دانشکده حقوق و علوم سیاسی

چالش‌های مقابله با جرم جاسوسی سایبری با تأکید بر قوانین کیفری ایران

استاد راهنما

دکتر عبدالرضا جوان جعفری بجنوردی

استاد مشاور

دکتر سید حسین حسینی

دانشجو

احسان نوروزی

شماره دانشجویی

۹۵۱۳۲۳۱۱۰۳

زمستان ۱۳۹۸

فهرست مطالب

عنوان | صفحه

چکیده ۱

مسأله پژوهش ۲

اهمیت و ضرورت پژوهش ۴

هدف پژوهش ۷

پرسش پژوهش ۷

فرضیه پژوهش ۸

پیشینه‌ی پژوهش ۸

روش پژوهش ۱۳

دشواری پژوهش ۱۳

سامان‌دهی پژوهش ۱۴

بخش اول: چالش‌های بین‌المللی مقابله با جرم جاسوسی سایبری ۱۶

فصل نخست: چالش همکاری در سطوح بین‌المللی ۱۷

مبحث نخست:عدم همکاری در سطوح قانون‌گذاری ۲۱

گفتار نخست: کنوانسیون‌ها و معاهدات در فضای سایبر ۲۶

گفتار دوم: کنوانسیون بوداپست مدلی برای هماهنگ سازی ۲۹

مبحث دوم: همکاری در سطوح قضایی ۳۰

گفتار نخست: تعارض صلاحیت‌ها ۳۲
بند نخست: صلاحیت قضایی در قبال جاسوسان ۳۴
بند دوم: صلاحیت در کنوانسیون جرایم سایبری(بوداپست) ۳۶
گفتار دوم: تحصیل دلیل ۳۹
بند نخست: قابلیت آسیب‌پذیری سامانه‌های رایانه‌ای در برابر جاسوسان ۴۱
بند دوم: قابلیت آسیب‌پذیری ادله در برابر جاسوسان ۴۱
مبحث سوم: همکاری در سطوح اجرایی ۴۲
گفتار نخست: حق حاکمیت دولت‌ها و استقلال آن‌ها ۴۳
گفتار دوم: استرداد ۴۵
بند نخست: قاعده عدم استرداد اتباع دولت‌ها ۴۶
بند دوم: قاعده عدم استرداد به واسطه کیفرها ۴۷
گفتار سوم: ناشناختگی ۴۹
بند نخست: جعبه ابزار جاسوسان ۵۳
بند دوم: چرایی گمنامی و نظریه فردیت‌زدایی ۵۵
فصل دوم: جاسوسی و تقابل آن با نقض حریم خصوصی ۵۸
مبحث نخست: مفهوم حریم خصوصی و جنبه‌های آن ۵۹
گفتار نخست: جلوه‌های نقض حریم خصوصی در فضای سایبر ۶۳
گفتار دوم: تولید و گردآوری داده‌ها ۶۴

گفتار سوم: پردازش داده‌ها ۶۵
مبحث دوم: ناقضان حریم خصوصی ۶۶
گفتار نخست: دولت‌ها ۶۷
گفتار دوم: بخش خصوصی(شرکت‌ها) ۷۱
بند نخست: فیسبوک ۷۳
بند دوم: سیاست حفظ حریم خصوصی توسط شرکت‌ها ۷۵
گفتار سوم: بدافزارها ۷۶
بند نخست: فیلترشکن‌ها ۷۷
بند دوم: تلگرام ۷۸
گفتار چهارم: حریم خصوصی در پرتو قوانین داخلی و تقابل آن با جاسوسی(بحث انتقادی) ۷۹
بخش دوم: چالش‌های داخلی مقابله با جرم جاسوسی سایبری ۸۱
فصل نخست: چالش‌های پلیسی ۸۳
مبحث نخست: عدم همکاری داخلی و خارجی ۸۶
گفتار نخست: خلأهای تقنینی ۸۹
گفتار دوم: تعدد نهادها و موازی کاری‌ها ۹۱
مبحث دوم: کمبود منابع مالی و انسانی ۹۱
مبحث سوم: آموزش سایبری ۹۵
گفتار نخست: مهندسی اجتماعی ۹۸

گفتار دوم: کنفرانس دفکان ۱۰۰
فصل دوم: چالش‌های فناورانه ۱۰۱
مبحث نخست: شکاف نرم‌افزاری و سخت افزاری ۱۰۲
گفتار نخست: عدم وجود زیر ساخت‌ها و تجهیزات بومی ۱۰۴
گفتار دوم: نظارت بر شبکه و چالش پیش روی ۱۰۵
گفتار سوم: ویروس استاکس نت ۱۰۷
گفتار چهارم: ویروس فیلم ۱۱۲
مبحث دوم: وب پنهان ۱۱۴
گفتار نخست: تقابل قانون با جاسوسی و وب پنهان ۱۱۷
گفتار دوم: سرقت هویت ۱۱۹
گفتار سوم: خلأها و چالش‌های قانون جرائم رایانه‌ای(بحث انتقادی) ۱۲۰
نتیجه گیری و پیشنهادات ۱۲۳
فهرست منابع ۱۲۷

