ماهیت گروه‌های سازمان‌یافته جرایم سایبری

سهیلا محمدی* ـ عیسی مونس‌خواه**

چکیده:

اگر از بحث‌های کلیشه‌ای و تکراری درخصوص جرایم سایبری و اهمیت آن در هزاره سوم چشم‌پوشی کنیم، مسئله بررسی ماهیت گروه‌های دخیل در جرایم سایبری ازجمله مشکلات حائز اهمیت و کمتر بحث‌شده در حوزه جرایم سایبری است. بررسی ماهیت گروه‌های دخیل در جرایم سایبری، چالش‌های نظری و تجربی درخصوص مجرمان سایبری، نقش گروه‌های سازمان‌یافته در جرایم سایبری، ارائه مصادیق و نمونه‌های شناخته‌شده‌ای که بیانگر رفتارهای فردی و اجتماعی می‌باشد و نیز بررسی انگیزه‌های مجرمان سایبری من‌جمله مسئولین دولتی را می‌توان به‌عنوان اهداف پژوهش حاضر برشمرد.

در این مقاله سعی در توصیف انواع مختلف جرایم سایبری و گونه‌های متفاوت تشکیلات سازمان‌یافته مجرمان بر اساس نوع‌شناختی‌های مختلف ازجمله تیپولوژی ارائه‌شده توسط مک‌گایر*** و چابینسکی**** داریم. روشن است که طیف وسیعی از تشکیلات و سازمان‌ها در جرایم سایبری دخیل هستند. درزمینهٔ مشارکت‌ها و فعالیت‌های سودآور، به‌ویژه جرایم سایبری ارتکاب‌یافته توسط مقامات دولتی ظاهراً به رهبری، سازمان‌دهی و تخصص بیشتری نیازمند است. این درحالی است که به‌نظر می‌رسد در عمل اقداماتی با رهبری و سازمان‌دهی بسیار ضعیف دراین‌زمینه انجام شده است.

کلیدواژه‌ها:

جرایم سایبری، مجرمین سایبری، جرایم سازمان‌یافته، گروه‌های سازمان‌یافته.

مجلهٔ پژوهشهای حقوقی (فصلنامه علمی - ترویجی)، شمارهٔ ۴۰، زمستان ۱۳۹۸
صفحهٔ ۱۸۹-۲۱۱، تاریخ وصول: ۱۳۹۵/۱۰/۱۰، تاریخ پذیرش: ۱۳۹۵/۱۱/۱۳

* دانشجوی دکترای حقوق جزا و جرم‌شناسی، دانشکده حقوق، الهیات و علوم سیاسی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، ایران، نویسنده مسئول Email: soheyla.mohamadi90@gmail.com

** دانشجوی کارشناسی ارشد، حقوق بین‌الملل، دانشگاه علوم اسلامی رضوی، خراسان رضوی، ایران
Email: Mooneskhah@razavi.ac.ir

*** McGuire

**** Chabinsky

مقدمه

در بحث از جرایم سایبری و سازمان‌یافته یکی از مشکلات عمده کلیشه‌ای شدن مباحث مذکور می‌باشد. از یک‌سو تصویر شناخته‌شده از هکرها باعث انحراف از طبیعت جمعی اکثر جرایم سایبری شده است. به عبارتی این تصویر خط بطلانی بر ماهیت مشترک جرایم سایبری است. از سوی دیگر تعاریف مرسوم جرایم سازمان‌یافته منقضی و از رده خارج هستند، به‌طوری‌که سیر تکاملی این نوع جرایم به‌خودی‌خود از این تعاریف پیشی گرفته‌اند. مقاله حاضر به کشف تغییرات ایجادشده در شکل‌گیری جرایم سایبری می‌پردازد. باید توجه داشت درحالی‌که امروزه سازمان‌یافته‌ترین جرایم سایبری توسط تکنسین‌های ماهری که دانش خود را در فعالیت‌های مجرمانه به‌کار می‌گیرند، ارتکاب می‌یابد، باوجوداین گروه‌های مجرمانه به شکل مرسوم و شناخته‌شده آن که سعی در مهار فناوری دیجیتال به‌منظور پیشبرد و دستیابی به اهداف جنایی و مجرمانه داشته باشند، وجود ندارد. بدون شک این فاصله و شکاف به‌مرور زمان همان‌طور که استفاده از فناوری دیجیتال فراگیر می‌شود، از بین خواهد رفت.

امروزه به ذهنیتی فوق‌العاده نزدیک به این ذهنیت که توانایی و قدرت دولت‌ها را برای ارتکاب اعمال مجرمانه حاشا می‌کند، نیاز است. تاریخ، جرایم ارتکاب‌یافته بسیاری را توسط مسئولین و مقامات دولتی چه در زمان صلح و چه در زمان جنگ ثبت کرده است. یکی از نمونه‌های اخیر اتهام تولید مواد مخدر، جعل و تقلب توسط عوامل و نمایندگان جمهوری دموکراتیک خلق کره می‌باشد. به‌عنوان نمونه دیگر می‌توان به درگیری دوره‌ای دولت‌ها در آدم‌ربایی و ترورهای داخلی و خارجی اشاره نمود. بااین‌حال ادبیات جرایم سازمان‌یافته تاکنون تمایل به نادیده گرفتن جرایم ارتکابی توسط دولت‌ها و نیز جرایم موردحمایت دولت‌ها، داشته است. دولت‌ها مدت‌های مدیدی هم به‌طور مستقیم درگیر فعالیت‌های مجرمانه بوده‌اند و هم ازطریق حمایت و کمک به مجرمین، اعمال و نیّات کثیف و غیرانسانی خود را به انجام رسانده‌اند. امروزه ما با دولت‌های زیادی مواجه می‌شویم که از فناوری اینترنت برای ارتکاب جرایم بهره می‌گیرند. ادعاهایی مبنی بر اینکه؛ روسیه اتهامات حمله یا ترغیب و تشویق حمله به سرویس‌های امنیتی را رد کرده است، مقامات چینی در جاسوسی‌های گسترده صنعتی و اقتصادی درگیر و دخیل هستند، با افشاگری‌های ادوارد اسنودن[1] مبنی‌بر دخیل بودن دولت

1. Edward Snowden

ایالات‌متحده آمریکا در پروژه‌ها و برنامه‌های عظیم و گسترده کنترل و نظارت سایبری، مطابقت داشته است، به‌طوری‌که شرکت امنیت رایانه‌ای مک‌آفی اعلام کرده است آمریکا بیشترین آمار کاربران رایانه‌ای جهان را داراست. کسانی که دائماً درحال سیر در شبکه‌ها، ایجاد اختلال و انتشار ویروس‌های رایانه‌ای هستند و حتی دورافتاده‌ترین کاربران اینترنتی را در سراسر جهان کنترل می‌کنند. جوزف من[۲] می‌گوید: دولت آمریکا در ارتکاب جرایم سایبری هم اندازه کشورهایی که به آنها در برابر قوانین بازدارنده جرایم سایبری هشدار می‌دهد، مقصر و خطاکار است.[۳] البته نباید از یاد برد که در پی افشاگری‌های ادوارد اسنودن دولت آمریکا با چالش‌های زیادی ازجمله بی‌اعتمادی مردم و حتی شرکت‌های کوچک و بزرگ مواجه شده است. اظهارات اسنودن پیمانکار سابق آژانس امنیت ملی آمریکا (NSA) در سال ۲۰۱۳ سبب افزایش نگرانی‌های عمومی شد چراکه در اظهارات وی مشخص شد آژانس امنیت ملی آمریکا با همکاری برخی از کمپانی‌ها به شنود مکالمات تلفنی و جمع‌آوری اطلاعات خصوصی میلیون‌ها هکر پرداخته است که کوچک‌ترین ردپایی از هیچ‌یک از آنها در جنایت و حمله‌های سایبری دیده نمی‌شود و همین موضوع سبب شده است مردم اطلاعات خود را از شرکت‌های کوچک و بزرگ مخفی نگه دارند تا مبادا به دست آژانس امنیت ملی آمریکا بیفتد.[۴]

۱- گروه‌های مجرمانه سازمان‌یافته در فضای سایبری

درحالی‌که بسیاری از جرایم سایبری نیازمند سازمان‌یافتگی و تخصص بسیار بالایی می‌باشند، مدارک و مستندات کافی برای اثبات اینکه، این جرایم اکنون توسط گروه‌های مجرمانه سازمان‌یافته ارتکاب می‌یابد و یا اینکه این گروه‌ها چه شکل یا ساختاری دارند، وجود ندارد. تکنولوژی دیجیتال به افراد قدرتی اعطاء کرده است که پیش از این هرگز در اختیار نداشته‌اند. نوجوانان به‌تنهایی قادر به از کار انداختن و مختل کردن سیستم‌های کنترل ترافیک هوایی، تعطیل کردن کار خرده‌فروشان اینترنتی و دستکاری و اخلال در معاملات بازارهای بورس در

2. Joseph Man

۳. محمدابراهیم شمس ناتری، «آمریکا بزرگ‌ترین هکر و عامل جرایم سایبری جهان»، ۲۹ اردیبهشت ۱۳۹۲، http://www.yjc.ir/fa/news/4389396 (۱۳۹۵/۰۷/۰۱).

