فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹
مقاله اول از صفحات ۴۲-۷

مقاله پژوهشی: ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور (بر اساس نظریه‌پردازی داده‌بنیاد)

مهراب رامک[۱] و علی محمدی[۲]

تاریخ دریافت: ۱۳۹۷/۱۰/۱۰ **تاریخ پذیرش: ۱۳۹۸/۰۵/۰۳**

چکیده

وابستگی روزافزون زیرساخت‌های حیاتی کشور به فضای سایبری (مجازی)، زمینه‌ساز افزایش آسیب‌پذیری ناخواسته کشور در برابر حملات و تهدیدهای سایبری شده است و با مروری بر تهدیدات دفاعی و امنیتی مهم کشور در سال ۱۳۹۷ و پس از آن، تهدید مثلث آمریکا، رژیم صهیونیستی و عربستان سعودی قابل توجه بوده و می‌تواند در فضای سایبر نیز به‌صورت حملات سایبری بروز نماید؛ لذا تقویت دفاع سایبری کشور اجتناب‌ناپذیر خواهد بود و بهره‌گیری از همکاری‌های بین‌المللی می‌تواند نقش مؤثری در این مهم داشته باشد (به دلیل ماهیت فراملی فضای سایبر). پژوهش حاضر، با هدف ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور، ضمن جستجو و شناسایی عوامل اثرگذار در دفاع سایبری کشور، دیدگاه‌های مختلف را در خصوص همکاری بین‌المللی مورد بررسی قرار داده است و با تجزیه‌وتحلیل داده‌های کیفی حاصل، به روش نظریه‌پردازی داده‌بنیاد (گراندد تئوری) در نرم‌افزار مکس کیودا[۳]، ابعاد، مؤلفه‌ها و شاخص‌های قابل توجه را احصاء نموده و ضمن ارزیابی تأثیر آن‌ها بر دفاع سایبری کشور و تجمیع یافته‌ها، مدل مفهومی مورد نظر را ارائه می‌نماید. نتایج نشان می‌دهد که همکاری بین‌المللی می‌تواند در سه بُعد قابلیت بازدارندگی (ثبات نظر، اعتبار، قابلیت و ارتباط)، قابلیت پدافند (پدافند غیرعامل و پدافند عامل) و قابلیت برگشت‌پذیری (مقاومت، قابلیت اطمینان، افزونگی و پاسخ و بازیابی)، در تقویت دفاع سایبری کشور نقش داشته باشد.

کلیدواژه‌ها: مدل مفهومی، همکاری بین‌المللی، دفاع سایبری، نظریه‌پردازی داده‌بنیاد

۱. دانشجوی دکتری مدیریت راهبردی امنیت فضای سایبری- دانشگاه عالی دفاع ملی، M. Ramak@sndu.ac.ir
۲. هیئت‌علمی دانشگاه عالی دفاع ملی، Mohammadi@sndu.ac.ir

3. MaxQDA 2018

مقدمه

هدف کلان کشور در صحنه بین‌الملل را می‌توان دفاع از منافع ملی (هدف‌های عام و ماندگاری که یک ملّت برای دستیابی به آن‌ها تلاش می‌کند) دانست (زمانی و پیری، ۱۳۹۱: ۴۱)؛ لذا، حیطه وسیعی شامل دستیابی به انرژی، منابع مواد خام، فناوری جدید، توسعه اقتصادی، دفاع از اتباع خود در خارج از مرزها و غیره را در خود جای می‌دهد (روشندل، ۱۳۹۴: ۳۸). نظر به اینکه منافع ملّی کشور، هدف‌های اساسی و سیاست خارجی کشور را تعیین می‌کند، منشأ منافع ملی را می‌توان وحدت ملی، قدرت ملی و امنیت ملی و اهداف کلی آن را، تحقق رفاه مردم و ثبات سیاسی کشور، حفظ استقلال و تمامیت ارضی، حفظ و اشاعه ارزش‌های ملی و اعتقادی، اعتبار و پرستیژ در برابر کشورهای دیگر و فراهم آوردن فراغت خاطر در مقابل تهدیدهای احتمالی دانست (ربیعی، ۱۳۹۳: ۱۳۶) که در برنامه‌های پنج‌ساله توسعه اقتصادی، اجتماعی و فرهنگی کشور نیز مورد توجه جدی قرار گرفته‌اند (اسماعیلی و بالایی، ۱۳۹۲: ۴۷).

