فصلنامهٔ محیط‌شناسی راهبردی ج.ا.ایران، سال هفتم، شمارهٔ ۳، پائیز ۱۴۰۲

راهبردها، الزامات و راهکارهای همکاری بین‌المللی ج.ا.ایران در فضای سایبر

محمدرضا حسینی،[۱] محمدحسن فرخی[۲]

تاریخ دریافت: ۱۴۰۲/۰۸/۱۶ پذیرش مقاله: ۱۴۰۲/۰۹/۲۸

چکیده

همکاری بین‌المللی در فضای سایبر ناظر به مشارکت در فرایندهای تعریف‌شده در سازمان‌های بین‌المللی و منطقه‌ای فعال در زمینه فضای سایبر و نیز حضور در اسناد و معاهدات دوجانبه، چندجانبه و بین‌المللی مرتبط با این فضا است. شرایط خاص ج.ا.ایران الزاماتی را برای موضوع همکاری بین‌المللی کشور در فضای سایبر به وجود آورده است که لازم است راهبردها و الزامات به‌طور دقیق تعیین گردند تا با مشارکت و حضور در مجامع به‌طور حداکثری منافع ملی محقق شود و از آسیب‌های احتمالی مشارکت در اسناد و پیمان‌نامه‌های بین‌المللی جلوگیری به عمل آید. پژوهش «توسعه‌ای - کاربردی» حاضر، شاخص‌ها و الزامات همکاری بین‌المللی ج.ا.ایران در فضای سایبر را مورد مداقه قرار داده است. بر همین اساس ابتدا مبانی نظری مورد واکاوی قرار گرفته و به روش نظریه‌پردازی داده‌بنیاد، عوامل اثرگذار احصاء گردید. سپس از طریق پرسش‌نامه‌ای بر اساس طیف لیکرت و پس از انجام روایی‌سنجی آن، آلفای کرونباخ ۰/۸۱۲ که نشان‌گر پایایی مطلوب آن است، احصاء شد. سپس با استفاده از مدل‌سازی معادلات ساختاری در نرم‌افزار اسمارت پی.ال.اس، داده‌های حاصل از پرسش‌نامه و با روش حداقل مربعات جزئی، تجزیه‌وتحلیل و برازش کلی مدل معادل ۰.۵۷۹ بوده و چون از ۰.۳۶ بیشتر است، برازش مدل را قوی ارزیابی می‌کنیم.

واژگان کلیدی: راهبرد، ج.ا.ایران، همکاری بین‌المللی، فضای سایبر، راهبردها.

۱. دانشیار حقوق بین‌الملل و عضو هیئت علمی دانشگاه عالی دفاع ملی. rezahsn88@gmail.com

۲. دکتری مدیریت راهبردی فضای سایبر گرایش امنیت سایبری دانشگاه عالی دفاع ملی (نویسنده مسئول). mhf1364@gmail.com

۱. مقدمه

همکاری‌های بین‌المللی در فضای سایبر در قالب تشکیل نهادهای منطقه‌ای و فرامنطقه‌ای یا بازتعریف کارکردهای سابق این نهادها به شکل فزاینده‌ای رو به گسترش است. تشکیل مرکز عالی دفاع سایبری ناتو پس از حملات انتساب داده‌شده به روسیه نمونه‌ای از این موارد است. از سویی مختصات بدیع فضای سایبر نظیر فراسرزمینی بودن آن سبب شده کشورها توان اِعمال قوانین حاکمیتی سرزمینی خود را نداشته باشند و نیازمند همکاری با سایر کشورها جهت تأمین امنیت ملی خود باشند. در ج.ا.ایران، مقام معظم رهبری(مدظله‌العالی) در بند سوم حکم انتصاب دور دوم اعضاء شورای عالی فضای مجازی، خواستار برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه گردیده‌اند که لازمه این مهم کنشگری فعال در زمینه همکاری بین‌المللی در فضای سایبری علی‌الخصوص با کشورهای مسلمان و هم‌پیمان است. تاکنون موضوع همکاری‌های بین‌المللی مورد توجه پژوهشگران و سیاست‌گذاران متعدد این عرصه قرار گرفته است؛ لیکن جنبه همکاری بین‌المللی فضای سایبر این مهم کمتر مدنظر بوده است و در حال حاضر، راهبرد و سیاست مشخص و مدونی برای این در کشور ایران موضوعیت ندارد. پژوهش حاضر با مورد نظر قراردادن جنبه بین‌المللی فضای سایبر مترصد ارائه راهبردها، الزامات و راهکارهای همکاری بین‌المللی کشور در فضای سایبر است. ابعاد و مؤلفه‌های مربوطه از پیشینه‌ها و مبانی نظری استخراج و با روش‌های تجزیه‌وتحلیل استاندارد مورد بررسی قرار گرفته و در نهایت فرضیه‌های مورد نظر پژوهش مورد ارزیابی قرار گرفته‌اند.

۲. مبانی نظری و پیشینه‌شناسی تحقیق

۱-۲. پیشینه‌شناسی تحقیق

اهم پیشینه‌های مقاله حاضر که مورد بررسی قرار گرفته‌اند و در مقوله همکاری‌های بین‌المللی در فضای سایبر به طرح مسائل پرداخته‌اند، به شرح زیر ارائه می‌گردد:

«تیلور»[1] و «هافمن»[2] در پژوهشی با عنوان «ارتباطات آمریکا - اروپا حول محور حکمرانی اینترنت»[3] (۲۰۱۹) نسبت به تحقیق از منابع اولیه و ثانویه متنوع (شامل مصاحبه با افراد مختلف که از مقامات فعلی یا سابق دولت‌های ایالات‌متحده، اتحادیه اروپا، اعضای ارشد کارکنان حوزه اینترنتِ سازمان نام‌ها و شماره‌ها[4] هستند) اقدام نموده‌اند. تحقیقات شامل جمع‌آوری اسناد و منابعی از سازمان‌های حکمرانی اینترنت، اسناد، گزارش‌ها و مقالات خروجی در مورد اینترنت، حکمرانی و روابط بین‌الملل هستند. نویسندگان از روش‌های تجزیه‌وتحلیل کیفی استفاده نموده‌اند و نقاط هم‌گرایی و واگرایی بین اتحادیه اروپا و ایالات‌متحده و تفاوت‌های موجود در حکمرانی اینترنت بین بازیگران را تعیین نموده‌اند. نتیجه تحقیق آن است که آینده چند سهام‌داری برای حکمرانی اینترنت تضمین نشده است. ۸۶ کشور اقتدارگرا ازجمله چین با حوصله از این سرمایه‌های فعلی (وضعیت موجود) بهره می‌برند و از فرایندهای چندجانبه موجود بهره می‌برند. ازبین‌رفتن توجه و منابع نهادهای اتحادیه اروپا منتج به تضعیف اینترنت آزاد و رایگان که جزء اصول کشورهای غربی است؛ خواهد شد. خطر واقعی برای کشورهای غربی آن است که با شکست متحدان غربی میدان به کشورهایی واگذار شود که کاملاً متفاوت عمل می‌نمایند و این به معنی ترویج یک اینترنت غیرآزاد (به تعبیر آنچه کشورهای غربی اعتقاد دارند)، یا حتی چندپاره است. با همکاری مؤثرتر، با تأکید بر اشتراکات بیش از اختلافات، اتحادیه اروپا و ایالات‌متحده می‌توانند خطرات تقسیم اینترنت را کاهش دهند که هدف آن حفظ یک اینترنت آزاد، آزاد و آزاد است.

«رامک» و «محمدی» در مقاله‌ای پژوهشی با عنوان «ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور (بر اساس نظریه‌پردازی داده‌بنیاد)» (۱۳۹۹) به روش توسعه‌ای-کاربردی به مسائلی همچون ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل (حوزه فضای سایبر)، وابستگی متقابل منافع ملی کشور با منافع ملی سایر

1. Emily Taylor
2. Stacie Hoffmann
3. EU–US Relations on Internet Governance
4. ICANN

کشورها، وقوع مداوم جنگ در جهان لزوم دفاع قاطع از کشور و مظلومان جهان و رفع دغدغه کشور در دستیابی به امنیت بین‌المللی در فضای سایبر، همکاری بین‌المللی با رویکرد تقویت دفاع سایبری اشاره می‌نمایند و در این راستا تاکید می‌نمایند باید محیط همکاری و منابع در دسترس برای دفاع سایبری کشور دقیقاً شناسایی گردد و بستر همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاقی در فضای سایبر و همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها در فضای سایبری فراهم شود و توجه ویژه داشت که آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد و سوابق همکاری و مشارکت در دفاع سایبری کشورها می‌تواند در تسریع و کندی اقدامات اثرگذار باشد و چهار راهبرد کلان (کنش و واکنش)، تدوین منشور و قوانین حاکم بر همکاری جهت دفاع سایبری، تدوین و به‌کارگیری دیپلماسی مشترک تعاملی کارآمد و قوی در حوزه دفاع سایبری کشور، تقویت رژیم‌ها و نهادهای بین‌المللی در حوزه دفاع سایبری و اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی در حوزه سایبری را برای شکل‌گیری همکاری فوق می‌توان اتخاذ نمود. طبق مدل، دقت لازم باید انجام شود که همکاری‌های بین‌المللی فوق در راستای تقویت سه محور کلان دفاع سایبری کشور، تأمین قابلیت بازدارندگی، تأمین قابلیت پدافند و تأمین قابلیت برگشت‌پذیری (تاب‌آوری) هدف‌گذاری گردد.

«رامک» در پژوهشی با عنوان «الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران و با رویکرد مبارزه با جرایم سایبری» (۱۳۹۸) در دانشگاه عالی دفاع ملی نشان داد؛ همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران با رویکرد مبارزه با جرایم سایبری باید در دو بخش مجزای مبارزه با جرایم سایبری و امنیت فضای مجازی تحت نظارت و کنترل یک بخش هماهنگی واحد (در حال حاضر مرکز ملی فضای مجازی کشور) انجام شود و اجرای آن نیز نیازمند تشکیل و سازمان‌دهی دفتر ملی مبارزه با جرایم سایبری، دفتر ملی امنیت فضای مجازی کشور و دفتر ملی همکاری‌های بین‌المللی سایبری

جمهوری اسلامی ایران بوده و انجام هدفمند اقدامات طبق الگوی راهبردی و پیشنهادهای ارائه‌شده، راهگشا خواهد بود.

۲-۲. مبانی نظری

۲-۲-۱. همکاری بین‌المللی

از دیدگاه اسلام، همکاری بین کشورهای مسلمان و غیرمسلمان باید بر مبنای نگاه تکریم‌آمیز به انسان‌ها، هم‌زیستی مسالمت‌آمیز، نفی اساسی خشونت، پایبندی به اصول اخلاقی و عهد، گفت‌وگو، مقابله‌به‌مثل و تجهیز قوا باهدف بازدارندگی شکل گیرد (رامک و محمدی، ۱۳۹۹ به نقل از علیخانی، ۱۳۹۰). خداوند متعال در قرآن کریم، رعایت اصل برقراری ارتباط با گفتار حسن (آیه ٦٤ سوره آل‌عمران)، اصل برقراری ارتباط با تأکید بر مشترکات (آیه ٦٤ سوره آل‌عمران)، اصل برقراری ارتباط با گفتار نرم و لین (آیه ٤٤ سوره طه)، اصل وفای به پیمان‌های سیاسی در روابط بین‌الملل (آیه ۱ سوره مائده)، اصل عدم اهانت به ارزش‌های ملل دیگر (آیه ۱۰۸ سوره انعام)، اصل ایجاد ارتباط بر اساس صلح (آیه ۲۰۸ سوره بقره)، اصل ایجاد روابط دیپلماسی همراه با حکمت و برهان (آیه ۱۲۵ سوره نحل) و اصل برقراری ارتباط بر اساس عزت اسلام (آیه ۱٤۱ سوره نساء) را لازم دانسته است. امام خمینی(ره) رعایت ویژگی اخلاق، حفظ صلح و امنیت بین‌المللی، عدم تجاوز به خاک کشورها، حسن هم‌جواری با همسایگان و همکاری با دولت‌ها برمبنای احترام متقابل و مقام معظم رهبری(مدظله‌العالی)، انطباق با جهان‌بینی توحیدی و آموزه‌های اسلامی و تعاملات انسانی در سطح فردی، جمعی و جهانی را برای همکاری بین‌المللی جزو اصول و اساس آن برشمرده‌اند.

