

The Position of Security and Resilience in Cyberspace Policymaking Based on the Islamic-Iranian Model of Progress

Sepehr Ghazinoory

Professor of IT Management Tarbiat Modares University, Tehran, Iran (corresponding author).


Email: ghazinoory@modares.ac.ir

 0000-0000-0000-0000

Hadi Safari

PhD Student of Science and Technology Policy Tarbiat Modares University, Tehran, Iran.

Email: hadi.safari@modares.ac.ir

 0000-0002-4240-8077

Abstract

The special features of cyberspace, such as universality, providing the possibility of anonymity, and rapid changes, along with its great impact on individual and collective life, make its policymaking and regulation challenging. The security and resilience of cyberspace as one of the complex aspects of cyberspace policymaking and the intersection point of technical, security, cultural, and social points of view have also been considered in upstream documents, and Tadbir No. 15 of the document of the Islamic-Iranian model of progress is dedicated to the security and resilience of cyberspace and the need to use local knowledge and global partnerships in it. An issue that seems to have been left aside in many policies and practical decisions related to cyberspace in favor of a non-specialist security perspective. This article, based on qualitative research methodology and analytical-descriptive research methods, by examining some of the most important challenges of cyberspace and its security and resilience in Iran and comparing them with similar global samples, tries to provide suggestions for policy regarding cyberspace in Iran. Staying away from the security discourse in everyday life issues, reducing criminalization, improving the conditions and attracting foreign companies in the field of cyberspace instead of repelling them, improving the economic and cultural conditions for the non-immigration of specialists in this field, leaving space for popular regulation of cyberspace away from governmental interventions, and paying attention to upstream documents, including the Islamic-Iranian Model document, are the progress of some of the solutions and policy proposals presented in this article.

Keywords: cyberspace, cyber security, cyber resilience, national security, technology policy.



جایگاه امنیت و تاب‌آوری در سیاست‌گذاری فضای مجازی بر اساس الگوی اسلامی ایرانی پیشرفت

سپهر قاضی‌نوری

استاد مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران (نویسنده مسئول).

Email: ghazinoory@modares.ac.ir

0000-0000-0000-0000

هادی صفری

دانشجوی دکتری سیاست علم و فناوری دانشگاه تربیت مدرس، تهران، ایران.

Email: hadi.safari@modares.ac.ir

0000-0002-4240-8077

چکیده

ویژگی‌های خاص فضای مجازی همانند جهانی‌بودن، فراهم آوردن امکان گمنامی و تحولات سریع در کنار تأثیرگذاری فراوان آن در زندگی فردی و جمعی باعث می‌شود سیاست‌گذاری و تنظیم‌گری آن چالش‌برانگیز گردد. امنیت و تاب‌آوری فضای مجازی به‌عنوان یکی از جنبه‌های پیچیده سیاست‌گذاری فضای مجازی و نقطه تقاطع دیدگاه‌های فنی، امنیتی، فرهنگی و اجتماعی، در اسناد بالادستی نیز مورد توجه بوده است و 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 امنیتی غیرتخصصی کنار گذاشته شده است. این نوشتار مبتنی بر روش تحقیق کیفی و روش توصیفی-تحلیلی، با بررسی برخی از مهم‌ترین چالش‌های فضای مجازی و امنیت و تاب‌آوری آن در ایران و مقایسه با نمونه‌های مشابه جهانی، تلاش می‌کند تا پیشنهادهایی برای سیاست‌گذاری در خصوص فضای مجازی در ایران ارائه کند. فاصله‌گرفتن از گفتمان امنیتی در مسائل زندگی روزمره، کاهش جرم‌انگاری‌ها، بهبود شرایط و جذب شرکت‌های خارجی حوزه فضای مجازی به‌جای دفع آن‌ها، بهبود شرایط اقتصادی- فرهنگی برای عدم مهاجرت متخصصین 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 پیشنهادها سیاستی مطرح شده در این نوشتار هستند.

کلیدواژه‌ها: فضای مجازی، امنیت سایبری، تاب‌آوری سایبری، امنیت ملی، سیاست‌گذاری فضای مجازی.



مقدمه و بیان مسئله

سند الگوی اسلامی ایرانی پیشرفت به‌عنوان سندی بالادستی برای هدایت ایران در مسیر تبدیل به خاستگاه تمدن نوین اسلامی در مرکز اسلامی ایرانی پیشرفت تدوین شده است. با وجود برخی انتقاداتی که به این سند وارد است (زاهدی‌مازندرانی، ۱۳۹۸، ص. ۷۳)، سند مذکور یک نقشه راه سطح بالا برای دستگاه‌های اجرایی و نهادهای قانون‌گذار فراهم می‌کند تا پیمودن مسیر پیشرفت کشور 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 مرتبط هستند که بیانگر اهمیت فضای مجازی در نقشه راه پیشرفت کشور و آینده جهان است. تدبیر شماره ۱۵ «ارتقای دانش و توسعه بومی و تأمین امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی با مشارکت مردمی و همکاری‌های بین‌المللی در تراز کشورهای پیشرو جهان» را به‌عنوان اولین اصل مرتبط با فضای مجازی مورد تأکید قرار می‌دهد (مرکز الگوی اسلامی ایرانی پیشرفت، ۱۳۹۷، ص. ۱۸).

فضای مجازی ویژگی‌های خاصی دارد که آن را از فضای واقعی متمایز می‌کند. به‌طور خلاصه، هزینه پایین آغاز فعالیت، 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 ویژگی‌های فضای مجازی هستند (زندى و سیاه‌بالایی، ۱۳۹۹، ص. ۲۱۵). این ویژگی‌ها، در کنار تأثیرگذاری بالای فضای مجازی در زیست روزمره انسان معاصر (ذکایی و ویسی، ۱۳۹۹، ص. ۱۱) و رفتار اجتماعی او (کاستلز، ۱۳۹۳، ص. ۱۴) و حتی روابط بیناکشوری، دیپلماسی و قدرت نرم (ایزدی و خادم‌زاده، ۱۳۹۸، ص. ۱۵۹)، باعث می‌شود نگاهی ویژه به مسائل فضای مجازی ضرورت داشته باشد.

امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی مسئله پیچیده‌ای است که جنبه‌های فنی، امنیتی، جامعه‌شناختی، فرهنگی، روان‌شناختی و اقتصادی را در برمی‌گیرد. 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.

