نشریه علمی سیاست دفاعی

# حاکمیت حقوقی دولت‌ها بر فضای مجازی و تأثیر آن بر امنیت ملی

ابوالفضل پاسبان[1]

۱۲۵
سال سی و دوم
زمستان ۱۴۰۲
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۱/۰۲/۲۶
تاریخ پذیرش:
۱۴۰۲/۰۳/۱۳
صص: ۴۸-۱۱
شاپا چاپی: ۵۰۸۷-۱۰۲۵
الکترونیکی: ۴۹۷۱-۲۶۵۴

## چکیده

امروزه فضای مجازی به‌عنوان ستون فقرات فناوری‌های نوین اطلاعاتی و ارتباطی، در شکل‌گیری و ظهور فضاهای جدید اقتصادی، فرهنگی، اجتماعی، سیاسی و امنیتی نقش اساسی دارد. اکنون مسئله‌ی کنترل و حاکمیت حقوقی دولت به‌عنوان سردمدار جامعه بر فضای مجازی و همچنین تأثیرات سوء مدیریت آن، بر امنیت ملی از دغدغه‌های اصلی قانونگذار در کشور می‌باشد. پژوهش حاضر باهدف بررسی حاکمیت حقوقی دولت بر فضای مجازی و تأثیر آن بر امنیت ملی انجام گردیده است. نتایج بررسی نشان می‌دهد، چنانچه در حوزه قانونگذاری فضای مجازی، قوانین بازدارنده پیش‌بینی نگردد، می‌تواند در حوزه امنیت ملی دارای اثرات مخرب و جدی باشد. سیاست‌گذاری جزیره‌ای، ضعف در قانون‌گذاری و سوءاستفاده از خلأهای قانونی، در قوانین مربوط به فضای مجازی در جمهوری اسلامی ایران، می‌تواند در برخی از موارد موجب آسیب‌پذیری حوزه امنیت داخلی و بعضاً امنیت ملی گردد. هم‌اکنون برخی از شبکه‌های اجتماعی در فضای مجازی به طور جدی در جهت تخریب و القای ناکارآمدی نظام ج.ا.ا.، مشروعیت زدایی ساختاری از نظام سیاسی، تضعیف انسجام ملی، شکاف و تقابل بین جامعه و حاکمیت و تضعیف باورهای ملی فعالیت و در حوزه‌ی امنیتی نیز با اقدامات جاسوسی، پایش اطلاعات کاربران، مهیاسازی ابزار ارتباطی برای گروه‌های براندازی، جمع‌آوری اطلاعات افراد و مشاغل خاص، آموزش‌های مخرب به افراد و انتقال اطلاعات طبقه‌بندی در جهت مخدوش‌سازی امنیت ملی فعالیت می‌کنند. تأسیس ساختاری قدرتمند و فرا قوه‌ای مبتنی بر الزامات حقوقی برای سیاست‌گذاری، قانون‌گذاری، جرم‌انگاری و همچنین ساماندهی فضای مجازی در کشور و راه‌اندازی شبکه ملی اطلاعات می‌تواند در رفع بسیاری از مشکلات در این حوزه مؤثر باشد.

کلیدواژه‌ها: حاکمیت حقوقی فضای مجازی، فناوری‌های ارتباطی، امنیت ملی، قانون‌گذاری

DOR: 20.1001.1.10255087.1402.32.125.1.3

۱. نویسنده مسئول: دانشجوی دکتری، پژوهشکده دفاعی امنیتی، دافوس، دانشگاه جامع امام حسین(ع)، تهران، ایران
halmataha110@gmail.com

## مقدمه

فضای مجازی و بالطبع آن شبکه‌های اجتماعی به عنوان یک بستر رسانه‌ایی با داشتن خصائصی همچون سرعت بالای انتقال و سهولت دسترسی، امروز در جهان به یکی از تأثیرگذارترین ابزار تبدیل و از قدرت تأثیرگذاری بالایی بر جنبه‌های مختلف زندگی بشری برخوردار می‌باشد. فضای‌مجازی علاوه بر اینکه قدرت تاثیرگذاری مثبت در باورها، ارزش‌ها، اعتقادات، ادراکات و ذهنیات جامعه را دارا می‌باشد؛ می‌تواند بستر رشد اعتراض‌های اجتماعی را فراهم و لایه‌های مختلف جامعه را به مخالفت با قالب‌های فرهنگی و اجتماعی نظام سیاسی حاکم وادار، یا چنان تصویری از ساختار قدرت به مردم ارائه نمایدکه باعث ایجاد شکاف بین آن‌ها با مردم گردد و پذیرش حکومت توسط مردم را با چالش مواجه کنند. با چنین ویژگی‌هایی، فضای مجازی می‌تواند، کارکرد امنیتی پیدا کرده و توانایی تاثیرگذاری بر امنیت ملی کشورها را دارا باشد و به صورت مستقیم بر محیط امنیتی تاثیرگذاری نماید. اکنون شواهد و قرائن متعددی درخصوص ماهیت خرابکارانه و براندازانه‌ی فضای مجازی درسطح جهان به خصوص در کشورهای در حال توسعه ازجمله جمهوری اسلامی ایران وجود دارد، که یکی از عوامل آن ضعف در اقدامات کنترلی و زیرساخت‌های حقوقی و قانونی مبتنی بر الزامات زمان و مکان می‌باشد. باتوجه به آثار فراگیر فضای مجازی در ابعاد مختلف زندگی بشری، لزوم و ضرورت ایجاد کنترل‌های قانونی و حقوقی کارا، قانونگذاری و جرم‌انگاری و همچنین ایجاد بستر مدیریتی هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از فضای مجازی در جهت پیشرفت همه جانبه‌ی کشور و ارائه خدمات گسترده و به حداقل رساندن تهدیدهای امنیتی و آسیب‌پذیری‌های ناشی از این فضا، اجتناب‌ناپذیر بوده و اقتضا می‌نمایدکه مسئولین امر در راستای این مهم نسبت به بررسی همه جانبه ی امر اقدام و اقدامات حقوقی سازنده را به منظور استفاده حداکثری و مثبت و همچنین جلوگیری از فعالیت‌های مخرب دشمنان و آسیب رساندن به حوزه امنیت ملی از بستر این فضا، که می‌تواند با قانونگذاری و یا رفع خلأهای احتمالی در قوانین موجود رفع گردد، اقدام لازم را مبذول دارند. با عنایت به اهمیت مسئله، بررسی حاکمیت حقوقی دولت بر فضای مجازی و تأثیر بر امنیت ملی هدف اصلی این تحقیق بوده که در قالب سئوال اصلی، «حکمرانی دولت بر فضای مجازی چگونه است؟ و چه تأثیری بر امنیت ملی دارد؟»، مطرح شده است.

## ادبیات و مبانی نظری

### دولت و حکمرانی در فضای مجازی

دولت، به مجموعه‌ای که انحصار استفاده مشروع از خشونت فیزیکی و خشونت نمادین را بر یک سرزمین معین و روی مجموعه‌ی جمعیت متعلق به آن، با موفقیت اعمال می‌کند، اطلاق می‌شود. در این تعبیر اگر دولت یک راهکار اعمال خشونت نمادین است، بدین دلیل است که دولت در دو قالب متجسد می‌شود؛ نخست در عینیت (ساختارهای سیاسی و اجتماعی) و دیگر در ذهنیت، یعنی درک و اندیشه افراد. دولت‌ها از طریق مجاری نرم مختلفی همچون رسانه‌ها، فضای مجازی، مدارس، مساجد، نهادها و چارچوب‌های قانونی و نظام آموزشی سعی در گسترش و تداوم نظام ارزشی و فرهنگی و بازتولید مناسبات سیاسی و اجتماعی مستقر دارند. دولت‌ها همواره و به طور مداوم در تلاش تولید و بازتولید هژمونی خود در عرصه‌ی سیاست هستند (آرزمی و همکاران،۱۳۹۷: ۴)، دولت گاهی مستقیماً از زور و سرکوب وگاهی به شیوه‌ی غیرمستقیم و نرم، یعنی از طریق نظام ایدئولوژیکی دولتی به بازتولید نظام حاکم می‌پردازد. آلتوسر وسایل ارتباطات جمعی را جزء دستگاه‌های ایدئولوژیک دولت سرمایه‌داری می‌داند که نقش مهمی در بازتولید قدرت به شیوه نرم آن و گرایش به رفتار و فکر کردن در شیوه‌های مقبول اجتماعی دارد. (فیسک، ۱۳۸۱: ۳۷)

حکمرانی[1] بیان شیوه و حالت حکومت کردن است. حکومت و دولت[2] ابزار و نتیجه حکومت کردن را ترسیم می‌کنند. حکمرانی به

مجموعه‌ایی از فرآیندها اشاره دارد که با قدرت، اقتدار و نفوذ، سیاست‌ها و رویه‌هایی را برای حکومت کردن در دست می‌گیرد. وادی حکمرانی(حاکمیت) وادی هدایت و کنترل است و با خلق و بازتولید قوانین، هنجارهای اجتماعی و ساختاریافته در ارتباط است. روی دیگر حکمرانی، قدرت، نفوذ و اقتدار است. قدرت ملی به عنوانی مفهومی ژئوپلتیکی، صفت جمعی افراد یک ملت یا ویژگی کلی یک کشور را منعکس می‌کند که برآیند توانایی‌ها و مقدورات آن کشور محسوب می‌شود.(حافظ‌نیا و دیگران، ۱۳۸۲: ۵۱)، حکمرانی در واقع قدرت برتری است که در حیطه دولت کشور، اراده‌ایی فراتر از آن وجود ندارد، به گونه‌ایی که در مقابل اعمال اراده و

1. Governance
2. Government

اجرای اقتدارش مانعی نمی‌پذیرد و از هیچ قدرت دیگری تبعیت نمی‌کند. حکمرانی با ساختارهای اقتصادی، فرهنگی و سیاسی، اعمال قدرت پیدا کرده و دروندداد و بروندداد ساختارهای اداره کشور، جریان اطلاعات و دانش راهبردی در حرکت جامعه و ملت را شکل می‌دهد. این اقتدار درونی و هویت ملی و مشترک با گسترش فضای مجازی در حال به چالش کشیدن شدن است.(کیان خواه، ۱۳۹۷: ۱۵۸)

حکمرانی در فضای مجازی از چهارلایه‌ی «زیرساخت»، «لایه‌ی منطقی»، «لایه‌ی محتوا»، «لایه‌ی اجتماع» تشکیل شده است. در حال حاضر

لایه‌ی زیرساخت تحت سلطه آمریکا است. در لایه‌ی منطقی سازمان‌هایی مانند آیکن فعال هستند و در لایه‌ی محتوا شرکت‌هایی مانند اپل و مایکروسافت و ... مشغول فعالیت می‌باشند. به نظر می‌رسد در لایه‌ی زیرساخت، قدرت مانور جمهوری اسلامی ایران کمتر از سایر کشورها است، اما در سه لایه دیگر یعنی لایه‌ی منطقی، محتوا و اجتماع می‌تواند فرصت خوبی برای اعمال اراده کشور و توسعه حکمرانی ایران باشد. در حوزه‌ی فضای مجازی مدل‌های متفاوتی از قدرت وجود دارند که عبارتند از: «قدرت فرهنگی- رسانه‌ای»، «قدرت بازدارندگی»، «قدرت سخت- نظامی»،«قدرت هژمونیک» و «قدرت اطلاعاتی». در حوزه‌ی فرهنگی- رسانه‌ای، شبکه‌های اجتماعی به عنوان ابزار قدرت مطرح می‌شوند. در حوزه‌ی بازدارندگی، قدرت ایجاد اختلال شدید در سامانه‌ها و زیرساخت‌های مجازی می‌تواند به عنوان ابزار قدرت سایبری در نظر گرفته شود. در حوزه‌ی سخت و نظامی نیز اقداماتی از جمله حملات سایبری مانند استاکسنت به نوعی ابزار قدرت است. از جنبه اطلاعاتی دسترسی به داده و تحلیل داده، یکی از مهم‌ترین منابع قدرت است. حکمرانی خوب در مدیریت فضای مجازی محصول مشارکت و اجماع سه نهاد دولت، جامعه مدنی و بخش خصوصی است و این امر در فضای اعتماد متقابل شکل می‌گیرد. (مرکز بررسی‌های استراتژیک ریاست جمهوری، ۱۳۹۹: ۲)

## حاکمیت دولت‌ها؛ حفظ امنیت یا نقض آزادی در فضای مجازی

دولت‌ها می‌توانند به‌عنوان یک ناقض بزرگ حریم خصوصی در فضای مجازی شناخته شوند. دلیل این موضوع در وقایعی است که در حملات تروریستی صورت گرفته و خصوصاً پس از

حادثه یازدهم سپتامبر آمریکا نهفته است. در این وقایع دولت آمریکا (و پس‌ازآن بیشتر دولت‌های جهان) به این نتیجه رسیدند که در دوگانه‌ی حریم خصوصی و امنیت، باید طرف امنیت را بگیرند. حاصل این نظریه بعداً در قالب شنود تلفن‌های شهروندان آمریکایی و متعاقباً در شنود تلفن‌های سران کشورها و مقررات سخت‌گیرانه در خصوص مهاجرت و مسافرت به امریکا دیده شد. قوانینی در این زمینه‌ها تصویب شد، توسط اکثر کشورها مورد الگوبرداری قرارگرفته است. بدبینی و فضایی ایجادشده، موجب گردیده، دولت‌ها با توجیه برقراری امنیت و نظم عمومی، مضیق‌ترین تعریف را از حریم خصوصی در فضای مجازی ارائه دهند. بارزترین مثال در این خصوص اقدام دولت آمریکا است که بدون اطلاع شهروندان اقدام به نظارت بر عملکرد کاربران اینترنتی و حتی برخی کشورهای دیگر می‌کند. (فتحی، شاهمرادی، ۱۳۹۵: ۲۳۹)