روابط بین‌الملل، به مجموعه اقدامات و کنش‌های متقابل واحدهای حکومتی، نهادهای غیردولتی و روندهای سیاسی میان ملت‌ها اطلاق می‌شود. همکاری بین‌المللی، با روابط بین‌المللی دوجانبه یا چندجانبه با مشارکت بیش از دو دولت یا نهاد شکل می‌گیرد و ضرورت دارد که عوامل متعددی موردتوجه قرار گیرند تا با مشارکت مؤثر طرفین، یک همکاری اثربخش شکل‌گرفته و منافع ذی‌نفعان تأمین شود (رامک و محمدی، ۱۳۹۹).

۲-۲-۲. فضای سایبر

واژه سایبر از لغت یونانی «کیبرنتس»[1] به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام «نوربرت وینر»[2] در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹٤۸ میلادی به‌کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (و کامپیوترها) است (صدیق بنای، ۱۳۸۵).

واژه «فضای سایبر» را نخستین‌بار «ویلیام گیبسون»[3] نویسنده داستان علمی- تخیلی در کتاب «نورومنسر»[4] در سال ۱۹۸٤ بکار برده است (نگاهی متفاوت به سایبر، ۱۳۹۱). فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود (صدیق بنای، ۱۳۸۵).

۳-۲-۲. برخی مجامع بین‌المللی مرتبط با فضای سایبر همراه وظایفشان

اینترنت (فضای سایبر) یک سازه جهانی است و کنترل آن به‌تنهایی از سوی حکومت‌ها مشکل است. بنابراین پاسخ به مقوله‌های تعریف‌شده در فضای سایبر، همکاری و مشارکت بازیگرانی را در سطح بین‌المللی و منطقه‌ای می‌طلبد. اتحادیه اروپا، سازمان کشورهای آمریکایی، گروه ۸، سازمان همکاری‌های اقتصادی آسیای جنوب شرقی، سازمان همکاری شانگهای و اتحادیه آفریقا نمونه‌ای از این بازیگران هستند. بین این گروه‌ها، بیشترین اقدامات مربوط به کنوانسیون جرایم رایانه‌ای و اینترنتی شورای اروپا است (محمدی، ۱۳۹۹، به نقل از حافظنیا). در جدول (۱) برخی نهادها و سازمان‌های فعال و اثرگذار در موضوع فضای سایبر بین‌الملل به همراه وظایفشان ارائه شده است.

جدول شماره ۱. نهادهای کلیدی تأثیرگذار بر فضای سایبر بین‌الملل

1. Kybernetes
2. Norbert Wiener
3. William Gibson
4. Neuromancer

سازمان همکاری‌های آسیا – اقیانوسیه[1] (اَپک)

سازمان همکاری اقتصادی آسیا – اقیانوسیه در سال ۱۹۸۹ تأسیس شد و اکنون دارای ۲۱ عضو است که تمامی اعضاء آن مرز ساحلی با اقیانوس آرام دارند. این سازمان جرایم سایبری را به‌عنوان حوزه‌ای بااهمیت برای فعالیت تلقی می‌نماید. به طور نمونه، قوانین سایبری کشورهای مختلفی ازجمله استرالیا، کانادا، چین، ژاپن، مالزی، سنگاپور، تایلند و ایالات‌متحده آمریکا را به شکل جامع مورد بررسی قرار داده است. سران اَپک در سال ۲۰۰۲ بیانیه‌ای را در خصوص «مبارزه با تروریسم و ارتقای سطح رشد»[2] به‌منظور وضع مقررات جامع در رابطه با جرایم سایبری و توسعه ظرفیت‌های پیگیری جرایم سایبری منتشر نمودند. سازمان اقدام به تأسیس «کارگروه اطلاعات و ارتباطات سازمان همکاری اقتصادی آسیا – اقیانوسیه» نمود که کارگروه مذکور در سال ۲۰۰۲ «راهبرد امنیت سایبری سازمان اپک»[3] را تدوین نمود که متضمن توصیه‌هایی در مورد قانون‌گذاری در حوزه جرایم سایبری، خطوط راهنمای فنی و امنیتی، آگاهی عمومی و آموزش‌وپرورش است (زنگی‌آبادی، ۱۳۹۶).

انجمن ملل آسیای جنوب شرقی[4] (آسه‌آن)

مجمع دولت‌های آسیای جنوبی یا آسه‌آن در سال ۱۹۶۷ از اجتماع ۱۰ کشور تشکیل گردید. هدف این سازمان، ایجاد همکاری در زمینه‌های سیاسی، اجتماعی، اقتصادی و ... است. در سال ۱۹۹۴ آسه‌آن مجمع منطقه‌ای خود[5] را باهدف تقویت گفتگوهای سازنده و مشاوره در موضوعات سیاسی و مسائل امنیتی مشترک تأسیس نمود. البته علاوه بر کشورهای منطقه، ایالات‌متحده آمریکا، روسیه، چین و اتحادیه اروپا نیز در این مجمع مشارکت می‌نمایند.

فعالیت آسه‌آن در حوزه سایبری از دهه ۹۰ میلادی و در زمینه جرایم فراملی به‌عنوان نمونه‌ای از مسائل امنیتی غیرسنتی آغاز گردید. آسه‌آن در برنامه اجرایی که در نوامبر سال ۲۰۰۴ در اجلاس سران خود تدوین نمود، به موضوع امنیت و تمامیت زیرساخت‌های اطلاعاتی سازمان توجه نمود. ازجمله موارد مطرح‌شده در این برنامه ایجاد گروه‌های عکس‌العمل سریع رایانه‌ای (CERT) است. در سال ۲۰۰۶ کشورهای شرکت‌کننده در مجمع منطقه‌ای آسه‌آن، بیانیه خود را در مورد «همکاری در مبارزه علیه حملات سایبری و سوءاستفاده تروریستی از فضای سایبری»[6] صادر نمودند. همچنین اهمیت وجود زیرساخت‌های اطلاعاتی ایمن در منطقه بار دیگر در سال ۲۰۰۸ و در «برنامه کاری جامعه اقتصادی آسه‌آن»[7] مورد تأکید قرار گرفت. در سال ۲۰۱۲ آسه‌آن در نوزدهمین مجمع منطقه‌ای خود، بیانیه‌ای را از سوی وزرای امور خارجه کشورهای عضو در مورد همکاری در حوزه تضمین امنیت سایبری صادر نمود. در جولای ۲۰۱۳ و در طول بیستمین

1. Asia-Pacific Economic Cooperation (APEC)
2. Statement on Fighting Terrorism and Promoting Growth
3. APEC Cybersecurity Strategy
4. The Association of Southeast Asian Nations (ASEAN)
5. ASEAN Regional Forum (ARF)
6. Statement by the Ministers of Foreign Affairs on Cooperation in ensuring Cyber Security
7. ASEAN Economic Community Blueprint

مجمع سازمان نیز موضوع امنیت سایبری در ارتباط با جرایم فراملی و مبارزه با تروریسم و تأکید بر تقویت همکاری‌ها در این حوزه مدنظر قرار گرفت (تقی‌زاد، ۱۳۹۵).

شورای اروپا[1]

شورای اروپا –که در سال ۱۹٤۹ تأسیس شد و مقر آن در استراسبورگ است– نقش بسیار فعالی در زمینه پرداختن به مسائل و چالش‌های جرایم سایبری ایفا می‌نماید. این شورا سازمانی بین‌المللی با ٤۷ کشور عضو در ناحیه اروپا است. در سال ۱۹۷٦ شورای اروپا ماهیت بین‌المللی جرایم رایانه‌ای را مورد بحث قرار داد. در سال ۱۹۸۵ شورای اروپا کمیته‌ای تخصصی را برای بحث در مورد جنبه‌های قانونی و حقوقی جرایم رایانه‌ای تعیین نمود. در سال ۱۹۸۹ «کمیته اروپایی بررسی مشکلات جرایم»[2] گزارشی در مورد جرایم رایانه‌ای منتشر نمود. در سال ۱۹۸۹ «کمیته وزیران شورا»[3] توصیه‌نامه‌ای را که مشخصاً به ماهیت بین‌المللی جرایم رایانه‌ای می‌پرداخت صادر نمود همچنین شورای اروپا در سال ۲۰۰۱ معاهده جرایم سایبری را به تصویب رسانده است (هنریکسن، ۲۰۱۹).

اتحادیه اروپا[4]

اتحادیه اروپا یک اتحادیهٔ اقتصادی – سیاسی است که از ۲۷ کشور اروپایی تشکیل شده است. در سال ۱۹۹٦ اتحادیه اروپا از طریق صدور توصیه‌نامه‌ای راجع به محتوای غیرقانونی و مضر در اینترنت به بررسی خطرات ناشی از اینترنت پرداخت. در سال ۱۹۹۹ پارلمان اروپا و شورای اتحادیه اروپا یک برنامه اجرایی چندمحوری با موضوع «ارتقای سطح استفاده ایمن‌تر از اینترنت و مبارزه با محتوای غیرقانونی و مضر در شبکه‌های جهانی» تدوین نمودند. در همین سال اتحادیه اروپا ابتکار «اروپای الکترونیکی»[5] را با صدور توصیه‌نامه کمیسیون اتحادیه اروپا تحت عنوان «اروپای الکترونیکی – جامعه‌ای اطلاعاتی برای همه» به مرحله اجرا درآورد. در سال ۲۰۰۰، شورای اتحادیه اروپا، برنامه اجرایی جامع دیگری را تحت عنوان «برنامه اجرایی اروپای الکترونیکی» تدوین نمود. در سال ۲۰۰۱، کمیسیون اروپا توصیه‌نامه‌ای با عنوان «ایجاد جامعه اطلاعاتی ایمن‌تر از طریق بهبود امنیت زیرساخت‌های اطلاعاتی و مبارزه با جرایم مرتبط با رایانه» را صادر نمود. بعلاوه کمیسیون توصیه‌نامه‌ای با عنوان «امنیت اطلاعات و شبکه»[6] در سال ۲۰۰۱ منتشر نمود. در سال ۲۰۰۷ کمیسیون توصیه‌نامه‌ای در خصوص سیاست کلی راجع به مبارزه با جرایم سایبری منتشر کرد. این ابلاغیه ضمن بیان خلاصه وضعیت کنونی، بر اهمیت کنوانسیون جرایم سایبری شورای اروپا به‌عنوان ابزار برجسته بین‌المللی در مبارزه علیه جرایم سایبری تأکید دارد.

1. Council of Europe
2. European Committee on Crime Problems
3. Committee of Ministers
4. European Union (EU)
5. Europe
6. Network and Information Security – A European Policy approach

مؤسسه مهندسان برق و الکترونیک[1]

مؤسسه مهندسان برق و الکترونیک، یک انجمن تخصصی است که بر روی علوم کامپیوتر و الکترونیک، مهندسی و رشته‌های مرتبط تمرکز دارد. فعالیت‌های مربوط به امنیت سایبری این مؤسسه شامل توسعه استانداردهای فنی از سوی انجمن استاندارد مؤسسه بوده که تصویب استانداردها بر مبنای روندی توافقی است. برای مثال استانداردهای این مؤسسه شامل استانداردهای ۸۰۲.۱۱ می‌شود که یک استاندارد شناخته شده بین‌المللی برای رمزگذاری و شبکه‌های بی‌سیم است. به‌علاوه، بر اساس گزارش‌های این مؤسسه، انجمن استاندارد این نهاد در نوشتن پیش‌نویس استانداردهای امنیت سایبری برای سیستم‌های کنترل برق با «مؤسسه ملی استاندارد و فناوری آمریکا»[2] همکاری کرده است (زنگی‌آبادی، ۱۳۹۶).