تأمین الزامات سیاست‌گذاری در حوزه فضای مجازی و امنیت و تاب‌آوری آن، ضمن توجه به توسعه بومی، مشارکت مردم و همکاری‌های بین‌المللی در اسناد بالادستی (مرکز اسلامی ایرانی پیشرفت، ۱۳۹۷، ص. ۱۸) و بیانات مقام معظم رهبری (رضایپور و اسکندری‌نسب، ۱۳۹۸، ص. ۱۹۱) بسیار مورد توجه بوده است. ایشان در سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) بر ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور، استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، حفظ فرهنگ و هویت اسلامی - ایرانی و ارزش‌های اخلاقی، حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی و پایش، پیشگیری، دفاع و ارتقای توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات تأکید کرده‌اند. با این حال، به نظر می‌رسد برخی سیاست‌گذاری‌های این حوزه، قوانین مصوب و تصمیمات اجرایی ناظر بر محدودسازی فضای مجازی بدون توجه به ظرافت‌های تصمیم‌گیری درباره مسائل فضای مجازی صورت گرفته و تصمیم‌گیرندگان توجهی به تبعات آسیب‌زای تصمیماتشان نداشته‌اند. سیاست‌گذاری یک‌طرفه مبتنی بر روش‌های سلبی و محدودسازی بیش‌ازحد فضای مجازی، برخلاف تصور اولیه، می‌تواند باعث آسیب‌دیدن شدید امنیت و تاب‌آوری فضای مجازی کشور گردد. اثر حاضر تلاش می‌کند تا به شیوه توصیفی - تحلیلی، با در نظر داشتن جنبه‌های مختلف امنیت و تاب‌آوری و مقایسه تجربیات داخلی و خارجی، 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.

پژوهش حاضر با استناد به سند الگوی اسلامی ایرانی پیشرفت به دنبال پاسخ به این پرسش است که امنیت و تاب‌آوری در سیاست‌گذاری فضای مجازی چه جایگاهی داشته و دیدگاه‌های مختلف سیاست‌گذاران فضای مجازی چه تأثیری بر امنیت و تاب‌آوری آن دارد؛ چراکه هرچند تأمین امنیت و تاب‌آوری فضای مجازی در اسناد بالادستی و بیانات مقام معظم رهبری بسیار مورد توجه بوده است، به نظر می‌رسد سیاست‌گذاران شیوه مناسبی برای قانون‌گذاری در این خصوص در پیش

نگرفته‌اند و سیاست‌های موجود به نتایج مناسبی منجر نمی‌شود. همچنین در نوشته حاضر از پارادایم کیفی و روش تحقیق توصیفی - تحلیلی استفاده شده است. این روش یک روش تحقیق کیفی است که در آن محقق از مرحله توصیف صرف واقعیات بیرونی فراتر می‌رود و به تشریح و تبیین دلایل و چرایی این واقعیات می‌پردازد. نویسندگان با بررسی نمونه‌های مختلف تصمیمات سیاستی کشورهای مختلف جهان، به خصوص آمریکا، اروپا و کشورهای خاورمیانه و تحلیل و تبیین دلایل و تبعات آن‌ها برای تبیین نظریات خود بهره برده‌اند و تلاش نموده‌اند تا تأثیرات دیدگاه‌های مختلف در سیاست‌گذاری فضای مجازی را بر وجوه سخت و نرم امنیت و تاب‌آوری فضای مجازی نشان دهند. در انتها، با بررسی برخی تجربیات پیشین سیاست‌گذاری در ایران و مقایسه آن‌ها با نظریات نویسندگان، درستی این نظریات تأیید شده‌اند.

۲. پیشینه تحقیق

پیشینه پژوهشی موجود را می‌توان به دو دسته کلی تقسیم کرد. بخشی از پژوهش‌ها به تأثیرات فرهنگی و امنیتی فضای مجازی با محوریت ایران اختصاص داشته‌اند. بخش دیگری از پژوهش‌ها نیز به بررسی تجربیات کشورهای دیگر در سیاست‌گذاری فضای مجازی پرداخته‌اند. اثر حاضر را می‌توان به نوعی تلفیق این دو نگاه دانست.

عمده پژوهش‌های غیرفنی فارسی در حوزه امنیت و تاب‌آوری فضای مجازی بر تبعات فرهنگی و امنیتی فضای مجازی متمرکز بوده‌اند. امنیت ملی و هویت ملی بخش جدایی‌ناپذیر این پژوهش‌هاست که نشانگر غلبه دیدگاه امنیتی بر پژوهش‌های سیاستی حوزه فضای مجازی است. رضاپور و اسکندری‌نسب (۱۳۹۸) با تأکید بر جنبه‌های فرهنگی به امنیت فضای سایبر از دیدگاه مقام معظم رهبری پرداخته‌اند. آن‌ها اعتمادسازی و تقویت سرمایه 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 دانسته‌اند. زندی و سیاه‌بالایی (۱۳۹۹) به نقش فضای مجازی در تهدید علیه امنیت ملی پرداخته‌اند. به عقیده آن‌ها، توجه به رفتارشناسی کاربران فضای مجازی، ایجاد بستر مناسب برای تولید محتوای اسلامی ایرانی به دست خود کاربران و بدون دخالت حکومتی، توجه به مسئله شکاف دولت - ملت و تقویت انسجام اجتماعی

از جمله مسائل قابل‌توجه در برخورد با فضای مجازی هستند (زندى و سیاه‌بالایی، ۱۳۹۹، ص. ۲۱۸). خلیلی جولرستانی (۱۳۹۶) به چالش‌ها و تهدیدات فضای مجازی برای امنیت ملی پایدار پرداخته است. یافته‌های بررسی وی درباره دانشجویان دو دانشگاه دولتی کشور نشان می‌دهد بیش از هشتاد درصد جمعیت مورد بررسی از سایت‌های فیلترشده بازدید می‌کنند. او معتقد است فرهنگ‌سازی درباره کاربری اینترنت و آفندها و مخاطرات سایبری نتیجه‌ای مطلوب‌تر از فیلترینگ خواهد داشت (خلیلی جولرستانی، ۱۳۹۶، ص. ۱۴۷). همچنین، از نظر او در مسیر همراه‌سازی هویتی باید هویت ملی و هویت دینی به شکل مکمل یکدیگر عمل کنند (خلیلی جولرستانی، ۱۳۹۶، ص. ۱۶۲) چراکه 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. پالیزبان (۱۳۹۴). 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. آن‌ها معتقدند 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، ص. 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 که داعش از فضای مجازی برای ایجاد تهدیداتی مانند جذب نیرو از میان اقلیت‌های مذهبی ایران، ایجاد رعب و وحشت و اختلاف‌افکنی کمک گرفته است. این دسته از پژوهش‌ها اغلب نگاهی کوتاه‌مدت به امنیت داشته‌اند و از میان آن‌ها، مقالاتی مانند زندی و سیاه‌بالایی (۱۳۹۹) که اثرات بلندمدت و ضمنی امنیتی و اجتماعی را مد نظر داشته‌اند، به نتایج متفاوتی رسیده‌اند و لزوم توجه به مسائلی مانند شکاف دولت - ملت و تقویت انسجام اجتماعی را دریافته‌اند.

