

## رابطه شاخص‌های جنگ نرم و ماهیت جرم در فضای سایبری

فرزین فولادی<sup>۱</sup>، رضا قیاسی<sup>۲</sup> و عبدالله هندیانی<sup>۳</sup>

تاریخ دریافت: ۱۳۹۷/۰۲/۰۱

تاریخ پذیرش: ۱۳۹۷/۰۶/۱۵

### چکیده

**زمینه و هدف:** جنگ نرم، کاربرد ابزارهای نرم علیه جامعه خاص با هدف تاثیر بر فرهنگ، ارزش‌ها، باورها و اعتقادات به منظور استحاله آن و جایگزینی نظام فرهنگی موردنظر است، در این راستا هم جرایمی در فضای سایبری صورت می‌گیرد. هدف از پژوهش حاضر بررسی ارتباط میان جنگ نرم و ماهیت جرم در بین دانشجویان دانشگاه علوم انتظامی امین است. تاثیری که جنگ نرم در هر یک از ابعاد فرهنگی، اجتماعی و سیاسی جامعه گذاشته و نقش آن در ایجاد جرم در فضای سایبری مورد بررسی قرار می‌گیرد.

**روش:** پژوهش حاضر از نظر هدف کاربردی و از نظر روش توصیفی - تحلیلی است که به روش پیمایشی انجام شده است. برای گردآوری داده‌های مورد نیاز از پرسشنامه محقق ساخته استفاده شد. جامعه آماری این پژوهش کلیه دانشجویان دانشگاه علوم انتظامی امین است. نمونه مورد بررسی با استفاده از جدول کرجسی-مورگان، ۳۸۴ نفر براساس نمونه‌گیری تصادفی ساده محاسبه شد. برای تجزیه و تحلیل داده‌ها، از آزمون همبستگی اسپیرمن و آزمون رتبه‌ای فریدمن استفاده شد.

**یافته‌ها:** یافته‌های توصیفی پژوهش موید آن است که بیشترین افراد پاسخ‌دهنده از نظر جنسیت مرد؛ از نظر تحصیلات، کارشناسی و از نظر سن، بین ۲۰-۳۰ سال بودند. همچنین نتایج آمار استنباطی و تجزیه و تحلیل داده‌ها نشان داد که جنگ نرم از طریق سست کردن ابعاد فرهنگی، اجتماعی و سیاسی افراد جامعه با وقوع جرم در فضای سایبری در سطح اطمینان ۹۹ درصد رابطه معناداری دارد. همچنین ضریب همبستگی رابطه سستی ابعاد فرهنگی جامعه از طریق جنگ نرم با وقوع جرم در فضای سایبری ۰/۵۰۸ به دست آمد که دارای بیشترین رتبه در نزد پاسخ‌گویان بود.

**نتایج:** نتایج پژوهش نشان داد که جنگ نرم از طریق سست کردن ابعاد فرهنگی جامعه بیشترین رابطه را با وقوع جرم دارد. بعد از ابعاد فرهنگی، به ترتیب ابعاد اجتماعی و سیاسی با وقوع جرم رابطه دارند. نتایج پژوهش نشان داد که فضای سایبر، بهترین ابزاری است که جنگ نرم از طریق آن بر افراد نفوذ کرده و موجب سست کردن اعتقادهای فرهنگی، اجتماعی و سیاسی جامعه می‌شود.

**کلیدواژه‌ها:** شاخص‌های جنگ نرم، قدرت نرم، فضای سایبری، ماهیت جرم

□ **استناد:** فولادی، فرزین؛ قیاسی، رضا؛ هندیانی، عبدالله (پاییز، ۱۳۹۷). رابطه شاخص‌های جنگ نرم و ماهیت جرم در فضای سایبری.

فصلنامه پژوهش‌های مدیریت/انتظامی، ۱۳(۳)، ۵۰۵-۵۲۴.

۱. مربی گروه خدمات ترافیک، دانشکده علوم و فنون راهنمایی و راندگی، دانشگاه علوم انتظامی امین. رایانامه: frznfouladi@yahoo.com

۲. مربی گروه فتا، دانشکده علوم و فنون اطلاعات و آگاهی، دانشگاه علوم انتظامی امین. (نویسنده مسئول). رایانامه: rezaghiasi@rocketmail.com

۳. دانشیار گروه مدیریت راهبردی، دانشکده فرماندهی و ستاد، دانشگاه علوم انتظامی امین. رایانامه: hendiani.s1343@gmail.com

## مقدمه

وقوع انقلاب اسلامی ایران باعث بروز شرایط نوین و شکل‌گیری مناسبات جدید سیاسی و فرهنگی در منطقه و جهان شد، از این رو دشمنان نظام اسلامی انواع روش‌ها را برای مقابله با آن مورد آزمون قرار داده و پس از ناکامی در تقابل مستقیم، اقدام به تهاجم آشکار و جدیدی با عنوان جنگ نرم، برای مقابله با پیشرفت و گسترش انقلاب اسلامی در سطح منطقه‌ای و بین‌المللی کردند. جمهوری اسلامی ایران همواره مورد تهاجم نظام سلطه قرار داشته و جنگ نرم نیز یکی از شیوه‌های این تهاجم است. جنگ نرم، امروزه مؤثرترین، کارآمدترین و کم‌هزینه‌ترین و درعین حال خطرناک‌ترین و پیچیده‌ترین نوع جنگ علیه امنیت ملی یک کشور است که با حذف لشکرکشی و از بین بردن مقاومت‌های فیزیکی مخاطب به هدف خود، که همان استحاله فرهنگی و سیاسی است، خواهد رسید (عیوضی و دامیار، ۱۳۹۵، ص ۸). جنگ نرم روشی برای جنگ و غلبه بر طرف مقابل، بدون استفاده از زور نظامی اولیه و به صورت جذب و اقناع افکار عمومی است تا با اقدام نرم‌افزارانه و روانی، افکار و باورهای جامعه را به منظور تحقق اهداف خود اشغال کند و تغییر اساسی و ساختاری در جامعه هدف بر جای گذارد (قربانزاده سوار، قلخانپاز و رحمتی، ۱۳۹۱، ص ۶). نمونه‌های زیادی از بکارگیری اقدامات نرم در کشورهای مختلف وجود دارد که بدون وجود تهدید و اجبار و از طریق انقلاب‌های مخملی موجب تغییر در ساختار یک نظام را فراهم آورده است. بنابراین بی‌توجهی به چنین موضوعاتی، مخاطرات امنیتی گسترده‌ای را برای کشور به دنبال خواهد داشت (شمولی، رشیدحفظ‌آباد و یعقوبی، ۱۳۹۴، ص ۱۴۷).

عصر حاضر، در پرتو دانش و فناوری، شاهد تحولات بی‌شماری است که گسترش امکانات ارتباطی در رأس آنها قرار دارد. در چنین شرایط زمانی، اینترنت، ماهواره‌ها و رسانه‌های گوناگون با انتقال اطلاعات هم‌زمان، معلومات و مبادله افکار و عقاید نقش زیادی در تحولات سیاسی، اقتصادی، فرهنگی و اجتماعی دارند (رفیعی، ۱۳۸۲، ص ۱۳). پیشرفت فناوری و در راستای آن توسعه وسایل ارتباطی - اطلاعاتی، که رابطه‌ای مستقیم با مردم دارند و بر افکار عمومی مؤثرند، بیانگر اهمیت آن در تمامی ابعاد جامعه جهانی است. به قول کارشناسان ارتباطات، قرن حاضر، عصر تبادل اطلاعات است. بنابراین امروزه کشورها برای دستیابی به اهداف و منافع خود در سایر

نقاط جهان، از این فناوری‌ها بهره‌های فراوان می‌برند. از جمله مواردی که این فناوری‌ها در آن بکار گرفته می‌شوند، جنگ نرم است (شاه‌محمدی، ۱۳۸۲، ص ۴۵).