امروزه سیستم‌های رایانه‌ای و فضای مجازی، تجاوز و تعدی به حریم خصوصی و عمومی اشخاص حقیقی و حقوقی را که از بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی می‌شود، بیش از پیش سهل‌الوصول کرده است؛ به گونه‌ای که مجرمان در اقصی نقاط جهان، فارغ از مرزهای جغرافیایی و به دور از نگاه کنترل کننده و رها از تفتیش و تجسس، زیستن را مورد تعرض قرار می‌دهند. اگرپیش از این جاسوسان، با مشکلاتی برای جاسوسی و اقدامات امنیتی مواجه بودند و چندان امیدی به اقدامات مجرمانه خود نداشتند، اکنون با استفاده از بستر فضای مجازی، در کمترین زمان ممکن و با دقت و وضوح بسیار بالا، اطلاعات سرّی و غیرسرّی موردنظر خود را به دست می‌آورند. قبلاً اگر استراق سمع و شنود، تنها واجد این مفهوم بود که باید شخصی مستور درجایی یا با برداشتن تلفنی، اطلاعات دیگران را کسب کند و درواقع تنها از این طریق بود که مجرمان می‌توانستند به آنچه از فعل مجرمانه خود دنبال می‌کردند نائل شوند، اکنون سیستم‌های رایانه‌ای در بستر فضای مجازی این امکان را فراهم آورده‌اند که در فرای مرزها و اقصی نقاط جهان، اطلاعات دیگران بدون آن‌که خودشان متوجه شوند، سرقت و ارزش ذاتی آن از بین برود و از حالت خصوصی و سرّی بودن، خارج شود.(فتحی، شاهمرادی، ۱۳۹۵: ۲۳۵)

## نظریات حاکمیت بر فضای مجازی

شیوه‌ی قانون‌گذاری در فضای سایبر، بسته به نوع نگرش به حاکمیت دولت متفاوت است، درمجموع، دو نگرش نسبت به حاکمیت دولت در این فضا وجود دارد: الف)حاکمیت انحصاری دولت بر فضای سایبر، ب) تعمیم نظریه میراث مشترک بشریت بر فضای سایبر. روش قانون‌گذاری ملی، منبعث از نگرش حاکمیت انحصاری دولت، و روش‌های قانون‌گذاری بین‌المللی، خود انتظامی و مختلط، منبعث از نگرش میراث مشترک بشریت در فضای سایبر است. کشورهای درحال‌توسعه، از نگرش مبتنی بر حاکمیت، و کشورهای غربی، حامیان حقوق بشر و نهادهای فنی فضای سایبر، از نگرش مبتنی بر میراث مشترک بشریت حمایت کرده‌اند. (ضیایی، شکیب نژاد،۱۳۹۵: ۲۲۹)

### ۱) حاکمیت انحصاری بر فضای مجازی

این دیدگاه، حاصل پذیرش مفهوم وستفالیایی حاکمیت[1] در فضای سایبر است. حامیان این نگرش معتقدندکه دولت، بهترین نهاد حاکمیتی، در فضای سایبر است. این نگرش، یادآور نظریه‌ی« متعلق به هیچ‌کس[2]» راجع به دریای آزاد درگذشته است[3] که به هر دولتی اجازه می‌دهد به‌اندازه قدرت خود بر فضای سایبر، اعمال حاکمیت کند. در فضای مجازی، اینترنت مرز گذر است، اعمال حاکمیت از سوی همه دولت‌ها می‌تواند مشکلات حقوقی متعددی برای کشورها و افراد ایجاد کند؛ ضمن آنکه فضای سایبر برخلاف دریای آزاد درگذشته، میان چند دولت تقسیم‌نشده است. سخت‌افزارهای رایانه‌ای ازجمله سرورهای اینترنتی ازنظر فیزیکی تحت حاکمیت صلاحیت‌های ملی قرار دارد و همین امر، مستمسک برخی دولت‌ها برای توجیه کنترل سخت‌گیرانه‌ی اینترنت شده است. ازآنجاکه اینترنت، فاقد حاکمیت مرکزی است، طبق این نظریه، میان حاکمیت‌ها تعارض شکل خواهد گرفت.(ضیایی،شکیب نژاد، ۱۳۹۵: ۲۲۹)

1. Westphalian Concept of Sovereignty
2. Res nullis
۳ نظریه «متعلق به هیچکس» که تا ابتدای قرن هفدهم بر دریا حاکم بود، معادل نظریه دریای بسته بوده است که قابل مالکیت و حاکمیت بود. با انتشار کتاب دریای آزاد گروسیوس در سال ۱۶۰۵میلادی، نظریه متعلق به همه نضج گرفت. ن.ک: احمد متین دفتری؛ سیر تحول حقوق بین الملل دریایی (از گروسیوس تا کنفرانسهای ژنو)، گنج دانش، ۱۳۸۷، صص ۱۳۰-۱۳۴.

### ۲) فضای مجازی به‌مثابه میراث مشترک بشریت

با انقلاب مردمی فرانسه و تحولات بعدی در سایر کشورها، حاکمیت مردم به‌عنوان یکی از مفروضات بنیادین مشروعیت سیاسی دولت مطرح شد. در این دوره که در آن« حاکمیت فراوستفالیا[1]» مطرح می‌شود، حاکمیت دولت‌ها تحت‌الشعاع دو پدیده جهان‌شمولی و حقوق بین‌الملل قرار گرفت. دو نظریه«متعلق به همه» و « میراث مشترک بشریت[2]» برآمد این نگرش به حاکمیت است که طبق آن، هیچ کشوری حق اعلام حاکمیت بر مناطق خارج از صلاحیت خود را نداشته و همچنین نمی‌تواند مانع استفاده کشورهای دیگر از آن شود.[3] طبق این نظر، صلاحیت قانون‌گذاری به مرجعی فراتر از دولت‌ها واگذار می‌شود. امروزه این نظریه در مناطقی چون دریای آزاد، بستر عمیق دریا، قطب جنوب، فضای ماورای جو و اجرام آسمانی پذیرفته‌شده است. با این‌حال، انگاشت فضای سایبر به‌عنوان میراث مشترک بشریت، با مشکلاتی فنی و حقوقی روبه‌روست. به‌طور مثال، عواملی چون برتری دانش و ثروت، حاکمیت برابر در فضای سایبر را تحت تأثیر قرار می‌دهد. همچنین اگرچه اصل میراث مشترک بشریت در برخی مناطق، تبدیل به عرف بین‌المللی شده، لیکن، نحوه بهره‌برداری از آن، موضوعی مستقل محسوب می‌شود.(ضیایی،شکیب نژاد، ۱۳۹۵: ۲۳۰)

## جایگاه قواعد بین‌المللی و قوانین حاکمیتی کشورها در فضای مجازی

فضای مجازی و قابلیت‌های آن، امکان کنجکاوی و جستجو در فضای اینترنت را برای کاربران بیش‌ازپیش فراهم ساخته و این می‌تواند علاوه بر خدشه‌دار نمودن حریم خصوصی، در برخی موارد باعث تحت تأثیر قرار گرفتن ملاحظات امنیت ملی در کشورها قرار بگیرد.

ساماندهی بهینه با قوانین و مقرره‌هایی محقق می‌شود که متناسب با اصول بنیادین حقوق بشری و همکاری‌های بین‌المللی وضع گردد. ازآنجاکه یکی از پیامدهای نقض حریم خصوصی، زیرسؤال قرار گرفتن امنیت ملی کشورها، می‌تواند تلقی گردد، مادۀ ۱۲ اعلامیۀ جهانی حقوق بشر،

1. Post-Westphalian Sovereignty
2. Common Heritage of Mankind
۳. جالب توجه است که در خصوص دریاها موضع کشورهای غربی و قدرتمند بر نظریه متعلق به هیچکس، و موضع کشورهای درحالتوسعه بر نظریه متعلق به همه قرار داشت(ن.ک.متین دفتری، همان) درحالیکه در فضای سایبر، موضع این دو گروه برعکس است.

به لزوم حمایت قانونی از حریم خصوصی در برابر تعرضات پرداخته و مادۀ ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی و مادۀ ۸ کنوانسیون اروپایی حقوق بشر نیز بر این حمایت قانونی تأکید نموده‌اند. همچنین کشورها در این زمینه قوانینی را وضع کردند؛ لیکن ضوابطی که از سوی اعلامیه و میثاق در خصوص حفظ امنیت ملی، سلامت و اخلاق عمومی ذکر شده است، باعث گردیده، برخی کشورها در تفسیر حدود و ثغور آن‌ها بی‌ملاحظگی‌هایی به خرج دهند. اتحادیه بین‌المللی مخابرات، در مادۀ ۳۷ اساسنامه به این امر توجه داشته و اشعار می‌دارد:« اعضای اتحادیه موافقت می‌نمایند تا تدابیر لازم را جهت تضمین محرمانه ماندن مکالمات بین‌المللی اتخاذ کنند»، اما دربند ۲ این ماده به مقامات دولتی اجازه داده، نظارت قانونی خود را (به‌منظور حفظ امنیت ملی) اعمال کنند، شورای حقوق بشر و مجمع عمومی سازمان ملل در قطعنامه ۶۹/۱۶۶ تأکید بر اصلاح مقررات و تعهد دولت‌ها در حفظ حریم خصوصی تحت لوای حقوق بشر و در قطعنامه۲۸/۱۶خواستار ارائه یک روش مؤثر برای شناسایی اصول، استانداردها و شیوه‌های بهینۀ حفاظت از حریم خصوصی شده است.(رئیسی، قاسم‌زاده، ۱۳۹۹: ۱۲۷)

در ۱۰جولای۲۰۱۳ مرکز امنیت اطلاعات ملی ژاپن (NISC)[1] سند راهبرد سایبری ژاپن را به دنبال وقوع حمله به صنایع میتسوبیشی، هک

شدن سایت پارلمان، مورد هدف قرار گرفتن نهادهای هوایی، فضایی و وزارت امور خارجه این کشور و شدیدترین آن‌ها حمله به شرکت سونی، تدوین و منتشر نمود. در کشور ژاپن چهار نهاد اصلی در حوزه سایبری فعالیت می‌نمایند؛ پلیس ملی، مسئولیت رصد، شناسایی و پیشگیری از ارتباطات غیرمجاز در راستای مبارزه با فعالیت اطلاعات سایبری را بر عهده دارد. وزارت امور داخلی و ارتباطات مسئول تعیین سیاست‌های ارتباطاتی و شبکه‌ای ازجمله انجام اقدامات برای تبادل و مشارکت در امنیت اطلاعات سایبری و توجه به زیرساخت‌ها می‌باشد. وزارت دفاع ژاپن نیز مسئول تأمین امنیت و مقابله با چالش‌های تبادل اطلاعات در سطح ملی و بین‌المللی است و در این راستا به توسعه منابع انسانی، تقویت سیستم‌های حفاظتی، ارتقای امنیت سیستم‌های اطلاعاتی می‌پردازد. شورای سیاست‌گذاری امنیت اطلاعات آخرین نهاد کشور ژاپن در راستای "استراتژی‌های ملی راجع به امنیت اطلاعات می‌باشد. در کشور چین در سال ۱۹۹۴، اولین قانون

1 .National Information Security Center

راجع به جرائم رایانه‌ای مورد تصویب قرار گرفت. سپس قانون مجازات جرائم رایانه‌ای و فضای مجازی چین به‌عنوان اصلی‌ترین قانون در حوزه سایبری در سال ۱۹۹۷ تدوین و در مهروموم‌های ۲۰۰۰، ۲۰۰۹ و ۲۰۱۱ مورد اصلاح قرار گرفت. در سال ۲۰۰۰ لایحه‌ایی در خصوص حفاظت از امنیت شبکه مورد تصویب شورای ملی قرار گرفت که مشتمل بر ۲۱ عنوان جرم رایانه‌ای بود. (تقی زاد، ۱۳۹۶: ۱۲۹)

## فضای مجازی[1]

منظور از فضای سایبر یا فضای مجازی ترکیبی از ده‌ها هزار رایانه به هم پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها و کابل‌های فیبرنوری است که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد(افتخاری،۵،۱۳۸۲)، فضای مجازی مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از عقاید و باورها را در قالب دادوستد رد و بدل می‌کند. این فضا می‌تواند عامل اساسی در فرهنگ‌سازی و هویت‌سازی و به تبع آن تأثیر مهمی در روند اجتماعی شدن افراد داشته باشد.(بل،۲۰۰۱: ۷۹)[2] واژه فضای مجازی برای توصیف یک جهان الکترونیکی گسترده استفاده می‌شود که در آن، فنّاوری کامپیوتری با سیستم‌های ارتباطی پیشرفته پیوند می‌خورد. در این فضا هرکس به همان آسانی که با شخص کنارش ارتباط برقرار می‌کند، می‌تواند با فردی در دورترین نقطهٔ جهان مرتبط شود. در جهان امروز، به حدی استفاده از این فضا فراوان شده، که گاهی اصطلاح واقعیت مجازی را برای آن به کار می‌برند. واقعیت مجازی جایی است که تصاویر مردم و یا حوادث به کمک یک کامپیوتر طوری ایجاد می‌شودکه کاملاً مشابه نمونهٔ واقعی به نظر می‌رسد. (جفریس، ۱۳۸۱ : ۴)

با توجه به تعاریف ارائه شده می‌توان گفت؛ که فضای مجازی یا فضای سایبر محیطی است مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی (به صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود داشته، مقابل استفاده و دسترس استفاده کنندگان و کاربران

1. Cyber Space
2. Bell

کامپیوتر و شبکه‌های بین المللی می‌باشد(باستانی،۱۳۸۶: ۳۶)، با گسترش استفاده از مفهوم نوین سایبر هر آنچه پس یا پیش از واژه «سایبر» قرار گیرد، به نوعی به بیان رابطه انسان و رایانه می‌پردازد. مفهوم فضای مجازی معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می‌شود. فضای مجازی با ویژگی‌هایی چون؛ دسترسی، راهبری، فعالیت اطلاع‌یابی، بالندگی و اعتماد شناخته می‌شود. (خانیکی و بابائی، ۱۳۹۰: ۷۶-۷۷)

## فضای مجازی، فضای حقیقی

حضرت آیت‌الله خامنه‌ای (مدظله العالی)، فضای مجازی را فضای حقیقی دانسته و می‌فرمایند: «یکی از خصوصیات ممتاز عصر حاضر، آماده بودن وسایل پیام‌رسانی است. فضای مجازی در حقیقت فضای حقیقی است و در زندگی بسیاری از مردم حضور دارد»، آیت‌الله جوادی آملی در این‌باره می‌فرماید:«هرکس غافل از خطرات و آسیب‌های این فضاست، باید بداند این فضا حقیقی است، نه مجازی؛ هرجا فکر و اندیشه منتقل شود، فضای حقیقی است». فضای مجازی، نخستین بار توسط ویلیام گیبسون نویسنده‌ی داستان‌های علمی تخیلی در سال ۱۹۸۴ بکار برده شد. از نظر او فضای مجازی، فضایی تخیلی است که از اتصال رایانه‌ها پدیدآمده و تمامی انسان‌ها و منابع اطلاعاتی را به هم متصل کرده است. فضای مجازی فقط مجموعه‌ای از سخت افزار نیست، بلکه مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از باورها را در چارچوب داد و ستد، بیت رد و بدل می‌کند. فضای مجازی به فضای تعاملی اینترنت اطلاق می‌شود،که در آن افراد در درون آن با هویت‌هایی پنهان، به مثابه پیام‌هایی بر صفحات رایانه حضور می‌یابند. فضای مجازی، حقیقتاً مجازی نیست، بلکه باتوجه به آثار آن یک دنیای حقیقی است.گسترش فناوری‌های اینترنتی و در دسترس بودن آن، فضای مجازی را شبیه‌ساز، دنیای واقعی کرده است (www.savaderesane.ir)، یکی از جلوه‌های جهانی‌شدن معاصر، ظهور انقلاب اطلاعات و گسترش فضای مجازی است.«سیالیت بر بال رسانه‌ها» و«زمان بی‌زمان و فضای جریان‌ها» تعابیری است که کاستلز در توصیف فضای مجازی به کار می‌برد. (کاستلز،۱۳۸۰: ۱۶۵)، به تعبیر وی، جامعه‌ی شبکه‌ای جهانی، جامعه‌ای است که ساختارهای اجتماعی آن پیرامون شبکه‌های فعال‌شده از طریق فناوری‌های اطلاعاتی، ارتباطی و پردازش‌شده دیجیتالی و مبتنی بر میکروالکترونیک

شکل گرفته است، در این جامعه، حاکمیت شبکه‌ها بر فعالیت‌ها و مردمی است که نسبت به شبکه‌ها «بیرونی و خارجی» محسوب و از این نظر شبکه‌های جهانی به زوال شبکه‌های محلی می‌انجامند(کاستلز، ۱۳۸۰: ۸۶).

## طرح صیانت از فضای مجازی

طرح «نظام تنظیم مقررات خدمات فضای مجازی» که با نام طرح صیانت از فضای مجازی شهرت یافته است، نمونه‌ایی از حاکمیت دولت بر فضای مجازی می‌باشد.کلیات این طرح تحت عنوان«اصل ۸۵ شدن طرح صیانت از کاربران فضای مجازی» با ۱۸ رای موافق، در تاریخ ۳ اسفند ۱۴۰۰ در کمیسیون مشترک مجلس شورای اسلامی تصویب شد، این طرح در هفت فصل و ۲۱ ماده تدوین گردیده است. بر اساس پیش‌نویس این طرح، کارگروه مدیریت گذرگاه مرزی متشکل از رئیس مرکز ملی فضای مجازی (ریاست کارگروه) و نمایندگان وزارت ارتباطات و فناوری اطلاعات، سازمان پدافند غیر عامل، وزارت اطلاعات، نیروی انتظامی، قوه قضائیه، ستاد کل نیروهای مسلح و سازمان اطلاعات سپاه، سازمان کارگروه تعیین محتوای مصادیق مجرمانه را ایجاد تا نسبت به امنیت ارتباطات، اطلاعات و مدیریت ترافیک ورودی و خروجی ایران در گذرگاه‌های ایمن مرزی تصمیمات لازم را اتخاذ کند. هدف از طرح حمایت از حقوق کاربران، ساماندهی فضای مجازی بیان شده است (www.alef.ir)

## مدل‌های قدرت در فضای مجازی:


شکل ۱. مدل‌های قدرت سایبری (مرکز بررسی‌های استراتژیک ریاست جمهوری، ۱۳۹۹: ۶)

## رویکردهای حکمرانی در فضای مجازی

**۱) رویکـرد کالیفرنیـایی:** در ایـن رویکـرد، دولـت مداخلـه نمـی‌کنـد و اختیـار در دسـت شرکت‌های بزرگ است. یعنی سیاست‌های دولت منتج از رشد شرکت‌های بزرگ می‌باشد. چـون شرکت‌ها به دنبال رشد هستند، سیاست تهاجمی را در پیش می‌گیرند.

**۲) رویکرد اروپایی:** اروپایی‌ها در اعتراض بـه رویکـرد آمریکـایی‌هـا، بـر حکمرانـی چنـد ذینفعی[1] تاکید دارند. بدیهی است که آمریکا با این نگرش نسبت بـه حکمرانـی مخـالف و معتقـد است که؛ وقتی فضای مجازی در اختیار آمریکا است، آمریکا باید تعیـین کنـد کـه اسـتانداردها و پروتکل‌های مربوط به فضای مجازی و اینترنت چگونه باشد. اروپایی‌ها به منظور تقویت حکمرانی چندذینفعی، چند اقدام انجام دادند:

- دولت‌ها باید برای حمایت از شهروندان خود ساختارهای قانونی ایجاد کنند؛
- بخش خصوصی می‌بایست برای مقررات‌گذاری جدید آماده باشد (خودتنظیمی پلتفرم‌ها کافی نیست)؛
- جامعه مدنی باید نقش خود را در نظارت و بررسی فعالیت‌های دولت و کسب و کار تقویت کند؛
- در الگوی مشارکت چندذینفعی، پاسخگویی پلتفرم‌ها، حفظ ارزش‌های عمومی، اعتماد به حریم خصوصی، ارتقای ظرفیت؛
- مشارکت و کاهش تهدیدات سایبری ازجمله اهداف مهم است.

۱) **رویکرد چینی:** در رویکرد چینی کنترل کامل فضای مجازی توسط دولت‌ها انجام می‌شود و بر بعد هژمونیک قدرت سایبری تاکید می‌شود. روسیه هم بیشتر با این رویکرد به فضای مجازی نگاه می‌کند. در رویکرد چینی حریم خصوصی و اعتماد عمومی با تهدید مواجه می‌شود، اما در مقابل امنیت و قدرت ژئوپلیتیک فضای مجازی افزایش پیدا می‌کند.

در کنفرانس ۲۰۱۹ در رابطـه بـا موضـوع اینترنـت، رویکـرد چینـی بـا اقبـال بیشـتری از سـوی کشورها مواجه شد. دو ابزار سانسور و فـایروال (محافظـت) بـه‌عنـوان ابزارهـای مـورد اسـتفاده در

1. Multi-stakeholder governance

رویکرد چینی پذیرفته شد، اما با این ملاحظه که حد و مرز آن مشخص شود. در کشور چین این ابزارها بدون حدومرز استفاده می‌شوند. (مرکز بررسی های استراتژیک ریاست جمهوری، ۱۳۹۹: ۶)

## محورهای حکمرانی در فضای مجازی

حکمرانی سایبری شش محور کلی را شامل می‌شود که لازم است مورد توجه قرار گیرد. این شش محور عبارتند از؛ محورهای زیست محیطی، فرهنگی- اجتماعی، سیاسی- نهادسازی، اقتصادی، حقوق و مقررات و فناوری و زیرساخت.(همان: ۶)


شکل ۲. محورهای حکمرانی در فضای مجازی (مرکز بررسی‌های استراتژیک ریاست جمهوری، ۱۳۹۹: ۸)

## رویکردهای توسعه حکمرانی فضای مجازی

**۱) حکمرانی از طریق فضای مجازی:** در این رویکرد، فضای مجازی ابزاری است برای مدیریت فضای واقعی. حکومت‌ها وظایف حاکمیتی خود را از طریق فضای مجازی انجام می‌دهند. برای مثال، خدمات دولتی از طریق اینترنت ارائه می‌شود. مفهوم «دولت الکترونیک» در این حوزه جای می‌گیرد. مانند کره و مالزی.

**۲) حکمرانی در فضای مجازی:** حکومت‌ها سعی می‌کنند حاکمیت سرزمینی خود را در فضای مجازی بازتعریف و اعمال کنند. آنها دامنه‌های ملی تعریف و در پی امنیت سایبری شهروندان خود هستند و...، مانند ترکیه و عربستان.

**۳) حکمرانی بر فضای مجازی:** حکومت‌ها سعی می‌کنند سیاست‌هایی را برای شکل دادن به فعالیت‌ها در فضای مجازی تدوین و اجرا کنند، رویه‌های عمل قانونی را در فضای مجازی تعیین و روابط میان بازیگران و گروه‌های اجتماعی مختلف را تنظیم کنند. مانند آمریکا. (مرکز بررسی‌های استراتژیک ریاست جمهوری، ۱۳۹۹: ۵)

**امنیت:**

امنیت از جمله مفاهیم علوم انسانی است که مانند بسیاری مفاهیم دیگر (جامعه، فرهنگ، ارزش و ..) پیچیدگی و گنگ بودن خصیصه

ذاتی و ماهوی آنست. معماگونگی امنیت و فرورفتن در هاله‌ای از رمز و رازهای تئوریکی و ایدئولوژیکی تا جایی است که بوزان، بیان کرده:«کوششی برای درک مفهوم امنیت، بدون آگاهی کافی از تناقضات و نارسایی‌های موجود در خود این مفهوم ساده اندیشانه است»(مایل افشار،۱۳۸۹: ۵۴)، امنیت مفهومی غیر توسعه‌یافته، مبهم، نارسا، ماهیتاً جدال‌برانگیز و شخصیتاً متباین و متناقض است. امنیت در لغت به معنی درامان بودن، ایمنی، آرامش و آسودگی است و کلمه امن به معنی بی بیم شدن، بی ترس، اطمینان، آسایش، آرامش قلب و ضد خوف است. همچنین جایگاهی است که عالی‌ترین احساس و عواطف انسانی در آن رشد و نمو کرده است. (پاسبان،۱۳۹۳: ۴۰)، مک سوئینی امنیت را واژه‌ای لغزنده و بی‌ثبات می‌خواند که در گستره‌ی گیج‌کننده‌ای از زمینه‌های متنوع و در جهت اهداف چندگانه به وسیله افراد، شرکت‌ها، حکومت‌ها و متخصصان آکادمیک به کار رفته و در این فضا مجموعه‌ای از چیزها، مردم، وسایل، اهداف، حوادث خارجی و احساسات درونی منظور شده‌اند (چگنی‌زاده، ۱۳۷۹: ۸۵-۸۴)، دایره‌المعارف بزرگ لاروس ذیل واژه security[1] آورده است: «وضعیتی که شخص در آن از خطر واهمه ندارد و آرامش نفسانی از آن حاصل می‌شود.» در واژه‌نامه‌ی دپو از امنیت این مفاهیم به‌دست می‌آید: «حالت نفسانی قابل‌اعتماد و آرام که انسان خود را مصون از خطر می‌یابد و وضعیت و حالت آرامی که از فقدان خطر به‌دست می‌آید. در زبان انگلیسی نیز ذیل واژه امنیت، حالت یا احساس آزاد بودن از ترس و بیمناکی، آمده است. (بشیری، روزنامه جام جم، شماره ۲۵۳۶)، کلمه‌ی امنیت ریشه در واژه «امن» از زبان عربی دارد و به معنی در امان و آسایش بودن، مصونیت از خطر و ترس و آرامش خاطر

1. Security

می‌باشد. در تعریف لغوی امنیت می‌توان گفت:«حالت فراغت از هرگونه تهدید یا حمله و یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. در اصطلاح سیاسی و حقوقی به‌صورت امنیت فردی، امنیت اجتماعی، امنیت ملی و بین‌المللی به‌کاربرده می‌شود.» (آشوری، ۱۳۸۴: ۳۸)

برژنیسکی در رابطه با واژه امنیت، معتقد است:« منظور من ازامنیت، یعنی امنیت نظامی صرف نیست، گرچه قدرت نظامی یکی از ابعاد مهم رقابت تاریخی آمریکا و شوروری است؛ در عوض معتقدم که امنیت ملاحظات بیشتری را در برمی‌گیرد؛ از جمله زمامداری سیاسی، قدرت اقتصادی، نوآوری تکنولوژیک، حیات ایدئولوژیک و ...؛ تلاش برای نیل به امنیت بدون عنایت به چنین ملاحظاتی چندان مؤثر نخواهد بود و احتمالاً به شکست می‌انجامد»(مک‌کین لای، ۱۳۸۰: ۱۷). والترلیپمن درسال ۱۹۴۳ واژه امنیت را این چنین تعریف کرد:«یک ملت هنگامی از امنیت برخوردار است که درموقع خطر مجبور به فدا کردن ارزش‌های حیاتی خود نباشد. اگر مایل بود بتواند از جنگ اجتناب و اگر واردجنگ شد، بتواند ارزش‌های حیاتی خود را از طریق پیروزی در نبرد پاس دارد»(مارتین، ۱۳۸۲: ۹۶).

## امنیت ملی[1]

دانش‌نامه علوم اجتماعی، «امنیت ملّی» را «توان یک کشور در حفظ ارزش‌های خودی در برابر تهدیدهای خارجی» و یا «احساس آزادی کشور در تعقیب هدف‌های ملّی و ترس از خطر جدّی نسبت به منافع اساسی و حیاتی کشور» بیان کرده است.(بهزادی،۱۳۶۹: ۱۰۱)، بنابراین، «امنیت» یعنی؛ تضمین ایمنی قرارهای تنظیمی سیاسی برای کاهش احتمال بروز جنگ، برقراری مذاکره به‌جای محاربه و قصد حفاظت از صلح به عنوان شرط طبیعی بین دولت‌ها و نیز یعنی؛«مصونیت از تعرّض و تصرف اجباری و بدون رضایت و دور ماندن از مخاطرات تعدّیات به حقوق و آزادی‌های مشروع». امنیت ملی مصونیت نسبی یا مطلق یک کشور از حمله مسلّحانه یا خرابکارانه سیاسی یا اقتصادی احتمالی همراه با واردکردن ضربه‌کاری و مرگبار است. در صورت حمله، امنیت ملی بیانگر تمام مقاصد دفاعی کشور است؛ یعنی آمادگی برای مخاصمه به خاطر بازداشتن آن یا دوری گزیدن از آن، بااین‌همه، خود سیاست‌های مربوط به امنیت ملّی ممکن است در شرایط به خصوصی (مثل مسابقه تسلیحاتی و کنترل تسلیحات) موجب ناامنی گردند. روحیه

1. National Security

نیروهای نظامی، تعداد و هوشمندی دانشمندان، فناوری، ویژگی‌های رهبران و شخصیت‌های سیاسی و نظامی، موقعیت ژئوپلیتیکی و قدرت اقتصادی کشور ازجمله عوامل مؤثر در امنیت ملی هستند(پاسبان،۱۳۹۵: ۱۲۶)، مفهوم امنیت ملی به عنوان پرکاربردترین مفهوم در مطالعات امنیت است که از اضافه شدن واژه‌ی«ملی» به امنیت تشکیل می‌شود، یعنی بنا دارد امنیت را دربارهٔ یک ملت و برای آن مورد بحث قرار دهد. این مفهوم ، پس از قرارداد وستفالیا و تشکیل دولت- ملت‌ها در قرن هفدهم شکل گرفت. (عصاریان‌نژاد،۱۳۸۷: ۴)، در رهیافت نو از امنیت ملی، با لحاظ کردن تغییر و تحولات ایجادشده در محیط داخلی و بین‌المللی و چالش‌های ناشی از جهانی‌شدن، محلی شدن و بین‌المللی شدن مسائلی نظیر، مواد مخدر، محیط‌زیست، رکود اقتصادی، ظهور بمب اتم، فناوری، فضای مجازی و ... مفهوم امنیت ملی را جرح‌وتعدیل کرده و آن را اساساً از جنبه نرم‌افزاری بررسی می‌نماید. درنتیجه آن امنیت ملی علاوه بر بررسی تهدید، استفاده وکنترل نیروی نظامی شامل؛ اولویت‌بخشی به تهدیدات محیطی، اقتصادی، سیاسی و فرهنگی است که برخی از این تهدیدات، نه‌تنها برخلاف گذشته، شکل و ماهیت ابهام‌آمیزی پیدا می‌کنند، بلکه در شرایط ظهور وابستگی متقابل، ارتباط و نزدیکی روزافزون کشورها با یکدیگر، تهدیدات امنیتی شکل و ماهیت جهانی پیدا می‌کنند. از زمان پایان جنگ سرد، تغییراتی در الگوهای امنیتی دولت‌ها مشاهده می‌شود و تحت تأثیر جهانی‌شدن، تأکید بر امنیت نظامی دولت، به سمت «امنیت بین‌المللی» سوق یافته است. در این چارچوب معنای بین‌المللی شدن، جهانی‌شدن یا چندجانبه‌گرایی است. (amniati.hormozgan.ir)

## مفهوم امنیت ملی و دولت‌ها

برداشت از مفهوم امنیت ملی و شرایط و لوازم آن، یکسان نیست. دولت‌ها برحسب مقام و موقعیتی که در عرصه مناسبات بین‌المللی دارند و نیز بر اساس مبانی ارزشی خود، تصورات و تلقی‌های متفاوتی از مفهوم امنیت دارند. از طرفی می‌توان گفت که دامنه امنیت یک کشور، با قدرت آن کشور ارتباط مستقیم داشته و قدرت کشورها نیز متفاوت است. هرچند اکثر متخصصین علم سیاست بر این اعتقادند که تفاوتی آشکار میان دولت‌ها در عرصه سیاست بین‌الملل از نظر ماهیت، اندازه و نفوذ آن‌ها وجود دارد، اما در مورد چگونگی دسته‌بندی آن‌ها نیز اختلافات قابل‌توجهی به چشم می‌خورد. معمولاً ایده‌ی امنیت ملی بر دو فرضیه استوار است که عمدتاً از تحول تاریخی نظام حکومتی اروپای مدرن ناشی می‌شود. اولاً همان‌گونه که در مدل توپ

بیلیاردی سنت «رئالیستی» مشهور است، دولت- ملت، عاملی وحدت‌بخش است که در قالب آن، امنیت ملی به‌طور خودکار با امنیت حکومت، مساوی می‌شود. ثانیاً، همان‌گونه که در سنت سیاسی پلورالیستی غرب مفروض است، امنیت یک دولت- ملت، سرجمع امنیت‌های افرادی هم‌سنخ است. ازاین‌رو طبق تعریف امنیت ملی در غرب، امنیت آن دولتی، ملی است که از تک‌تک شهروندان تشکیل می‌شود که از طریق بسط جامعه‌پذیری سیاسی دارای سرنوشت مشترکی هستند(آزرچونگ اینمون،۳۶:۱۳۷۹)، شاید این استدلال دقیق‌تر باشد که امنیت ملی برابر است با امنیت جمعی، و امنیت حکومت برابر است با امنیت رژیم حاکم که نماینده بخشی از علایق اجتماعی یا جمعی است. خطر استفاده از عنوان امنیت ملی برای دولت‌هایی که به لحاظ سیاسی ضعیف‌اند، این است که این مسئله به‌راحتی، به استفاده آنان از زور در امور سیاسی داخلی مشروعیت می‌بخشد. همچنین محیط امنیتی در دو طیف از کشورها متفاوت است. در میان کشورهای پیشرفته به‌خصوص دو بلوک شرق و غرب محیط امنیتی تحت تأثیر روابط معمول تعادل قوا می‌باشد. اما در کشورهای جهان سوم، محیط امنیتی تحت تأثیر روابط غیرمتقارن و فراملی توازن قوا می‌باشد. به‌عبارت‌دیگر، محیط داخلی این‌گونه کشورها تحت تسلط حکومت‌های ضعیف و محیط جهانی‌شان تحت سلطه یک گروه از قدرت‌های بزرگ قرار دارد. (آزرچونگ اینمون،۵۲:۱۳۷۹)

## امنیت ملی در فضای مجازی

در نظر همه بازیگران در نظام بین‌الملل، امنیت ملی واقعیتی کلیدی و حتی نخستین علت وجودی و مهم‌ترین هدف نهایی دولت‌ها می‌باشد. استقرار امنیت ملی به منظور چهار هدف صورت می‌گیرد:

- برقراری امنیت و حفاظت از شهروندان و دولت در مقابل حمله‌های فیزیکی ناشی از منابع خارجی؛
- ایجاد رونق اقتصادی و تأمین رفاه برای شهروندان؛
- حفظ اموال و ارزش های حاکم بر جامعه؛
- بهبود هنجارها، سنت‌ها و روش‌های متداول زندگی و حفظ آن‌ها.

امنیت بیش از آن که واقعیتی بیرونی باشد، ماهیتی ذهنی و گفتمانی داشته و تنها در رابطه‌ی همنشینی یا جانشینی با مفهوم‌های دیگرهمچون قدرت، منافع، اهداف، مصالح، تهدیدها که

همگی مفهوم‌های مبهم و سیالی هستند، مصداق خود را می‌یابد (تاجیک، ۱۳۸۱: ۹)، در حالی که می‌خواهیم تهدیدهای امنیتی خود را در دنیای واقعی جست‌وجو کنیم، متغیرهای جدیدی از سویی دیگر، دست اندرکار معماری دنیای مجازی شده‌اند. هر پدیده‌ی امنیتی با تهدیدها و فرصت‌هایی قرین بوده و نمی‌توان برای آن هویتی شفاف ترسیم نمود. از جمله تهدیدهای امنیتی که ممکن است فضای مجازی در آن‌ها تأثیر بسزایی داشته باشد، می‌توان به موارد زیر اشاره نمود:

- ✓ اقدام‌های مخل امنیت و برانداز گروه‌های مسلح و غیر مسلح؛
- ✓ گسترش نابسامانی‌های اجتماعی از قبیل مواد مخدر، فساد اخلاقی، جرائم اجتماعی، سرقت و ... ؛
- ✓ شکاف بین اقلیت‌های قومی، مذهبی و زبانی با نظام و افزایش گرایش‌های تجزیه طلبانه قومی؛
- ✓ اقدام‌های تروریستی، خرابکاری و هکتیویسم؛
- ✓ آماده سازی افکار عمومی علیه دولت‌ها؛
- ✓ اقدام سریس‌های اطلاعاتی بیگانه به عملیات جاسوسی در بستر اینترنت و فضای مجازی.

موضوعات در عصر اطلاعات، متنوع‌تر نسبت به گذشته در مسائل امنیت ملی تلقی می‌شود. در این عصر گردش آزاد اطلاعات در سراسر جهان که از راه فضای مجازی صورت می‌گیرد، موضوع امنیت اطلاعات را تا سطح مسائل امنیت ملی بالا می برد.(پالیزان،۱۳۹۳: ۶۴۱)

## توصیف محیط امنیتی در فضای مجازی

برای داشتن درک صحیح از وضعیت امنیت ملی، لازم است ماهیت فضای مجازی و محیط امنیتی و راهبردی مترتب بر آن را بهتر بشناسیم. در فضای مجازی سرعت و گردش اطلاعات در بین بازیگران ملی و فراملی دارای افزایش چشمگیری است. در بستر فضای مجازی افزون بر دولت‌ها، شرکت های چند ملیتی، سازمان‌های غیر دولتی، گروه‌های جنایی و تروریست‌ها و حتی افراد ممکن است به جنگ اطلاعاتی و تخریبی اقدام نمایند. فناوری اطلاعات توانایی بازیگران را در زمینه فرماندهی، کنترل و برقراری ارتباط با نیروهای تحت امر را افزایش و به جمع‌آوری اطلاعات دقیق درباره اهداف، توانمندی ها و عملکردهای دشمنان بالقوه و بالفعل کمک می‌کند. از نظر داخلی فناوری اطلاعات در ایجاد توانمندی‌های دفاعی، اقتصادی و سیاسی به دولت ها کمک می نماید. در محیط امنیتی جدید مبتنی بر فضای مجازی، افزایش سرعت اطلاعات، توانمندی و انعطاف پذیری گردش اطلاعات سبب کنترل دشوار دولت ها بر ورود و خروج

اطلاعات می شود. (سلطانی نژاد، ۱۳۸۶: ۱۳) افزایش تأثیر فضای مجازی بر فناوری‌های نظامی موجب شده است که دولت‌های متوسط و حتی گروه‌های شبه نظامی، به سلاح‌هایی دسترسی پیدا کنند که آنها را قادر می سازد در جنگی نامتقارن به مقابله با قدرت های پیشرفته نظامی برخیزند. قابلیت و خصوصیت منحصر به فرد فضای مجازی به گونه ایی است که خلافکاران، تروریست ها و به ویژه دستگاه‌های اطلاعاتی کشورهای بزرگ، از آن برای مقاصد مختلف از جمله جاسوسی به شیوه جدید یعنی جاسوسی به شیوه رایانه‌ایی استفاده می‌کنند. فضای مجازی به اندازه ایی گسترده شده است که اقتدار و حاکمیت کشورها را با مشکل مواجه نموده ، به طوریکه یک دولت واحد نمی تواند آن را به راحتی کنترل نماید. در جهان امروز ارتباطات و تبادل اطلاعات می تواند برتری های اقتصادی، نظامی و ...، را به ارمغان داشته و یا فقدان آن می‌تواند باعث نقایص و مشکلات برای دولت‌ها گردد و به این ترتیب موضوع‌های امنیتی جدید یا بی‌سابقه‌ایی ظهور پیدا کرده است. بنابراین محیط امنیتی و راهبردی نو مبتنی بر فضای مجازی، بسیار پیچیده تر از محیط امنیتی کنونی خواهد بود به طوری که این فناوری ها در عرصه های سیاسی، اقتصادی، نظامی، اجتماعی، فرهنگی و ارزشی نمود پیدا خواهد نمود. بنابراین لازم است برنامه ریزان و قانونگذاران در حوزه امنیت ملی ضمن درک کامل شرایط محیط امنیتی و راهبردی نوظهور، قوانین، و راهبردهای تأمین امنیت را در فضای مجازی تدوین و تبیین نمایند. (پالیزبان،۱۳۹۴: ۶۴۰)

## جرائم در فضای مجازی

سهولت در دسترسی و جستجوی اطلاعات موجود در سیستم‌های رایانه‌ای و فضای مجازی توأم با امکانات، در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی، منجر به رشد سرسام‌آور مقدار اطلاعات گردیده که این به نوبه خود می‌تواند باعث پیدایش انواع جرایم در این حوزه گردد. فناوری‌های جدید مفاهیم قانونی موجود را دچار چالش‌هایی ساخته است. جرائم رایانه‌ای یا جرائم در فضای مجازی (سایرجرائم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرائم رایانه‌ای صرفًا عبارت از جرائمی است که در فضای سایبر رخ می‌دهد. در تعریف موسع، هر فعل و ترک فعلی که در اینترنت یا از طریق آن، چه به‌طور مستقیم یا غیرمستقیم رخ می‌دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است، جرم رایانه‌ای نامیده می‌شود. براین اساس اینگونه جرائم را می‌توان به سه دسته تقسیم نمود: دسته اول: جرائمی هستند

