Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 2, Issue 1, 2022

Cybercrime and Threats against Security and the Challenges Ahead

Sadegh Moradi [1], Mohsan Shekarchizadeh *[2], Amirreza Naghsh [3], Gholamhossein Masoud [4]

1. Ph.D Student, Department of Law, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
2. Assistant Professor, Department of Law, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran. (Corresponding Author)
3. Assistant Professor, Department of Management, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
4. Assistant Professor, Department of Law, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 37-50

Corresponding Author's Info
ORCID: *0000-0001-8769-9798*
TELL: *+983142292929*
Email: *mohsen.shekarchi@gmail.com*

Article history:
Received: *03 Nov 2021*
Revised: *01 Feb 2022*
Accepted: *21 Feb 2022*
Published online: *21 Mar 2022*

Keywords:
Security Crimes, Cyber Threat, Cyber Disruption.

ABSTRACT

Security is considered as one of the basic elements of efficiency and providing services to citizens and beyond that, it is the survival of existing political systems. Crimes against security have always been an significant topic of discussion. The present paper is an attempt to examine the threats and crimes against security in the Iranian legal system and its future challenges. The present paper is an analytical descriptive study and using the library method to investigate the subject under study. The findings of the study show that cyber crimes, such as espionage and unauthorized cyber access are among the crimes against security that have been criminalized. But security is also exposed to other important cyber threats that pose future security challenges. Cyber terrorism, cyber warfare, cyber disruption and hacking, phishing, farming, and smashing are among the security threats that are considered as future challenges because of the unclear nature of cyber security challenges, and dealing with it requires criminal and non-criminal prevention.

How to Cite This Article: Moradi, S; Shekarchizadeh, M; Naghsh, AR & Masoud, GhH (2022). "Cybercrime and threats against security and the challenges ahead". *Journal of Comparative Criminal Jurisprudence*, 2(1): 37-50.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره دوم، شماره اول، بهار ۱۴۰۱

تهدیدات و جرایم سایبری علیه امنیت و چالش‌های پیش‌رو

صادق مرادی[۱]، محسن شکرچی‌زاده[۲]*، امیر رضا نقش[۳]، غلامحسین مسعود[۴]

۱. دانشجوی دکتری، گروه حقوق، دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۲. استادیار، گروه حقوق، دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران. (نویسنده مسؤول)

۳. استادیار، گروه مدیریت، دانشکده علوم انسانی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۴. استادیار، گروه حقوق، دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۳۷-۵۰

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۱-۸۷۶۹-۹۷۹۸

تلفن: ۹۸۳۱۴۲۲۹۲۹۲۹+

ایمیل: mohsen.shekarchi@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۰/۰۸/۱۲

تاریخ ویرایش: ۱۴۰۰/۱۱/۱۲

تاریخ پذیرش: ۱۴۰۰/۱۲/۰۲

تاریخ انتشار: ۱۴۰۱/۰۱/۰۱

واژگان کلیدی:

جرایم علیه امنیت، تهدید سایبری، اخلال سایبری.

چکیده

امنیت از مؤلفه‌های اساسی کارآمدی و و ارائه خدمات به شهروندان و فراتر از آن بقاء نظام‌های سیاسی موجود است. جرایم علیه امنیت همواره از موضوعات مهم و محل بحث و نظر بوده است. در این مقاله تلاش شده به بررسی تهدیدات و جرایم علیه امنیت در نظام حقوقی ایران و چالش‌های آینده آن پرداخته شود. مقاله پیش‌رو توصیفی تحلیلی بوده و با استفاده از روش کتابخانه‌ای به بررسی موضوع مورد اشاره پرداخته شده است. یافته‌های تحقیق حاکی است که جرایم سایبری مانند جاسوسی و دسترسی غیر مجاز سایبری از جمله جرایم علیه امنیت است که جرم‌انگاری شده است. اما امنیت در معرض تهدیدهای سایبری مهم دیگری نیز قرار دارد که چالش‌های آینده امنیت محسوب می‌شود. تروریسم سایبری، جنگ سایبری، اخلال و هک سایبری، فشینگ، فارمینگ، اسمیشینگ از جمله تهدیدهای امنیتی است که به دلیل ماهیت نامشخص چالش‌های امنیتی موجود در فضای سایبر از چالش‌های آینده محسوب شده و مقابله با آن نیازمند پیشگیری کیفری و غیرکیفری است.

مقدمه

امنیت اساسی‌ترین نیاز بشر است و به همین دلیل تأمین یا حفظ آن نخستین وظیفه حکومت‌ها است (شمس، ۱۳۸۸: ۲۹). یکی از اهداف حقوق حفظ امنیت است (آشوری، ۱۳۹۲: ۸۲). هیچ مکتب و نظام حقوقی نمی‌تواند فارغ از مسأله امنیت و فاقد سیاست‌های انتظامی باشد وگرنه نسبت به علت و فلسفه وجودی خود بی‌اعتنا است و نمی‌تواند جدی و پایدار تلقی شود. (کوشکی، ۱۳۹۲: ۴۷) از طرفی حق حیات افراد در شرایطی تضمین می‌شود که امنیت و اطمینان و آرامش در جامعه حکم‌فرما گردد و هیچ رفتاری نتواند امنیت اشخاص را به خطر انداخته و آرامش آن‌ها را سلب کند، مگر قانونی که حدود این حق را به همراه ضمانت اجراهای آن مشخص می‌کند. در همه کشورها، آنچه امنیت حاکمیت را دستخوش ناامنی نماید جرم تلقی می‌شود هر چند ممکن است عناوین مجرمانه متفاوت باشد اما حفظ و تأمین کشور در صدر اولویت‌های هر کشوری قرار دارد. علم حقوق نیز به مقوله امنیت بی‌توجه نبوده و اقدامات برهم زننده امنیت جرم‌انگاری شده است (آشوری، ۱۳۹۲:۵). همواره مجازات جرایم علیه امنیت از شدیدترین عقوبت‌ها بوده است (صانعی،۱۳۷۲: ۳۲۸). به نحوی که مثلاً حبس کردن مجرمان سیاسی به همراه جانوران موذی یا انداختن این افراد در «قلعه فراموشی» از جمله مجازات‌های معمول در ایران باستان بوده است (راوندی، ۱۳۶۸: ۱۹). در عصر جدید بحث امنیت اما تحت تأثیر متغیرهای نوینی قرار گرفته که تبیین رویکردها در این خصوص را به یک ضرورت مبدل ساخته است. رایانه و فضای سایبر مهم‌ترین متغیر نوین تأثیرگذار در این حوزه است. رایانه و فضای سایبر در زندگی بشر روز به روز توسعه پیداکرده و تحولات شگرفی را در جوامع ایجاد کرده است، اما این پدیده نیز همانند سایر امور، دارای دستاوردهای مثبت و منفی است. باوجود منافع زیاد استفاده از رایانه و فضای مجازی، این ابزار خالی از آسیب نیز نبوده است. ظهور جرایم جدید رایانه‌ای یکی از پیامدهای منفی گسترش به‌کارگیری رایانه در شؤون مختلف اطلاعاتی و ارتباطی بوده است. واقعیت این است که هر اختراع و نوآوری به‌سرعت می‌تواند نظر مجرمان را به خود جلب کرده و مورد استفاده قرار گیرد اما جامعه نیز مقدوراتی برای برخورد با چنین سوء استفاده‌هایی در اختیار دارد که حقوق جزا یکی از این ابزارها به شمار می‌رود. در خصوص جرایم علیه امنیت تألیفات متعددی انجام شده است: محمدرضا الهی‌منش و محسن مرادی‌اوجقاز، در کتابی به بررسی جرایم علیه امنیت و آسایش عمومی پرداخته‌اند. (الهی‌منش و مرادی‌اوجقاز ،۱۳۹۴) محمد محمودی، سید محمود میرخلیلی و کریم بخنوه، در مقاله‌ای، جرایم علیه امنیت و حقوق شهروندی در پرتو اصول جرم‌انگاری را بررسی کرده‌اند. (محمودی و همکاران، ۱۳۹۸) همچنین جلیل محبی و زینب ریاضت، در مقاله‌ای، مبانی و مدل کیفرگذاری جرایم علیه امنیت را مورد بررسی قرار داده‌اند. (محبی و ریاضت، ۱۳۹۵) اما چالش‌های آینده در خصوص امنیت از موضوعات مهمی است که چندان مورد توجه قرار نگرفته است. سؤال اساسی که در این خصوص مطرح و بررسی می‌شود این است که رویکرد نظام حقوقی ایران نسبت به تهدیدها و جرایم علیه امنیت چگونه بود و امنیت در آینده با چه چالش‌های مواجه است؟ به منظور بررسی و پاسخ به سؤال مورد اشاره ابتدا رویکرد نظام حقوقی ایران به جرایم سایبری علیه امنیت پرداخته شده و در ادامه از چالش‌های آینده و راه‌کارهای پیشگیری در این خصوص بحث شده است.

