امنیت، تاب‌آوری و محدودسازی فضای مجازی

سیدسپهر قاضی‌نوری[۱]، هادی صفری[۲]

چکیده

تدبیر شماره ۱۵ سند الگوی اسلامی ایرانی پیشرفت به امنیت و تاب‌آوری فضای مجازی و لزوم استفاده از دانش بومی و مشارکت‌های جهانی در آن اختصاص دارد. مسئله‌ای که به نظر می‌رسد در بسیاری از سیاست‌گذاری‌ها و تصمیمات عملی مرتبط با فضای مجازی به نفع نگاه امنیتیِ غیرتخصصی کنار گذاشته شده است. این نوشتار، با بررسی برخی از مهم‌ترین چالش‌های فضای مجازی و امنیت و تاب‌آوری آن در ایران، تلاش می‌کند تا پیشنهادهایی برای سیاست‌گذاری در خصوص فضای مجازی در ایران ارائه کند. فاصله گرفتن از گفتمان امنیتی در مسائل زندگی روزمره، کاهش جرم‌انگاری‌ها، بهبود شرایط و جذب شرکت‌های خارجی حوزه فضای مجازی به جای دفع آنها، بهبود شرایط اقتصادی- فرهنگی برای عدم مهاجرت متخصصان این حوزه، باز گذاشتن فضا برای تنظیم‌گری مردمی فضای مجازی به دور از دخالت‌های حاکمیتی و توجه به اسناد بالادستی از جمله سند الگوی اسلامی ایرانی پیشرفت برخی از راهکارها و پیشنهادهای سیاستی مطرح شده در این نوشتار هستند.

واژگان کلیدی: فضای مجازی، امنیت سایبری، تاب‌آوری سایبری، امنیت ملی، سیاست‌گذاری فناوری.

۱. مقدمه

سند الگوی اسلامی ایرانی پیشرفت به عنوان سندی بالادستی برای هدایت ایران در مسیر تبدیل به خاستگاه تمدن نوین اسلامی در "مرکز اسلامی ایرانی پیشرفت" تدوین شده و به‌رغم برخی انتقاداتی که به این سند وارد است (زاهدی مازندرانی: ۱۳۹۸: ۷۳)، سند مذکور نقشه‌راهی سطح بالا برای دستگاه‌های اجرایی و نهادهای قانون‌گذار فراهم می‌کند تا پیمودن این مسیر را تسهیل نمایند. قلب این سند را «تدبیر»های پنجاه‌ودوگانه‌ای تشکیل می‌دهند که تصمیمات و اقدامات اساسی و بلندمدت مورد نیاز برای پیمودن مسیر را مشخص می‌کنند. از این بین، سه تدبیر ۱۵ تا ۱۷ به‌طور مستقیم به فضای مجازی و سیاست‌گذاری آن مرتبطند که بیانگر اهمیت فضای مجازی در نقشه‌راه پیشرفت کشور و آیندهٔ جهان است. تدبیر شمارهٔ ۱۵ «ارتقای دانش و توسعهٔ بومی و تأمین امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی با مشارکت مردمی و همکاری‌های بین‌المللی در تراز کشورهای پیشرو جهان» را به عنوان اولین اصل مرتبط با فضای مجازی مورد تأکید قرار می‌دهد (مرکز الگوی اسلامی ایرانی پیشرفت: ۱۳۹۷: ۱۸).

فضای مجازی ویژگی‌های خاصی دارد که آن را از فضای واقعی متمایز می‌کند. به طور خلاصه، هزینهٔ ورود پایین، فراهم آوردن امکان گمنامی، آسیب‌پذیری نامتقارن، جهانی و فرامرزی بودن، دسترسی دائم و آسان به آخرین اطلاعات، تنوع، استقلال از زمان و مکان، چندرسانه‌ای بودن، سهولت استفاده و تعامل و سرعت بالای تبادل اطلاعات،

۱. استاد گروه مدیریت فناوری اطلاعات دانشگاه تربیت مدرس، عضو اندیشکده چرخه نوآوری مرکز الگوی اسلامی ایرانی پیشرفت، نویسنده مسئول، ghazinoory@modares.ac.ir.

۲. دانشجوی دکتری سیاست‌گذاری علم و فناوری دانشگاه تربیت مدرس.

برخی از مهم‌ترین ویژگی‌های فضای مجازی هستند (زندی و سیاه‌بالایی: ۱۳۹۹: ۲۱۵). این ویژگی‌ها، در کنار تأثیرگذاری بالای فضای مجازی در زیست روزمرهٔ انسان معاصر (ذکایی و ویسی: ۱۳۹۹: ۱۱) و رفتار اجتماعی او (کاستلز: ۱۳۹۳: ۱۴) و حتی روابط بیناکشوری، دیپلماسی و قدرت نرم (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۵۹)، باعث می‌شود نگاهی ویژه به مسائل فضای مجازی ضرورت داشته باشد.

امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی مسألهٔ پیچیده‌ای است که جنبه‌های فنی، امنیتی، جامعه‌شناختی، فرهنگی، روان‌شناختی و اقتصادی را در بر می‌گیرد. جنبه‌های سخت امنیت و تاب‌آوری بر مسائل فنی و امنیت سخت‌افزاری و نرم‌افزاری متمرکز است و جنبه‌های نرم آن به مسائل فرهنگی، اجتماعی و محتوایی می‌پردازد. با نگاهی جامع‌تر، اثرات فضای مجازی بر امنیت ملی، تاب‌آوری اجتماعی و فرهنگ جامعه را نیز می‌توان جزئی از جنبه‌های نرم امنیت و تاب‌آوری فضای مجازی دانست.

به‌رغم تأکید بر الزامات سیاست‌گذاری در حوزهٔ فضای مجازی و امنیت و تاب‌آوری آن، ضمن توجه به توسعهٔ بومی، مشارکت مردم و همکاری‌های بین‌المللی در اسناد بالادستی (مرکز اسلامی ایرانی پیشرفت: ۱۳۹۷: ۱۸) و بیانات مقام معظم رهبری (رضاپور و اسکندری‌نسب: ۱۳۹۸: ۱۱۹)، به نظر می‌رسد برخی سیاست‌گذاری‌های این حوزه، قوانین مصوب و تصمیمات اجرایی ناظر بر محدودسازی فضای مجازی بدون توجه به ظرافت‌های تصمیم‌گیری دربارهٔ مسائل فضای مجازی صورت گرفته و تصمیم‌گیرندگان توجهی به تبعات آسیب‌زای تصمیمات‌شان نداشته‌اند. سیاست‌گذاری یک‌طرفهٔ مبتنی بر روش‌های سلبی و محدودسازی بیش از حد فضای مجازی، بر خلاف تصور اولیه، می‌تواند باعث آسیب دیدن شدید امنیت و تاب‌آوری فضای مجازی کشور گردد. اثر حاضر تلاش می‌کند تا به شیوهٔ توصیفی تحلیلی به این سؤال پاسخ دهد که برای تأمین امنیت و تاب‌آوری شبکه چه تدبیری باید اندیشیده شود و جایگاه محدودسازی فضای مجازی در این بین کجاست.

