ساختارشناسی گروه‌های مجرمانه سازمان‌یافته در فضای سایبر

جعفر کوشا*
حسین روزگار**
علی رحمتی***

چکیده

محدودیت‌های موجود در دنیای فیزیکی طرفین قرارداد مشارکت جنایی را بر آن داشت تا در راستای نیل به اهداف مجرمانه و کسب سود بیشتر نسبت به سازمان‌دهی منابع و تمرکز خود در قالب ساختارهایی منسجم و ثابت با زنجیره فرماندهی مشخص اقدام کنند. به‌کارگیری ساختارهای هرمی در فضای واقعی، تلاش مؤثری در جهت جامه عمل پوشاندن به سازوکار اعمال قدرت بود. فضای سایبر با ظهور خود محدودیت‌های دنیای فیزیکی را از میان برداشت و همگام با شکل‌گیری نسل نوینی از جرائم، مدل‌های ساختاری جدیدی از سازمان‌دهی ائتلاف شرکای قرارداد مجرمانه در این فضا پدیدار شد که از جهات متعددی با همتایان سنتی خویش متفاوت بود. فقدان منابع تحقیقی لازم در این زمینه، ایده نخستین لزوم واکاوی ماهیت و نحوه سازمان‌یافتگی جرائم در فضای سایبر را به ذهن نگارندگان پژوهش تداعی کرد که مقاله پیش‌رو حاصل این واکاوی است. جوینده حقیقت را پوشیده نیست که سگالش و تحلیل چیستی این پدیده قادر خواهد بود تا روزنه‌های مطالعاتی- کاربردی مؤثری را به‌منظور جلوگیری از پیدایش و تکوین صنعت مجرمانه سازمان‌یافته در فضای سایبر در اختیار مقامات مجری قانون قرار دهد.

واژگان کلیدی

گروه مجرمانه سازمان‌یافته، فضای سایبر، ساختار هرمی، بازار سیاه

---

* دانشیار گروه حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی
Email: jkoosha@yahoo.com
** کارشناسی‌ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی (نویسنده مسئول)
Email: hossein.roozegar@yahoo.com
*** دانشجوی دکترای حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی
Email: alirahmati_69@yahoo.com

تاریخ ارسال: ۹۶/۳/۲۹ تاریخ پذیرش: ۹۶/۷/۳۰

فصلنامه راهبرد / سال بیست‌وششم / شماره ۸۵ / زمستان ۱۳۹۶ / صص ۱۴۹-۱۱۷

جستارگشایی

با آغاز هزاره سوم میلادی، جامعه جهانی راه خود را در ورود به عصر چهارم جرائم سازمان‌یافته هموار دید. سده گذشته سه دوره مجزا را در ظهور و گسترش جرائم سازمان‌یافته پشت سر گذاشت. نخست، دوره ممنوعیت دهه ۱۹۲۰ میلادی که گروه‌های مجرمانه سازمان‌یافته ظهور کرده و از قماربازی، فروش الکل و اخاذی کسب سود می‌کردند. در دهه ۱۹۴۰ میلادی، هرج‌ومرج به‌وجودآمده از جنگ جهانی دوم باعث ایجاد عصر دوم بر مبنای منتفع‌شدن از بازارهای سیاه شد. دوره سوم در دهه‌های ۱۹۷۰ تا ۱۹۸۰ میلادی و با جهانی‌شدن بازارهای مربوط به مواد مخدر و ظهور شرکت‌های مجرمانه بین‌المللی جدید ظاهر شد. اکنون همپوشی دنیای آفلاین و آنلاین و فرصت‌های مجرمانه جدید ایجادشده توسط فناوری اطلاعات و ارتباطات، هم‌زمان با پیدایش اشکال جدید تهدیدات الکترونیکی، منجر به آغاز عصر چهارم حیات و استمرار جرائم سازمان‌یافته شده است که در آن، علاوه‌بر گروه‌های مجرمانه سنتی، اشکال جدید سازمان‌های مجرمانه نیز می‌توانند رونق یافته و رشد کنند.

باوجود اینکه برخی از نویسندگان منکر شکل‌گیری نوع خاصی از سازمان‌دهی در فضای سایبر به‌منظور ارتکاب جرم می‌باشند (Williams, 2001: 1)، یافته‌های موجود نشان می‌دهند که رفتارهای مجرمانه سایبری علاوه‌بر اینکه می‌توانند به‌صورت فردی انجام شوند، همچنین امکان ارتکاب آنها به‌صورت گروهی نیز وجود دارد. حتی با در نظر گرفتن اینکه ارتکاب بسیاری از رفتارهای مجرمانه سایبری نیازمند درجه بالایی از تخصص و سازمان‌دهی است،(۱) این احتمال وجود دارد که سطح مداخله گروه‌های مجرمانه سازمان‌یافته در جرائم سایبر، دست‌کم در فعالیت‌های مجرمانه مالی مانند کلاهبرداری اینترنتی و جعل بیشتر باشد؛ با توجه به اینکه اینترنت و فناوری‌های مرتبط فرصت‌های خوبی را برای ایجاد مشارکت و هماهنگی میان گروه‌های مختلف در سراسر جهان ایجاد کرده‌اند.

تاریخ ارتکاب نخستین شکل مدرن جرم سازمان‌یافته گزارش‌شده در بستر شبکه جهانی اینترنت، به تاریخ تکامل نخستین نوع جرم رایانه‌ای محض؛ یعنی هکینگ یا دسترسی غیرمجاز، در اوایل دهه ۱۹۸۰ میلادی و ایجاد گروه «414s» بازمی‌گردد که طی آن گروهی از نوجوانان ۲۲-۱۶ ساله با ائتلاف در فضای واقعی از ویسکانسین اقدام به ورود به سیستم‌های کامپیوتری لابراتوار ملی لوس آلاموس، مرکز سرطان ممواریال اسلون- کترینگ و غیره کردند. در همان سال‌ها گروه دیگری با نام لژیون مرگ (یا اربابان فریب)[1] به رهبری *مارک آبن* (فیبرابتیک)[2] شکل گرفت که درصدد کاوش سیستم‌های ارتباط از راه دور، مینی‌کامپیوترها و سیستم‌های عامل بزرگ رایانه بود. این گروه به دلیل ساختار منحصربه‌فرد خود، از شناخته‌شده‌ترین

1. Legion of Doom (Masters of Deception)
2. Mark Abene (Fiber Optic)

ائتلافات جنایی در ارتکاب گروهی جرائم در فضای سایبر به شمار می‌رفت. در دهه ۱۹۹۰ میلادی موج حملات علیه تمامیت، محرمانگی و دسترس‌پذیربودن داده‌ها و سیستم‌های رایانه‌ای به‌شدت افزایش یافت، به‌نحوی‌که به گزارش اداره کل حسابداری وزارت دفاع ایالات‌متحده تنها در این کشور حدود ۲۵۰ هزار حمله نفوذی فقط در سال ۱۹۹۵ صورت گرفته بود که میزان چشمگیری از این حملات به گروه‌های هکر کلاه‌مشکی[3] منتسب شد. در سال ۱۹۹۴ چند نفر از اعضای فرقه مذهبی- تروریستی *اوم شینری کیو*[4] به‌فرمان *شیزو ماتسوموتو*[5] در ژاپن موفق به نفوذ به پردازنده مرکزی کارخانه صنایع سنگین میتسوبیشی و سرقت مگابایت اطلاعات حساس شدند. نخستین شکل کراکینگ[6] کاملاً سازمان‌یافته در سال ۱۹۹۵ توسط هکرهای روسی با رهبری *ولادیمیر لوین*[7] انجام شد که طی آن ۱۰ میلیون دلار از سیتی بانک به سرقت رفت. نسل جدید حملات گروه‌های سازمان‌یافته به سیستم‌های رایانه‌ای از سال ۱۹۹۸ رقم خورد که با تشدید تنش‌ها در خلیج‌فارس، هکرها به سایت پنتاگون رخنه و اقدام به سرقت نرم‌افزارهای سیستم ماهواره‌ای نظامی کردند. در همین سال نخستین نمونه اسب تروجان[8] توسط اعضای فرقه گاو مرده[9] در فضای اینترنت منتشر شد. با شروع هزاره سوم و ظهور نسل جدید جرائمی همچون دیداس، سرقت هویت، ارسال ایمیل‌های ناخواسته، اخاذی رایانه‌ای[10] و غیره اشخاص، شرکت‌ها و سازمان‌های متعددی مانند *لکسیز نکسیز*،[11] *پی‌پال*،[12] *یاهو*، *مایکروسافت* و غیره هدف حملات سازمان‌یافته گروه‌های طرف قرارداد مشارکت جنایی قرار گرفتند که با تمرکز قوای خود در قالب فروم‌ها، بازارها و سایت‌های سیاه آنلاین نسبت به توسعه اقتصاد زیرزمینی گام برداشته‌اند.

نظر به جهات بالا، این ادعا که مجرمان آنلاین این روزها در حال شکل‌دهی نوع جدیدی از شبکه‌های مجرمانه سازمان‌یافته می‌باشند، چندان دور از واقع و گزاف نخواهد بود (BAE System Detica, 2012: 4). باوجود اینکه طبق برخی تحقیقات، دلایل تجربی کمی برای روشن‌سازی این موضوع وجود دارد که تا چه اندازه جرائم سایبری به شکل سازمان‌یافته تحقق یافته و تا چه حد گروه‌های مجرمانه در قالب اشکال سنتی و جدید اقدام به فعالیت می‌کنند (Lusthaus, 2013: 59)، تحقیقات دیگری ادعا می‌کنند که در آینده نزدیک اکثریت قریب به‌اتفاق

3. Black Hat Hackers
4. Aum Shinri Kyo
5. Chizuo Matsumoto (Shoko Asahara)
6. Cracking
7. Vladimir Levin
8. Back Orifice at Defcon
9. Cult of Dead Cow
10. Computer Extortion
11. Lexis Nexis
12. PayPal

تحقیقاتی که در مورد جرائم سازمان‌یافته فراملی صورت می‌گیرد، الزاماً پیرامون تحقیق جرائم سازمان‌یافته سایبری خواهد بود (Europol IOCTA, 2011: 3).

در این پژوهش تلاش می‌شود تا به پرسش‌های زیر پرداخته شود: ۱- آیا ماهیت خاص فضای سایبر، به‌عنوان فضایی غیرقابل‌کنترل، سیال و ساختگی، در ایجاد ساختارهای نوین مجرمانه منطبق با این فضا و شکل آنها تأثیری داشته است یا خیر؟ ۲- آیا امکان مهاجرت ساختارهای سنتی وابسته به دنیای فیزیکی به محیط آنلاین وجود دارد؟ در صورت مثبت‌بودن پاسخ، دامنه و ماهیت این انتقال تا چه حد بوده و وجه تمایز بارز این گروه‌ها از همتایان آنلاین و نوین خویش چیست؟ ۳- آیا تعاریف و سازوکارهای پیش‌بینی شده در اسناد مکتوب بین‌المللی و ملی می‌توانند به‌خوبی تأمین‌کننده آرمان‌های عدالت کیفری در به محاکمه‌کشاندن طرفین ائتلافات جنایی سازمان‌یافته باشند یا خیر؟

در ادامه با تعریف جرم سازمان‌یافته و معیار شناسایی آن، ضمن تأکید بر فقدان منابع اطلاعاتی کافی در این زمینه، به تشریح مختصر ساختارهای منسجم موجود در فضای واقعی، مهاجرت این ساختارها به فضای سایبر، چگونگی شکل‌گیری تشکل های مجرمانه سازمان‌یافته در این فضا و تفاوت آنها با همتایان سنتی خود پرداخته خواهد شد.

۱. معیار جرم سازمان‌یافته؛ سازمان‌یافتگی گروه

در پژوهش‌های متعدد، زمانی که بحث از جرم سازمان‌یافته به میان می‌آید، سازمان‌یافتگی گروه، معیاری برای سازمان‌یافتگی جرم در نظر گرفته می‌شود. تشکیل گروه سازمان‌یافته نماد عینی ائتلاف جنایی میان سه نفر یا بیشتر است که همگی روابط ساختاریافته‌ای را بنا بر اصول خاصی پایه‌ریزی می‌کنند. در چنین پژوهش‌هایی دلیل سازمان‌یافتگی گروه، مؤلفه‌های عقلانی و سودجویی عنوان می‌شود و گروه مجرمانه، گروهی متشکل از حداقل سه نفر است که اکثریت تلاش‌های آن در راستای ارتکاب جرائم به‌منظور عمده کسب سود اختصاص داده می‌شود» (Brenner, 2002: 7). از نظر اینترپل عنوان گروه سازمان‌یافته بر «هرگونه مشارکت یا گروهی از افراد دخیل در فعالیت‌های غیرقانونی مستمر به‌منظور کسب منفعت، صرف‌نظر از مرزهای سرزمینی» اطلاق می‌شود (Brenner, 2002: 7). تأکید بر منفعت‌طلبی به‌عنوان انگیزه اصلی شکل‌گیری گروه مجرمانه و مهم‌ترین عامل تمایز آن با رفتارهای مجرمانه فردی درواقع نشئت‌گرفته از نظریه تجاری‌بودن مدل ارتکاب جرم[13] در این گروه‌ها است.

در کنار نگرش مدل تجاری، رویکردهای دیگری نیز وجود دارند که در راستای شناسایی و طبقه‌بندی یک جرم خاص به‌عنوان جرم سازمان‌یافته گام برداشته‌اند. یوروپل به این منظور که یک گروه مجرمانه به‌عنوان گروهی سازمان‌یافته طبقه‌بندی شده و به‌تبع آن جرم نیز خصیصه

13. Business Model of Crime

سازمان‌یافته به خود بگیرد، وجود حداقل ۶ مورد از ۱۱ ویژگی زیر را که چهار مورد ۱، ۳، ۵ و ۱۱ باید الزاماً وجود داشته باشند، ضروری می‌داند:

۱- لزوم وجود همکاری بیش از دو نفر؛ ۲- برای هر یک از اعضا باید وظایف خاصی در نظر گرفته شده باشد؛ ۳- برای یک دوره طولانی یا نامحدود ایجاد شده باشد؛ ۴- از آشکالی از انضباط و نظارت تبعیت کند؛ ۵- مظنون به ارتکاب جرائم شدید باشد؛ ۶- در سطح بین‌المللی فعالیت داشته باشد؛ ۷- از خشونت یا دیگر ابزارهای مناسب برای ارعاب استفاده کند؛ ۸- از ساختاری تجاری یا منظم استفاده کند؛ ۹- در پولشویی دخالت داشته باشد؛ ۱۰- بر سیاست، رسانه‌ها، مدیریت عمومی، مراجع قضایی یا اقتصادی تأثیر داشته باشد و ۱۱- به‌عنوان سودجویی یا قدرت‌طلبی شناخته شده باشد.[۱۴]

همان‌گونه که مشاهده می‌شود در این رویکرد نیز، سازمان‌یافتگی گروه، معیاری برای سازمان‌یافتگی جرم در نظر گرفته شده است، ولی انگیزه سودجویی تنها انگیزه شکل‌گیری و شناسایی گروه سازمان‌یافته محسوب نمی‌شود.