جنبه‌های غیر امنیتی فضای مجازی ایران نیز مورد توجه تعدادی از پژوهشگران قرار گرفته است. از آن جمله، 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.

همان‌طور که پیش از این بیان شد، پژوهش‌هایی نیز درباره مسائل امنیت و تاب‌آوری فضای مجازی در کشورهای دیگر صورت گرفته است که نگاه امنیتی بر آن‌ها غلبه ندارد. رستمعلی‌زاده و حاجی‌ملا میرزایی (۱۳۹۹) به بررسی نظام حقوقی فیلترینگ در آمریکا پرداخته‌اند. مواردی همچون محتوای جنسی برای کودکان، حفاظت از مالکیت فکری و تنظیم‌گری قماربازی آنلاین از جمله مسائلی هستند که ممکن است به فیلترشدن یک پایگاه اینترنتی در آمریکا منجر شوند. با این حال، متمم اول قانون اساسی آمریکا در خصوص تضمین آزادی بیان، به‌عنوان قانون بالادستی حاکم بر قوانین فدرال و ایالتی، فیلترینگ فضای مجازی را در آمریکا بسیار محدود می‌کند. همچنین در این کشور، فیلترینگ بر عهده یک نظام قضایی مستقل است که باعث می‌شود اعمال سلیقه‌ها و جهت‌گیری‌های سیاسی و مقطعی دولت حاکم باعث محدودسازی پایگاه‌های اینترنتی نشود (رستمعلی‌زاده و حاجی‌ملا میرزایی، ۱۳۹۹، ص. ۱۶۷۸). «داهان»^۱ (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»^۲ (۲۰۱۸) به اهمیت برنامه‌های امنیت سایبری در تأمین امنیت ملی کشورها اشاره کرده است. «آسوغوا»^۳ (۲۰۲۰) به اهمیت فضای مجازی، در کنار انواع سنتی‌تر رسانه‌ها، در تأمین امنیت ملی اشاره کرده است. «هاروپ»^۴ و «متیسون»^۵ (۲۰۱۴) به اهمیت مقاوم‌سازی زیرساخت‌های سایبری در برابر گستره وسیعی از تهدیدات و حملات سایبری با تأکید بر عملکرد آمریکا و انگلیس پرداخته‌اند. «گلداسمیت» و «تیم 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

1. Dahan
 2. Kovács
 3. Asogwa
 4. Harrop
 5. Matteson

باعث می‌شود اجماع جهانی بر چگونگی مدیریت فضای سایبری به امری دشوار بدل شود. مقایسه تطبیقی شاخصی میان وضعیت ایران و کشورهای مورد بررسی صورت نگرفته است و در نتیجه، سیاست‌گذاران نمی‌توانند به‌طور مستقیم آموخته‌های این مقالات را در سیاست‌گذاری برای ایران به کار گیرند.

با توجه به پیشینه پژوهشی مذکور، اثر حاضر تلاش می‌کند با تلفیق دو نگاه بررسی تطبیقی تجربیات سایر کشورها و بررسی جنبه‌های امنیتی و فرهنگی فضای مجازی و پرهیز از نگاه محدود کوتاه‌مدت، با در نظر داشتن رهنمودهای الگوی اسلامی ایرانی پیشرفت، به تبیین جایگاه امنیت و تاب‌آوری در سیاست‌گذاری فضای مجازی بپردازد.

۳. چهارچوب نظری

۳-۱. فضای مجازی

تلاقی علوم ارتباطات، الکترونیک، کامپیوتر و فناوری‌های ارتباطی نوین، دنیای معاصر را به جهانی چهاربعدی تبدیل می‌کند که در گذشته نظیر آن وجود نداشته است. زمان، مکان، فاصله و سرعت، چهار بعد این جهان جدید را تشکیل می‌دهند و مرزها، قوانین، مقررات قضایی و محدودیت‌ها را تحت تأثیر قرار می‌دهند (ایزدی و خادم‌زاده، ۱۳۹۸، ص. ۱۵۸). به‌خصوص در اوایل دوران ظهور اینترنت، تصور بر این بود که این ابزار با متصل کردن همه انسان‌های روی زمین، جهان را به‌جایی بهتر تبدیل می‌کند، انسان را از جهانی که در آن زندگی می‌کند می‌رهاند، بر ساخت دولت - ملت را به کناری می‌زند و اقتدار دولت‌ها و نظام حکومت سرزمینی را به چالش می‌کشد (گلداسمیت و وو، ۱۴۰۱، ص. 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 (خجسته باقرزاده، ۱۴۰۰، ص. ۱۸۰)؛ چنان‌که برای مثال، تنظیم‌گری نرخ کرایه حمل‌ونقل که سابقاً در انحصار حاکمیت بود، امروزه عملاً در اختیار شرکت‌های حمل‌ونقل آنلاین است. فضای مجازی ساختار ارتباطات را تغییر داده و خود ارتباطی توده‌ای به وجود آورده که به‌نوبه خود، باعث خودمختاری بیشتر کنشگران اجتماعی می‌شود (کاستلز، ۱۳۹۳، ص. ۱۴). افزایش اتصالات و جهانی‌شدن از جمله روندهای راهبردی مؤثر فضای مجازی بر آینده دیپلماسی عمومی هستند (افشار و همکاران، ۱۳۹۹، ص. ۹۷).