یکی از حوزه‌هایی که عمق و دامنه تهدیدات نرم را گسترش می‌دهد، رشد فزاینده جرایمی است که در محیط‌های مجازی و سایبر به وقوع می‌پیوندد و به صورت مستقیم امنیت اجتماعی را تهدید می‌کند. برخی مصادیق جرایم سایبر که در زیرمجموعه تهدیدات نرم افزاری قرار می‌گیرند، عبارت‌اند از: افزایش نشر فیلم‌های شخصی و خانوادگی به‌ویژه افراد مشهور در حوزه‌های ورزشی و هنری؛ افزایش انتشار کلیپ‌های مستهجن و غیراخلاقی؛ گسترش شایعات و یا تبلیغ علیه نظام توسط شبکه‌های اجتماعی مبتنی بر تلفن همراه و وب؛ گسترش پایگاه‌ها، کانال‌ها و گروه‌های براندازانه (نائینی، ۱۳۸۶، ص ۲۸).

یکی از شیوه‌های جنگ نرم در محیط‌های سایبر (اینترنت)، گسترش هدفمند و روزافزون وبلاگ‌نویسی توسط برخی افراد، گروه‌ها یا سازمان‌های مخالف نظام جمهوری اسلامی ایران است. وبلاگ‌های ساختارشکن و برانداز که معمولاً به‌سادگی ایجاد شده و نیاز به تخصص بالای بلاگرها ندارد، به راحتی در محیط‌های مجازی به یک هویت مستقل تبدیل و بدون اینکه شناسایی شوند به ترویج عقاید براندازانه اقدام می‌کنند (قربانزاده‌سوار، قلخان‌باز و رحمتی، ۱۳۹۱، ص ۲۱). در نتیجه توجه به جنگ نرم و به‌ویژه در زمینه ایجاد جرم در فضای سایبری از اهمیت دوچندان برخوردار است.

کنعانی و همکاران (۱۳۹۵) در پژوهش خود با عنوان «شناسایی حوزه‌های تاثیرگذار تهدید نرم با رویکرد انتظامی» نشان دادند که تهدید نرم از دیدگاه انتظامی بر ۷ حوزه شامل حوزه‌های اقتصادی، اجتماعی، سیاسی، فرهنگی، مدیریتی، فن آوری و دفاعی - امنیتی تاثیرگذار است. رفیعی‌کیا (۱۳۹۴) در پژوهش خود با عنوان «مبانی تهدیدشناسی در پیشگیری از تهدید نرم» مولفه‌های عملیات روانی، تهدیدهای رسانه‌ای، اختلاف‌افکنی قومی و مذهبی، گسترش بی‌اعتمادی میان مردم و نظام را مورد بررسی قرار داده و بیان می‌دارد تهدیدهای نرم در عرصه سیاسی، اجتماعی، فرهنگی و اقتصادی وارد شده اثرگذار است. شمولی و همکاران (۱۳۹۴) در پژوهش خود با عنوان «بصیرت‌گرایی و بصیرت‌افزایی، راهبردی اساسی در مقابله با جنگ نرم» نشان دادند

که استقرار تفکر بسیجی (مدیریت بسیجی) در بدنه نهادها و سازمان‌ها به‌عنوان خلق‌کننده بصیرت در جامعه در مقابله با جنگ نرم دشمن از جمله راهبردی است که می‌تواند نقشه راه تمام عوام و خواص باشد. فایق آمدن بر جنگ نرم و توجه به لایه‌های جنگ نرم دشمن مانند جریحه‌دار کردن احساسات، عواطف، هنجارها، ارزش‌ها و باورهای مهم جامعه از طریق مدیریت بر ادراکات، احساسات و باورسازی در مقابل باورسوزی دشمن، از الزامات بصیرت است. یعقوبی (۱۳۹۴)، در پژوهشی با عنوان «پیشگیری وضعی از تروریسم سایبری» نتیجه گرفته است که رسانه‌ای شدن سیاست یا همان سیاست رسانه‌ای به این معناست که نهادهای سیاسی به‌طور فزاینده‌ای به رسانه‌ها وابسته هستند و به کمک رسانه‌های جمعی شکل می‌گیرند و این رسانه‌ای شدن نقش مهمی در جنگ نرم ایفا می‌کند. دارا و الفی (۱۳۹۲) در پژوهش خود نشان دادند که مسئولان باید با موضعی تدافعی توأم با بصیرت و تدبیر و با تقویت توان علمی و اعتلای باورهای دینی و فرهنگی دانشجویان، به خنثی‌سازی عملیات روانی، شبه‌زدایی علمی و ژورنالیستی آنان بپردازند. هندیانی و میرزاخانی (۱۳۹۳) در مطالعه خود با عنوان «نقش سرمایه اجتماعی در کاهش آثار تهدیدهای نرم با نگاهی به فرماندهی و مدیریت آینده پلیس» به این یافته رسیده‌اند که سرمایه اجتماعی می‌تواند اثر تهدیدات نرم را کاهش داده و با عنایت به اشتراک یا همسویی مولفه‌ها با رویکرد اجتماعی پلیس، زمینه پیاده‌سازی آن را برای مدیریت آینده پلیس فراهم کند، پژوهشگران یادشده نتیجه‌گیری کرده‌اند که: برای کاهش اثر تهدیدات نرم بر سرمایه اجتماعی باید نسبت به تقویت مولفه‌های سرمایه اجتماعی همچون هنجارهای اعتمادساز، مشارکت‌جو، هویت‌بخش، ارزش‌مدار مبتنی بر روابط اقدام شود تا ضمن برخوردار شدن جامعه از آثار مثبت سرمایه اجتماعی، پیاده‌سازی رویکردهای جدید پلیس از پشتوانه‌ای قوی‌تر برخوردار شود.

## مبانی نظری

اولین بار جوزف نای این اصطلاح را در کتابش با نام «ناگزیر از تقدم: طبیعت متغیر قدرت آمریکایی» و سپس در کتاب سال ۲۰۰۴ خود با نام «قدرت نرم: ابزارهایی برای موفقیت در سیاست‌های جهانی» این‌گونه تعریف می‌کند: «قدرت نرم، توانایی کسب چیزی است که می‌خواهیم از طریق جذب

به جای اجبار به دست آوریم» (نی<sup>۱</sup>، ۲۰۰۴؛ برگر<sup>۲</sup>، ۱۹۹۷). جنگ نرم، کاربرد ابزارهای نرم علیه جامعه خاص با هدف تاثیر بر فرهنگ، ارزش‌ها، باورها و اعتقادات به منظور استحاله آن و جایگزینی نظام فرهنگی مورد نظر مهاجم با مدافع است. به نظر «هیرام جانسون<sup>۳</sup>» هنگامی که جنگ آغاز می‌شود، حقیقت، اولین قربانی است و غلبه بر فرد در صورتی که نداند تحت سیطره است، آسان‌تر است. از نظر «ایگناسیو رامونه<sup>۴</sup>» استعمارشدگان و استعمارگران هر دو می‌دانند که سلطه‌گری تنها مبتنی بر برتری فیزیکی نیست و تسخیر روان و اذهان در پی تسخیر نظامی انجام می‌گیرد. از این رو، هر امپراطوری خواهان دوام بیشتر سلطه خویش، در صدد تسخیر روح و ذهن اتباع و مخاطبان خود است (افتخاری، ۱۳۸۹، ص ۲۵۷).