در ایران تا قبل از تصویب قانون مجازات اسلامی ۱۳۹۲، قانون‌گذار بدون ارائه تعریفی از جرم سازمان‌یافته، تنها در قوانین متفرقه و خاص تشکیل و رهبری شبکه چندنفری برای ارتکاب ارتشا، اختلاس و کلاهبرداری،[۲] اقدام باندی و تشکیلاتی جهت اخلال در نظام صادراتی کشور[۳] و مواردی از این قبیل را از مؤلفه‌های تشدید مجازات، ارتکاب جرم مجزا یا تعیین صلاحیت دادگاه رسیدگی‌کننده به جرم تلقی می‌نمود. با افزایش حملات سازمان‌یافته در سال‌های اخیر، قانون‌گذار ضمن پیش‌بینی حداکثر مجازات شدیدترین جرم ارتکابی اعضای گروه برای سردسته گروه مجرمانه در ماده ۱۳۰، در تبصره ۱ این ماده گروه مجرمانه را به‌عنوان گروهی «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» تعریف کرد، بدون آنکه مقرره خاصی را در قانون جرائم رایانه‌ای به موضوع جرائم سازمان‌یافته در فضای سایبر، یا گروه سازمان‌یافته مجرمانه سایبر اختصاص دهد که با درک کامل ماهیت خاص و منحصربه‌فرد این فضا تدوین شده باشد.

ازنظر قانون‌گذار کشور، انسجام نسبی در برخورداری سلسله‌مراتب فرماندهی از حداقل انضباط و کنترل، علاوه‌بر تقسیم وظایف مجزا برای اعضا و استمرار فعالیت، معنی می‌شود. به همین صورت وجود یک فرمانده مشخص برای گروه مجرمانه، طبق ماده ۱۳۰، شرط سازمان‌یافتگی آن گروه است. در این صورت هرگونه جرم ارتکابی توسط گروه در راستای پیاده‌سازی طرح‌های مجرمانه مشارکتی، صرف‌نظر از اینکه قصد اعضای گروه کسب سود یا منفعت مالی بوده است یا خیر،[۴] جرم سازمان‌یافته نام می‌گیرد.[۵] با توجه به‌مراتب ذکرشده،

14. Europol Doc. 6204/2/97. ENFOPOL 35 Rev, 1997

مشخص می‌شود که قانون‌گذار ایران سازمان‌یافتگی گروه را تنها معیار شناخت جرم سازمان‌یافته، در تمامی زیرشاخه‌های خانواده‌های بزرگ جرائم در نظر گرفته و برای آن ماهیتی مجزا از گروه سازمان‌یافته قائل نشده است. در حال حاضر با فقدان ماده قانونی خاص، تنها می‌توان به استناد ماده ۱۳۰ قانون مجازات اسلامی نسبت به شناسایی گروه‌های سازمان‌یافته مجرمانه در فضای سایبر، شناسایی سردسته گروه مجرمانه و تحمیل اشد مجازات به وی اقدام کرد.

در سطح بین‌الملل، سند موسوم به *کنوانسیون سازمان ملل متحد برای مقابله با جرم سازمان‌یافته فراملی*[۱۵] به‌عنوان تنها سند بین‌المللی مورد اتفاق کشورها در زمینه مقابله با جرائم سازمان‌یافته، در ماده ۲ خود به تعریف گروه سازمان‌یافته مجرمانه پرداخته است.(۶) واقعیت آن است که در تدوین پیش‌نویس این کنوانسیون، تهیه‌کنندگان، مؤلفه‌های تعریفی گروه سازمان‌یافته را، نظیر سازمان متشکل از سه یا چند نفر، با توجه به واقعیت‌های روز دنیای فیزیکی اواخر قرن بیستم در متن ماده گنجاندند (UNODC, 2004: iv)، اما تاکنون هیچ مبنای مورد اتفاقی برای توصیف و تحلیل عناصر متشکله گروه‌های سازمان‌یافته مجرمانه که در فضای سایبر شکل گرفته یا فعالیت می‌کنند، در اسناد، قوانین و ادبیات حقوقی شکل نگرفته است. بسیاری از نویسندگان و محققان، با توجه به عمومیت تعریف کنوانسیون پالرمو، عین این تعریف را برای همتای آنلاین گروه سازمان‌یافته نیز انتخاب کرده‌اند.

با توجه به تعاریف متعدد از گروه سازمان‌یافته، چشم‌انداز بین‌المللی این پژوهش و پذیرش این واقعیت که تنها تعریف بین‌المللی مورد اتفاق از این گروه‌ها، تعریف ارائه‌شده در کنوانسیون پالرمو است، لذا این پژوهش نیز تعریف مندرج در متن ماده ۲ این کنوانسیون را برای شناسایی گروه مجرمانه سازمان‌یافته در زمینه جرم سایبر، اساس تحلیل قرار خواهد داد. اگرچه در ادامه بر لزوم پیش‌بینی تعریف خاص و مورد اتفاق برای گروه‌ها و جرائم سازمان‌یافته ارتکابی در فضای مجازی تأکید خواهد شد. لازم به بیان است اگرچه که طبق بند ۳ ماده ۳۶ کنوانسیون پالرمو، ایران به دلیل عدم تودیع سند الحاق کنوانسیون، به علت عدم تصویب مجلس شورای اسلامی، ملزم به پایبندی به اصول و مقررات کنوانسیون نیست، اما قانون‌گذار در عمل، برخی از مقررات کنوانسیون را به‌عنوان الگو مورد استفاده قرار داده و ماده ۱۳۰ قانون مجازات اسلامی اقتباس ناقصی از ماده ۲ کنوانسیون پالرمو است.

توجه به تعریف کنوانسیون از گروه سازمان‌یافته می‌تواند روشن‌کننده نکاتی باشد: نخست اینکه با مشارکت کمتر از سه نفر، گروه سازمان‌یافته‌ای شکل نخواهد گرفت. درواقع، ازنظر منطقی، در ارتکاب یک جرم می‌توان سه روش را متصور شد: ارتکاب جرم به‌صورت انفرادی، از طریق همکاری دو نفر و درنهایت توسط سه نفر یا بیشتر. تنها شق سوم می‌تواند شکل‌دهنده

15. United Nations Convention against Transnational Organized Crime

یک رفتار مجرمانه سازمان‌یافته باشد. دلیل این امر ازنظر برخی نویسندگان این است که لازمه تشکل و سازمان‌یافتگی، وجود رابطه‌ایی نظام‌مند میان افراد است و برای رفتار ارتکاب‌یافته توسط یک نفر نمی‌توان هیچ‌گونه سازمان‌یافتگی قائل شد. در مورد اجتماع دو نفر به‌منظور ارتکاب جرم نمی‌توان موضوع را از دو حالت خارج دانست: یا این دو نفر سهم مساوی در قرارداد مشارکت خود دارند یا اینکه یکی رئیس است و دیگری مرئوس؛ بنابراین بحث نظام‌مندی منتفی خواهد بود. اما زمانی که نفر سومی به این اجتماع اضافه می‌شود پیچیدگی روابط موجود افزایش می‌یابد (Kurt, 1950: 135). همچنین اجتماع و مشارکت دو نفر در ارتکاب جرم نمی‌تواند به اشکال جدید، متفاوت و خطرناک‌تر مجرمانه تعمیم یابد، حال آنکه ائتلاف میان سه نفر یا بیشتر تهدید جدی‌تری را متوجه شهروندان و جامعه خواهد ساخت (Coser, 1977: 186)؛ بنابراین در این مقاله اصطلاح گروه سازمان‌یافته، به‌رسم دیگر پژوهش‌ها، در مفهوم ائتلاف جنایی متشکل از حداقل سه نفر مورد استفاده قرار می‌گیرد که طبق اصول مشخصی ایجاد شده است و به‌منظور نیل به اهداف مجرمانه اقدام می‌کند.

نکته دوم اینکه، در فضای سایبر به دلایلی نظیر وجود حملات خودکار[16] نباید نیاز مبرمی به ائتلاف و انعقاد قرارداد مشارکت مجرمانه میان چندین فرد، آن‌گونه که در جرائم سنتی شاهد آن بوده‌ایم، باشد چرا که برخلاف فضای واقعی، در این فضا ماشین‌ها و نرم‌افزارهایی چون ویروس‌ها، کرم‌ها، باج‌افزارها، بدافزارها و غیره نقش‌آفرینان اصلی صحنه جرم هستند. بنابراین، این امکان وجود دارد که در فضای سایبر حملات ماهیتاً منسجم و نظام‌مند انجام شوند، اما تنها توسط یک مغز متفکر انسانی طراحی و برنامه‌ریزی شده باشند.

تجربه عملی نشان می‌دهد در حملاتی که توسط شبکه‌ای از زامبی‌ها[17] یعنی بات‌نت[18](۷) انجام می‌شود برنامه‌ریزی به گونه‌ایی صورت می‌گیرد تا نرم‌افزارهای متعددی در راستای ارسال هرزنامه، از دسترس خارج‌کردن وب‌سایت‌ها و اخاذی از مالکان آنها، تقلب در کارت‌های اعتباری، راه‌اندازی حملات دیداس و غیره به کار گرفته شوند (UNODC, 2013, 32). فرمان‌های صادرشده ربات‌ها را قادر می‌سازد تا بتوانند در یک‌زمان اقدام به تخریب داده‌ها، سرقت، متوقف‌کردن سیستم‌ها، راه‌اندازی باج افزارها و غیره کنند.(۸) کنترل شبکه ربات‌ها از راه دور است و حتی یک نفر نیز می‌تواند اقدام به فرماندهی رایانه‌های آلوده شده، کند (Broadhurst & Chang, 2013: 51).

بات‌نت‌ها تقریباً تمامی عناصر شناسایی یک جرم سازمان‌یافته را در خود دارند. یک بات‌نت دارای ساختاری مجتمع است، برای مدت‌زمان معینی شکل می‌گیرد، می‌تواند منجر به ارتکاب جرائم شدید شود و در صورتی که قائل به لزوم تجاری‌بودن مدل ارتکاب جرم شویم، باتنت‌ها

16. Automated Attacks
17. A Network of Zombies
18. Bot-Net (Robot-Network)

غالباً به منظور فعالیت‌های سودجویانه و کسب منفعت راه‌اندازی می‌گردند. باتنت‌ها حتی ازنظر فنی نیز از گروه‌های سازمان‌یافته سنتی پیچیده‌تر هستند؛ ساختار آنها سیال‌تر است و شبکه ایجادشده گسترده‌تر. اعضای یک باتنت که سیستم‌های آلوده‌شده (زامبی‌ها) می‌باشند، می‌توانند به‌جای قرار گرفتن در یک منطقه جغرافیایی معین، در نواحی مختلف جهان قرار بگیرند. با استفاده از سیستم باتنت که از آن به‌عنوان مهم‌ترین سازوکار تجاری و صنعتی‌کردن جرم سایبر نام برده شده است، مرتکب یا مرتکبان قادر خواهند بود تا با راه‌اندازی زامبی‌ها از نقاط مختلف دنیا امر تحقیقات مأموران مجری قانون را مختل ساخته یا آن را متوقف کنند چرا که در این صورت محل و منشأ دقیق راه‌اندازی حملات غیرقابل‌شناسایی خواهد شد و حتی در صورت شناسایی مرتکب یا مرتکبان اصلی، از آنجا که جامعه بین‌الملل همچنان در زمینه همکاری های بین‌المللی رهنمود الزام‌آور و مشخصی ندارد، محاکمه و استرداد مرتکبان با موانع بسیاری روبه‌رو خواهد شد (Broadhurst & Chang, 59). باوجود این واقعیت‌ها، باتنت‌ها همچنان در سطح بین‌الملل به‌عنوان ملاکی برای شناسایی جرم سازمان‌یافته در نظر گرفته نشده‌اند، چرا که می‌توانند توسط یک فرد انسانی راه‌اندازی گردند و در این صورت فاقد یکی از عناصر الزامی تعریف جرم سازمان‌یافته در کنوانسیون پالرمو، یعنی گروه سازمان‌یافته متشکل از سه نفر یا بیشتر می‌باشند (Chang, 2012: 224).

۲. چالش نظری و ادله

در حالی که تعداد زیادی از متخصصان علم جرم‌شناسی ادعا می‌کنند که فضای سایبر میدان خوبی برای جولان گروه‌های مجرمانه محسوب شده و روزگار هکر تنها[19] به سر آمده است، یافته‌ها و اطلاعات اندکی درخصوص ساختارهای برتر، طول عمر گروه‌ها در این فضا، نحوه شکل‌گیری اعتماد بین اعضای گروه‌های مجرمانه و رابطه با دیگر اشکال جرم وجود دارد. به‌نوبه خود، فقدان اطلاعات و منابع لازم در زمینه‌هایی نظیر کمیت و کیفیت رفتارهای مجرمانه مرتکبان و دامنه فعالیت‌های آنان، نحوه استخدام و به‌کارگیری نیرو، چگونگی اعمال زور در فضای سایبر و غیره، مهم‌ترین مانع طراحی و بسط راهبردها و اقدامات لازم به‌منظور مقابله با چنین گروه‌هایی تلقی می‌شود.