در یک تعریف مفهومی، فضای سایبر کشور را می‌توان دنیایی شکل‌گرفته در امتداد دنیای واقعی دانست که در آن، افراد از طریق شبکه‌های متعدد، بدون محدودیت زمان و مکان، با یکدیگر در ارتباط بوده و به دادوستد اطلاعات می‌پردازند (غلامحسین‌زاده، ۱۳۹۳) که باید همانند منافع ملی کشور مورد حراست قرار گرفته و از آن دفاع نمود. دانشگاه عالی دفاع ملی، موضوع فوق را طی مطالعه‌ای گروهی با عنوان «طراحی نظام دفاع سایبری کشور و تدوین الزامات تحقق آن» مورد توجه قرار داد (تقی‌پور و همکاران، ۱۳۹۷) و ضمن استخراج مدل مفهومی دفاع سایبری کشور در مقاله‌ای با عنوان «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران» را در زمستان ۱۳۹۷ به چاپ رساند (تقی‌پور و اسماعیلی، ۱۳۹۷) و ۱۲ فرایند را در این خصوص احصاء نمود:

۱) برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هدایت فعالیت‌ها
۲) فرهنگ‌سازی، آموزش، آگاه‌سازی و اطلاع‌رسانی
۳) همکاری و تعاملات بین‌المللی
۴) مشارکت بخش‌های دولتی و خصوصی

۵) بومی‌سازی، استانداردسازی، نوآوری و ایجاد خودکفایی
۶) ایجاد رمزنگاری و امنیت اطلاعات متمرکز
۷) نظارت و ارزیابی
۸) ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری
۹) پیگیری مؤثر قانونی و حقوقی جرائم و حملات سایبری
۱۰) پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری
۱۱) حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری
۱۲) بازیابی و مدیریت بحران

طبق مطالعه گروهی فوق، «همکاری و تعاملات بین‌المللی» می‌تواند در دفاع سایبری کشور ایفای نقش نماید (منظور، همکاری بین‌المللی در مفهوم عام است و قید فضای سایبری برای آن وجود ندارد)؛ لذا پژوهش حاضر، با هدف توسعه نتایج مطالعه فوق، به شناسایی ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی پرداخته و ضمن بررسی تأثیر آن‌ها بر دفاع سایبری کشور، طبق ابعاد، مؤلفه‌ها و شاخص‌های احصاءشده در مطالعه فوق، مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور را ارائه می‌نماید.

بیان مسئله

زیرساخت‌های حیاتی کشور روزبه‌روز وابستگی بیشتری به فضای سایبری (مجازی) برای توسعه فعالیت‌ها پیدا می‌کنند و در ازای آن، زمینه آسیب‌پذیری ناخواسته کشور در برابر حملات و تهدیدهای سایبری افزایش می‌یابد. محور قرار گرفتن فضای اطلاعاتی و سایبری در ساختارهای قدرت ملی (قدرت اقتصادی به زیرساخت‌های سایبری و تعاملات اطلاعاتی، قدرت نظامی به سامانه‌های سایبری آفندی، پدافندی و پشتیبانی، قدرت سیاسی به دانش و آگاهی و توان دستیابی به قدرت نرم، قدرت فرهنگی و اجتماعی به ابزارهای اطلاع‌رسانی رسانه‌ای و سایبری)، اگرچه باعث افزایش چشم‌گیر کارایی، انعطاف‌پذیری، نوآوری و تحول می‌شود اما می‌تواند به نقطه‌ضعف عمده کشور مبدل گردد.

با مروری بر تهدیدات دفاعی و امنیتی مهم کشور در سال ۱۳۹۷، تهدید مثلث آمریکا، رژیم صهیونیستی و عربستان سعودی قابل توجه است (کانون تفکر سیاست خارجی، ۱۳۹۷). در سند جدید استراتژی امنیت ملی آمریکا، ایران به‌عنوان یکی از تهدیدهای مهم در خاورمیانه مطرح شده است. رژیم صهیونیستی، جمهوری اسلامی ایران را به‌عنوان اصلی‌ترین دولت تهدیدکننده امنیت خود می‌داند و رهبران سعودی، جمهوری اسلامی ایران را به‌عنوان مهم‌ترین تهدید نظامی خود مطرح ساخته و به توسعه تنش‌ها و اختلاف‌ها بین دو کشور پرداخته‌اند؛ بنابراین، می‌توان پیش‌بینی کرد، عربستان سعودی تلاش خواهد کرد که با ایجاد تهدیدهای امنیتی مختلف، مانند نفوذ درون ایران و بهره‌گیری از شکاف‌ها و ضعف‌های احتمالی اقتصادی و اجتماعی در ایران، نفوذ ایران را در منطقه کاهش دهد. تهدیدات فوق می‌تواند در فضای سایبر نیز به‌صورت حملات سایبری بروز نماید و برنامه‌ریزی دقیق برای دفاع سایبری در مقابل آن‌ها ضروری است و با نظر به فرامرزی بودن این فضا، بهره‌گیری از همکاری‌های بین‌المللی (توافق‌نامه‌های دوجانبه و چندجانبه و موارد مشابه) می‌تواند نقش به‌سزایی در دفاع داشته باشد؛ لذا لازم است که ضمن شناخت همکاری بین‌المللی (دلایل لزوم همکاری، محیط و منابع مورد نیاز، روابط و منافع اثرگذار، راهبردهای قابل توجه و پیامدهای مورد انتظار)، تأثیر آن بر دفاع سایبری کشور را مورد ارزیابی قرار دهیم که پژوهش حاضر، به این مهم پرداخته و مدل مفهومی مربوطه را ارائه می‌نماید.