۱- تهدیدها و جرایم سایبری علیه امنیت

۱-۱- جاسوسی سایبری

جرم «جاسوسی سایبری» امروزه به دلیل ورود اینترنت در تمام زوایای زندگی بشری و استفاده از شیوه‌های مدرن و جدید جهت جاسوسی و خرابکاری در اطلاعات، در زمره

جرایمی می‌باشد که جایگاه بخصوصی را در زمینه جرایم در فضای سایبر به خود اختصاص داده است و ازجمله جرایم علیه امنیت و آسایش عمومی می‌باشد، زیرا این جرم مخاطرات شدیدی را برای امنیت ملی خواهد داشت. جاسوسی سایبری «یکی از غالب‌ترین اشکال استفاده‌شده برای جرم رایانه‌ای است. اهمیت آن به‌ویژه از حیث مرتکب و خطرات برای دولت متضرر از آن‌جهت است که اطلاعات ارزشمند در مراکز رایانه‌ای بیشتر سازمان‌ها و حتی شرکت‌ها ذخیره می‌شود.» (بیگی، ۱۳۸۴: ۲۱۱) جاسوسی رایانه‌ای جرمی است که در آن در عمل رایانه به‌منزله‌ی موضوع جرم جزء رکن مادی اعلام‌شده است. به‌عبارتی‌دیگر، در جاسوسی رایانه‌ای داده‌ها و اطلاعات یا به عبارتی موضوع جرم در مرحله مقدماتی انجام جرم دارای پایه و قالب مادی نیست که قابل لمس باشد و دارای وجود خارجی نبوده و صرفاً در فضای سایبر وجود دارند؛ بدون اینکه به‌صورت خارجی مثل سی‌دی درآمده باشد (رهامی و پرویزی، ۱۳۹۱: ۱۸۰). در جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه جمع‌آوری شود. برخلاف جرایم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است (خلیلی پور رکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۷۴).

جاسوسی رایانه‌ای علی‌رغم جاسوسی سنتی به‌صراحت در قانون مجازات اسلامی بیان‌شده است. مواد ۳ تا ۵ قانون جرایم رایانه‌ای به موضوع جاسوسی اختصاص داده‌شده است. قانون‌گذار ایران نیز ماده ۳ قانون جرایم رایانه‌ای را به جرم جاسوسی رایانه‌ای اختصاص داده است. ازنظر ماهیت تفاوتی بین جاسوسی سایبری و جاسوسی کلاسیک وجود ندارد و در هر دو نوع جاسوسی مرتکب در جهت کسب اطلاعات می‌باشد و تنها تفاوت بین این دو نوع جاسوسی در استفاده از رایانه می‌باشد و آن‌هم به دلیل الکترونیکی شدن فعالیت‌ها در جهت کسب اطلاعات مختلف است. جرم جاسوسی سایبری از لحاظ انجام عملیات نظیر جاسوسی به شیوه سنتی و کلاسیک می‌باشد. در هر دو نوع از جاسوسی هدف و انگیزه مرتکب یکسان است، تنها طرق و شیوه‌ی دستیابی به این انگیزه متفاوت است یعنی در جاسوسی سایبری از طریق سامانه‌های الکترونیکی و رایانه‌ای به این اهداف دسترسی پیدا می‌کنند.

در قانون مجازات اسلامی مصادیق جرم جاسوسی به‌صورت مبهم اشاره شده است ماده ۵۰۱ ق.م.ا **«هرکس نقشه‌ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند قرار دهد یا از مفاد آن مطلع کند به‌نحوی‌که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال حبس محکوم می‌شود.»**

عنصر مادی این جرم افشای اسرار، نقشه‌ها، اسناد داخلی و خارجی می‌باشد یعنی مرتکب باهدف و نیت جاسوسی و خبرچینی اخبار و اطلاعات محرمانه غیرمجاز و مهم کشور را در اختیار افراد فاقد صلاحیت قرار دهد. پس اگر عمل شخص از روی سهل‌انگاری و بر اثر بی‌احتیاطی باشد را نمی‌توان مشمول حکم این ماده قرارداد و عمل شخص را جاسوسی دانست.

«به دلیل فقدان قانون در زمینه تعریف جاسوسی و مصادیق آن، فضای ابهام‌آلودی درباره مصادیق این جرم وجود دارد لیکن از آنجا که تحقق جرایم مذکور، خود موکول به وجود آمدن جرایم جاسوسی می‌باشد، مصادیق یادشده را تنها باید به‌عنوان جرایم مرتبط با جاسوسی در حقوق کیفری ایران قلمداد نمود» (مجیدی، ۱۳۸۶: ۱۱۵).

جاسوسی سایبری شامل دسترسی غیرقانونی به اطلاعات سری طبقه‌بندی‌شده و حفاظت‌شده به‌وسیله رایانه یا وسایل الکترونیکی می‌باشد که باهدف و نیت انجام عملیات تروریستی و ضربه وارد ساختن به اطلاعات صورت می‌پذیرد.