جنگ نرم، مجموعه تدابیر و اقدامات از پیش اندیشیده فرهنگی، سیاسی و اجتماعی کشورهاست که بر نظرات، نگرش‌ها، انگیزش و ارزش‌های مخاطبان، حکومت‌ها، دولت‌ها، گروه‌ها و مردم کشورهای خارجی تاثیر می‌گذارد و در بلندمدت موجب تغییر منش، رفتار و کنش فردی و اجتماعی آنان می‌شود (الیاسی، ۱۳۸۷، ص ۱۲). جنگ نرم، حالت تنش و مخاصمه شدیدی است که بین کشورها پدیدار می‌شود و رزمایش‌های سیاسی، مشاجره‌های دیپلماتیک، جنگ‌های روانی، مخاصمه‌های ایدئولوژیک، جنگ اقتصادی و رقابت برای کسب قدرت از ویژگی‌های آن است. هدف‌های این تهاجم می‌تواند تضعیف روحیه و وحدت ملی، ایجاد شکاف میان مردم و حاکمیت و تضعیف اراده مقاومت در مردم باشد. جنگ نرم به معنی بکارگیری هوشمندانه، طرح‌ریزی و هدایت اقدامات غیررزمی است که سرانجام موجب تغییر نگرش و رفتار گروه‌های هدف برای برنامه‌ها و منافع طراح جنگ نرم خواهد شد (نائینی، ۱۳۸۹، صص ۵-۶). جنگ نرم، روشی برای جنگ و غلبه بر طرف مقابل، بدون استفاده از زور نظامی اولیه و به صورت جذب و اقتناع افکار عمومی است تا با اقدام نرم‌افزارانه و روانی، حوزه افکار و باورهای جامعه را به منظور تحقق اهداف خود اشغال کند و تغییر اساسی و ساختاری در جامعه هدف بر جای گذارد (سنجایی‌شیرازی، ۱۳۸۹، ص ۱۲۱).

1. Nye

2. Berger

3. Hiram Jonson

4. Ignacio Romona

هدف اصلی در جنگ نرم علیه جمهوری اسلامی، مقابله با عناصر و مؤلفه‌های قدرت نرم و مقوم‌های نظام جمهوری اسلامی است. به‌طور دقیق، این هدف بر مقابله با عوامل موفقیت در مبارزه با رژیم شاهنشاهی و دشمنان خارجی در دفاع مقدس، متمرکز است. این تهاجم به‌صورت پیچیده و نامحسوس در دوره هشت‌ساله سازندگی شروع شد، هرچند درک آن برای بسیاری از خواص و نخبگان مشکل بود، مقام معظم رهبری با بهره‌گیری از تجارب تاریخی، صحنه این نبرد را کالبدشکافی کردند. در این دوره هشدارهای رهبری مورد توجه قرار نگرفت. در دوره سازندگی، روشنفکران غرب‌گرا در حوزه نظری، ده‌ها مقاله و نشریه با هدف به چالش کشیدن عناصر قدرت نرم نظام جمهوری اسلامی منتشر کردند. به‌طور قطع، یکی از پیچیده‌ترین جلوه‌های جنگ نرم علیه نظام جمهوری اسلامی ایران، در سال ۱۳۸۸ ظاهر شد که به‌عنوان «فتنه» توسط مقام معظم رهبری نامگذاری شد (عیوضی و دامپار، ۱۳۹۵، ص ۲۸). بنابراین، جنگ نرم مجموعه‌ای از اقدامات روانی و تبلیغات رسانه‌ای است که دگرگونی در هویت فرهنگی و الگوهای رفتاری مورد قبول یک نظام سیاسی را دنبال می‌کند و در واقع به‌دنبال نوعی سلطه در ابعاد سه‌گانه حکومت، اقتصاد و فرهنگ است. همچنین تعریف جنگ نرم از دیدگاه مقام معظم رهبری عبارت است از «جنگ به‌وسیله ابزارهای فرهنگی، نفوذ، دروغ و شایعه‌پراکنی با ابزارهای پیشرفته‌ای که امروزه وجود دارد (عبدی، ۱۳۸۹، ص ۱۳۵).

جنگ نرم دارای ابعاد سیاسی، فرهنگی، اجتماعی، دفاعی و امنیتی است که دارای ویژگی‌هایی به‌شرح زیر است:

- ۱- جنگ نرم، مبارزه‌ای غیرخشونت‌آمیز است و از شیوه‌های نرم استفاده می‌شود.
- ۲- در جنگ نرم تلاش اصلی بر ایجاد تردید در مبانی و زیرساخت‌های فرهنگی نظام سیاسی متمرکز می‌شود.
- ۳- در جنگ نرم نیروی مهاجم به‌دنبال بحران‌سازی، مقبولیت‌زدایی و مشروعیت‌زدایی از حکومت مستقر است (مهم‌ترین هدف جنگ نرم).
- ۴- تغییرات جنگ نرم ماهوی، آرام، ذهنی و تدریجی است.
- ۵- مبارزه در جنگ نرم بسیار پیچیده است و محاسبه و اندازه‌گیری در جنگ نرم، کاری دشوار

است.

۶- در جنگ نرم عواطف، احساسات و اندیشه‌ها از سوی نیروی مهاجم نشانه‌رو می‌شود (شمولی و همکاران، ۱۳۹۴، ص ۱۹۷).

جدول ۱. ابعاد جنگ نرم در رویکردهای مختلف (نائینی، ۱۳۸۹، ص ۳۲)

نوع رویکرد	ابعاد
سیاسی - فرهنگی	اجتماعی: تغییر ساخت‌ها و کنش‌های اجتماعی فرهنگی: تغییر در ارزش‌ها، هنجارها، باورها و نگرش‌های پایه سیاسی: تغییر در ترجیحات، جهت‌گیری‌ها و کنش‌های سیاسی - حکومتی
روان‌شناسی - اجتماعی	شناختی: تغییر در نظام ذهنی و اندیشه عاطفی: القای احساسات و هیجانات خاص اجتماعی: تغییر در تعاملات و کنش‌های عمومی منش شناختی: تغییر در رفتارها و اندیشه‌های اخلاقی معنوی و اعتقادی: تغییر در عقاید و رفتار مذهبی شهروندان جامعه هدف

**فضای سایبری:** «دیوید بل»، یکی از نظریه‌پردازان رسانه‌های مجازی، معتقد است تعریف فضای سایبر پیچیده است. وی سه تعریف هم‌پوشان از فضای سایبر ارائه می‌کند: اول، تعریف فضای سایبر از دیدگاه سخت‌افزاری، یعنی شبکه‌ای جهانی از رایانه‌ها که از طریق زیرساخت‌های ارتباطی به هم متصل شده‌اند و اشکال گوناگون تعامل میان کنش‌گران دور از هم را تسهیل می‌سازند. دوم، فضای سایبر را می‌توان به‌عنوان فضایی خیالی بین رایانه‌ها تعریف کرد که در آنجا افراد ممکن است خودهای جدید و دنیاهای جدیدی بسازند. فضای سایبر مجموع سخت‌افزار و نرم‌افزار و همچنین مجموعه‌ای از تصویرها و ایده‌هاست. سوم، تعریف فضای سایبر بر مبنای ماهیت کاری آن به معنی بازنمایی‌کننده نوعی تلاقی میان عناصر مادی و نمادین است که بسته به نوع استفاده هر فرد، ارزش‌های متفاوتی را بروز می‌دهد. «مایکل بندیکت» نیز در تعریف خود می‌گوید: فضای سایبر یک جغرافیای ذهنی عام است که در مقابله با اجماع و انقلاب، اصول و تجربه ساخته می‌شود، قلمروی که مملو از داده‌ها، دروغ‌ها، موضوع‌های ذهنی و خاطره‌های طبیعی، با یک میلیون صدا و دو میلیون چشم در یک هماهنگی ساکت و نامرئی نسبت به پژوهش، انجام معامله، سهیم شدن در رویاها و مشاهده ساده است (دیوید، ۱۳۸۹، ص ۲۲).