اهمیت و ضرورت پژوهش

نظام مقدس جمهوری اسلامی ایران پس از پیروزی انقلاب، به عناوین مختلف مورد هجمه‌های گوناگون قرار گرفته است. جنگ تحمیلی، تحریم‌های اقتصادی و توطئه‌های گوناگون دیگر را می‌توان نمونه بارز این تلاش‌ها برشمرد که در این مدت، مسیر انقلاب را دچار فراز و نشیب‌های زیادی نموده است. با گسترش فضای سایبر و به همان نسبت، آسیب‌پذیری و تهدیدات خاص آن، هجمه‌های فوق به این فضا نیز تسری داده شد و به‌صورت تهدیدات و حملات سایبری بروز نمود و برای مقابله با آن‌ها باید دفاع سایبری کشور تقویت گردد. عوامل متعددی می‌تواند در این امر نقش ایفاء کند که از آن جمله

می‌توان همکاری‌های بین‌المللی را برشمرد و شناخت عوامل اثرگذار مرتبط حائز اهمیت است (مورد توجه پژوهش حاضر است):

- شناخت دلایل لزوم بهره‌گیری از همکاری‌های بین‌المللی برای تقویت دفاع سایبری کشور
- محیط و منابع لازم برای شکل‌گیری همکاری‌های بین‌المللی برای تقویت دفاع سایبری کشور
- روابط و منافع اثرگذار در شکل‌گیری همکاری‌های بین‌المللی برای تقویت دفاع سایبری کشور
- راهبردهای (کنش‌ها و واکنش‌ها) مؤثر در شکل‌گیری همکاری‌های بین‌المللی برای تقویت دفاع سایبری کشور
- پیامدهای همکاری‌های بین‌المللی برای تقویت دفاع سایبری کشور

با توجه به ماهیت فرامرزی فضای سایبر، نتایج پژوهش و مدل مفهومی همکاری بین‌المللی فوق می‌تواند، نگاه کل‌نگرانه‌ای را در دفاع سایبری کشور ایجاد کند و درواقع، نگاه سیستمی را جایگزین نگاه واکنشی محض نماید. در نگاه سیستمی، مقابله با تهدید یا حمله را قبل از وقوع، حین وقوع (حمله) و بعد از آن (بحران) به‌صورت برنامه‌ریزی‌شده در موقعیت زمانی و مکانی دنبال می‌کنیم ولی در نگاه واکنشی، تنها وقتی عمل خواهیم کرد که اتفاقی رخ دهد؛ لذا، با توجه به گسترش سریع فضای سایبر و قریب‌الوقوع بودن تهدیدات و حملات در این فضا، ضرورت ایجاب می‌کند پژوهش‌های گسترده‌ای در همه جوانب دفاع سایبری کشور صورت گیرد که پژوهش حاضر از آن جمله است.

سؤال‌های پژوهش

پژوهش، با هدف اصلی پاسخگویی به این سؤال که «مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور چگونه است؟»، انجام و سؤالات فرعی ذیل را نیز مورد توجه قرار می‌دهد.

۱. ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی کدام‌اند؟
۲. ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور کدام‌اند؟
۳. تأثیر همکاری‌های بین‌المللی بر دفاع سایبری کشور چگونه است؟

مبانی نظری

در این سرفصل، مفاهیم کلیدی پژوهش را مورد بررسی دقیق‌تری قرار می‌دهیم.