امروزه با توجه به نقش و کارکرد کامپیوتر در زندگی انسان‌ها و ورود آن به زندگی بشر سبب شده است که اطلاعاتی به‌عنوان اسرار در زمینه‌های سیاسی، اجتماعی، اقتصادی در آن نگهداری و ذخیره شود که افشای این اسرار لطمات جبران‌ناپذیری را برای امنیت کشور داشته باشد (دزیانی، ۱۳۸۵: ۴۷). بنابراین می‌توان جاسوسی سایبری را به مرز صنعت و تجارت کشاند و حتی در در فضای سایبر جاسوس با اهداف مختلف مانند سرقت هویت می‌باشد. سرقت هویت عبارت است از تصاحب یا ادعای هویت شخص دیگر است. اتخاذ عنوان یا هویت دیگری برای کسب مال یا خدمات است یا برای ارتکاب جرم (پاکزاد، ۱۳۹۰: ۲۹۳). زمینه‌های مختلف مبادلات نیز از کامپیوتر به‌عنوان وسیله‌ای در جهت کسب اطلاعات و به دست آوردن اسرار تجاری استفاده کرد به‌عبارت‌دیگر جاسوس به هر طریقی به دنبال ضربه زدن و کسب اطلاعات محرمانه می‌باشد.

قانون‌گذار ایران در ماده ۳ قانون جرایم رایانه‌ای چنین مقرر می‌دارد: **«هر کس به‌طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد: الف) دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون ریال تا سقف شصت میلیون ریال یا هر دو مجازات. ب) در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها، به حبس از پنج تا پانزده سال. تبصره ۱: داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می‌زند.»** برای تحقق عنصر قانونی این جرم عمل شخص باید به‌صورت دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا افشای آن‌ها باشد و بر اساس حکم این ماده صورت بگیرد پس اگر عمل شخص با عناصر تشکیل‌دهنده این ماده مغایر باشد مشمول حکم این ماده نمی‌باشد.

۱-۲- دسترسی غیرمجاز

دسترسی غیرمجاز یکی از مهم‌ترین افعال مجرمانه می‌باشد که توسط سیستم‌های رایانه‌ای انجام می‌شود و به‌عنوان نخستین گام در ارتکاب سایر جرایم سایبری و به‌عنوان تهدیدی خطرناک بر علیه محرمانگی داده‌ها و سیستم‌ها تلقی می‌شود. فصل یکم قانون جرایم سایبری در فضای تبادل اطلاعات، جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را شامل می‌شود که شامل موضوعاتی از قبیل دسترسی غیرمجاز، جاسوسی سایبری می‌باشد. جایگاه بحث این‌گونه جرایم در تقسیم‌بندی‌های حقوق جزای اختصاصی در مبحث جرایم علیه امنیت و آسایش عمومی می‌باشد. **«دسترسی غیرمجاز شامل جرایمی می‌باشد که تهدیدهای خطرناک و تعرض علیه امنیت (یعنی محرمانگی، تمامیت و دسترسی‌پذیری) سیستم‌ها و داده‌های رایانه‌ای را در برمی‌گیرد. نیاز به محافظت، منافع سازمان‌ها و افراد در مدیریت، اجرا و کنترل سیستم‌هایشان را بدون وجود مزاحمت بازتاب می‌دهد. صرف تعرض غیرمجاز، یعنی هک کردن، کرک کردن و یا ورود به عنف رایانه باید غیرقانونی تلقی شود»** (جلالی فراهانی، ۱۳۸۹: ۲۶).

گاهی مجرم با دستیابی غیرمجاز سبب از کار افتادن سیستم‌های رایانه‌ای یا مخابراتی، از بین رفتن اطلاعات مهم و محرمانه افراد گردد و یا گاهی با ارتکاب این عمل سبب آسیب رساندن به سیستم‌های بیمارستان‌ها، اورژانس، مراکز بهداشتی شود که حتی کوچک‌ترین اختلالی بتواند صدمات جبران‌ناپذیری را به همراه داشته باشد. **«برخی هکینگ را مترادف با دسترسی غیرمجاز می‌دانند ولی این واژه چه در آماج و**

چه در نوع سیستم با دسترسی غیرمجاز متفاوت است زیرا واژه هکینگ در دانش فنی- مهندسی به‌کار می‌رود و به سیستم‌های رایانه‌ای مربوط است و علاوه بر دسترسی غیرمجاز شامل اعمالی مانند تجزیه، تحلیل و نسخه‌برداری یا اختلال در سیستم و وصف مجرمانه می‌باشد» (تحیری، ۱۳۸۴: ۸۹). شخص در دسترسی غیرمجاز می‌تواند از طریق شبکه‌های رایانه‌ای و مخابراتی به داده‌ها حتی در سیستم‌هایی که حالت امن نصب نمی‌باشد دسترسی یافته و مرتکب جرم شود.

عنصر قانونی این بزه مطابق ماده ۱ قانون جرایم رایانه‌ای است. بر اساس ماده مورد اشاره **«هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت‌شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.»**

برای تحقق جرم باید عمل شخص مصداق مشخص این ماده باشد و توسط قانون‌گذار نیز حکمی وضع‌شده باشد پس اگر عمل شخص با عناصر تشکیل‌دهنده این ماده مغایر باشد مشمول حکم این ماده نخواهد شد. دسترسی غیرمجاز به معنای دستیابی غیرقانونی به داده‌ها یا اطلاعات در سیستم‌های رایانه‌ای یا مخابراتی می‌شود. منظور از تدابیر امنیتی حفاظت‌شده به وجود آوردن شرایطی است که فقط افراد مجاز در یک سازمان بتوانند به اطلاعات موجود در رایانه یا مخابرات دسترسی یابند و افراد غیرمجاز حق دستیابی به این‌گونه اطلاعات را ندارند.

۱-۳- تروررسیم سایبری

ازلحاظ لغوی واژه «تروریسم» از کلمه «ترور» برگرفته‌شده است؛ و در زبان لاتین به معنای «ترس» به معنای وحشت است. ولی واژه تروریسم سایبری از دو اصطلاح تروریسم و سایبر برگرفته‌شده است. واژه تروریسم دارای گونه‌های متفاوتی می‌باشد مانند تروریسم رسانه‌ای، تروریسم بین‌المللی، تروریسم فرهنگی، تروریسم سایبری و غیره. در تروریسم سایبری که برجسته‌ترین انواع آن می‌باشد، خشونت به شکلی که در اقسام دیگر تروریسم است، وجود ندارد ولی ارتکاب رفتار مجرمانه می‌تواند آسیب‌های جبران‌ناپذیری بر پیکره جامعه وارد نماید و به‌عنوان تهدید جدی برای امنیت ملی به شمار آید.