«یارون لاینر»، نظریه پرداز واقعیت مجازی، فراتر از این را می‌گوید. او در کتاب «شما یک ابزارک نیستید» هشدار می‌دهد که ارتباطات اینترنتی، به صورتی گله‌وار افراد را درون «عشیره‌های مجازی متضاد» دسته‌بندی می‌کنند. واقعاً مبنای خصومت آن‌ها با یکدیگر چندان مهم نیست، بلکه اینترنت است که جزئیات اختلافی را برجسته می‌سازد و افراد را نسبت به آن‌ها حساس می‌کند. وی هشدار می‌دهد که این موضوع، سبب افزایش خصومت‌های اجتماعی می‌شود. ادامه صحبت‌های لاینر، تأکید بر تمامیت‌گرایی آمریکایی در اینترنت است که سبب افزایش دشمنی افراد جوامع می‌شود. یکی از مسائلی که ساخت‌شکنان در مورد فضای مجازی می‌گویند و جای تأمل دارد، این است که فضای مجازی مرز بین انسان و ماشین را برداشته است. ریشه این بحث در مجازی بودن واقعیت در صفحه اینترنت است که از آن به واقعیت مجازی تعبیر می‌شود. قابلیت اینترنت در شبیه‌سازی سه‌بعدی، غوطه‌ورسازی رایانه‌ای و دیداری- شنیداری از واقعیت یا تصوره‌های واقعیت برای مدت طولانی سبب شده تا برخی بین انسان و رایانه مرزی قائل نباشند و فضای مجازی را محیطی تلقی کنند که در آن، انسان بدن گوستی خود را فراموش می‌کند، کنار می‌گذارد و در نهایت از آن عبور کرده و می‌تواند بدون آن و تنها متکی بر هوش و تخیل نیز زیست کند. این‌ها البته خیال‌پردازی‌هایی است که از همان ابتدای گسترش رایانه و پدید آمدن فضای مجازی در داستان‌های علمی تخیلی افرادی همچون ویلیام گیسون، تخیلی‌نویس داستان‌های رایانه‌ای، وجود داشته است؛ اما این داستان‌های تخیلی با گسترش اینترنت هرچه بیشتر به محیط فکری فرهنگی انسان غربی وارد شده و تصوره‌های عجیبی را در نوع نگاه آنان به انسان پراکنجته است. واژه پسانسان، زندگی مصنوعی، هوش مصنوعی و... از جمله مفاهیمی است که نشان‌دهنده این موضوع است. برای نمونه دو دانشمند به نام‌های «منفرد کلاینر» و «ناثان کلاین» به دنبال انجام آزمایش‌ها برای یک مسافرت فضایی، تصویر «رایاندامگان» را واقعی جلوه دادند. آنان در مقاله خود از تغییرات ضروری در بدن انسان برای زندگی آینده در فضا سخن گفتند. در دیدگاه آنان، رایاندامگان «سامانه‌ای انسانی- ماشینی و خویش‌تنظیم» است که می‌تواند در موقعیت‌های مختلف به زندگی خود ادامه دهد. بعدها «هاراوی» با توسعه بیشتر ادبیات رایاندامگان، آن را نوع نگاه کنونی به هستی دانست. مفهوم پسانسان که نظریه پردازان غربی فضای مجازی منتشر



می‌کنند، در همین جهت است. این نظریه می‌گوید یا گونه انسان در بن‌بست تکامل است و باید فناوری‌ها را در هم آمیزد تا به «سطح بعدی» تکامل یابد و یا ما مدت‌هاست به دلیل روابط نزدیک روزافزون خود با غیرانسان‌هایی چون دست‌ساخته‌های فناوری، انسان نیستیم. از همین منظر است که موضوع هویت در فضای مجازی رنگ می‌بازد و سیال، متغیر و متکثر می‌شود (دیوید، ۱۳۸۹، ص ۱۵۰).

نتیجه‌ای که از نظریه‌های بالا برمی‌آید اینکه به‌نظر می‌رسد فضای مجازی پیوند وثیقی با ساخت‌شکنی مورد اشاره پسامدرن‌ها دارد. قابلیت‌های این محیط سبب تقویت این گرایش‌ها می‌شود: گرایش گریز از مرکز؛ به‌صحنه آمدن هویت‌های متعدد، متکثر و ناشناخته با سلاقی مخصوص خود؛ عبور فرد از مرزهای عرفی و قانونی و بی‌اعتبار شدن مراجع و الگوهای عرفی و قانونی در محیط مجازی در اثر کم‌رنگ شدن ارتباطات واقعی و اصالت یافتن ارتباطات بر مبنای علاقه‌مندی در محیط مجازی. این وضعیت در شبکه‌های اجتماعی مجازی و با شدت بیشتری همراه است (دیوید، ۱۳۸۹، ص ۱۵۱).

قدرت مبتنی بر اطلاعات، بحث تازه‌ای نیست اما قدرت سایبر یک امر بدیهی است. ده‌ها تعریف از فضای سایبر وجود دارد به‌طور کلی، «سایبر» پیشوندی است که برای فعالیت‌های مرتبط با الکترونیک و رایانه بکار می‌رود. در تعریفی دیگر «فضای سایبر، حوزه عملیاتی است که به‌وسیله الکترونیک، امکان بهره‌مندی از اطلاعات توسط سیستم‌های یکپارچه را میسر می‌سازد»، بیان شده است. قدرت، وابسته به ماهیت است و قدرت سایبر مبتنی بر منابعی است که حوزه فضای سایبر را توصیف می‌کند. فضای سایبر را می‌توان براساس برخی از لایه‌های فعال آن مفهوم‌سازی کرد اما ساده‌ترین تقریبی که برای به‌تصویر درآوردن آن می‌توان زد این است که ماهیت ترکیبی از خصوصیات فیزیکی و مجازی است. لایه زیرساخت فیزیکی از قوانین اقتصادی، منابع رقیب، افزایش حاشیه سود، قوانین سیاسی قدرت‌های حاکم پیروی می‌کند. لایه مجازی و اطلاعاتی دارای ویژگی‌های اقتصاد شبکه‌ای، افزایش بازده نسبت به مقیاس و اقدامات سیاسی مراکز قدرت است. حملاتی از ناحیه لایه اطلاعاتی با هزینه‌های اندک در برابر حوزه فیزیکی که دارای منابع گران و کمیاب‌اند، می‌تواند راه‌اندازی شود و برعکس، کنترل لایه فیزیکی می‌تواند

اثرات منطقه‌ای و فرامنطقه‌ای بر لایه اطلاعاتی داشته باشد (قیاسی و مجید، ۱۳۹۴، ص ۳۴۸). می‌توان فضای سایبر را محیطی مجازی و غیرملموس و موجود در شبکه‌های بین‌المللی تعریف کرد که تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر آنچه در کره خاکی به‌صورت فیزیکی و ملموس وجود دارد، در این فضا به‌شکل دیجیتال وجود داشته و قابل استفاده و در دسترس کاربران بوده و از طریق رایانه، اجزاء آن و شبکه‌های بین‌المللی به هم مرتبط می‌شوند (آگاروال و همکاران، ۲۰۱۴). فضای مجازی، محیط الکترونیک واقعی است که در آن، ارتباطات انسانی به شیوه‌ای سریع و فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد. برخلاف فضای واقعی، در فضای مجازی نیاز به جابه‌جایی‌های فیزیکی نیست و همه اعمال فقط از طریق فشردن کلیدها با حرکات موشواره صورت می‌گیرد. فضای مجازی، مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی، بدون در نظر گرفتن جغرافیای فیزیکی، گفته می‌شود. ماهیت فضای مجازی، ماهیتی فرافیزیکی و غیرملموس است و به‌طور کلی، متفاوت با ماهیت فضای سنتی است. با توسعه فضای مجازی، مفاهیم و اصطلاحاتی در ادبیات الکترونیکی جهان رایج شد که اساس خود را از فعالیت‌ها و توسعه بشری در فضای فیزیکی به امانت گرفتند، از جمله: دولت الکترونیک، تجارت الکترونیک، جنگ مجازی و... (نجات‌پور و همکاران، ۱۳۹۱، ص ۵۳).

جنگ مجازی و همچنین سایبرنتیک به‌صورت استفاده از رایانه و اینترنت برای جنگیدن در فضای مجازی تعریف می‌شود (عبداله‌خانی، ۱۳۸۶، ص ۱۳۶). به‌عبارت دیگر؛ جنگ مجازی را می‌توان هرگونه عمل جنگی دانست که در آن سیستم‌های اطلاعاتی یا فناوری دیجیتال، چه به‌عنوان ابزار حمله و چه به‌عنوان آماج حمله استفاده می‌شود. این حملات منجر به اعمال خشونت بر ضد اشخاص یا دارایی‌ها، به میزانی که ایجاد رعب و وحشت کند، انجام می‌شود (قربان‌نیا، ۱۳۸۳، ص ۲۰).

**ماهیت جرم:** جرم پدیده چندوجهی است که تحقق آن نیازمند عوامل متعددی است. از یک سو پدیده ظاهری و عینی و از سوی دیگر، دارای وصف مجرمانه. از نظر حقوقی برای آنکه عمل انسانی جرم تلقی شود؛ باید چند نکته اساسی در آن محرز شود: نخست قانونگذار این عمل یا فعل را

جرم شناخته و کیفری برای آن در نظر گرفته باشد؛ دوم فعل یا ترک فعل مشخص به منصف ظهور و بروز یا به فعلیت برسد و سوم با علم و اختیار، این عمل ارتکاب یافته باشد (حسینی‌خواه و رحمتی، ۱۳۸۹). برخی ویژگی‌ها که بیشتر آنها از ویژگی‌های منحصر به فرد فضای سایبر محسوب می‌شوند عبارت‌اند از:

**نامحدود بودن فضای سایبر:** محیط سایبر، محیطی بدون مرز است. این ویژگی مثبت که امکان استفاده شایسته از محیط سایبر را برای آسان کردن فعالیت‌ها فراهم می‌سازد، در صورت استفاده نادرست، می‌تواند آثار منفی بر جای بگذارد.

**ناملموس بودن فضای سایبر:** محیط سایبر، محیطی فیزیکی و ملموس نیست. عامل مراقب مثل پلیس، در این محیط وجود خارجی و ملموس ندارد تا جنبه بازدارندگی داشته باشد. همچنین بزه‌دیدگان جرایم سایبری، با بزه‌کار مواجه نمی‌شوند و مجاورتی بین این دو وجود ندارد.

**توسعه و تغییرپذیری:** ماهیت فضای سایبر و پیشرفت روزافزون علوم مرتبط موجب شده است روزانه شاهد ظهور برنامه‌ها، نرم‌افزارها و خدمات اینترنتی متنوعی باشیم که وجود برنامه‌ریزی‌های مناسب برای استفاده صحیح این ابزارها را ضرورت می‌بخشد.

**پیچیدگی و تخصصی بودن:** برنامه‌ریزی‌های رایانه‌ای تخصصی، تشخیص اقدامات آسیب‌زا در فضای سایبر، نحوه استفاده ایمن از این فضا، نحوه شناسایی و مقابله با منحرفان سایبری، تاثیر فضای سایبر بر فرهنگ و جامعه و بسیاری از امور اساسی و کلیدی که در این راستا باید بر آن اشراف داشت، نیازمند وجود تخصص‌های متناسب پیچیدگی این فضا است.

**دسترسی آسان و سریع:** این دسترسی، به گونه‌ای است که افراد به راحتی با استفاده از رایانه شخصی یا حضور در کافی‌نت‌ها قادر خواهند بود از کلیه امکانات این فضا بدون محدودیت استفاده کنند. این ویژگی با توجه به محیط پرجاذبه و آسیب‌زای فضای مجازی ممکن است آثار نامطلوبی از شکل‌گیری جرایم تا انحرافات اخلاقی به‌ویژه در قشر کم سن‌وسال به‌بار آورد.

**استفاده گسترده از فضای سایبر:** امروزه به دلیل پیشرفت فناوری و خودکار شدن فعالیت‌های تولیدی، تجاری و اقتصادی، استفاده از فضای مجازی برای تسهیل و تسریع امور، رشد روزافزونی داشته است (جلالی‌فراهانی، ۱۳۸۳، ص ۹۸).

**جرم رایانه‌ای (اینترنتی):** جرم رایانه‌ای بر دو نوع است که در تعریف محدود، جرمی که در فضای سایبری رخ می‌دهد جرم رایانه‌ای است. براساس این دیدگاه اگر رایانه ابزار و وسیله ارتکاب جرم باشد آن جرم را نمی‌توان در زمره جرایم رایانه‌ای قلمداد کرد (قانون جرایم رایانه‌ای، مصوب ۱۳۸۹). در تعریف گسترده (موسع) هر فعل یا ترک فعلی که «از طریق» یا «به کمک سامانه‌های رایانه‌ای» رخ می‌دهد جرم رایانه‌ای قلمداد می‌شود. از این دیدگاه جرایم به ۳ دسته تقسیم می‌شوند.

۱. رایانه موضوع جرم: در این دسته از جرایم رایانه و تجهیزات رایانه‌ای، موضوع جرایم سنتی (کلاسیک) هستند مثل سرقت، تخریب تجهیزات و ...
۲. رایانه واسط جرم: رایانه وسیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک، گواهینامه و... استفاده می‌شود.

۳. جرایم محض رایانه‌ای: دسته سوم جرایمی مانند هک یا ویروسی کردن که فقط در فضای سایبر اتفاق می‌افتد.

در کنفرانس بین المللی بوداپست (۲۰۰۱) چیزی باعنوان جرم رایانه‌ای مطرح نشده است بلکه در فضای سایبری از جرم سایبری نام برده شده که در فارسی به جرم مجازی تعبیر می‌شود. در اسناد و کنفرانس‌های بین‌المللی پیرامون جرایم رایانه‌ای رویکردی دوگانه وجود دارد؛ به این معنا که هم ارتکاب جرایم رایانه‌ای محض مانند هک کردن و هم ارتکاب برخی جرایم مانند جرایم سنتی با استفاده از سامانه‌های رایانه‌ای مانند نقض حقوق مالکیت معنوی جرم تلقی شده است. در کشور ما تعاریفی که در پیش‌نویس جرایم رایانه‌ای آمده است، جرم‌ها را به جرم‌هایی از قبیل کلاهبرداری رایانه‌ای، جعل رایانه‌ای، جاسوسی رایانه‌ای، سابوتاژ رایانه‌ای (تغییر، محو، متوقف‌سازی، ملاحظه در خطوط ارتباطی و...) تخریب رایانه‌ای، دستیابی غیرمجاز، شنود غیر قانونی و... تقسیم کرده و مجازات‌هایی برای برخورد با این جرایم در نظر گرفته است (قانون جرایم رایانه‌ای، مصوب ۱۳۸۹).

**جرایم در حوزه فضای مجازی:** جرم برای برخی از انسان‌ها جذاب است و این جذابیت در برخی از فضاها و شرایط بیشتر می‌شود. فضای سایبر یکی از این فضاهاست که قابلیت و جوانب منفی و مثبت بسیاری دارد. فضای سایبر شامل شبکه‌های رایانه‌ای و مخابراتی متصل به هم می‌شود که

اطلاعات را در کمترین زمان و در بیشترین مکان مبادله می‌کند. اغلب افراد برای گذراندن وقت و سرگرمی، ارتباطات گسترده‌ای در فضاهای اینترنتی برقرار می‌کنند غافل از آنکه ارتباطی به ظاهر ساده و پیش پا افتاده، کوچک‌ترین اطلاعات فردی و شخصی افراد را در اختیار مجرمان می‌گذارد. امروزه اطلاعات مهمی درباره اشخاص و مشاغل به صورت الکترونیکی ایجاد، ذخیره، پردازش و مبادله می‌شود که باید امنیت این اطلاعات به طور کامل حفظ شود. تحولات سریع و روزافزون فناوری اطلاعات و ظهور جامعه اطلاعاتی، دستاوردهای مهمی را برای بشر به ارمغان آورده است؛ اما تهدیدات بسیاری در حوزه امنیت شبکه و سیستم اطلاعات وجود دارد که به مشکلات پیچیده و متعددی منجر می‌شود (زندى، ۱۳۸۹، ص ۹۵).