شرکت اینترنتی نام‌ها و شماره‌های واگذارشده[3] **(آیکان)**

شرکت اینترنتی برای اعداد و نام‌های اختصاص‌یافته (آیکان) یک سازمان بین‌المللی غیرانتفاعی است که مسئول پروتکل اینترنتی، تخصیص فضای آدرس، تعیین پروتکل، مدیریت سیستم دامنه‌های کشوری و عمومی و مدیریت سیستم سرور ریشه است. آیکان در قالب یک شرکت غیرانتفاعی در ایالت کالیفرنیا برای توسعه سیاست‌های حکمرانی «سیستم نام دامنه اینترنت»[4] شکل گرفت. همچنین سایر مشخصه‌های آن مشارکت با بازیگران غیردولتی است. هدف آیکان حفظ ثبات در عملکرد اینترنت، افزایش رقابت، نمایندگی جوامع اینترنت بین‌المللی و توسعهٔ سیاست‌های متناسب با مأموریت آن در سطح پایین‌به‌بالا و بر اساس اجماع است. در سند تأسیس این سازمان ۳۵ هدف برای آیکان طراحی شده که بعضی از آن‌ها به شکل تخصصی و فنی و برخی به شکل‌های رفتاری برای سازماندهی آیکان قابل‌شناسایی هستند. آیکان در سال ۱۹۹۸ طی تفاهم‌نامه‌ای با وزارت بازرگانی آمریکا و آیکان با اهداف گوناگونی تأسیس شد.

ازجمله این اهداف می‌توان موارد زیر را ذکر کرد: (۱) حفظ ثبات در عملکرد اینترنت؛ (۲) ایجاد رقابت در ثبت دامنه‌های عمومی از طریق ازدیاد تعداد دامنه‌ها و ازدیاد تعداد مراکز ثبت؛ (۳) بین‌المللی نمودن مدیریت امور مربوط به اسامی و شماره‌های اینترنتی؛ (٤) ایجاد مکانیسم ارتباط با کلیه جوامع اینترنت بین‌المللی.

در خصوص تصویب موضوعات مطروحه در هیئت‌مدیره آیکان، درصورتی‌که جمیع دولت‌ها روی یک موضوعی اجماع نظر داشته باشند و برد (هیئت‌مدیره) آیکان نصف بعلاوه یک می‌توانند آن را وتو کنند. هیئت‌مدیره آیکان عبارت‌اند از شهروندانی از کشورهای استرالیا، برزیل، بلغارستان، کانادا، چین، فرانسه، آلمان، غنا، ژاپن، کنیا، کره، مکزیک، هلند، پرتغال، سنگال، اسپانیا، انگلستان و ایالات‌متحده. سایر موارد موردتوجه کاربران اینترنت از قبیل دادوستدهای مالی، کنترل محتوای اینترنت، هرزنامه‌ها و محافظت از داده‌ها، خارج از محدودهٔ مأموریت فنی و وظایف آیکان است. در حال حاضر نماینده جمهوری اسلامی ایران از وزارت ارتباطات و فناوری اطلاعات است. اساسنامه آیکان از سال ۱۹۹۸ تاکنون در حدود ٤۱

1. Institude of Electrical and Electronic Engineers (IEEE)
2. National Institude of Standards and Technology (NIST)
3. International Corporation for Assigned Names and Numbers (ICANN)
4. Internet’s Domain Name System (DNS)

مرتبه ویرایش و اصلاح شده است (آیکان، ۲۰۲۳).

گروه ویژه مهندسی اینترنت[1] (آی‌ای‌تی‌اف)

کارگروه مهندسی اینترنت سازمانی است که استانداردهای اینترنت را ایجاد کرده و بهبود می‌بخشد. این گروه با «کنسرسیوم وب جهان‌شمول»[2] و «سازمان بین‌المللی استانداردسازی»[3] همکاری نزدیکی داشته و به‌طور ویژه بر روی مجموعه پروتکل اینترنت کار می‌کند. این گروه یک مؤسسه استاندارد باز بوده که هیچ عضویت رسمی یا شرایط عضویتی ندارد. همه شرکت‌کنندگان و مدیران داوطلب هستند، هرچند معمولاً کار آن‌ها به‌وسیله کارفرمایان یا حامیانشان از نظر مالی پشتیبانی می‌شود. نخستین اقدام برای سازمان‌دهی و مدیریت فضای سایبری را می‌توان تأسیس این کارگروه دانست که در سال ۱۹۸٦ به‌منظور مدیریت توسعه استانداردهای فنی اینترنت به وجود آمد. هرچند تا پیش‌ازاین تاریخ، «اتحادیه بین‌المللی تلگراف» در سال ۱۸٦۵ و «سازمان نام‌های اختصاص‌یافته اینترنت»[4] در دهه ۱۹٦۰ و ۱۹۷۰ به وجود آمدند، اما کارگروه مهندسی اینترنت را می‌توان نخستین گسترش‌دهنده استانداردهای فنی اینترنت دانست که در سال ۱۹۹۲، بخشی از «جامعه اینترنتی»[5] شد و از این سال به بعد، جامعه اینترنتی بود که استانداردهای فنی اینترنت را تنظیم کرده و استفاده از آن را تشویق می‌کرد (عاملی، ۱۳۹۷، به نقل از مارچانت و رابرتسون، ۲۰۱۵، به نقل از شبکه سیاست‌های مجازی، ۲۰۰۹).

پلیس بین‌الملل[6] (اینترپل)

«اینترپل» که بزرگترین سازمان پلیسی بین‌المللی است، با هدف تسهیل همکاری‌های پلیسی فرامرزی ایجاد شد. این سازمان، اطلاعات مربوط به جرایم سایبری را از میان ۱۸۸ کشور عضو و از طریق سیستم ارتباطی جهانی پلیس جمع‌آوری، ذخیره و تحلیل می‌کند و در میان آن‌ها به اشتراک می‌گذارد. به‌علاوه این سازمان مسئولیت هماهنگی منابع عملیاتی مثل تحلیل‌های «فارنزیک رایانه‌ای»[7] را برای پشتیبانی و حمایت از بررسی‌های جرایم رایانه‌ای بر عهده دارد. همچنین اینترپل شبکه‌ای از محققان در واحدهای ملی جرایم رایانه‌ای دارد تا به مجریان قانون کمک کنند در اسرع وقت اسناد دیجیتال مورد نیاز را به دست آورند و در صورت وقوع حمله‌ای سایبری که به چند حوزه قضایی مربوط می‌شود، همکاری میان آن‌ها را تسهیل کنند.

1. Internet Engineering Task Force (IETF)
2. World Wide Web Consortium (W3C)
3. International Organization for Standardization (ISO/IEC)
4. Internet Assigned Names Authority (IANA)
5. Internet Society
6. INTERPOL
7. Computer Forensic

فارنزیک رایانه‌ای، شاخه مهمی از دانش رایانه در رابطه با جرایم صورت‌گرفته در حوزه رایانه و اینترنت است که هدف آن انجام تحقیقات با استفاده از اسناد و مدارک دیجیتالی جهت مشخص‌کردن مجرمین و مسببان اعمال مجرمانه است.

در جهت ایجاد و توسعه راهبردهایی برای روش‌های نوظهور جرایم رایانه‌ای، این سازمان گروه‌هایی از کارشناسان را به‌صورت کارگروه‌های منطقه‌ای تشکیل داده است تا تخصص موجود در اروپا، آسیا، آمریکا، غرب آسیا و شمال آفریقا را کنترل کند و بهترین بهره‌برداری را از این کارشناسان داشته باشد. فعالیت‌های این کارگروه‌ها شامل تبادل اطلاعات درباره جرایم سایبری منطقه‌ای، ارتقاء همکاری میان کشورهای عضو و تهیه و توسعه مواد آموزشی برای مجریان قانون است (زنگی‌آبادی، ۱۳۹۶).

سازمان ملل متحد – گروه متخصصین دولتی

سازمان ملل متحد[1] سازمانی بین‌المللی است که در سال ۱۹۴۵ میلادی تأسیس و جایگزین جامعه ملل[2] شد. این سازمان توسط ۵۱ کشور تأسیس و در سال ۲۰۱۱ میلادی، ۱۹۳ کشور عضو داشته است. اعضای آن تقریباً شامل همه کشورهای مستقلی می‌شود که از نظر بین‌المللی به رسمیت شناخته شده‌اند.

روسیه در سال ۱۹۹۸ پیش‌نویس قطعنامه‌ای را به کمیته اول مجمع عمومی سازمان ملل با موضوع «توسعه اطلاعات و ارتباطات راه دور در بستر امنیت بین‌المللی» مسائل مربوط به فضای سایبر، بدواً ازنقطه‌نظر امنیت بین‌المللی، ارائه می‌نماید که مورد پذیرش واقع می‌گردد. این قطعنامه مبین تأثیر سوءاستفاده از فناوری‌های ارتباطی و اطلاعاتی بر امنیت کشورها است. در سال‌های بعد نیز روسیه پیش‌نویس‌های دیگری به سازمان ملل ارائه نموده است که نهایتاً مجمع عمومی در سال ۲۰۰۲ از دبیرکل تقاضای تشکیل «گروه متخصصین (کارشناسان) دولتی»[3] را جهت تهیه گزارشی برای «تقویت امنیت سیستم‌های اطلاعاتی و ارتباطی جهانی» نموده است. از آن زمان به بعد کمیته به‌منظور «بررسی تهدیدهای موجود و بالقوه در حوزه امنیت اطلاعات و اقدامات مشترک ممکن برای حذف این تهدیدات، و برای بررسی مفاهیم مرتبط بین‌المللی با هدف تقویت امنیت نظام‌های اطلاعات و ارتباطات راه دور جهانی» فعالیت منظم داشته است.

اولین گروه متخصصین دولتی با عنوان «متخصصین دولتی ملل متحد در زمینه اطلاعات و ارتباطات در حوزه امنیت بین‌المللی»[4] و با ۱۵ عضو در ژوئن ۲۰۰۴ تشکیل شد. دومین گروه متخصصین دولتی در اواخر سال ۲۰۰۵ توسط دبیرکل جهت ادامه مطالعه پیرامون تهدیدهای فناوری اطلاعات و ارتباطات ایجاد گردید. با این وجود از سال ۲۰۰۶ که روسیه قطعنامه «توسعه اطلاعات و ارتباطات» را برای حمایت سایر کشورها باز گذاشته، کشورهای بسیاری از جمله کشورهای عضو سازمان همکاری شانگهای و ایالات متحده به حامیان قطعنامه پیوسته‌اند. که به نظر می‌رسد با ورود ایالات‌متحده آمریکا به حامیان قطعنامه، دولت این کشور سعی در تسلط بر این قطعنامه داشته و دارد؛ از سویی حملات سایبری گسترده از سال ۲۰۰۰ یکی از دلایل این تغییر موضع بوده است. برخلاف گروه اول، گروه دوم در سال ۲۰۱۰ موفق به دستیابی به یک توافق ابتدایی گردید؛ که منتج به گزارشی گردید که در این گزارش به ضرورت بازنگری دستورالعمل‌های

1. United Nations
2. League of Nations
3. Group of Governmental Experts
4. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

موجود در زمینه حفاظت از زیربناهای اساسی، اعتمادسازی، ظرفیت‌سازی و نیز در خصوص تعاریف و واژگان تأکید شده بود.

گروه سوم در دسامبر ۲۰۱۱ توسط مجمع عمومی تشکیل شد؛ و از آن خواسته شد تا پیرامون «هنجارها و قواعد یا اصول رفتار مسئولیت‌پذیری کشورها» گفتگو نمایند. در این دوره از تشکیل گروه، پیشرفت قابل توجهی حاصل شد؛ که گزارش اجماعی متعاقب نشست تأیید کرد که «حقوق بین‌الملل و به‌ویژه منشور سازمان ملل متحد قابل اعمال است» و «تلاش‌های دولتی برای پرداختن به امنیت فناوری‌های اطلاعات و ارتباطات باید به همراه رعایت حقوق بشر و آزادی‌های بنیادینی باشد که در اعلامیه جهانی حقوق بشر و سایر اسناد بیان شده است». گروه سوم متخصصین دولتی، در ژوئن ۲۰۱۳ اقدام به ارائه گزارش اجماعی با تأکید بر درک مشترک از «هنجارها، قواعد و اصول قابل کاربست در استفاده از فناوری‌های اطلاعاتی و ارتباطی» که کمک‌کننده به پیشرفت صلح و امنیت باشد، نمود. در همین سال مجمع عمومی قطعنامه‌ای را با عنوان «حق برخورداری از حریم خصوصی در عصر دیجیتال» پذیرفت. در دسامبر ۲۰۱۳ چهارمین گروه متخصصین دولتی تشکیل گردید؛ و در جولای ۲۰۱۵ گروه اقدام به ارسال گزارش اجماعی که تشریح کننده برخی یافته‌های دو گزارش پیش‌تر ارائه‌شده بود، نمود. گروه پنجم متخصصین دولتی در دسامبر ۲۰۱۵ با امید به افزایش انتظام قواعد فضای سایبری ایجاد شد؛ ولی در ژوئن ۲۰۱۷ تلاش متخصصین برای رسیدن به گزارش اجماعی به شکست انجامید. ظاهراً کوبا، چین و روسیه تصمیم به عدم پذیرشِ پیش‌نویس نموده‌اند (هنریکسن، ۲۰۱۹). گروه متخصصین (کارشناسان) دولتی در سال ۲۰۲۱ آخرین گزارش خود را ارائه نمود که بند F پاراگراف گزارش نهایی آن به‌صورت رسمی فضای سایبر را به‌عنوان فضای مخاصمه اعلام کرد و برای همیشه GGE جمع شد. بند مذکور بدین شرح است: «این گروه خاطرنشان می‌سازد که قوانین بین‌المللی بشردوستانه فقط در شرایط درگیری مسلحانه اعمال می‌شود. این قانون اصول حقوقی بین‌المللی تثبیت‌شده را یادآور می‌شود، از جمله، در صورت لزوم، اصول انسانیت، ضرورت، تناسب و تمایز که در گزارش سال ۲۰۱۵ نیز ذکر شده است. این گروه نیاز به مطالعه بیشتر در مورد چگونگی و زمان اعمال این اصول در استفاده از فناوری اطلاعات و ارتباطات توسط دولت‌ها را تشخیص داد و تأکید کرد که یادآوری این اصول به هیچ وجه باعث مشروعیت یا تشویق درگیری نمی‌شود» (جنرال اسمبلی، ۲۰۲۱). به‌تازگی دبیرکل سازمان ملل در سخنانی ایراد داشته که «مطمئنم که رویارویی‌های بزرگ آینده – که خدا کند هیچ‌وقت رخ ندهند – با حمله سایبری بزرگی آغاز خواهد شد» (گوترش، ۲۰۲۱).

سازمان ملل متحد – اجلاس جهانی سران درباره جامعه‌ی اطلاعاتی

مجمع عمومی سازمان ملل، در دسامبر سال ۲۰۰۱، در قطعنامه‌ی A/RES/56/183 خود، نهادی تحت عنوان «اجلاس جهانی جامعه‌ی اطلاعاتی»[1] را که پیرو قطعنامه سال ۱۹۹۸ کنفرانس تام‌الاختیار اتحادیه بین‌المللی ارتباطات راه دور صادر شده بود، تصویب و امضا نمود؛ که بر اساس آن، دبیر کل سازمان ملل، همراه با «اتحادیه جهانی مخابرات» که نقش راهنما و سرپرست کشورهای میزبان را دارد، با همراهی سایر

1. World Summit on the Information Society (WSIS)

سازمان‌های تخصصی، این اجلاس را برگزار نمودند. اجلاس جهانی سران درباره جامعه اطلاعاتی در سال‌های ۲۰۰۳ در ژنو و ۲۰۰۵ در تونس برگزار شد. پس از این تاریخ هر سال در ماه می، نشستی با میزبانی اتحادیه بین‌المللی مخابرات و همکاری برخی دیگر از سازمان‌های بین‌المللی به منظور پیگیری مصوبات آن دو اجلاس برگزار شده است. برپایی این اجلاس بر اساس قطعنامه‌ی شماره ۷۳ کنفرانس سران «اتحادیه جهانی مخابرات» بود که با مشورت با آژانس‌های تخصصی سازمان ملل و موافقت آن‌ها، به این نتیجه رسیدند که نیاز به اجلاسی جهانی در مورد جامعه‌ی اطلاعاتی وجود دارد. اتحادیه جهانی مخابرات در نشست سال ۲۰۰۱ تصویب کرد که این اجلاس را در دو فاز داشته باشند: – ژنو از ۱۰ تا ۱۲ دسامبر سال ۲۰۰۳ و در گام دوم– در تونس سال ۲۰۰۵ (خوشنویس، ۱۳۹۸الف، به نقل از سلطانی، ۱۳۹٤).

سازمان ملل متحد – گروه کاری پایان باز[1]

گروه کاری پایان باز از طریق قطعنامه ۲۷/۷۳، توسط مجمع عمومی ایجاد گردید؛ که در آن از همه کشورهای عضو سازمان ملل دعوت شده است که در آن شرکت کنند. این گروه برای اولین بار در سال ۲۰۱۹ تشکیل شده است و در سال ۲۰۲۰ به مجمع عمومی گزارشاتی را ارائه داده است. فرایند گروه کاری پایان باز همچنین امکان برگزاری جلسات مشورتی بین جلساتی را با صنعت، سازمان‌های غیردولتی و دانشگاه‌ها فراهم می‌کند (UN, 2023).

سازمان ملل متحد – گروه کاری پایان باز دو [2]

گروه کاری باز ۲ برای امنیت و استفاده از فناوری اطلاعات و ارتباطات (۲۰۲۵–۲۰۲۱) در نوامبر ۲۰۲۰، مجمع عمومی از طریق قطعنامه A/RES/75/240، به ایجاد گروه کاری باز (OEWG) در زمینه امنیت و استفاده از فناوری‌های اطلاعات و ارتباطات رأی داد. این سازمان در سال ۲۰۲۱ کار خود را آغاز نموده است و در سال ۲۰۲۵ به مجمع عمومی گزارش می‌دهد. این دومین OEWG سازمان ملل در زمینه فناوری اطلاعات و ارتباطات در زمینه امنیت بین‌المللی است (پیس اند فریدام، ۲۰۲۳).

سازمان ملل متحد – اتحادیه بین‌المللی مخابرات[2]

اتحادیه بین‌المللی مخابرات از سازمان‌های تخصصی سازمان ملل است که اکثر کشورهای جهان عضو آن هستند (سلطانی، ۱۳۹۹)؛ اکنون ۱۹۳ کشور و ۷۰۰ نهاد خصوصی از سرتاسر جهان عضو این اتحادیه هستند و دارای ۱۲ اداره مختلف در سطوح منطقه‌ای است. این اتحادیه که مقر آن در ژنو است، سازمانی بین‌المللی است که دولت‌ها و بخش خصوصی از طریق آن شبکه‌ها و خدمات ارتباطات جهانی را هماهنگ می‌کنند و نقشی کلیدی در استانداردسازی و توسعه صنعت ارتباطات و البته موضوعات امنیت سایبری ایفا می‌نماید (تقی زاد، ۱۳۹۵). در سال ۲۰۱۲ هم‌زمان با بازنگری قواعد اتحادیه بین‌المللی مخابرات، روسیه پیشنهاد تحویل کلیه اقدامات و مسئولیت‌های آیکان به اتحادیه را داد (مولر، ۲۰۱۹). بر اساس شاخص GCI منتشرشده از سوی اتحادیه بین‌المللی مخابرات در سال‌های ۲۰۱٤، ۲۰۱۷ و ۲۰۱۸، وضعیت ج.ا.ایران در سطح متوسطی قرار دارد. شاخص GCI شاخصی است که اتحادیه بین‌المللی مخابرات برای ارزیابی

1. OEWG
2. International Telecommunications Union (ITU)

سطح امنیت سایبری کشورهای مختلف، بر مبنای شاخص‌های متعددی منتشر می‌کند، بر اساس این شاخص، ج.ا.ایران در بین کشورهای جهان، نه در دسته کشورهای پیشتاز و نه در دسته کشورهای ضعیف قرار دارد، بلکه توانسته در دسته‌بندی متوسط در سطح جهانی قرار گیرد. پنج رکن اصلی در شاخص GCI شامل (۱) سنجه‌های قانون‌گذاری (۲) سنجه‌های فنی (۳) سنجه‌های سازمانی (٤) ظرفیت‌سازی و (۵) همکاری بین‌المللی است که با امتیازگذاری هر رکن درنهایت به‌صورت حاصل جمع تمامی آن‌ها ارائه می‌گردد (آی‌تی‌یو، ۲۰۱۸).

مجمع حکمرانی اینترنت[1]

مجمع حکمرانی اینترنت یک بستر باز و فراگیر برای مشارکت ذی‌نفعان در مباحثات سیاستی اینترنت و ارائه راه‌حل در موضوعات و چالش‌های مشترک و هنجارسازی در حوزه حکمرانی فضای سایبری است (مکبری، ۱۳۹۸)؛ که بر مبنای مصوبه دومین اجلاس سران جامعه اطلاعاتی در سال ۲۰۰۵ و در کشور تونس، تأسیس شده است؛ که دبیر کل سازمان ملل متحد، تأسیس آی‌جی‌اف را در جولای ۲۰۰٦ به‌صورت رسمی اعلام نمود و اولین جلسه آن در اکتبر ۲۰۰٦ برگزار شد؛ و با مأموریت تقویت همکاری‌ها در ایجاد مکانیزم‌های حکمرانی اینترنت، تشکیل گردیده است. گردهمایی‌های این مجمع به طور سالانه برگزار می‌شود که اساس تشکیل آن بر اساس درخواست مندرج در بند ۷۲ از برنامه اقدام اجلاس سران جامعه اطلاعاتی در تونس (۲۰۰۵) از دبیرکل سازمان ملل متحد برای اجرای فرایندی باز، با هدف ایجاد و پی‌ریزی یک مجمع جدید برای گفتگو و تبادل نظر ذی‌نفعان در حوزه سیاست‌گذاری راهبری اینترنت ایجاد شد. البته طی سال‌های ابتدایی تأسیس آن، با اعمال نفوذ آمریکا و مجامع فنی وابسته به آن، مأموریت مجمع به بحث و هنجارسازی محدود گردیده است.

سازمان آموزشی، علمی و فرهنگی سازمان ملل متحد (یونسکو)

«یونسکو»[2] یک سازمان تخصصی سازمان ملل متحد است که باهدف کمک به «ایجاد صلح، ریشه‌کن‌کردن فقر، توسعه پایدار و گفتگوی بین فرهنگی از طریق آموزش، علوم، فرهنگ، ارتباطات و اطلاعات» به وجود آمده است و جانشین کمیته بین‌المللی همکاری اندیشمندانه جامعه ملل است. یونسکو ۱۹۳ عضو رسمی و ۱۱ عضو وابسته دارد. اکثر دفاتر آن در شهر پاریس مستقر است. البته دارای دفاتر ملی و منطقه‌ای است و از فعالیت‌های مشارکتی یونسکو می‌توان به خطوط یازده‌گانه اجلاس سران جامعه اطلاعاتی که عبارت‌اند از فعالیت در خصوص خطوط عمل ۳ دسترسی به اطلاعات، آموزش الکترونیکی از خط عمل شماره ۷، دانش الکترونیکی از خط عمل شماره ۷، هویت و تنوع فرهنگی از خط عمل شماره ۸، تنوع زبانی و محتوای بومی از خط عمل شماره ۹ رسانه‌ها، ابعاد اخلاقی جامعه اطلاعاتی از خط عمل شماره ۱۰ اشاره کرد.

۳-۲. مطالعه تطبیقی همکاری بین‌المللی در فضای سایبر سایر کشورها

1. Internet Governance Forum (IGF)
2. United Nations Educational, Scientific and Cultural Organization (UNESCO)

۱-۳-۲. ژاپن

ژاپن ازجمله کشورهایی است که کلید اعتمادسازی و توسعهٔ قابلیت‌های حکمرانی سایبری را ناشی از ترویج و اجرای توصیه‌های گروه متخصصان دولتی در هر یک از کشورها و مناطق جهان می‌داند و بر این اساس در زمینه‌ی توسعه‌ی همکاری‌های بین‌المللی و مشارکت در مدیریت و حکمرانی فضای سایبر تلاش‌های خود را در سه بخش عمده پیگیری می‌نماید (کریمی قهرودی و زارعی، ۱۳۹۹).

الف) حاکمیت قانون در فضای سایبری: ترویج اعمال قوانین بین‌المللی موجود در فضای سایبری و تدوین مشترک هنجارهای رفتار ملی مسئولانه در این فضا.

ب) اعتمادسازی: توسعهٔ اعتمادسازی از طریق چارچوب‌های دوجانبه و چندجانبه از قبیل انجمن‌های منطقه‌ای اتحادیهٔ کشورهای جنوب شرقی آسیا (آسه‌آن).

پ) توسعهٔ قابلیت‌ها: مشارکت فعال در زمینه کمک به توسعه منابع انسانی و همکاری‌های فنی با تمرکز بر منطقه آسه‌آن.