۴. میترا جلیلی، «جبهه‌ای که با دستور مستقیم اوباما گشوده شد، جنجالی‌ترین طرح آمریکا برای مبارزه با هکرها»، مؤسسه فرهنگی مطبوعاتی ایران، http://iran-newspaper.com/Newspaper/MobileBlock?NewspaperBlockID=58281 (۱۳۹۵/۰۷/۱۳).

سطح ملی و فراملی می‌باشند (کمیسیون بورس اوراق بهادار آمریکا، سال ۲۰۰۰ میلادی). آنچه افراد قادر به انجام آن هستند قطعاً سازمان‌ها نیز توانایی انجام آن را اغلب به‌نحو مطلوب‌تری دارند. واضح است که تمام انواع تشکیلات و گروه‌های مجرمانه قادر به انجام جرایم سایبری هستند. می‌دانیم اینترنت و تکنولوژی‌های مربوط به آن به‌طور کامل در اختیار ایجاد هماهنگی در سرتاسر منطقه‌ای هستند که در آن توزیع شده است. در زیر به برخی از نمونه‌ها و انواع گروه‌های مجرمان سازمان‌یافته اشاره می‌کنیم:

۱- یک گروه مجرمانه سازمان‌یافته ممکن است یک مافیای سنتی با سطح بالایی از سازمان‌یافتگی باشد که از مهارت‌های مجرمانه درزمینهٔ فناوری اطلاعات استفاده می‌کند؛

۲- نوع دیگر گروه‌های سازمان‌یافته مجرمانه می‌تواند پروژه کوتاه‌مدتی باشد که توسط گروهی که جرم آنلاین خاص و یا یک گروه یا بزه‌دیده خاص را هدف قرار می‌دهند، راه‌اندازی شده باشد؛

۳- به‌جای گروه‌ها تشکیلات مجرمانه می‌تواند شامل انجمن‌ها و شبکه‌های بزرگ‌تری باشند که مبتنی‌بر ارتباط آنلاین و معامله اموال و کالاهای دیجیتال می‌باشند (به‌عنوان مثال خریدوفروش نرم‌افزارهای کرک‌شده (هک‌شده) و پخش تصاویر مستهجن از کودکان)؛

۴- همچنین ممکن است شامل افرادی باشد که به‌تنهایی فعالیت می‌کنند، اما درواقع وابسته به یک شبکه و سازمان بزرگ مجرمانه می‌باشند درنتیجه ممکن است در شبکه‌های مخفی یا تور[۵] سایت‌های زیرزمینی با چنین افرادی مواجه شویم.

دولت‌ها، سازمان‌های مجری قانون، محققان دانشگاهی و صنعت امنیت سایبری بر این باورند که گروه‌های جرایم سازمان‌یافته معمولی به‌طور فزاینده‌ای درگیر جرایم دیجیتال شده‌اند. آمارها و مشاهدات تجربی موجود بیانگر این حقیقت هستند که مجرمان آنلاین و غیرآنلاین به‌جای تشکیلات و سازمان‌های رسمی بیشتر تمایل به حضور و مشارکت در شبکه‌های غیرقانونی غیرمرتبط به یکدیگر دارند. در سال‌های اخیر گروه‌های افراطی از فناوری اینترنت به‌عنوان ابزار سرقت جهت افزایش توان مالی خود استفاده کرده‌اند. امام

۵. تور یک سرویس مسیریابی مجدد رمزگذاری‌شده است که برای پنهان کردن منبع اصلی یک ایمیل و یا وب‌سایت در اینترنت طراحی شده است.

سمودرا[۶] محکوم به طراحی بمب‌گذاری‌های جزیره بالی در سال ۲۰۰۲، بنابر گزارش طرفداران و پیروانش مرتکب جعل، تقلب و کلاهبرداری در کارت‌های اعتباری به‌منظور تأمین مالی اعمال و فعالیت‌های ستیزه‌جویانه و جنگ‌طلبانه شده بود.[۷]

مجرمان سایبری ممکن است به‌صورت آزادانه یا شبکه‌های غیرمرتبط به هم عمل کنند، اما شواهد حاکی از آن است که اعضاء به‌لحاظ جغرافیایی حتی هنگامی‌که حملات و اعمالشان فراملی است، نزدیک به هم هستند. برای مثال شبکه‌های محلی کوچک دقیقاً مانند گروه‌های متمرکز بر روابط خانوادگی و دوستانه، به‌عنوان فعالان اصلی ایفای نقش می‌کنند.

مراکز مهم و حساس جرایم سایبری با برقراری ارتباط مخفی و پنهانی با گروه‌های مجرمانه سازمان‌یافته در کشورهای اروپای شرقی و اتحاد جماهیر شوروی سابق عمل می‌کنند.[۸] هکرهای روسی و اوکراینی به‌عنوان مبتکران ماهر همواره موردتوجه بوده‌اند. برای مثال جرایم سایبری انجام‌شده در شهر کوچک رمنیکو ولچا[۹] رومانی ازجمله جرایم سایبری گسترده‌ای است که در اروپای شرقی گزارش شده است. همچنین نگرانی فزاینده‌ای درباره جرایم سایبری در چین وجود دارد.[۱۰] منبع و گستره حملات (چه با منشأ داخلی و چه با منشأ خارجی) و مقیاس فعالیت نرم‌افزار مخرب (بدافزار) بات‌نت[۱۱] همچنان مشخص نیست، اما بخش عمده‌ای از کامپیوترهای چینی بررسی شده و احتمال اینکه گروه‌های مجرمانه محلی

---

6. Imam Samudra

۷. امام سمودرا ۳۸ساله، تروریست اندونزیایی، سال ۱۳۸۷ به همراه دو تروریست دیگر به این اتهام اعدام شد. جالب است که پسر امام سمودرا، افراط‌گرای اندونزیایی و طراح و فرمانده بمب‌گذاری بالی که جان ۲۰۲ نفر را گرفت، در سوریه کشته شد. عمر عبدالعزیز، پسر این تروریست، از دیدگاه کارشناسان یک نسل جدید از نیروهای تروریستی اندونزیایی است. این نیروها، روش‌های تروریستی را از پدران خود به‌عنوان رهبران القاعده آموخته و با وعده‌های گروه تروریستی داعش وارد حرکت‌های تروریستی در سوریه شدند. (میترا جلیلی، «پسر تروریست اندونزیایی، عامل قتل ۲۰۲ نفر در سوریه کشته شد»، ۲۴ مهر ۱۳۹۴، خبرگزاری جمهوری اسلامی، http://www.irna.ir/fa/News/81801228/ (۱۳۹۵/۰۷/۱۳).)

8. N. Kshetri, *Cyber-Victimization and Cyber-Security in China* (New York, NY, United States: Communications of the ACM, 2013), 35-57.

9. Râmnicu Vâlcea

10. D. Pauli, "China is the "World's Biggest Cybercrime Victim," SC Magazine (2012) http://www.scmagazine.com.au/News/294653china-is-the-worlds-biggestcybercrime-victim.aspx (Accessed September 15, 2016).

۱۱. بات‌نت‌ها شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها که بات نامیده می‌شوند، تشکیل می‌شوند. این شبکه‌ها توسط یک و یا چند مهاجم که بات مسترها (Bot Masters) نامیده می‌شوند، با هدف انجام فعالیت‌های مخرب کنترل می‌گردند.

نقش اساسی در آن داشته باشند، وجود دارد.[۱۲و۱۳] یافته‌های مطالعه اخیر از منابع اسپم[۱۴] و فیشینگ[۱۵] نشان می‌دهد که اینها نشئت‌گرفته از تعداد کمی ISP هستند که می‌توان لقب «همسایگان بد اینترنتی» را به آنها داد. به‌عنوان یک نمونه خاص اسپکترانت (نیجریه) هاست ۶۲٪ از آدرس‌های IP که مربوط به اسپم‌هاست، می‌باشد. درحالی‌که هاست‌فیشینگ‌ها اغلب واقع در ایالات‌متحده آمریکاست. اسپم‌ها نشئت‌گرفته از ISPهای واقع در هند، برزیل و ویتنام می‌باشند.[۱۶]

باتوجه‌به آنچه گفته شد و نیز باتوجه‌به تنوعِ انواع و منابعِ جرایم اینترنتی جلوگیری از تصویرسازی کلیشه‌ای از مجرمان سایبری و نیز جلوگیری از انتشار داستان‌های جنجال‌آفرین و ایجاد وحشت روحی و روانی، بسیار مهم است. برخی از این تصاویر کلیشه‌ای و عمومی عبارتند از یک هکر روسی پلید منفعت‌گرا، یا یک هکر چینی وطن‌پرست. چنین تصویرسازی‌هایی درواقع به ارائه و معرفی نوع خاصی از شیاطین قومی و قبیله‌ای منجر می‌شود که می‌توان به آنها به‌عنوان مغلطه یا گمراه‌سازی درمورد فرضیات منابع و فعالیت مجرمانه سایبری نگریست. برخلاف چنین تصویرسازی‌های رسانه‌ای، مجرمان سایبری از قومیت‌ها، ملیت‌ها و با انگیزه‌های مختلف هستند، اگرچه به‌نظر می‌رسد انگیزه مالی، انگیزه غالب است.