«جرائم مجازی» به جرایمی گفته می‌شود که در «فضای مجازی» رخ می‌دهد. فضای مجازی مجموعه به هم پیوسته دنیای امروز از طریق رایانه و ارتباطات راه دور، بدون در نظر گرفتن مکان جغرافیایی است. در چنین شرایطی، موضوعات مختلف ناشی از بکارگیری صحیح و مجاز دستاوردهای این فناوری، مسائل، مشکلات، اختلافات و دعاوی مرتبط با آن و همچنین جرائم و تخلفات ناشی از استفاده غیرمجاز و اعمال مجرمانه شامل جرائم مجازی می‌شود. برای رویارویی با تهدیدات فضای سایبری و اقدامات قابل سرزنش که امنیت و سلامت این فضا را به خطر می‌اندازد، سه رویکرد وجود دارد:

**جرم‌انگاری با توسل به قانون:** لازمه رویکرد جرم‌انگاری با توسل به قانون، داشتن قانون «جرائم رایانه‌ای» و بسیاری از قوانین مکمل دیگر است تا بتوان با استناد به آن علیه مجرمان فعالیت کرد. جرائم رایانه‌ای مانند سایر جرائم دارای مباحث خاص جرم‌شناسی، بزه‌دیده‌شناسی، سیاست جنایی، کشف علمی جرائم و پیشگیری است. پیشگیری در اینجا روش‌ها و ابزارهای خاص خود را دارد. استفاده از انواع نرم‌افزارهای فیلترینگ، بلوکه کردن و کنترل محتوا، از جمله مباحث در زمینه پیشگیری از این جرائم است (عالی پور، ۱۳۹۳، ص ۸۰).

**بکارگیری تدابیر حفاظتی و کنترلی:** تدابیر حفاظتی و کنترلی شامل پیشگیری و همچنین آموزش کاربران و توانمندسازی آنان در برابر تهدیدات است (غلامی، ۱۳۹۱، ص ۱۹۵).

**پیشگیری اجتماعی:** پیشگیری اجتماعی به معنای آموزش جامعه برای اجتناب از محیط‌های

خطر ساز و همچنین فرهنگ‌سازی برای افراد و پیشگیری از ارتکاب جرم است. برای رسیدن به هدف مورد نظر و همچنین ایجاد فضاهای امن، بهترین کار استفاده هم‌زمان از این سه رویکرد است. در جمهوری اسلامی ایران، شبکه‌ها به‌طور عمده، پیچیده و چندلایه هستند و ممکن است در لایه‌های مختلف آن، اطلاعات سرقت، «هک» و تخریب شوند. نصب نرم‌افزارها و سخت‌افزارهای متناسب هر لایه کمک شایانی به حفظ اطلاعات می‌کند. اگر به موارد امنیتی توجه شود با صرف هزینه‌ای اندک، اطلاعات مهم و اساسی حفظ می‌شود و از بروز خسارت‌های جبران‌ناپذیر پیشگیری می‌شود (غلامی، ۱۳۹۱، ص ۱۹۶).

با توجه به مطالب ارائه‌شده در رابطه با فضای سایبری و جرم و همچنین اهمیتی که جنگ نرم بر نگرش‌های افراد جامعه و ایجاد جرم دارد، در این پژوهش ارتباط میان جنگ نرم در سست کردن ابعاد فرهنگی، اجتماعی و سیاسی جامعه با وقوع جرم در فضای سایبری مورد بررسی قرار می‌گیرد. در ادامه به بررسی فرضیه‌های پژوهش و تجزیه و تحلیل‌های آماری پرداخته شد.

### روش پژوهش

این پژوهش از لحاظ جهت‌گیری‌های پژوهش، کاربردی؛ از لحاظ هدف، توصیفی، از لحاظ راهبردهای پژوهش، پیمایشی و از لحاظ ماهیت، علی است. برای جمع‌آوری داده‌ها از روش کتابخانه‌ای و میدانی استفاده شد. در این پژوهش از پرسشنامه محقق‌ساخته برای جمع‌آوری داده‌های بخش میدانی استفاده شد. روایی پرسشنامه با استفاده از نظر اساتید تایید شد و برای اندازه‌گیری پایایی کل آن، ۳۰ پرسشنامه به‌طور نمونه و آزمایشی، میان افراد جامعه توزیع و ضریب آلفای کرونباخ آن، ۰/۸۹ به‌دست آمد. همچنین پایایی متغیرها در جدول ۲ درج شده است. جامعه آماری پژوهش کلیه دانشجویان دانشگاه علوم انتظامی امین هستند که حجم نمونه با استفاده از جدول کرجسی- مورگان، ۳۸۴ نفر برآورد شد و با استفاده از نمونه‌گیری تصادفی ساده، در نهایت ۳۴۱ پرسش‌نامه کامل جمع‌آوری شد. داده‌های پژوهش با استفاده از آزمون‌های آماری همبستگی اسپیرمن و آزمون رتبه‌ای فریدمن مورد تحلیل قرار گرفته‌اند.

جدول ۲. نتایج محاسبه ضریب آلفای کرونباخ متغیرهای پژوهش

ضریب پایایی	سستی ابعاد فرهنگی	سستی ابعاد سیاسی	سستی ابعاد اجتماعی	وقوع جرم
آلفای کرونباخ	۰/۹۰۲	۰/۸۳۶	۰/۸۹۱	۰/۹۰۰

### یافته‌ها

یافته‌های توصیفی: همان‌طور که نتایج نشان می‌دهد، بیشترین افراد پاسخ‌دهنده از نظر جنسیت مرد، از لحاظ تحصیلات، کارشناسی؛ و از لحاظ سن در رده سنی ۲۰-۳۰ سال بوده‌اند. نتایج داده‌های جمعیت‌شناختی پژوهش در جدول ۳ درج شده است.

جدول ۳. ویژگی‌های جمعیت‌شناختی پاسخ‌گویان

ویژگی	شاخص	درصد فراوانی
جنسیت	زن	۲۷
	مرد	۷۳
تحصیلات	کارדانی	۳۲
	کارشناسی	۴۷
	کارشناسی ارشد	۲۱
سن	زیر ۲۰ سال	۲۸
	۲۰-۳۰ سال	۶۳
	بالای ۳۰ سال	۹

یافته‌های استنباطی: در ابتدا برای بررسی نرمال یا غیرنرمال بودن داده‌ها، از آزمون کولموگروف اسمیرنوف<sup>۱</sup> استفاده شد که مقدار معناداری از ۰/۰۵ کمتر بوده و نشان از غیرنرمال بودن داده‌ها دارد. همچنین با توجه به داده‌های غیرنرمال، برای بررسی روابط بین فرضیه‌ها از آزمون همبستگی اسپیرمن و آزمون رتبه‌ای فریدمن استفاده شده است.

نتایج آزمون همبستگی اسپیرمن نشان می‌دهد که در سطح اطمینان ۹۹ درصد، می‌توان نتیجه گرفت که همبستگی خطی معناداری بین جنگ نرم و وقوع جرم در فضای سایبری وجود دارد. همچنین جنگ نرم از طریق سست کردن ابعاد فرهنگی جامعه، بیشترین ضریب همبستگی

(۰/۵۰۸) را با وقوع جرم دارد. نتایج این یافته‌ها در جدول ۴ درج شده است.