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، ص. ۱۵۹). در جامعه شبکه‌ای چند نوع قدرت وجود دارد که بر شبکه و کنشگران آن تأثیرگذارند (کاستلز، ۱۳۹۸، ص. ۶۱). از این بین، قدرت شبکه‌سازی، به‌عنوان 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 (کاستلز، ۱۳۹۸، ص. ۶۶). زندگی فردی و روابط بینافردی افراد نیز از تأثیر فضای مجازی به دور نمانده است. از منظر فردی، ویژگی‌هایی مانند هزینه ورود پایین برای آغاز فعالیت، 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، تعامل و سرعت بالای تبادل اطلاعات برخی از مهم‌ترین فضای مجازی را از رسانه‌ها و فضاهای سنتی‌تر متمایز می‌کنند (زندگی سیاه‌بالایی، ۱۳۹۹، ص. ۲۱۵). فضای مجازی همچنین زیست عاطفی مردم را به‌عنوان بخشی مهم از روابط بینافردی افراد دگرگون کرده و نظم و منطق تازه‌ای بر زندگی انسان معاصر حاکم نموده است (ذکایی و ویسی، ۱۳۹۹، ص. ۱۱). «هان» (۱۳۹۸) سرمایه‌داری مبتنی بر فضای مجازی را به رژیم الهیاتی برای دنیای مدرن تشبیه کرده است: از نظر او، گوشی‌های هوشمند همانند تسبیح همیشه در دست هستند، لایک همانند آمین دیجیتال 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، ص. ۲۵).

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

۳-۲. امنیت و تاب‌آوری فضای مجازی

امنیت فناوری، هم‌چالشی برای دولت‌ها و هم‌مانعی بر سر استفاده شهروندان از امکانات و تسهیلات فضای مجازی است. امنیت یک سامانه اطلاعاتی به معنی حمایت از اطلاعات و سامانه‌ها در برابر افشای تصادفی یا عمدی در برابر

دسترسی‌های غیرمجاز یا تغییرات و تخریب غیرمجاز است. بر این اساس، در توسعه فضای مجازی باید هم در لایه امنیت شبکه و هم در لایه امنیت اسناد تمهیدات مناسب اندیشیده شود و خط‌مشی‌ها و استانداردهای لازم تعیین گردد (عاملی، ۱۳۹۶، ص. ۷۸). تاب‌آوری نیز ارتباط تنگاتنگی با امنیت دارد و به معنی توانایی تولید متداوم خروجی مورد انتظار یک سامانه مجازی حتی در شرایط وقوع حملات سایبری است (بیورک و دیگران، ۲۰۱۵، ص. ۳۱۱). با یک دیدگاه گسترده‌تر، امنیت پایدار دیجیتالی را نه فقط به‌عنوان توسعه فنی بلکه باید به‌مثابه حالتی روحی، طرز تفکر و یک حرکت عمومی جهانی توصیف نمود (خلیلی جولرستانی، ۱۳۹۶، ص. ۱۵۸).

مسائل مرتبط با امنیت و تاب‌آوری فضای مجازی در سیاست خارجی و روابط میان کشورها نیز بازتاب یافته است (داوند و سلطانی‌نژاد، ۱۳۹۷، ص. ۷۱).

امنیت و تاب‌آوری زیرساخت، فناوری و خدمات فضای مجازی مسئله پیچیده‌ای است که جنبه‌های فنی، امنیتی، جامعه‌شناختی، فرهنگی، روان‌شناختی و اقتصادی را در برمی‌گیرد. به همین دلیل، روش‌های سنتی ارزیابی ریسک برای حل مسئله 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^۱ و کات^۲، ۲۰۱۹، ص. ۲). جنبه‌های سخت امنیت و تاب‌آوری بیشتر بر زیرساخت فنی متمرکز است و مسائلی مانند تأمین و تعمیر سخت‌افزارهای رایانه‌ای نوین، توسعه نرم‌افزارهای رایانه‌ای مورد نیاز، ارتباط مطمئن با نرم‌افزارهای رایانه‌ای خارجی، شبکه 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، نحوه 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.

۴. 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 توسعه جنبه سخت فضای مجازی چالش‌هایی ایجاد کند (عاملی، ۱۳۹۶، ص. ۶۹). تأمین امنیت فیزیکی و مجازی مراکز تهیه و توزیع برق در شبکه، یکی از اولین لایه‌های تأمین تاب‌آوری در این سطح است. در وهله بعد، مراکز داده متعدد، مجهز و ارزان در نقاط مختلف، امنیت و به‌خصوص تاب‌آوری فضای مجازی را تضمین می‌کنند. قراردادن 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 خصمانه دولت‌های غربی و به‌خصوص آمریکا، توزیع جغرافیایی داده‌ها و خدمات فضای مجازی بسیار دشوار است.

از سمت دیگر، حضور مشتریان خارجی در مراکز داده^۱ داخلی می‌تواند هزینه 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 توسعه اقتصادی و انتقال فناوری، می‌تواند به نهادهای قضایی و قانون‌گذار کشور اجازه بدهد تأثیرگذاری بر رفتار شرکت‌های خارجی تأثیر بگذارند. حضور شرکت آمریکایی یا هوآ با دارایی‌های فراوان در کشور فرانسه بارها به‌نظام 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 پرهزینه مانند مسدودسازی کلی اینترنت یا اعمال قانون از طریق واسطه‌های شبکه مانند تأمین‌کنندگان محلی اینترنت^۳ (ISP) (ها) محدود می‌کند (گلداسمیت و وو، ۱۴۰۱، ص. ۱۱۴). تجربه‌های متعدد از مکاتبات نهادهای

1. datacenter

2. Yahoo!

3. Internet Service Provider (ISP)

اعمال قانون ایران با سکوه‌های خارجی فضای مجازی مانند اینستاگرام، فارغ از رعایت‌نشدن بدیهیات مکاتبات قانونی بین‌المللی از سمت طرف ایرانی و ناآشنایی با فضای بین‌المللی، نشانگر آن است که ایران نیز در این زمینه جایگاهی مانند فیجی دارد.

به‌عنوان نمونه‌ای دیگر، شرکت «ای‌بی»^۱ 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، به سراغ کشورهایی با اقتصادی کوچک‌تر اما با نظام قضایی مناسب‌تر رفته است (گلداسمیت و وو، ۱۴۰۱، ص. ۱۷۲).

نمونه‌ای متفاوت، اتحادیه اروپا و قوانین حفاظت از داده‌های کاربران آن است. دستورالعمل سال ۱۹۹۸ اتحادیه اروپا در این خصوص شرکت آمریکایی میکروسافت^۲ را در دوراهی انتخاب بین پیروی از خواسته‌های حقوقی اتحادیه اروپا یا خروج از بازار اروپا قرار داد. خروج از بازار اروپا برای میکروسافت به معنی از دست‌دادن یک‌سوم سهم بازارش بود و بنابراین، گزینه اول را برگزید. علاوه بر این، میکروسافت این قوانین را نه‌فقط برای کاربرانش در اتحادیه اروپا، بلکه برای همه کاربرانش در هر جای دنیا اجرایی کرد (گلداسمیت و وو، ۱۴۰۱، ص. ۲۰۷). بدیهی است در شرایط مشابه، شرکتی همانند میکروسافت 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 می‌رانند.