که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند. مانند سرقت، تخریب و غیره، دسته دوم: جرائمی هستند که در آن‌ها رایانه به عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم بکار گرفته می‌شود. دسته سوم: جرائمی هستند که می‌توان آنها را جرائم رایانه‌ای محض نامید. این نوع از جرائم کاملاً با جرائم کلاسیک تفاوت داشته و در دنیای مجازی به وقوع می پیوندند، لیکن آثار آن‌ها در دنیای واقعی ظاهر می‌شود، مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای. اولین تقسیم بندی از جرائم رایانه‌ای در سال۱۹۸۳ ارائه و طی آن پنج دسته اعمال، مجرمانه تلقی و پیشنهاد گردید.کمیتهٔ منتخب جرائم رایانه‌ای شورای اروپا، پس از بررسی حقوقی- فنی، این پنج عنوان، دو لیست تحت عناوین لیست حداقل و لیست اختیاری را به کمیته وزراء پیشنهاد و آنان نیز آن را تصویب نمودند. سازمان‌های دیگر نیز اقدامات مشابه را انجام دادند. نقطه مشترک در همه این بررسی‌ها و پیشنهادات، جرائم علیه امنیت می‌باشد.(گنجی،۱۳۹۵: ۲۰)

فضای مجازی، فضایی متشکل از شبکه‌های ارتباطی است که در آن محتوا و خدمات در چارچوب مبانی و ارزش‌ها وقوانین و مقررات کشورها ارائه می‌شود که این خود علاوه بر داشتن محاسن فراوان، می‌تواند بستری را برای بروز جرائم سایبری(درون مرزی و فرامرزی) فراهم نماید. برقراری امنیت در فضای مجازی کاری بسیار دشوار است. زیرا از آن می‌توان به عنوان ابزاری متعارف برای حمله به تشکیلات دولتی، نهادهای مالی، زیر ساخت های انرژی، حمل و نقل ملی و همچنین روحیه عمومی استفاده نمود. لذا ناامنی در فضای سایبری شامل تمام زیرساخت هایی که به نحوی با فناوری اطلاعات در ارتباط هستند، می باشد. با توجه به ویژگی‌های ژئوپلتیک فضای مجازی، از جمله؛ مدیریت و کنترل، هویت، همگرایی و همکاری، رقابت و ستیز، تولید قدرت و حاکمیت ملی، می‌تواند در فرآیند رقابت بازیگران سیاسی و حکومت‌ها و نقش‌آفرینی در تولید قدرت و مناسبات آن در سیستم‌های جهانی به کار گرفته شود. لذا تعامل و همکاری مطلوب کشورها در مبارزه با جرائم و ارتقاء امنیت سایبری می‌تواند اثر بخش باشد، لیکن عواملی همچون تعارض قوانین بین‌المللی، نبود نظام حقوقی منسجم جهانی برای مقابله با جرائم سایبری فراملی، حاکمیت مطلق آمریکا بر اینترنت و ...، باعث گردیده که علیرغم اقدامات ارزشمند و مؤثر، موفقیت چندانی در این خصوص کسب نگردد و این به نوبه خود باعث وقوع مداوم جرائم سایبری با ماهیت فراملی و اجتناب‌ناپذیر بودن آن‌ها بر منافع ملی کشورها (وحدت ملی، امنیت ملی و قدرت ملی) می‌گردد. (رامک و همکاران، ۱۳۹۷: ۲۷۶)

## تأثیر فضای مجازی بر امنیت ملی

امنیت ملی، شرایط و فضای ملی و بین‌المللی است که ملت در چارچوب آن می‌تواند اهداف و ارزش‌های حیاتی موردنظر خویش را در

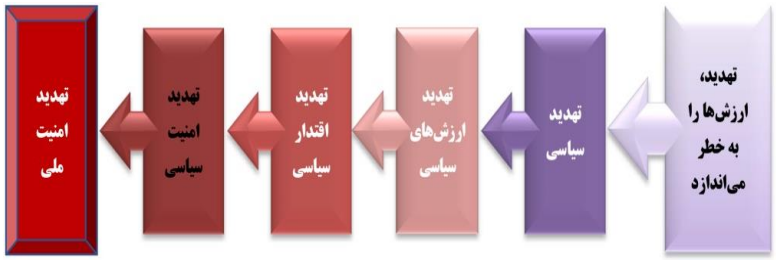
سطح ملی و بین‌المللی گسترش دهد و یا دست‌کم، آن‌ها را در برابر تهدیدهای داخلی و خارجی و دشمنان بالقوه و بالفعل حفظ نماید.

بنابراین هر آنچه، به‌صورت عینی یا ذهنی، ارزش‌ها و منافع ملی یک کشور را تهدید کند یا مانعی برای رسیدن کشور به اهدافش باشد تهدید امنیت ملی محسوب می‌شود. این تهدیدات ممکن است سخت، نیم‌سخت یا نرم باشند. برخی از کارکردهای سیاسی و امنیتی فضای مجازی مرتبط با امنیت ملی که تاکنون احصا شده است (ندری و همکاران، ۱۳۹۸: ۷۲) عبارت‌اند از:

### الف) تضعیف ارزش‌ها و باورهای ملی

مهم‌ترین کار ویژه ارزش‌ها و باورهای ملی حفظ همبستگی و مشروعیت دهنده به قواعد و ضوابط اجتماعی است؛ هرگونه تهدید معطوف به آن‌ها می‌تواند بی‌ثبات کننده نظام سیاسی یک کشور باشد. جانسون معتقد است ارزش‌های حاکم بر جامعه از چنان اهمیتی در پایداری و مانایی یکی نظام برخوردارند که هرگونه بی‌توجهی به آن‌ها می‌تواند زمینه‌ساز بروز یک تحول عمده باشد.بی‌توجهی به ارزش‌ها، مشروعیت و مقبولیت یک نظام را زیر سؤال می‌برد. این پدیده سبب نوعی ناهماهنگی بین نظام اجتماعی و نظام حاکم می‌شود. ازنظر جانسون، ورود ارزش‌های جدید و نامناسب با یک نظام اجتماعی به آن جامعه، سبب ناهماهنگی نظام اجتماعی با نظام حاکم می‌شود و زمینه‌ساز تغییرات بنیادین در آن جامعه خواهد شد. بنابراین ارزش‌ها مبانی دوام و قوام ثبات جامعه هستند. در بررسی تهدید فرهنگ، ارزش‌ها و باورهای ملی جامعه ایران، باید به دو بعد توجه کرد: یکی تهدید ارزش‌ها و باورهای ملی به‌صورت غیر عامدانه و تنها ناشی از ورود ناخواسته این فناوری‌ها به کشور است. بعد دیگر، تهدید ارزش‌ها و باورهای ملی به‌صورت یک برنامه از پیش تعیین‌شده وغیرخشونت آمیز به‌منظور تغییر نظام سیاسی کشوراست(سلطانی نژاد و دیگران،۱۳۹۲: ۹۵) امروزه ظهور اینترنت و فضای مجازی شدت و دامنه این‌گونه فعالیت‌ها را وسیع‌تر ساخته است. این تهدیدها که در قالب جنگ نرم صورت گرفته و با تهدیدهای سابق یعنی نظامی و اقتصادی ماهیت متفاوتی دارد و در راستای دیدگاه ابزارگرایانه دولت‌های غربی به فناوری‌های نوین قرار دارد. بیشتر نظریاتی که در مورد جنگ نرم ارائه‌شده است، بر این نکته

تأکیددارند که هدف اصلی و ماهوی عاملان جنگ نرم، ایجاد لغزندگی، شک و تردید در باورهای افراد یک جامعه نسبت به الگوهای ارزشی، فکری و فرهنگی موجود در آن جامعه است تا در مرحله بعد، الگوهای موردنظر خود را بر این افراد تحمیل کنند. ( ندری و همکاران ،۱۳۹۸: ۷۳)




شکل۳. بررسی اثر تهدیدها (ندری و همکاران، ۱۳۹۸: ۷۳)

## ب)تخریب و القای ناکارآمدی نظام سیاسی

شبکه‌های اجتماعی مجازی می‌توانند چنان تصویری از حکومت و قدرت به مردم معرفی کنند که سبب ایجاد جدایی و شکاف بین آن‌ها با حکومت شود و پذیرش حکومت توسط مردم را با چالش مواجه می‌کند؛ این کار بیشتر با ارائه چهره غیر دموکراتیک و ناکارآمد از حاکمیت و مغایرت آن با خواست عمومی انجام می‌شود. جنگ نرم در حوزه مشروعیت‌زدایی ساختاری از یک‌سو، معطوف به تخریب نظام سیاسی و از سوی دیگر معطوف به تغییر ادراک مردم نسبت به‌نظام سیاسی است. ( ندری، ۱۳۹۸: ۷۴)

## ج) انسجام زدایی ساختاری:

تخریب انسجام اجتماعی یکی از اهداف و نشانگاه‌های اصلی جنگ نرم است. برای انجام این کار، عاملان جنگ نرم تلاش می‌کنند لایه‌های جامعه را بر مبنای انگاره‌ها و دیدگاه‌های معارض با نظام سیاسی هدف به تحرک وادارند. در این وضعیت، انسجام اجتماعی به هم می‌ریزد و جامعه رو درروی نظام سیاسی قرار می‌گیرد. بنابراین انسجام زدایی ساختاری از جامعه به بی‌ثبات‌سازی سیاسی منجر می‌شود. به اذعان بسیاری از متخصصان فضای مجازی و حوزه جنگ نرم ، یکی از کارکرده‌ای ویژه اینترنت و شبکه‌های اجتماعی مجازی به‌عنوان فناوری‌های نوین ارتباطی تلاش جهت انسجام زدایی از جامعه مورد هدف نظام سلطه دارند (عالمی،۱۳۹۱: ۳۷)

### د) تشویق به نافرمانی مدنی و ایجاد تنش سیاسی:

کمتر کسی است که در رابطه با نقش بارز فضای مجازی در سازماندهی فعالیت‌ها، راه‌اندازی تجمعات و اعلام روز و ساعت دقیق آن، بهره‌گیری از نمادهای هماهنگ مانند رنگ خاص و شعارهای مشخص، آن‌هم در مدت‌زمان کوتاه و در حد وسیع، تنها با استفاده از ابزارهایی چون شبکه‌های اجتماعی تردید داشته باشد. وجود صفحات، پست وال[1] و فیدهای[2] متعدد با موضوع اغتشاشات دی‌ماه ۹۶ ج.ا.ا. و شمار قابل‌توجه اعضای آن‌ها، دلالت بر نقش وسیع شبکه‌های اجتماعی و پیام‌رسان‌هایی چون تلگرام، فیس بوک و توییتر در این حوادث داشت. هرچند این اخبار و اطلاعات بسیار ضد و نقیض و بی‌نظم و منشأ تولید شایعه و پراکندن دروغ بود؛ اما چالش امنیت ملی محسوب می‌شد. این چالش به‌ویژه از سویی اختلاف میان دولت و مردم و کاهش مشروعیت دولت از دیدگاه معترضان بوده که به عقیده باری بوزان چنین تنشی می‌تواند منشأ بزرگ‌ترین ضعف و آسیب‌پذیری باشد(بوزان،۱۳۷۸: ۹۹)

### ه) جاسوسی و پایش اطلاعات کاربران:

اطلاعات، منبع اصلی قدرت است. انسان به هراندازه که از اطلاعات و آگاهی بهره‌مند باشند، به همان اندازه قادر است در عرصه‌های مختلف سیاسی، اجتماعی، فرهنگی و نظایر آن، ایفای نقش کند. شبکه‌های اجتماعی بیرونی اطلاعات حریم خصوصی کاربران را در اختیار دولت‌ها و شرکت‌های تجاری و جاسوسی قرار می‌دهند و این اطلاعات توسط کشور مبدأ مورد تجزیه‌وتحلیل قرار می‌گیرد. به‌طور مثال هنگام نصب برنامه بر روی دستگاه تلفن همراه از کاربر تأیید چند موضوع را طلب می‌کند: اول اینکه به شماره تلفن‌های او دسترسی داشته باشد و آن‌ها را به اشتراک بگذارد. عکس‌ها و پیام‌ها و پیج‌های او را هم به اشتراک می‌گذارد و تأیید همه این‌ها را قبل از نصب برنامه می‌گیرد و اگر کاربر یکی از موارد را هم قبول نکند برنامه نصب نمی‌شود. اطلاعات دفترچه تلفن گوشی همراه با تکنیک داده‌کاوی[3] و باهوش مصنوعی[4] باهم تلفیق‌شده و یک شبکه‌ای از ارتباطات ایجاد می‌شود و با جمع‌آوری اطلاعات مشخص می‌شود که صاحب

1. Post wall
2. Feeds
3. data mining
4. Artificial Intelligence

تلفن همراه با چه کسانی ارتباط دارد و این افراد که با او در ارتباط هستند چه ویژگی‌ها و مشخصاتی دارند. به بیان رابینسون واپایش اطلاعات در عصر جدید، اهرم اصلی قدرت بازیگران جهانی، ملی و محلی است. (حسینی، ۱۳۹۰: ۱۱)

## و) تهدید حریم خصوصی کاربران

حریم، قلمرویی است که دارنده‌اش نمی‌خواهد دیگران بدون اجازه‌اش از آن آگاهی یابند یا با بهره‌برداری از آن آگاهی اقدامی کنند.