تعریف استاندارد جرایم سازمان‌یافته در کنوانسیون پالرمو سازمان ملل متحد مبتنی است بر مشارکت سه نفر یا بیشتر که به‌طور هماهنگ اقدام می‌کنند که این اقدام هماهنگ به برخی اشکال بسیار پیچیده سازمان مانند بسیج شبکه‌های ربات، گسترش پیدا نمی‌کند و ممکن است توسط یک نفر اداره شود.[۱۷] به عبارتی می‌توان گفت جرم سازمان‌یافته عبارت از فعالیت‌های غیرقانونی و هماهنگ گروهی منسجم از اشخاص که با تبانی هم و برای تحصیل منافع مشترک ازجمله قدرت و منافع مادی به ارتکاب جرم مستمر مجرمانه شدید

12. Y. C. Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait* (Cheltenham, UK: Edward Elgar Publishing, 2012), 64-79.

13. R. Broadhurst, & Y. C. Chang, *Cybercrime in Asia: Trends and Challenges*. *Asian Handbook of Criminology* (New York: Springer, 2013), 46-49.

۱۴. ارسال یک پیام به‌صورت بی‌وقفه به تعداد زیادی کاربر اینترنت.

۱۵. اقدام به فریب و کلاهبرداری از اطلاعات مالی یک دارنده حساب آنلاین ازطریق وانمود کردن به‌عنوان یک شرکت قانونی.

16. G. C. Moura, *Internet Bad Neighborhoods* (Enschede, The Netherlands: Centre for Telematics and Information Technology, 2013), 103-108.

۱۷. غلامحسین بیابانی، «جرایم سازمان‌یافته ملی و فراملی»، *نشریه کارآگاه* ۶(۲۴) (۱۳۹۲)، ۳۴–۳۱.

می‌پردازند و برای رسیدن به هدف از هر نوع ابزار مجرمانه نیز استفاده می‌کنند.[۱۸] در یک جمله می‌توان گفت جرم سازمان‌یافته عبارتست از فعالیت مجرمانه مستمری که با هماهنگی صورت می‌گیرد.[۱۹] به‌عنوان مثال اصطلاح باتنت مشمول مجرمی است که نرم‌افزارهای مخرب (بدافزارها) را برای به‌دست گرفتن کنترل تعداد زیادی کامپیوتر به‌کار می‌گیرد (بزرگ‌ترین مورد آن شامل بیش از یک میلیون دستگاه مجزا می‌باشد). اگر چنانچه متولیان و محافظان فردی و سازمانی کامپیوترها در معرض خطر قرار بگیرند، زمینه مشارکت ناآگاهانه و غیرعمدی در یک اقدام جنایی مهم، فراهم می‌شود. برخی از مفسران بر این باورند که یک باتنت هماهنگ و بسیج‌شده توسط یک مجرم منفرد، تنها یک نوع از انواع جرایم سازمان‌یافته است.[۲۰] برمبنای دیپلماسی، شمول و اجراست که سازمان ملل متحد مایل به مقابله با فعالیت‌های مجرمانه دولت‌ها و تحت حمایت دولت‌ها چه در فضای مجازی و چه در غیر آن می‌باشد. اگرچه می‌توان مشکلات ذاتی و درونی برخی از کشورهای عضو سازمان ملل متحد به‌عنوان مجرمین و جنایتکاران سایبری و غیرسایبری را درک کرد، باوجودِاین مایه تأسف است که سازمان ملل متحد یکی از بزرگ‌ترین و مقتدرترین سازمان‌های مرتبط با جرایم سازمان‌یافته فراملی است.

۲- چالش‌های نظری و استنادی

فقدان شواهد و مدارک قابل‌استناد درمورد میزان، نقش و ماهیت گروه‌های جرایم سازمان‌یافته در فضای مجازی مانع از توسعه اقدامات متقابل درست، بی‌خطر و دقیق شده است. درحالی‌که تعداد رو به رشدی از متخصصان بر این باورند که جرایم سایبری در حوزه و قلمرو فعالیت گروه‌های سازمان‌یافته هستند و گمان می‌کنند روزگار هکرهای منفرد سپری شده است، بااین‌حال هنوز اطلاعات کمی درمورد ساختارهای ترجیحی، طول عمر گروه‌ها، چگونگی حصول اطمینان و اعتماد و رابطه با سایر اشکال جرم در دست است و به جرئت

۱۸. محمدابراهیم شمس ناتری، «بررسی سیاست کیفری ایران در قبال جرایم سازمان‌یافته با رویکردی به حقوق جزای بین‌الملل» (رساله دکتری، تهران: دانشگاه تربیت مدرس، ۱۳۸۰)، ۲۵-۱۳.

۱۹. محمدابراهیم شمس ناتری، «جرایم سازمان‌یافته»، *نشریه فقه و حقوق* ۱ (۱۳۸۳)، ۱۱۱-۱۰۹.

20. Chang, *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. op.cit. 46-49.

می‌توان گفت جرایم سایبری جرایمی صرفاً سازمان‌یافته نیستند و فقط شامل سرقت‌های دولتی و یا هک‌های سازمان‌یافته نمی‌شوند.[۲۱]

درزمینهٔ رفتار مجرمین و فرایند به‌کارگیری و به خدمت گرفته شدنشان در فضای مجازی، با فقدان و کمی پژوهش‌های مبتنی‌بر شواهد و مدارک قابلِ‌استناد مواجه هستیم، اگرچه می‌دانیم یادگیری و تقلید درزمینه‌های مذکور نقش مهمی را ایفاء می‌کنند. بنابراین ماهیت گروه‌های جرایم سازمان‌یافته را نمی‌توان به‌تنهایی برمبنای فعالیت‌های غیرقانونی‌شان درک کرد، بلکه فاکتورهای فرهنگی و اجتماعی نیز نقش مهمی در پیدایش و پایداری چنین گروه‌هایی بازی می‌کنند (شبکه‌های اجتماعی سودجو، بخش عقلایی و منطقی فعالان جنایی هستند). در برخی از این موارد حساسیت و وسواس مشهود است، اما در برخی دیگر احساس مصونیت از مجازات آشکار است (اعتماد به نفس کاذب به گمنامی و عدمِ‌شناسایی). همان‌طور که در بالا اشاره شد حرص و آز تنها یکی از ده‌ها انگیزه مجرمین می‌باشد؛ سایر انگیزه‌ها بسته به نوع جرم ممکن است شامل درجات و طبقه‌بندی‌های مختلفی باشند.

۳- ساختار

بررسی‌های مک‌گایر (۲۰۱۲) بر اساس نمونه بزرگی از موارد شناخته‌شده نشان می‌دهد که تا ۸۰٪ جرایم سایبری می‌تواند درنتیجه فعالیت‌های سازمان‌یافته باشد. بااین‌حال این بدین‌معنا نیست که این گروه‌ها، شکل گروه‌های سازمان‌یافته مجرمانه سنتی را به خود گرفته‌اند یا اینکه این گروه‌ها به‌طور انحصاری مرتکب جرایم دیجیتالی می‌شوند. در عوض مطالعات نشان می‌دهد که گروه‌های جرایم سازمان‌یافته سنتی درحال گسترش فعالیت‌های خود به دنیای دیجیتال، پهلوبه‌پهلوی انواع شبکه‌های مجرمانه سست و بی‌پایه جدید، می‌باشند. گروه‌های مجرمانه بیانگر انواع و سطوح مختلف سازمان‌ها بسته به اینکه آیا این گروه‌ها فعالیت‌های خود را منحصر به فعالیت‌های آنلاین در فضای مجازی می‌کنند، یا ابزارهای آنلاین را برای ارتکاب جرایم در دنیای واقعی و غیرمجازی به‌کار می‌گیرند و یا اینکه ترکیبی از اهداف آنلاین و آفلاین را دنبال می‌کنند، می‌باشند.

مطالعات و بررسی‌ها بیان می‌کند که نیمی از گروه‌های جرایم سایبری در نمونه او از شش نفر یا بیشتر تشکیل شده‌اند و یک‌چهارم گروه‌ها دارای بیش از ده نفر عضو می‌باشند.

---

۲۱. میترا جلیلی، «جرایمی که صرفاً سازمان‌یافته نیستند»، پلیس فتا، http://www.cyberpolice.ir/cyberspace/48991 (۱۳۹۵/۰۷/۰۱).

عمر یک‌چهارم جرایم گروه‌های سایبری کمتر از شش ماه بوده است و به‌عبارت‌دیگر یک‌چهارم این گروه‌ها کمتر از شش ماه فعالیت داشته‌اند. البته تعداد اعضای گروه یا مدت فعالیت آنها، مقیاسی برای میزان وقوع جرم نیست، چراکه گروه‌های کوچک هم می‌توانند آسیب‌های جدی و قابل‌توجهی را در مدت زمان کوتاه وارد کنند.