همکاری بین‌المللی

معمولاً از واژه همکاری[1] (استفاده از منابع و اطلاعات طرفین همکاری برای تحقق هدف همدیگر)، هماهنگی[2] (فعالیت گروهی برای اجرای طرح مشخص بدون خلق چیزی جدید) و مشارکت[3] (کار کردن با یکدیگر برای خلق و ایجاد چیزی جدید با داشتن یک دیدگاه و هدف مشترک به‌صورت غیر فردی) برای توصیف کار گروهی استفاده می‌شود؛ اما معنای آن‌ها یکسان نیست و استفاده از این کلمات به‌جای یکدیگر، معنای آن‌ها را کم کرده و پتانسیل آن‌ها را برای ایجاد فضای کاری قدرتمند کاهش می‌دهد (Lyn Stoner, 2013). مشارکت، بستر خلاقیت و نوآوری در سازمان است لذا، همکاری را باید با مفهوم ایجاد مشارکت مؤثر مورد توجه قرار داد (Lukas & Andrews, 2006: 1). از دیدگاه اسلام، همکاری بین کشورهای مسلمان و غیرمسلمان باید بر مبنای نگاه تکریم‌آمیز به انسان‌ها، همزیستی مسالمت‌آمیز، نفی اساس خشونت، پایبندی به اصول اخلاقی و عهد، گفت‌وگو، مقابله‌به‌مثل و تجهیز قوا با هدف بازدارندگی شکل گیرد (علیخانی، ۱۳۹۰: ۱۳) و خداوند در قرآن کریم نیز، رعایت اصل برقراری ارتباط با گفتار حسن (آیه ۶۴ سوره آل‌عمران)، اصل برقراری ارتباط با تأکید بر مشترکات (آیه ۶۴ سوره آل‌عمران)، اصل برقراری ارتباط با گفتار نرم و لین (آیه ۴۴ سوره طه)، اصل وفای به پیمان‌های سیاسی در روابط بین‌الملل (آیه ۱ سوره المائده)،

1.Cooperation
2.Coordination
3.Collaboration

اصل عدم اهانت به ارزش‌های ملل دیگر (آیه ۱۰۸ سوره الأنعام)، اصل ایجاد ارتباط بر اساس صلح (آیه ۲۰۸ سوره البقره)، اصل ایجاد روابط دیپلماسی همراه با حکمت و برهان (آیه ۱۲۵ سوره النحل) و اصل برقراری ارتباط بر اساس عزت اسلام (آیه ۱۴۱ سوره النساء) را لازم دانسته است. حضرت امام خمینی (ره)، رعایت ویژگی اخلاق، حفظ صلح و امنیت بین‌المللی، عدم تجاوز به خاک کشورها، حسن هم‌جواری با همسایگان و همکاری با دولت‌ها بر مبنای احترام متقابل (غفرانی، ۱۳۹۱: ۲) و مقام معظم رهبری (مدظله‌العالی)، انطباق با جهان‌بینی توحیدی و آموزه‌های اسلامی و تعاملات انسانی در سطح فردی، جمعی و جهانی[1] را برای همکاری بین‌المللی 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 یکدیگر شکل می‌گیرد و ضرورت دارد که عوامل متعددی مورد توجه قرار گیرند تا با مشارکت مؤثر طرفین، یک همکاری اثربخش شکل گرفته و منافع ذی‌نفعان تأمین شود.

دولت‌ها، سازمان‌ها و نهادهایی که جامعه بین‌المللی را تشکیل می‌دهند، دارای روابط و مناسبات سیاسی، اقتصادی و فرهنگی هستند که بیانگر روابط متقابل آن‌ها است و می‌تواند به‌صورت روابط دوستانه (مشارکت)، رقابتی و تعارض‌آمیز (ستیز یا مناقشه) باشد (جمالی، ۱۳۸۲: ۲۰۹). با توجه به موارد فوق، همکاری بین‌المللی را می‌توان، مشارکت بین‌المللی مؤثر و روابط بین‌المللی دوستانه (مشارکت) دانست و مفهوم آن را در دیدگاه‌های مختلف روابط بین‌الملل و نظریه‌های بین‌المللی جستجو نمود (۰).

---

۱. دیدار با دانش‌آموزان و دانشجویان در آستانه سیزده آبان و روز ملی مبارزه با استکبار جهانی ۱۳۷۵/۸/۹

جدول (۲-۱): مفهوم همکاری بین‌المللی از دیدگاه‌های مختلف روابط بین‌الملل و نظریه‌های بین‌المللی

دیدگاه	مختصری از نظرات در خصوص همکاری بین‌المللی
لیبرالیسم	در روابط بین‌الملل، سه جریان عمده، وابستگی متقابل میان کشورها (به‌ویژه اقتصادی)، ظهور یک سلسله هنجارها و قواعد بین‌المللی و جریان دموکراسی شدن بین‌المللی (موجب کاهش منازعه و افزایش همکاری) را عامل همکاری کشورها می‌دانند (یوسفی، ۱۳۸۲: ