات اسلامی مصوب ۱۳۹۲ استنباط نمود. البته این در حالی است که اداره حقوقی قوه قضادیه در نظریه شماره ۷/۹۲/۲۰۰۰ مورخ ۹۲/۱۰/۱۵ در پاسخ به سوالی در مورد مصادیق ماده ٤٧ قانون مجازات اسلامی که یکی از آنها جرائم سازمان یافته می‌باشد که مشمول مقررات

[۲۷] انتشار، توزیع، معامله، ذخیره یا نگهداری داده محتویات مستهجن به قصد تجارت یا افساد اعمال مذکور در این ماده هستند.

تعلیق اجرای مجازات نمی‌باشند با این عنوان که "جرائم سازمان یافته که مشمول این ماده است چه نوع جرائمی است؟" بیان داشته است: " با عنایت به عبارت مندرج در عنوان فصل چهارم از بخش سوم قانون مجازات اسلامی مصوب ۱۳۹۲ و مقررات ماده ۱۳۰ آن و تعریف مقرر در تبصره یک این ماده می‌توان گفت جرایم سازمان یافته، جرایمی است که توسط گروه مجرمانه که عبارت است از گروه نسبتاً منسجم، متشکل از سه نفر یا بیشتر که برای ارتکاب جرم تشکیل می‌شود یا پس از تشکیل، هدف آن برای ارتکاب جرم منحرف می‌گردد، ارتکاب می‌یابد."

به نظر می‌رسد این نظریه اداره حقوقی قوه قضائیه نیز بدون تامل در معنا و مصداق و ویژگی‌های گروه‌های جرم سازمان یافته مطرح شده و این نوع تفسیر آن هم در قوانین جزایی نمی‌تواند مطمح نظر باشد چه آنکه با لحاظ تمام شرایط، تعریف مقنن در تبصره ۲ ماده ۱۳۰ ق.م.ا مصوب ۱۳۹۲ صرفاً ناظر به گروه‌های مجرمانه‌ای می‌باشد که ممکن است سازمان یافته نیز نباشند و از این‌رو تعریف اخیر ابتر بوده و با لحاظ کیفیات مشدده پیش‌بینی شده در خصوص جرایم سازمان یافته از سوی مقنن و حتی تسری احکام محاربه و افساد فی الارض در مواردی که مصداق آن را داشته باشند که در زمره مجازات‌های جسمانی و حتی سالب حیات نیز می‌باشند، توسعه تعریف در چنین مواردی محل ایراد و خلاف اصول کلی حقوقی و اصل تفسیر به نفع متهم است.

در مجموع این‌گونه می‌توان عنوان نمود که در نظام حقوقی ایران تعریفی از جرم سازمان یافته ارائه نشده چه رسد به جرم سازمان یافته سایبری و در این خصوص متون قانونی قابل اتکایی نیز وجود ندارد. به‌علاوه مهم‌ترین سند بین‌المللی در خصوص جرایم سازمان یافته "کنوانسیون مقابله با جرایم سازمان یافته فراملی و پروتکل‌های الحاقی آن"می‌باشد که با وصف امضای آن در ۱۲ دسامبر سال ۲۰۰۰ میلادی مطابق با ۲۲ آذرماه ۱۳۷۹ خورشیدی و تصویب لایحه الحاق دولت ایران به کنوانسیون سازمان ملل متحد برای مبارزه با جرائم سازمان یافته فراملی از سوی مجلس شورای اسلامی در مهرماه ۱۳۹۷، لکن این مصوبه با اصلاحات انجامی از سوی مجلس به جهت مغایرت با سیاست‌های کلی نظام موضوع بند۲ اصل ۱۱۰ قانون اساسی به تأیید شورای نگهبان نرسید و هم اکنون در مجمع تشخیص مصلحت نظام، در حال بررسی است. بنابراین این جرم در نظام حقوقی ما جایگاه مدون ندارد و در انتظار وضع قانون خاص خود است و البته همراهی مقرره مجلس با لزوم پیوستن به گروه ویژه اقدام مالی مشترک (FATF) که توضیحات آن به‌صورت خلاصه در بخش پیشین نوشتار حاضر ارائه گردید. با این وجود با توجه به عمومات حاکم بر قانون مجازات اسلامی و نیز قواعد مسلم حاکم بر حقوق کیفری در صورتی که جرایم سازمان یافته سایبری از مصادیق محاربه باشد می‌توان از احکام قانون مجازات اسلامی استفاده و مرتکبین آن را مجازات نمود؛ همان‌طور که در رویه جاری دستگاه قضایی در برخورد با برخی گردانندگان شبکه‌ای سایت های ضداخلاقی با این استدلال برخورد شد.