تروریسم سایبری همگرایی تروریسم و فضای سایبری است و عموماً به معنای تهاجم غیرقانونی و تهدید به تهاجم علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن‌ها، به‌منظور ارعاب یا اعمال زور بر دولت یا ملتی جهت پیشبرد هدف‌های سیاسی یا اجتماعی است. بعلاوه، در توصیف تروریسم سایبری، تهاجم باید منجر به تعرضی علیه شخص یا اموال شود یا حداقل سبب صدمه‌ای شود که ایجاد ترس نماید. تهاجماتی که موجب مرگ یا جراحت بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارت‌های شدید اقتصادی می‌شوند، مثال‌هایی در این زمینه هستند. تهاجمات شدید علیه زیرساخت‌های حیاتی را بسته به میزان اثرات آن‌ها، می‌توان در رده اقدامات تروریستی قرارداد و تهاجماتی که خدمات غیراساسی را مختل می‌سازند یا عمدتاً مزاحمتی پرهزینه هستند، در این مقوله قرار نخواهند گرفت (پاکزاد ۱۳۹۰: ۹۰). تروریست‌ها از فضای سایبری به‌عنوان کارزاری جهت انجام اقدامات خاص با نیت‌های متفاوت و ضربه و خسارات مالی زدن و اقدامات مجرمانه استفاده می‌کنند، در حقیقت از دنیای واقعی به جهان مجازی واردشده‌اند و با آگاهی کامل و شناختی که از این فضا دارند و بدون آنکه به‌راحتی مورد شناسایی مجریان قانون قرار بگیرند دست به خرابکاری بزنند.

۱-۴- جنگ سایبری

جنگ در فضای سایبری را می‌توان حمله‌های اینترنتی طراحی‌شده از سوی گروه‌ها، سازمان‌های مختلف، علیه سامانه‌ها و برنامه‌های رایانه‌ای با اهداف به‌مراتب بزرگ‌تر

مانند دستیابی به سود مالی یا آسیب جدی واردکردن به شهروندان یا دولت به‌وسیله روش‌های مجرمانه مانند کلاهبرداری، جعل، تخریب و اخلال در داده‌ها، سرقت، تضعیف یا غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی انجام می‌شود، تعریف نمود.

«عملیات جنگ اطلاعات تهاجمی، عملیاتی است که یک منبع اطلاعات خاصی را هدف و مورد بهره‌برداری قرار می‌دهد و هدفش افزایش ارزش آن برای بازیگر مهاجم و کاستن ارزش آن برای بازیگر دفاعی است. بنابراین این حالت یک موقعیت برد- باخت را برای هردو بازیکن پیش می‌آورد. فرض این است که دفاع با چنین تهمیدی موفق نیست. عملیات یک عمل خصمانه و یا حداقل بدون اجماع محسوب می‌شود منبع اطلاعات، لازم نیست که تحت مدیریت یا مالکیت دفاع باشد، هرچند که اغلب این‌گونه است» (دنینگ، ۱۳۸۳: ۳۲).

در جنگ سایبری هدف حمله‌کننده برهم ریختن ساختار اداری، خدماتی و در یک جمله می‌توان گفت تعادل کشور موردحمله از طریق فضای سایبری می‌باشد. این حملات در اشکال گوناگون خود را نمایان می‌سازد. مهاجم می‌تواند یک فرد یا یک گروه یا یک کشور باشد و در مقابل نیز فرد یا گروه یا کشور قرار دارند و به دفاع می‌پردازند، که در فضای سایبری تهاجم بسیار آسان‌تر از دفاع می‌باشد. در این فضا باید سعی نمود تا بتوان جغرافیای فضای مجازی را به نفع خود تغییر نمود.

جنگ سایبری شکل جدیدی از مبارزه در فضای مجازی می‌باشد که توسط گروه‌ها یا دول متخاصم انجام می‌شود ولی تروریسم سایبری اقدامی است که از طرف تروریست‌ها به‌صورت حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات انجام می‌گردد.

۱-۵- اخلال سایبری

اخلال سایبری به معنای ایجاد هرج‌ومرج و برهم زدن نظم و به‌عبارت‌دیگر خلل وارد ساختن در ساختار شبکه‌ای داده‌ها و ایجاد مانع در جهت دستیابی کاربر مجاز به اطلاعات و سیستم‌های رایانه‌ای و مخابراتی می‌باشد. همین اقدام سبب از کار انداختن یا مختل شدن و درنتیجه برهم خوردن یکپارچگی سامانه‌ها و شبکه‌ها خواهد شد (پاکزاد، ۱۳۹۰: ۳۸۱). اخلال در زیرساخت‌های حیاتی به‌عنوان یکی از اصول‌ترین و خشن‌ترین تهدیدات سایبری می‌باشد که می‌تواند امنیت ملی را تهدید کند. سیستم‌های رایانه‌ای در برابر حملات و تهدیدات سایبری از آسیب‌پذیری بیشتری برخوردار می‌باشند و به همین دلیل درصدد افزایش قدرت مقابله با عملکردها و حملات هستند. آسیب‌پذیری زیرساخت‌ها نسبت به حمله‌های سایبری بستگی به میزان وابستگی آن‌ها به فضای سایبر است. در کشورهای پیشرفته به علت افزایش این وابستگی امکان حمله تروریستی نیز افزایش می‌یابد.

۱-۶- خرابکاری سایبری

خرابکاری سایبری به معنای تحریف و جعل یا از بین بردن داده‌ها و اطلاعات می‌باشد. خربکاری به‌وسیله اتلاف داده‌ها یا تحریف اطلاعات صورت می‌گیرد. به‌طورکلی اتلاف داده به معنای از بین بردن، مختل کردن، تخریب، حذف داده‌ها می‌باشد که توسط رایانه و در فضای سایبری رخ می‌دهد. تخریب داده‌ها به اشکال مختلف صورت می‌گیرد گاهی نتیجه حمله فیزیکی به تأسیسات کامپیوتری و آسیب رساندن به سرویس‌دهنده‌های وب می‌باشد و گاهی نیز این اعمال از طریق و روش‌های مختلف مانند ویروس‌های کامپیوتری یا بمب‌های منطقی صورت می‌گیرد و خطرناک‌ترین موارد، برنامه‌های ویروسی می‌باشد که سبب اخلال و تخریب در داده‌ها می‌باشد. «از میان بردن داده‌ها جزو جرایم رایانه‌ای

خاص یا محض نیست؛ زیرا از میان بردن و تخریب به‌طور سنتی از قدیم وجود داشته و اکنون نسبت به داده نیز اعمال می‌شود، بنابراین نمی‌توان آن را جزو جرم‌هایی دانست که صرفاً با روی کار آمدن محیط سایبر خلق‌شده‌اند.» (فضلی، ۱۳۸۴: ۱۶۹) تخریب اطلاعات به معنای تغییر ماهیت و محتوای آن‌ها است. تحریف اطلاعات از طریق تغییر در برنامه و کنترل داده‌ها که سبب تغییر در شکل، صفحه وب می‌باشد. اختلال و تخریب در یک سیستم سبب اختلال در دیگر سیستم‌ها خواهد شد و همین امر سبب ایجاد حملات اینترنتی خواهد شد که می‌تواند امنیت ملی را تهدید کند.

ازآنجاکه در مورد تأثیر تهدیدات سایبری بر امنیت ملی نظرات و دیدگاه‌های مختلفی توسط تحلیل گران مسائل امنیتی بیان گردیده است ولی آنچه به‌طورکلی حائز اهمیت است بیان این مطلب می‌باشد که امروزه مسائل مختلفی مانند مبادلات، ارتباطات، بانکداری، تجارت الکترونیکی و غیره در فضای سایبر سبب تخریب اطلاعات و درنتیجه ایجاد چالش در حوزه امنیت شده است. پس پایان یافتن جنگ سرد نه‌تنها سبب امن‌تر شدن جهان نشده است بلکه به وجود آمدن چنین چالش‌هایی، امنیت جهانی را با تهدید مواجه ساخته است. امروزه حمله‌های مختلف مانند محوریت هک (استفاده از قوه خلاقیت در یک مسأله یا پروژه برنامه‌سازی و همچنین تغییر رفتار یک برنامه کاربردی یا یک سیستم‌عامل از طریق تغییر دستورات و نه اجرای برنامه و انتخاب گزینه‌ها) و کرک (دستیابی غیرمجاز به یک شبکه از طریق گذشتن از اقدامات امنیتی است و متضمن تفسیر و درک اطلاعات رمزگذاری شده می‌باشد.)، کرم‌ها، بمب منطقی (که سبب ایجاد خسارت، تغییر و تخریب در داده‌ها و یا برنامه‌های کامپیوتر می‌شود) جزء واقعیت‌های غیرقابل‌انکار می‌باشند. این حملات وسیع می‌تواند به‌عنوان تهدید جدی منافع ملی یک کشور را به چالش بکشاند. به طوری که کشورهای مختلف مانند ایالات‌متحده آمریکا، چین، مالزی، به برخورد فیزیکی با این حملات پرداخته‌اند و اسناد مختلفی درزمینه تأمین امنیت در فضای سایبر به تصویب رسیده است.

۲- چالش‌های پیش‌رو

۲-۱- نامعین بودن تهدیدها

امروزه مفهوم امنیت تنها محدود به دو بعد امنیت داخلی و خارجی نمی‌باشد بلکه این واژه گسترش بیشتری یافته است و دارای متغیری نسبی است. از آنجا که تهدیدات سایبری دارای گستردگی و ویژگی جهان‌شمول بودن است دیگر امروزه نمی‌توان از آن غافل شد و باید به رویکردهای متفاوت در روابط بین‌المللی اشاره شود و راهکارهای مقابله با این تهدیدات بیان شود. در مقابل رویکردهای متفاوتی نیز جهت مقابله با تهدیدات سایبری بیان گردیده است. بسیاری از دانشمندان، شرکت‌های خصوصی، نهادهای دولتی در تلاش جهت ارائه راهکارهای مناسب برای ایمن‌سازی سیستم‌های رایانه‌ای ارائه کرده‌اند. در رویکرد نخست بیشتر سعی در «پیشگیری وضعی» و ارائه راهکاری فنی در جهت مبارزه با حملات است. براین اساس در مواردی نظیر حفظ امنیت و محرمانگی اطلاعات بر عهدهٔ صنعت مربوطه است و علاوه بر استفاده از راه‌کارهای فنی همچون استفاده از نرم‌افزارهای ضدویروس و ضداختلال، با وضع مقرارت لازم جهت برخورد با حملات و خطرات این فضا و تهدیدات آن گام برداشته شود. در رویکرد دوم فرهنگ‌سازی و آموزش مبارزه با برنامه‌های مخرب و حملات رایانه‌ای به کاربران موردتوجه قرار می‌گیرد تا کاربران کمتر مورد حملات خطرناک اینترنتی قرار گیرند (فضلی،۱۳۸۳: ۱۹۵). همان‌طور که مرزهای فیزیکی کشورها درخطر حملات مختلف می‌باشند، مرزهای سایبری و مجازی بسیار پرنفوذتر هستند که می‌توانند زیرساخت‌های حیاتی کشورها مخصوصاً زیرساخت اقتصادی

هر کشوری را هدف حمله قرار دهند و بر امنیت ملی تأثیر بگذارند.

امروزه جهان وارد عرصه جدیدی از مبادله اطلاعات درزمینه تجارت، اقتصاد، بازرگانی و غیره شده است که هرگونه تحول در مفهوم قدرت سبب تغییر و تحول در مفهوم امنیت خواهد شد. دانشمندان علم سیاست بین دو مفهوم قدرت و امنیت وابستگی می‌دانند و معتقدند که تغییر در مفهوم قدرت سبب تغییر در مفهوم امنیت خواهد شد. بر همین اساس، منابع قدرت در حال تغییرند. در سده هجدهم، سرزمین، جمعیت و کشاورزی منبع قدرت تعیین‌کننده بود. در سده نوزدهم، ظرفیت صنعتی، در میانه سده بیستم نیز علم و به‌ویژه فیزیک هسته‌ای، منابع قدرت تعیین‌کننده‌ای در اختیار قدرت‌ها قرار داده بود. در سده حاضر، توانایی اطلاعاتی در تعریف وسیع خود، احتمالاً تعیین‌کننده‌ترین منبع قدرت است. (خلیلی پور، ۱۳۹۱: ۱۸۱) امروزه اینترنت ارتباط نامحدود بین افراد با یکدیگر در سطح گسترده‌ای به وجود آورده است و سبب افزایش قدرت کنترل بر اطلاعات شده است. افراد می‌توانند سریعاً و با صرف هزینه اندک به پیام‌های اینترنتی دسترسی پیدا کنند. همین امر باعث ایجاد چالش در کنترل جریان اطلاعات توسط حکومت‌ها شده است. بنابراین تحولاتی که در سطح جهانی در زمینه تکنولوژی ارتباطات و فناوری آن به وجود آمده است، سبب ایجاد تحول و دگرگونی در منابع قدرت شده است همان‌گونه که بیان شد تحول در قدرت سبب تحول در امنیت خواهد شد زیرا این دو به یکدیگر وابسته هستند و بر یکدیگر تأثیر مستقیم خواهند گذاشت، همین امر موجب شده که هرگونه چالش و تهدید در منابع قدرت سبب ایجاد اختلال در امنیت کشور شود.