تقدیر و تشکر

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت‌های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام و درود بر محمد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است؛ و نفرین پیوسته بر دشمنان ایشان تا روز رستاخیز... بدون شک جایگاه و منزلت معلم، اجل از آن است که در مقام قدردانی از زحمات بی‌شائبه‌ی او، با زبان قاصر و دست ناتوان، چیزی بنگاریم. اما ازآنجایی‌که تجلیل از معلم، سپاس از انسانی است که هدف و غایت آفرینش را تأمین می‌کند و سلامت امانت‌هایی را که به دستش سپرده‌اند، تضمین؛ بر حسب وظیفه و از باب " من لم یشکر المنعم من المخلوقین لم یشکر الله عزوجل":

از پدر و مادر عزیزم•••این دو معلم بزرگوارم... که همواره بر کوتاهی و درشتی من، قلم عفو کشیده و کریمانه از

کنار غفلت‌هایم گذشته‌اند و در تمام عرصه‌های زندگی یار و یاوری بی چشم داشت برای من بوده‌اند؛ از استاد با کمالات و شایسته؛ جناب آقای دکتر عبدالرضا جوان جعفری که در کمال سعه‌صدر، با حسن خلق و فروتنی، از هیچ کمکی در این عرصه بر من دریغ ننمودند و زحمت راهنمایی این پایان‌نامه را بر عهده گرفتند؛ از استاد صبور و باتقوا، جناب آقای دکتر سید حسین حسینی، که زحمت مشاوره این پایان‌نامه را در حالی متقبل شدند که بدون مساعدت ایشان، این پروژه به نتیجه مطلوب نمی‌رسید؛ و از اساتیدی که سعادت تلمذ در محضرشان را داشتیم، اساتیدی فرزانه و دلسوز؛ جناب آقای دکتر ساداتی و جناب آقای دکتر قپانچی؛ کمال تشکر و قدردانی را دارم.

باشد که این خردترین، بخشی از زحمات آنان را سپاس گوید.

چکیده

امروزه با گسترش اینترنت و فضای مجازی و عجین شدن این فضا با زندگی بشر، سبب شده که جرائم رایانه‌ای رشد لحظه‌ای به خود بگیرد، تا جایی‌که به نظر می‌رسد از این به بعد باید مفهوم امنیت و منافع ملی را در این فضا جست‌وجو کرد. به‌عبارتی باید حوزه سایبر را حوزه‌ی چهارم، در کنار سایر حوزه‌ها(هوایی، زمینی، دریایی) قلمداد کرد. اما این محیط و ویژگی‌های لاینفک آن(لامکانی، لا زمانی، گمنامی، ارزان بودن جرم، فراملی) باعث شده که بهترین شرایط برای تهدیدات سایبری مهیا شود.

علی‌ای حال یکی از مهم‌ترین تهدیدات سایبری که امنیت ملی را هدف خود قرار می‌دهد جرم جاسوسی سایبری است. هدف این جرم صرفاً در حوزه نظامی خلاصه نمی‌شود، بلکه در تمامی حوزه‌ها(اقتصادی، صنعتی، فرهنگی و...) نقش بسزایی ایفا می‌کند. اکنون یکی از اساسی‌ترین دغدغه‌های تمامی دولت و کشورها در رابطه با این جرم ارتقای سطح توانایی جهت کنترل، پیشگیری و مبارزه با این چنین جرمی است. اما این دغدغه زمانی بزرگ‌تر و حادتر می‌شود که همراه این دغدغه‌ها، چالش‌هایی (داخلی، خارجی) نیز دیده شود. این دغدغه‌ها و بالتبع چالش-های به دنبال آن موجب شده ما را بر آن دارد که در این پژوهش؛ چالش‌هایی که ممکن است دول بر سر راه خود جهت مبارزه با این جرم، ببینند را مطرح و سپس بررسی شود.

کلیدواژه‌ها: چالش‌ها، جاسوسی سایبری،کنوانسیون، بوداپست، همکاری همه جانبه، حریم خصوصی.

مسئله‌ی پژوهش

در عصر ارتباطات شاهد آنیم که جهان در حال تحول است. تحولاتی که با تأثر از فناوری‌های پیشرفته توانسته تغییراتی مهم در تمامی عرصه‌های اقتصادی، اجتماعی، فرهنگی، نظامی و صنعتی به وجود بیاورد. مفهوم امنیت هم از این قاعده مستثنی نبوده و جدای از مخاطرات و موضوعات مستحدثه در محدودیت امنیت و تهدیدات سایبری، این نگرانی‌ها از دنیای مجازی به زندگی واقعی بشر در هزاره سوم سرازیر شده و مسائلی را به وجود آورده که نیازمند توجه جدی و مسئولانه‌ی فعالان حوزه امنیت است. تا جایی که سخن از گره خوردن جنگ‌های سایبری در منازعات آینده است، جنگ‌هایی که برای مقابله با آن‌ها تدارک یک ارتش سایبری ضروری تلقی می‌شود.

در این بین ویژگی‌های دنیای سایبر نظیر دسترسی آسان، ناشناختگی، فقدان مرز، لامکان و لازمان و سرعت بالای اطلاعات باعث شده تا جرائم این فضا با معیار و مقیاس متفاوت‌تر و با گستره و آثار وسیع‌تر رخ دهد، طوری که جرائم سایبری نظام عدالت کیفری را با چالش‌های گریزناپذیری مواجه ساخته‌اند.

چالش‌هایی که تا قبل از ظهور این نوع جرائم وجود نداشته و سیاست جنایی نوینی را می‌طلبند (فرهادی آلاشتی، ۱۳۹۵).