نتیجه‌گیری

در نوشتار حاضر که مبتنی بر دو محور اصلی و چند زیرمجموعه بود، مشخص شد که فضای سایبر بستر جرایم مختلفی است که یکی از مهم‌ترین آنها جرم سازمان یافته سایبری می‌باشد. از این‌رو تشکیک‌های به‌عمل آمده از سوی عده‌ای مبنی بر اینکه جرم سایبری مطلقاً سازمان یافته است و یا اینکه فضای سایبر بنابر ویژگی‌هایی که دارد و در این نوشتار به

تفصیل مورد بررسی قرار دادیم قابلیت ارتکاب جرم به‌صورت سازمان یافته را ندارد، کاملاً رد شد و مشخص گردید که فضای سایبر محلی برای وقوع جرایم سازمان یافته است و این جرایم به وسیله دو گروه عمده به وقوع می‌پیوندند:

۱) گروه‌های جرم سازمان یافته فضای واقعی که در راستای فعالیت‌های مجرمانه خود به دو طریق در فضای سایبر فعالیت می‌کنند؛ نخست آنکه از این فضا و توانمندی‌های ارتباطی خاص آن برای تسهیل فعالیت‌های مجرمانه خویش در فضای واقعی بهره می‌گیرند و دوم آنکه این محیط را با توجه به ویژگی‌های خاص آن برای انجام اعمال مجرمانه خود مورد استفاده قرار می‌دهند و در آن مرتکب جرم می‌شوند.

۲) گروه‌های جرم سازمان یافته خاص فضای سایبر که در این فضا شکل گرفته و غالباً از خرده فرهنگ‌های هکری که گروه‌های مجرمانه سایبری هستند تشکیل شده و به انجام اقدامات مجرمانه در فضای سایبری می‌پردازند. البته این گروه‌ها نیز به دو شکل عمده به فعالیت می‌پردازند: **نخست)** گروه‌های جرم سازمان یافته خاص فضای سایبر که با اجتماع مجرمان و هکرها به منصه ظهور می‌رسند و شروع به اقدامات مجرمانه در فضای سایبر می‌کنند و غالباً اهداف منفعت طلبانه دارند؛ هرچند که در برخی موارد این گروه‌های به انگیزه های سیاسی، عقیدتی و... نیز وارد عمل می‌شوند، لکن در اکثر موارد سودای مالی آنها را به انجام فعالیت‌های مجرمانه سوق می‌دهد. **دوم)** گروه‌های جرم سازمان یافته خاص فضای سایبر که از حمایت‌های دولت‌ها برخوردارند و در واقع ابزاری هستند که دولت‌ها از آنها برای پیشبرد مقاصد پنهان خویش استفاده می‌کنند. این گروه در دو شکل تماماً دولتی و نیمه دولتی فعالیت می کنند و با توجه به مباحث مطروحه در این نوشتار نمی‌توان عنوان ارتش سایبری را بر آنها اطلاق نمود.

شناخت گروه‌های جرم سازمان یافته سایبری و تفکیک نوع و حیطه عملکرد آنان تأثیر به سزایی در شناخت راه‌های مقابله با آنها و پیشگیری از این دسته از جرایم دارد به نحوی که در ترسیم نمودن اقدامات قانونی و تبیین جنبه‌های مختلف تقنینی مواجهه با جرایم سازمان یافته سایبری نقش به سزایی ایفا می‌کند که این مهم می‌بایست از سوی قانون‌گذار کشور ما نیز مورد توجه قرار گیرد، چرا که صرف تدوین قواعد کلی در خصوص جرایم رایانه ای نمی‌تواند پاسخگوی نیازها و ضرورت‌های این حوزه باشد. زیرا شناخت یک موضوع و جنبه‌های مختلف آن و نیز فرآیند تکوینی حاکم بر شکل‌گیری این گروه‌ها و این دسته از جرایم می‌تواند راهگشای نظام کیفری باشد. در واقع تفکیک جرایم سازمان یافته خاص فضای سایبر از جرایم سازمان یافته سنتی که با کمک فضای سایبر به وقوع می‌پیوندند، تأثیر آشکاری بر روش‌های پیشگیری و مقابله با این دسته از جرایم دارند.