بسیاری از دانشمندان سیاسی امنیت را در عصر اطلاعات یکی از مهم‌ترین عواملی می‌دانند که گریبان‌گیر دولت‌ها شده است. زیرا دریک نظام سیاسی، وظیفه دولت تأمین امنیت ملی می‌باشد. تأمین امنیت ملی به مفهوم ایجاد امنیت برای تمامی افراد ملت می‌باشد. از کاربرد اصطلاح «امنیت اطلاعات» بیش از دو دهه نمی‌گذرد. امروزه امنیت و حفاظت از اطلاعات یکی از مهم‌ترین بخش‌هایی است که قدرت دولت‌ها را نشان می‌دهد. زیرا با افزایش استفاده از اینترنت و تکنولوژی ارتباطات و انقلابی که در جوامع بشری به وجود آمده است جرایم مختلفی در زمینه‌های مختلف زندگی بشری ازجمله بانکداری، تجارت الکترونیک، کلاهبرداری سایبری، جاسوسی سایبری، جعل، سرقت سایبری سبب تهدید امنیت ملی و افزایش روزافزون این‌گونه جرایم شده است. پس هدف از ایجاد امنیت سایبری دریک کشور محافظت از سیستم‌ها و ساختارهای اطلاعاتی یک کشور و جلوگیری از افشای اطلاعاتی است که می‌تواند به تمامیت ارضی یک سرزمین آسیب جدی وارد سازد. (دنینگ، ۱۳۸۳: ۴۵) به وجود آمدن چالش در امنیت سایبری یکی از مسائل مهم و پیچیده می‌باشد، از آنجا که تهدیدات سایبری تنها به‌عنوان خطری برای دولت‌ها محسوب نمی‌شود بلکه به‌عنوان تهدید جدی برای افراد و سازمان‌های خصوصی نیز هست باید سعی در رسیدن به امنیتی در این زمینه نمود. دررسیدن به چنین امنیتی نیاز به برنامه‌ریزی اصولی و مهم تنها از طرف دولت‌ها نمی‌باشد بلکه در این زمینه باید ارگان‌های مختلف، سازمان‌ها، افراد و گروه‌های جامعه، بخش خصوصی به همکاری با دولت بپردازند (باستانی، ۱۳۸۳: ۳۲۹). در روابط بین‌الملل نیز جامعه جهانی سعی در ارائه راه‌کارهایی جهت حمایت از امنیت سیستم‌ها و همکاری بین دولت‌ها در این زمینه نموده است.

امروز در بسیاری موارد منبع تهدید امنیت دولت‌ها مشخص نیست (افضلی، ۱۳۸۷: ۱۲۳). همین امر امنیت در پرتو فضای سایبر دستخوش ناامنی شده و تأمین امنیت با چالش‌هایی مواجه شده است. در دهه ۸۰ و به‌خصوص دهه ۹۰ ایران با

شاکله امنیتی جدیدی روبه‌رو شد که رویه‌های سرعت، نسبیت، عدم قطعیت و بهره‌گیری از فضای مجازی در آن وجود دارد. امنیت پسامدرن به‌خصوص در میان نوجوانان، جوانان و نسل جدید که اغلب تحصیل‌کرده، بیکار و آشنا به تکنولوژی‌های روز جامعه می‌باشند، به‌خوبی مشاهده می‌شود. جهانی‌شدن و کاهش قدرت دولت‌ها بااینکه ایران دارای فرهنگ مذهبی و دولت نفتی می‌باشد نیز تأثیر گذاشته است و به ناگاه جامعه وارد عصر اطلاعات گردید. بمباران اطلاعات در قالب تکنولوژی‌های جدید باعث شده است که سبک نگاه ایرانیان نیز همانند سایر شهروندان با ۱۵ سال عقب‌ماندگی تغییر بنیادین داشته باشد. فرهنگ پسامدرن اقلیت‌ها و حاشیه‌ها را به مرکز کشانده است، قدرت را بیشتر به‌صورت نرم و مجازی در جریان انداخته و باعث شده که اعمال و محدود کردن قدرت، سبکی مجازی و سایبری پیدا کند (کلهر، ۱۳۸۸: ۲۶۱).

۲-۲- حملات سایبری

حملات سایبری که می‌توانند به جمعیت کثیری لطمه وارد سازند، شامل تراکم بسته‌ای محرومیت از خدمات، بهره‌برداری از مؤلفه‌های زیرساختی و تخریب سیستم‌های ارباب‌رجوع با شبکه‌های رباتی گسترده هستند. تراکم بسته‌ای محرومیت از خدمات، سرورهای وب شرکت‌ها و سازمان‌های مختلف اغلب از سوی مشتریان ناراضی، مخالفان سیاسی یا سایرین مورد حملات تراکم پست‌های قرار می‌گیرند. برخی آسیب‌پذیری‌های نرم‌افزاری به فرد مهاجم اجازه می‌دهند تا ماشین مقصد را دچار خرابی و آسیب وارد کند که این خود منجر به ازکارافتادن خدمات می‌شود، یا سیستم با خطراتی مواجه شود که به‌واسطه آن فرد مهاجم بتواند کنترل مدیریتی ماشین و تبادلات فعالیت‌های ایمنی معمول را در دست بگیرد (مؤذن‌زاده جامی، ۱۳۸۵: ۲۵۱). فرد مهاجم می‌تواند به‌سادگی سیستم را از کار بیندازد (خاموش کند) و یا از آن برای اجرای حملات به‌مراتب مخرب‌تر استفاده نماید. مهاجمان با به دست گرفتن کنترل مؤلفه‌های زیرساختی حساس مانند ردیاب‌ها یا سرورهای سیستم نام دامنه می‌توانند ترافیک را به مقاصد دیگر بر روی اینترنت هدایت نمایند به‌طوری‌که به‌عنوان‌مثال تمام ترافیک که برای بانک‌های یک کشور مفروض انتخاب‌شده‌اند به کشور دیگر منتقل شوند. به مخاطره انداختن سیستم به مهاجم اجازه می‌دهد تا ترافیکی که از طریق اینترنت مبادله می‌شود مانند مبادلات مالی حساس، داده‌های مدیریت مرتبط با خود زیرساخت یا ارتباطات تجاری را که برای تجزیه‌وتحلیل و کاربردهای بعدی ثبت می‌شوند تحت کنترل خود درآورد. برای شروع یک حمله در مقیاس بزرگ که مستلزم بهره‌برداری از سیستم‌های زیرساختی حساس می‌باشد. مهاجمان می‌بایست قبل از فروشندگان محصولات یا محققان امنیتی مصمم اقدام به یافتن نکات ضعف یا آسیب‌پذیری‌ها نمایند.

شکل‌گیری مصادیقی چون فیشینگ و فارمینگ، آینده امنیت را با چالش مواجه ساخته است. فیشینگ در انجام اهداف غیرقانونی توسط سازمان‌های جنایی کاربرد بسیاری دارد. تحریف و سوءاستفاده از نام شرکت‌ها، بانک‌ها و نهادهای معتبر یک تکنیک رایج است که برای به دست آوردن اطلاعات شخصی و مالی کاربران ناآگاه از آن استفاده می‌شود. این جرم ارتباط زیادی با کارت‌های اعتباری و همچنین دیگر اطلاعات مالی چون جزییات حساب‌های بانکی دارد که توسط مجرمان به‌صورت متقلبانه مورداستفاده قرار می‌گیرد. مخاطبین و گیرندگان ایمیل‌های فریب‌کارانه معمولاً بعد از مدتی طولانی متوجه کلاهبرداری می‌شوند که کار از کار گذشته و یک آسیب جبران‌ناپذیر به آن‌ها واردشده است.