کمبود منابع اطلاعاتی کافی، منجر به روی آوردن محققان و پژوهشگران به نظریات متعددی در ارتباط با علت شکل‌گیری گروه‌های مجرمانه در فضای سایبر شده است. از یک‌طرف، درحالی‌که ازنظر برخی نویسندگان یادگیری و تقلید می‌تواند مهم‌ترین دلایل در ایجاد این گروه‌ها به‌حساب آید (Broadhurst et al. 2005: 3)، گروه‌های مجرمانه سایبر را نمی‌توان صرفاً بر مبنای نقش آنها در ارتکاب رفتارهای غیرقانونی، به معنی یک شبکه بر محور عقلانی و

19. Lone Hacker

سودجو از بازیگران درگیر در فعالیت‌های مجرمانه، مورد شناسایی قرار داد چـرا کـه الگـوهـایی نظیر اجبارهای اجتماعی- فرهنگی یا اقتصادی- اجتماعی احتمالاً تأثیر مهمی در ایجاد و تـداوم این گروه‌ها دارند. به‌عنوان‌مثال، فشار بر سرمایه‌گذاران بخش خصوصی به‌منظور کاهش هزینه‌ها و همچنین کاهش سطح استخدام کارکنان می‌تواند به‌عنـوان‌مثـال، موجبـات کـاهش امنیـت و ایجاد فرصت‌های جدید برای منتفع شدن غیرقانونی از روزنه‌های آسیب‌پذیر فناوری اطلاعـات و ارتباطات را رقم زند (UNODC, 2013: 10). از آنجـا کـه شـرکت‌هـا در ایـن صـورت مجبـور بـه استخدام تعداد محدود یا موقت پیمانکاران می‌شوند، متعاقباً کارمندان از وضعیت خود، به دلیـل دستمزدهای پایین و ترسِ از دست دادن شغل، احسـاس نارضـایتی مـی‌کننـد. بنـابراین خطـر ارتکاب فعالیت‌های مجرمانه و تأثیر فعالیت‌های گروه‌های سازمان‌یافتـه بـر کارکنـان شـرکت‌هـا افزایش می‌یابد (UNODC, 2013: 10). برخی از شرکت‌های تأمین‌کننده امنیت در فضای سایبر از این موضوع که کارمندان سابقِ بیکار شده و بازنشسته یک خطـر بـالقوه را طـی دوره‌هـای رکـود اقتصادی ایجاد می‌کنند، اظهار نگرانی کرده‌اند (McAfee, 2009: 9).

همچنین گزارش شده است که تعداد زیادی از افراد باسواد فارغ‌التحصیل شده استخدام نشده یا بازنشسته و اخراج شده که دارای توانایی‌های فنی رایانه‌ای می‌باشند، منابع جدید بالقوه‌ای برای جرائم سازمان‌دهی شده محسوب می‌شوند. در نیجریه تحقیقات در مورد ویژگی‌هـای اجتمـاعی- جمعیتی گروه مجرمانه پسران یاهو[20] نشان می‌دهد که تعداد بسیار زیـادی از افـراد ایـن گـروه، دانشجویانی با تحصیلات دانشگاهی می‌باشند که کلاهبرداری آنلایـن را بـه‌عنـوان روشـی بـرای امرارمعاش و کسب درآمد اقتصادی مرتکـب مـی‌شـوند (Aransiola, 2011: 760). درواقـع معضـل بیکاری موجب شده است تا تعداد زیادی از جوانان بین ۲۲ تا ۲۹ سال خود را راغب به پیوستن به این گروه مجرمانه آنلاین بیابند. شبیه همین مطالعات نیز در کشور غنـا، سـودجوبـودن گـروه مجرمانه موسوم به «پسران ساکاوا»[21] را تأیید می‌کنـد (Warner, 2011: 746). علـت ایجـاد ایـن گروه‌ها همچنین به وسواس‌های فکری و عملی[22] نسبت داده شده اسـت (Broadhurst, 2014: 4) درحالی‌که به نظر مـی‌رسـد تـأثیر احسـاس مصـونیت، زاییـده اعتمادبـه‌نفـس ناشـی از حـس ناشناختگی[23] در فضای سایبر، در ایجاد این گروه‌ها برجسته‌تر است (Brenner, 2012: 13).

با این‌حال برخلاف تصور رایج شـکل‌گرفتـه از تجربیـات محـیط فیزیکـی (شـمس، ۱۳۸۳: ۱۱۹)، کسب منفعت مالی می‌تواند تنها یکی از انگیزه‌هـای مجرمـان در ارتکـاب جـرائم سـایبر به‌صورت سازمان‌یافتـه بـه شـمار رود (House of commons, 2013: 7) و دیگـر انگیـزه‌هـا، نظیـر اعتراضات سیاسی یا سرگرمی، بسته به نوع جرم متغیر می‌باشند.

20. Yahooboys
21. Sakawaboys
22. Obsessive-Compulsive Behavior
23. Ability to be Anonymity

۳. جرم سازمان‌یافته در فضای سایبر یا جرم سایبریِ سازمان‌یافته؟[۱۰] دو روی یک سکه

جرم سایبر در نخستین روزهای ظهور خود، عمدتاً توسط هکرهای جوانی ارتکاب می‌یافت که به‌صورت غیرقانونی با نقض اقدامات و تدابیر امنیتی، به‌منظور سرگرمی یا به نمایش گذاردن توانایی‌های فنی خود، به سیستم‌های رایانه‌ای متعددی دسترسی پیدا می‌کردند (Tropina, 2012: 159). رشد اقتصاد دیجیتالی موجب شد تا هم چشم‌انداز جنایی[۲۴] و هم انگیزه مرتکبان به‌صورت چشمگیری تغییر کند. امکان کسب عواید و سود بالا در کنار خطر اندک دستگیری، فضای سایبر را محیط جذابی برای انواع مختلف مجرمان کرد که به دنبال کسب سود یا متزلزل‌نمودن مشروعیت و اساس نظام‌های سیاسی و ارزش‌های حاکم بر فرهنگ یک جامعه از طریق ارتکاب جرم بودند.

از زمان پیدایش تاکنون، شبکه‌های اطلاعات جهانی به دو شکل توسط مجرمان دستاویز انتفاع و بهره‌مندی قرار گرفته است؛ نخست به‌عنوان رسانه جدید برای ارتکاب جرائم سنتی در کنار دیگر انواع وسایل ارتکاب جرم و دوم به‌عنوان بستری نوین برای ارتکاب اشکال جدیدی از جرائم با ماهیت منحصربه‌فرد. مسئله فضای سایبر به‌عنوان وسیله جدید ارتکاب جرم، باید وابستگی تنگاتنگی با امکانات و توانمندی‌های مجرمانی دارد که قصد استفاده از شبکه‌های اطلاعات را به‌منظور کسب حداکثر سود دارند. این موضوع همچنین می‌تواند ناشی از این واقعیت باشد که اعضای گروه‌های سازمان‌یافته سنتی، همواره به‌منظور فرار از تعقیب و گرفتاری در چنگال عدالت، درصدد یافتن پناهگاه‌های امنی[۲۵] می‌باشند که در کشورهای دارای حاکمیت ضعیف و نظام‌های سیاسی ناپایدار ایجاد می‌شود (Williams, 2001: 2). فضای سایبر با قابلیت غیرقابل‌کنترل بودن، ناشناس ماندن، فقدان حدود و مرزهای مشخص و ارائه فرصت‌های جدید برای ارتکاب جرائم متعدد بدون لزومِ حضور فیزیکی در صحنه جرم، شکل‌دهنده محیطی مطلوب و ارجح نسبت به فضای فیزیکی برای ارتکاب جرم است؛ به‌ویژه با در نظر گرفتن این مهم که مجرمان، به دلیل ماهیت جهان‌شمول این فضا، می‌توانند از کشورهایی مرتکب جرم شوند که چارچوب‌های قانونی مطلوب و توانایی‌های فنی لازم را به‌منظور مبارزه با جرائم سایبری دارا نمی‌باشند (Goodman, 2010: 315). در این مورد شبکه جهانی اینترنت به‌عنوان وسیله‌ای برای تسهیل ارتکاب تمام انواع جرائم سازمان‌یافته آفلاین، ازجمله سوءاستفاده از کودکان، قاچاق غیرقانونی مواد مخدر، قاچاق انسان به‌منظور استثمار جنسی، مهاجرت غیرقانونی، انوع مختلف کلاهبرداری، جعل و غیره مورد استفاده قرار می‌گیرد.

24. Criminal Landscape
25. Safe Havens

به‌موازات این واقعیت، برخی تحقیقات نشان‌دهنده این موضوع هستند که در عصر حاضر گروه‌های مجرمانه سازمان‌یافته سنتی، در کنار ساختارهای سازمان‌یافته‌ای که به‌عنوان میراث، از دنیای فیزیکی به دنیای دیجیتالی انتقال داده‌اند، اقدام به ایجاد ساختارهای منسجم و هدفمندی کرده‌اند که صرفاً بر ارتکاب جرم در شبکه‌های اطلاعات جهانی و فضای سایبر تمرکز دارند (Ben-Itzhak, 2009: 10). گزارش‌های اخیر که توسط شرکت‌های متعدد امنیت در فضای سایبر ارائه شده است بر این واقعیت تأکید کرده است که فنی‌شدن و پیچیده‌سازی حملات در فضای سایبر به‌منظور ارتکاب جرائم متعدد، بالاخص جرائم مالی، از ساختارهایی متفاوت، سیال، پویا، منسجم و در حال تکامل تبعیت می‌کند که درصدد ارائه اشکال جدیدی از انحاء بهره‌مندی از تکنولوژی، به‌منظور به دست آوردن منافع مالی غیرقانونی می‌باشند (Europol, IOCTA, 2015: 31).

لازم به ذکر است تفکیک میان دو موضوع مطرح شده، یعنی مهاجرت جرائم و گروه‌های سازمان‌یافته سنتی به فضای سایبر و ظهور شکل جدیدی از جرم سازمان‌یافته، نباید در معنای مستثنی شدن هر یک با وجود دیگری تفسیر شود و این دو ساختار در کنار یکدیگر در فضای سایبر ادامه حیات می‌دهند.

۴. ساختار گروه‌های مجرمانه سازمان‌یافته

بسیاری از دولت‌ها، آژانس‌های مجری قانون، پژوهشگران دانشگاهی و سردمداران صنعت امنیت در فضای سایبر، می‌پندارند که گروه‌های مجرمانه سازمان‌یافته با همان شکل سنتی به‌شدت خود را در ارتکاب جرائم دیجیتالی درگیر می‌کنند، اما طبق نظر برخی پژوهشگران، یافته‌ها نشان می‌دهند که احتمال بیشتری وجود دارد که مجرمان به‌منظور ارتکاب جرائم سایبر، در شبکه‌های غیرقانونی با ساختاری توزیع‌شده و سیال سازمان‌هایی با ساختار رسمی درگیر شوند (Décary-Hétu et al, 2012: 3). در ادامه با بررسی مختصر ساختارهای هرمی[۲۶] در فضای واقعی، به تحلیل ماهیت و نحوه سازمان‌دهی جرائم در فضای سایبر پرداخته خواهد شد.(۱۱)

۴-۱. سازمان‌دهی در فضای واقعی؛ ساختار هرمی

موانع و محدودیت‌های موجود در دنیای واقعی، نظیر فاصله مکانی، آب‌وهوا، لزوم حضور فیزیکی و غیره که بخشی از ماهیت مقدر دنیای واقعی را شکل می‌دهند، مؤید این واقعیت می‌باشند که بسیاری از فعالیت‌های انسانی در دنیای فیزیکی نمی‌توانند با دخالت تنها یک نفر انجام گیرند و تلاش گروهی چندین نفر را اقتضا می‌کنند. بنابراین از دیرباز به‌کارگیری سازمان‌دهی سلسله مراتبی به‌عنوان روشی مؤثر برای تمرکز تلاش‌های گروهی جهت نیل به هدف مشترک شرکا،

26. Hierarchical Structures

به دلیل برخورداری از سیستم تقسیم وظایف[۲۷] و زنجیره فرماندهی،[۲۸] تلقی می‌شده است (Ronfeldt, 1996: 7-8)[۱۲]

در زمینه ارتکاب جرم در فضای فیزیکی، وجود ساختارهای هرمی به همراه سازمان‌دهی پیچیده و تقسیم وظایف به‌منظور مشارکت در سناریوی مجرمانه و برقراری نظم در گروه اجتناب‌ناپذیر است. توضیح اینکه در دنیای واقعی که در آن ساختار گروه‌های مجرمانه سنتی شکل می‌گیرد، قربانیان، اعم از دولت و شهروندان، اغلب از ضعف و آسیب‌پذیری خود آگاه می‌باشند و با توجه به این آگاهی در پی اجتناب از بزه‌دیدگی برمی‌آیند؛ به‌عنوان‌مثال از طریق مسلح‌کردن خود یا ساختن دیوار یا دیگر اقدامات پیشگیرانه در پاسخ به این اقدامات، سارقان و دیگر مجرمان به‌وسیله سازمان‌دهی نیروهای خود در قالب تشکیلاتی که گنگ[۲۹] یا گروه مجرمانه نام دارد، درصدد غلبه بر مقاومت و پایداری قربانی، از طریق ارعاب یا حملات فیزیکی برمی‌آیند. شکستن حرز و فائق آمدن بر دیگر تدابیر دفاعی قربانی نیازمند قدرتمندی گروه مجرمانه است (Brenner, 2002: 27). موفقیت این دسته‌ها در جرائم سازمان‌یافته سنتی تا حد زیادی معلول روش‌های مؤثری بوده است که آنها در کسب درآمد از دارایی قربانی به کار می‌برده‌اند. چنین گروه‌هایی همانند یک تقویت‌کننده قدرت[۳۰] عمل می‌کردند؛ به‌نحوی‌که با بهره‌گیری از تلاش‌های چندین نفر در راستای غلبه بر مقاومت قربانی به صورتی مؤثر به کسب منفعت نائل می‌آمدند (Rollins et.al, 2013: 6).

با توسعه و بسط دامنه جغرافیایی با (حاکمیت یک گروه مجرمانه)، نظارت بر فعالیت‌های اعضای گروه و کنترل مستقیم آن که اکنون به دلیل متنوع‌شدن، نیازمند نظارت بیشتر و پیچیده‌تری بودند، عملاً توسط رئیس سازمان مجرمانه مشکل شد. برای رهبر گروه امکان حضور فیزیکی در هر زمان در مناطق مختلف و نظارت بر فعالیت هر یک از اعضا امکان‌پذیر نبود. در راستای حل مشکل اعمال نظارت، به‌ویژه در گروه‌های مافیایی مدرن، سطوح متعدد نظارت از جانب کسانی ایجاد شد که از طرف رئیس اصلی بر این امر گماشته شده بودند (Pijv ek, 2009: 22). سازمان شکل هرمی به خود گرفت و نظارت در قالب سلسله دستوراتِ زنجیره‌ایی پدیدار شد؛[۳۱] از کاپو (رئیس‌کل)[۳۲] یا جانشین وی[۳۳] به کاپیتان[۳۴] و درنهایت سرباز مافیا[۳۵] پدیدار شد.