۲. پیشینهٔ پژوهش

عمدهٔ پژوهش‌های غیرفنی فارسی در حوزهٔ امنیت و تاب‌آوری فضای مجازی بر تبعات فرهنگی و امنیتی فضای مجازی متمرکز بوده‌اند. رضاپور و اسکندری‌نسب (۱۳۹۸) با تأکید بر جنبه‌های فرهنگی به امنیت فضای سایبر از دیدگاه مقام معظم رهبری پرداخته‌اند. آن‌ها اعتمادسازی و تقویت سرمایهٔ اجتماعی، مشارکت‌آفرینی، آگاه‌سازی، دیپلماسی فرهنگی، بصیرت اجتماعی و استفاده از هنر و به بیانی کلی، کاهش تهدیدها و افزایش فرصت‌ها در بستر اجتماع را شیوه‌های رسیدن به امنیت فضای سایبر از دیدگاه ایشان دانسته‌اند (همان: ۱۱۹). زندی و سیاه‌بالایی (۱۳۹۹) به نقش فضای مجازی در تهدید علیه امنیت ملی پرداخته‌اند. آن‌ها معتقدند رفتارشناسی کاربران فضای مجازی و ایجاد بستر مناسب برای تولید محتوای ایرانی اسلامی به دست خود کاربران و بدون دخالت حکومتی و توجه به مسألهٔ شکاف دولت-ملت و تقویت انسجام اجتماعی را از جمله مسائل قابل توجه در برخورد با فضای مجازی است (زندی و سیاه‌بالایی: ۱۳۹۹: ۲۱۸). خلیلی جولرستانی (۱۳۹۶) به چالش‌ها و تهدیدات فضای مجازی برای

امنیت ملی پایدار پرداخته است. یافته‌های بررسی او دربارهٔ دانشجویان دو دانشگاه دولتی کشور نشان می‌دهد بیش از هشتاد درصد جمعیت مورد بررسی از سایت‌های فیلترشده بازدید می‌کنند. او معتقد است فرهنگ‌سازی دربارهٔ کاربری اینترنت و آفندها و مخاطرات سایبری نتیجه‌ای مطلوب‌تر از فیلترینگ خواهد داشت (خلیلی جولرستانی: ۱۳۹۶: ۱۴۷). همچنین، از نظر او در مسیر همراه‌سازی هویتی باید هویت ملی و هویت دینی به شکل مکمل یکدیگر عمل کنند (همان: ۱۶۲) و تأکید بر یکی بدون دیگری کارساز نیست. پالیزبان (۱۳۹۴) معتقد است اینترنت قابلیت‌های فراوان و نیز تهدیدات و ناامنی‌هایی برای کشورها ایجاد می‌کند؛ ولی در مجموع، امنیت ملی کشور با اینترنت و امنیت فضای مجازی پیوستگی مثبتی دارد. او فقدان گفتمان امنیتی مناسب و انعطاف‌ناپذیری نهادهای متولی را از مشکلات برخورد با اینترنت در ایران می‌داند. میربیک سبزواری و دیگران (۱۴۰۱) معتقدند عملکرد، ادراک، احساس، رفتار، تولید محتوا و میزان توان‌مندی کاربران بر چگونگی امنیت فرهنگی در فضای مجازی اثرگذار است. او معتقد است فضای مجازی هم می‌تواند برای کاربران حس امنیت ایجاد کند و هم می‌تواند امنیت آن‌ها را مختل کند و در این بین، عامل تعیین‌کننده آگاه‌سازی کاربران است (میربیک سبزواری و دیگران: ۱۴۰۱: ۶۰). دانش و دیگران (۱۳۹۸) معتقدند که ابعاد اجتماعی، اقتصادی و سیاسی شایعات فضای مجازی بر امنیت جامعه تأثیر می‌گذارد. محمدی (۱۳۹۷) نشان داده است داعش از فضای مجازی برای ایجاد تهدیداتی مانند جذب نیرو از میان اقلیت‌های مذهبی ایران، ایجاد رعب و وحشت و اختلاف‌افکنی کمک گرفته است.

جنبه‌های دیگری از ماجرا نیز مورد توجه پژوهشگران بوده است. ایزدی و خادم‌زاده (۱۳۹۸) به تأثیر فضای مجازی در دیپلماسی عمومی ایران و قدرت نرم کشور پرداخته‌اند. آن‌ها ضمن اشاره به ضرورت توجه به فضای مجازی در شکل‌گیری دیپلماسی نرم، به ضعف کشور در استفاده از ظرفیت سازمان‌های غیردولتی، شبکه‌های اجتماعی و برندسازی ملی اشاره کرده‌اند. ذکایی و ویسی (۱۳۹۹) به بررسی انواع مختلف احساسات، عواطف و خرده‌فرهنگ‌ها در فضای مجازی پرداخته‌اند. عبدلی‌پیران (۱۳۹۹) معتقد است هرچند فضای مجازی می‌تواند معنای زندگی جوانان را تحت تأثیر قرار دهد، اما میزان استفاده از آن بر تاب‌آوری اجتماعی جوانان تأثیری نمی‌گذارد.