مطالعات صورت گرفته نشان می‌دهد جاسوسی سایبری۱(من بعد جاسوسی نامیده می‌شود)یکی از شایع‌ترین فعالیت‌های سایبری است. خواه برای افشای اطلاعات حساس دولتی و سرقت اسرار تجاری و داده‌های بازرگانی به کار رود و خواه بخشی از کار اطلاعات و شناسایی باشد. به عبارتی دقیق‌تر جاسوسی از منظر دکترین، در چارچوب، استفاده از برتری اطلاعات برای رسیدن به پیروزی‌های بزرگ با هزینه‌ای کمتر، قرار می‌گیرد(موسسه فرهنگی مطالعات و تحقیقات بین‌المللی،[ابرار معاصر تهران]، ۱۳۹۱). بنابراین شیوه‌های کشف، تعقیب، تحقیق و پیشگیری سنتی در مورد این جرم دیگر پاسخگو نیستند و طراحی و هماهنگی برای مقابله با این جرم نیازمند ابزارها و

1.cyber spying/espionage

مهارت‌های هم‌تراز با مجرمین در این حوزه است (فرهادی آلاشتی، ۱۳۹۵). ناگفته پیداست مقابله با جرم جاسوسی خالی از چالش نیست. چالش‌هایی نظیر عدم همکاری کشورها در سطوح قانون‌گذاری، قضایی و اجرایی، دارک وب(وب پنهان)، ناشناختگی و.. باعث شده که جاسوسان این فضا را بهشت و مأمنی امن فرض کرده تا از این طریق اعمال مجرمانه خود را به مرحله اجرا برسانند. به عبارتی دقیق‌تر جاسوسان در پرتو این چالش‌ها می‌توانند از این آنارشیسم سایبری، نهایت استفاده را ببرند. در همین راستا مطالعات این حوزه، گویای این امر است که فهم دقیق ابعاد و چالش‌های این فضای جدید اطلاعاتی (جاسوسی سایبری) نیازمند کسب آگاهی از آخرین یافته‌های علمی و اطلاع از رویکرد کشورهای پیشرو در حوزه فناوری اطلاعات و زیرساخت‌های سایبری است. چه‌بسا اینکه برطرف نکردن خلأهای موجود و چالش‌ها، در عین نامتقارن بودن ظرفیت‌های فنی و ابزاری پیشرفته طرف منازعه، کشور را در رده کنشگران ضعیف عرصه اطلاعات و امنیت قرار داده و از این طریق تمامی حوزه‌ها (اقتصادی، اجتماعی، نظامی و...) را تحت تأثیر قرار می‌دهد و خسارات غیرقابل جبرانی به جای می‌گذارد(قرناوتی، ۲۰۱۳). همچنین در این بین شکاف نرم‌افزاری و سخت‌افزاری که در فضای سایبر ایجاد شده، موضوعی مهمی است که نباید از آن غافل ماند چرا که این مسئله، قدرت مانور بسیاری به ابرقدرت‌های جهان (چین- آمریکا) اعطا کرده است. تبعاً این کشورها نیز برای پیش بردن اهداف خود، حاضر نیستند این فناوری‌ها را در اختیار کشورهای ثالث قرار دهند. این سیاست (عدم انتقال دانش)، باعث شده کشورهای پیش‌رو در این فضا، اهرم فشار سیاسی، اجتماعی، اقتصادی و نظامی بر کشورها را همیشه در دست خود نگاه دارند.

اکنون اگرچه با توجه به گسترش ضریب نفوذ استفاده از رایانه و فضای سایبر به خصوص در میان جمعیت جوان کشور، خطر شیوع جرائم رایانه‌ای بالا رفته است، لیکن در طول یک دهه گذشته مقنن تلاش کرده تا با استفاده از مقررات بین‌المللی و کنوانسیون‌های موجود از طریق بومی‌سازی آن‌ها قوانین موردنیاز را تصویب و ابلاغ کند (محمد نسل، ۱۳۹۵). بارزترین این تلاش‌ها تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸ است، قوانینی که لازم‌اند ولی کافی نیستند. گرچه این فضا تراوش ذهنی حقوقدانان را به سمتی سوق داده است که مقررات انبوهی را وضع

نمایند، اما برای بهره‌برداری صحیح از این فضا و تبدیل شدن آن به فضایی قابل تحسین، نه فضایی سرشار از تهدید، کشورها بایستی بدانند تصویب قوانین کارآمد، باید در راستای ویژگی‌های منحصربه‌فرد این فضا صورت گیرد.

با این اوصاف چالش‌های موجود در حیطه جاسوسی، مزید بر علت شد که پژوهشگر در بعد حقوقی جاسوسی ورود کرده و چالش‌های موجود را مورد تجزیه‌وتحلیل قرار دهد. چالش‌هایی نظیر عدم هماهنگی قوانین کشورها یا فقدان قوانین در این حوزه با وضعیت بین‌المللی، هویت ناشناخته و به دنبال آن دادرسی کیفری در مقابله با این جرم (استرداد- تحصیل دلیل) و حریم خصوصی مورد بررسی قرار خواهد گرفت.

اهمیت و ضرورت پژوهش

اهمیت:

در جهان کنونی اطلاعات هر کشور از محرمانه گرفته تا خیلی سری، بسیار حیاتی و مهم تلقی می‌شود و طبیعتاً دولت-کشورها اجازه دسترسی به این اطلاعات و اسناد مهم را به ارگان‌ها و سازمان‌های بین‌المللی و کشورهای بیگانه نمی‌دهند. کشورهای جهان برای اینکه عنوان ابرقدرتی را یدک بکشند از هیچ تلاشی در عرصه‌های مختلف دریغ نمی‌کنند. آن‌ها هرروز برای رسیدن به این هدف علوم جدیدی را کشف می‌کنند تا از طریق آن بتوانند اطلاعات کشورهای دیگر را به دست آورند و قدمی در جهت اهداف خود بردارند (فاطمی راد،۱۳۹۱).