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^۳ خارج از ایران به سایت‌های دولتی برای مقابله با حملات امنیتی، محرومیت از خدمت توزیع‌شده^۴ (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

1. eBay

2. Microsoft

3. Internet Protocol address (IP address)

4. Distributed Denial-of-Service (DDoS)

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.

توسعه نرم‌افزارهای تشکیل‌دهنده فضای مجازی و دسترسی به نرم‌افزارهای خارجی، جنبه دیگری از وجه سخت تأمین امنیت و تاب‌آوری فضای مجازی است. از یک‌سو، توسعه زیرساخت‌های نرم‌افزار مانند سیستم‌عامل‌ها و ضدویروس‌ها و به‌روز نگه‌داشتن آن‌ها فعالیت‌هایی است که در همه دنیا در سطح جهانی صورت می‌گیرد و شیوه دیگری برای پیاده‌سازی آن‌ها، متفاوت از تجربه همه کشورهای دنیا، متصور نیست. تحریم‌های آمریکا از یک‌طرف و نگاه امنیتی داخلی و کیفیت و پایداری اندک ارتباطات اینترنتی بین‌المللی ایران از سوی دیگر، امنیت و تاب‌آوری فضای مجازی را در این جنبه با چالش‌هایی جدی روبه‌رو کرده است. در زمینه توسعه نرم‌افزارهای داخلی در ایران نیز ناپایداری و شرایط نامناسب اقتصادی شرکت‌های کوچک و بزرگ حوزه 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 ضروری است که به دلیل مشکلات زیرساختی و نگاه امنیتی تأمین نمی‌گردد.

شرایط دشوار اقتصادی و فرهنگی در ایران، هم‌زمان با سرمایه‌گذاری گسترده کشورهای جهان هم در غرب و هم در حوزه خلیج فارس برای جذب متخصصین این حوزه، بسیاری از متخصصین حوزه فناوری اطلاعات و کارگران باسابقه را به سمت مهاجرت سوق داده و کشور را در این حوزه با بحران نیروی انسانی روبه‌رو نموده است؛ به خصوص که اکثر این افراد از اعضای طبقه متوسط هستند که شرایط اقتصادی و ارزش‌های فرهنگی آن‌ها در سال‌های اخیر بیش از سایر اقشار در معرض تهدید قرار گرفته است. همچنین، کارکنان حوزه فناوری اطلاعات به‌عنوان یک فعالیت دانشی به شدت نیازمند آرامش ذهنی هستند و بیش از برخی از مشاغل دیگر تحت تأثیر متغیرهای اقتصادی و فرهنگی قرار می‌گیرند.

در جنبه نرم امنیت و تاب‌آوری فضای مجازی مسائل دیگری مطرح است. فضای مجازی به شکل بالقوه می‌تواند بستری مناسب برای جنگ مجازی و نیز سازماندهی آشوب‌های دنیای واقعی به کار رود. از سوی دیگر، انقلاب اطلاعاتی باعث دسترسی شهروندان به اطلاعات گسترده و قدرت‌یابی نهادهای غیردولتی در عرصه سیاست و اجتماع شده است. دخالت مستقیم دولتی و حکومتی در حوزه فضای مجازی کارایی

پایینی دارد و پیش از این نیز شکست خورده است (خلیلی جولرستانی، ۱۳۹۶، ص. ۱۶۸). به‌جای بازآزمودن آزموده، باید با ایجاد بسترهای مناسب، تولید محتوا را به خود کاربران سپرد (زندى و سیاه‌بالایی، ۱۳۹۹، ص. ۲۱۸) که می‌تواند به شکل فردی یا 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 حوزه فضای سایبری عدم بهره‌گیری از ظرفیت‌های سازمان‌های غیردولتی است. تأکید بر سلسله‌مراتب بوروکراسی دولتی، تفکر و گاه دولت‌محور، نگاه امنیتی به فعالیت‌های به همه 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، ص. ۱۶۶).

در میان انبوه اطلاعات درحال پراکنده‌شدن 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، ص. ۴۹۰). مقام معظم رهبری نیز در دیدار مسئولان قوه قضاییه در تیرماه ۱۴۰۱ به اهمیت این مسئله اشاره کرده‌اند: «یکی از حقوق عمومی مردم همین است که امنیت روانی داشته باشند. امنیت روانی یعنی چه؟ یعنی هرروز یک شایعه‌ای، یک دروغی، یک حرف هراس‌افکننده‌ای در ذهن‌ها پخش نشود. حالا تا دیروز فقط روزنامه‌ها بودند که این کارها را می‌کردند، حالا فضای مجازی هم اضافه شده. هرچند وقت یا چند روز یک‌بار، گاهی چند ساعت یک‌بار یک شایعه‌ای، یک دروغی، یک حرفی را یک آدم مشخصی یا نامشخصی در فضای مجازی منتشر می‌کند، مردم را نگران می‌کند، ذهن مردم را خراب می‌کند. یک دروغی را مطرح می‌کند، شایع می‌کند، خب، این امنیت روانی مردم از بین می‌رود. یکی از وظایف قوه قضائیه برخورد با این مسئله است». شایعات فضای مجازی یکی از چالش‌های مهم این فضا برای دولت‌هاست؛ چراکه 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 شبکه 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، ص. ۷۳). اگر نیاز به آگاهی سیاسی مورد نیاز از رسانه‌های رسمی تأمین نشود، این اطلاعات از منابع قابل دسترس دیگر به منطبق 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، ص. ۴۹۰). بنابراین با افزایش شکاف دولت - ملت و قطبی‌سازی، شایعات علیه دولت که امنیت ملی را دچار مخاطره می‌کنند بیشتر پخش می‌شود. قطبی‌شدن فضای مجازی با قطبی‌شدن جامعه رابطه‌ای دوسویه دارد (دلآوری و دیگران، ۱۴۰۲، ص. ۳۰) و با کاهش شکاف دولت - ملت در جامعه واقعی، می‌توان قطبیت فضای مجازی و در نتیجه انتشار شایعات در آن را نیز کنترل کرد. استفاده صحیح از فضای مجازی می‌تواند نظرات کاربران داخلی و خارجی را به نفع کشور تغییر دهد (صفری، ۱۴۰۱، ص. 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 درباره یک کشور مؤثر است (ایزدی و خادم‌زاده، ۱۳۹۸، ص. ۱۶۹) و هم باعث تقویت هویت ملی مردم کشور (خلیلی جولرستانی، ۱۳۹۶، ص. ۱۶۲) می‌شود و در نتیجه، امنیت فرهنگی (میربیک سبزواری و دیگران، ۱۴۰۱، ص. 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 مسئولان امر توجه کافی به برندسازی و تقویت هویت ملی در فضای مجازی نشان نداده‌اند (ایزدی و خادم‌زاده، ۱۳۹۸، ص. ۱۷۰). تبلیغ و اشاعه 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، ص. ۷۱). کره جنوبی نیز با استفاده از مجموعه‌های تلویزیونی (فاضلی حق‌پناه و خوش‌سلیقه، ۱۳۹۷، ص. 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، ص. ۷۶۶). در فضای مجازی ایران نیز طرفداران پاپ کرهای به‌عنوان 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).