فارمینگ یکی دیگر از گونه‌های خطرناک مهندسی اجتماعی که بسیار شبیه فیشینگ است. فارمینگ با دست‌کاری در

آدرس دامنه‌ها باعث هدایت کاربر به یک سایت جعلی و قلابی می‌شود. تأثیر این جرم بر کاربر بسیار زیاد است، زیرا قسمت سایت‌های دلخواه در مرورگر تغییر می‌یابد و حاوی اطلاعات جعلی می‌شود هنگامی‌که یک مشتری ناآگاه قصد دارد از طریق میانبر موجود در این قسمت به‌حساب بانکی آنلاین خود متصل شود به یک سایت جعلی که توسط کلاهبردار مدیریت‌شده هدایت می‌گردد. ممکن است علاوه بر این، تله‌های دیگری که باعث صدمه و ضرر رسانی به کامپیوتر قربانی شود در اینجا کار گذاشته شود. (شاه‌بند زاده و یوسفی ده بیدی، ۱۳۹۱: ۴۱۵)

اسمیشینگ از دیگر جرایم و تهدیدهای جدید علیه امنیت است. در این جریم، مجرمین تلفن‌های همراه متصل به اینترنت را مورد هدف قرار می‌دهد در این شیوه کاربران لینک یک وب‌سایت را دریافت می‌کنند به‌محض کلیک بر آن‌یک تروجان شروع به فعالیت می‌کند که عواقب آن در خصوص محتویات تلفن‌های همراه قابل پیش‌بینی نیست (عالی پور هفشجانی، ۱۳۷۰: ۱۵). می‌توان به گروه‌های ویروس‌های رایانه‌ای نیز اشاره کرد. دسته ویروس‌های رایانه‌ای (شامل ویروس‌ها، کرم‌ها، نرم‌افزارهای جاسوسی و ...) در حقیقت نرم‌افزارهایی هستند که باهدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند و معمولاً از طریق یک دیسک و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند، بعضی ویروس‌ها ممکن است قادر به حمله به فایل سیستم و ذوب کردن مادر بورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت و از کار انداختن رایانه باشند و مثلاً عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیسی که می‌توانند دیسک سخت یک رایانه را ذوب کنند. نوشتن ویروس رایانه‌ای در همه جای دنیا یک جرم است به گونه‌ای که نویسنده ویروس در برابر تمام خسارات‌های وارده به همه رایانه‌های آلوده مسؤول است.

در مواجه با چالش‌های مورد اشاره لازم است پیشگیری‌کیفری و غیرکیفری مورد توجه قرار گیرد. زمانی که افراد در شبکه‌های اجتماعی هک شوند، گاه پیام نیز برای آن‌ها ارسال می‌شود و این موضوع نوعی هشدار است که از قرار دادن مطالب حساس و مهم در این شبکه‌ها خودداری نموده و از سوءاستفاده احتمالی مجرمین سایبری علیه افراد و امنیت ملی پیشگیری شود (ولیدی، ۱۳۷۸: ۲۹۹). گاها بی‌ثبات‌سازی امنیت از طریق اهدافی چون جمع‌آوری اطلاعات، جریان‌سازی و جنگ روانی علیه نظام جمهوری اسلامی ایران، تأسیس سایت‌های مبتذل، حمایت خبری و رسانه‌ای از گروهک‌های تروریستی، اقدامات ایذایی و هکری و نفوذ به سرورهای دولتی، برنامه‌ریزی برای اخلال در سیستم مدیریت شهری ازجمله سامانه سوخت‌رسانی و تهییج و تشویق به تجمعات غیرقانونی را دنبال می‌کرد (وزیری، ۱۳۹۰: ۱۵۵). در حوزه پیشگیری وضعی و غیرکیفری هدف سلب فرصت و ابزار ارتکاب جرم از مجرم باانگیزه است. به ویژه که در سال‌های اخیر تخلیه بانک‌های اطلاعاتی کشور، نفوذ و خرابکاری در سایت‌های اینترنتی ایران روند فزاینده‌ای به خود گرفته است لازم است مواجه با چالش‌های مورد اشاره با رویکرد پیشگیرانه مد نظر قرار گیرد.

نتیجه‌گیری

نتایج نشان داد در کنار جرایمی چون محاربه و فساد فی الارض، تهدید به بمب گذاری و تبلیغ علیه نظام جمهوری اسلامی ایران، شاهد شکل‌گیری نوع جدیدی از تهدیدها و جرایم سایبری هستیم که چالش‌های امنیت در آینده هستند. فضای سایبری به‌عنوان یکی از مهم‌ترین منابع قدرت در عصر جدید می‌باشد. این فضا با ویژگی‌های منحصربه‌فرد خود سبب شکل‌گیری جرایم مختلفی و به وجود آمدن مجرمین سایبری گردیده است که به‌راحتی می‌توانند امنیت جامعه را مختل سازند. تکنولوژی‌های جدید اطلاعات موجب

جلب بزهکاران فراوانی به این فضا می‌باشد از این فضا می‌توان به‌عنوان محیطی جهت انجام اقدامات تروریست‌ها بر ضد داده‌ها نام برد. تهدیدات سایبری به‌عنوان یکی از مسائل مهم و انکارناپذیر در حوزه سیاست جنایی دولت‌ها می‌باشد. از آنجا که تکنولوژی‌های کامپیوتر و اینترنت سبب تغییر ماهیت جرایم از شیوه‌های کلاسیک به نسل جدیدی از آن با عنوان داده‌ها و اطلاعات می‌باشد دیگر قوانین کلاسیک در حقوق کشورها کافی نبوده و نیاز به وضع قوانین جدید در این خصوص است. امنیت اطلاعات می‌تواند افشاء اطلاعات سری و محرمانه باشد که سبب ضربه زدن به امنیت ملی می‌شود. تأمین امنیت و حفاظت از اطلاعات یکی از مهم‌ترین بخشی‌هایی است که قدرت دولت‌ها را نشان می‌دهد. امنیت سایبری محافظت از سیستم‌ها و ساختارهای اطلاعاتی یک کشور می‌باشد که جهت مهار و مقابله با این‌گونه تهدیدات تلاش دولت‌ها به‌تنهایی کافی به نظر نمی‌رسد و نیاز به همکاری مؤثر بین دولت‌ها و افراد می‌باشد. با توجه به گستردگی و اهمیت جرایم سایبری و از نظر اینکه این‌گونه جرایم ماهیتی کاملاً جدید در حوزه حقوق کیفری دارند باید تدوین قوانین و تعقیب مجرمین سایبری اهمیت بسیاری را داشته باشد. قوانین وضع‌شده توسط قانون‌گذار در زمینه جرایم سایبری ازآنجاکه مربوط به سال ۱۳۸۸ می‌باشد بهتر می‌بود که در مجازات‌های نقدی که در نظر گرفته‌شده است تجدیدنظر صورت گرفته و مقدار آن افزایش می‌یافت. در زمینه تهدیدات مرتبط با جرایم سایبری ازآنجاکه این تهدیدات در ذیل جرایم سایبری به شمار می‌آیند این به معنای حذف عنوان آن‌ها نمی‌باشد و این‌گونه تهدیدات در قانون جرایم رایانه‌ای کم‌رنگ جلوه داده‌شده است باید در این مورد نیز توجه بیشتری توسط قانون‌گذار صورت بگیرد. جرایم امنیتی که در فضای سایبر ارتکاب می‌یابد، جدیدترین و پیچیده‌ترین تهدید علیه زندگی بشر به شمار می‌آید. در این فضا تهدیدها حساس‌تر و حصار امنیت ملی شکننده‌تر می‌شود، زیرا فضای سایبر پدیده بسیطی نیست تا به‌راحتی در مسیر موافق با امنیت ملی قرار گیرد. فضای سایبر تهدیدات جدیدی چون جاسوسی رایانه‌ای، تروریسم سایبری و اخلال در سیستم‌های نهادها و سازمان‌های حساس به وجود آورده که به‌راحتی و در زمان اندک می‌توانند امنیت یک کشور را با تهدید جدی مواجه سازند.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نویسندگان مقاله به صورت مشترک مقاله را نگارش کرده و مسؤولیت ارائه مطالب بر عهده نویسنده مسؤول مقاله می‌باشد.