پژوهش‌هایی نیز دربارهٔ مسائل امنیت و تاب‌آوری فضای مجازی در کشورهای دیگر صورت گرفته است. از جمله، رستمعلی‌زاده و حاجی‌ملامیرزایی (۱۳۹۹) به بررسی نظام حقوقی فیلترینگ در آمریکا پرداخته‌اند. مسائل مربوط به پورنوگرافی کودکان، حفاظت از مالکیت فکری و تنظیم‌گری قماربازی آنلاین از جمله مسائلی هستند که ممکن است به فیلتر شدن یک پایگاه اینترنتی در آمریکا منجر شوند. با این حال، متمم اول قانون اساسی آمریکا در خصوص تضمین آزادی بیان، به عنوان قانون بالادستی حاکم بر قوانین فدرال و ایالتی دیگر، فیلترینگ فضای مجازی را در آمریکا بسیار محدود می‌کند. همچنین در این کشور، فیلترینگ بر عهدهٔ یک نظام قضایی مستقل است که باعث می‌شود اعمال سلیقه‌ها و جهت‌گیری‌های سیاسی و مقطعی دولت حاکم باعث محدودسازی پایگاه‌های اینترنتی نشود (رستمعلی‌زاده و حاجی‌ملامیرزایی: ۱۳۹۹: ۱۶۷۸). داهان (۱۹۹۹) معتقد است ورود اینترنت، فضای سیاسی رژیم صهیونیستی را تغییر داده و ضمن تضعیف محدودیت‌های سنتی و سانسور گسترده، باعث گسترش فرهنگ دموکراتیک و تقویت امنیت ملی گشته است. کوواکس (۲۰۱۸) به اهمیت برنامه‌های امنیت سایبری در تأمین امنیت

ملی کشورها اشاره کرده است. آسگوا (۲۰۲۰) به اهمیت فضای مجازی، در کنار انواع سنتی‌تر رسانه‌ها، در تأمین امنیت ملی اشاره کرده است. هاروپ و متیسون (۲۰۱۴) به اهمیت مقاوم‌سازی زیرساخت‌های سایبری در برابر گسترهٔ وسیعی از تهدیدات و حملات سایبری با تأکید بر عملکرد آمریکا و انگلیس پرداخته‌اند. گلداسمیت و وو (۱۴۰۱) نیز به سازوکارهای کنترل دولت‌ها بر اینترنت می‌پردازند و از جمله، به قوانین متفاوت کشورها در حوزه‌هایی مانند آزادی بیان اشاره می‌کنند که باعث می‌شود اجماع جهانی بر چگونگی مدیریت فضای سایبری به امری دشوار بدل شود.

۳. فضای مجازی

تلاقی علوم ارتباطات، الکترونیک، کامپیوتر و فناوری‌های ارتباطی نوین، دنیای معاصر را به جهانی چهاربُعدی تبدیل می‌کند که در گذشته نظیر آن وجود نداشته است. زمان، مکان، فاصله و سرعت، چهار بُعد این جهان جدید را تشکیل می‌دهند و مرزها، قوانین، مقررات قضایی و محدودیت‌ها را تحت تأثیر قرار می‌دهند (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۵۸). به‌خصوص در اوایل دوران ظهور اینترنت، تصور بر این بود که این ابزار با متصل کردن همهٔ انسان‌های روی زمین، جهان را به جایی بهتر تبدیل می‌کند، انسان را از جهانی که در آن زندگی می‌کند می‌رهاند، برساخت دولت-ملت را به کناری می‌زند و اقتدار دولت‌ها و نظام حکومت سرزمینی را به چالش می‌کشد (گلداسمیت و وو: ۱۴۰۱: ۴۱). در عصر شبکه، دولت تنها به یکی از کنشگران تأثیرگذار شبکه تبدیل می‌شود و کنشگران دیگری مانند تولیدکنندگان، مصرف‌کنندگان و منتشرکنندگان اطلاعات نیز در قدرت سهیم می‌گردند (خجستهٔ باقرزاده و خجستهٔ باقرزاده: ۱۴۰۰: ۱۸۰)؛ چنان‌که برای مثال، تنظیم‌گری نرخ کرایهٔ حمل‌ونقل که سابقاً در انحصار حاکمیت بود، امروزه عملاً در اختیار شرکت‌های حمل‌ونقل آنلاین است. فضای مجازی ساختار ارتباطات را تغییر داده و خودارتباطی توده‌ای به وجود آورده که به نوبهٔ خود، باعث خودمختاری بیشتر کنشگران اجتماعی می‌شود (کاستلز: ۱۳۹۳: ۱۴).

اینترنت سیاست خارجی را نیز دگرگون کرده است. در دنیای امروز، قوی‌ترین دولت‌ها آن‌هایی نیستند که بزرگ‌ترین ارتش‌ها را در اختیار دارند؛ بلکه دولت‌هایی هستند که از بیشترین ارتباطات برخوردارند و در مرکز بیشترین شبکه‌ها قرار دارند (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۵۹). در جامعهٔ شبکه‌ای چند نوع قدرت وجود دارد که بر شبکه و کنشگران آن تأثیرگذارند (کاستلز: ۱۳۹۸: ۶۱). از این بین، قدرت شبکه‌سازی، به عنوان مهم‌ترین نوع قدرت شبکه، از دو طریق حاصل می‌شود: برنامه‌ریزان توانایی ساخت و برنامه‌ریزی مجدد شبکه‌ها را دارند و راه‌گزین‌ها می‌توانند شبکه‌های مختلف را به هم متصل کنند و از آن بهره بگیرند (همان: ۶۶).

زندگی فردی و روابط بینافردی افراد نیز از تأثیر فضای مجازی به دور نمانده است. از منظر فردی، ویژگی‌هایی مانند هزینهٔ ورود پایین، فراهم آوردن امکان گمنامی، آسیب‌پذیری نامتقارن، جهانی و فرامرزی بودن، دسترسی دائم و آسان به آخرین اطلاعات، تنوع، استقلال از زمان و مکان، چندرسانه‌ای بودن، سهولت استفاده و تعامل و سرعت

بالای تبادل اطلاعات برخی از مهم‌ترین فضای مجازی را از رسانه‌ها و فضاهای سنتی‌تر متمایز می‌کنند (زندی و سیاه‌بالایی: ۱۳۹۹: ۲۱۵). فضای مجازی همچنین زیست عاطفی مردم را دگرگون کرده و نظم و منطق تازه‌ای بر زندگی انسان معاصر حاکم نموده است (ذکایی و ویسی: ۱۳۹۹: ۱۱). هان (۱۳۹۸) سرمایه‌داری مبتنی بر فضای مجازی را به رژیمی الهیاتی برای دنیای مدرن تشبیه کرده است: از نظر او، گوشی‌های هوشمند همانند تسبیح همیشه در دست هستند، لایک همانند آمین دیجیتالی از همراهی افراد با آرزوهایی که دیگران بیان کرده‌اند حکایت می‌کند و شبکه‌های مجازی نیز همانند کلیساهای کیش جدید، محل تجمع مؤمنین و نیز اعتراف آن‌ها به اعمالشان است (هان: ۱۳۹۸: ۲۵).

نقش گسترده و فراگیر فضای مجازی بر جنبه‌های مختلف فردی و اجتماعی زندگی بشری، توجه دولت‌ها به این حوزه و دقت در ظرافت‌های سیاست‌گذاری را ضروری می‌سازد.