مسائل مربوط به تنظیم‌گری و قانون‌گذاری بخش دیگری از چالش‌های مرتبط با وجه نرم امنیت فضای مجازی را تشکیل می‌دهند. 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 بیش‌ازحد برای توسعه 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 به‌شمار می‌رود (گلداسمیت و وو، ۱۴۰۱، ص. ۱۳۸). در مقابل، جرم‌انگاری محصولات فناورانه جدید علاوه بر این که مانعی مهم در توسعه فناوری به‌شمار می‌رود، بسیار ناکار است و با تلف‌کردن زمان و انرژی نیروهای قضایی و اعمال قانون، آن‌ها را از رسیدگی به وظایف واقعی‌شان باز می‌دارد. اتفاقی که در ایران در مقابل فناوری‌هایی مانند ویدیو، ماهواره و تماس تصویری شاهد آن بوده‌ایم. محدودیت بازدارندگی قوانین با افزایش مجازات وجه دیگری از چالش قانون‌گذاری و تنظیم‌گری است. 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 این‌که شهروندان چه کار باید بکنند و چه کار نباید بکنند از دست خواهد داد (گلداسمیت و وو، ۱۴۰۱، ص. ۱۰۲). جرم‌انگاری بیش‌ازحد استفاده از محصولات فناورانه جدید نیز نتایج مشابهی به بار خواهد آورد. به نظر می‌رسد تدوین «اسناد ملی» متعدد و قوانینی که در ظاهر برای حفظ حقوق کاربران و در عمل برای محدودسازی آن‌ها، با در نظر گرفتن نظریات یک جریان سیاسی خاص و بدون توجه به دغدغه‌های متخصصان و کارشناسان عملیاتی این حوزه نگاشته شده‌اند، نمی‌توان بر چالش‌های فضای مجازی غلبه نمود.

امروزه استفاده دولت‌ها از شبکه‌های اجتماعی برای پیگیری دیپلماسی عمومی و صیانت از امنیت ملی از الزامات اساسی و ناگزیر دولت‌هاست. باین‌حال، ارزیابی‌های بین‌المللی نشان می‌دهد ایران در این حوزه بین کشورهای جهان در رتبه ۱۱۲ قرار

داشته است و از کشورهای 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 به‌شمار می‌رود (ایزدی و خادم‌زاده، ۱۳۹۸، ص. ۱۶۴).

۵. نتیجه‌گیری و پیشنهاد

با مقایسه وضعیت سیاست‌گذاری فضای مجازی در ایران با نمونه‌های بررسی‌شده از تجربیات جهانی، به نظر می‌رسد غلبه نگاه امنیتی، سلبی و غیرتخصصی بر نگاه‌های ایجابی مبتنی بر فرهنگ‌سازی مردمی در حوزه فضای مجازی یکی از علل اصلی مشکلات فضای مجازی در ایران است. این نگاه‌ها و جرم‌انگاری افراطی ناشی از آن‌ها با آنکه به بهانه بهبود امنیت فضای مجازی - چه از جنبه سخت و فنی و چه از جنبه 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.

قدیمی‌بودن قوانین و ساختارهای تنظیم‌گری و اعمال قانون از فناوری‌های جدید از چالش‌های ذاتی قانون‌گذاری این فناوری‌ها برمی‌خیزد؛ اما در ایران اقدامات اندکی برای غلبه بر این مشکلات ذاتی صورت گرفته است. جرم‌انگاری افراطی فناوری‌های نو مانع مهمی در توسعه آن‌ها به‌شمار می‌رود و در صورت اعمال در سطح ملی کشور را از قطار پیشرفت جهانی بازمی‌دارد. همچنین، چنین قوانینی کارآیی اندکی دارند و با تلف کردن وقت و توان نیروهای قضایی و اعمال قانون، مانع انجام وظایف اصلی آن‌ها می‌گردد؛ اتفاقی که در ایران در مقابل فناوری‌هایی مانند ویدیو، ماهواره و تماس تصویری شاهد آن بوده‌ایم. همچنین، جرم‌انگاری افراطی فناوری‌های جدید که دیدگاه‌های امنیتی صرف کوتاه‌مدت ناشی می‌گردد باعث می‌شود قوانین بازدارندگی خود را از دست بدهند و نتوانند بر رفتار شهروندان تأثیری بگذارند.

به نظر می‌رسد فاصله گرفتن از گفتمان امنیتی در حوزه‌های مربوط به زندگی روزمره، کاهش جرم‌انگاری‌های بی‌اساس و بازگذاشتن 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 درست‌گرفتن از آن، علاوه بر این، بهبود شرایط اقتصادی- فرهنگی برای جذب متخصصی فناوری اطلاعات، بهبود شرایط تعامل با شرکت‌های خارجی برای افزایش مشارکت آن‌ها در بازار ایران به‌جای دفع ضربتی آن‌ها و درنهایت توجه عملی به سیاست‌های بالادستی از جمله تدبیر شماره 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، بازکردن 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 به‌عنوان بهانه‌هایی برای محدودسازی بیشتر آن به‌کار می‌رود بی‌اثر کند.