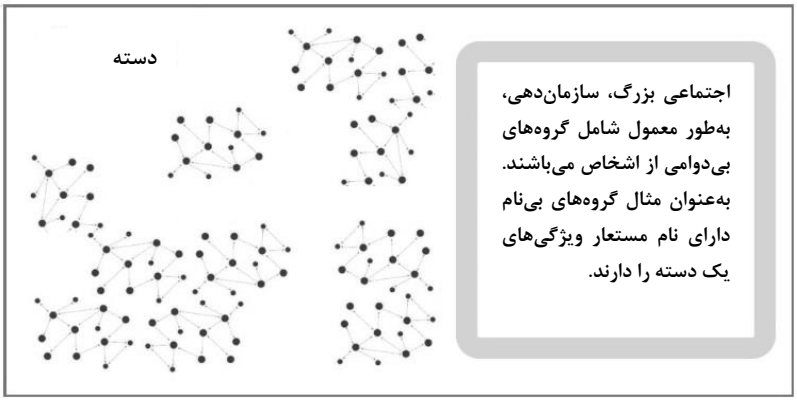
مک گایر یک نوع‌شناختی برای گروه‌های جرایم سایبری پیشنهاد کرده است که متشکل از شش نوع ساختار گروهی می‌باشد. او تأکید کرده است که این تیپولوژی او از گروه‌های سازمانی بنیادی، درواقع راه میان‌بری با درجه انعطاف‌پذیری و تغییرپذیری بالا و شیوه‌ای بسیار گیج‌کننده می‌باشد، ولی می‌توان گفت نوع‌شناختی نمایانگر و ارائه‌دهنده بهترین معیار تخمین برمبنای چیزی است که درحال‌حاضر درباره مجرمین سایبری می‌دانیم.

همچنین خاطرنشان می‌شود که این نوع‌شناختی احتمالاً با تکامل محیط‌های دیجیتال، تغییر می‌کند. نوع‌شناختی مک گایر شامل سه گروه اصلی است که هرکدام بسته به استحکام و انسجام روابط میان اعضاء به دو گروه فرعی تقسیم می‌شوند:

۱. گروه‌های نوع نخست اساساً به‌صورت آنلاین عمل می‌کنند و می‌توانند به دسته یا قطب‌ها تقسیم شوند. آنها اغلب مجازی بوده و اعتبارشان ازطریق شهرتی که در فعالیت‌های غیرقانونی آنلاین دارند، سنجیده و برآورد می‌شود؛

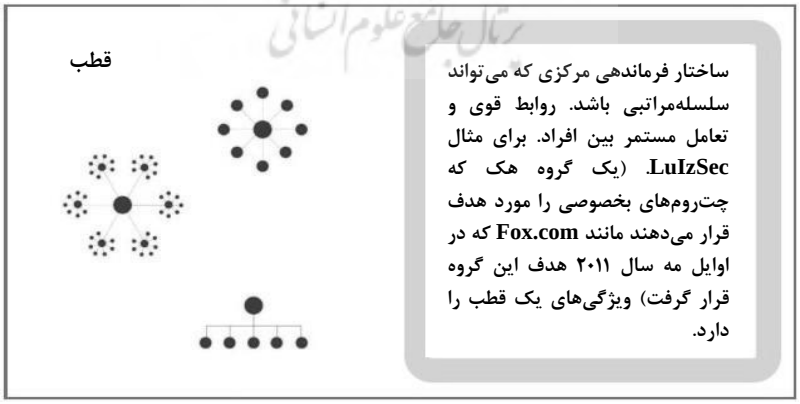
الف) دسته‌ها از بسیاری از امکانات شبکه‌ها بهره می‌برند و به‌عنوان تشکیلات سازمان‌نیافته با اهداف معمول و بدون رهبر توصیف می‌شوند. معمولاً دسته‌ها دارای حداقلِ سلسله‌مراتب دستوری هستند و ممکن است انواعی از ویروس‌ها را به شیوه‌ای که یادآور هکتیویست‌هاست[۲۲] به کار بیندازند. این‌طور به‌نظر می‌رسد که دسته‌ها بیشتر در فعالیت‌های آنلاین مانند مقاومت سیاسی و جرایم مبتنی‌بر نفرت فعالیت دارند؛ (نمودار ۱ را ببینید.)

۲۲. هکتیویست: یک هکر کامپیوتر که با هدف و انگیزه دستیابی به اهداف سیاسی و اجتماعی فعالیت می‌کند.



شکل ۱. تصویر عینی ساده از دسته‌ها

ب) قطب‌ها همانند دسته‌ها اساساً به‌صورت آنلاین فعالیت می‌کنند اما سازمان‌یافته‌تر و دارای ساختار فرماندهی (سلسله‌مراتبی) واضح‌تری هستند. قطب‌ها شامل یک نقطه کانونی (قطب) از مجرمان هسته‌ای نزدیک به هم هستند که اعضای جانبی و ثانوی گرداگرد آن اجتماع کرده‌اند. فعالیت‌های آنلاین آنها متنوع است که شامل دزدی دریایی، حملات فیشینگ، بات‌نت‌ها و جرایم جنسی آنلاین می‌باشد. مطالعات نشان می‌دهد که اشاعه و پخش این برنامه‌ها (ترس‌افزارها) اغلب توسط گروه‌های هم‌مرکز (هم‌قطب) انجام می‌شود. فروشگاه‌هایی که در آنها خریدوفروش ازطریق (جزئیات و اطلاعات) کارت‌های اعتباری انجام می‌شود و بازارهای (مربوط به) مواد مخدر مانند جاده ابریشم با این مدل سازگاری دارند. (ایالات‌متحده آمریکا علیه رز ویلیام آلبریچت، ۲۰۱۳) (شکل ۲ را ببینید.)



شکل ۲. تصویر عینی ساده از قطب‌ها

۲. نوع دوم گروه‌های سازمان‌یافته مجرمین ترکیبی از مجرمان آنلاین و آفلاین هستند که می‌توان از آنها تحت عنوان «دورگه»، «هیبرید» یا «ترکیبی» نام برد که به‌نوبه خود به دو گروه خوشه‌ای و گسترش‌یافته تقسیم می‌شوند:

الف) در یک گروه ترکیبی خوشه‌ای، بزهکار در گروه کوچکی از افراد تعریف می‌شود و بر روی فعالیت‌ها یا روش‌های خاصی تمرکز می‌شود. آنها تا حدّی از لحاظ ساختاری شبیه به قطب‌ها هستند، اما به‌طور یکپارچه و مستمر از مجرمین آنلاین به آفلاین و برعکس درحال تغییر و جابه‌جایی هستند. یک گروه معمولی تماس مختصر و سطحی با کارت‌های اعتباری برقرار می‌کند، سپس اطلاعات این کارت‌ها را برای اهداف و مقاصد آنلاین یا برای فروش اطلاعات ازطریق شبکه‌های کاردینگ[۲۳]، مورداستفاده قرار می‌دهد؛[۲۴]

ب) گروه‌های ترکیبی گسترش‌یافته بسیار شبیه گروه‌های ترکیبی خوشه‌ای عمل می‌کنند با این تفاوت که در این گروه‌ها تمرکز بسیار کمتری وجود دارد. آنها به‌طور معمول مشمول تعداد زیادی همکار، زیرگروه و انجام انواع فعالیت‌های مجرمانه هستند، اما هنوز هم حفظ درجه‌ای از هماهنگی برای اطمینان از موفقیت فعالیت‌هایشان ضروری به‌نظر می‌رسد.

۳. گروه‌های نوع سوم عمدتاً به‌صورت آفلاین عمل می‌کنند، اما تکنولوژی آنلاین، فعالیت‌های آفلاین آنها را تسهیل می‌کند. این نوع گروه‌ها درخور توجه هستند چراکه به‌طور فزاینده‌ای به انجام جرایم دیجیتالی کمک می‌کنند. همانند انواع گروه‌های قبلی، گروه نوع سوم را می‌توان به دو صورت سلسله‌مراتبی و تجمعی تقسیم کرد که این تقسیم‌بندی باتوجه‌به میزان درجه انسجام و سازمان‌یافتگی آنها انجام می‌شود؛

الف) گروه‌های سلسله‌مراتبی بهترین توصیف برای گروه‌های مجرمانه سنتی است (به‌عنوان مثال خانواده تبهکار) که برخی فعالیت‌های خود را به‌صورت آنلاین انجام می‌دهد. به‌عنوان مثال تمایل سنتی برخی از گروه‌های مافیایی به فحشا درحالِ‌حاضر به سایت‌های پورنوگرافی نیز گسترش یافته است. مثال‌های دیگر شامل قماربازی آنلاین، باج‌خواهی و اخاذی ازطریق تهدید به از کار انداختن سیستم و یا دستیابی به اطلاعات

---

۲۳. کاردینگ معمولاً به ربودن اطلاعات کارت‌های بانکی و خریدوفروش آنها و یا استفاده در شستشوی پول‌های ربوده‌شده گفته می‌شود. اما درواقع کاردینگ بسیار وسیع‌تر از این است و شامل جعل اسناد و مدارک نیز می‌شود.