در خاتمه باید اذعان نمود که جرم سازمان یافته سایبری به عنوان یک واقعیت ملموس و فراگیر که همواره در حال گسترش است در جامعه جهانی ظهور یافته و هر لحظه خطرات بیشتری را برای جوامع مختلف به ارمغان می‌آورد و مقابله با آن مستلزم فعالیت همه جانبه و هماهنگ جوامع جهانی است. چرا که فضای سایبر با عنایت به ویژگی‌های منحصربه فرد خود توانمندی‌هایی را به گروه‌های جرم سازمان یافته سایبری داده است تا در عرصه جهانی و بدون حد و مرز حاضر شوند و از این حیث مقابله با آنها نیز نیازمند یک عزم جهانی است. هرچند که برخی از کشورهای جهان خود از بانیان و حامیان این گروه‌ها هستند و این امر مقابله با این گروه‌ها را بسیار دشوار می‌کند.

در نظام حقوقی ایران نیز همان‌طور که در این نوشتار عنوان گردید جرم سازمان یافته در معنای عام فاقد تعریف و مقرره قانونی است چه رسد به جرم سازمان یافته سایبری و از این حیث خلاء قانونی در این حوزه به چشم می‌خورد و امکان تبیین و تحلیل قانونی را برمبنای قوانین موجود از محققان و متصدیان امر قضا می‌گیرد. هرچند که با برخی کلیات مندرج در قانون مجازات اسلامی و قانون جرایم رایانه‌ای که در پژوهش حاضر بدانها اشاره گردید می‌توان تا برخی مصادیق را بر موازین موجود منطبق نمود و البته با تفسیر عام مواد آن موارد را جرم‌انگاری نموده و مجازات کرد، لکن این شیوه نادرست است و می‌بایست نسبت به جرم‌انگاری مستقل و مدون در خصوص جرایم سازمان یافته سایبری با لحاظ زیرساخت‌های حقوق داخلی و بهره‌گیری از اسناد حقوقی بین‌المللی مرتبط و نیز رویه تقنینی کشورهای پیش‌رو همانند برخی نمونه‌های مطروحه در این نوشتار اقدام لازم از سوی مقنن معمول گردد تا خلاء قانونی از میان رفته و امکان مقابله با این دسته از جرایم و مرتکبان آنها به نحو کامل فراهم گردد.

منابع

۱. جلالی فراهانی(۱۳۸٤) امیرحسین؛ ***پول‌شویی الکترونیکی***، فصلنامهٔ *فقه و حقوق*، شمارهٔ ٤.

۲. جلالی فراهانی(۱۳۸٤) امیرحسین؛ ***پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر***، فصلنامهٔ *فقه و حقوق*، شمارهٔ ٦.

۳. خرم‌آبادی، عبدالصمد(۱۳۸٤) ***تاریخچه تعریف و طبقه بندی جرم‌های رایانه‌ای***، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، تهران: سلسبیل.

٤. دزیانی، محمد حسن(۱۳۷٦) ***جرائم کامپیوتری***، جلد اول، دبیرخانهٔ شورای عالی انفورماتیک.

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

٦. زررخ، احسان(۱۳۸۸) ***نیم نگاهی به ذهن یک هکر: آیا نظریه های جرم شناسی می‌توانند هک کردن را تبیین کنند؟*** مجموعه مقالات فناوری اطلاعات (بزرگداشت مرحوم دزیانی)، معاونت توسعه قضایی، انتشارات روزنامه رسمی.

۷. شمس ناتری، محمد ابراهیم(۱۳۸۰) ***بررسی سیاست کیفری ایران در قبال جرایم سازمان‌یافته با رویکرد به حقوق جزای بین‌المللی***، رساله دکتری، دانشگاه تربیت مدرس.

۸. شمس ناتری، محمد ابراهیم(۱۳۸۳) ***جرائم سازمان‌یافته***، فصلنامهٔ *فقه و حقوق*، شمارهٔ ۱.

۹. نجفی ابرندآبادی، علی حسین(۱۳۸۵) ***تقریرات درس جرم‌شناسی (کلیات، بزهکاری مزمن، پیشگیری زودرس، جرایم سازمان یافته)***، دورهٔ کارشناسی ۱۳۷۹.

۱۰. نجفی ابرندآبادی، علی حسین(۱۳۸۵) ***تقریرات درس جرم‌شناسی (جرایم سازمان یافته)***، دورهٔ کارشناسی ۱۳۸۰.