27. Divisions of Labor
28. Chain of Commands
29. Gangs
30. Force Multiplier
31. Chain of Commands
32. Capo Crimini/Capo de tutti capi (super boss/boss of bosses)
33. Capo Bastone (Underboss, second in command)
34. Caporegime or Capodecina (lieutenant, typically heads a faction of ten or more soldiers comprising a `crew)
35. Piciotto (Lower-Ranking Soldiers; Enforcers. ....)

بنا به‌مراتب مذکور، ایجاد و گسترش الگوی هرمی در جرائم سازمان‌یافته سنتی بیشتر به دلیل حفظ نظارت و کنترل بر رفتارهای مجرمانه متعددی بوده است که گروه در یک منطقه جغرافیایی به‌نسبت گسترده مرتکب می‌شده است؛ چرا که در فضای واقعی جرائم تا حد زیادی توسط نیروی انسانی انجام می‌شوند و این افراد موضوع اصل لزوم سازمان‌دهی و هماهنگی رفتارها در دنیای واقعی قرار می‌گیرند (Brenner, 2002: 33). لازمه بقا و کارکرد صحیح گروه‌های مجرمانه در چنین فضایی، استخدام منابع انسانی لازم و پرداخت هزینه جهت حصول اطمینان از وفاداری اعضایی است که دارای توانایی مورد نیاز برای اعمال قدرت و درگیری در فعالیت‌های مجرمانه هستند. فروش و نقدکردن مصنوعات و اقلام غیرقانونی، نیازمند نقل‌وانتقال این اقلام، تعیین محل مناسب و مطمئن برای تبادل، تأمین امنیت برای خود و مشتریان است. انجام صحیح و مؤثر تمام این عملیات و اقدامات توسط یک فرد انسانی یا در قالب یک ساختار ساده مجرمانه امکان‌پذیر نیست و ساختارهای هرمی در راستای سازمان‌دهی تعاملات انسانی[۳۶] و تضمین نیل به هدف مجرمانه در فضای واقعی به‌صورت عمودی، متمرکز، خشک و ثابت شکل گرفته‌اند. بنابراین، شکل این ساختارها برگرفته از ماهیت مقدر و محدود دنیای فیزیکی پیرامون ما است.

در ایران در قرن اخیر سندیکاهای متعددی به‌منظور خریدوفروش مواد مخدر و مشروبات الکلی تأسیس شدند که به‌صورت سازمان‌یافته نسبت به حمل‌ونقل بین دولت‌ها این اقلام و توزیع آنها اقدام می‌کردند و موجب توسعه صنعت قاچاق شدند. ساختارهای سلسله‌مراتبی و تقسیم وظایف در این سازمان‌ها بعدها توسط کارتل‌های بزرگ ملی و بین‌المللی به‌منظور ارتکاب دیگر جرائم وام گرفته شد و در دو دهه اخیر به‌عنوان‌مثال برای مدیریت سازمانی برخی شبکه‌های غیرقانونی و مجرمانه کوئست[۳۷] به کار گرفته شد. در تمامی این سازمان‌ها ساختار هرمی مؤثرترین شکل مدیریت برای تمرکز قوا، نظارت بر اعضا و کسب حداکثر منفعت در دنیای فیزیکی برای اقلیت رهبران حاکم به شمار می‌آمد.

۴-۲. سازمان‌دهی در فضای سایبر

برخلاف دنیای واقعی که به دلیل مقدر بودن فضای حاکم و به تبع آن محدودیت‌های موجود در آن ساختارها به شکل عمودی، ثابت و متمرکز شکل می‌گرفتند، فضای سایبر ساختگی و ناشی از جعل انسان است. ساختگی‌بودن به معنی متغیر و پویابودن است؛ به‌نحوی‌که اکثر بخش‌های آن را می‌توان تغییر یا انتقال داد. بنابراین در دنیای سایبر محدودیت‌های دنیای فیزیکی وجود ندارد.

36. Human-to-Human Interactions
37. Quest

باوجود تردیدهایی که از آغاز هزاره جدید درخصوص شکل‌گیری گروه‌های مجرمانه در فضای سایبر وجود داشته است، تحقیقات اخیر نشان می‌دهند ماهیت جهانشمول فضای سایبر زمینه شکل‌گیری گروه‌های مجرمانه را از تجمع اعضایی از سراسر جهان، برخلاف گروه‌های سنتی که اعضای آن اغلب در مناطق خاصی مستقر می‌باشند، فراهم کرده است[۱۳] (Wall, 2015: 79). فقدان محدودیت‌ها موجب شده تا فضای سایبر، به‌عنوان فضای شبکه‌ها یا شبکه‌ای از شبکه‌ها، به‌صورت افقی، گسترده، سیال و در حال تحول شکل بگیرد. وجود این مشخصات می‌تواند تأکیدکننده این فرض باشد که ساختارهای سازمانی هرمی برای فعالیت‌هایی که در فضای سایبر روی می‌دهند، مناسب نیستند. همان‌گونه که در ادامه بحث بیان خواهد شد، در ساختارهای توده‌ای، وضعیت و جایگاه اعضای گروه به حالت نزدیک به‌هم[۳۸] و مساوی[۳۹] گرفته است؛ چرا که حملات راه‌اندازی شده توسط اعضا و واحدها به‌صورت مستقل، خودمختار و خودجوش صورت می‌گیرد و سازمان‌دهی شکل عرضی دارد.

به همین صورت، برخلاف دنیای واقعی، در فضای سایبر، اگرچه اعمال قدرت به‌منظور غلبه بر تدابیر و تمهیدات دفاعی الکترونیکی قربانی مانند دور زدن دیواره آتشین یا تهدید قربانی به پرداخت منفعتی مالی به‌منظور کاهش اذیت و آزار از طریق باج‌افزار و درنتیجه تصاحب دارایی وی ضروری است، ولی لازمه چنین اعمال قدرتی جمع‌آوری و تمرکز نیروی ترکیبی و تلاش دیگر مجرمان سایبری نظیر هکرها نیست؛ چرا که خصوصیات گروه‌های سازمان‌یافته در دنیای واقعی، مانند توسل به خشونت و کنترل محله یا منطقه خاص، برای فعالیت‌های مجرمانه سازمان‌یافته در دنیای سایبر قابل‌تصور نیست. برعکس، نیروی لازم به‌منظور تحقق جرائمی نظیر سرقت در چنین فضایی، نتیجه عملکرد فناوری و اصل خودکار بودن حملات است؛ بنابراین در دنیای سایبر اهمیت قدرت فیزیکی بسیار ناچیز می‌نماید[۱۴] و قدرت، نه در تعداد افراد، بلکه در نرم‌افزارها نهفته است. در این فضا فنون خودکارسازی جایگزین تعداد بسیار زیادی از نیروهای انسانی شده‌اند که در فضای واقعی برای انجام وظایف مجزا، به‌عنوان بخشی از سازمان بزرگ مجرمانه، اختصاص داده شده‌اند. به‌عنوان‌مثال، در جرم کپی و توزیع غیرقانونی نرم‌افزار[۴۰] یا پخش روانگردان‌های مجازی،[۴۱] تنها اقدام لازم به‌منظور تحقق جرم، به اشتراک‌گذاری نرم‌افزار در وب‌سایت است و سپس این نرم‌افزار بدون نیاز به‌واسطه و تأمین امنیت به‌راحتی از طریق کپی‌برداری با چند کلیک ساده قابل‌انتشار توسط مشتریان است. وجود چنین مزیتی نیاز به وجود سطوح متعدد فرماندهی و سازمان‌دهی را برطرف می‌کند.

38. Close-in
39. Stand-off
40. Software Piracy
41. Virtual Drug

اهمیت نداشتن تعدادِ نفرات در ارتکاب جرائم در فضای سایبر نشان می‌دهد که شرط نخست، ایجاد و بسط ساختار دسته‌های مجرمانه، اگر بتوانیم برای آن نقشی قائل شویم، در سازمان‌دهی جرم سایبر تأثیر ناچیزی ایفا می‌کند. به‌عبارت‌دیگر، به دلیل اینکه مجرمان سایبری می‌توانند به‌تنهایی این‌چنین در اقدامات مجرمانه موفق باشند، نیازی به پیوستن به دیگر مجرمان به‌منظور افزایش قدرت ندارند، بلکه شکل‌گیری گروه مجرمانه در فضای سایبر نشان‌دهنده تمایل اعضای گروه به هدف قرار دادن چندین قربانی به‌صورت همزمان و تمرکز تلاش‌ها به‌منظور نیل به کسب سود بیشتر در موارد بسیار پیچیده است (Brenner, 2002: 29).

در گروه‌های سازمان‌یافته مجرمانه سایبری، اعتماد در مفهوم سنتی،(۱۵) آن‌گونه که در گروه‌هایی نظیر مافیای مدرن به‌عنوان جزیی از اجزای حاکمیت[۴۲] می‌توان شاهد آن بود، معنایی ندارد (UNODC, 2013: 45)، از آنجا که دنیای سایبر فرصت‌های بیشتری را برای مخفی‌ماندن و تضمین ناشناخته‌ماندن هویت یک نفر ایجاد می‌کند و از این طریق خطر افشا و دستگیری اعضا یا سردمداران اصلی کاهش می‌یابد (Brenner, 2002: 47). بنابراین میزان وفاداری ملاک اعتماد به اعضا نیست، بلکه درجه تخصص و توانایی است که می‌تواند دوام عضویت در یک گروه مجرمانه را برای فرد عضو تضمین کند. وجود توانایی‌های فنی مساوی میان اعضا، موجب تمایز ساختارهای فرماندهی در گروه‌های مجرمانه سایبری از همتایان سنتی خویش می‌شود؛ چرا که در این ساختار هر یک از اعضا می‌تواند یک کارآفرین غیرقانونی مستقل[۴۳] باشد. گروه‌های مجرمانه آنلاین اغلب از ساختاری رسمی و پایدارخاصی در ارتکاب جرم و جرائم، تبعیت نمی‌کنند. علت این امر به فقدان سازوکارهای کنترل و نظارت در فضای سایبر و عدم نیاز به برقراری ارتباط زیاد توسط اعضا بازمی‌گردد (Tropina, 2012: 162).

به‌علاوه، برخلاف گروه‌های مجرمانه سنتی، عضویت در گروه‌های مجرمانه سایبری اغلب موقتی است. در فضای سایبر، پیوندهای مجرمانه برای زمان نامعینی و به‌منظور نیل به هدف غیرقانونی مورد نظر شکل گرفته و بعد از آن از هم گسسته می‌شود. توانایی ترک گروه توسط اعضای گذرا و عضویت در این گروه‌ها در هر زمان، شکل‌دهنده مؤلفه قدرتمندی در برابر ساختار فرماندهی خشک و سلسله‌مراتبی و این به معنای سیال‌بودن است. موقتی‌بودن ماهیت سازمان‌های مجرمانه به این معنی است که معیارهای سنتی تعهد و عضویت، برخلاف گروه‌های مجرمانه سنتی، نباید در این گروه ها از اهمیت چندانی برخوردار باشند و به همین صورت، گذرا بودن ساختارهای آنلاین باعث می‌شود تا نتوان آن‌گونه که در متن ماده ۲ کنوانسیون جرائم سازمان‌یافته شرط دانسته شده است، آنها را تشکیل‌شده برای یک دوره زمانی مشخص قلمداد

42. Governance
43. Criminal Entrepreneur

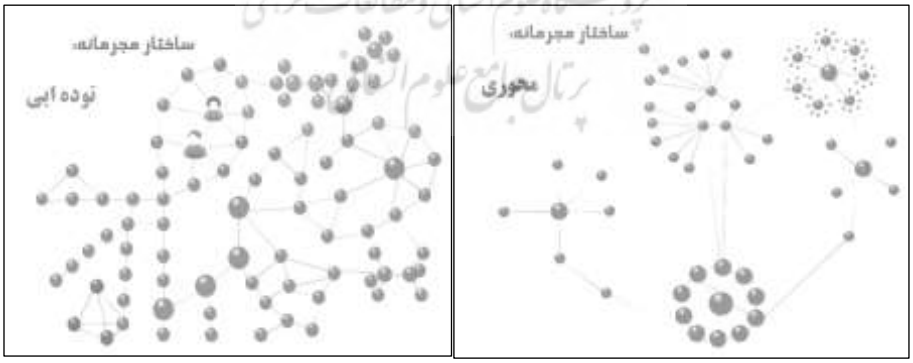
کرد و از این جهت، اعمال تعریف ماده مربوطه در کنوانسیون بر گروه‌های سازمان‌یافته موجود در فضای سایبر خالی از اشکال نخواهد بود.

با درنظرگرفتن مطالب ارائه‌شده و ماهیت خاص فضای سایبر می‌توان نتیجه گرفت ساختار گروه‌های مجرمانه در جرائم سایبری تا حد زیادی از ساختارهای هرمی و مافیایی از جهت انعطاف‌پذیری، ناپایدار، متغیر و سیال‌بودن در جرائم سنتی متفاوت است (Brenner, 2002: 1). این ایده که جرائم سایبری، به دلیل ماهیت منحصربه‌فرد خود، ساختارهای مجرمانه متفاوتی را ارائه می‌کنند، موجب شد تا در سال ۲۰۱۲ گونه‌شناسی جدیدی از سوی برخی پژوهشگران مطرح گردد. *مایک مک‌گوایر*[۴۴] بر مبنای پژوهش‌های خود، از مطالعه حدود ۵۰۰ پرونده ثبت شده مربوط به جرم سایبری، نتیجه گرفت که بیش از ۸۰ درصد از فعالیت‌های مجرمانه ارتکابی در فضای سایبر محصول برخی از اشکال فعالیت‌های سازمان‌یافته می‌باشند(۱۶) و گروه‌های مجرمانه سازمان‌یافته سنتی، فعالیت‌های مجرمانه خود را با انواع جدیدتر و متغیر از شبکه‌های مجرمانه به دنیای دیجیتالی وارد کرده‌اند (BAE Systems Detica, 2012: 3). گونه‌شناسی وی بر مبنای درجه مشارکت گروه‌ها در فعالیت‌های آنلاین و ساختار مشارکت در داخل گروه ارائه شد. بر این اساس، گونه‌شناسی وی از سه مجموعه شکل گرفته است که در ادامه به بررسی هریک از آنها می‌پردازیم.

۴-۲-۱. گروه‌های مجرمانه آنلاین

این گروه‌ها در ارتکاب جرم به‌صورت آنلاین، فعالیت دارند و می‌توانند به دو زیرگروه توده‌ای[۴۵] و محوری[۴۶] تقسیم‌بندی شوند. زیرگروه‌ها اغلب مجازی بوده و اعتماد میان اعضا از طریق میزان شهرت در انجام فعالیت‌های غیرقانونی آنلاین سنجیده می‌شود.

نمودار (۱)-گروه‌های مجرمانه آنلاین



44. Dr. Mike McGuire
45. Swarms
46. Hubs

۴-۲-۱-۱. ساختارهای توده‌ای

این گروه‌ها بسیاری از ویژگی‌های شبکه‌های مجرمانه را دارا بوده و به ساختارهای سازمان‌نیافته و غیرمتمرکز با هدفی مشترک برای ارتکاب جرم، بدون داشتن رهبری خاص و البته بعضاً دارای حداقلی از زنجیره دستورات توصیف می‌شوند. چنین ساختارهایی ممکن است در انجام عملیات مجرمانه خود به شیوه‌هایی که یادآور عملیات گروه‌های هکتیویست[۴۷] است، به‌صورت ویروسی عمل کنند. توده‌ها در زمینه‌هایی که ازنظر مفهومی، آنلاین‌محور می‌باشند، مانند مخالفت‌ها و مقاومت‌های سیاسی، بیشترین فعالیت را دارند. گروه مشهور هکرهای ناشناس[۴۸] در این دسته قرار می‌گیرد. ساختار گروه مجرمانه باشگاه سرزمین عجایب[۴۹] را می‌توان، با توجه به اطلاعات موجود، یک ساختار توده‌ای تلقی کرد که در آن گروهی از کودک‌بازها،[۵۰] بدون اینکه واجد رهبر خاصی باشند، با یک ایده مشترک به‌صورت شبکه‌ای گرد یکدیگر جمع شده و به‌صورت غیرمتمرکز با به اشتراک‌گذاری تجربیات خود اقدام به برقراری ارتباط با کودکان از طریق تالارهای آنلاین، آماده‌سازی آنان برای ارتکاب عمل جنسی و درنهایت تحصیل پورنوگرافی کودکان و انتشار آنها می‌کردند (Harlow et al, 2003: 115).

از منظر اجرای قانون، ماهیت غیرمتمرکز، موقتی و سلولی توده‌ها با سلسله دستورات غیرواضح، می‌تواند چالش‌هایی برای پلیس در جلوگیری از گسترش این گروه‌ها به دنبال داشته باشد. از طرف دیگر این واقعیت که توده‌ها اغلب تازه‌کار می‌باشند و گزینش اعضا در آنها به‌صورت دقیق صورت نمی‌گیرد، علاوه‌بر فقدان رهبر مشخص، می‌تواند فراهم‌آورنده فرصت‌های خوبی در انجام تحقیقات پلیسی تلقی شود.

۴-۲-۱-۲. ساختارهای محوری

همانند توده‌ها، ساختارهای محوری به‌صورت آنلاین فعالیت دارند، اما ساختار فرماندهی در آنها مشخص‌تر است. این گروه‌ها دارای یک نقطه کانونی به نام محور، متشکل از رؤسا و رهبران اصلی، می‌باشند که در اطراف آنها شرکای جانبی گرد می‌آیند. فعالیت‌های آنلاین آنها طیف وسیعی از رفتارهای مجرمانه را ازجمله توزیع غیرمجاز نرم‌افزارها، حملات فیشینگ، راه‌اندازی باتنت‌ها، جرائم جنسی آنلاین و توزیع ترس‌افزارها[۵۱] با مقاصد متعدد مالی یا غیرمالی را دربر می‌گیرد. گروه مجرمانه معروف به لولزسِک[۵۲] و بازارهای مربوط به مواد مخدر مانند جاده ابریشم[۵۳] از این الگو پیروی می‌کنند. گروه معروف درینک اُر دای[۵۴] به‌عنوان یکی از انواع

47. Hacktivist
48. Anonymous
49. Wonderland Club
50. Pedophile
51. Scareware
52. Lulz Security (LulzSec)
53. Silk Road. (United States of America v Ross William Ulbricht, 2013)

ائتلافات و ارز در به اشتراک‌گذاری آثار به‌دست‌آمده درنتیجه نقض حق تکثیر، برخوردار از چنین ساختاری بود. با تحلیل ساختار این گروه‌ها و درنظرگرفتن سناریوی ورز[۵۵] می‌توان به نکات زیر پی برد:

۱) ساختارهای محوری در تخصیص و انجام وظایف از سازمان‌یافتگی برخوردار هستند؛

۲) سیال‌بودن این سازمان‌یافتگی در هر زیر گروه بیشتر می‌شود؛

۳) رهبر در گروه‌های مجرمانه آنلاین با ساختار نقش والا، مشاور متخصص و هدایتگر تمام مجموعه را ایفا می‌کند؛

۴) رهبران محلی در هر کشور از خودمختاری برخوردارند و موقعیت آنان از حیث اهمیت ذیل مؤسس اصلی شبکه قرار نمی‌گیرد، بلکه در عرض سایر رهبران شکل می‌گیرد.

از دیدگاه پلیسی، نفوذ به درون محورها مشکل‌تر است، به‌ویژه اینکه این گروه‌ها از کدها و علائمی استفاده می‌کنند که کشف آنها بسیار مشکل است. اما از طرف دیگر این گروه‌ها دارای ساختار فرماندهی روشنی می‌باشند که می‌تواند عملیات کلیدی اجرای قانون علیه مهره‌های کلیدی گروه را در خود متمرکز کند (UNODC, 2013: 46).

۴-۲-۲. گروه‌های مجرمانه دوفضایی

در این دسته، گروه‌ها هم در فعالیت‌های مجرمانه آنلاین و هم آفلاین دخالت دارند و به‌عنوان گروه‌هایی ترکیبی[۵۶] و دوفضایی توصیف می‌شوند که می‌توان آنها را به دو زیرگروه ترکیبی دسته‌ایی[۵۷] و ترکیبی گسترده تقسیم کرد.[۵۸] طبق پژوهش مک‌گوایر بیش از ۶۰ درصد گروه‌های مجرمانه در فضای سایبر، دارای ساختاری متشکل از این دو زیرگروه هستند.

۴-۲-۲-۱. ساختارهای ترکیبی دسته‌ایی

در این گروه، ارتکاب جرم توسط جمع به‌نسبت کوچکی از افراد صورت می‌گیرد. فعالیت‌های مجرمانه این گروه‌ها پیرامون جرائم خاص با اتخاذ روش‌های خاصی می‌چرخد. ساختار این گروه‌ها تا حد زیادی شبیه گروه محوری است اما به‌طور پیوسته در هردو فضای آنلاین و آفلاین مرتکب جرم می‌شوند. یکی از معمول‌ترین فعالیت‌های مجرمانه این گروه‌ها، سرقت اطلاعات کارت‌های اعتباری و استفاده از آنها به‌منظور خرید آنلاین یا فروش اطلاعات از طریق شبکه‌های خریدوفروش کارت‌های اعتباری[۵۹] است (Soudjin et al, 2012: 111-129).

---

54. DrinkOrDie
55. Warez Scene
56. Hybrids
57. Clustered Hybrid
58. Extended Hybrids
59. Carding Networks

محل حضور گروه‌هایی که درتولید ورز یا نرم‌افزارهای قفل شکسته را صحنه ورز یا به اصطلاح «صحنه» می‌گویند.

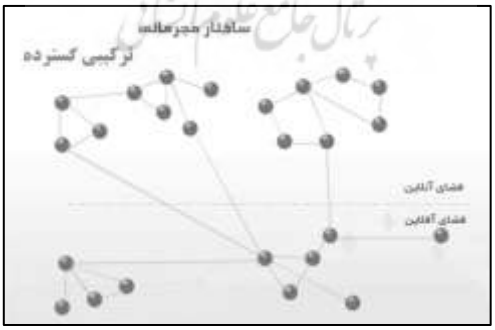
نمودار (۲)- ساختارهای ترکیبی دسته‌ایی

۴-۲-۲-۲. ساختارهای ترکیبی گسترده

ازنظر عملکرد شبیه زیرگروه ترکیبی دسته‌ایی است، ولی تمرکز اعضا در آن بسیار کمتر است. این گروه‌ها از گردآمدن تعداد زیادی شرکا و زیرگروه‌ها شکل می‌گیرد و نسبت به ارتکاب طیف گسترده‌ای از فعالیت‌های مجرمانه اقدام می‌نماید، اما مقداری از هماهنگی را به‌منظور اطمینان از موفقیت در عملیات، حفظ می‌کند.

از دیدگاه پلیسی، گروه‌های دسته دوم به دلیل دارا بودن ساختارهای چند پیوندی و زنجیرهایی که تنها از طریق راهبرد و عملیات خاص می‌توان آنها را هدف قرار داد، می‌توانند بسیار گمراه‌کننده باشند. حضور بیشتر این گروه‌ها در فضای واقعی می‌تواند در تداوم ساختارهای فرماندهی آنها و تمرکز بیشتر بر طرح‌های مجرمانه، مؤثر واقع شود؛ اگرچه این واقعیت که چنین گروه‌هایی می‌توانند تا حدودی با یکدیگر هماهنگ شوند، فرصت‌های مطلوبی برای اتخاذ رویکردهای جامع پلیسی و اقدامات متوالی علیه عملیات اعضای آنها ایجاد می‌کند (BAE Systems Detica, 2012: 4).

نمودار (۳)- ساختارهای ترکیبی گسترده



۴-۳. گروه‌های مجرمانه مهاجر

با مطالعه برخی گزارش‌ها می‌توان به وجود دسته‌ای از گروه‌های تبهکارانه پی‌برد که بیشتر به‌صورت آفلاین فعالیت دارند، اما از فناوری آنلاین به‌منظور تسهیل ارتکاب رفتارهای مجرمانه خود بهره می‌برند. این گروه‌ها به دلیل مشارکت بسیار زیاد در ارتکاب جرائم سنتی مهاجرت کرده به فضای آنلاین، نظیر کلاهبرداری، حائز اهمیت می‌باشند و تعداد آنها از یک دهه قبل رو به افزایش بوده است. بسته به درجه همبستگی و سازمان‌دهی، برای این گروه می‌توان دو زیرگروه متصور شد: هرمی[۶۰] و مجتمع.[۶۱]

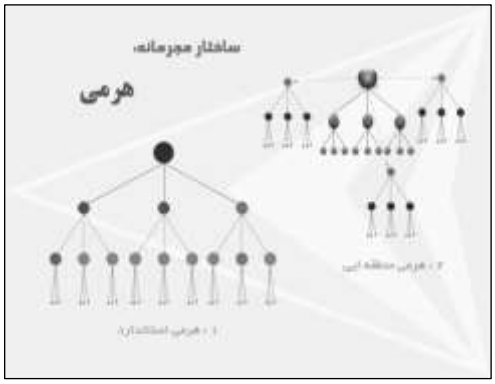
۴-۳-۱. ساختارهای هرمی

به دلیل وجود مزایای ویژه در استفاده از شبکه جهانی اینترنت در فائق‌آمدن بر الگوهای سنتی اجرای قانون، از دیدگاه نظری احتمال حضور گروه‌های سازمان‌یافته سنتی در قالب‌های جدید در این فضا وجود دارد. با این وجود، پژوهش‌های ملی و منطقه‌ایی نشان می‌دهند شاخص‌ترین گروه‌های مجرمانه سنتی، نظیر خانواده‌های تبهکار، با همان ساختارهای سنتی سلسله‌مراتبی به‌قصد ارتکاب جرائم وارد فضای سایبر شده‌اند. به‌عنوان نمونه علاقه سنتی برخی گروه‌های مافیایی به روسپیگری، اکنون به ایجاد وب‌سایت‌های پورنوگرافی گسترش‌یافته است. دیگر مثال‌ها شامل ایجاد کازینوهای آنلاین، قماربازی و اخاذی از طریق تهدید به خاموش‌کردن سیستم‌ها است. اتحادیه‌های فراملی سازمان‌یافته‌ای مانند یاکوزا[۶۲] در ژاپن و مثلث‌های چینی[۶۳] در هنگ‌کنگ، در دو دهه قبل اقدام به ارتکاب جرائمی مانند قاچاق پول،[۶۴] تکثیر و توزیع غیرقانونی نرم‌افزارها و تقلب در کارت‌های اعتباری کرده‌اند. همچنین *امام سامودرا* با تشویق اعضای ائتلاف مجرمانه خود در فضای واقعی نسبت به تقلب در کارت‌های اعتباری در فضای سایبر اقدام می‌نمود.(۱۷) بنابراین، برخلاف آنچه فرض گرفته شد، گروه‌های سازمان‌یافته سنتی نیز نسبت به توسعه بازارهای مجرمانه خود در فضای سایبری گام برداشته‌اند و جالب‌توجه است که ساختار اولیه و انعطاف‌ناپذیر گروه‌های هرمی در فضای آفلاین با انتقال به فضای آنلاین تغییری نمی‌کند، اما گزارش‌های ارائه‌شده حاکی از آن است که برخی از این تشکل‌ها، پس از ورود به فضای سایبر در جذب اعضای جدید و ارتکاب فعالیت‌های مجرمانه حالت شبکه‌ای، غیرمتمرکز و عرضی به خود می‌گیرند (Group IB, 2011: 7). چنین گروه‌هایی از ماهیتی کاملاً منحصربه‌فرد تبعیت می‌کنند که در عین دوفضایی بودن از دو ساختار مجزا و منطبق با محیط

60. Hierarchies
61. Aggregates
62. Yakuza
63. Chinese Triads
64. Money Muling

حاکم برخوردار هستند، ساختار هرمی در فضای آفلاین و ساختار محوری یا ترکیبی (گسترده یا دسته‌ایی) در فضای آنلاین.

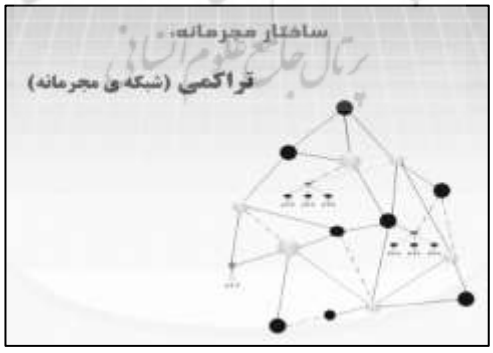
نمودار (۴)- ساختارهای هرمی



۴-۳-۲. ساختارهای مجتمع

ساختارهای مجتمع با سازمان‌یافتگی موقت، سیال و اغلب بدون هدف مشخص هستند، شبیه آنچه در پژوهش سازمان ملل متحد به‌عنوان شبکه‌های مجرمانه معرفی شد. این گروه‌ها از فناوری دیجیتالی به صورت موردی[۶۵] بهره می‌برند که به‌هرحال می‌تواند منجر به ایجاد ضرر شود. استفاده از بلک‌بری[۶۶] یا دیگر تلفن‌های همراه به‌منظور ایجاد هماهنگی برای فعالیت‌های گروهی یا برهم‌زدن نظم عمومی از زمره شیوه‌های عملکرد این گروه‌ها است؛ همانند آنچه در شورش سپتامبر ۲۰۱۲ استرالیا (ایالت ولز جنوبی) در اعتراض به فیلم ضداسلامی بی‌گناهی مسلمانان[۶۷] صورت گرفت.

نمودار (۵)- ساختارهای مجتمع



65. Ad Hoc
66. BlackBerry
67. Innocence of Muslims

در ارتباط با گروه‌های دسته سوم نیز سطح دانش پیشرفته مأموران پلیس از ساختار و ترکیب این گروه‌ها، درصورتی‌که با مهارت و سرعت در کشف، تحقیق و مقابله همراه باشد، می‌تواند امتیاز مطلوبی در مقابله هرچه بهتر با ساختارهای سازمان‌یافته مجرمانه تلقی شود. اما این واقعیت که این گروه‌ها از ابزارهای دیجیتالی بهره می‌برند و تعدادی از آنها، چون خانواده‌های بزرگ مافیایی، قدرتی ورای قانون و نهادهای مجری آن دارند از موانع عمده‌ایی است که مأموران مجری قانون را در تحقق اهداف عدالت کیفری ناتوان می‌سازد.

اکنون پاسخ به این پرسش ضروری به نظر می‌رسد که آیا در ایران که از کشورهای با بیشترین کاربر اینترنتی میان کشورهای خاورمیانه و دنیا محسوب می‌شود،[۱۸] جرائم سایبر، شکل سازمان‌یافته به خود گرفته‌اند یا خیر؟

در ابتدای بحث ذکر دو نکته لازم است. نخست آنکه متأسفانه در سطح ملی تحقیقات لازم در این زمینه صورت نگرفته است. با این‌وجود، نظر به ماهیت خاص فضای سایبر، بعد فراملی آن و مطالعه اخباری که گهگاه از طریق وب‌سایت رسمی مرکز بررسی جرائم سازمان‌یافته[۱۹] و پلیس فتا در مورد مجرمان سایبر منتشر می‌شود می‌توان تا حدی به این پرسش‌ها پاسخ داد. البته ناگفته نماند که هرگونه نتیجه‌گیری در این راستا، به دلیل فقدان اطلاعات لازم، باید در کمال احتیاط صورت گیرد. دوم اینکه با بررسی منابع و اخبار رسمی می‌توان تا حدودی به این نتیجه نائل شد که مجرمان سایبری در ایران، در ارتکاب بسیاری از جرائم علیه اموال در فضای سایبر، مانند کلاهبرداری، جرائم مربوط به افترا و هتک حیثیت به میزان زیادی به‌صورت انفرادی عمل می‌کنند، ولی در زمینه جرائم علیه اخلاقیات، دین، نظام سیاسی، تروریسم، قاچاق موادمخدر، داروهای غیرقانونی و نقض حق تکثیر با ایجاد ساختاری سازمان‌یافته تشکیل می‌شوند و با حمایت دولت‌ها یا سازمان‌های منطقه‌ایی در قالب شبکه‌ای اقدام می‌کنند. از علل این امر می‌توان به گسترده‌بودن دامنه فعالیت به‌منظور تحقق اهداف خرابکارانه، جذب طرفداران بیشتر و بازاریابی وسیع برای فروش یا به اشتراک‌گذاری محصولات و محتویات غیرقانونی خود، اشاره کرد. درهرحال، اخذ نتایج دقیق‌تر نیازمند در دسترس‌بودن منابع تحلیلی و آماری موثق است. در ادامه به تجزیه و شرح ساختار یک گروه سازمان‌یافته شناخته‌شده می‌پردازیم که از فضای سایبر به‌منظور ارتکاب جرم در ایران بهره برد.

طبق اطلاعات ارائه‌شده توسط مرکز، در پرونده معروف به مضلین ۲ سردسته اصلی شبکه با ثبت دامنه و راه‌اندازی سایت‌های غیراخلاقی و غیرقانونی «آویزون» و «ایران سکس» از کانادا اقدام به انتشار محتوای پورنوگرافی و مطالب حاوی تصاویر و فیلم‌های مستهجن پرداخت. با توسعه سایت و نیاز به تمرکز بر فعالیت بیشتر، وی از طریق محیط سایت‌های ایجادشده و تالار گفتگو، نسبت به جذب و به‌کارگرفتن بیش از ۲۰ مدیر جانبی اقدام کرد.

شبکه مضلین ۲ را می‌توان یکی از مصادیق بارز ساختارهای محوری دانست که در اطراف مدیر اصلی، به‌عنوان نقطه کانونی، اعضای جانبی، از اقصی نقاط داخل و خارج کشور باهدف مشخصی گرد آمده و در امور محوله از خودمختاری برخوردار می‌باشند. وظیفه هر یک از مدیران میانی تعریف شده بود و هریک مسئولیت‌های مجزایی را در اداره سایت، تالارها و انجمن‌های مختلف برعهده گرفته بودند.

نمودار (۶)- ساختار گروه سازمان‌یافته مضلین ۲

فرماندهی مدیر اصلی در این پرونده، معلول تخصص بیشتر وی در امر مدیریت سایت و آشنایی با امور رایانه‌ای بود (ویدیو اعترافات متهمان پرونده مضلین ۲، وب‌سایت گرداب). از این‌رو، نظریه افتراق مفهوم قدرت در رهبری گروه جنایی سایبری، دست‌کم در ساختارهای مجرمانه آنلاین در ایران قابل تأیید است. ماهیت سیال این ساختار، نه‌تنها از آزادی عمل مدیران در مدیریت دیگر بخش‌های سایت مشخص می‌شود، بلکه حتی مدیر اصلی، به‌عنوان مؤسس سایت و طراح نخست جذب اعضا و همچنین برخی از دیگر اعضا در وب‌سایت‌های مشابه دیگر (نظیر «بیا کلیپ») نقش‌های فرعی را در عرض دیگر مدیران بر عهده داشته‌اند که این واقعیت، یادآور پیوند بین گروهی ساختارهای مجرمانه محوری و ایجاد شبکه گسترده‌تر از افرادی است که در انعقاد پیمان جنایی مشارکت می‌کنند. مطرح‌نبودن ساختار هرمی به دلیل مصداق نداشتن قدرت فیزیکی موجب شد تا برخلاف گروه‌های مجرمانه سنتی، فعالیت مدیران جانبی بر مبنای همکاری و تشریک مساعی در عرض یکدیگر، بدون تبعیت از زنجیره دستورات، شکل گیرد.

۵. جرم سایبری سازمان‌یافته و بازارهای سیاه مجرمانه

از سال ۲۰۰۵ میلادی، با ظهور و گسترش گروه‌های سازمان‌یافته در فضای سایبر و درآمدهای سرشار حاصل از عضویت در این گروه‌ها، پدیده‌هایی شبیه آنچه در دنیای واقعی به‌عنوان بازار سیاه[۶۸] نامیده می‌شوند، به‌ویژه در کشورهای اروپای شرقی نظیر رومانی و اوکراین (Bhattacharjee, 2011: 82)، پدیدار گشت. این بازارها که می‌توان آنها را کارآفرینان اقتصاد غیررسمی دانست (McCarthy, 2011) به‌عنوان ساختاری شناخته می‌شوند که در آن اعضای شرکت‌های مجرمانه با نقش‌های متعدد، ازجمله کدنویسی، فروشندگی، متخصص فنی، هکر، میزبانی، ریاست و رهبری، صندوق‌داری، دلالی و قاچاقچی پول و غیره) در فرایند ایجاد بدافزارها، پخش ویروس‌های رایانه‌ای (برای مثال از طریق ایمیل‌های فیشینگ)، مدیریت بات‌نت، جمع‌آوری اطلاعات مالی و شخصی، فروش داده‌ها و نقدکردن اطلاعات مالی دخالت دارند و بدین ترتیب موجب تکوین صنعت مجرمانه[۶۹] در فضای سایبر شده‌اند.

درمجموع، بازار را می‌توان به‌عنوان شبکه‌ای اجتماعی از افراد درگیر در فعالیت‌های مجرمانه سازمان‌یافته توصیف و تعریف کرد (Spapens, 2010: 213) که اغلب به‌صورت موقت و در برخی موارد برای مدتی کمتر از شش ماه فعالیت می‌کند (BAE Systems Detica, 2012: 5). باوجود کمبود منابع پژوهشی می‌توان افراد و گروه‌های کوچک مجرمانه، نظیر برنامه‌نویسان اصلیِ بدافزارها و مالکان بات‌نت را تشکیل‌دهنده هسته اصلی بازار دانست که در اطراف آنها دیگر شرکا، توده‌ها و محورها که طبق برخی پژوهش‌ها با طراحان اصلی بازار دارای مؤلفه‌های زبانی و فرهنگی مشترک هستند، فعالیت دارند (Yip, 2011: 3).

نکته قابل ذکر این است که بازارهای زیرزمینی[۷۰] علاوه‌بر اینکه خود دارای ساختاری سازمان‌یافته می‌باشند، منبع تغذیه و تقویت دیگر ساختارهای مجرمانه نیز قلمداد می‌شوند. گردش صنعت مجرمانه در فضای سایبر از طریق تبادل اطلاعات، وساطت برای دادن مشاوره فروش، ایجاد سرویس‌های توزیع ویروس، اجاره بات‌نت، فروش سرویس‌های انتشار هرزنامه، تهیه فهرست ایمیل‌ها و جزئیات اطلاعات مالی، درواقع نتیجه فعالیت چرخه جنایی[۷۱] است که در محیط‌هایی نظیر تالارهای گفتگو و انجمن‌های زیرزمینی و از مشارکت مجرمان متعدد با وظایف مجزا و تخصیص‌یافته ایجاد شده است (Tropina, 2012: 160). از آنجا که سهامداران طرح‌های مجرمانه(۲۰) با ارائه طیف گسترده‌ایی از نرم‌افزارهای غیرقانونی (نظیر تروجان‌های مخرب و نرم‌افزارهای کاوشگر)، زیرساخت‌ها (نظیر بات‌نت و سیستم‌های میزبانی)، سیستم‌های جلوگیری از کشف جرم و غیره به مشتریان خود (مباشران و شرکای جرم) در بازارهای

68. Black Market
69. Criminal Industry
70. Underground
71. Criminal Ecosystem

غیرقانونی، فناوری را به‌عنوان ابزاری در خدمت تهاجم به افراد، شرکت‌ها و زیرساخت‌ها بـه کـار بسته‌اند، ماهیت خدمت‌رسانی فناوری اطلاعات و ارتباطات نیز بـر رشـد سـریع‌تـر ایـن صـنعت مجرمانه در بازارهای زیرزمینی تأثیر شدیدی داشته است (McAfee, 2013).[۷۲]

نمودار (۷)- چرخه بازارهای سیاه

در ایران، توجه مخاطرات و تهدیدات جرائم سازمان‌یافته به «فضای تولید و تبادل اطلاعات» (فتا) و لزوم ایمن‌سازی شبکه‌ها و زیرساخت‌های الکترونیکی حیاتی که به نحوی با امنیت ملـی گره خورده‌اند، برای نخستین‌بار در مصوب هیئت وزیـران درخصـوص تعیـین «سـند راهبـردی امنیت فضای تولید و تبادل اطلاعات کشور» مورد توجه قرار گرفت. برنامه پـنجم توسـعه (۹۴-۱۳۹۰) «به‌منظور بسط خدمات دولت الکترونیک، صنعت فناوری اطلاعـات، سـواد اطلاعـاتی و افزایش بهره‌وری در حوزه‌های اقتصادی، اجتمـاعی و فرهنگـی» از یـک‌سـو، وزارت اطلاعـات و ارتباطات را مکلف کرد تا نسبت به ایجاد و توسعه شبکه ملی اطلاعات و مراکز داده داخلی امـن و پایدار اقدام کند و از سوی دیگر، به‌موجب این قانون کلیه دستگاه‌های اجرایی مکلف شدند تـا ضمن اتصال به شبکه ملی اطلاعات و توسعه و تکمیل پایگاه‌های اطلاعاتی خود حداکثر تا پایان سال دوم، اطلاعات خود را در مراکز داده داخلی با رعایت مقررات امنیتـی و اسـتانداردهای لازم نگهداری و به‌روزرسانی نمایند و تا پایان برنامه، خدمات قابل ارائه خود را به‌صـورت الکترونیکـی از طریق شبکه ملی اطلاعات عرضه نمایند» (قانون برنامه پنجم توسعه، ۱۳۸۹: بند ب و ج ماده ۴۶).

72. Crimeware (Cybercrime or infrastructure or Hacking) as-a-Service.

ماده ۲۳۱ قانون برنامه پنجم، طرحی دومرحله‌ای را به‌منظور تأمین امنیت برای تمام نهادها و سازمان‌های دولتی و غیردولتی ارائه‌دهنده زیرساخت‌های حیاتی الکترونیک، پیش‌بینی کرد تا هر نهاد در چارچوب «سند افتا» نسبت به ایجاد و حفظ امنیت تبادل اطلاعات تا پایان سال ۱۳۹۲ اقدام کرده و سپس با اجرای استانداردهای افتا در مسیر اجرای سامانه مدیریت اطلاعات گام بردارد. برخلاف چنین انتظاری، با گذشتن چندسال از زمان مورد نظر همچنان بسیاری از نهادها نسبت به ایمن‌سازی استاندارد سامانه‌های رایانه‌ای خود، اقدامات مؤثری به عمل نیاورده‌اند که از مهم‌ترین دلایل آن کمبود بودجه و ظرفیت‌های فنی و پرسنلی کشور به شمار می‌رود.

فرجام

این فرض که همانند مجرمان منفرد، این امکان وجود دارد که گروه‌هایی با ساختارهایی نوین که محصول ماهیت منحصربه‌فرد فضای سایبر می‌باشند، از طریق استخدام، جذب و به‌کارگیری اعضای متخصص، از اقصی نقاط دنیا، شکل گرفته و با انگیزه‌های متعدد و نه صرفاً سودجویی، به‌قصد ارتکاب جرائم متعدد در فضای سایبر به فعالیت بپردازند، صحت دارد.