بر اساس نتایج این پژوهش، پیشنهاد می‌شود سیاست‌گذاران به موارد زیر توجه نمایند:

- ❖ رسانه‌ای و تنظیم‌گران حوزه روابط عمومی، با افزایش آزادی عملکرد رسانه‌ای سیاست‌گذاران فضای مجازی به‌جای رویکردهای سلبی مبتنی بر محدودسازی ارتباطات بر رویکردهای ایجابی و تولید محتوا تمرکز کنند؛
- ❖ سیاست‌گذاران و بالابردن آستانه تحمل خود تلاش کنند تا مرجعیت رسانه‌ای ارتباطات به داخل کشور بازگردد؛
- ❖ سیاست‌گذاران فضای مجازی و قانون‌گذاران در زمان قانون‌گذاری به مقتضیات زندگی در دنیای امروز بیشتر توجه کنند و از تصویب قوانین و محدودیت‌هایی که نیازمندی‌های اساسی شهروندان دنیای معاصر را مختل می‌کند بپرهیزند؛
- ❖ با استفاده از سازوکارهای ارزیابی سیاستی و نظرسنجی‌های مکرر، اثرگذاری و تأثیرات جنبی سیاست‌ها از جمله موارد پیشنهادی سنجیده شود؛
- ❖ سیاست‌گذاران و سیاست‌سازان باید با بهره‌گیری از تجربه تاریخی سیاست‌گذاری در ایران معاصر و آشنایی با تجربیات مشابه سایر کشورها، از تکرار اشتباهات پیشین بپرهیزند.

فهرست منابع

- ادیب سرشکی، میلاد (۱۳۹۱). قدرت نرم کره جنوبی و گسترش موج کره‌ای، سیاست خارجی، ۲۶ (۳).
- افشار، محمدمهدی؛ برزگر، کیهان؛ کیانی، داود (۱۳۹۹). شناسایی فراروندهای فضای سایبر مؤثر بر آینده دیپلماسی عمومی (با رویکرد تحلیل ساختاری، تأثیر متقابل). راهبرد ۲۹ (۱).
- ایزدی، جهانبخش؛ خادمزاده، جواد (۱۳۹۸). مؤلفه‌های نوین دیپلماسی عمومی مدرن و افزایش قدرت نرم جمهوری اسلامی ایران. مطالعات روابط فرهنگی بین‌المللی ۵ (۱۱).
- خجسته باقرزاده، حسن؛ خجسته باقرزاده، کمیل (۱۴۰۰). تحول مؤلفه‌های قدرت در عصر شبکه. مطالعات رسانه‌های نوین ۷ (۲۸).
- خلیلی جولرستانی، احمد (۱۳۹۶). نگاهی دوباره به چالش‌ها و تهدیدات فضای مجازی بر امنیت پایدار. بصیرت و تربیت اسلامی، ۱۴ (۴۲).
- خوش سلیقه، مسعود؛ فاضلی حق پناه، الهام (۱۳۹۵). فرایند و ویژگی‌های زیرنویس غیرحرفه‌ای در ایران. مطالعات زبان و ترجمه، ۴۹ (۲).
- دانش، پروانه؛ شواخی زواره، محمدرضا؛ عظیمی، فریبا (۱۳۹۸). تأثیر شایعه فضای مجازی بر نظم و امنیت جامعه: دیدگاه پژوهی کارمندان شهرداری تهران. علوم خبری ۸ (۲۹).
- داوند، محمد؛ سلطانی‌نژاد، احمد (۱۳۹۷). امنیتی‌سازی تنش سایبری جمهوری اسلامی ایران و عربستان سعودی: تهدیدها و الزامات راهبردی. راهبرد ۲۷ (۱).
- دلاوری، ابوالفضل؛ رهبری، محمد؛ صفری، هادی (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؛ ویسی، سیمین (۱۳۹۹). زیست مجازی در ایران: عواطف و خرده‌فرهنگ‌ها در شبکه‌های اجتماعی. تهران: آگاه.
- رستمعلی‌زاده، سعید؛ حاجی ملامیرزایی، حامد (۱۳۹۹). نظام حقوقی حاکم بر فیلترینگ اینترنت در ایالات متحده آمریکا. مطالعات حقوق عمومی ۵۰ (۴).
- رضاپور، دانیال؛ اسکندری‌نسب، علی (۱۳۹۸). امنیت فضای سایبر در رویکرد فرهنگی مقام معظم رهبری. مطالعات روابط فرهنگی بین‌المللی ۵ (۱۰).
- رهبری، محمد؛ صفری، هادی (۱۴۰۰). تأملی بر فیواستارهای توییت‌ر فارسی در زمستان ۱۴۰۰. ۳۰ بهمن ۱۴۰۱

- زاهدی مازندرانی، محمدجواد (۱۳۹۸). *نقد سند الگوی پایه اسلامی- ایرانی پیشرفت از منظر الزامات توسعه*. برنامه‌ریزی و آمایش فضا ۲۳ (ویژه‌نامه بهار).
- زندگی، محمدرضا؛ سیاه‌بالایی، بهرام (۱۳۹۹). *نقش فضای مجازی در تهدید علیه امنیت ملی*. مجموعه مقالات 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).
- صفری، هادی (۱۴۰۱). *تحلیل شبکه‌ای کارزارهای مرتبط به افغانستان در توئیتر فارسی*. علوم رایانشی، ۲۶ (۳).
- عاملی، سعیدرضا (۱۳۹۶). *نظریه‌ها و مفاهیم اساسی دولت الکترونیک*. تهران: امیرکبیر.
- عبدلی‌پیران، فاطمه (۱۳۹۹). *رابطه میزان استفاده از فضای مجازی با معنای زندگی و تاب‌آوری اجتماعی جوانان ۱۵ تا ۳۵ ساله*. روان‌شناسی و علوم تربیتی در هزاره سوم (۲).
- فاضلی حق‌پناه، الهام؛ خوش‌سلیقه، مسعود (۱۳۹۷). *انگیزه‌ها و دلایل طرفدار زیرنویسی فیلم‌ها و سریال‌های کره‌ای*. مطالعات زبان و ترجمه، ۵۱ (۳).
- محمدی، مصطفی (۱۳۹۷). *بررسی فعالیت داعش در فضای مجازی و تهدیدات آن بر امنیت ملی جمهوری اسلامی ایران*. پژوهش‌های سیاسی و بین‌المللی، ۹ (۳۵).
- مرکز اسلامی ایرانی پیشرفت (۱۳۹۷). *سند الگوی اسلامی ایرانی پیشرفت*. مرکز اسلامی ایرانی پیشرفت.
- میربیک سبزواری، علی؛ تقی‌پور، فائزه؛ اسماعیلی، رضا (۱۴۰۱). *ادراک کاربران از امنیت فرهنگی در فضای مجازی: فضای مجازی امنیت‌آفرین یا امنیت‌سستان*. مطالعات رسانه‌ای، ۱۷ (۳).
- هان، بیونگ‌چول (۱۳۹۸). *روان سیاست: نئولیبرالیسم و فناوری‌های جدید قدرت*. ترجمه انصافی، مصطفی. تهران: لوگوس.
- پالیزبان، محسن (۱۳۹۴). *بررسی رابطه اینترنت و امنیت ملی جمهوری اسلامی ایران*. سیاست ۴۵ (۳).
- کاستلز، مانوئل (۱۳۹۳). *شبکه‌های خشم و امید: جنبش‌های اجتماعی در عصر اینترنت*. ترجمه قلی‌پور، مجتبی. تهران: مرکز.
- کاستلز، مانوئل (۱۳۹۸). *قدرت ارتباطات (ویرایش ۲)*. ترجمه بصیریان جهرمی، حسین. تهران: علمی و فرهنگی.