24. M. McGuire, *Organised Crime in the Digital Age* (London: John Grieve Centre for Policing and Security, 2012), 50.

شخصی ازطریق حملات مخرب و یا هک کردن می‌باشد؛ (ایالات‌متحده علیه فیور، دادستانی ایالات‌متحده، حوزه شرق نیویورک، ۲۰۱۳)

ب) گروه‌های تجمعی (متراکم و توده‌ای) از سازمان‌یافتگی کمتری برخوردارند، این گروه‌ها موقت و اغلب بدون هدف مشخصی هستند، آنها از فناوری دیجیتال به شیوه‌ای تک‌منظوره استفاده می‌کنند که به هر صورت می‌تواند آسیب‌رسان باشد. نمونه‌های این گروه‌ها عبارتند از استفاده از بلک‌بری[۲۵]، یا تلفن همراه برای هماهنگ کردن فعالیت‌های باند یا ایجاد بی‌نظمی عمومی مانند شورش انگلستان در سال ۲۰۱۱ و شورش سیدنی در سال ۲۰۱۲.[۲۶]

مشخصه پیچیده‌ترین سازمان‌های جرایم اینترنتی تخصص و تقسیم کار قابل‌توجه است. نقش‌های زیر که در سخنرانی نماینده بخش تحقیقات سایبری اداره فدرال ایالات‌متحده آمریکا ارائه شده است، بیانگر نقش‌هایی است که دسیسه‌ها و برنامه‌های بزرگ شیادی، تقلب و کلاهبرداری مستلزم آن می‌باشد.

۱. برنامه‌نویسان و رمزنگاران (کدگذاران) که بدافزارها را طراحی کرده، به‌کار می‌اندازند و دیگر ابزارهای لازم برای ارتکاب جرم را فراهم می‌کنند؛
۲. توزیع‌کنندگان یا فروشندگان که مسئولیت انجام معاملات، فروش اطلاعات مسروقه و تأیید و تضمین محصولات تولیدشده توسط دیگر متخصصان را برعهده دارند؛
۳. تکنسین‌ها که وظیفه حفظ زیرساخت‌های مجرمانه و تکنولوژی‌های حمایتی و معین مانند سرورها، ISPها و رمزگذاری‌ها را برعهده دارند؛
۴. هکرها نواقص و نقاط آسیب‌پذیر را در برنامه‌های کاربردی، سیستم‌ها و شبکه‌ها به‌منظور دستیابی به مدیریت بیشتر یا منفعت بیشتر موردِجستجو و بهره‌برداری قرار می‌دهند؛

---

۲۵. یک نوع دستگاه تلفن همراه که امکان دسترسی به اینترنت را همراه با ایمیل، شماره تلفن و خدمات پیام‌های متنی فراهم می‌کند (Blackberry).

26. B. Cubby, & A. McNeilage, "Police Investigate Rioters' Text Messages," Sydney Morning Herald, Sept 117, 2012, http://www.smh.com.au/nsw/police-investigate-rioters-text-messages-20120916-260mk.html (Accessed September 5, 2016).

۵. کلاهبرداران و متخصصان حرفه‌ای که وظیفه توسعه و به‌کارگیری طرح‌ها و برنامه‌های مهندسی اجتماعی و جمعی ازجمله فیشینگ[۲۷] و اسپمینگ[۲۸] (هرزنگاری) را برعهده دارند؛
۶. هاست‌ها که وظیفه ارائه تسهیلات سرورها و سایت‌های (با محتوا و مضمون) غیرقانونیِ امن و بی‌خطر را برعهده دارند؛
۷. صندوقداران یا کشرها که حساب‌ها را کنترل می‌کنند و درنهایت اسامی و حساب‌ها را درمقابل دریافت دستمزد و اجرت به دیگر مجرمین ارائه می‌دهند؛
۸. قاطران پول[۲۹] که وظیفه انتقال ماحصل کلاهبرداری‌هایی را که آنها انجام داده‌اند را به یک شخص ثالث، برای انتقال بعدی آن به یک مکان امن عهده‌دار می‌باشند؛
۹. تحویلداران که مسئولیت انتقال و شستشوی درآمدهای غیرقانونی را ازطریق خدمات ارزی دیجیتالی و بین ارزهای مختلف ملی برعهده دارند؛
۱۰. مدیران (اجرایی) سازمان‌ها که تعیین‌کننده اهداف سازمان هستند که وظیفه استخدام و به‌کارگیری نیروهای جدید و واگذاری وظایف مذکور در فوق را به اعضاء دارند. به‌علاوه توزیع درآمدهای مجرمانه و جنایی را مدیریت می‌کنند.

این نوع ایده‌آل از سازمان‌ها لزوماً محدود به یک سازمان و تشکیلات دائمی نمی‌شود. بعضی از وظایف ممکن است به بیرون از سازمان واگذار شود مانند مورد مربوط به گروه کوب‌فیس.[۳۰و۳۱] سازمان جرایم اینترنتی در یک سطح گسترده‌تر می‌تواند شامل شبکه‌ای از افراد که در انواع انجمن‌های آنلاین و چت‌روم‌ها حضور و تعامل دارند، باشد که بعضی از این انجمن‌ها تحت عنوان «بازار سیاه مجازی» تبلیغات می‌کنند به‌عنوان مثال تبلیغ و آگهی برای فروش کارت‌های اعتباری اعضاء. در میان مجرمان سایبری چینی QQ یک سرویس پیام‌رسانی فوری و چت محبوب و همچنین انتخابی ارجح برای برقراری ارتباط و تماس با اشخاص مربوط به کاردینگ ـ خریدوفروش کارت‌های اعتباری ـ می‌باشد. باتوجه‌به طبیعت

27. Fishing
28. Spaming
۲۹. قاطران پول به‌عنوان واسطه برای مجرمان و سازمان‌های جنایی خدمت می‌کنند. این کار، گاه آگاهانه و گاهی غیرآگاهانه انجام می‌شود. به‌هرحال وظیفه حمل‌ونقل متقلبانه پولی را که از کلاهبرداری حاصل شده است، برعهده دارند. استفاده از واسطه‌ها، تشخیص هویت کلاهبرداران و متقلبان واقعی را دشوار می‌کند.
30. Koobface
31. R. Richmond, "Web Gang Operating in the Open," New York Times, 2012, http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-usedfacebook-to-spread-worm-operates-in-the-open.html?pagewanted=all&_r=0 (Accessed September 14, 2016).

بی‌دوام و زودگذر بسیاری از فعل‌وانفعالات، چنین شبکه‌هایی به‌جای گروه‌هایی با بافت فشرده و به‌هم‌پیوسته، به‌عنوان شبکه‌های کلان جنایی راه‌اندازی و به‌کار گرفته می‌شوند.

همچنین ممکن است نمونه‌های کاربردیِ مفید و بالقوه دیگری از سازمان‌های موردبحث در جرایم سایبری وجود داشته باشد. به‌عنوان نمونه ترسیم طرح جغرافیای اقتصادی که در آن دسته‌های کسب‌وکار و تجارت محصولاتی مشابه با نمونه اصلی و در مجاورت آن که معمولاً در سرتاسر جهان یافت می‌شود را ارائه می‌دهند. تورسایت‌ها مانند جاده ابریشم که نقاط کانونی برای بازارهای غیرقانونی، ازطریق جذب فروشندگان و خریداران درگیر و دخیل در تجارت آنلاین مواد مخدر می‌باشند، شامل تراکم بالا یا خوشه‌ای مجرمان هستند.

در مطالعات سازمانی نظریه پیچیدگی[۳۲]، برگرفته از نظریه سیستم‌ها می‌تواند به شرح و توصیف ماهیت پویا و رفتارهای جمعی گروه‌ها کمک کند.[۳۳و۳۴] گروه‌های جرایم سایبری ممکن است درگیر یکی از انواع جرم باشند اما بعداً به انواع دیگر جرایم که از شیوه‌های متفاوتی استفاده می‌کنند، روی آورند و تغییر جهت دهند. به‌عنوان مثال کاربرپ[۳۵] یک جعبه ابزار نرم‌افزاری طراحی‌شده برای سرقت از بانک‌هاست که در ابتدا برای استفاده شخصی در نظر گرفته شده بود و تنها در دسترس گروه‌های انحصاری جرایم سایبری قرار داشت، اما بعدها زمینه فروش آن به دیگران فراهم شد، تصویری از شیوه‌های گسترش کسب‌وکار مجرمانه را ارائه می‌دهد.

۴- نمونه‌هایی از جرایم و مجرمان سایبری

در این بخش ابتدا نمونه‌هایی از مجرمان انفرادی و به‌دنبال آن نمونه‌هایی از گروه‌های سازمان‌یافته خصوصی و در انتها نیز مواردی از جرایم سایبری دولت‌ها و موردحمایت دولت‌ها را ارائه می‌دهیم.