در فضای واقعی ساختارهای هرمی در راستای سازمان‌دهی تعاملات انسانی و تضمین نیل به هدف مجرمانه به‌صورت عمودی، متمرکز، غیرقابل انعطاف و ثابت شکل گرفته‌اند. ظهور فضای سایبر منجر به پدید آمدن نسل جدیدی از سازمان‌دهی در سناریوی مجرمانه شده است به‌نحوی‌که الگوهای متشکل مجرمانه نظیر توده‌ها و محورها در این فضا، بر خلاف اشکال سنتی ساختارهای مجرمانه هرمی، به‌صورت عرضی، افقی و با ماهیتی سیال و متغیر، به وجود آمده‌اند، بدون اینکه از سلسله دستورات و فرماندهی قوی، حاکم و مشخصی تبعیت کنند.

با توجه به مهاجرت گروه‌های مجرمانه‌ای همچون خانواده‌های تبهکار به فضای اطلاعات و ارتباطات و ارتکاب جرائم سنتی یا نوین در بستر این فضا، این پندار درست نیست که امکان فعالیت ساختارهای مجرمانه سنتی در فضای سایبر، به دلیل غیرقابل انعطاف‌بودن و دارابودن سرشت سلسله‌مراتبی وجود ندارد، اما می‌توان نتیجه گرفت این ساختارها در تلاش برای گسترش فعالیت‌های غیرقانونی خود و جذب اعضای جدید در فضای سایبر با تغییر شکل روبه‌رو شده و به‌صورت شبکه‌ای عرضی هماهنگ می‌شوند. لذا می‌توان به‌درستی این فرض که ساختارهای مجرمانه در شکل‌گیری تا حد زیادی متأثر از فضای حاکم بر ایجاد آنها می‌باشند نه ماهیت جرم ارتکابی پی برد.

پیدایش الگوهای نوین ساختارهای مجرمانه آنلاین سازمان‌یافته، چالش‌های متعددی را برای مأموران مجری قانون به‌منظور شناسایی و دستگیری هسته‌های اصلی گروه و پیشگیری از عملیات موضوع قرارداد مشارکت مجرمانه ایجاد کرده است. ماهیت سیال، متغیر و موقتی این گروه‌ها موجب از بین رفتن تمام امتیازاتی شده است که نیروهای پلیس و واحدهای کشف جرم

تاکنون در ارتباط با جرائم سازمان‌یافته سنتی از آنها برخوردار بودند. استفاده از فناوری ارتباطات ناشناس، خودکارشدن حملات و پراکندگی اعضای گروه‌های مجرمانه در کشورها و نقاط مختلف دنیا، از مهم‌ترین چالش‌هایی هستند که شکل جدید سازمان‌دهی مجرمانه در فضای سایبر پدید آورده است. در صورت تداوم وضعیت بیم آن می‌رود که جرم سایبر از یک الگوی تجاری فراملی صرف به سمت صنعتی غیرقانونی و سازمان‌یافته با ابعاد بین‌المللی حرکت کند؛ صنعتی که در دست کارتل‌ها، سندیکاها و اتحادیه‌های پیچیده اداره می‌شود. حل این مشکلات، علاوه‌بر ضرورت به‌روزکردن چارچوب‌های قانونی و ایجاد هماهنگی میان قوانین، نیازمند اتخاذ یک رویکرد جامع بلندمدت متضمن همکاری و هماهنگی بین‌المللی و فهم این درک منطقی است که هیچ کشوری نمی‌تواند به‌تنهایی در برابر فرصت‌های مجرمانه‌ای که فناوری اطلاعات و ارتباطات ایجاد کرده است، پایداری کند. بنابر مراتب ذکرشده، افزایش مشارکت میان مأموران مجری قانون و متخصصان فنی، در کنار همکاری با بخش خصوصی و مؤسسات دانشگاهی به‌منظور آموزش و افزایش توانمندی‌های پرسنلی و ایجاد فرصت‌های تحقیقی جدید در ارتباط با زوایای پنهان فناوری‌های مدرن اطلاعات توصیه می‌شود.

در ارتکاب جرائم سایبر بازیگران اصلی صحنه جرم، برخلاف جرائم سنتی، ماشین‌ها و نرم‌افزارهای مختلف هستند. در فضای سایبر حملات متعددی نظیر دی‌داس از طریق ربات‌های شبکه (بات‌نت) سازمان‌دهی می‌شوند و بعضاً در ورای ارتکاب این حملات، درعمل هیچ‌گونه تشکل انسانی وجود ندارد. در بسیاری از آثار حقوقی تعریف جرم سازمان‌یافته سایبر متأثر از واقعیت‌های دنیای فیزیکی است. بنابراین، به‌منظور مقابله مؤثرتر با این جرائم، پیشنهاد می‌شود در مواردی که هیچ گروه سازمان‌یافته‌ای در ارتکاب جرم دخیل نبوده است، ولی حملات به دلیل طراحی هدفمند و برنامه‌ریزی ماشین‌ها و نرم‌افزارها، ماهیتاً نظام‌مند و سازمان‌یافته ارتکاب یافته‌اند، نیز جرم سازمان‌یافته تلقی شود.

با توسعه دولت الکترونیک در ایران و انتقال زیرساخت‌های حیاتی به شبکه ملی اطلاعات موج حملات سازمان‌یافته گروه‌های مجرمانه در آینده علیه این زیرساخت‌ها افزایش خواهد یافت. بنابراین پیش‌بینی و تجهیز سازوکارهای لازم برای تأمین امنیت سامانه‌ها و سیستم‌های رایانه‌ای قبل از پیاده‌سازی زیرساخت‌ها در بستر شبکه تبادل اطلاعات از اهمیت فزاینده‌ای برخوردار است. این در حالی است که با گذشت شش سال از تصویب قانون پنجم توسعه همچنان انتظارات این قانون برآورده نشده است. از سوی دیگر در زمینه پاسخ به جرم نیز در قوانین مربوط به این فضا خلأها و ایراداتی وجود دارد که مهم‌ترین آنها را می‌توان بدین ترتیب برشمرد:

۱- بسیاری از قوانین و اسناد بین‌المللی درباره پیش‌بینی سازوکارهای لازم برای مقابله با مجرمان سایبری ماهیت خاص فضای تبادل اطلاعات و ارتباطات را در نظر نگرفته‌اند. این

تساهل در سطح ملی پررنگ‌تر است. به‌عنوان‌مثال موضوع همکاری‌های بین‌المللی و منطقه‌ایی، سازوکارهای ایجاد آنها، نقش بخش خصوصی در این راستا از مهم‌ترین عناصری هستند که در قانون جرائم رایانه‌ای کشور و قانون آیین دادرسی مربوط به آن نادیده گرفته شده‌اند. از این جهت به یکی از مهم‌ترین اقتضائات مبارزه با جرم فراملی سایبری پرداخته نشده است.

۲- زمزمه‌هایی از عزم ایران برای عضویت رسمی در سازمان همکاری‌های شانگهای (SCO) به گوش می‌رسد. در صورت به واقعیت پیوستن این امر، نخستین گام منطقه‌ای و فراملی ایران به‌منظور تضمین امنیت فضای اطلاعات و ارتباطات محور سیستم‌ها و شبکه‌های رایانه‌ای و نیل به اهداف عدالت کیفری در این عرصه می‌تواند از طریق الحاق به توافقنامه همکاری در زمینه تأمین امنیت اطلاعات بین‌الملل (توافقنامه سازمان همکاری‌های شانگهای) برداشته شود تا ضمن هماهنگ‌سازی قوانین، سازوکار جمع‌آوری و دسترسی فراملی به ادله، توسعه نظام همکاری‌های متقابل منطقه‌ایی و اجتناب از ایجاد پناهگاه‌های امن برای مجرمان سازمان‌یافته سایبری، نسبت به ظرفیت‌سازی و افزایش توان فنی مأموران مجری قانون داخل و خارج از کشور، تمهیدات، سازوکارها و زیرساخت‌های لازم در نظر گرفته شود. تعامل نزدیک با اداره مبارزه با جرم و مواد مخدر سازمان ملل متحد می‌تواند در این زمینه برای ایران بسیار حیاتی تلقی شود. کلید این تعامل در سال‌های قبل زده شده است و باید بر حفظ، استمرار و توسعه آن اصرار ورزید.

پی‌نوشت‌ها:

(۱) در یکی از پژوهش‌های سازمان ملل متحد به این نکته اشاره شده است که: ماهیت جرائم سایبری ضرورتاً نیازمند سازمان‌دهی تعداد زیادی از منابع انسانی و ابزاری است (ر.ک. UNODC, 2013: 114).

(۲) قانون تشدید مجازات مرتکبان اختلاس، ارتشا و کلاهبرداری، ماده ۴، مصوب ۱۳۶۷. برای کسب اطلاعات بیشتر ر.ک: (میرمحمدصادقی، ۱۳۹۲: ۲۲۰).

(۳) قانون مجازات اخلالگران در نظام اقتصادی کشور، بند «و» ماده ۱، مصوب ۱۳۶۹.

(۴) به نظر می‌رسد اقدام قانون‌گذار در محدود نکردن تبصره ماده ۱۳۰ قانون مجازات اسلامی به لزوم وجود قصد منفعت‌طلبی و سودجویی کاملاً عامدانه صورت گرفته است. حاکمیت ارزش‌های اسلامی- اخلاقی و روح امنیت‌محوری در تدوین بسیاری از مقررات قوانین جزایی و تجربه حاصل از مشاهده جنایات وحشتناک و تأسف‌برانگیزی نظیر حادثه تاسوکی توسط گروهک‌های کاملاً سازمان‌یافته تروریستی در کنار به اشتراک‌گذاری محتویات مستهجن از طریق سایت‌هایی نظیر «آویزون»، قانون‌گذار را بر آن داشت تا در تدوین مقرره جدید به‌درستی قصد منفعت‌طلبی مالی را در تعریف گروه سازمان‌یافته شرط نداند. قوانین باید برگرفته از واقعیت‌ها و شرایط روز اجتماعات انسانی باشند و تا امروز این واقعیت‌ها در مورد ایران و برخی کشورهای خاورمیانه نظیر سوریه و عراق معادله‌ایی متفاوت را در مقایسه با بسیاری از کشورهای غربی در عرصه‌های متعدد رقم زده است. برای تأیید نظر ر.ک: (Council of Europe, 2005: 20).

(۵) در تبصره ماده ۱۳۰ قانون مجازات اسلامی، برخلاف کنوانسیون جرائم سازمان‌یافته پالرمو (بند دوم ماده ۲) و قوانین ملی کشورهایی نظیر جمهوری ایرلند (شق سوم بند اول ماده ۷۰ قانون عدالت کیفری ۲۰۰۶) و تونگا

(ماده ۲۳ قانون جرائم فراملی ۲۰۰۶) که حداقل مجازات چهار سال حبس یا مجازات شدیدتر را برای شدید به شمار آوردن جرم ارتکابی شدید شرط می‌دانند، ارتکاب جرائم شدید لازمه سازمان‌یافته تلقی‌کردن گروه مجرمانه محسوب نمی‌شود.

(۶) طبق ماده ۲ این کنوانسیون: «a- گروه مجرمانه سازمان‌یافته گروهی متشکل از سه یا چند نفر است که برای یک دوره زمانی مشخص وجود داشته و به طور هماهنگ باهدف ارتکاب یک یا چند جرم شدید یا جرائم مندرج در این کنوانسیون به‌منظور تحصیل، مستقیم یا غیرمستقیم، منافع مالی یا سایر منافع مادی فعالیت می‌کند» و «c- گروه متشکل گروهی است که به‌طور تصادفی یا غیرمنظم به‌منظور ارتکاب فوری جرم تشکیل نشده باشد و به داشتن نقش های تعریف شده رسمی برای اعضای خود، ادامه عضویت در آن یا به ساختار توسعه‌یافته نیاز نداشته باشد».

(۷) باتنت‌ها نتیجه عملکرد نرم‌افزارهای مخرب می‌باشند که با نصب بر روی سیستم قربانی، باعث می‌شوند که کنترل سیستم وی، به منظورهای مجرمانه‌ای نظیر پخش ویروس، حملات دیداس، فیشینگ و سرقت اطلاعات شخصی مانند نام کاربری و رمز، در اختیار حمله‌کننده قرار بگیرد؛ بدون اینکه قربانی از وجود آنها آگاهی داشته باشد. سیستم‌هایی که به این نرم‌افزارهای آلوده مخرب می‌شوند، شبکه‌ای را شکل می‌دهند که باتنت نام دارد (شبکه‌ای از بات‌ها یا Bot-Net). هر یک از سیستم‌های آلوده در داخل این شبکه را زامبی می‌نامند.

(۸) در اوایل سال ۲۰۰۹ میلادی، گروهی از پژوهشگران امنیتی دانشگاه کالیفرنیا در سانتاباربارا توانستند با به دست گرفتن کنترل باتنت «تورپیگ» (Torpig) طی تنها ۱۰ روز موفق به جمع‌آوری اطلاعات ۱۷۰۰ کارت بانکی، ۸۳۰۰ اکانت در ۴۰۰ موسسه‌ی مالی مختلف، نام کاربری و رمز عبور مربوط به شبکه‌های اجتماعی و صندوق‌های پستی ۲۹۸ هزار کاربر و ارسال آنها به سرور فرماندهی و کنترل (C&C Server) شوند. در این حملات ده روزه ۱۸۳ هزار سیستم تبدیل به زامبی شدند.

(۹) پژوهش‌های صورت‌گرفته دیگر نیز مؤید چنین نتیجه‌ایی می‌باشند؛ همان‌گونه که در یکی از جدیدترین تحقیقات صورت‌گرفته مشخص شد ۷۵ که درصد از ۶۲۱ مورد از نقض داده‌ها با انگیزه‌های مالی صورت گرفته بود ر.ک: (Verizon, 2012).