۴. امنیت و تاب‌آوری فضای مجازی

امنیت فناوری هم چالشی برای دولت‌ها و هم مانعی بر سر استفادهٔ شهروندان از امکانات و تسهیلات فضای مجازی است. امنیت یک سامانهٔ اطلاعاتی به معنی حمایت از اطلاعات و سامانه‌ها در برابر افشای تصادفی یا عمدی در برابر دسترسی‌های غیرمجاز یا تغییرات یا تخریب غیرمجاز است. بر این اساس، در توسعهٔ فضای مجازی باید هم در لایهٔ امنیت شبکه و هم در لایهٔ امنیت اسناد تمهیدات مناسب اندیشیده شود و خط‌مشی‌ها و استانداردهای لازم تعیین گردد (عاملی: ۱۳۹۶: ۷۸). تاب‌آوری نیز ارتباط تنگاتنگی با امنیت دارد و به معنی توانایی تولید متداوم خروجی مورد انتظار یک سامانهٔ مجازی حتی در شرایط وقوع حملات سایبری است (بیورک و دیگران: ۲۰۱۵: ۳۱۱). با یک دیدگاه گسترده‌تر، امنیت پایدار دیجیتالی را نه فقط به عنوان توسعهٔ فنی بلکه باید به مثابهٔ حالتی روحی، طرز تفکر و یک حرکت عمومی جهانی توصیف نمود (خلیلی جولرستانی: ۱۳۹۶: ۱۵۸).

امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی مسألهٔ پیچیده‌ای است که جنبه‌های فنی، امنیتی، جامعه‌شناختی، فرهنگی، روان‌شناختی و اقتصادی را در بر می‌گیرد. به همین دلیل، روش‌های سنتی ارزیابی ریسک برای حل مسألهٔ امنیت و تاب‌آوری سامانه‌های مجازی چندان مؤثر نیستند و نمی‌توانند مخاطرات مختلف ناشی از حوزه‌های گوناگون فیزیکی، اطلاعاتی، شناختی، اجتماعی و... سامانه‌های مجازی را پوشش دهند (لینکوف و کات: ۲۰۱۹: ۲). جنبه‌های سخت امنیت و تاب‌آوری بیشتر بر زیرساخت فنی متمرکز است و مسائلی مانند تأمین و تعمیر سخت‌افزارهای رایانه‌ای نوین، توسعهٔ نرم‌افزارهای رایانه‌ای مورد نیاز، ارتباط مطمئن با نرم‌افزارهای رایانه‌ای خارجی، شبکهٔ ارتباطی پرسرعت و اتکاپذیر، مراکز فیزیکی امن و مجهز در نقاط مختلف کشور و زیرساخت تأمین و توزیع برق و ارتباطات جهانی اختصاص دارد. در مقابل، جنبه‌های نرم امنیت و تاب‌آوری بیشتر به محتوا، فرهنگ، نحوهٔ استفاده، ظرفیت جذب فناوری‌ها و دانش وارداتی، توان اشاعه و تبلیغ فرهنگ داخلی، حفاظت اطلاعات و مواردی از این دست

می‌پردازد. با نگاهی جامع‌تر، اثرات فضای مجازی بر امنیت ملی، تاب‌آوری اجتماعی و فرهنگ جامعه را نیز می‌توان جزئی از جنبه‌های نرم امنیت و تاب‌آوری فضای مجازی دانست.

۵. چالش‌های امنیت و تاب‌آوری فضای مجازی در ایران

بخشی از مسائل امنیت و تاب‌آوری فضای مجازی در ایران به جنبه‌های سخت و مسائل فنی برمی‌گردد. موانع زیرساختی، اقتصادی و سازمانی می‌تواند در توسعهٔ جنبهٔ سخت فضای مجازی چالش‌هایی ایجاد کند (عاملی: ۱۳۹۶: ۶۹) تأمین امنیت فیزیکی و مجازی مراکز تهیه و توزیع برق در شبکه، یکی از اولین لایه‌های تأمین تاب‌آوری در این سطح است. در وهلهٔ بعد، مراکز دادهٔ متعدد، مجهز و ارزان در نقاط مختلف، امنیت و به‌خصوص تاب‌آوری فضای مجازی را تضمین می‌کنند. قرار دادن نسخه‌های متعدد از داده‌ها در نقاط فیزیکی مختلف و اجرای همزمان نسخه‌های مختلف از خدمات فضای مجازی از طریق نقاط فیزیکی مختلف تاب‌آوری خدمات را در مقابل حملات فضای مجازی افزایش می‌دهد. توزیع داده‌ها و خدمات در سطح دنیا می‌تواند تاب‌آوری را از این منظر به‌شدت افزایش دهد؛ با این حال، به دلیل نگاه امنیتی برخی سیاست‌گذاران و تصمیم‌گیران اجرایی داخلی، کیفیت پایین ارتباطات اینترنتی بین‌المللی کشور، محدودیت‌ها و فیلترینگ اعمال‌شده و نیز ناپایداری و قطعی مکرر آن و همچنین اقدامات خصمانهٔ دولت‌های غربی و به‌خصوص آمریکا، توزیع جغرافیایی داده‌ها و خدمات فضای مجازی بسیار دشوار است.

از سمت دیگر، حضور مشتریان خارجی در مراکز دادهٔ داخلی می‌تواند هزینهٔ تهدید امنیتی این مراکز داده را بالا ببرد و نقشی مهم در تأمین امنیت فضای مجازی کشور ایفا کند. به دلایل مشابه، مشتریان خارجی به‌ندرت از مراکز داده و زیرساخت فناوری اطلاعات ایران استفاده می‌کنند. حضور مشتریان خارجی در کشور، علاوه بر کمک به توسعهٔ اقتصادی و انتقال فناوری، می‌تواند به نهادهای قضایی و قانون‌گذار کشور اجازه بدهد تأثیرگذاری بر رفتار شرکت‌های خارجی تأثیر بگذارند. حضور شرکت آمریکایی یاهو با دارایی‌های فراوان در کشور فرانسه بارها به نظام قضایی فرانسه اجازه داده که قوانین سرزمینی خود را بر یاهو نیز اعمال کند؛ اما یاهو در فیجی یا غنا حضور ندارد و در نتیجه، انتخاب‌های کشوری مانند فیجی در اعمال حاکمیت به گزینه‌هایی ناکارا و پرهزینه‌ای مانند مسدودسازی کلی اینترنت یا اعمال قانون از طریق واسطه‌های شبکه مانند تأمین‌کنندگان محلی اینترنت (ISPها) محدود می‌کند (گلداسمیت و وو: ۱۴۰۱: ۱۱۴).