از دیدگاه ژاپن، پذیرفتن قابل‌اعمال بودن قوانین بین‌المللی در فضای سایبری و تدوین هنجارهای رفتار مسئولانه در این فضا برای امنیت و ثبات بین‌المللی حیاتی است. این کشور بر پنج اصل «گردش آزاد اطلاعات، حاکمیت قانون، آزادی، استقلال و حکمرانی چند ذی‌نفعی» تأکید می‌کند.

۲-۳-۲. هند

از دیدگاه کشور هند، همان‌گونه که گروه متخصصان دولتی سازمان ملل در گزارش خود در سال ۲۰۱۵ تصریح می‌کند، لازم است جامعه‌ی بین‌المللی درک مشترکی از رفتار مسئولانه در فضای سایبری داشته باشند و اقدامات بیشتری در راستای توسعه‌ی قابلیت‌ها و اعتمادسازی اتخاذ کنند. تفاوت‌های معنایی نباید موجب توقف بحث و تبادل‌نظر در مورد حکمرانی اینترنت شوند. از نگاه هندوستان دولت باید در حکمرانی چند ذی‌نفعی بر فضای سایبری بین‌المللی نقش اصلی را ایفا کند (خوشنویس، ۱۳۹۸ب).

۳-۳-۲. اندونزی

کشور اندونزی نیز معتقد است باید تمام بازیگران به مشارکت در حکمرانی جهانی بر اینترنت ترغیب شوند. اندونزی عمدتاً بر اتکا به سازمان ملل جهت حکمرانی بر اینترنت جهانی و به رسمیت شناختن حاکمیت فضای سایبری تأکید کرده است (قنبری باغستان، ۱۳۹۸).

٤-۳-۲. فنلاند

فنلاند نیز که ازجمله‌ی کشورهایی است که در گفتمان بین‌المللی در زمینهٔ مسائل سایبری مشارکت فعال داشته است و از حکمرانی بر اینترنت بر اساس یک مدل چند ذی‌نفعی حمایت می‌کند و فعالیت گروه متخصصان دولتی را بسیار مهم تلقی نموده و از آن پشتیبانی می‌نماید. فنلاند همواره به ترغیب گفتمان چند ذی‌نفعی و بهبود همکاری‌های ملی و بین‌المللی همت گمارده است (کریمی قهرودی و زارعی، ۱۳۹۹).

۵-۳-۲. استرالیا

استرالیا معتقد است هنگام تدوین هرگونه قانون ملی جدید در زمینهٔ فضای سایبری باید از قوانین بین‌المللی پیروی شود. این کشور بر این باور است که گزارش گروه متخصصان دولتی[1] در حوزه تحولات در بخش اطلاعات و ارتباطات در زمینه امنیت بین‌المللی یک راهنمای مهم برای کشورها است و می‌توان رهنمودهای این گزارش را گسترش داد و با تمرکز بر اقدامات در حوزه‌ی اعتمادسازی معطوف به افزایش شفافیت در فعالیت‌های مشترک شد (کشاورز و دیگران، ۱٤۰۱).

---

۱. گزارش گروه متخصصان دولتی در سال ۲۰۱۵ م. رهنمودهایی در زمینه حفاظت از زیرساخت‌های حیاتی، واکنش به فوریت‌های رایانه‌ای، ضرورت مساعدت و همکاری کشورها در زمینه مقابله با جرایم سایبری و جلوگیری از اشاعه ابزارها و فناوری‌های شبکه‌ای مخرب ارائه نموده است.

٦-۳-۲. آلمان

آلمان نیز در راستای ورود به موضوعات بین‌المللی فضای سایبر عمدتاً بر موارد ذیل در عرصهٔ حکمرانی بین‌المللی این فضا تأکید می‌کند (شعبانی، ۱۳۹۸):

(۱) تقویت همکاری‌های بین‌المللی، دستیابی به‌اتفاق نظر در مورد اصل رفتار مسئولانه در فضای سایبری.

(۲) صادق بودن حاکمیت ملی و هنجارها و اصول بین‌المللی حاکمیت در خصوص فعالیت‌های ملی در زمینهٔ فناوری‌های اطلاعاتی و ارتباطی و اختیار کشورها بر زیرساخت‌های اطلاعاتی و ارتباطی موجود در قلمروی آن‌ها.

(۳) مشارکت در اقدامات در زمینه اعتمادسازی و بهبود اعتماد متقابل

(٤) حل مناقشات در زمینه فناوری‌های اطلاعاتی و ارتباطی به‌صورت مسالمت‌آمیز از طریق گفتمان.

۷-۳-۲. آمریکا

آمریکا مدعی است هنگام بحث پیرامون حاکمیت سایبری باید آن را با قوانین مدیریت فناوری‌های اطلاعاتی و ارتباطی موجود در قلمروی خود پیوند دهیم و نحوهٔ صادق بودن قوانین بین‌المللی در مورد استفاده‌ی ملی از فناوری‌های اطلاعاتی و ارتباطی را تبیین کنیم. درعین‌حال باید از همسو بودن اقدامات تنظیمی با الزامات بین‌المللی کشور از قبیل الزامات حقوق بشر اطمینان حاصل کرد. اصل عدم‌مداخله در امور داخلی کشورهای دیگر مبتنی بر رعایت مفاد قوانین بین‌المللی و خودداری از استفاده از قوه‌ی قهریه است (کریمی قهرودی و زارعی، ۱۳۹۹).

ازآنجاکه فعالیت‌های سایبری توسط حاکمیت فضای سایبری، حکمرانی می‌شوند، فعالیت‌های سایبری بازیگران غیر کشوری نیز باید تابع حاکمیت فضای سایبری باشند. ازاین‌رو، پیامدهای قضایی فعالیت‌های سایبری این بازیگران بر عهدهٔ کشورها است.

آمریکا نسبت به حاکمیت فضای سایبری مواضع دوگانه‌ای دارد. این کشور از یک‌سو از «نظریهٔ فضای سایبری به‌عنوان یک حوزه‌ی مشترک جهانی» و «آزادی اینترنت» حمایت

و با مفهوم حاکمیت فضای سایبری مخالفت می‌کند و از سوی دیگر اقدامات گسترده‌ای جهت حفاظت از حاکمیت و امنیت فضای سایبری خود انجام می‌دهد. آمریکا در برخی مواقع در راستای کمک به توسعه‌ی دموکراسی از «نظریه‌ی فضای سایبری به‌عنوان یک حوزه‌ی مشترک جهانی» حمایت و با مدیریت اینترنت توسط یک کشور خاص مخالفت می‌کند. به‌عنوان‌مثال، آمریکا با این دیدگاه که اینترنت به تمام جهان تعلق دارد مخالف بود و از متوقف سازی مدیریت اینترنت جهانی خودداری می‌کرد. با این حال به‌موجب فشارهای جامعه‌ی بین‌الملل در سال ۲۰۱۵ از مدیریت شرکت اینترنتی نام‌ها و شماره‌های تخصیص‌یافته (آیکان) دست کشید ولی تأکید کرد این شرکت باید خصوصی‌سازی شود نه اینکه به نهادهای دولتی یا بین دولتی واگذار گردد (کریمی قهرودی و زارعی، ۱۳۹۹).

شماری از نهادهای دولت فدرال آمریکا که مسئول در امر حکمرانی و امنیت فضای سایبری هستند، شامل وزارت بازرگانی، وزارت دفاع، وزارت امنیت میهنی، وزارت دادگستری و وزارت امور خارجه هستند؛ این نهادهای ویژه در توسعه استانداردهای بین‌المللی، تدوین سیاست دفاع سایبری، بررسی‌های برون‌مرزی، قانون‌گذاری و دفاع از منافع آمریکا در مراکز بین‌المللی، نقش دارند.

نهادهای فدرال نقش‌های مختلفی در تأثیرگذاری‌های بین‌المللی این کشور در حوزهٔ حکمرانی و امنیت فضای سایبری دارند که می‌توان از جمله آن‌ها به روابط دوجانبه و چندجانبه آمریکا با کشورهای دیگر، اعزام کارمند به آژانس‌های خارجی، رهبری یا عضویت در نمایندگی‌های آمریکا، هماهنگی سیاست آمریکا با نهادهای این کشور از طریق امور میان سازمانی و یا شرکت در نشست‌ها، اشاره کرد.

جنبه‌های جهانی فضای سایبری چالش‌هایی کلیدی را برای سیاست آمریکا به وجود آورده است و تا زمانی که این چالش‌ها مطرح باشد، آمریکا قادر به ارتقاء منافع ملی خود در زمینه فضای سایبری نخواهد بود (زنگی‌آبادی، ۱۳۹۶).

۸-۳-۲. فرانسه

فرانسه را می‌توان منتقد جدی انحصارگرایی در اینترنت دانست؛ به‌طوری‌که رئیس‌جمهور فرانسه «ماکرون» در مراسم افتتاحیه آی‌جی‌اف ۲۰۱۸[1] در پاریس، با انتقاد جدی از چالش‌ها و تهدیدات روزافزون ناشی از اینترنت موجود برای حیات و بقاء جوامع و دموکراسی‌ها، در خصوص مسئله بحران اعتماد دیجیتال سخن گفت و با انتقادهای خود از اینترنت آمریکایی و اینترنت چینی، ضرورت ایجاد مدل جدیدی از فضای مجازی و ایجاد چارچوب جدید تنظیم مقررات بین‌المللی برای اینترنت را مطرح نمود.

سناریوهای حکمرانی فضای مجازی فرانسه شامل موارد زیر است:

(۱) تأکید بر استقلال، بی‌طرفی و تنظیم‌گری داده‌محور؛

(۲) تلاش برای همکاری با کشورهای عضو اتحادیه اروپا؛

(۳) توجه نهاد تنظیم‌گر به توسعه زیرساخت‌ها خصوصاً در مناطق دورافتاده؛

(٤) حاکمیت به نیابت از مردم، تأکید بر تنظیم‌گری مشارکتی؛

(۵) حوزه‌های فیلترینگ و تعقیب قضایی: سایت‌های ناقض حق‌تألیف و محدودیت پورنوگرافی برای کودکان (تسنیم، ۱۳۹۹).

۹-۳-۲. چین

در سال ۲۰۱۷ میلادی جمهوری خلق چین، سند راهبرد بین‌المللی همکاری فضای سایبری را با چهار فصل و یک دیباچه با امضای رئیس جمهور منتشر کرده است. اهم فصول و زیرفصل‌های آن شامل دیباچه، فصل اول: فرصت‌ها و چالش‌ها، فصل دوم: اصول اساسی (اصل صلح، اصل حاکمیت، اصل حکمرانی مشترک و اصل منافع مشترک)، فصل سوم: اهداف راهبردی (حفاظت از حاکمیت و امنیت، ایجاد یک سیستم از قواعد بین‌المللی، ترویج حکمرانی عادلانه اینترنت، حفاظت حقوق و منافع مشروع شهروندان، ترویج همکاری در اقتصاد دیجیتال و بسترسازی جهت تبادل فرهنگ سایبری)، فصل چهارم: طرح اقدام (صلح و ثبات در فضای سایبر، نظم مبتنی بر قاعده در فضای سایبری، مشارکت در

1. IGF 2018

فضای سایبر، اصلاح نظام جهانی حکمرانی اینترنت، همکاری بین‌المللی در خصوص تروریسم سایبری و جرایم سایبری، حمایت از حقوق و منافع شهروندان از جمله حریم خصوصی، اقتصاد دیجیتال و اشتراک‌گذاری سود دیجیتال، توسعه و حفاظت از زیرساخت اطلاعاتی جهانی و تبادل فرهنگ‌های سایبری) که خلاصه‌ای از آنکه مرتبط با پژوهش حاضر است در ادامه ذکر شده است:

با روند شتابان در شکل‌گیری جهان چندقطبی، جهانی‌شدن اقتصاد در عین وجود تنوع فرهنگی در جهان و نظام حکمرانی جهانی به‌شدت در حال تغییر، بشر وارد عصر جدیدی از انقلاب اطلاعات شده است؛

فضای سایبر در حال تبدیل به مسیر جدیدی برای انتشار اطلاعات، حوزه‌ای جدید برای کار و زندگی مردم، موتوری جدید برای رشد اقتصادی، حاملی جدید برای شکوفایی فرهنگی، بستری جدید برای حکمرانی اجتماعی و پلی جدید برای ارتباط و همکاری و حوزه حاکمیت دولت است؛

نظام حکمرانی جهانی موجود بر منابع پایه اینترنت به‌سختی تمایلات و منافع اکثر کشورها را منعکس می‌نماید؛