حریم می‌تواند مکان، سند یا جسمی باشد که از دستیابی به اطلاعات و داده‌های درون آن به طرق ناروا باید جلوگیری شود، حتی اگر تهی باشد؛ چراکه حریم اشخاص، به‌نوعی باحیثیت و آبروی افراد در ارتباط است. اشخاص هم از طریق حریم و هم از طریق حرمت می‌توانند حق باحیثیت خود را استیفا کنند؛ لذا بعضی از امور در دایرهٔ حریم اشخاص، شاید مستقلاً حرمت شخص را مورد تعرض قرار ندهد؛ اما ممکن است زمینهٔ داوری‌هایی را فراهم آورند که به هتک حرمتش بینجامد. (انصاری،۱۳۹۱: ۳۸-۱۱) برخی، حریم خصوصی اطلاعات را حوزه‌هایی از زندگی اشخاص دانسته که از سوی دیگران تسخیرناپذیر است. در تعریف این حق باید توجه داشت که قلمرو این حق، ناظر به مسائلی است که صرفاً در حیطهٔ موضوعات شخصی افراد بوده و ذی‌حق به‌هیچ‌وجه تمایلی به افشای آن نداشته باشد و نیز افشاشدن بخشی از اطلاعات خصوصی افراد و نقض حریم شخصی آن‌ها باعث نمی‌شود که افشای بقیهٔ اطلاعات یا انتشار مجدد بخش فاش شده را مجاز محسوب کرد. بحث حریم خصوصی در فضای مجازی، بحث حمایت از داده‌هاست و حق بر حریم خصوصی به اشخاص حقوقی نیز تسری می‌یابد؛ چراکه از حق بر داده‌ها برخوردارند، ازآنجاکه حق بر حریم خصوصی از حقوقی است که به‌نوعی تضمین‌کنندهٔ امنیت،آزادی، آسایش و کرامت شهروندان است، تدوین قوانین و مقررات شفاف و کارآمدی که بتواند از حریم خصوصی و داده‌های شخصی صیانت به عمل آورد و با ناقضین آن برخور د کند، از اهمیت ویژه‌ای برخوردار است؛ به‌نحوی‌که حتی دولت نیز نتواند جز در موارد مصرح قانونی، متعرض آن گردد.(رئیسی، قاسم‌زاده، ۱۳۹۹: ۱۲۶).

## مدل‌های قانون‌گذاری در فضای مجازی

### ۱) قانون‌گذاری ملی

در این روش، نهادهای قانون‌گذاری ملی نسبت به قانون‌گذاری و جرم‌انگاری در فضای مجازی اقدام می‌کنند. در این روش اولاً، نمی‌توان از جرم انگاری تمام جرائم در فضای مجازی، اطمینان خاطر داشت و ثانیاً، این روش می‌تواند موجب تعارض قوانین در فضای مجازی شده و اصل قانونی بودن جرم و مجازات و اصل منع مجازات مضاعف را تحت تأثیر قرار دهد. ازآنجاکه این روش، مستعد تصویب قوانین فراسرزمینی و انحصاری سازی فضای مجازی است، می‌تواند منجر به تصویب قوانین انسدادی[1] توسط کشورها برای جلوگیری از اعمال صلاحیت کشورهای خارجی شود. از سوی دیگر، عملکرد برخی کشورها ازجمله چین در قانون‌گذاری حداکثری، منجر به خودسانسوری در فضای مجازی شده است. قانون‌گذاری در فضای مجازی توسط مراجع ملی مبتنی بر چهار صلاحیت سرزمینی، شخصی، واقعی و جهانی است، که به‌صورت مختصر به آن پرداخته می‌شود: (افضلی و همکاران،۱۳۹۲: ۲۳۵)

### الف) صلاحیت سرزمینی

لازمه توسل به صلاحیت سرزمینی در فضای مجازی، وجود مرزهای دقیق است تا مقررات دولتی در حیطه آن عینیت یابد. یکی از معضلات صلاحیت سرزمینی در این فضا، ناپیدا بودن محل ارتکاب جرم در فضای مجازی است، که نمی‌توان محل وقوع جرم را شناسایی کرد. عدم امکان اجرای قواعد سنتی بر فضای مجازی از پیچیدگی‌های دیگر این فضاست.(افضلی و همکاران، ۱۳۹۲: ۲۳۵)

### ب) صلاحیت شخصی

اعمال صلاحیت شخصی در فضای مجازی، مستلزم احراز تابعیت مجرم یا بزه دیده است. شناسایی مجرم در این فضا منوط به تعیین شناسه‌ی اوست. درحالی‌که فرد به‌راحتی با استفاده از برنامه‌های رایانه‌ای، قادر به جعل شناسه‌ی خود است. همچنین، لازمه اعمال صلاحیت شخصی منفعل در این فضا، انجام تحقیقات در رایانه‌های واقع در خارج از کشور(ولو از راه دور)است که موجب نقض حاکمیت سرزمینی کشور محل اطلاعات خواهد شد. (ضیایی،شکیب نژاد،۱۳۹۵: ۲۳۲)

1. Blocking Laws

### ج) صلاحیت واقعی

اشکال اعمال صلاحیت واقعی این است که ضابطه دقیقی برای توسل به آن وجود ندارد. البته دست دولت‌ها برای اعمال صلاحیت واقعی کاملاً بازنیست و باید از اعمال موسع صلاحیت واقعی امتناع کرد. لذا در این زمینه لازم است میان اعمال صلاحیت واقعی و اصل آزادی اینترنت، موازنه‌ای عادلانه برقرار شود که درنتیجه آن، اعمال صلاحیت واقعی در فضای سایبر در چارچوب موازین حقوق بشری صورت پذیرد. دادگاه آلمان در قضیه توبن در رابطه با انکار هولوکاست توسط یک استرالیایی در تارنمایی در استرالیا، صلاحیت واقعی را اعمال کرد. همچنین طبق قانون میهن‌دوستی امریکا، اداره تحقیقات فدرال مجاز است با قرار قضایی، به پیام‌های پست‌های صوتی افراد، دسترسی داشته یا مقامات مجاز بدون رعایت الزامات قانون شنود، اطلاعات رایانه‌ای افراد را رهگیری کنند. (ضیایی، شکیب نژاد،۱۳۹۵: ۲۳۲)

### د) صلاحیت جهانی

صلاحیت جهانی، یکی دیگر از مبانی قانون‌گذاری در فضای سایبر است. برخی اقدامات در برخی مناطق، مورد ادعای صلاحیت هیچ دولتی نیست و لذا اعمال صلاحیت در خصوص آن‌ها نه‌تنها مداخله در حاکمیت دیگر دولت‌ها نیست، بلکه برای جلوگیری از تبدیل‌شدن آن منطقه به پناهگاه امن متخلفین و پرهیز از شکل‌گیری«سرزمین بی‌قانون[1]» لازم است. اقدامات مجرمانه در اینترنت در زمان حاضر از نمونه‌های این وضعیت است. ماده ۲۲ کنوانسیون جرائم سایبری شورای اروپا (کنوانسیون بوداپست[2]) جایگاه صلاحیت جهانی در فضای مجازی را تأیید می‌کند. مبانی صلاحیت جهانی برای برخی جرائم سایبری مانند تحریک به نسل‌کشی در معاهدات بین‌المللی موجود است و قوانین داخلی دولت‌ها، برخی جرائم سایبری را مشمول صلاحیت جهانی قرار داده‌اند. (کیلی‌گابل،۲۰۱۰: ۴۵)

### ۲) قانون‌گذاری بین‌المللی

روش قانون‌گذاری بین‌المللی با توجه به یکپارچگی اینترنت و مشکلات ناشی از قانون‌گذاری ملی مطرح شد (جلالی‌فراهانی، ۱۳۸۹: ۹۷)، این شیوه در بهترین شکل با انعقاد معاهدات بین‌المللی

1. Lawless Territory
2. Council of Europe Cybercrime Convention, Budapest, (Adopted 2001, Entered into Force 2004).

محقق می‌شود. کنوانسیون بوداپست مهم‌ترین کنوانسیون در خصوص جرائم سایبری است. با این‌حال، این کنوانسیون نمی‌تواند به‌عنوان معاهده‌ای جامع تلقی شود، چه آنکه اولاً، تمام جرائم سایبری را در برنمی‌گیرد و ثانیاً، این کنوانسیون صرفاً برای کشورهای اروپایی لازم‌الاجراست. درهرصورت، معاهدات منطقه‌ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهده اینترنتی در سطح بین‌المللی موردنیاز است (سولونگ[1]، ۲۰۱۰: ۵)، سازمان‌های بین‌المللی نیز در فرآیند بین‌المللی قانون‌گذاری در فضای سایبر، نقش قابل‌توجهی داشته‌اند. آنسیترال با تصویب قانون نمونه آنسیترال[2] نقش چشمگیری در هماهنگ‌سازی قوانین ملی کشورها درباره مسائل مربوط به تجارت الکترونیک داشته است. گروه هشت[3] در سال ۱۹۹۷ کمیته فرعی جرائم رایانه‌ای را برای مقابله با جرائم سایبری تأسیس و یک برنامه اقدام ده اصلی را در این رابطه تصویب کرد. مجمع عمومی سازمان ملل متحد در سال‌های ۲۰۰۰ و ۲۰۰۳ تلاش‌هایی برای امنیت اطلاعاتی و سایبری انجام داد. اتحادیه عرب به پیشنهاد ایالات‌متحده عربی، شورای همکاری خلیج‌فارس، سازمان کشورهای آمریکایی، سازمان همکاری و توسعه اقتصادسی، سازمان همکاری و اقتصادی آسیا اقیانوسیه و سازمان کشورهای مشترک‌المنافع نیز در یکسان‌سازی قواعد بین‌المللی تلاش‌هایی داشته‌اند. در این میان مهم‌ترین تلاش را اجلاس جهانی جامعه اطلاعات داشت که در سال ۲۰۰۳ در آن تشکیل سازمان بین‌المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد. اتحادیه بین‌المللی مخابرات، آژانس جهانی جرائم سایبری را باهدف ارائه پیشنهادهایی برای جرم‌انگاری سایبری بنیانگذاری کرد. (سولونگ، ۲۰۰۹: ۱۰)

### ۳) قانونگذاری خود انتظامی

ازنظر برخی حقوقدانان، به جهت ماهیت یکپارچه و فرامرزی فضای مجازی، قواعد سنتی صلاحیت، مناسب بافت اینترنت نبوده و بایستی برای اینترنت، حاکمیتی جداگانه به رسمیت شناخت. نتیجه این نگرش، شیوه خود انتظامی در قانون‌گذاری در فضای مجازی خواهد بود. در روش خود انتظامی به جای دولت‌ها، شرکت‌های سایبری یا مالکان تارنما ملزم به ایجاد محدودیت در فضای مجازی هستند. مهم‌ترین دلیل خود انتظامی فضای مجازی این است که فضای مجازی

1. Solange
2. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996.
۳. شامل؛ کانادا، فرانسه، آلمان، ژاپن، ایتالیا، امریکا، بریتانیا و روسیه.

برخلاف دولت‌ها، غیرمتمرکز و جهانی است. همچنین این روش، علاوه بر اینکه کارایی قانون‌گذاری ملی را داراست، به‌مراتب، ساده‌تر و ارزان‌تر بوده و به دلیل نقش پیشگیرانه این روش، از آمار جرائم در فضای مجازی نیز کاسته خواهد شد (مولی‌لاند،۲۰۱۳: ۱۶)، روش خود انتظامی در عمل با مشکلاتی روبه‌روست. اولاً، به دلیل حذف نهاد دولت به‌عنوان رکنی فرادستی، موجب هرج‌ومرج در فضای مجازی خواهد شد. ثانیاً، ازنظرحامیان«مشترکات ابتکاری»، الزام تأمین‌کنندگان خدمات اینترنتی به خودسانسوری، خلاقیت در محیط دیجیتال را تحت‌الشعاع قرار می‌دهد. لازمه‌ی اقدام نهادهای فنی و صاحبان تارنماها، داشتن پشتوانه قانونی توسط دولت‌هاست، درحالی‌که دولت‌ها در حال حاضر از این نظر حمایت نمی‌کنند. (اندریو ماریا ،۲۰۰۷: ۷۷)

### ۴) قانون‌گذاری مختلط

هر یک از سه شیوه قانون‌گذاری فوق‌الذکر در خصوص مشروعیت یا اجرا، اشکالاتی دارد. قانون‌گذاری بین‌المللی از بالاترین سطح اجرا و پایین‌ترین سطح مشروعیت برخوردار است. خود انتظامی دارای بالاترین سطح مشروعیت و پایین‌ترین سطح اجراست. قانون‌گذاری ملی، حالتی بینابین بوده و همواره با ضعف نسبی در اجرا و مشروعیت مواجه است. انتخاب روشی مختلط، زمینه را برای حل معضلات ناشی از مشروعیت و اجرا و همچنین نیل به تفاهم میان همه بازیگران فعال در فضای سایبر بازخواهد کرد. در این خصوص همکاری بین‌المللی برای یکسان‌سازی حقوقی لازم است. کنوانسیون بوداپست به شیوه مختلط توجه داشته و در مادۀ ۲۳ به همکاری بین‌المللی و در ماده ۱۱ به قانون‌گذاری متقابل توجه کرده است. (ضیایی،شکیب نژاد، ۱۳۹۵: ۲۳۸)

## قواعد حاکم بر فضای مجازی در حقوق ایران

### الف) رویکرد ایران در قانون‌گذاری در فضای مجازی

در سند چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ بر تعامل سازنده و متوازن در روابط بین‌الملل و در سیاست‌های کلی نظام در فضای تولید و تبادل اطلاعات کشور، بر ارتقاء سطح همکاری‌های بین‌المللی در زمینه امنیت فضای مجازی تأکید شده است. رویکرد جمهوری اسلامی ایران برای کنترل و مدیریت فضای مجازی مبتنی بر روش قانون‌گذاری ملی است. پس از ابلاغ «سیاست‌های کلی شبکه‌های اطلاع رسانه‌ای رایانه‌ای» از سوی مقام معظم رهبری(نامه