۳۲. حسین رحمان سرشت، «پیچیدگی در سازمان»، *فصلنامه مطالعات مدیریت* ۴۹ (۱۳۸۵)، ۲۴–۱.
۳۳. سید مهدی الوانی، *مدیریت عمومی* (تهران: نشر نی، ۱۳۸۶)، چاپ سی و یکم، ۴۸۶–۴۸۵.
۳۴. علی رضائیان، *تجزیه و تحلیل و طراحی سیستم* (تهران: سمت، ۱۳۸۳)، ۱۰۸–۱۰۰.
35. Carberp

۴-۱- مجرمان سایبری انفرادی

۴-۱-۱- آرون اسوارتز:[۳۶] دانلودکننده محتوا[۳۷]

برنامه‌نویس دانشگاه هاروارد، آرون اسوارتز ۲۴ساله، در سال ۲۰۱۱، پس از دانلود بیش از چهار میلیون مقاله علمی ازطریق شبکه مربوط به Jstor ـ یک مخزن دانشگاهی آنلاین ـ مؤسسه تکنولوژی ماساچوست (MIT)، تحت تعقیب قرار گرفت. در سپتامبر ۲۰۱۰ اسوارتز لاگین‌های بی‌نام‌ونشانی را برای ورود به شبکه مورداستفاده قرار داد و تا هنگامی‌که MIT و Jstor سعی بر متوقف کردن و جلوگیری از حجم عظیم کپی‌رایت‌های مخفیانه و غیرقانونی داشتند، با جدّیت و پشتکار به پنهان‌سازی لاگین‌های خود ادامه داد. بعد از اینکه Jstor دسترسی به پایگاه داده (دیتابیس[۳۸]) خود را از تمام شبکه MIT متوقف نمود، او به محوطه دانشگاه رفت و به‌طور مستقیم لپ‌تاپ خود را به زیرساخت‌های یک اتاق شبکه MIT متصل و همانجا پنهان کرد و درنتیجه موفق به دانلود محتوای بیشتری شد. بااین‌حال یکی از مدیران بخش IT از وجود لپ‌تاپ مطلع و آن را به مقامات گزارش داد. یک وب‌کم مخفی نصب شد و هنگامی‌که اسوارتز برای برداشتن لپ‌تاپش آمده بود، شناسایی و دستگیر شد. اسوارتز هیچ اطلاعات محرمانه‌ای را سرقت نکرد و به‌دلیل آنکه محتوای سایت حفظ شده بود، Jstor تمایل به اقدام قانونی دراین‌زمینه نداشت. بااین‌حال دادستان فدرال اقدام و اسوارتز به سیزده فقره جرم متهم شد. (ایالات‌متحده آمریکا علیه آرون اسوارتز، ۲۰۱۲) اسوارتز به‌عنوان یک فعال آزادی اطلاعات شناخته شد که به‌خاطر نقض قوانین کپی‌رایت، به‌خصوص در رابطه با انتشار تحقیقات سرمایه‌گذاری‌شده عمومی و دولتی متهم شده بود. اسوارتز بنا به گفته خودش درواقع به رکود، افول و مخفی کردن تحقیقات علمی و دانشگاهی توسط Jstor اعتراض داشته و برنامه او درواقع فراهم نمودن امکان دانلود مقالات برای عموم و دسترسی آزاد به آنها بوده است. او در اوایل سال ۲۰۱۳ پیش از اینکه حکم نهایی صادر شود دست به خودکشی زد. خانواده‌اش دولت را مسئول مرگ اسوارتز می‌دانستند چراکه دادستان نسبت به یک جرم بدون قربانی غیرخشونت‌بار، بسیار متعصبانه برخورد کرده بود. در مارس ۲۰۱۳ پس از مرگش جایزه جیمز مدیسون توسط انجمن کتابخانه‌های آمریکا به او اهدا شد، یک جایزه برای قدردانی از آنهایی که مبارزان آزادی اطلاعات ـ دسترسی عموم به

36. Aaron Swartz
37. Content Downloader
38. Data Base

اطلاعات ـ می‌باشند.[۳۹] فعالیت‌های اسوارتز منطبق با صفات و شخصیت افراد خواهان آزادی اطلاعات بود، بااین‌حال بدیهی است که عمل او تمرد و طغیان علیه نظام حاکم بر حمایت از مالکیت معنوی می‌باشد.

۴-۱-۲- سم یین:[۴۰] هکر گوچی[۴۱]

سم یین ۳۴ساله، پس از اینکه به اتهام فروش کیف و کفش‌های به سرقت‌رفته مارک گوچی در بازار خاکستری آسیا، اخراج شد، موفق به هک سیستم‌های کمپانی گوچی با استفاده از یک حساب مخفی ـ در زمان اشتغال آن را ساخته بود ـ شد و از یک نام کارمندی ساختگی استفاده کرد. او عملکرد تمام کامپیوترها را از کار انداخت و دسترسی کارمندان به فایل‌ها و ایمیل‌ها را حدوداً به مدت یک روز کامل کاری قطع کرد. در طول آن روز سرورها را حذف، ذخیره‌ها و تنظیمات را نابود کرد و صندوق‌های پستی را از بین برد. گوچی هزینه‌های این نفوذ را ۲۰۰ هزار دلار برآورد کرده است. در سپتامبر ۲۰۱۲ یین به مدت حداقل دو سال و حداکثر شش سال، به زندان محکوم شد. این مورد به‌نظر می‌رسد یک نمونه واضح و روشنِ اقدامات تلافی‌جویانه توسط یک کارمند خشمگین اخراج‌شده می‌باشد.

۴-۲- گروه‌های کوچک سازمان‌یافته جرایم سایبری

۴-۲-۱- دریم‌بورد[۴۲]

دریم‌بورد یک گروه از اعضای انفرادی بود که تصاویر مستهجن از کودکان زیر ۱۲ سال را تا زمانی که در سال ۲۰۰۹ با تحقیقات پلیس چندملیتی[۴۳] تحریم و قدغن شد، مبادله می‌کردند. نتیجه این عملیات ایراد اتهام علیه ۷۲ نفر در چهارده کشور، در پنج قاره مختلف بوده است. سرور دریم‌بورد در ایالات‌متحده واقع و مدیران ارشد این گروه در فرانسه و کانادا بودند. قواعد رفتار و عملکرد گروه به زبان‌های روسی، انگلیسی، ژاپنی و اسپانیایی بر روی بولتن هیئت‌مدیره سایت قرار گرفته بود. انتخاب اعضای مناسب عملی بسیار پیچیده، مشکل و نیازمند همکاری مستمر در موضوع مواد مخدر به‌عنوان یکی از شرایط عضویت و پاداش‌دهی

39. A. Cohen, "Was Aaron Swartz Really "Killed by the Government"?," Time Ideas, http://ideas.time.com/2013/01/18/was-aaron-swartz-really-killed-by-thegovernment.
40. Sam Yin
41. Gucci
42. Dreamboard
43. Multi-National Police

کسانی که مطالب خود را به اشتراک می‌گذاشتند، بود. کاربران سطح‌های رده‌بندی‌شده ـ پلکانی ـ که منعکس‌کننده کمیت و کیفیت همکاری و عملکرد آنها بود، به‌دست می‌آوردند. اعضای گروه از نام‌های مستعار به‌جای نام اصلی خود استفاده می‌کردند. لینک‌های مربوط به محتواهای غیرقانونی رمزگذاری شده و رمز عبور به‌شدت محافظت می‌شد. امکان دسترسی به بولتن هیئت‌مدیره گروه ازطریق سرورهای پروکسی فراهم می‌شد. (وزارت امنیت اطلاعات داخلی، ۲۰۱۱) می‌توان گفت در دریم‌بورد هدف اصلی و عمده اعضای گروه ارضای جنسی بوده، اگرچه رقابت برای کسب جایگاه بالاتر در داخل گروه نیز مشهود است.

۴-۳- جرایم سایبری دولت‌ها و موردحمایت دولت‌ها

در طول سه دهه گذشته شاهد پیشرفت و افزایش قابل‌توجهی در جرایم اینترنتی بوده‌ایم، افزایشی آشکار در حجم و میزان فعالیت‌های غیرقانونی دولت‌ها و نمایندگان آنها. به‌دلیل طبیعت حساس چنین پدیده‌هایی است که هم ماهیتشان و هم میزان گرایش به آنها، از دید عموم پنهان می‌شود. باوجوداِین افشاگری‌های اخیر که به برخی از موارد آن در ادامه اشاره می‌شود، آموزنده و حاوی اطلاعات مفیدی بوده است. می‌توانیم زنجیره‌ای از تعامل دولت و بخش خصوصی را تجسم کنیم، از انحصار دولت در فعالیت‌های مجرمانه که در یک انتهای آن قرار دارد تا ناآگاهی و جهل دولت‌ها از فعالیت‌های مجرمانه بخش خصوصی که در انتهای دیگر این زنجیره قرار دارد. در بین تقابل و تضاد این دو قطب افراطی؛ همکاری رسمی بین نهادهای دولتی و غیردولتی، سطح پایین همکاری بین مقامات دولتی و مجرمان بخش خصوصی، سطح بالای حمایت از سوی دولت، تشویق ضمنی جرایم غیردولتی، تبدیل شدن دولت به چشمی نابینا نسبت به فعالیت‌های مجرمانه و ناتوانی دولت برای کنترل فعالیت غیرقانونی بخش خصوصی ممکن و مشاهده می‌شود.[۴۴]

44. M. Stohl, "Strange Web: Or How They Stopped Worrying and Learned to Love Cyber War," in *Cyberterrorism: A Multidisciplinary Approach*, ed. T. Chen, L. Jarvis, S. Macdonald (New York: Springer, 2014), 141-156.