منابع لاتین

11. Anne H. Soukhanor and others, the American Heritage Dictionary of the English Language, Thirded, Houghton Mifflin, 1992

12. Brenner, w.s, Organized Cybercrime-How Cyberspace May Affect the Structure of Criminal Relationships, North Carolina Journal of Law & Technology, Volume 4, Issue 1: Fall 2002

13. Casey, Eoghan, Digital Evidence and Computer Crime**,** Academic Press, 2001.

14. Communication From the European Commission of the Council and the European Parliament Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime, [2000].

15. Council of Europe (2005). Organised crime situation report: Focus on the threat of cybercrime,

http://www.coe.int/T/E/Legal_Affairs/Legal_cooperation/Combating_economic_crime/8_Organised_crime/Documents/Organised%20Crime%20Situation%20Report%202005.pdf

16. Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states, [1995].
17. Council of Europe, Recommendation no.4 (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime, 1995.
18. Cressey, D. R. Theft of a nation: The structure and operations of organized crime in America. NewYork: Harper & Row, 1969.
19. Criminal Intelligence Service of Canada (2005):
20. Eighth U.N Congress on the Prevention of Crime and the Treatment of Offenders. Doc. A/CONF.144 /L.11 of 4 September 1990 section 2.
21. Europol (2006). Organised Crime Threat Assessment 2006: 18http://www.europol.europa.eu/publications/OCTA/OCTA2006.pdf
22. GOODMAN M. D. and S. BRENNER, The Emerging Consensus on CriminalConduct in Cyberspace (Oxford, International Journal of Law and Information Technology), [200] Vol. 10, n. 2, p. 165.
23. Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social and Legal Studies, 10(2).
24. Grabosky, peter, The Internet, Technology, and Organized Crime, Asian Journal of Criminology, Volume 2, Number 2 / December, 2007, pp. 145-161.
25. Howard, Abadinsky; Organized Crime, 6thed. Belmont, U.S.A, Wadseorth, 2000.
26. James D.Torr, organized Crime, Sandiago,USA, Green haven press Inc. 1999.
27. Jay Albense, Organized Crime in America, 2nded. Ohio, Cincinneti, 1989.
28. Joseph V, A mafia member, testified before the McClellan Committee, Details of his life maybe found in Maas, P. (1968), The Valachi papers, New York: G.P. Putnam.
29. Kim-Kwang Raymond Choo & Russell G. Smith, Criminal Exploitation of Online Systems by Organised Crime Groups, Asian Journal of Criminology, Volume 3, Number 1, June, 2008, pp 37-59.
30. Majid Yar. (2005). the novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407–427:408.
31. Marjie T. Britz, A New Paradigm of Organized Crime in the United States: Criminal Syndicates, Cyber gangs, and the Worldwide Web, Sociology Compass, Vol. 2, November 2008.
32. McAfee (2006). McAfee virtual criminology report: Organised crime and the internet : http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual%20Criminology%20Report.pdf
33. McMillan, R (2006). FBI: Cybercriminals taking clues from Mafia: http://www.pcworld.com/article/id, 126664-c, cybercrime/article.html
34. Nisbett, C (2002). New directions in cyber-crime. White Paper, QineticQ: http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0012.File.pdf
35. OECD Recommendation on the Council concerning Guidelines for the Security of Information Systems [1992].

36. Parizo, E.B. (2005). Busted: The inside story of 'Operation Firewall', Security.com:http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1146949,00.html
37. Rafael Etges, CISSP CISA and Emma Sutcliffe, An Overview of Transnational Organized Cyber Crime, Information Security Journal: A Global Perspective, vol.17 no.2, pp.87-94
38. SHINDER, D. Scene of the Cybercrime (U.S.A, Syngress), [2002] p. 6.
39. SIEBER, U. Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission,1998, p 33.
40. The Convention at : <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
41. ttp://www.cisc.gc.ca/annual_reports/annual_report2005/document/annual_report_2005_e.pdf:15
42. UN Convention against transnational organized Crimes, 2000, Art2.
43. United Nations Manual on the Prevention and Control of Computer Related Crime, NO 43-44 (c) (2) – 117 (1994).
44. Williams, P. (2001). Organized crime and cybercrime: Synergies, trends and responses. Global Issues 6(2), 25, US Department of State: http://usinfo.state.gov/journals/itgic/0801/ijge/ijge0801.pdf