اکنون وظیفه کشور ما چیست؟ در پاسخ به این پرسش بایستی گفت: ما هم نظیر کشورها باید از این نکته غافل نباشیم که تلاش ما برای حفظ اطلاعات حیاتی در همه زمینه‌ها ما را به اهداف ملی و بین‌المللی خود نزدیک‌تر می‌کند. لذا در این راستا باید تهدیدها را شناسایی کنیم. به عبارتی دقیق‌تر خود ما باید به این مطلب امعان نظر داشته باشیم که اطلاعات ما توسط کشورهای بیگانه ربایش نشود. بنابراین همواره بایستی راه‌های نوین جاسوسی را بشناسیم تا بتوانیم راهکارهای مقابله با این پدیده را پیدا کرده و ابعاد آن‌ها را جهت جرم انگاری در قانون معین کنیم.

اکنون جاسوسی از طریق روش سنتی (نیروی انسانی) یک امر سخت، هزینه‌بر، خطرناک، وقت‌گیر و تیرگی روابط سیاسی میان کشورها[۲] را در بردارد. لذا کشورها با یک نگرش معقول به این فکر فرو رفتند که از راه‌های علمی، ساده‌تر و کم‌خطر اطلاعات کشورهای دیگر را جمع‌آوری کنند. "یکی از شایع‌ترین این راه‌ها جاسوسی سایبری است که در حال حاضر بیشتر کشورها از این روش استفاده می‌کنند" (فاطمی راد،۱۳۹۱:۱۸).

در سال‌های اخیر دستگیری جاسوس رژیم اشغالگر قدس در ایران[۳] و برپایی نمایشگاهی از ادوات مورد استفاده‌ی وی و نیز بیانات رهبری در جمع کارکنان وزارت اطلاعات در تاریخ ۱۳۸۷/۵/۲۳ در خصوص ارتقاء فناوری در وزارت اطلاعات که مفهوم کلی آن شناخت هرچه بیشتر فن‌آوری و زیرساخت‌های مخابراتی بود(بوجار،۱۳۸۸) و ایضاً حملات گسترده دستگاه‌های متخاصم، اهمیت این موضوع را روشن ساخت که: اولاً تهدیدهای جاسوسی را شناسایی کرده و نقاط ضعف خود را برطرف کنیم.

۲- سرگئی اسکریپال، سرهنگ بازنشسته اطلاعات ارتش روسیه، در سال۲۰۰۶ با حکم ۱۳ حبس در روسیه زندانی شد.
او متهم بود که با هویت مأموران اطلاعات روسیه به صورت مخفیانه در اروپا و بریتانیا فعالیت می‌کرد و اطلاعات را در اختیار ام آی سیکس سرویس اطلاعات مخفی بریتانیا قرار داده است.(" پایگاه بی‌بی سی فارسی"، ۱۳۹۶)

۳- علی اشعری، ۴۳ ساله فرزند محمود که به اتهام جاسوسی برای سرویس اطلاعاتی رژیم صهیونیستی، توسط وزارت اطلاعات دستگیر شده بود و در شعبه ۱۵ دادگاه انقلاب به اعدام محکوم و حکم وی در سحرگاه دوشنبه ۱۳۸۷/۸/۳۰ اجرا شد. .وی مدیریت یک شرکت تجاری را در تهران، دبی و یک کشور خارجی دیگر بر عهده داشت و محصولات مخابراتی، حفاظتی و امنیتی را به مراکز حساس می‌فروخت .توانایی اشتری در حوزه الکترونیک سبب شد برخی ادارات دولتی ازجمله مراکز تحقیقاتی کشور، سازمان انرژی اتمی و مجموعه‌های دفاعی و نظامی در پروژه‌های مرتبط از این فرد به عنوان یک متخصص امور فنی مشاوره بگیرند و این موضوع باعث دستیابی بیشتر فرد مذکور به اطلاعاتی شد که آن‌ها را به دستگاه امنیتی اسرائیل منتقل می‌کرد. از موضوعات نگران‌کننده تزریق تجهیزات الکترونیکی قابل شنود (نظیر بیسیم)توسط نامبرده به مراکز مهم کشور بود. او با هدایت موساد قطعات معیوب و نامناسبی را در اختیار دستگاه‌های مهم دولتی قرار می‌داد و در برخی موارد نیز مشاوره‌های غلط داشت که این خیانت باعث عدم پیروزی مجموعه‌ها در پروژه‌هایشان بود. بوجار(۱۳۸۸، به نقل از اظهارات مدیرکل ضد جاسوسی وزارت اطلاعات،۱۳۸۷)

دوما خود را در عرصه‌ی اطلاعات و زیرساخت‌های مخابراتی جزء کنشگران آن قرار داده تا بتوانیم اطلاعات حیاتی رایانه‌های کشورمان را حفظ کنیم و با وضع قوانین هماهنگ با جامعه جهانی و انجام مطالعات، نواقص قانونی و فنی را برطرف کرده تا از این طریق از ورود خسارات گسترده بر پیکره‌ی نظام عدالت کیفری و زیرساخت‌های کشورمان جلوگیری کنیم. فلذا بنده بر آن شدم با اهمیت فوق‌الذکر پژوهش خود را با عنوان یادشده دنبال کنم.