۴-۳-۱- واحد PLA 61398 [۴۵]

در فوریه سال ۲۰۱۳ شرکت امنیت اطلاعات مندینت[۴۶] گزارش کرد که یک برنامه جاسوسی صنعتی در مقیاس بسیار وسیع از سال ۲۰۰۶ توسط واحد ۶۱۳۹۸ ارتش آزادی‌بخش خلق چین به اجرا درآمده است. مقر این سازمان در شانگهای، اعلام کرده باید حجم بالایی از اطلاعات را از طیف گسترده‌ای از صنایع در کشورهای انگلیسی‌زبان به‌دست آورد. اطلاعات موردِادعا شامل مشخصات فنی، استراتژی‌های مذاکره، اسناد قیمت‌گذاری و دیگر اطلاعات اختصاصی می‌شود. یکی از اهداف موردِادعا یک تولیدکننده عمده محصولات غذایی و آشامیدنی ایالات‌متحده آمریکا (برنامه‌ریزی‌شده در سال ۲۰۰۹) بود که درواقع بزرگ‌ترین هدف یک کمپانی چینی تا به امروز می‌باشد. این‌طور گزارش شده است که ظاهراً یک ایمیل بی‌خطر به یکی از مدیران اجرایی کمپانی آمریکایی حاوی لینکی ارسال شده بود که هنگام بازگشایی اجازه دسترسی و دستیابی مهاجمین به شبکه کمپانی را می‌داد. اطلاعات حساس مربوط به مذاکرات به شکل گزارش توسط اخلال‌گران چینی و به‌گونه‌ای منظم قابل‌دسترسی بود. هنوز معلوم نیست که این واحد منحصراً مجهز به پرسنل نظامی است یا شامل پیمانکاران غیرنظامی نیز می‌شود.[۴۷] در مه سال ۲۰۱۴، پنج افسر PLA توسط مقامات ایالات‌متحده به‌طور غیابی به جرم جاسوسی صنعتی متهم شدند (دادگاه بخش ایالات‌متحده آمریکا، ایالات‌متحده برعلیه وانگ). همچنین به‌عنوان نمونهٔ دیگر سال‌ها قبل جاسوسان سایبری چین موفق شدند که اسناد مربوط به ساخت هواپیمای بسیار پیشرفته و ضدِرادار آمریکا به نام اف–۳۵ را بدزدند و اکنون بعد از گذشت مدتی توانستند مانند آن را به نام هواپیمای ضدِرادار جی ۲۰ تولید کنند. در آن زمان که آمریکا دزدی اطلاعات مربوط به این هواپیمای جنگنده را ردیابی کرده بود، متوجه شد که کشور چین این کار را انجام داده اما چین این را یک تهمت قلمداد کرد و انجام این کار را انکار کرد.

در سال ۲۰۱۱ دفتر اطلاعاتی پنتاگون متوجه شد که از این اطلاعات در سازمان «ای‌وی‌آی‌سی» چین که کار ساخت هواپیماهای جنگنده را به‌عهده دارد، استفاده می‌شود اما

---

۴۵. یک واحد از ارتش آزادی‌بخش خلق چین می‌باشد که ادعا شده، مرجع حملات هک کامپیوتری به‌عنوان بخشی از سلسله عملیات نظامی چینی (کمپین چینی) برای سرقت اسرار تجاری و نظامی از اهداف خارجی (سایر کشورها) می‌باشد.

46. Mandiant

47. D. E. Sanger, D. Barboza & N. Perlroth, “China’s Army Is Seen as Tied to Hacking against U.S,” The New York Times, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seenas- tied-to-hacking-against-us.html (Accessed September 18, 2016).

کاخ سفید به این موضوع اهمیتی نداد و این مسئله را باور نکرد. به‌هرحال آمریکا هنوز نتوانسته است جلوی دزدی‌های سایبری دولت چین را بگیرد و این دزدی‌ها آمریکایی‌ها را بسیار عصبانی کرده است.[۴۸]

۴-۳-۲- عملیات بازی‌های المپیک

بنابر گزارش‌ها، عملیات بازی‌های المپیک یک همکاری بین آژانس امنیت ملی آمریکا و همتای صهیونیست خود، واحد ۲۰۰۸، به‌قصد اخلال در برنامه غنی‌سازی هسته‌ای ایران بوده است. ظاهراً آن‌طور که ادعا شده این طرح شامل مجموعه بسیار پیچیده، سطح بالا و ماهرانه‌ای از نرم‌افزار در ارتباط با ارتباطات (تعاملات) و سیستم‌های کنترلی تأسیسات هسته‌ای نطنز می‌باشد (که به‌طور عمومی تحت عنوان استاکس‌نت[۴۹ و ۵۰] شناخته می‌شود). این نرم‌افزار بنابر گزارش‌ها دارای ظرفیت و قابلیت نظارت بر ارتباطات، عملیات پردازش و همچنین قادر به تخریب سیستم‌های کنترلی تأسیسات مذکور بوده است. عملیات فوق‌الذکر موفق به تأخیر در جریان غنی‌سازی اورانیوم ازطریق تخریب کنترل از راه دورِ تعدادی از سانتریفیوژهای مورداستفاده در فرایند غنی‌سازی بوده است. اما سرانجام محرمانه و سرّی بودن عملیات در معرض خطر قرار گرفت، زمانی که نرم‌افزارهای مخرب به‌دلیل خطای برنامه‌نویسی و ضعف در برنامه‌نویسی از بین رفتند. به‌هرحال نه دولت آمریکا و نه رژیم صهیونیستی، هنوز وجود چنین عملیاتی را تصدیق و به آن اعتراف نکرده‌اند. به‌هرحال بنابر گزارش‌ها و اخبار در گذشته تنها تهدیدات آمریکا در جنگ سایبری فقط روسیه و چین بوده‌اند اما اکنون ایران هم به یک قدرت نوظهور دراین‌زمینه تبدیل شده است و به‌سرعت درحال جبران ضعف‌ها و مشکلات خود می‌باشد. برای مثال ایران در اقدامی متقابل و تلافی‌جویانه چندین بار به سازمان‌های پولی و مالی، اطلاعاتی و نظامی آمریکا حمله کرده است.[۵۱]

---

۴۸ میترا جلیلی، «دزدی دولت چین، آمریکایی‌ها را بسیار عصبانی کرده است»، ۲۲ اسفند ۱۳۹۲، جام‌نیوز، http://www.jamnews.ir/detail/News/329849.

۴۹. استاکس‌نت یک کرم کامپیوتری مخرب است که تصور می‌شود سلاحی سایبری آمریکایی ـ صهیونیستی است که به‌طور مشترک ساخته شده.

50. Stuxnet

۵۱. «ایران هیچ حمله سایبری را بی‌پاسخ نمی‌گذارد»، جام‌نیوز، ۲۵ اسفند ۱۳۹۲، http://www.jamnews.ir/detail/News/330781 (۱۳۹۵/۰۶/۲۷).

نتیجه

مباحث بالا دو مسئله اساسی را مطرح می‌کند. اول اینکه آیا سازمان‌ها و مجرمان فردی اهداف مشابهی را دنبال می‌کنند؟ دوم اینکه طبقات نوع‌شناختی (تیپولوژی) مک گایر و چابینسکی متناسب با نمونه‌هایی که ما به‌اختصار بیان کردیم و رابطه بین جرم و شکل سازمانی (درصورت وجود) می‌باشد؟

ازآنجاکه نمونه‌های موردبحث به‌صورت تصادفی انتخاب شده‌اند لذا نتایج ما نیز نمی‌تواند به‌عنوان نتایج قطعی در نظر گرفته شود. در عوض نتایج تجربی مذکور می‌تواند مبنایی برای تحقیق بیشتر باشد. اگرچه موارد مذکور نمی‌تواند نماینده و نمایانگر جرایم سایبری به‌طورکلی باشند، اما می‌توان گفت مجرمین فردی موردبحث در بالا نسبت به ایدئولوژی آزادی فردی، به چالش کشاندن تکنولوژی، عقده و وسواس شهرت و انتقام‌جویی برعلیه کارفرمای سابق کمتر گرفتار انگیزه‌های مالی می‌باشند. البته این امر بیان‌گر این نیست که پول برای مجرمین اینترنتی انفرادی مهم نیست، در عوض تنوع نمونه‌های موردِمشاهده می‌تواند درک ما را نسبت به محدوده و تنوع انگیزه‌های فردی افزایش دهد.