جدول ۴. نتایج آزمون همبستگی اسپیرمن

تفسیر	سطح معناداری	تعداد	ضریب همبستگی	فرضیه
رابطه مثبت و معنادار	۰/۰۱	۳۴۱	۰/۵۰۸	رابطه سستی ابعاد فرهنگی جامعه از طریق جنگ نرم با وقوع جرم در فضای سایبری
رابطه مثبت و معنادار	۰/۰۱	۳۴۱	۰/۴۳۸	رابطه سستی ابعاد اجتماعی جامعه از طریق جنگ نرم با وقوع جرم در فضای سایبری
رابطه مثبت و معنادار	۰/۰۱	۳۴۱	۰/۴۱۲	رابطه سستی ابعاد سیاسی جامعه از طریق جنگ نرم با وقوع جرم در فضای سایبری

همچنین مطابق با خروجی حاصل از آزمون فریدمن و میانگین رتبه‌های متغیرها در جدول ۵، سستی ابعاد فرهنگی ناشی از جنگ نرم دارای بیش‌ترین رتبه و سستی ابعاد سیاسی ناشی از جنگ نرم دارای کمترین رتبه در نزد افراد است.

جدول ۵. نتایج آزمون فریدمن

متغیرها	میانگین رتبه‌ها
سستی ابعاد فرهنگی	۲/۹۶
سستی ابعاد اجتماعی	۱/۸۹
سستی ابعاد سیاسی	۱/۳۶

## بحث و نتیجه‌گیری

نتایج پژوهش نشان داد که فضای سایبر، بهترین ابزاری است که جنگ نرم از طریق آن بر افراد نفوذ کرده و موجب سست کردن اعتقادهای فرهنگی، اجتماعی و سیاسی جامعه می‌شود. مطابق با فرضیه اول، «جنگ نرم از طریق سست کردن ابعاد فرهنگی جامعه با وقوع جرم در فضای سایبری رابطه دارد»، ضریب همبستگی میان رابطه سستی ابعاد فرهنگی جامعه از طریق جنگ نرم با وقوع جرم، ۰/۵۰۸ محاسبه شد و همچنین سطح معناداری ۰/۰۱ است و نشان از معناداری این رابطه و تایید فرضیه اول دارد. به عبارتی جنگ نرم از طریق سست کردن ارزش‌های بنیادی جامعه همانند خدامحوری، ولایت‌مداری، دشمن‌ستیزی، ضعف اعتقادی و مذهبی مردم، بی‌حجابی و ترویج



فرهنگ غربی، ترویج نسبی‌گرایی، افزایش سلفی‌گری، از میان رفتن قبح روابط با نامحرم و...، سبب ایجاد جرم در فضاهای سایبری می‌شود. همچنین نتایج فرضیه دوم پژوهش «جنگ نرم از طریق سست کردن ابعاد اجتماعی جامعه با وقوع جرم در فضای سایبری رابطه دارد» نشان از تایید این فرضیه دارد. ضریب همبستگی برای فرضیه دوم  $0/438$  و ضریب معناداری  $0/01$  است و نشان می‌دهد که این رابطه معنادار است. از جمله سست کردن ابعاد اجتماعی افراد جامعه شامل جرم و بزهکاری، کم‌رنگ شدن ارزش‌های جامعه، نزاع‌های خیابانی، فقدان پایبندی زن و مرد به خانواده، افزایش سبک زندگی غربی، تجاوز، رواج فمینیسم، تشدید آسیب‌های اجتماعی، افزایش بی‌اعتمادی و... است. درنهایت، نتایج فرضیه سوم «جنگ نرم از طریق سست کردن ابعاد سیاسی جامعه با وقوع جرم در فضای سایبری رابطه دارد»، نشان از تایید این فرضیه دارد. ضریب همبستگی برای این فرضیه  $0/412$  و سطح معناداری  $0/01$  است که نشان از معناداری فرضیه سوم دارد. از جمله سستی ابعاد سیاسی شامل بی‌عدالتی، وادار کردن افراد به نافرمانی مدنی، مخالفت با فرهنگ داخلی، افزایش واگرایی ملی، رواج لیبرالیسم، شکل‌گیری و انسجام احزاب مخالف و... است.

#### پیشنهادها

- در بعد فرهنگی، انجام اقدامات فرهنگی به منظور افزایش ارزش‌های بنیادی جامعه همانند خدامحوری، ولایت‌مداری، دشمن‌ستیزی، از طریق برنامه‌های مختلف فرهنگی در بین دانشجویان توصیه می‌شود؛
- در بعد اجتماعی، مقابله با افزایش سبک زندگی غربی، تجاوز، رواج فمینیسم، مقابله افزایش بی‌اعتمادی در بین دانشجویان از طریق معرفی و ترویج سبک زندگی اسلامی ایرانی توصیه می‌شود.
- در بعد سیاسی پژوهش مقابله با بی‌عدالتی همچنین مقابله با وادار کردن افراد به نافرمانی مدنی در بین دانشجویان توصیه می‌شود. همچنین موارد زیر در کاهش جرایم فضای مجازی موثر است:
- به‌وجود آوردن امید و آینده مطلوب بین دانشجویان برای مقابله با حوزه‌های جنگ نرم؛
- معنوی کردن فضای دانشگاه و ایجاد جذابیت برای دانشجویان؛

- دانش‌افزایی استادان و دانشجویان برای مقابله با تهدیدات جنگ نرم؛
- ترغیب اساتید و دانشجویان به مطالعه و تحقیق درباره غرب، علوم غربی و مبانی آن و نمایش تناقضات و تضادهای درونی آنها با مبانی اسلام اصیل؛
- فراهم‌ساختن فضا و الگوهای رقابت سالم سیاسی و تلاش هوشمندانه برای ارتقا آستانه تحمل مردم و مسئولان در قبال انتقادهای سازنده و جلوگیری از هرگونه اقدام منجر به تنش و هرج و مرج؛
- تقویت هویت اجتماعی به‌عنوان یکی از ارکان سرمایه اجتماعی در بین دانشجویان؛
- فراهم‌کردن زمینه‌های شناخت ریشه‌های فرهنگی ایرانی و اسلامی به‌منظور ترک پذیرش فرهنگ غربی؛
- توانمندسازی دانشجویان در بعد مسائل اجتماعی درخصوص ترک پذیرش خرده‌فرهنگ‌های اجتماعی مغایر با مسائل اجتماعی جامعه؛
- پیشگیری از تمایل و گرایش دانشجویان به‌سمت آموزش‌های رفتاری نابهنجار سرچشمه گرفته از فضای مجازی که از خارج کشور هدایت می‌شود.