ضرورت:

گسترش سریع اینترنت و وسایل هوشمند، استفاده از این فضا را به بخش مهمی از زندگی بشر تبدیل کرده است. پس این انتظار وجود دارد بهره‌مندی از این فضا و تمرکز بر داده‌های و اطلاعات عظیم و حیاتی، تبدیل به عامل مهمی در تعیین قدرت رقابت‌پذیری کشورها شود. درعین‌حال زیان ناشی از حملات تاکنون سردرگمی‌هایی را به وجود آورده است چراکه این حملات فزاینده، باقدرت و پیچیدگی بیش از پیش نقش ایفا می‌کنند. همچنین ویژگی‌های فضای مذکور باعث شده اختلاف بین بازیگران این عرصه کاهش‌یافته و آسیب‌پذیری کشورها (حتی کشورهای پیشرو در این عرصه) بروز و نمود یابد. در این میان طبیعی است که کشورهای پیشرو در این عرصه به دلیل وابستگی زیاد به زیرساخت‌های اطلاعاتی و مخابراتی بایستی اقدامات اساسی را در جهت مقابله با تهدیدات در دستور کار خود قرار دهند. لازمه چنین اقدامی شناختن این فضا و بازیگران آن و در پی آن جستجوی برنامه‌های استراتژیک است، برنامه‌هایی که قادر باشند بعد جهانی مخاطرات جاسوسی را خنثی کنند. اکنون لزوم آشنایی با گفتمان حاکم بر جرم جاسوسی زمانی هویدا می‌شود که دریابیم در سال‌های اخیر جلوه‌های مختلف تحقق این جرم از بعد سنتی خود خارج شده است و شکلی نوین به خود گرفته. اما بیشتر آثار علمی منتشره در این حوزه همچنان به تبیین بعد سنتی آن جرم پرداخته است. لذا از یک‌سو نوین بودن این چالش‌ها و از سوی دیگر قلت آثار علمی حقوقی و فنی در رابطه با موضوع پژوهش و نیز عدم ارائه راه‌حل مناسب برای خنثی‌سازی چالش‌ها سبب شده این چالش‌ها از آثار علمی پیشی گیرد و مجال پرداختن به چالش‌ها سلب شود. لذا ضرورت دارد همگام با این چالش‌ها حقوق فناوری نیز به‌روز شود و این هدف در صورتی دست یافتنی است که تمامی ابعاد چالش‌ها به‌طور دقیق واکاوی شود. لذا پژوهشگر با این ضرورت به بررسی ابعاد می‌پردازد.

هدف پژوهش

محققان و اهل فن معتقدند هدف هر پژوهش در موضوع و عنوان تحقیق نهفته است. زیرا که محقق به دنبال آن چرایی و چیستی است که به صورت یک جمله خود را نشان داده است.

قانون‌گذار ما در ماده ۴ (" قانون جرائم رایانه‌ای"، ۱۳۸۸) به نقض تدابیر امنیتی برای دسترسی غیرمجاز به داده‌های سری اشاره‌کرده است. از فحوای کلام درمی‌یابیم امنیت قابل نقض می‌باشد، نقضی که اصولاً از طریق جاسوسی رخ می‌دهد. همان‌طور که در دنیای حقیقی و زندگی روزمره برقراری امنیت به‌طور کامل با مشکلاتی همراه است در فضای سایبر نیز به طریق اولی امنیت کامل دست‌نیافتنی است، چراکه با انبوهی از شبکه‌های درهم تنیده مواجهیم. امروزه بیشتر سیستم‌ها دارای نقاط ضعفی هستند. نقاطی که شاید از منظر ما بی‌اهمیت باشند ولیکن روزنه‌ای برای هکرها و سازمان‌های جاسوسی تلقی می‌شود تا از این طریق به اعمال مجرمانه خود دست پیدا کنند. پس در فضای سایبر امنیت کامل دست‌نیافتنی و موضوعی مهم، پیچیده و درعین‌حال مبهم است. نتیجتاً مقابله در برابر این تهدید سهمگین(جاسوسی در فضای سایبر)، در جامعه‌ای که روزبه‌روز رایانه‌ای می‌شود، جز با شناسایی درست و کامل آن(جاسوسی) امکان‌پذیر نیست. پس هدف شناسایی این فضا و در رأس آن جاسوسی سایبری، آگاهی از چالش‌ها، تنگناهای قانونی است تا قانون‌گذار و ارگان‌ها مرتبط با دیدی بازتر به این موضوع توجه و در مقابل آن ایستادگی کنند.

پرسش‌های پژوهش

۱- مهم‌ترین چالش مقابله با جرم جاسوسی سایبری کدام است ؟

۲- آیا قوانین ما و کشورها توانسته‌اند بر چالش‌های جرم جاسوسی ، فائق آید ؟

۳- جبران خلأ کدام یک از چالش‌های مطرح‌شده در حوزه‌ی جاسوسی (داخلی _ خارجی)، کمک حداکثری به قانون‌گذار در جهت مقابله با این جرم می‌کند؟

فرضیه‌های پژوهش

۱- چالش عدم همکاری و هماهنگی کشورها در تمامی سطوح در رابطه با جرم جاسوسی، مهم‌ترین چالش تلقی می‌شود؛ چراکه سایر چالش‌ها در سایه همکاری کشورها با یکدیگر رنگ می‌بازند. از طرفی عدم همکاری برای رسیدن به امنیت واقعی و قانونی منسجم در دنیای سایبر، سبب می‌شود فضای سایبر را بیش از پیش به محیطی جنگی، خطرناک، نامتقارن و توهین‌آمیز تبدیل می‌کند

۲- قوانین کشور ما مانند بسیاری از کشورها در این حوزه کافی نیست لذا کشورهای جهان می‌توانند با استفاده از هنجارهای مشترک در رویارویی با چالش‌ها و تنگناها قانونی ایستادگی کرده و فناوری سایبری، روش‌ها و فرصت‌ها مقابله با این جرم را بهبود ببخشند ولیکن جنبه فراملی این جرم پای کار بودن همه کشورها را می‌طلبد.

۳- چالش‌های جاسوسی سایبری مختص یک کشور خاص نیست. برطرف کردن خلاهای داخلی یا خارجی آن هم به تنهایی، تدابیر کشورها را در مقابله با این جرم با شکست مواجه می‌کند. این چالش‌ها دو روی یک سکه‌اند و کمک حداکثری به قانون‌گذاری زمانی ملموس می‌شود که خلأهای هر دو بعد جبران شود.

پیشینه‌ی پژوهش

پژوهش در ظاهر اگرچه امری فردی است ولی با دقت در آن درمی‌یابیم کاری گروهی است. هر مطالعه ضمن آنکه مبتنی بر مطالعات قبلی است خود نیز مقدمه‌ای برای مطالعات بعدی بشمار می‌رود. به همین دلیل یک راه ساده برای اینکه محقق از عقاید و آراء افرادی که در زمینه‌ی تخصص او کارکرده‌اند آگاه شود، مطالعه چکیده مقالات و مقدمه کتبی است که محتوایی نظیر محتوای تحقیق او دارد.

پیشینه جهانی در زمینه‌ی چالش‌های جاسوسی کارنامه درخشانی دارد. این پیشینه بعد کلی جرائم سایبری را در برگرفته طوری که اهم توجهات بر روی کلیه جرائم سایبری بوده است ولیکن بعد چالش‌ها در این حوزه مدنظر قرار نگرفته است، این بدان معنا نیست که اصلاً این بعد مدنظر نبوده، بلکه کانون توجهات نسبت بدان‌ها کم‌رنگ بوده است.

در این زمینه کتاب جرائم سایبری: راهنمایی و برای کشورهای در حال توسعه مارگو گرگی ترجمه مرتضی اکبری، انتشارات پلیس امنیت فضای تولید و تبادل اطلاعات ناجا درخور توجه است. کتابی که در ۶ فصل به رشته‌ی تحریر درآمده که در فصل ۳ کتاب مذکور چالش‌های مبارزه علیه سایبر را گوشزد کرده و در فصل ۶ کتاب واکنش‌های حقوقی نسبت به این پدیده را موردبررسی قرار داده است و جزئا به جاسوسی سایبری پرداخته است.

۲- کتاب آینده‌ی قدرت نوشته جوزف نای، انقلاب اطلاعاتی را دست‌اندرکار تغییر ماهیت قدرت و عامل پراکندگی آن معرفی کرده است. سپس با کاهش هزینه‌های جابجایی اطلاعات و حجم عظیم داده‌ها این نتیجه را بیان می‌کند که سیاست جهانی دیگر درید دولت‌ها نیست، چراکه هم افراد و هم جاسوسان سازمان‌های خصوصی و غیردولتی و تروریست‌ها توان نقش‌آفرین مستقیم در سیاست جهانی را دارند. ایشان به پراکندگی قدرت در فضای سایبر اشاره می‌کنند و در ادامه اهم توجه خود را به دولت آمریکا معطوف می‌کنند. دولتی که توانسته با تسلط بر فضای سایبر و جاسوسی موقعیت خود را در جامعه جهانی حفظ کند.

۳- سولانژ قرناوتی نگارنده کتاب قدرت سایبر خشونت، منازعه و امنیت در فضای سایبر است. کتابی که به زعم نویسنده افقی نو در ذهن خواننده درباره فضای سایبر ایجاد می‌کند. نویسنده در این کتاب به اقدامات دولت‌ها جهت آسیب رساندن به زیرساخت‌ها اشاره و چند صفحه‌ای به جاسوسی سایبری می‌پردازد و جهت روشن شدن موضوع مثال‌هایی ذکر می‌کند ازجمله اشاره کوتاه به ویروس استاکس نت(۲۰۱۰) دارند

پیشینه داخلی نیز هم در مورد چالش‌های جاسوسی سایبری کارنامه درخشانی ندارد و کتب موجود به بررسی جاسوسی سایبری به عنوان یک موضوع مهم، درخور کتاب بدان نپرداخته‌اند و لزوماً در حد یک فصل مورد واکاوی قرارگرفته است:

۱-کتاب حقوق جزای اختصاصی جرائم رایانه‌ای نوشته‌ی غلامرضا محمد نسل که در سال ۱۳۹۵ توسط نشر میزان به چاپ رسیده است. نویسنده در فصل اول کتاب خود جرم جاسوسی سایبری را در ذیل جرائم علیه محرمانگی

داده‌ها و سامانه‌ها بررسی کرده است. نویسنده رکن قانونی، مادی و معنوی جرم مذکور را واکاوی کرده و سعی بر آن داشته که نظرات دکترین متخصص این حوزه را نقد نماید و سخنی از چالش‌ها به چشم نمی‌خورد.

۲- کتاب حقوق و امنیت در فضای سایبر نوشته دکتر ابراهیم حسن بیگی، همچون بقیه نویسندگان جاسوسی سایبری را در فصل چهارم ذیل تشریح جرائم علیه امنیت موردتوجه قرار داده و تنها به ذکر تفاوت میان جاسوسی در فضای سایبر با جاسوسی کلاسیک بسنده کرده است.

۳- شاید بتوان اذعان کرد که یکی از کتب کامل در زمینه‌ی قدرت سایبر و جرائم رایانه‌ای، کتاب امنیت سایبری است. این کتاب در چهار جلد توسط موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران در سال ۱۳۹۱ به چاپ رسیده است. جلد نخست این کتاب ویژه مفاهیم و مبانی سایبری است، جلد دوم آن ویژه سلاح‌ها، جنگجویان و حملات سایبری است، جلد سوم مباحث سیاست‌ها و راهبردهای فضای سایبری است و جلد چهارم کتاب مذکور قوانین سایبر را موردمطالعه قرار داده است. از میان این چهار جلد، تنها جلد اول این کتاب به جرم جاسوسی سایبری پرداخته است.

همچنین پژوهشگر با رجوع به پایگاه‌های اطلاعاتی کتابخانه مرکزی دانشگاه فردوسی ، ایرانداک و سایر دانشگاه‌ها دریافت که؛ مجموعه پایان‌نامه‌هایی زیادی در زمینه‌ی جرائم رایانه‌ای به رشته تحریر درآمده است. از این میان پایان‌نامه‌هایی که جرم جاسوسی سایبری را بررسی کرده به نسبت مابقی پایان‌نامه‌ها میزان کمی از مطالعات را به خود اختصاص داده بود.

۱- از مهم‌ترین آن‌ها جاسوسی در فضای سایبر که توسط محمد عقیلی تدوین‌شده و در دانشگاه علامه طباطبایی دفاع شده(۱۳۹۰)، مدنظر قرار گرفت. ایشان در فصل چهار به یک چالش درزمینه‌ی مقابله با این جرم پرداخته است.

۲- جاسوسی رایانه‌ای دومین پایان‌نامه‌ای است که توسط سعید فاطمی راد(۱۳۹۱) در واحد تهران مرکز تدوین و دفاع شده، که موردتوجه بنده واقع شد. در این پایان‌نامه ابتدا در مورد دو عنوان جاسوسی و رایانه صحبت می‌شود، یعنی اینکه به بررسی ابعاد فنی و علمی این دو عنوان پرداخته است. همچنین جرم جاسوسی سایبری را در قوانین

کشور بررسی کرده و نهایتاً راهکارهای مقابله با جرائم رایانه‌ای را شرح داده است ولیکن به طور خاص چالش‌های مقابله با جرم جاسوسی سایبری را به عنوان یکی از جرائم رایانه‌ای مطرح نکرده است.

۳- حمایت کیفری از حریم خصوصی در فضای سایبر عنوان پایان‌نامه‌ای است که در سال ۱۳۸۵توسط دانشجو جعفر حسنی در دانشگاه شهید بهشتی دفاع شده است. این پایان‌نامه از این جهت که حریم خصوصی را در تقابل با فضای سایبر مورد مطالعه قرار داده نظر پژوهشگر را به عنوان یکی از چالش‌ها به خود جلب کرده است. در این پایان‌نامه به بدون مرز بودن فضای سایبر و به دنبال آن امکان ارتکاب جرائم بین‌المللی و نقض حریم خصوصی اشاره می‌کند و بیان می‌دارد که برخی کشورها لنگرگاهانی امن برای ارتکاب جرائم سایبری شده‌اند که بایستی برای پیشگیری از این جرائم و نقض نشدن حریم خصوصی افراد قوانین ملی هماهنگ و هم‌نوا شوند.

در حوزه مقالات باید اشاره کرد، از آنجایی که مقالات علمی پژوهشی نسبت به پایان‌نامه‌ها و کتب حجم انبوهی از پژوهش‌ها را به خود اختصاص می‌دهند، سبب شده که پژوهشگر بیشتر به آن‌ها در جهت تکمیل تحقیق خود استناد کند.

مقالات علمی پژوهشی

۱- جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن نوشته محسن رهامی و سیروس پرویزی.

۲- جرائم سایبر و چالش‌های نوین سیاست کیفری نوشته دکتر عبدالرضا جوان جعفری بجنوردی، مقاله‌ای که موضوع اصلی آن بیان دلایل و ضرورت‌های وجودی رویکرد افتراقی قوانین کیفری در مبارزه با جرائم رایانه‌ای است و ویژگی‌های این نوع جرائم را به طور کلی بررسی نموده‌اند.

۳- چالش‌های حقوقی جرائم سایبری در نظام بین‌المللی و نظام حقوقی ایران نوشته رضا صبح خیز، در این مقاله ضمن تشریح مبانی نظری پیرامون فضا و جرائم سایبری؛ اقدامات حقوقی ماهوی و شکلی انجام‌شده در خصوص جرائم سایبری در بین نظام حقوق بین‌الملل و ایران مورد تحلیل قرار داده و در ادامه، در یافته‌های خود بر این امر صحه می‌گذارد که نظام بین‌الملل و ایران با چالش‌های فراگیر و عمیقی همچون تعرض قوانین و دادگاه‌ها مواجه‌اند

که در نتیجه با لحاظ کردن شرایط همگون حقوقی با سایر کشورها و همکاری بین‌المللی می‌توان این چالش‌ها را به صورت نسبی مرتفع کرد.