به عنوان نمونه‌ای دیگر، شرکت ای‌بی در سال ۲۰۰۵ در بسیاری از اقتصادهای برتر دنیا حضور داشته ؛ اما به‌رغم وجود بازاری بزرگ در ایران، ترکیه و روسیه، به دلیل شرایط نامساعد و نظام قضایی ناسازگار با حضور شرکت‌های چندملیتی و خارجی، عطای حضور در این بازارها را به لقای‌شان بخشیده و به جای آن به سراغ کشورهایی با اقتصادی کوچک‌تر اما با نظام قضایی مناسب‌تر رفته است (همان: ۱۷۲).

نمونه‌ای متفاوت، اتحادیهٔ اروپا و قوانین حفاظت از داده‌های کاربران آن است. دستورالعمل سال ۱۹۹۸ اتحادیهٔ اروپا در این خصوص، شرکت آمریکایی مایکروسافت را در دوراهی انتخاب بین پیروی از خواسته‌های حقوقی اتحادیهٔ اروپا یا خروج از بازار اروپا قرار داد. خروج از بازار اروپا برای مایکروسافت به معنی از دست دادن یک‌سوم سهم بازارش بود و بنابراین، گزینهٔ اول را برگزید. علاوه بر این، مایکروسافت این قوانین را نه فقط برای کاربرانش در اتحادیهٔ اروپا، بلکه برای همهٔ کاربرانش در هر جای دنیا اجرایی کرد (همان: ۲۰۷). بدیهی است در شرایط مشابه، شرکتی همانند مایکروسافت ترجیح می‌دهد از بازار ایران خارج شود و قوانین آن را رعایت نکند، چون بازار بزرگی در ایران ندارد. قوانین سخت‌گیرانه و بیش‌ازحد و محیط نامساعد و ناپایدار اقتصادی، همراه با نگاه امنیتی و سایر دلایل مطرح‌شده شرکت‌های خارجی را از کشور می‌راند.

اتخاذ راهکارهای ساده‌انگارانه و پرهزینه بدون توجه به تبعات مستقیم و غیرمستقیم آن‌ها که عمدتاً برآمده از نگاه امنیتی و غیرتخصصی هستند در تأمین امنیت و تاب‌آوری در این سطح نیز مشکلاتی ایجاد کرده است. برای مثال، محدودسازی ارتباطات بین‌المللی و قطع دسترسی آدرس‌های IP خارج از ایران به سایت‌های دولتی برای مقابله با حملات امنیتی، محرومیت از خدمت توزیع‌شده (DDoS) با شیوه‌های مختلف، منجر به محدودسازی ارتباط از خارج از کشور با سامانه‌های بانکی برخط برای مقابله با جرائم مالی فضای مجازی، دسترسی ایرانیان خارج از کشور را به این سامانه‌ها مختل می‌کند و بر دیپلماسی نرم کشور نیز تأثیرات منفی جدی دارد، اما مقاومت چندانی در برابر مخاطرات امنیتی مذکور ایجاد نمی‌نماید.

توسعهٔ نرم‌افزارهای تشکیل‌دهندهٔ فضای مجازی و دسترسی به نرم‌افزارهای خارجی، جنبهٔ دیگری از وجه سخت تأمین امنیت و تاب‌آوری فضای مجازی است. از یک سو، توسعهٔ زیرساخت‌های نرم‌افزار مانند سیستم‌عامل‌ها و ضدویروس‌ها و به‌روز نگه داشتن آن‌ها فعالیتی است که در همهٔ دنیا در سطح جهانی صورت می‌گیرد. تحریم‌های آمریکا از یک طرف و نگاه امنیتی داخلی و کیفیت و پایداری اندک ارتباطات اینترنتی بین‌المللی ایران از سویی دیگر، امنیت و تاب‌آوری فضای مجازی را در این جنبه با چالش‌هایی جدی روبه‌رو کرده است. در زمینهٔ توسعهٔ نرم‌افزارهای داخلی نیز ناپایداری و شرایط نامناسب اقتصادی شرکت‌های کوچک و بزرگ حوزهٔ فناوری اطلاعات را با مشکلات جدی روبه‌رو ساخته و بسیاری از این شرکت‌ها را به تعطیلی کشانده است. اتصال پایدار، ارزان، سریع و بدون محدودیت به اینترنت جهانی برای این شرکت‌ها همانند هوا برای موجودات زنده ضروری است که به دلیل مشکلات زیرساختی و نگاه امنیتی تأمین نمی‌گردد.

شرایط دشوار اقتصادی و فرهنگی در ایران، همزمان با سرمایه‌گذاری گستردهٔ کشورهای جهان هم در غرب و هم در حوزهٔ خلیج فارس برای جذب متخصصین این حوزه، بسیاری از متخصصین حوزهٔ فناوری اطلاعات و کارگران یقه‌سفید باسابقه را به سمت مهاجرت سوق داده و کشور را در این حوزه با بحران نیروی انسانی روبه‌رو نموده است؛ به‌خصوص که اکثر این افراد از اعضای طبقهٔ متوسط هستند که شرایط اقتصادی و ارزش‌های فرهنگی آن‌ها در سال‌های اخیر بیش از سایر اقشار در معرض تهدید قرار گرفته است. همچنین، کارکنان حوزهٔ فناوری اطلاعات به

عنوان یک فعالیت دانشی به‌شدت نیازمند آرامش ذهنی هستند و بیش از برخی از مشاغل دیگر تحت تأثیر متغیرهای اقتصادی و فرهنگی قرار می‌گیرند.

در جنبهٔ نرم امنیت و تاب‌آوری فضای مجازی مسائل دیگری مطرح است. انقلاب اطلاعاتی باعث دسترسی شهروندان به اطلاعات گسترده و قدرت‌یابی نهادهای غیردولتی در عرصهٔ سیاست و اجتماع شده است. دخالت مستقیم دولتی و حکومتی در حوزهٔ فضای مجازی کارایی پایینی دارد و پیش از این نیز شکست خورده است (خلیلی جولرستانی: ۱۳۹۶: ۱۶۸). به جای بازآزمودن آزموده، باید با ایجاد بسترهای مناسب، تولید محتوا را به خود کاربران سپرد (زندی و سیاه‌بالایی: ۱۳۹۹: ۲۱۸) که می‌تواند به شکل فردی یا به صورت جمعی و در قالب سازمان‌های مردم‌نهاد، احزاب و... صورت گیرد. استفاده از ظرفیت‌های مشارکت مردم در اسناد بالادستی جمهوری اسلامی ایران مانند الگوی اسلامی ایرانی پیشرفت نیز مورد تأکید قرار گرفته است. با این حال، یکی از مهم‌ترین مشکلات ساختاری جمهوری اسلامی ایران در حوزهٔ فضای سایبری، عدم بهره‌گیری از ظرفیت‌های سازمان‌های غیردولتی است. تأکید بر سلسله‌مراتب بوروکراسی دولتی، تفکر دولت‌محور، نگاه امنیتی به فعالیت‌ها و به همهٔ مسائل، از جمله سازمان‌های غیردولتی و فضای مجازی و سیاست خارجی، کمبود منابع مالی و ضعف انجمن‌های دوستی و انجمن‌های مشترک علمی، از جمله دلایل عملکرد ضعیف ایران در این حوزه است (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۶۶).