تشکر و قدردانی: در پایان لازم می‌دانم از اساتید، منتقدان و دوستانی که باعث غنی‌ترشدن محتوای مقاله حاضر شده‌اند، تقدیر و تشکر نمایم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

منابع و مآخذ

– آشوری، محمد (۱۳۹۲). *آیین دادرسی کیفری*. چاپ چهارم، تهران: سم.

– آشوری، محمد (۱۳۹۲). *عدالت کیفری (مجموعه مقالات)*. چاپ دوم، تهران: دادگستر.

– افضلی، مهدی (۱۳۸۷). «جنگ در عصر اطلاعات، تهران». *نشریه اطلاع‌رسانی*، ۱۹: ۱۲۳.

– افضلی، مهدی (۱۳۹۲)، *مسؤولیت کیفری در فضای سایبر*. چاپ اول، تهران: انتشارات خرسندی.

– الهی‌منش، محمدرضا و مرادی‌اوجقاز، محسن (۱۳۹۴). *جرایم علیه امنیت و آسایش عمومی*. چاپ ششم، تهران: انتشارات مجد.

– باستانی، برومند (۱۳۸۳). *جرایم کامپیوتری و اینترنتی جلوهای نوین از بزهکاری*. چاپ اول، تهران: بهنامی.

– پاکزاد، بتول (۱۳۹۰). *جرایم‌کامپیوتری*. پایان‌نامه کارشناسی ارشد، تهران: دانشگاه شهید بهشتی.

– تحیری، فرزاد (۱۳۸۴). *دسترسی غیرمجاز به سیستم‌های رایانه‌ای در حقوق ایران و اسناد بین‌المللی*. پایان‌نامهٔ کارشناسی ارشد، قم: دانشگاه مفید.

– جلالی فراهانی، امیرحسین (۱۳۸۹). *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. چاپ اول، تهران: انتشارات خرسندی.

– حسن بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*. چاپ اول، تهران: موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

– خلیلی پور رکن‌آبادی، علی و نورعلی وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تأثیر آن بر امنیت ملی». *فصلنامه مطالعات راهبردی*، ۱۵(۲): ۱۶۷– ۱۹۶.

– دزیانی، محمدحسن (۱۳۸۵). «درآمدی بر سیاست جنایی جرایم سایبری». *ماهنامه قضاوت*، ۳۹: ۵۳ – ۵۱

– دنینگ، دی‌ای (۱۳۸۳). *جنگ اطلاعات و امنیت*. چاپ اول، تهران: مؤسسه فرهنگی هنری پردازش هوشمند علائم.

– راوندی، مرتضی (۱۳۶۸). *سیر قانون و دادگستری در ایران*. چاپ اول، تهران: نشر سرچشمه.

– رهامی، محسن و پرویزی، سیروس (۱۳۹۱). «جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن». *فصلنامه حقوق*، ۴۲(۳): ۱۷۷– ۱۹۶.

– شاه‌بند زاده؛ سعید و یوسفی ده بیدی؛ شهلا (۱۳۹۱). «مقاله تعیین درجه اهمیت جرایم رایانه‌ای از دیدگاه صاحب‌نظران انتظامی بوشهر». *فصلنامه نظم و امنیت انتظامی*، ۵(۱): ۱۳۷– ۱۵۶.

– شمس، عبدالله (۱۳۸۸). *آیین دادرسی مدنی دوره بنیادین*. چاپ سوم، تهران: انتشارات دراک.

– صانعی، پرویز (۱۳۷۲). *حقوق جزای عمومی*. چاپ پنجم، تهران: گنج دانش.

– عالی پور هفشجانی، خداداد (۱۳۹۰). نقش پلیس در ارتباط با جرایم سایبری. پایان‌نامه کارشناسی ارشد، تهران: دانشگاه پیام نور.

– عبدالله خانی، علی (۱۳۸۱). نظریه‌های امنیت. چاپ اول، تهران: موسسه فرهنگی مطالعات بین‌المللی ابرار معاصر.

– فضلی، مهدی (۱۳۸۳). مسؤولیت کیفری در فضای سایبر. چاپ اول، تهران: انتشارات خرسندی.

– فضلی، مهدی (۱۳۸۴). مسؤولیت کیفری در فضای سایبر. چاپ دوم، تهران: انتشارات خرسندی.

– کلهر، علی (۱۳۸۸). *نقش نظارت تعقیبی و پیشگیرانه در رابطه با آزادی مطبوعات در نظام حقوقی ایران*. تهران: دانشگاه آزاد تهران مرکز.

– کوشکی، غلام حسن (۱۳۹۲). *بررسی مهم‌ترین نوآوری‌های «حمایتی» و «سازمانی» قانون آیین دادرسی کیفری در مرحله تحقیقات مقدماتی دایره المعارف علوم جنائی (مجموعه مقالات)*. چاپ اول، تهران: نشر میزان.

– مجیدی، محمود (۱۳۸۶). *حقوق کیفری اختصاصی (جرایم علیه امنیت)*. چاپ دوم، تهران: میزان.

– محبی، جلیل و ریاضت، زینب، (۱۳۹۵). «مبانی و مدل کیفرگذاری تعزیری (مطالعه موردی در جرایم علیه امنیت)». *فصلنامه آفاق امنیت*،۳: ۳۳–۶۲.

– محمودی، محمد؛ میرخلیلی، سید محمود و بخنوه، کریم (۱۳۹۸). «جرایم علیه امنیت و حقوق شهروندی در پرتو اصول جرم‌انگاری». *تحقیقات حقوق بین‌المللی*، ۴۳ :۲۱۳–۲۳۸

– مؤذن‌زاده جامی، محمدهادی (۱۳۸۵). *مقدمه‌ای بر امنیت و مؤلفه‌های آن*. چاپ اول، تهران: مرکز تحقیقات کامپیوتری اسلامی.

– میر محمدصادقی، حسین (۱۳۹۲). *جرایم علیه امنیت و آسایش عمومی*. چاپ بیست و یکم، تهران: نشر میزان.

– وزیری، علیرضا (۱۳۹۰). «بررسی جنگ نرم استکبار علیه جمهوری اسلامی». *نشریه مبلغان*، ۱۴۶: ۱۵۵.

– ولیدی، محمد صالح (۱۳۷۸). «بررسی و نبین نظم و امنیت و آسایش عمومی و فردی». *مجله نیروی انتظامی*،۱(۲): ۵۰–۶۵.