فقدان قواعد عمومی بین‌المللی در فضای سایبر که به شکل مؤثری بر رفتار همه طرف‌ها حاکم باشد، توسعه فضای سایبر را با مشکل مواجه می‌کند؛

هیچ کشوری نمی‌تواند از چنین مشکلات و چالش‌هایی مصون بماند. جامعه بین‌الملل تنها می‌تواند از طریق تشدید همکاری با روحیه احترام و درک متقابل، سازگاری با یکدیگر کار نماید تا یک نظام حکمرانی جهانی مبتنی بر قاعده در فضای سایبر برقرار گردد؛

چین نیرویی برای صلح جهانی، مشارکت‌کننده در توسعه جهانی و مدافع نظم بین‌المللی بوده است. این کشور با استواری، مسیر توسعه مسالمت‌آمیز را دنبال می‌نماید، برای حمایت از عدالت و دوستی و پیگیری منافع مشترک تلاش می‌کند و خواستار نوع جدیدی از روابط بین‌المللی با همکاری برد – برد، و تمرکز بر توسعه صلح‌آمیز و پیام اصلی همکاری برد – برد است؛

راهبرد بین‌المللی همکاری در فضای سایبر چین از اصول صلح، حاکمیت، حکمرانی مشترک و منافع مشترک در تبادلات بین‌المللی و همکاری در فضای سایبری حمایت می‌کند؛

در فضای سایبری به‌هم‌پیوسته، کشورها با منافع درهم‌تنیده به یکدیگر پیوند خورده‌اند. فضای سایبری امن، باثبات و مرفه برای همه کشورها و جهان اهمیت زیادی دارد؛

جامعه بین‌الملل باید اهداف و اصول مندرج در منشور ملل متحد، به‌ویژه عدم توسل به‌زور و حل‌وفصل مسالمت‌آمیز اختلافات را به‌منظور تضمین صلح و امنیت در فضای سایبر، به‌طورجدی رعایت کند؛

همه کشورها باید با اقدامات خصمانه و تجاوزکارانه مخالفت کنند که به پشتوانه فناوری اطلاعات و ارتباطات صورت می‌گیرد؛

از مسابقه تسلیحاتی و درگیری در فضای سایبر جلوگیری کرده و اختلافات خود را از طریق روش‌های مسالمت‌آمیز حل‌وفصل نمایند؛

تروریسم سایبری تهدید جدی را نسبت به صلح و امنیت بین‌المللی تحمیل می‌کند. جامعه بین‌المللی باید اقدامات عمل‌گرایانه را برای جلوگیری و مبارزه علیه فعالیت‌های تروریسم سایبری اتخاذ نماید. باید اقداماتی جهت ممانعت استفاده تروریست‌ها از اینترنت برای گسترش ایدئولوژی افراطی یا برنامه‌ریزی و سازماندهی فعالیت‌های تروریستی سایبری صورت پذیرد؛

به‌عنوان یک هنجار مبنایی در روابط بین‌الملل معاصر، اصل حاکمیت مندرج در منشور سازمان ملل متحد، تمامی وجوه روابط دولت با دولت را که شامل فضای سایبری نیز می‌شود، در برمی‌گیرد. کشورها باید به حق یکدیگر در انتخاب مسیر توسعه سایبری خود، الگوی تنظیم مقررات سایبری و سیاست‌های عمومی اینترنت احترام گذارند و در حکمرانی فضای سایبری بین‌المللی به‌صورت برابر مشارکت داشته باشند. هیچ کشوری نباید استیلا[۱] سایبری را دنبال نموده، در امور داخلی دیگر کشورها مداخله کند و یا در فعالیت‌های

۱. هژمونی.

سایبری که امنیت ملی دیگر کشورها را تضعیف می‌کند مشارکت داشته باشد یا از آن حمایت نماید؛

حمایت از حاکمیت در فضای سایبر نه‌تنها نشان‌دهنده مسئولیت و حق دولت‌ها برای اداره فضای سایبری مطابق با حقوق است، بلکه کشورها را قادر می‌سازد تا بسترهایی را برای تعاملات صحیح بین حکومت‌ها، مشاغل و گروه‌های اجتماعی ایجاد کنند. این امر باعث تقویت یک زیست‌بوم سالم برای پیشرفت فناوری اطلاعات و تبادل و همکاری بین‌المللی می‌شود؛

فضای سایبر، فضای مشترکی برای فعالیت‌های بشری است از این‌رو لازم است تا توسط همه کشورها ساخته و مدیریت گردد. حکمرانی بین‌المللی فضای سایبری باید از رویکرد چندجانبه‌گرایی تبعیت نماید. کشورها، اعم از بزرگ یا کوچک، قوی یا ضعیف، غنی یا فقیر، همگی اعضای برابر در جامعه بین‌الملل هستند که حق مشارکت برابر در توسعه نظم و قواعد بین‌المللی در فضای سایبری را از طریق سازوکارها و بسترهای حکمرانی بین‌المللی دارند تا اطمینان حاصل گردد که توسعه آینده فضای سایبر در دست همه مردم هست؛

حکمرانی بین‌الملل فضای سایبر باید دارای خصیصه مشارکت چند طرفی-چند عضوی- باشد. همه طرف‌ها، از جمله دولت‌ها، سازمان‌های بین‌المللی، شرکت‌های اینترنتی، جوامع فناوری، مؤسسات غیردولتی و تک‌تک شهروندان، باید نقش خود را در ایجاد یک بستر حکمرانی همه‌بعدی و چندلایه ایفا کنند؛

کشورها باید ارتباطات را تقویت کرده، گفتگوها و سازوکارهای مشاوره مرتبط با فضای سایبر را بهبود بخشیده و قواعد بین‌المللی سایبری را به طور مشترک توسعه دهند؛

هدف راهبردی مشارکت چین در همکاری‌های بین‌المللی فضای سایبری عبارت‌اند از:

(۱) محافظت قاطعانه از حاکمیت، امنیت و منافع توسعه کشور در فضای سایبری؛

(۲) تضمین جریان امن و منظم اطلاعات در اینترنت؛

(۳) بهبود اتصال جهانی؛

(٤) حفظ صلح، امنیت و ثبات در فضای سایبری؛

(۵) تقویت حاکمیت قانون بین‌المللی[1] در فضای سایبری؛

(٦) ترویج توسعه جهانی اقتصاد دیجیتال؛

(۷) تبادل فرهنگی و یادگیری متقابل را تعمیق بخشیده تا ثمره توسعه اینترنت به گوشه‌وکنار جهان برسد و به نفع مردم تمامی کشورها باشد.

چین متعهد به حفظ صلح و امنیت در فضای سایبر و ایجاد نظم بین‌المللی فضای سایبری عادلانه و معقول بر اساس حاکمیت دولت است و فعالانه برای ایجاد اجماع بین‌المللی در این زمینه تلاش نموده است؛

فضای سایبر به‌عنوان یک حریم جدید، باید با قوانین و هنجارهای رفتاری اداره گردد. چین از تدوین قواعد بین‌المللی پذیرفته‌شده جهانی‌ای و هنجارهای رفتار دولت‌ها در فضای سایبر در چارچوب سازمان ملل متحدی حمایت می‌نماید که اصول اصلی را برای دولت‌ها و سایر بازیگران جهت تنظیم رفتار خود و تشدید همکاری به‌منظور حفظ امنیت، ثبات و رفاه در فضای سایبری ایجاد می‌نماید؛

چین معتقد است که باید از طریق مشارکت برابر و تصمیم‌گیری مشترک جامعه بین‌المللی، یک نظام حکمرانی جهانی اینترنت چندجانبه، دموکراتیک و شفاف ایجاد گردد. کشورها حق دارند به‌صورت برابر در حکمرانی اینترنت مشارکت کنند. اطمینان از توزیع عادلانه منابع پایه اینترنت و مدیریت مشترک زیرساخت‌های اطلاعاتی حساس مانند سرورهای ریشه[2]، مهم است. فرایندهای بین‌المللی مربوطه باید باز و فراگیر و نماینده و صدای بیشتر کشورهای درحال‌توسعه باشد؛

چین خواستار افزایش ارتباط و همکاری میان همه ذی‌نفعان از جمله دولت‌ها، سازمان‌های بین‌المللی، شرکت‌های اینترنتی، جوامع فناوری، نهادهای غیردولتی و شهروندان است. تلاش‌های مربوطه باید منعکس‌کننده مشارکت گسترده، مدیریت صحیح و تصمیم‌سازی دموکراتیک باشد به‌گونه‌ای که همه ذی‌نفعان بر اساس ظرفیت خود در آن

1. International Rule of Law

۲. روت.

سهیم بوده و دولت‌ها در حکمرانی اینترنت به‌ویژه خط‌مشی‌های عمومی و امنیتی پیشرو باشند؛

چین به مشارکت فعال در فرایندهای بین‌المللی مرتبط با سایبر، تقویت گفتگو و همکاری‌های دوجانبه و منطقه‌ای و بین‌المللی، ارتقاء اعتماد متقابل بین‌المللی و توسعه مشترک و مقابله با تهدیدات از طریق تلاش‌های مشترک، باهدف دستیابی به قواعد بین‌المللی پذیرفته‌شده جهانی و ایجاد یک سیستم حکمرانی سایبری منطقی عادلانه جهانی ادامه خواهد داد؛

چین در پیگیری نتایج اجلاس سران درباره جامعه اطلاعاتی شرکت خواهد نمود. از جامعه بین‌المللی برای تحکیم اجماع و اجرای نتایج، اطمینان از اشتراک مساوی مزایای جامعه اطلاعاتی و حکمرانی اینترنت به‌عنوان موارد مهم برای بررسی حمایت خواهد کرد؛

چین برای اصلاح نهاد مجمع حکمرانی اینترنت سازمان ملل متحد تلاش خواهد کرد تا بتواند نقش بیشتری در حکمرانی اینترنت ایفا نماید. ظرفیت تصمیم‌سازی خود را تقویت کرده، تأمین مالی ثابت را تضمین نموده و رویه‌های باز و شفاف را در انتخاب اعضای خود و ارائه گزارش به کار خواهد گرفت؛

چین همراه با سایر کشورها، هنجارهای رفتاری و اقدامات مشخصی را برای همکاری بین‌المللی علیه تروریسم سایبری، از جمله بحث در مورد کنوانسیون بین‌المللی مبارزه با تروریسم سایبری و ایجاد اجماع در خصوص مبارزه با جرایم سایبری و تروریسم سایبری را بررسی خواهد کرد تا زمینه همکاری اجرای قانون را در میان کشورها فراهم نماید؛

چین به‌منظور تقویت زیرساخت‌های اطلاعاتی جهانی جهت تسهیل جریان روان اطلاعاتی با سایر کشورها همکاری خواهد کرد. برای این امر اتصال زیرساخت‌های اطلاعاتی و ابتکار کمربند و راه را با کشورهای همسایه و فراتر از آن ارتقا خواهد داد تا کشورهای بیشتری و مردم آن‌ها بتوانند فرصت‌های توسعه‌ای را که اینترنت به ارمغان می‌آورد به اشتراک بگذارند (وزارت امور خارجه جمهوری خلق چین، ۲۰۱۷).