شماره۱۰۷۲/۱ تاریخ ۱۳۸۰ /۰۳/۱۳ دفتر مقام معظم رهبری)، شورای عالی انقلاب فرهنگی «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» را در سال ۱۳۸۰ به تصویب رسانید. همچنین مقررات پراکنده‌ی دیگری مانند آیین‌نامه نحوه اخذ مجوز و ضوابط فنی نقطه تماس بین‌المللی، آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا(ISP)[1]، مصوبات کمیسیون تنظیم مقررات ارتباطات درسال ۱۳۸۴، قوانین پنج‌ساله توسعه و قانون تجارت الکترونیک نیز وجود دارد، لیکن نخستین قانون جامع و متمرکز در ایران، قانون جرائم رایانه‌ای، مصوب ۱۳۸۸و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ است (که در رأس آن رسیدگی به جرائم تهدیدکننده امنیت کشور بیان‌شده است). اگرچه رویکرد قوانین داخلی ایران بر روش قانون‌گذاری ملی تکیه دارد، لیکن، نگرش انتقادی ایران به نحوهٔ مدیریت زیرساخت‌های سایبری در سازمان اینترنتی، انتصاب اسامی وکدهای رقمی(آیکان)[2] مبیّن پذیرش روش قانون‌گذاری بین‌المللی در این عرصه از سوی ایران است. آیکان یکی از مراجع مهم در شیوه خود انتظامی در فضای مجازی است که درعین‌حال از قوانین داخلی آمریکا تبعیت می‌کند. انتقاد دولت‌ها به آیکان، مربوط به اساسنامه این سازمان است که طبق آن، وزارت بازرگانی آمریکا دارای حق وتو بر تصمیمات سازمان بوده و تغییرات سازمان باید به تصویب دولت آمریکا برسد (ریبیس کیسی، ۲۰۰۸: ۲)[3]، بدین‌جهت در یادداشت ایران بر پیش‌نویس چهارم گزارش دبیر کل اتحادیه بین‌المللی مخابرات چنین آمده است:«مهم‌ترین بخش‌های اینترنت که مربوط به سیاست عمومی است تحت حاکمیت همکاری میان دولت‌ها یا سازمان‌های بین‌المللی نیست، بلکه تحت حاکمیت دولت‌های انفرادی است...، موضوع فاجعه‌بار آن است که برخی دولت‌ها کنترل اساسی بر بخش‌های حیاتی اینترنت دارند.» حمایت ایران از نتایج اجلاس اتحادیه بین‌المللی مخابرات که منجر به ایجاد فشار بر ایالات‌متحده و تغییر اساسنامه آیکان شد، مؤید عدم مخالفت ایران با شیوه قانون‌گذاری بین‌المللی عادلانه است. رأی مثبت ایران به سند اصلاحی اتحادیه بین‌المللی مخابرات در سال ۲۰۱۲ نیز بیانگر حمایت از رویکرد بین‌المللی است. رویکرد ایران در کنار کشورهای دیگری نظیر چین و کوبا در تقابل با سیطره ایالات‌متحده بر این فضا، مبتنی بر مشارکت بیشتر سازمان ملل و دولت‌ها در مدیریت کلان فضای سایبر است. (جان‌بری[4]،۲۰۰۶: ۱۰)

1. Internet Service Provider
2. Internet Corporation for Assigned and Numbers (ICANN)
3. Rebecca E. Casey
4. John W. Berry

امروزه طرح شبکه ملی اطلاعات[1] و مجموعه قوانین حاکم بر فضای سایبر در ایران، نشان‌دهنده رویکرد ملی ایران به قانون‌گذاری در فضای سایبر است. بااین‌حال، اعمال روش قانون‌گذاری ملی در قوانین داخلی و پذیرش روش بین‌المللی در مدیریت آینده این فضا حاکی از تمایل ایران به اعمال روش مختلط در قانون‌گذاری در این فضا است. (حسینی و ظریف منش، ۱۳۹۶: ۴۴)

## ب) اقدامات حقوقی ایران در قانون‌گذاری در فضای مجازی

وقوع جرم رایانه‌ای به‌تدریج از دهه ۱۳۷۰ در ایران آغاز شد. سوءاستفاده از رایانه برای ارتکاب جرائم سنتی، به‌کارگیری ویروس‌ها از طریق توزیع حامل‌های واژه آلوده به ویروس، سوءاستفاده‌های مالی و تکثیر غیرمجاز نرم‌افزارهای رایانه‌ای ازجمله جرائم رایانه‌ای‌اند که در مقیاس بسیار اندک در دهه ۱۳۷۰ واقع شده و با قوانین کیفری مرسوم در آن زمان مورد رسیدگی قرار گرفتند؛ ازجمله این رسیدگی‌ها صدور دادنامه مورخه ۳/ ۴/ ۸۸ – شعبه۶۵ کیفری ۲ در خصوص شکایت یک شرکت نرم‌افزاری از شرکت دیگر می‌باشد که نمونه‌ایی از آرایی است که بیانگر به‌کارگیری قوانین کیفری سنتی در خصوص جرائم رایانه‌ای است.اولین اقدام قانون‌گذار ایران در سال ۱۳۷۹ در برابر برخی از جرائم رایانه‌ای و با الحاق تبصره ۳ به ماده ۱ قانون مطبوعات صورت پذیرفته است. همچنین قانون‌گذار در سال ۱۳۸۲، از رهگذر تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ مجلس شورای اسلامی، در ماده ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و انشای غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آن را ندارند، سرقت یا تخریب حامل‌های داده و سوءاستفاده‌های مالی از طریق به‌کارگیری رایانه(کلاه‌برداری و اختلاس) از جانب نظامیان جرم انگاشته شده و مرتکب حسب مورد به مجازات‌های مقرر محکوم می‌شد.

قانون جرائم رایانه‌ای ایران در پنجم خرداد ۱۳۸۸ به تصویب و پس از تأیید شورای نگهبان در هفتم تیرماه همان سال، در تاریخ ۱۰ تیرماه سال ۱۳۸۸ توسط رئیس‌جمهور برای اجرا ابلاغ گردید. در خصوص جرائم فضای مجازی مربوط به امنیت ملی در ایران، مرکز بررسی تهدیدات سایبری

۱. تبصره ۲ ماده ۱۶ قانون برنامه پنجساله توسعه و مصوبه جلسه پانزدهم شورای عالی فضای مجازی در تاریخ ۹ شبکه ملی اطلاعات و راهکارهای ایجاد آن را تبیین کردهاند.

سپاه پاسداران انقلاب اسلامی به‌منظور شناسایی و انهدام جرائم سازمان‌یافته اجتماعی، اقتصادی، جاسوسی، فرهنگی و تروریستی در فضای مجازی و ساماندهی و هدایت فعالیت‌ها در اینترنت جهت مقابله با تهدیدات فضای مجازی،تمام فعالیت‌های معاند را رصد و با توجه به ماهیت تهدیدات، اقدامات لازم ازجمله نابودی سرورها، عملیات نفوذ و هک سایت‌های غیراخلاقی و موردحمایت غرب و ناامن کردن فضا برای معاندان و شناسایی و دستگیری مجرمان در داخل و خارج از کشور را انجام می‌دهد.(شریعت پناه،۱۳۸۹: ۱۶)، قرارگاه دفاع سایبری نیز در راستای سیاست‌های کلی در بخش امنیت فضای تولید و تبادل اطلاعات است که توسط مقام معظم رهبری ابلاغ‌شده است که ازجمله مأموریت‌های آن عبارت است از رصد تهدیدات سایبری علیه زیرساخت‌های امنیت ملی کشور، اجرایی شدن سیاست‌های نظام در بخش فتا، اعلام هشدارهای ملی در برابر تهدیدات امنیتی کشور، ایمن‌سازی زیرساخت‌های کشور نسبت به تهدیدات سایبری و ایجاد توان بازدارندگی در حوزه سایبری و نهایتاً تدوین سند دفاع غیرعامل و تهیه برنامه جامع دفاع سایبری. شورای عالی فضای مجازی هم به دستور حضرت آیت‌الله خامنه‌ای رهبر معظم انقلاب در تاریخ ۱۳۹۰/۱۲/۱۷تشکیل و تحت ریاست رئیس‌جمهور می‌باشد. در این دستور آمده است:«گسترش فزآینده فناوری‌های اطلاعاتی و ارتباطاتی، شبکه جهانی اینترنت و آثار چشمگیرآن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه‌جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به‌منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطه کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به وجود آید. در همین راستا شورای عالی فضای مجازی کشور با اختیارات کافی به ریاست رئیس‌جمهور تشکیل می‌گردد و لازم است به کلیه مصوبات آن ترتیب اثر قانونی داده شود (حسینی و ظریف منش، ۱۳۹۶: ۴۶)

قانون مجازات اسلامی مصوب ۱۳۹۲ یکی دیگر از مراجعی است که در آن در خصوص جرائم فضای مجازی که تهدیدکننده امنیت می‌باشد، بحث گردیده است. با عنایت به این‌که رویکرد ایران در قانون‌گذاری فضای مجازی، رویکرد قانون‌گذاری ملی است، در قانون مجازات اسلامی در خصوص صلاحیت، اصل بر صلاحیت سرزمینی می‌باشد. تقریباً در تمام مواد قانون

جرائم رایانه‌ای و مواد مرتبط در قانون آیین دادرسی کیفری، عبارت« هرکس» بدون توجه به تابعیت مرتکب به کار رفته است. هرچند معیار صلاحیت سرزمینی در جرائم گوناگون سایبری متفاوت است، معیار صلاحیت سرزمینی در ماده ۱ (دسترسی غیرمجاز) ، ماده ۲ (شنود غیرمجاز) و ماده ۳ (جاسوسی رایانه‌ای) قانون جرائم رایانه‌ای، معیار وقوع«سامانه‌های رایانه‌ای» در قلمرو ایران است. بند (الف) ماده۶۶۴ قانون آیین دادرسی کیفری «ذخیره اطلاعات» در قلمرو ایران را نیز مشمول صلاحیت سرزمینی ایران قرار می‌دهد. صلاحیت واقعی در ماده ۵ قانون مجازات اسلامی آمده است و صراحتاً اقدام علیه امنیت داخلی یا خارجی را در حیطه صلاحیت ایران می‌داند. همچنین مطابق بند (پ) ماده ۶۶۴ قانون آیین دادرسی کیفری، ارتکاب جرم در خارج از ایران علیه سامانه‌ها یا تارنماهای مورداستفاده قوای سه‌گانه، نهاد رهبری، نمایندگی‌های رسمی دولت، نهادهای ارائه‌کننده خدمات عمومی و علاوه بر این، حمله گسترده به تارنما در خصوص صلاحیت جهانی، ماده ۱ قانون مجازات اسلامی، جرائمی را که طبق عهدنامه‌ها و مقررات بین‌المللی تحت صلاحیت جهانی قرارگرفته در صلاحیت تمامی کشورها و ازجمله ایران می‌داند. در قوانین ایران در این خصوص صراحتی وجود ندارد.اهای مرتبه بالای کدکشوری را در شمول صلاحیت محاکم ایران کرده است. (ضیایی،شکیب نژاد،۱۳۹۵: ۲۴۱)

## نتیجه‌گیری

حاکمیت ملی، در جغرافیای سیاسی، یکی از مفاهیم بنیادی در مطالعه‌ی حکومت‌ها می‌باشد. امنیت ملی، ناشی از شناسایی عوامل موثر درکاهش یا افزایش توان حکومت‌ها در اعمال حاکمیت ملی محسوب، و این مهم، همیشه از دغدغه های اصلی دولت ها برای حکمرانی موثر و مفید بوده است.

فضای مجازی و فناوری‌های وابسته به آن، یکی از مهم‌ترین منابع قدرت در هزاره سوم محسوب می گردد. با گسترش روز افزون فناوری اطلاعات و تعریف نو، از تهدیدهای نوظهور در بستر فضای مجازی، ضمن قائل شدن ابعاد چند وجهی برای امنیت ملی، دیگر نمی‌توان امنیت ملی را همانند گذشته در ارتباط با مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد. تهدیدات در حوزه فضای مجازی بنا به دلایلی از جمله؛ غیر ملموس بودن، محرک بودن، هدف قراردادن

کیفیت زندگی شهروندان، نداشتن مرز جغرافیایی، بی‌مفهوم بودن زمان و مکان، نامتقارن بودن، فقدان هویت مخاطبین، برخورداری از جذابیت‌های کافی و ...، تهدیداتی چند بعدی و چند سویه بوده و به همین دلیل آسیب‌رسانی آن بر مراکز هدف، بسیار بالا می‌باشد. پر واضح است که اینگونه تهدیدات را نمی‌توان به شیوه‌های سنتی همانند به‌کارگیری ارتش و نیروی قهری مهار کرد.

قانونگذاری از الزامات بنیادین و اساسی در راستای اداره بهینه جامعه و برقراری نظم و امنیت که هدف غایی حاکمیت می‌باشد، محسوب می‌گردد. دولت‌ها موظف هستند از طریق کنترل و اعمال نظارت، در جهت حفظ حقوق شهروندان و نظم عمومی تلاش نموده و با تدوین قوانین مناسب و موثر، نسبت به ایمن نگه داشتن بستر فضای مجازی، امنیت شهروندان در همه حوزه های مربوط به آن تأمین نمایند. گسترش روز افزون فناوری ارتباطی و در رأس آن فضای مجازی و همچنین تهدیدات متصور در بستر آن، می طلبد تا سیاست‌گذران و مسئولین امر در حوزه‌ی تهدیدات، درک واقع بینانه از تهدیدات امنیتی بالاخص در کارکردهای امنیت ملی داشته و نسبت به این مهم، از تمام ظرفیت های موجود در بستر جامعه استفاده نموده و با نگاه فراملی نسبت به صدور قوانین کارا و بازدارنده اقدام نمایند.