در میان انبوه اطلاعات در حال پراکنده شدن در فضای مجازی، مرز واقعیت و فراواقعیت و حقیقت و دروغ مشخص نیست؛ بنابراین شایعه‌سازی به یکی از ویژگی‌های مهم این فضا بدل می‌شود (ذکایی و ویسی: ۱۳۹۹: ۴۹۰). شایعات فضای مجازی یکی از چالش‌های مهم این فضا برای دولت‌هاست؛ چرا که ابعاد اجتماعی، اقتصادی و سیاسی شایعات فضای مجازی بر امنیت جامعه تأثیر می‌گذارد (دانش و دیگران ،۱۳۹۸). با این حال، اثرگذاری شایعات به عواملی خارج از شبکهٔ مجازی وابسته است. در شرایط محدودیت و ضعف رسانه‌های داخلی و محدودیت‌های دسترسی کاربران داخلی به زیرساخت‌های ارتباطی و نیز فقدان اطلاع‌رسانی‌های رسمی یا بی‌اعتمادی مردم به آن‌ها، مرجعیت شبکه به خارج از ایران منتقل می‌شود و شایعات می‌توانند فضای اینترنت را در دست بگیرند (صفری: ۱۴۰۰: ۷۳). اگر نیاز به آگاهی سیاسی مورد نیاز از رسانه‌های رسمی تأمین نشود، این اطلاعات از منابع قابل دسترس دیگر به منطق و باور مردم وارد می‌شود. عدم امنیت سیاسی و شکاف دولت-ملت نیز زمینه‌های پذیرش شایعات را مهیا می‌کند (دانش و دیگران ،۱۳۹۸). شایعاتی بیشتر رواج می‌یابد که به روایت‌ها و عواطف دلخواه فردی و جمعی کاربران فضای مجازی نزدیک‌تر باشد (ذکایی و ویسی: ۱۳۹۹: ۴۹۰)؛ بنابراین با افزایش شکاف دولت-ملت و قطبی‌سازی، شایعات علیه دولت که امنیت ملی را دچار مخاطره می‌کنند بیشتر پخش می‌شود. قطبی شدن فضای مجازی با قطبی شدن جامعه رابطه‌ای دوسویه دارد (دلاوری و دیگران: ۱۴۰۲: ۳۰) و با کاهش شکاف دولت-ملت در جامعهٔ واقعی، می‌توان قطبیت فضای مجازی و در نتیجه انتشار شایعات در آن را نیز کنترل کرد. استفادهٔ صحیح از فضای مجازی می‌تواند نظرات کاربران داخلی و خارجی را به نفع کشور تغییر دهد (صفری: ۱۴۰۱: ۷۶) و در تقویت هویت ملی و برندسازی مؤثر باشد.

ایجاد برند ملی هم در سطح جهانی باعث افزایش قدرت نرم، تقویت دیپلماسی عمومی و زدودن تصورات و ذهنیت‌های غلط دربارهٔ یک کشور مؤثر است (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۶۹) و هم باعث تقویت هویت ملی مردم کشور (خلیلی جولرستانی: ۱۳۹۶: ۱۶۲) می‌شود و در نتیجه، امنیت فرهنگی (میربیک سبزواری و دیگران: ۱۴۰۱: ۱۶۲) را نیز بهبود می‌دهد. با وجود امکاناتی مانند تاریخ و فرهنگ کهن، جغرافیای سیاسی، جغرافیای طبیعی، ادبیات و فرهنگ غنی برآمده از ترکیب پیش‌زمینه‌های ایرانی و آموزه‌های اسلامی، ایران در این زمینه هم جایگاه مناسبی ندارد و به نظر می‌رسد مسؤولین امر توجه کافی به برندسازی و تقویت هویت ملی در فضای مجازی نشان نداده‌اند (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۷۰). تبلیغ و اشاعهٔ تولیدات فرهنگی در فضای مجازی در بین کشورهای شرق آسیا نیز مورد توجه قرار گرفته است. برای مثال، ژاپن توانسته با استفاده از پویانمایی‌ها (انیمه) و کتاب‌های مصور (مانگا) خاص خود، فرهنگ ژاپنی را در جهان و به خصوص آمریکا گسترش دهد و جوانان کشورهای مختلف را به خود جذب نماید (خوش‌سلیقه و فاضلی حق‌پناه: ۱۳۹۵: ۷۱). کرهٔ جنوبی نیز با استفاده از مجموعه‌های تلویزیونی (فاضلی حق‌پناه و خوش‌سلیقه: ۱۳۹۷: ۸۸) و موسیقی (پاپ کره‌ای) هدف مشابهی را دنبال کرده است. دولت کره به این شکل توانسته است تصویر ملی کره را بهبود بخشد، صادرات آن کشور را افزایش دهد، گردشگر جذب کند و جوانان کشورهای خارجی را به کره علاقه‌مند کند (ادیب سرشکی: ۱۳۹۱: ۷۶۶). در فضای مجازی ایران نیز طرفداران پاپ کره‌ای به عنوان یک گروه منسجم حضور دارند و نوشته‌های برخی از خوانندگان پاپ کره‌ای به‌دفعات در اجتماعات مجازی ایرانیان خوانده می‌شود و بازنشر می‌یابد (رهبری و صفری: ۱۴۰۰).

امروزه استفادهٔ دولت‌ها از شبکه‌های اجتماعی برای پیگیری دیپلماسی عمومی و صیانت از امنیت ملی از الزامات اساسی و ناگزیر دولت‌هاست. با این حال، ارزیابی‌های بین‌المللی نشان می‌دهد ایران در این حوزه بین کشورهای جهان در رتبهٔ ۱۱۲ قرار داشته است و از کشورهایی نظیر قزاقستان، تاجیکستان، افغانستان و نپال نیز ضعیف‌تر عمل کرده است. نگاه منفی دولتمردان ایرانی به شبکه‌های اجتماعی، فقدان آموزش و برداشت صحیح از ماهیت فناوری در کشور و موانع سخت‌افزاری و فنی کشور از دلایل ضعف عملکرد جمهوری اسلامی ایران در این حوزه به شمار می‌رود (ایزدی و خادم‌زاده: ۱۳۹۸: ۱۶۴).