۴- انقلاب سایبر و تحول در پدیده‌ی جاسوسی عنوان مقاله‌ای است که توسط میر ابراهیم صدیق نگاشته شده است. در این مقاله ضمن تبیین ماهیت انقلاب سایبری، به دنبال پاسخ به این سؤال است که این انقلاب چگونه بر ماهیت و محتوای جاسوسی تأثیر گذاشته است. کما اینکه یافته‌های این مقاله نشان می‌دهد تحت تأثیر انقلاب سایبری، انقلاب در عرصه جاسوسی واقعیتی جدی و اجتناب‌ناپذیر است.

۵- چالش‌های رویارویی پیشگیری موقعیت مدار از جرائم سایبری فرامرزی نوشته دکتر عبدالرضا جوان جعفری بجنوردی و زهرا فرهادی آلاشتی، در این مقاله نگارنده به این مهم دست می‌یابد که چالش‌های حقوقی و پلیسی به عنوان مهم‌ترین چالش‌های پیشگیری از جرائم فرامرزی به‌حساب می‌آیند، لذا به بررسی آنان پرداخته است و سپس راهکارهای پیشنهادی را برای غلبه بر این چالش‌ها ارائه داده‌اند.

۶- جاسوسی رایانه‌ای در قانون ایران و تدابیر پیشگیری از آن نوشته مهرداد شریفی، نویسنده این مقاله جرم جاسوسی سایبری را به عنوان یکی از خطرناک‌ترین جرائم در سطح ملی و بین‌المللی یاد می‌کند و در پی آن وضعیت تقنینی جرم جاسوسی سایبری را بررسی و اقدامات پیشگیری از آن مهم را ذکر می‌کند.

همچنین مقالات همایشی که در کنفرانس پدافند غیرعامل در قلمرو فضای سایبر مورخ اسفندماه ۱۳۹۵ ارائه شد نیز مورداستفاده قرارگرفته است.

۱- جاسوسی سایبری به عنوان چالش عصر امروزی نوشته بابک پور قهرمان و سکینه برزگری.

۲- جاسوسی سایبری و ضرورت مقابله با آن نوشته بابک پور قهرمان و زینب محمدصادقی.

۳- پاسخ کیفری در مقابله با جاسوسی در فضای مجازی نوشته علی اسکان لو.

با این حال تفاوت این پژوهش با پیشینه‌های مذکور در بالا در این است که: آثار نوشته‌شده در جرم جاسوسی سایبری صرفاً به مباحث حقوقی از بعد شکلی و ماهوی و شناسایی خود جرم برای اعمال طرق قانونی بر آن‌ها بوده است و تحلیل اندکی روی چالش‌ها صورت گرفته است. به عبارتی رویه‌ی محققان این‌طور است که عناصر قانونی،

مادی و معنوی جرم را ذکر کرده و سپس بررسی نموده و در آخر نظرات موجود در آن حوزه را نقد و در صورت صاحب‌نظر بودن، نظر خود را مکتوب می‌کنند. غافل از آنکه در این رویه توجهی مبنایی بر روی چالش‌ها و تنگناهای جرم نمی‌شود، فلذا محقق در این پژوهش بر آن است عمده تمرکز مباحث بر روی چالش‌ها و تنگناهای موجود در این حوزه را قرار گیرد.

روش پژوهش

این پژوهش جز پژوهش‌های نظری بوده و روش علمی که در این پژوهش مورداستفاده قرارگرفته، روش توصیفی-تحلیلی می‌باشد. در این تحقیق سعی بر آن بود که از نظریه‌ها و مبانی موجود و اصول و ضوابط حاکم بر گفتمان سایبری، که در پرتو آن جاسوسی نهفته است، استفاده شود. در اینجا اهمیت عنوان پژوهش سبب شده است، مطالعه قوانین و کنوانسیون‌های مورد نیاز، امری اجتناب‌ناپذیر تلقی شود. همسو با مطالعه قوانین و کنوانسیون‌های ، استدلال‌هایی نیز بدان‌ها اضافه شده، تا حصول نتیجه مطلوب هر چه بهتر میسر شود. ضمن اینکه استفاده از منابع اینترنتی و پرونده‌های کیفری داخلی و خارجی در این زمینه، ذهن مخاطب را برای درک بهتر و تجزیه و تحلیل جامع آماده کند تا مخاطب بعد از درک اهمیت این فضا، بابی جدید از ابعاد این فضا و چالش‌های فراروی نظام عدالت کیفری پیش روی خود ببیند.

دشواری پژوهش

عنوان جاسوسی موضوعی است که به دلیل مشکلات امنیتی که در آینده ممکن است به وجود آید، دستگاه‌های اطلاعاتی، سازمان‌های مرتبط و دستگاه‌های رسیدگی‌کننده از دادن اطلاعات مورد نیاز برای پایان‌نامه‌ها و کتب-هایی با این موضوع، دریغ می‌کنند.

آنها برای همکاری در این زمینه بسیار محتاطانه عمل می‌کنند و همکاری‌های لازم را در این زمینه اعمال نمی‌دارند. لذا فقدان آگاهی مطلوب محققان حقوقی به امور اطلاعاتی و امنیتی(فنی) که خود دانش و رشته‌ای مجزاست، سبب شده نگاه در این حوزه، صرفاً نگاهی تک بعدی(حقوقی) باشد. تبعاً این قبیل جرائم برای تمامی کشورها و