٤-۲. ابعاد و مؤلفه‌های همکاری بین‌المللی ج.ا.ایران در فضای سایبر

جدول شماره ۲: ابعاد و مؤلفه‌های احصاء شده همکاری بین‌المللی ج.ا.ایران در فضای سایبر (یافته‌های نگارنده)

ابعاد	مؤلفه‌ها
سیاست‌گذاری	– ارزش‌ها و اصول – اقدامات فنی – چهارچوب‌های تصمیم‌گیری
قوانین و مقررات	– مقررات – رویه‌ها – منابع – قانون اساسی
اجرایی و قضایی	– فرایند – سازمان‌ها و نهادها – مدیریت و عملکرد – اخلاق پاسخ‌گویی و شفافیت – ساختار
بین‌المللی	– نیروهای بین‌المللی جهانی‌سازی – بازیگران – معاهده‌ها – تحقیق و پژوهش
اقدامات عملیاتی	– کنش‌ها – فنی –اقتصادی – سیاسی و امنیتی – فرهنگی و اجتماعی – حقوقی

۳. روش‌شناسی تحقیق

با مطالعه ادبیات تحقیق و با استفاده از نظریه‌پردازی داده‌بنیاد در این پژوهش کاربردی – توسعه‌ای، مقوله‌های تأثیرگذار استخراج شده است. قلمرو زمانی (افق سال ۱٤۰٤ شمسی)، قلمرو مکانی (فضای سایبر جهانی) و قلمرو موضوعی تحقیق، عرصه بین‌المللی فضای

سایبر است. روش‌های جمع‌آوری اطلاعات عبارتند از میدانی: مصاحبه، پرسش‌نامه و مشاهده (ثبت مباحث مرتبط با موضوع در جلسات و گروه کانونی) و کتابخانه‌ای (فیش‌برداری از کتاب‌های علمی و تخصصی، مقالات علمی و پژوهشی، اسناد و مدارک موجود در آرشیو سازمان‌های مرتبط با موضوع و سایت‌های اینترنتی). در بخش اسناد بالادستی قانون اساسی، احکام، تدابیر و فرمایشات مقام معظم رهبری مدظله‌العالی و اسناد سایبری فراملی و بین‌المللی موردتوجه‌اند. مدل مفهومی از طریق پرسش‌نامه تحلیلی و برگزاری مصاحبه کانونی مورد ارزیابی قرار گرفت و تصحیح گردید. جامعه نمونه (تعداد صاحب‌نظران در حدود ۱۰۰ نفر به‌صورت در دسترس)، روش نمونه‌گیری در حوزه اسناد، به‌صورت تمام شمار، حجم نمونه ۳٤ نفر از صاحب‌نظران و روش نمونه‌گیری صاحب‌نظران به روش گلوله‌برفی تعیین گردید. به‌منظور اخذ نظر خبرگان جهت ارزیابی مدل مفهومی، پرسش‌نامه‌ای بر اساس طیف لیکرت تنظیم گردید.

٤. یافته‌ها و تجزیه‌وتحلیل داده‌ها

پیشینه‌ها و مبانی نظری موضوع پژوهش مورد واکاوی قرار گرفت و با تحلیل کیفی مستندات جمع‌آوری‌شده شامل مشاهده، مصاحبه با خبرگان، کتاب‌ها، مقالات و سایت‌های معتبر اینترنتی به روش کدگذاری باز عوامل اثرگذار احصاء (تحلیل کیفی) گردید.

در ادامه مدل‌سازی معادلات ساختاری با روش حداقل مربعات جزئی توسط نرم‌افزار اسمارت پی.ال.اس برای تجزیه‌وتحلیل یافته‌ها انتخاب‌شده و بر آن اساس نیز پرسش‌نامه‌ای تنظیم و در اختیار ۱۰ نفر از صاحب‌نظران قرار گرفت و نظرات تخصصی در خصوص روایی و پایایی پرسشنامه اخذ شد. ضمن اعمال اصلاحات لازم، پرسشنامه نهایی تنظیم و به‌صورت کاغذی و الکترونیکی در اختیار ۱۰۰ نفر از خبرگان قرار گرفت و در نهایت نیز ۳٤ پرسشنامه تکمیل‌شده اخذ گردید.

٤-۱. اطلاعات جمعیت‌شناختی

داده‌های حاصل از پرسش‌نامه در نرم‌افزار اس.پی.اس.اس[1] درج و اطلاعات جمعیت‌شناختی سؤالات عمومی پرسش‌نامه طبق جدول شماره (۳) استخراج گردید. بالغ‌بر ۵۸.۹ درصد از پاسخگویان را دکتری و دانشجویان دکتری تشکیل داده و مابقی دارای مدارک تحصیلی کارشناسی ارشد بودند.

جدول شماره ۳. اطلاعات جمعیت شناختی تحقیق

تحصیلات	تعداد	درصد	درصد تجمیعی
کارشناسی	۰	۰	۰
کارشناس ارشد	١٤	٤١.٢	٤١.٢
دانشجوی دکتری	۹	٢٦.٥	٦٧.٦
دکتری	١١	٣٢.٤	١۰۰
کل	٣٤	١۰۰.۰	١۰۰.۰

٤-۲. بررسی برازش مدل کلی: معیار GOF

سه مقدار ۰.۰۱ و ۰.۲۵ و ۰.٣٦ به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF ارائه شده است، این مقدار از جذر حاصل‌ضرب میانگین ستون «متوسط مشترک»[2] و میانگین «ضریب تعیین» حاصل می‌گردد (جدول ٤).

جدول شماره ٤. محاسبه برازش کلی مدل (معیار GOF) (یافته‌های نگارنده)

ابعاد و مؤلفه‌ها	ضریب تعیین (R^2)	متوسط مشترک (AVE=)

1. SPSS
2. *Communality*

به‌صورت مشخص در نسخه ۲ نرم افزار وجود دارد؛ ولی در نسخه ۳ نرم‌افزار از مقدارAVE استفاده می‌شود.

اجرایی و قضایی	۰.٦٥٢	۰.٧٠٧
اخلاق پاسخ‌گویی و شفافیت	۰.٦٣٦	۰.٦٨٩
ارزش‌ها و اصول	۰.٢٦٩	۰.٥٦٧
اقتصادی	۰.٤٩٣	۰.٨٣٤
اقدامات عملیاتی	۰.٥٥	۰.٥٤١
اقدامات فنی	۰.٥٠٩	۰.٦٨٣
بازیگران	۰.٧٥٩	۰.٦٦٦
بین‌المللی	۰.٤٦٩	۰.٥٨٤
تحقیق و پژوهش	۰.٤٨٦	۰.٦٩٧
حقوقی	۰.٤٠٢	۰.٩٣٦
حکمرانی	۰.٦٦٦	۰.٦٧٤
رویه‌ها	۰.٣٤٦	۰.٧٧٣
ساختار	۰.٥٩٢	۰.٧٩٢
سازمان‌ها و نهادها	۰.٤٢٤	۰.٨١
سیاست‌گذاری	۰.٥٩٤	۰.٤٧
سیاسی و امنیتی	۰.٥٢	۰.٦٥٧
فرایند	۰.٥٢٤	۰.٦١٤
فرهنگی و اجتماعی	۰.٤٩	۰.٦٧٤
فنی	۰.٤٢٦	۰.٦٨٤
قانون اساسی	۰.٣٣٧	۰.٦٤٢
قوانین و مقررات	۰.٤٦٧	۰.٥٩٣
مدیریت و عملکرد	۰.٥١١	۰.٦٦٥
معاهده‌ها	۰.٦٣٥	۰.٦٧
مقررات	۰.٣٤٢	۰.٧٧٧
منابع	۰.١٢٢	۰.٧٩٦

نیروهای بین‌المللی جهانی‌سازی	۰.٦٦٣	۰.٦٩٢
چارچوب‌های تصمیم‌گیری	۰.٣٢٦	۰.٦٦٤
کنش‌ها	۰.٣٨٥	۰.٨٤٥
میانگین	۰.٤٨٥	۰.٦٩٢
$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{۰.٦٩٢ \times ۰.٤٨٥} = ۰.۵۷۹$		

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰.۵۷۹ بوده و چون از ۰.۳٦ بیشتر است، برازش مدل را قوی ارزیابی می‌کنیم لذا با استفاده از نتایج حاصل می‌توان اقدامات لازم را در خصوص ارزیابی فرضیه‌های پژوهش را به انجام رساند. در ادامه طبق جدول ۵ ضریب مسیر، ضرایب z و سطح معناداری فرضیه‌های پژوهش ارائه گردیده است.

جدول شماره ۵. ضریب مسیر و ضریب معناداری روابط بین سازه‌ها (یافته‌های نگارنده)

فرضیه	روابط	ضریب مسیر[1]	ضرایب z	رد یا تأیید	سطح معناداری
H1	همکاری بین‌المللی ج.ا.ایران در فضای سایبر -> سیاست‌گذاری	۰.۷۷۳	۷.۱۵٦	تأیید	٪۹۹.۹
H6	سیاست‌گذاری -> ارزش‌ها و اصول	۰.۵۹۵	۳.۹۱٤	تأیید	٪۹۹
H7	سیاست‌گذاری -> اقدامات فنی	۰.۷۲٤	۷.۰۲٤	تأیید	٪۹۹.۹
H8	سیاست‌گذاری -> حکمرانی	۰.۸۱۹	۱۲.٤۷۱	تأیید	٪۹۹.۹
H9	سیاست‌گذاری -> چهارچوب‌های تصمیم‌گیری	۰.٦	۳.۹۱۲	تأیید	٪۹۹.۹
H2	همکاری بین‌المللی ج.ا.ا. در فضای سایبر -> قوانین و مقررات	۰.٦۷۵	۵.۰۲۳	تأیید	٪۹۹.۹

1. Sample Mean (M)

H10	قوانین و مقررات -> مقررات	۰.٦۰٥	٤.۹۰۸	تأیید	٪۹۹.۹
H11	قوانین و مقررات -> رویه‌ها	۰.٦۲۲	٦.٦٦۳	تأیید	٪۹۹.۹
H12	قوانین و مقررات -> منابع	۰.۳۷٤	۱.۷۱۸	رد	-
H13	قوانین و مقررات -> قانون اساسی	۰.٦۲٤	٤.۳٤	تأیید	٪۹۹.۹
H3	همکاری بین‌المللی ج.ا.ا. در فضای سایبر -> اجرایی و قضایی	۰.۸۱	۱۰.۳۷٤	تأیید	٪۹۹.۹
H14	اجرایی و قضایی -> فرایند	۰.۷٤۲	۱۰.۳۸۸	تأیید	٪۹۹.۹
H15	اجرایی و قضایی -> سازمان‌ها و نهادها	۰.٦٦۱	٥.۸٥	تأیید	٪۹۹.۹
H16	اجرایی و قضایی -> مدیریت و عملکرد	۰.۷۳	۹.۷۳۲	تأیید	٪۹۹.۹
H17	اجرایی و قضایی -> اخلاق پاسخ‌گویی و شفافیت	۰.۸۰۲	۱۲.٦۷٦	تأیید	٪۹۹.۹
H18	اجرایی و قضایی -> ساختار	۰.۷۷۲	۱۰.۲٦٤	تأیید	٪۹۹.۹
H4	همکاری بین‌المللی ج.ا.ا. در فضای سایبر -> بین‌المللی	۰.۷۰۲	۷.٦۲۸	تأیید	٪۹۹.۹
H19	بین‌المللی -> نیروهای بین‌المللی جهانی‌سازی	۰.۸۰۹	۹.٤۲۷	تأیید	٪۹۹.۹
H20	بین‌المللی -> بازیگران	۰.۸۷۷	۲۰.٥۳۸	تأیید	٪۹۹.۹
H21	بین‌المللی -> معاهده‌ها	۰.۷۹۷	۹.۷٥۲	تأیید	٪۹۹.۹
H22	بین‌المللی -> تحقیق و پژوهش	۰.۷۱	۷.۷	تأیید	٪۹۹.۹
H5	همکاری بین‌المللی ج.ا.ا. در فضای سایبر -> اقدامات عملیاتی	۰.۷٥۲	۹.۰٥۹	تأیید	٪۹۹.۹
H23	اقدامات عملیاتی -> کنش‌ها	۰.٦٤٦	٦.٤۹۱	تأیید	٪۹۹.۹
H24	اقدامات عملیاتی -> فنی	۰.٦۹۳	۷.۲۹۱	تأیید	٪۹۹.۹
H25	اقدامات عملیاتی -> اقتصادی	۰.۷۱٥	٥.٥۳۲	تأیید	٪۹۹.۹
H26	اقدامات عملیاتی -> سیاسی و امنیتی	۰.۷٤۹	٥.۷۲۸	تأیید	٪۹۹.۹
H27	اقدامات عملیاتی -> فرهنگی و	۰.۷۳	٥.۹۱۸	تأیید	٪۹۹.۹

	اجتماعی				
H28	اقدامات عملیاتی -> حقوقی	۰.۶۵۵	۵.۹۵۲	تأیید	٪۹۹.۹

۳-٤. بررسی برازش مدل ساختاری

این برازش، باید با استفاده از محاسبات بوت استرپینگ[1] (خود راه‌اندازی) (شکل ۱)، به‌منظور ارزیابی روابط بین متغیرهای پنهان به صورت زیر صورت پذیرفته است.