۶. نتیجه‌گیری

به نظر می‌رسد غلبهٔ نگاه امنیتی، سلبی و غیرتخصصی بر نگاه‌های ایجابی مبتنی بر فرهنگ‌سازی مردمی در حوزهٔ فضای مجازی یکی از علل اصلی مشکلات فضای مجازی در ایران است. این نگاه‌ها و جرم‌انگاری افراطی ناشی از آن‌ها با آن که به بهانهٔ بهبود امنیت فضای مجازی - چه از جنبهٔ سخت و فنی و چه از جنبهٔ نرم و فرهنگی - تبلیغ شده‌اند، و در سیاست‌گذاری مورد استفاده قرار گرفته‌اند، در عمل، ضررهای جبران‌ناپذیری به فضای مجازی ایران و امنیت و تاب‌آوری آن وارد کرده‌اند.

قوانین و ساختارهای اعمال قانون معمولاً از فناوری‌های نوین عقب‌تر هستند و آن‌ها را تهدیدی برای خود می‌بینند. تسامح اولیه در برابر قانون‌شکنان و سپس به‌روزرسانی قوانین قدیمی و پرهیز از جرم‌انگاری بیش از حد برای توسعهٔ فناوری‌های نوین ضروری است. تعدیل قوانین حق نشر در قبال توسعه‌دهندگان صنایع ضبط که در آن زمان سارقان محصولات صوتی و تصویری محسوب می‌شدند و سپس تنظیم قوانین جدید مالکیت فکری که صنعت ضبط و نشر را به بخشی از خود نظام مالکیت فکری تبدیل کرد، نمونه‌ای از این رخدادها به شمار می‌رود (گلداسمیت و وو: ۱۴۰۱: ۱۳۸). در مقابل، جرم‌انگاری محصولات فناورانهٔ جدید علاوه بر این که مانعی مهم در توسعهٔ فناوری به شمار می‌رود و در صورت اعمال در سطح ملی، کشور را از قطار پیشرفت جهانی بازمی‌دارد، بسیار ناکارا است و با تلف کردن زمان و انرژی نیروهای قضایی و اعمال قانون، آن‌ها را از رسیدگی به وظایف واقعی‌شان بازمی‌دارد. اتفاقی که در ایران در مقابل فناوری‌هایی مانند ویدیو، ماهواره و تماس تصویری شاهد آن بوده‌ایم.

یک مسألهٔ قابل توجه دیگر در سیاست‌گذاری، محدودیت بازدارندگی قوانین با افزایش مجازات‌هاست. اگر حکومت‌ها جرائم نسبتاً کوچک را با همان شدت جرائم جدی (مانند قتل یا سرقت از بانک) مجازات کنند، قانون توانایی خود را برای تعیین این که شهروندان چه کار باید بکنند و چه کار نباید بکنند از دست خواهد داد (همان: ۱۰۲). جرم‌انگاری بیش از حد ناشی از دیدگاه امنیتی نیز نتایج مشابهی به بار خواهد آورد.

به نظر می‌رسد فاصله گرفتن از گفتمان امنیتی در حوزه‌های مربوط به زندگی روزمره، کاهش جرم‌انگاری‌های بی‌اساس و باز گذاشتن فضا برای تنظیم‌گری فضای مجازی به دست خود مردم و مطابق عرف جامعه و به دور از دخالت و تصدی‌گری‌های حکومتی و حاکمیتی، توجه به نظرات تخصصی متخصصین بدون سوگیری فضای مجازی، الگوگیری از مسیرهای پیموده‌شده در کشورهای دیگر و درس گرفتن از آن، علاوه بر این، بهبود شرایط اقتصادی-فرهنگی برای جذب متخصصین فناوری اطلاعات، بهبود شرایط تعامل با شرکت‌های خارجی برای افزایش مشارکت آن‌ها در بازار ایران به جای دفع ضربتی آن‌ها و در نهایت، توجه عملی به سیاست‌های بالادستی از جمله تدبیر شمارهٔ ۱۵ سند الگوی اسلامی ایرانی پیشرفت، می‌تواند در بهبود وضعیت فضای مجازی ایران و امنیت و تاب‌آوری آن مؤثر باشد. اعطای آزادی‌های بیشتر به رسانه‌های داخلی، باز کردن فضا برای تولید محتوا به دست خود مردم و تلاش برای کاهش قطبیت در جامعه و شکاف دولت-ملت نیز می‌تواند بسیاری از آن‌چه را آسیب‌های فضای مجازی دانسته می‌شود و به عنوان بهانه‌هایی برای محدودسازی بیشتر آن به کار می‌رود بی‌اثر کند.

مراجع

Asogwa, C. E. (2020). Internet -based communications: A threat or strength to national security? **Sage Open** 10(2), 2158244020914580.

Björck, F., M. Henkel, J. Stirna, and J. Zdravkovic (2015). Cyber resilience – fundamentals for a definition. In A. Rocha, A. M. Correia, S. Costanzo, and L. P. Reis (Eds.), ***New Contributions in Information Systems and Technologies***, Cham, pp. 311–316. Springer International Publishing.

Dahan, M. (1999). National security and democracy on the internet in Israel. **Javnost - The Public** 6(4), 67–77.

Harrop, W. and A. Matteson (2014). Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. **Journal of Business Continuity & Emergency Planning** 7(2), 149–162.

Kovács, L. (2018). National cyber security as the cornerstone of national security. **Land Forces Academy Review** 23(2), 113–120.

Linkov, I. and A. Kott (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview, **Cyber Resilience of Systems and Networks**, pp. 1–25. Cham: Springer International Publishing.

ادیب سرشکی، میلاد (۱۳۹۱). قدرت نرم کرۀ جنوبی و گسترش موج کره‌ای. **سیاست خارجی** ۲۶(۳)، ۷۵۹–۷۷۶.

ایزدی، جهانبخش و جواد خادم‌زاده (۱۳۹۸). مؤلفه‌های نوین دیپلماسی‌عمومی مدرن و افزایش قدرت نرم جمهوری اسلامی ایران. **مطالعات روابط فرهنگی بین‌المللی** ۵(۱۱)، ۱۴۳–۱۷۶.