(۱۰) در برخی از پژوهش‌ها، اصطلاح «جرائم مرتبط با رایانه» به‌منظور اطلاق بر آن دسته از جرائم سنتی به‌کار می‌رود که از طریق سیستم‌های اطلاعات الکترونیکی یا کامپیوترها ارتکاب می‌یابند (نظیر کلاهبرداری رایانه ایی) و اصطلاح «جرائم سایبر» برای جرائمی مورد استفاده قرار می‌گیرد که تنها در بستر شبکه جهانی اینترنت قابلیت ارتکاب را دارند (مانند حملات دی‌داس) (Wall, 2001: 3). برخی پژوهشگران در آثار خود دقیقاً عکس این تفکیک در مفهوم را دنبال کرده‌اند. به عقیده نگارندگان این پژوهش، تفکیک بین این اصطلاحات صرفاً از باب معناشناسی و سلیقه‌ای است. در قوانین و بسیاری از پژوهش‌های ملی نیز این اصطلاحات به‌جای یکدیگر به‌منظور توصیف هر دو شکل این جرم به کار رفته‌اند. با توجه به چشم‌انداز بین‌المللی این پژوهش و درنظرگرفتن این واقعیت که جرم سازمان‌یافته موضوع بحث در بیشتر موارد در محیط سایبر، از طریق یا علیه آن ارتکاب می‌یابد، بنابراین در این مقاله کاربرد اصطلاح جرم سایبر با هدف در برگرفتن هر دو دسته از جرائم ترجیح داده می‌شود. اطلاعات بیشتر ر.ک: (روزگار، ۱۳۹۵: ۲۵).

(۱۱) در گونه‌شناسی ارائه‌شده توسط اداره مبارزه با جرم و مواد مخدر سازمان ملل متحد پنج گونه از گروه‌های مجرمانه در فضای واقعی شناسایی شده‌اند که به ترتیب عبارتند از: ۱- گروه هرمی استاندارد (با سلسله‌مراتب منسجم، رهبری واحد و سیستم انضباط قوی داخلی) ۲- گروه هرمی منطقه‌ای (با سلسله مراتب منضبط و خطوط کنترل و نظارت داخلی قوی ولی خودمختاری داخلی نسبی برای عناصر منطقه‌ای) ۳- گروه هرمی خوشه‌ای (مجموعه‌ای از گروه‌های مجرمانه است که سیستم هماهنگی و نظارت را، از ضعیف به قوی، روی تمام فعالیت‌های خود ایجاد کرده‌اند) ۴- گروه هسته‌ای (گروه نسبتاً سازمان‌یافته با ساختاری همبسته، ولی غیرمتشکل که بعضاً توسط شبکه‌ای از افراد درگیر در فعالیت‌های مجرمانه محصور شده است) ۵- شبکه

مجرمانه (شبکه‌ای سیال، بی‌ثبات و متغیر است که از افراد با توانایی‌های خاص به‌منظور ارتکاب مجموعه‌ای از طرح‌های مجرمانه در دست اقدام تشکیل شده است) (UNODC, 2002: 33).

(۱۲) ساختار هرمی از دیرباز به‌منظور مدیریت سازمان‌های بسیار گسترده‌ی دولتی و نظامی و ایجاد قابلیت تقسیم وظایف متعدد و پیچیده مورد نیاز برای انجام فعالیت‌های گوناگون در مقیاس نسبتاً گسترده سازمانی مورد استفاده قرار می‌گرفته است. ایجاد نخستین شکل ساختار هرمی را به سال ۵۰۰ قبل از میلاد (ارتش امپراتوری روم باستان) منسوب می‌کنند (ر.ک: Alvinius, 2012) ولی به نظر می‌رسد در تمدن‌های بدوی نظیر مصر، پرو و میان‌رودان در اواخر دوران فورماتیو با روی کار آمدن سلسله‌مراتب اجتماعی (Hierarchie) و به قدرت رسیدن کاهنان جنگجو، مراتب حاکمیت مذهبی، زنجیره‌ای شد و نخستین شکل سازمان‌دهی هرمی ظهور کرد.

(۱۳) برای نظر مخالف ر.ک: (Broadhurst et al, 2014: 3).

(۱۴) موضوعیت نداشتن قدرت فیزیکی موجب شده است تا در دنیای سایبری شاهد راه‌اندازی حملات متعدد توسط افرادی مانند مایکل کالس (Michael Calce) بود که در ۱۵ سالگی به‌تنهایی اقدام به کسب درآمد میلیون دلاری از این طریق کرد. در دنیای واقعی، بزرگسالان نمی‌توانند به‌تنهایی چنین تجارت گسترده غیرقانونی را ترتیب دهند.

(۱۵) در مورد مفهوم اعتماد ر.ک: (Lampe et al, 2003).

(۱۶) شایان ذکر است که در تعریف مک‌گوایر، گروه مجرمانه می‌تواند از ائتلاف حداقل دو نفر شکل گیرد.

(۱۷) امام سامودرا (Imam Samudra) که به دلیل محکومیت به جرم طراحی و بمب‌گذاری منجر به کشته و زخمی‌شدن بیش از ۴۰۰ نفر در سال ۲۰۰۲ در جزیره بالی اندونزی در سال ۲۰۰۸ اعدام شد، بنابر برخی گزارش‌ها از زیردستان خود درخواست می‌کرد تا تقلب در کارت‌های اعتباری را به‌منظور فعالیت‌های نزاع‌طلبانه مالی مرتکب شوند. ر.ک: (Lormel, 2007: 14).

(۱۸) بنابر گزارش سایت «آمار زنده اینترنت» از ۸۰ میلیون نفر جمعیت ایران در سال ۲۰۱۶، حدود ۳۹ میلیون نفر؛ نزدیک به نیمی از جمعیت کشور در حال حاضر کاربر اینترنتی و دوفضایی هستند. در رده‌بندی سایت آمار زنده اینترنت، ایران ازنظر تعداد کاربر اینترنتی، در مقیاس جهانی در رده هجدهم و در مقیاس منطقه‌ای (خاورمیانه) در رده دوم پس از ترکیه قرار دارد.

(۱۹) مرکز بررسی جرائم سازمان‌یافته سایبر، بخشی از پدافند سایبری سپاه پاسداران انقلاب اسلامی است که در سال ۱۳۸۶ به‌منظور مقابله با حملات خطرناکی که در بستر شبکه جهانی اینترنت علیه اموال، فرهنگ اسلامی، اخلاقیات و نظام جمهوری اسلامی ایران ارتکاب می‌یافت، تشکیل شد.

(۲۰) در ارتباط با مفهوم شرکت سهامی ارتکاب جرم و نقش سهامداران ر.ک: (میرمحمدصادقی، ۱۳۹۰: ۲۵۳-۱۹۱).

منابع فارسی

روزگار، حسین (۱۳۹۵)، ***اجرای عدالت کیفری در جرائم سایبر؛ چالش‌ها و راهکارها***، پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی تهران، دانشکده حقوق.

شمس، محمدابراهیم (۱۳۸۳)، «جرائم سازمان‌یافته»، ***حقوق اسلامی***، شماره ۱: ۱۳۰-۱۰۹.

میرمحمدصادقی، حسین (۱۳۹۰)، ***حقوق جزای بین‌الملل***، چاپ سوم، تهران: میزان.

میرمحمدصادقی، حسین (۱۳۹۲)، ***جرایم علیه اموال و مالکیت: کلاهبرداری، خیانت در امانت، سرقت و صدور چک پرداخت نشدنی (مطالعه تطبیقی)***، چاپ سی‌وهشتم، تهران: میزان.

نصر اصفهانی، آرش، اسماعیل غلامی‌پور و اسماعیل شیرعلی (۱۳۹۴)، «علل پایداری و گسترش شبکه‌های هرمی در دهه ۱۳۸۰ (پژوهشی کیفی از تجربه فعالان شبکه کوئست در تهران)»، ***راهبرد اجتماعی فرهنگی***، سال پنجم، شماره ۱۷: ۲۰۴-۱۸۱.

منابع لاتین

Alvinius, A. (2012), The Inadequacy of Bureaucratic Organizations: Organizational Adaptation through boundary spanning in a Civil-Military Context , ***Res Militaris***, Vol.3, No.1: 1-23.

Aransiola, J. O., & Asindemade, S. O. (2011), Understanding cybercrime perpetrators and the strategies they employ in Nigeria , ***Cyberpsychology, Behavior, and Social Networking***, Vol.14, No.12: 759-763.

Aransiola, Joshua Oyeniyi & Asindemade, Suraj Olalekan (2011), Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria , ***Cyberpsychology, Behavior, and Social Networking,*** Vol. 14, No.12: 759-763.

BAE Systems Detica and the John Grieve Centre (2012), Executive Summary for Policing and Community Safety, ***Organised Crime in the Digital Age: The Real Picture.***

Ben-Itzhak, Y. (2009), Organised cybercrime and payment cards , ***Card Technology Today***, Vol.21 No.2: 10-11.

Bhattacharjee, Y. (2011), Why Does A Remote Town In Romania Have So Many Cybercriminals? , ***Wired***, Vol.19, No.2.

Brenner, S. W. (2002), Organized cybercrime-how cyberspace may affect the structure of criminal relationships , ***NCJL & Tech***, Vol.4, No.1.

Brenner, S. W. (2012), ***Cybercrime and the law: Challenges, issues, and outcomes***, UPNE.

Broadhurst, R, Grabosky, P. Alazab, M & Chon, S. (2014), Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime , ***International Journal of Cyber Criminology***, Vol.8, No.1: 1-20.

Broadhurst, R. & Chang, L. Y. (2013), Cybercrime in Asia: trends and challenges. In ***Handbook of Asian criminology*** (pp. 49-63), Springer New York.

Broadhurst, R. G. & Grabosky, P. (2005), Computer-related crime in Asia: Emergent issues, In ***Cyber-Crime: The Challenge in Asia*** (pp. 1-26), Hong Kong University Press.

Chang, Y. C. (2012), ***Cybercrime in the Greater China region: regulatory responses and crime prevention across the Taiwan Strait***, Edward Elgar Publishing.

Choo, K. K. R. (2008), Organised crime groups in cyberspace: a typology , ***Trends in organized crime***, Vol.11, No.3: 270-295.

Coser, L. (1977), ***Masters of Sociological Thought: Ideas in Historical and Social Context, Nueva York, Harcourt Brace and Company***, 428-463.

Council of Europe. Octopus Programme. (2005), ***Organised crime in Europe: the threat of cybercrime: situation report 2004***, Council of Europe.

Décary-Hétu, D. & Dupont, B. (2012), The social network of hackers , ***Global Crime***, Vol.13, No.3: 160-175.

Europol, European Law Enforcement Agency (2015), Internet Facilitated Organised Crime, ***The Internet Organised Crime Threat Assessment*** (IOCTA).

Goodman, M. (2011), International dimensions of cybercrime, In ***Cybercrimes: A Multidisciplinary Analysis*** (pp. 311-339***)***, Springer Berlin Heidelberg.

Group IB (2011), ***State and Trends of the Russian Digital Crime Market***, Report in English Version.

House of Commons (Home Affairs Committee), European Scrutiny Committee (30 July 2013), ***E-Crime***, Fifth Report of Session 2013˚14, HC 70.

Lampe, Klaus. V, & Johansen, P.Ole (29 August 2003), ***Criminal Networks and Trust***, Paper presented at the 3rd annual meeting of the European Society of Criminology (ESC), Helsinki, Finland.

Lormel, Dennis M. (2007), Terrorism and Credit Card Information Theft , ***Shift4 Secure Payment Processing.***

Lusthaus, J. (2013), How Organised is Organised Cybercrime? ,***Global Crime***, Vol.14, No.1: 52˚60.

Mc Afee (2013), ***Cybercrime Exposed; Cybercrime-as-a-Service***, Mc Afee publication.

McCarthy, D. M. (2011), ***An economic history of organized crime: A national and transnational approach***, Routledge.

Parliamentary Joint Committee on the Australian Crime Commission (2007), ***Inquiry into the future impact of serious and organised crime on Australian society***, Parliament House, Canberra September.

Pijv ek, Tomv (2009), The Importance of the Mafia Topic in Mario Puzo Fiction, Bachelor Thesis, ***Tomas Bata University in Zlín, Faculty of Humanities,*** Czech Republic.

Rollins, J. & Wyler, L. S. (2013), ***Terrorism and transnational crime: Foreign policy issues for Congress*** (Vol.1), Congressional Research Service.

Ronfeldt, D. (1996), ***Tribes, institutions, markets, networks: A framework about societal evolution,*** RAND publication

Sharma, Amit (March 2010), Cyber wars: A Paradigm Shift from Means to Ends , ***Strategic Analysis***, Vol.34, No.1: 62-73.

Simmel, Georg, Wolf, Kurt H (Ed.) (1950), ***Quantitative Aspects of the Group in the Sociology of Georg Simmel***, New York, Macmillan publishing (The Free Press).

Sipress, A. (2004), An Indonesian Prison Memoir Takes Holy War Into Cyberspace: In Sign of New Threat, Militant Offers Tips on Credit Card Fraud , ***Washington Post, Foreign Service***, Page A19.

Soudijn, M. R. & Zegers, B. C. T. (2012), Cybercrime and virtual offender convergence settings , ***Trends in organized crime***, Vol.15, No.2-3: 111-129.

Spapens, Antonius (2010), Macro networks, collectives, and business processes: An integrated approach to organized crime , ***European Journal of Crime, Criminal Law and Criminal Justice***, Vol.18: 185-215.

Tropina, Tatiana (2012), The Evolving Structure of Online Criminality; How Cybercrime Is Getting Organised , ***Eucrim (the European Criminal Law Associations' Forum),*** Vol.4: 158-165.

UNODC (2002), ***Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries***, United Nations.

UNODC (2004), ***United Nations Convention against Transnational Organized Crime and The Protocols Thereto***, United Nations.

UNODC (2012), ***Digest of Organized Crime Cases: A compilation of cases with commentaries and lessons learned***, United Nations.

UNODC (2012-2013), ***Comprehensive Study on Cybercrime***, United Nations.

Vejdani, Sajjad & Nik Khah (2014), Measures Taken by Iran to Prevent Transnational Organized Crimes and its Estimated Position Compared to the UN Criminal Policy , ***Journal of Educational and Management Studies,*** Vol.4, No.3: 519- 527.

Verizon (2012), Data Breach Investigation Report, ***Wired***.

Walker, George k. (2000), Information Warfare and Neutrality , ***Vanderbilt Journal of Trans-national Law,*** Vol.33:1079.

Wall, D. S. (2001), Cybercrimes and the Internet, ***Crime and the Internet***, 1-17.

Wall, David S. (2015), Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime , ***The European Review of Organised Crime***, Vol.2, No.2: 71-90.

Warner, Jason (2011), Understanding Cyber-Crime in Ghana: A View from Below , ***International Journal of Cyber Criminology***, Vol.5, No.1: 736-749.

Williams, Phil (2001-2002), Organized Crime and Cyber-Crime: Synergies, Trends and Responses , ***US Department of State global issues journal***, Vol.6, No.2: 22-26.

Yip, Michael (14-17 Jun 2011), ***An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis***, ACM WebSci '11, Koblenz, Germany (Conference or Workshop Item).