شکل شماره ۱. تحلیل خود راه‌اندازی (یافته‌های نگارنده)

۵. نتیجه‌گیری و پیشنهاد

نگرش تجویزی معتقد به طراحی رسمی و پیش‌بینی تدابیر تحلیلی برای تحقق هدف‌های بلندمدت است. این نگرش، شکل‌گیری راهبرد را فرایند مشخص، قابل پیش‌بینی و توأم با تدابیر تحلیلی و علت و معلولی می‌پندارد. عمده تعاریف در این نگرش راهبرد را به عنوان طرح، برنامه و یا نقشه در نظر می‌گیرد. به‌عبارت‌دیگر راهبرد در این نگرش، عبارت است

1. Bootstapping

از نوعی کار آگاهانه و یا مجموعه‌ای از رهنمودهاست که برای مقابله با وضعیت و یا رخدادی خاص در آینده، پیش‌بینی می‌شود. در این مکاتب راهبرد حاصل فرایندی تحلیلی و قاعده‌مند است. بحث اصلی تطابق و تعامل شرایط درونی با شرایط بیرونی است. الزامات پیاده‌سازی و تحقق راهبردها و راهکارهای پیشنهادی مربوطه در قالب نگرش تجویزی که شرح آن رفت؛ در جدول شماره ٦ که برگرفته از ابعاد و مؤلفه‌های ارایه شده در بخش قبل است، ارائه می‌گردد.

جدول شماره ۶. راهبردها، الزامات و راهکارهای همکاری بین‌المللی ج.ا.ایران در فضای سایبر

شماره	راهبرد، راهکارها و الزامات مرتبط
راهکارها و الزامات ۱	راهبرد: استفاده از ظرفیت بالای مشارکتی مردمی در تولید محتوای غنی فضای سایبر در پهنه بین‌المللی با سیاست‌گذاری و خط‌مشی‌گذاری ملی و حمایت حاکمیت.
	راهکارها: (۱) شناسایی، ارزیابی و تخصیص منابع به ظرفیت‌ها و جهت‌دهی و سیاست‌گذاری مناسب. (۲) تعیین سیاست‌ها در عرصه تولید محتوا به‌ویژه محتوای اسلامی – ایرانی.
	الزامات: (۱) تدارک زیرساخت مشارکت مردمی. (۲) تخصیص منابع لازم. (۳) سیاست‌گذاری برای تولید محتوای غنی.
راهکارها و الزامات ۲	راهبرد: تعامل مؤثر با کشورهای دوست به‌ویژه کشورهای اسلامی جهت تأسیس مراکز راهبری و عملیاتی فضای سایبر از مجرای دستگاه‌های ذی‌ربط.
	راهکارها: (۱) تشکیل ساختارهای متناسب برای راهبری ارتباط با سایر کشورها در زمینه فضای سایبر. (۲) تعیین مسئولیت‌ها و وظایف هریک از دستگاه‌ها اعم از فنی، حقوقی، قضائی و امنیتی.
	الزامات: (۱) ساختار و تشکیلات‌سازی متناسب و چابک. (۲) تعریف راهبرد تعامل با کشورهای دوست.
راهکار	راهبرد: نشر مبانی و اصول انقلاب اسلامی در عرصه بین‌المللی و اخلاق‌گرایی در فضای سایبر
	راهکارها:

	(۱) تشکیل هسته‌ها و گروه‌های خبره برای بازتعریف مبانی و اصول اسلامی– ایرانی و ایجاد کانال‌های رسمی – غیررسمی برای نشر معارف انقلاب اسلامی. (۲) نهادینه‌سازی در عمل به اصول و مبانی انقلاب اسلامی و اخلاق متعالی اسلام.
	الزامات: **(۱)** شناسایی و تربیت نخبگان عرصه مبانی و اصول اسلامی – ایرانی **(۲)** بسترسازی برای ایجاد کانال‌های بروز فضای سایبری
راهکارها و الزامات ٤	راهبرد: استفاده از ظرفیت‌های تجارتی و اقتصادی فضای سایبر
	راهکارها: (۱) شناسایی، ارزیابی و تخصیص منابع به ظرفیت‌های اقتصادی موجود در فضای سایبر به‌ویژه در تعامل با کشورهای دوست. (۲) حمایت از شرکت‌های دانش‌بنیان در حوزه فضای سایبری جهت توسعه و تبدیل به شرکت‌های معظم ملی و بین‌المللی و خدمات‌رسانی جهانی.
	الزامات: (۱) با تعریف ساختارهای اقتصادی بر مبنای فضای سایبر. (۲) ایجاد ظرفیت‌های جدید برای فعالیت در حوزهٔ فضای سایبر.
راهکارها و الزامات ٥	راهبرد: ایجاد و استفاده از زیرساخت‌های عرصه‌های جدید فناوری نظیر هوش مصنوعی، متاورس، ارزهای دیجیتال و...
	راهکارها: (۱) مطالعه و تحقیق جهت برخورداری از مزایا و اعراض از مضرات حوزه‌های جدید مالی نظیر ارزهای دیجیتال در ارتباط با سایر کشورهای مورد هدف جهت تجارت. (۲) تشکیل و راه‌اندازی زیرساخت‌های لازم جهت خلق فناوری‌های نوظهور نظیر رمز ارزها.
	الزامات: (۱) تشکیل ساختار رصد و پایش فناوری‌های نوظهور. (۲) طرح‌ریزی برای برخورداری حداکثری از مزایای فناوری‌های جدید.
راهکارها و الزامات ٦	راهبرد: دستیابی به تبادلات فرهنگی، سیاسی، اقتصادی، امنیتی و حقوقی در عرصه بین‌الملل با رعایت صیانت از هویت ملی و دینی
	راهکارها: (۱) تبیین طرح‌های راهبردی در حوزه‌های فرهنگی، سیاسی، اقتصادی، امنیتی و حقوقی بر اساس اصول و مبانی اسلامی– ایرانی جهت گسترش تعاملات در حوزه‌های مذکور.

	(۲) تربیت نیروی انسانی خبره در عرصه‌های فرهنگی، سیاسی، اقتصادی، امنیتی و حقوقی فضای سایبر بین‌الملل.
	الزامات: (۱) فعال‌سازی نهادهای ذی‌ربط جهت ایفای نقش در عرصهٔ بین‌الملل فضای سایبر. (۲) تدوین طرح‌های راهبردی سیاسی، اقتصادی، امنیتی و حقوقی فضای سایبر بین‌الملل.
راهکارها و الزامات ۷	راهبرد: مشارکت در تدوین اسناد و معاهده‌های بین‌المللی و منطقه‌ای فضای سایبر.
	راهکارها: (۱) تربیت و توسعه نیروی انسانی و طرح‌ریزی در خصوص نحوه مشارکت در اسناد منطقه‌ای و بین‌المللی فضای سایبر. (۲) شناسایی و رصد مستمر اسناد و معاهدات بین‌المللی و تشکیل کارگروه‌های ذی‌مدخل برای تصمیم‌سازی در خصوص چگونگی رویکرد ج.ا.ایران به آن‌ها.
	الزامات: (۱) ارتقای شناخت سازمان‌ها و نهادهای بین‌المللی فضای سایبر. (۲) بررسی دقیق معاهدات بین‌المللی فضای سایبر و تعیین رویکرد ج.ا.ا نسبت به آن‌ها.
راهکارها و الزامات ۸	راهبرد: نفی سلطه و مقابله با هژمونی آمریکا، کشورهای غربی و سلطه‌جو در حوزهٔ زیرساختی فنی و مدیریتی فضای سایبر
	راهکار: (۱) برنامه‌ریزی برای حضور فعال در نهادها، سازمان و ساختارهای منطقه‌ای و بین‌المللی و ایجاد پیمان‌های راهبردی با کشورهای همسو در زمینه فضای سایبر. (۲) ابتکار عمل پیش‌دستانه در خصوص قوانین و مقررات فضای سایبر بین‌الملل.
	الزامات: (۱) تقویت زیرساخت‌های فضای سایبر کشور علی‌الخصوص شبکه ملی اطلاعات. (۲) در دست‌داشتن ابتکار تدوین و توسعه پیمان‌های منطقه‌ای و بین‌المللی در فضای سایبر.

منابع

الف- فارسی

- پایداری ملی (۱۳۹۱). نگاهی متفاوت به سایبر، دوم دی، قابل دسترسی در: https://paydarymelli.ir/fa/news/1055/.
- تسنیم (۱۳۹۹). «شیوه حکمرانی فضای مجازی در فرانسه»، ***خبرگزاری تسنیم***، هفتم آذر.
- تقی‌زاد، مهرداد (۱۳۹۵). ***سازمان‌های بین‌المللی و قاعده‌مندسازی فضای سایبری***. تهران: خرسندی.
- خوشنویس، یاسر (۱۳۹۸الف). ***حکمرانی چند ذی‌ربطی فضای مجازی***، پژوهشگاه مرکز ملی فضای مجازی.
- خوشنویس، یاسر (۱۳۹۸ب). ***حکمرانی فضای سایبری در کشور هند***. تهران: پژوهشگاه مرکز ملی فضای سایبری- گروه مطالعات فرهنگی و اجتماعی.
- رامک، مهراب (۱۳۹۸). ***الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری***. پایان‌نامه دکتری، تهران: دانشگاه عالی دفاع ملی.
- رامک، مهراب، و محمدی، علی (۱۳۹۹). «ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور (بر اساس نظریه‌پردازی داده‌بنیاد)»، ***فصلنامه علمی امنیت ملی***، ۱۰(۳۷)، ۷-۴۲.
- زنگی‌آبادی، یونس (۱۳۹۶). ***چالش‌های پیش روی ایالات‌متحده در مواجهه با حکمرانی و امنیت سایبری جهانی***. تهران: شرکت انتشارات کیهان.
- سلطانی، نصرالله (۱۳۹۹). ***نگاهی به رقابت‌های سایبری در جهان و بن‌بست در گروه کارشناسان دولتی***، قابل دسترسی در: https://tfpsq.net/.
- شعبانی، یحیی (۱۳۹۸). ***حکمرانی فضای سایبری در کشور آلمان***. پژوهشگاه مرکز ملی فضای سایبری- گروه مطالعات فرهنگی و اجتماعی.
- صدیق بنای، هلن (۱۳۸۵). «مفاهیم: فضای سایبر چیست؟»، قابل دسترسی در: https://www.hamshahrionline.ir/news/4411
- عاملی، سعیدرضا (۱۳۹۷). ***الگوی حکمرانی دوفضایی***. تهران: انتشارات امیرکبیر.
- قنبری باغستان، عباس (۱۳۹۸). ***حکمرانی فضای سایبری در کشور مالزی***. تهران: پژوهشگاه

مرکز ملی فضای سایبری- گروه مطالعات فرهنگی و اجتماعی.

- کریمی قهرودی، محمدرضا، و زارعی، وحید (۱۳۹۹). ***حاکمیت فضای سایبری***. تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی و پژوهشگاه فرهنگ و اندیشه‌ی اسلامی.
- کشاورز، حسن، و همکاران. (۱٤۰۱). ***الگوی مشارکت جمهوری اسلامی ایران در نظام حاکمیتی بین‌المللی فضای سایبر***. پایان‌نامه دکتری. تهران: دانشگاه عالی دفاع ملی.
- گوترش، آنتونیو (۲۰۲۱). «متن سخنرانی آنتونیو گوترش، دبیرکل سازمان ملل متحد، در مجمع عمومی سازمان ملل متحد.»
- محمدی، حافظ (۱۳۹۹). «*چالش‌های حکمرانی فضای مجازی و ارائه راهکارها برای جمهوری اسلامی ایران*». دومین همایش ملی حکمرانی اسلامی، ۲۰ آبان.

ب- انگلیسی

- General Assembly (2021). "*Group of Governmental Experts on Advancing Responsible State Behaviour", In* ***Cyberspace in the Context of International Security***. United Nations.
- Henriksen, . (2019). "The end of the road for the UN GGE process: The future regulation of cyberspace", ***Journal of Cybersecurity***, 5 (1), PP. 1-9.
- ICANN. (2023, February 19). ***Bylaws Archives***.
- ITU. (2018). ***Global Cybersecurity Index*** *(v3)*. ITU.
- Ministry of Foreign Affairs, the People's Republic of China. International Strategy of Cooperation on Cyberspace (2017).
- Mueller, M. L. (2019). "Against Sovereignty in Cyberspace", ***International Studies Review,*** 22 (4), PP. 779-801.
- Peace and Freedom. (2023, February 19). Open-ended Working Group on security of and in the use of information and communications technologies (2021-2025).
- Taylor, E., Hoffmann, S. (2019). ***EU–US Relations on Internet Governance***. Chatham House, The Royal Institute of International Affairs.
- UN. (2023, February 19). Open-ended Working Group.