خجستۀ باقرزاده، حسن و کمیل خجستۀ باقرزاده (۱۴۰۰). تحول مولفه‌های قدرت در عصر شبکه. **مطالعات رسانه‌های نوین** ۷(۲۸)، ۱۶۹–۱۹۴.

خلیلی جولرستانی، احمد (۱۳۹۶). نگاهی دوباره به چالش‌ها و تهدیدات فضای مجازی بر امنیت پایدار. **بصیرت و تربیت اسلامی** ۱۴(۴۲)، ۱۰۳–۱۲۱.

خوش‌سلیقه، مسعود و الهام فاضلی حق‌پناه (۱۳۹۵). فرایند و ویژگی‌های زیرنویس غیرحرفه‌ای در ایران. **مطالعات زبان و ترجمه** ۴۹(۲)، ۶۷–۹۵.

دانش، پروانه، محمدرضا شواخی زواره، و فریبا عظیمی (۱۳۹۸). تأثیر شایعۀ فضای مجازی بر نظم و امنیت جامعه: دیدگاه‌پژوهی کارمندان شهرداری تهران. **علوم خبری** ۸(۲۹)، ۱۵۶–۱۷۵.

دلاوری، ابوالفضل، محمد رهبری، و هادی صفری (۱۴۰۲). فضای مجازی و قطب‌بندی سیاسی در ایران: مطالعه موردی واکنش‌های کاربران توییتر فارسی به تحولات ایران (سال‌های ۱۴۰۰-۱۴۰۱). **مطالعات فرهنگی و ارتباطات** ۱۹(۷۰).

ذکایی، محمدسعید و سیمین ویسی (۱۳۹۹). **زیست مجازی در ایران: عواطف و خرده‌فرهنگ‌ها در شبکه‌های اجتماعی**. تهران: آگاه.

رستمعلی‌زاده، سعید و حامد حاجی‌ملامیرزایی (۱۳۹۹). نظام حقوقی حاکم بر فیلترینگ اینترنت در ایالات متحده آمریکا. **مطالعات حقوق عمومی** ۵۰(۴)، ۱۶۶۳–۱۶۸۱.

رضاپور، دانیال و علی اسکندری‌نسب (۱۳۹۸). امنیت فضای سایبر در رویکرد فرهنگی مقام معظم رهبری. **مطالعات روابط فرهنگی بین‌المللی** ۵(۱۰)، ۱۹۹–۲۳۵.

رهبری، محمد و هادی صفری (۱۴۰۰). تأملی بر فیواستارهای توییتر فارسی در زمستان ۱۴۰۰.

http://mashghenow.com/?p=5664. دسترسی در ۳۰ بهمن ۱۴۰۱.

زاهدی مازندرانی، محمدجواد (۱۳۹۸). نقد سند الگوی پایه‌ی اسلامی-ایرانی پیشرفت از منظر الزامات **توسعه. برنامه‌ریزی و آمایش فضا** ۲۳(پیژه‌نامهٔ بهار).

زندی، محمدرضا و بهرام سیاه‌بالایی (۱۳۹۹). نقش فضای مجازی در تهدید علیه امنیت ملی. در مجموعه‌مقالات ***چهارمین کنفرانس بین‌المللی پژوهش‌های کاربردی در علوم انسانی و علوم اسلامی***.

صفری، هادی (۱۴۰۰). اینفودمی کرونا در رسانه‌های اجتماعی فارسی. **مطالعات کاربردی در علوم اجتماعی و جامعه‌شناسی** ۱۷(۴)، ۶۳–۷۶.

صفری، هادی (۱۴۰۱). تحلیل شبکه‌ای کارزارهای مرتبط با افغانستان در توییتر فارسی. **علوم رایانشی** ۲۶(۳)، ۶۹–۸۱.

عاملی، سعیدرضا (۱۳۹۶). **نظریه‌ها و مفاهیم اساسی دولت الکترونیک**. تهران: امیرکبیر.

عبدلی‌پیران، فاطمه (۱۳۹۹). رابطهٔ میزان استفاده از فضای مجازی با معنای زندگی و تاب آوری اجتماعی جوانان ۱۵ تا ۳۵ ساله. **روان‌شناسی و علوم تربیتی در هزارهٔ سوم** (۲)، ۷۳ – ۸۳.

فاضلی حق‌پناه، الهام و مسعود خوش‌سلیقه (۱۳۹۷). انگیزه‌ها و دلایل طرفدار زیرنویسی فیلم‌ها و سریال‌های کره‌ای. **مطالعات زبان و ترجمه** ۵۱(۳)، ۷۵–۱۰۱.

محمدی، مصطفی (۱۳۹۷). بررسی فعالیت داعش در فضای مجازی و تهدیدات آن بر امنیت ملی جمهوری اسلامی ایران. **پژوهش‌های سیاسی و بین‌المللی** ۹(۳۵)، ۵۵–۷۷.

مرکز اسلامی ایرانی پیشرفت (۱۳۹۷). **سند الگوی اسلامی ایرانی پیشرفت**، مرکز اسلامی ایرانی پیشرفت.

میربیک سبزواری، علی، فائزه تقی‌پور، و رضا اسماعیلی (۱۴۰۱). ادراک کاربران از امنیت فرهنگی در فضای مجازی: فضای مجازی امنیت‌آفرین یا امنیت‌ستان. **مطالعات رسانه‌ای** ۱۷(۳)، ۵۱–۶۶.

هان، بیونگ‌چول (۱۳۹۸). **روان سیاست: نئولیبرالیسم و فناوری‌های جدید قدرت**. ترجمه‌ی انصافی، مصطفی. تهران: لوگوس.

پالیزبان، محسن (۱۳۹۴). بررسی رابطهٔ اینترنت و امنیت ملی جمهوری اسلامی ایران. **سیاست** ۴۵(۳)، ۶۳۵–۶۵۴.

کاستلز، مانوئل (۱۳۹۳). **شبکه‌های خشم و امید: جنبش‌های اجتماعی در عصر اینترنت**. ترجمه‌ی قلی‌پور، مجتبی. تهران: مرکز.

کاستلز، مانوئل (۱۳۹۸). **قدرت ارتباطات** (ویرایش ۲). ترجمه‌ی بصیریان جهرمی، حسین. تهران: علمی و فرهنگی.

گلداسمیت، جک ل. و تیم وو (۱۴۰۱). **چه کسی اینترنت را کنترل می‌کند؟ توهم جهان بدون مرز**. ترجمه‌ی رضانژاد، سهیل. تهران: نشر مون.