## پیشنهادات

در سند چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ بر تعامل سازنده و متوازن در روابط بین‌الملل و در سیاست‌های کلی نظام در فضای تولید و تبادل اطلاعات کشور، بر ارتقاء سطح همکاری‌های بین‌المللی در زمینه امنیت فضای مجازی تأکید شده است. با توجه به رویکرد جمهوری اسلامی ایران برای کنترل و مدیریت فضای مجازی، که مبتنی بر روش قانون‌گذاری ملی است، باید توجه داشت که در این روش اولاً، نمی‌توان از جرم انگاری تمام جرائم در فضای مجازی، اطمینان خاطر داشت و ثانیاً، این روش می‌تواند موجب تعارض قوانین در فضای مجازی شده و اصل قانونی بودن جرم و مجازات و اصل منع مجازات مضاعف را تحت تأثیر قرار دهد.

با عنایت به منویات مقام معظم رهبری در خصوص حکمرانی دولت در فضای مجازی مبنی بر«تغییر رویکرد جمهوری اسلامی ایران از مواجهه انفعالی به مواجهه فعال، خردمندانه و مبتکرانه»،

عملکرد دولت در خصوص مدیریت و کنترل فضای مجازی، نیاز به هماهنگی و پیروی فعال از سند چشم انداز ۱۴۰۴ در این حوزه، به منظور تأمین حداکثری امنیت ملی می‌باشد.

دارا بودن گفتمان امنیتی مشترک در بین قانونگذاران و حاکمان، پرهیز از اقدامات جزیره‌ایی و مسکنی، مسئولیت‌پذیری دولت در سیاستگذاری علمی و عملی، مد نظر قرار دادن جوانب امر و بهره‌گیری از بسترهای قانونی موثر و هوشمند، شرط اصلی تحقق بیشترین منافع و کمترین آسیب‌ها از فضای مجازی در حوزه امنیت ملی محسوب می‌گردد. ایجاد مرکز نظارت و سیاستگذاری در حوزه فضای مجازی، تحت نظر بالاترین مرجع اجرائی و مدیریتی کشور، ایجاد مرکز مطالعات در حوزه فضای مجازی، در این راستا می تواند کمک بسیار شایانی به سیاستگذاران و مراجع قانونگذاری در این حوزه بنماید.

با توجه به ماهیت فراملی بودن تهدیدات در فضای مجازی و همچنین دولت محور نبودن امنیت، به طور قطع، برای مقابله و پیشگیری از وقوع آن، تلاش دولت‌ها به تنهایی کافی نبوده و همکاری مؤثر و همه‌جانبه دولت‌ها در عرصه بین‌المللی را می‌طلبد. امنیت ملی مفهومی فراگیرو مشترک در بین کشورها بوده و محصول تلاش قانونگذاران و حکمرانانی است که آن را کعبه آمال خود در عرصه حکمرانی می‌دانند.

# فهرست منابع

قرآن کریم.

آرزمی، علی و همکاران،(۱۳۹۷)، دولت، فضای مجازی و آینده پژوهی پروبلماتیک های بازتولید قدرت در ایـران پس از انقلاب، تهران، فصلنامه علمی پژوهشی پژوهشنامه انقلاب اسلامی، شماره ۲۶.

آزر چونگ این مون، ادوارد ای، (۱۳۷۹)، گفتاری دربـاره امنیـت ملـی، فصـلنامه امنیـت ملـی. تهران،پژوهشـکده مطالعات راهبردی.

آشوری داریوش،(۱۳۸۴) دانشنامه سیاسی،تهران.

آلتوسر، لویی (۱۳۹۲)، ایدئولوژی و سازو برگ های ایدئولوژیک دولت، ترجمه ی روزبه صدر آرا، تهـران: نشـر چشمه.

ابن فارس، ابوالحسین احمد بن زکریا(۱۳۶۳-۱۴۰۴ )؛ معجم مقایس اللغة، عبدالسلام محمد بن هارون، قـم، دفتـر تبلیغات اسلامی قم.

افضلی، رسول ، قالیباف، محمدباقر و احمدی فیروزجائی، میثم ،(۱۳۹۲)، تبیـین تحـولات مفهـوم مـرز در فضـای سیاسی مجازی، پژوهش‌های جغرافیای انسانی، دوره ۴۵ ، شماره ۱.

افتخاری، اصغر،(۱۳۸۲)، استراتژی ملی برای تأمین امنیت در فضای مجازی، پژوهشکده مطالعات راهبردی.

انصاری، باقر(۱۳۸۶)؛ حقوق حریم خصوصی، تهران، نشر سمت.

انصاری، باقر (۱۳۹۱ )، حقوق حریم خصوصی، تهران: سازمان مطالعه و تدوین کتب علوم انسانی (سمت).

انصاری، باقر،(۱۳۹۳)، حقوق ارتباط جمعی، چاپ هفتم، تهران، انتشارات سمت.

باستانی، برومند،(۱۳۸۶)، جرایم کامپیوتری و اینترنتی، جلوه ای نوین از بزهکاری، چاپ سوم، تهران، انتشارات بهنامی.

بشیری، عباس،(۱۳۸۸)، روزنامه جام جم، شماره ۲۵۳۶ به تاریخ ۸۸/۱/۲۹، صفحه ۱۰ سیاسی.تهران.

بهزادی، حمید(۱۳۶۹)،اصول روابط بین الملل و سیاست خارجی، تهران، دهخدا.

پاسبان، ابوالفضل، (۱۳۹۳)، بررسی عوامل موثر در بهره‌گیری سـپاه از بازنشسـتگان در اسـتان خراسـان رضـوی و ارائه راه کار مناسب، تهران، دانشگاه جامع امام حسین علیه السلام.

پاسبان، ابوالفضل(۱۳۹۵)، ژئوپلتیک ترکمنستان و تأثیر بر امنیت ملی ج.ا.ا، تهران، فصلنامه سیاست دفاعی، شماره ۹۶.

پالیزبان، محسن،(۱۳۹۴)، بررسی رابطه اینترنت و امنیت ملی ج.ا.ا، فصلنامه سیاست، دوره ۴۵، شماره۳.

تاجیک، محمدرضا(۱۳۸۱)، مقدمه‌ایی بر امنیت ملی ج.ا.ا، رهیافت ها و راهبردها، جلد۱،تهران، فرهنگ لقمان.

تقی‌زاد، مهرداد، (۱۳۹۶)، مطالعه تطبیقی نظام حقوقی حاکم بـر فضـای سـایبری، فصـلنامه مطالعـات بـین المللـی پلیس، شماره ۳۱.

حسینی، حسین،(۱۳۹۰)، جنگ نرم و شبکه‌های اجتماعی مجازی، قابل دسترسی در migna.ir

جفریس، دیوید؛(۱۳۸۱) فضای مجازی؛ ترجمهٔ داود شعبانی داریانی؛ تهران :دلهام.
جلالی فراهانی، امیر حسین، (۱۳۸۹)، درآمدی بر آیین دادرسی کیفری جرایم سایبری، انتشارات خرسندی.
چگنی زاده، غلامعلی، ( ۱۳۷۹)، رویکردی نظری به مفهوم امنیت ملی در جهان سوم، تهران، مجله سیاست خارجی، سال۴، شماره ۱.
حافظ نیا محمدرضا و دیگران،(۱۳۸۲)، تحلیل مبانی جغرافیایی قدرت ملی ج.ا.ا، نشریه علوم جغرافیایی دانشگاه تربیت معلم.
حسینی،حسین،(۱۳۹۰)، جنگ نرم و شبکه‌های اجتماعی مجازی، قابل دسترسی در migna.ir.
حسینی،پرویز،ظریف‌منش،(۱۳۹۲)، مطالعه تطبیقی ساختار دفاع سایبری کشورها، فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین(علیه السلام)، سال دوم، شماره ی ۵.
خانیکی، هادی و بابائی، محمود، (۱۳۹۰)، فضای سایبر و شبکه‌های اجتماعی، فصلنامه مطالعات جامعه اطلاعاتی، دوره اول، شماره ۱.
دفتر مقام معظم رهبری، نامه شماره۱۰۷۲/۱ تاریخ ۰۳/۱۳/ ۱۳۸۰.
رامک، مهراب و همکاران، (۱۳۹۷)، ارائه الگوی راهبردی همکاری بین المللی برای ارتقاء امنیت فضای مجازی و ...، تهران، ف .امنیت ملی، سال نهم، شماره ۳۳.
رییسی دزکی، لیلا، قاسم زاده لیاسی، فلور،(۱۳۹۸)، چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر، تهران، مجله حقوقی دادگستری، شماره ۱۱۰.
سلطانی نژاد، احمد(۱۳۸۶)، کاربرد فناوری اطلاعات در سیاست، جزوه درسی دکتری، دانشکده حقوق و علوم سیاسی دانشگاه تهران.
شهباز قهفرخی،سجاد، مسعودیان،مصطفی(۱۳۹۱)، حمایت از حریم خصوصی اشخاص از منظر آیات و روایات، دوفصلنامه تخصصی پژوهش‌های میان رشته‌های قرآن کریم، سال سوم، شماره دوم.
شریعت پناه، رضا،(۱۳۸۹)،فضای مجازی،تهران، نشریه پیام انقلاب، شماره۳۶.
ضیایی،سید یاسر، شکیب نژاد، احسان،(۱۳۹۵)، قانونگذاری در فضای سایبر؛ رویکرد حقوق بین‌الملل و حقوق ایران،مجله حقوقی بین‌المللی، شماره ۵۷.
طریحی، فخرالدین(۱۴۱۶)؛ مجمع البحرین، تهران، کتابفروشی مرتضوی.
عالمی، حمزه،( ۱۳۹۱)، )، نقش شبکه‌های اجتماعی مجازی در جنگ نرم، فصلنامه مطالعات سیاسی روز، سال یازدهم، شماره ۴۴.
عصاریان نژاد، حسین،(۱۳۸۷)، جوششی بر امنیت ملی، تهران: دانشکده علوم و فنون فارابی.

فتحی، یونس، شاهمرادی، خیراله، (۱۳۹۵)، گستره و قلمرو حریم خصوصی در فضای مجازی،مجله حقوقی دادگستری، سال ۸۱، شماره نود و نهم، پاییز ۱۳.

.فیسک، جان (۱۳۸۱)، فرهنگ و ایدئولوژی؛ ارغنون شماره‌ی۲۰ فرهنگ وزندگی روزمره ۲، تهران، سازمان چاپ و انتشارات.

.قناد، فاطمه، علیقلی، امیره،( ۱۳۹۹)، مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی، دوفصلنامهٔ حقوق قراردادها و فناوریهای نوین، دورهٔ اول، شمارهٔ ۱، بهار و تابستان ۱.

.کاستلز، مانوئل (۱۳۸۰)، عصر اطلاعات، اقتصاد، جامعه و فرهنگ، ترجمه؛ احد علیقلیان، افشین خاکباز و حسن چاوشیان، تهران،انتشارات طرح نو.

.کیان خواه، احسان،(۱۳۹۷)، چالشهای راهبردی حکمرانی با گسترش فضای سایبر، تهران، فصلنامه علمی امنیت ملی، سال نهم، شماره ۳۴، زمستان ۱۳۹۸.

.گنجی، علیرضا، امنیت شبکه: چالشها و راهکارها، مرکز اطلاعات و مدارک علمی ایران، علوم اطلاع رسانی، دورهٔ ۱۸ ، شماره ۳ و ۴.

.مارتین، لی.نور.جی؛ (۱۳۸۲)، چهره جدید امنیت در خاورمیانه، ترجمه قدیر نصیری، تهران: مرکز پژوهشکده مطالعات راهبردی.

.مایل افشار، فرحناز، عزتی، عزت ا...،(۱۳۸۹)، تحلیلی بر نقش قدرتهای مداخله گر در خلیج فارس و تأثیر آن بر امنیت جمهوری اسلامی ایران، فصلنامه جغرافیایی سرزمین، علمی – پژوهشی، سال هفتم، شماره ۲۶.

.مرکز بررسی های استراتژیک ریاست جمهوری،(۱۳۹۹)، گزارش نشست چهارم حکمرانی فناوری و فضای مجازی، شماره مسلسل۵۶۶.

.مکین لای، رابرت و آر.دی. و آر. لیتل، ( ۱۳۸۰ ): امنیت جهانی رویکردهای و نظریه ها، ترجمه اصغر افتخاری، تهران: مرکز پژوهشکده راهبردی.

.ندری،غلامرضا و همکاران،(۱۳۹۸)، بررسی نقش سیاسی – امنیتی شبکه‌های اجتماعی مجازی بر امنیت ملی ج.ا.ا.، فصلنامه پژوهش های حفاظتی امنیتی دانشگاه جامع امام حسین(علیه السلام)، سال هشتم، شمارهٔ ۲۹.

amniati.hormozgan.ir.

.Stein Schjølberg and Solange Ghernaouti-Hélie, A Global Protocol on Cybersecurity and Cybercrime, Cybercrimedata, Oslo, 2009, p. i.

.Solange Ghernaouti-Hélie, "We Need a Cyberspace Treaty: Regional and Bilateral Agreements Are Not Enough", I
nter Media, vol. 38, Issue 3, 2010, p. 5.

Bell, David (2001), an introduction to cyberculturse, USA, Routledge..

Andrew D. Murray, The Regulation of Cyberspace, Routledge Cavendish, Oxon, 2007, pp. 76-77 & 124..

Molly Land, "Toward an International Law of the Internet", New York Law School Legal Studies, vol. 5, 2013, p. 16.

Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law, vol. 43, Issue 1, 2010, p. 45.

John W. Berry, "The World Summit on the Information Society (WSIS): A Global Challenge in the New Millennium", Network of Illinois Learning Resources in Community Colleges, vol. 56, 2006, p. 10..

Rebecca E. Casey, "ICANN or ICANN't Represent Internet Users", Faculty of the Virginia Polytechnic Institute and State University, Virginia, 2008, pp. 1-2.

www.alef.ir
www.savaderesane.ir