## منابع

- افتخاری، اصغر. (۱۳۸۹). *قدرت نرم و سرمایه اجتماعی*. تهران: دانشگاه امام صادق (ع).
- الیاسی، محمدحسین (۱۳۸۷). مقدمه ای بر ماهیت و ابعاد تهدید نرم، فصلنامه نگاه، ۲(۵)، صص قابل بازیابی از: <http://yon.ir/qqQy8>
- جلالی‌فراهانی، امیرحسین. (۱۳۸۳). پیشگیری از جرایم رایانه‌ای، *مجله حقوقی دادگستری*، شماره ۴۷، صص ۸۷-۱۱۹. قابل بازیابی از: <http://ensani.ir/fa/article/download/221627>
- حسینی‌خواه، نورالله و رحمتی، داریوش. (۱۳۸۹). *پلیس و جرایم رایانه‌ای*. تهران: انتشارات نیروی انتظامی.
- دارا، جلیل؛ الفی، محمدرضا. (۱۳۹۲). نقش مدیران فرهنگی دانشگاه‌ها در مقابله با جنگ نرم، *فصلنامه علمی پژوهشی پژوهش‌های انقلاب اسلامی*، شماره ۵، صص ۱۹۵-۲۱۲. قابل بازیابی از: <http://yon.ir/kD1xv>
- دیوید، بل (۱۳۸۹). *درآمدی بر فرهنگ‌های سایبر*. (مسعود کوثری و حسین حسینی، مترجمان). تهران: جامعه‌شناسان.
- رفیعی، عبدالله. (۱۳۸۲). *دولت‌ها و افکار عمومی*، جنگ نرم. تهران: نشر دادار.
- زندی، محمدرضا. (۱۳۸۹). *تحقیقات مقدماتی در جرایم سایبری*. چاپ اول. تهران: انتشارات جنگل.
- سنجایی شیرازی، جهانبخش. (زمستان ۱۳۸۹). مفهوم شناسی و تبار شناسی قدرت و جنگ نرم، اصول و روش‌های رویارویی با آن در منابع علمی. *فصلنامه رنگار سیاستگذاری سیاسی، دفاعی و امنیتی*، ۱(۲)، صص ۱۲۰-۱۵۷. قابل بازیابی از: <http://yon.ir/wk87X>

شاه‌محمدی، عبدالرضا. (تابستان ۱۳۸۲). وسایل ارتباطی، سربازان اصلی میدان جنگ‌های نوین. *فصلنامه پژوهش‌های ارتباطی*. ۱۰(۳۴)، ص ۴۵-۴۴. قابل بازیابی از: <http://www.magiran.com/p497938>

شمولی، همت‌اله؛ رشیدحفظ‌آباد، موسی و یعقوبی، حسین. (۱۳۹۴). بصیرت‌گرایی و بصیرت‌افزایی، راهبردی اساسی در مقابله با جنگ نرم، *فصلنامه بصیرت و تربیت اسلامی*، ۳۵(۱۲)، صص ۱۴۷-۱۹۷. قابل بازیابی از: <http://yon.ir/ZFxcck>

عالی‌پور، ابراهیم. (۱۳۹۳). *فارنسیک کامپیوتر*. تهران: انتشارات ناقوس.

عبداله‌خانی، علی. (۱۳۸۶). *جنگ نرم: نبرد در عصر اطلاعات*. تهران: ایرار معاصر.

عبدی، فریدون. (۱۳۸۹). بررسی میزان آگاهی و باور دانشجویان دانشگاه افسری امام علی (ع) نسبت به ماهیت و ابعاد مختلف جنگ نرم، *فصلنامه علمی پژوهشی مدیریت نظامی*، ۱۱(۴۱)، ص ۱۳۵-۱۵۰. قابل بازیابی از: [http://jmm.iranjournals.ir/article\\_3834.html](http://jmm.iranjournals.ir/article_3834.html)

عیوضی، محمد رحیم؛ دامیار، محمود و ایوب. (۱۳۹۵). مبانی جنگ نرم در اندیشه‌های مقام معظم رهبری، *فصلنامه حبل‌المتین*، ۵(۱۴)، صص ۲۴-۴۵. قابل بازیابی از: <http://yon.ir/JfdfsF>

غلامی، مجید. (۱۳۹۱). *جرایم رایانه‌ای*. اصفهان: مرکز تحقیقات رایانه‌ای حوزه علمیه اصفهان.

*قانون جرایم رایانه‌ای مصوب ۱۳۸۹/۱۱/۱۱ مجلس شورای اسلامی*.

قربانزاده‌سوار، قربانعلی؛ قلخان‌باز، خلیل و رحمتی، مهدی. (۱۳۹۱). جنگ نرم و امنیت اجتماعی، *فصلنامه علمی پژوهشی پاسداری فرهنگی انقلاب اسلامی*، ۲(۶)، صص ۱-۲۱. قابل بازیابی از: <http://yon.ir/cMufo>

قربان‌نیا، ناصر. (۱۳۸۳). مواجهه با تروریسم: رویکرد نظامی، سیاسی و حقوقی. *نشریه نامه مفید*. ۱۰(۴۳)، صص ۱۴۱-۱۶۸. قابل بازیابی از: <https://www.sid.ir/fa/journal/ViewPaper.aspx?id=26220>

قیاسی، رضا و مجید، وحید. (۱۳۹۴). *اصول و مبانی اطلاعات در فضای سایبر*. تهران: انتشارات دانشگاه علوم انتظامی امین. کنعانی، اکبر و محمدی برزگر، جعفر. (۱۳۹۵). شناسایی حوزه‌های تأثیرگذار تهدید نرم با رویکرد انتظامی، *فصلنامه پژوهش‌های مدیریت انتظامی*، ۱۲(۴)، صص ۶۳۱-۶۵۲. قابل بازیابی از: <http://yon.ir/a1jvT>

لطیفی‌مهر، مژگان؛ میراسماعیلی، بی‌بی‌السادات و حسینی‌دانا، حمیدرضا. (۱۳۹۳). نقش و جایگاه شبکه‌های اجتماعی در جنگ نرم علیه جمهوری اسلامی ایران، *مجله مطالعات رسانه‌ای*، ۹(۳)، صص ۲۹-۴۰. قابل بازیابی از: [http://mediastudies.srbiau.ac.ir/article\\_8204.html](http://mediastudies.srbiau.ac.ir/article_8204.html)

نائینی، علی‌محمد. (۱۳۸۹). درآمدی بر ماهیت‌شناسی جنگ نرم، *فصلنامه راهبرد دفاعی*، ۲۸(۸)، صص ۱-۳۲. قابل بازیابی از: <https://www.sid.ir/fa/journal/ViewPaper.aspx?id=133186>

نائینی، علی‌محمد. (۱۳۸۶). ناتوی فرهنگی، کارویژه‌های آن و راهبردهای مقابله. *فصلنامه عملیات روانی*، ۵(۱۸)، صص ۹۲-۱۲۴. قابل بازیابی از: <http://yon.ir/suXda>

نجات‌پور، مجید؛ محمدی، مصطفی؛ اصغری، امید و شهریاری، حیدر. (۱۳۹۱). جنگ نرم و امنیت در فضای سایبرنتیک، *فصلنامه مطالعات راهبردی بسیج*، ۱۵(۵۴)، صص ۴۹-۶۹. قابل بازیابی از: <http://ensani.ir/file/download/article/20170315101103-9959-16.pdf>

هندیانی، عبدالله و میرزاخانی، عبدالرحمن. (۱۳۹۳). نقش سرمایه اجتماعی در کاهش آثار تهدیدهای نرم (با نگاهی به فرماندهی و مدیریت آینده پلیس). *پژوهش‌های مدیریت انتظامی*. ۹(۴)، صص ۲۹-۵۰. قابل بازیابی از: [magiran.com/p1386243](http://magiran.com/p1386243)

هندیانی، عبدالله. (۱۳۹۴). *اصول و مبانی تهدیدشناسی در پیشگیری از تهدید نرم*، مجموعه مقالات پیشگیری از تهدید نرم. تهران: نشر عرصه سیم‌رغ.

یعقوبی، فابع. (۱۳۹۴). پیشگیری وضعی/از تروریسم سایبری. حق گستر، پایگاه تخصصی نشر مقالات حقوقی. قابل بازیابی از: <http://yon.ir/6ZqAj>

Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on Cyber Crime and Security. *International Journal of Research in Engineering and Applied Sciences*, 2(1), pp 48-51. Retrieved from: <http://yon.ir/P1eNS>

Berger, P. (1997). Four Faces Global Culture. *National Interest*, (46) Retrieved from: <http://yon.ir/ya4vZ>

Nye, J., S. (2004). *Soft Power: the Means to Success in World Politics*, New York: Public Affairs. Retrieved from: <http://yon.ir/H6BaA>

Archive of SID