سازمان‌ها بیشتر انعکاسی از تنوع اهداف ازجمله مخالفت با قدرت، آزادی اطلاعات، لذت جنسی اعضاء و به چالش کشاندن تکنولوژی می‌باشند. بااین‌حال انگیزه کسب سود در نمونه‌های سازمانی بیشتر از مجرمین شخصی و انفرادی به چشم می‌خورد. همچنین بررسی و توجه‌به فعالیت‌های تقبّل‌شده توسط سازمان‌های فعال تحت نظارت دولت، به‌طور خاص شامل عملیات و فعالیت‌های جاسوسی و تهاجم سایبری می‌شود. این اهداف صریح و روشن سیاسی و اقتصادی به‌طور قطع شامل رسوایی و انگشت‌نمایی نمی‌شود. مقایسه مجرمین فردی و سازمان‌های جنایی نشان می‌دهد که هر دو گروه از مهارت قابل‌توجهی برخوردارند. با وجود مهارت‌ها، قابلیت‌ها و استعداد بسیار خوب برخی مجرمین فردی، مهارت و منابع برخی از سازمان‌ها حقیقتاً فوق‌العاده و درخور توجه می‌باشد. این امر به‌ویژه درمورد فعالیت‌های سایبری دولت‌ها مشهود است، اگرچه نباید فراموش کرد کار برخی از مجرمین فردی نشان‌دهنده پیچیدگی و پختگی قابل‌ملاحظه عملیات آنهاست. همان‌طور که در بالا موردبحث قرار گرفت ساختار سازمانی ارائه‌شده توسط مدل چابینسکی بیشتر بیانگر ویژگی‌های نمونه‌های سطح بالا و پیچیده مانند شرکت‌های پیچیده کلاهبرداری، نسبت به سایر انواع جرم می‌باشد.

گونه‌شناسی مک گایر نیز به‌نظر می‌رسد در تعدادی از نمونه‌هایی که بحث کردیم معتبر و موثق باشد. جرایم دولتی به‌نظر می‌رسد بیشتر با فرم سلسله‌مراتبی و در آنجا که نیروهای غیردولتی درگیر و دخیل هستند با فرم ترکیبی توسعه‌یافته سازگار می‌باشند. تقلب و کلاهبرداری‌های پیچیده دارای فرم سلسله‌مراتبی است. بازارهای آنلاین در ارتباط با فعالیت‌های مربوط به کلاهبرداری آنلاین، بیانگر و نمایانگر ویژگی‌های شبیه به دسته‌ها می‌باشند. از مدیران تا اعضای عادی در این گروه‌ها که سایت موردنظر طیفی از جرایم سایبری را مجاز می‌دارد و مجرمین بالقوه با منافع مشترک به‌منظور خریدوفروش اطلاعات مسروقه گردهم می‌آیند. فعالیت‌های اعتراضی موقتی با ماهیتی کوتاه‌مدت به‌وسیله گروه‌های تراکمی انجام می‌شود. بازارهای غیرقانونی شبیه قطب‌ها هستند.

این پژوهش بیانگر مراحل ابتدایی مطالعه و بررسی فعالیت‌های مجرمانه سایبری سازمان‌یافته می‌باشد. هر تکنولوژی جدید و هر نرم‌افزار جدید فرصتی را فراهم می‌آورد که بزهکاران درصدد سوءاستفاده از آن برمی‌آیند. برای حفظ هم‌سطحی و پهلوبه‌پهلو پیش رفتن با جرایم اینترنتی پیگیری و بررسی مداوم سیر تکاملی گونه‌های سازمانی‌ای که این فعالیت‌های مجرمانه را انجام می‌دهند از اهمیت ویژه‌ای برخوردار است. این مقاله گامی کوچک در این راستاست.

فهرست منابع

الف) منابع فارسی

الوانی، سیّد مهدی. *مدیریت عمومی*. چاپ سی و یکم. تهران: نشر نی، ۱۳۸۶.

بیابانی، غلامحسین. «جرایم سازمان‌یافته ملّی و فراملّی». *نشریه کارآگاه* ۶(۲۴) (۱۳۹۲): ۴۶–۳۱.

جام‌نیوز. «ایران هیچ حمله سایبری را بی‌پاسخ نمی‌گذارد». ۲۵ اسفند ۱۳۹۲. http://www.jamnews.ir/detail/News/330781 (۱۳۹۵/۰۶/۲۷).

جلیلی، میترا. «پسر تروریست اندونزیایی، عامل قتل ۲۰۲ نفر در سوریه کشته شد». ۲۴ مهر ۱۳۹۴. خبرگزاری جمهوری اسلامی. http://www.irna.ir/fa/News/81801228/ (۱۳۹۵/۰۷/۱۳).

جلیلی، میترا. «جبهه‌ای که با دستور مستقیم اوباما گشوده شد، جنجالی‌ترین طرح آمریکا برای مبارزه با هکرها». مؤسسه فرهنگی مطبوعاتی ایران، http://iran-newspaper.com/Newspaper/MobileBlock?NewspaperBlockID=58281 (۱۳۹۵/۰۷/۱۳).

جلیلی، میترا. «جرایمی که صرفاً سازمان‌یافته نیستند». پلیس فتا. http://www.cyberpolice.ir/cyberspace/48991 (۱۳۹۵/۰۷/۰۱).

جلیلی، میترا. «دزدی دولت چین، آمریکایی‌ها را بسیار عصبانی کرده است». ۲۲ اسفند ۱۳۹۲. جام‌نیوز. http://www.jamnews.ir/detail/News/329849.

رحمان‌سرشت، حسین. «پیچیدگی در سازمان». *فصلنامه مطالعات مدیریت* ۴۹ (۱۳۸۵): ۲۴–۱.

رضائیان، علی. *تجزیه و تحلیل و طراحی سیستم*. تهران: سمت، ۱۳۸۳.

شمس ناتری، محمدابراهیم. «آمریکا بزرگ‌ترین هکر و عامل جرایم سایبری جهان». ۲۹ اردیبهشت ۱۳۹۲. http://www.yjc.ir/fa/news/4389396 (۱۳۹۵/۰۷/۰۱).

شمس ناتری، محمدابراهیم. «بررسی سیاست کیفری ایران در قبال جرایم سازمان‌یافته با رویکردی به حقوق جزای بین‌الملل». رساله دکتری، تهران: دانشگاه تربیت مدرس، ۱۳۸۰.

شمس ناتری، محمدابراهیم. «جرایم سازمان‌یافته». *نشریه فقه و حقوق* ۱ (۱۳۸۳): ۱۳۰–۱۰۹.

ب) منابع انگلیسی

Broadhurst, R., & Y. C. Chang. *Cybercrime in Asia: Trends and* Challenges. Asian Handbook of Criminology. NewYork: Springer, 2013.

Chang, Y. C. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham, UK: Edward Elgar Publishing, 2012.

Cohen, A. *Was Aaron Swartz Really "Killed by the Government"?* Time Ideas. http://ideas.time.com/2013/01/18/was-aaron-swartz-really-killed-by-thegovernment.

Cubby, B., & A. McNeilage. "Police Investigate Rioters' Text Messages." Sydney Morning Herald. http://www.smh.com.au/nsw/police-investigate-rioters-text-messages-20120916-260mk.html (Accessed September 5, 2016).

Docket Alarm. United States of America v Aaron Swartz, Superseding Indictment (US District Court, District of Massachusetts September 12, 2012). Retrieved on 5th October, 2013 from https://www.docketalarm.com/cases/Massachusetts_District_Court/1--11-cr- 10260/USA_v._Swartz/53/.

International Computing Science Institute. United States of America v Ross William Ulbricht (2013) Sealed Complaint, Southern District of New York 27 September. Retrieved on 5th October, 2013. http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf.

Kshetri, N. *Cyber-Victimization and Cyber-Security in China*. New York, NY, United States: Communications of the ACM, 2013.

McGuire, M. *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security, 2012.

Moura, G. C. *Internet Bad Neighborhoods*. Enschede, The Netherlands: Centre for Telematics and Information Technology, 2013.

Pauli, D. "China is the "World's Biggest Cybercrime Victim." *SC Magazine* (2012). http://www.scmagazine.com.au/News/294653china-is-the-worlds-biggestcybercrime-victim.aspx (Accessed September 15, 2016).

Richmond, R. "Web Gang Operating in the Open." *New York Times* (2012). http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-usedfacebook-to-spread-worm-operates-in-the-open.html?pagewanted=all&_r=0 (Accessed September 14, 2016).

Sanger, D. E., D. Barboza & N. Perlroth. "China's Army Is Seen as Tied to Hacking against U.S." The New York Times (2013). http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seenas-tied-to-hacking-against-us.html (Accessed September 18, 2016).

Stohl, M. "Strange Web: Or How They Stopped Worrying and Learned to Love Cyber War." In *Cyberterrorism: A Multidisciplinary Approach*, edited by T. Chen, L. Jarvis, S. Macdonald. New York: Springer, 2014.

United States Attorney, Eastern District of New York (2003) Press Release Massive Internet and Credit Card Fraud Bilks Consumers out of $230 Million in Bogus "Free Tours" of Adult Entertainment Websites - Gambino Soldier, Two Executives and 5 Companies Indicted. Retrieved on 5th October, 2013. http://ebookbrowsee.net/cr-03-304-pressrelease-us-v-salvatore-locascio-pdfd19910473.

US Securities and Exchange Commission. In the Matter of Jonathan G. Lebed (2000). Retrieved on 5th October, 2013 http://www.sec.gov/litigation/admin/33-7891.htm; http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm (Accessed September 17, 2016); http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/01/18/mafiaboy010118.