— گلداسمیت، جک. ال؛ وو، تیم (۱۴۰۱). چه کسی اینترنت را کنترل می‌کند؟ توهم جهان بدون مرز. ترجمه رضانزاد، سهیل. تهران: نشر مون.

References

- AbdoliPiran, F. (2021). The relationship between the amount of use of cyberspace and the meaning of life and social resilience of 15-35-year-old youth. *Journal of Psychology and Education Science in the Third Millennium* (2). 73-83. [in Persian]
- Adib Sereshki, M. (2012). South Korea's soft power and the expansion of the Korean wave. *Journal of Foreign Policy* 26(3), 759-776. [in Persian]
- Afshar, M.M., K. Barzegar and D. Kiani (2020). Identify the Cyberspace Megatrend Affecting the Future of Public Diplomacy (with Structural Analysis Approach, Interaction). *The Scientific Journal of Strategy* 29(1). 97-129. [in Persian]
- Ameli, S.R. (2017). Theories and concepts of e-government. AmirKabir.
- 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.
- Castells, M. (2013). *Communication power*. Oxford University Press (UK).
- Castells, M. (2015). *Networks of outrage and hope: Social movements in the Internet age*. John Wiley & Sons.
- Center for the Islamic-Iranian Model of Progress (2018). *Iranian Islamic Model of Progress*. AmirKabir.
- Dahan, M. (1999). National security and democracy on the internet in Israel. *Javnost - The Public* 6(4), 67–77.
- Danesh, P., M.R. Shavakhi Zavareh and F. Azimi (2019). The influence of cyber space rumors on the order and security of society: the perspective of Tehran municipality employees. *News Science* 29(8). 156-175. [in Persian]
- Davand, M. and A. SoltaniNejad (2020). Securitization of the Islamic Republic of Iran and Saudi Arabia Cyber-Tensions; Threats and Strategic Requirements. *The Scientific Journal of Strategy* 27(1). 71-98. [in Persian]
- Delavari, A., M. Rahbari and H. Safari (2023). Twitter, echo chamber and intensifying political polarization Case study: reactions of Persian Twitter users to events in Iran (years 1400-1401). *Cultural Studies & Communication* 19(70). [in Persian]

- Fazeli Haghpanah, E. and M. Khoshsaligheh (2018). Fansubbers' Motivations and Reasons for Subtitling Korean Films and TV Series. *Language and Translation Studies* 51(3). 75-101. [in Persian]
- Goldsmith, J. and T. Wu (2006). Who controls the Internet? Illusions of a borderless world. *Strategic Direction*.
- Han, B.C. (2017). *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books.
- 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.
- Izadi, J. and J. Khademzadeh, J. (2020). Modern Components of Modern Diplomacy and Enhancement of Soft Power of the Islamic Republic of Iran. *Journal of Cultural Relation* 5(11). 143-176. [in Persian]
- Khalili Jolorestani, A (2017). A second look at the challenges and threats of cyber space on sustainable security. *Journal of Insight and Islamic Education* 14(42). 103-121. [in Persian]
- Khojasteh Bagherzadeh, H. and K. Khojasteh Bagherzadeh (2022). Evolution of Power Elements in the Network's Age. *New Media Studies* 7(28). 169-194. [in Persian]
- Khoshsaligheh, M. and E. Fazeli Haghpanah (2016). The Process and Features of Fansubtitling in Iran. *Language and Translation Studies* 49(2). 67-95. [in Persian]
- 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.
- Mirbeyk Sabzevari, A., F. Taghipour and R. Esmaili (2022). Users' Perception of Cultural Security in Cyberspace (Cyberspace Creates or Destroys Security). *Media Studies* 17(3). 51-66. [in Persian]
- Mohammadi, M. (2018). Investigating ISIL Activity in Cyberspace and its Threats to Iran's National Security. *Political and International Researches Quarterly* 35(9). 55-77. [in Persian]
- Palizban, M. (2015). The Relationship Between Internet and National Security in the Islamic Republic of Iran. *Politics Quarterly* 45(3). 635-654. [in Persian]
- Rahbari, M. and H. Safari (2022). A reflection on Persian Twitter favestars in the winter of 1400. Available Online at <http://mashghenow.com/?p=5664>. Last Access 2023-02-19. [in Persian]
- Rezapoor, D. and A. EskandaryNasab (2019). Cyberspace Security in the Cultural Approach of the Supreme Leader of the Islamic Revolution of Iran. *Journal of Cultural Relation* 5(10). 199-235. [in Persian]
- Rostamalizadeh, S. and H. Haji Molla Mirzaie (2021). Legal System of Internet Filtering in the United States. *Public Law Studies Quarterly* 50(4). 1663-1681. [in Persian]
- Safari, H. (2021). COVID-19-related Infodemics in Persian Social Media. *Applied Studies in Social Sciences and Sociology* 17(4). 63-76. [in Persian]

- Safari, H. (2022). Network Analysis of Afghanistan-related Campaigns in Persian Twitter. *Computing Science Journal* 26(3). 69-81. [in Persian]
- Zahedi Mazandarani, M.J. (2020). Criticism of the Islamic-Iranian basic model of progress document from the perspective of development requirements. *Spatial Planning* 23(Spring Special Edition). [in Persian]
- Zandi, M.R. and SiahBalaei B. (2021). The role of cyber space in the threat against national security. The 4th International Conference on Applied Research in Humanities and Islamic Sciences with the theme of Transformation in Humanities. [in Persian]
- Zokaei, M.S. and Veisi S. (2020). Cyber life in Iran: emotions and subcultures in social networks. *Agah*. [in Persian]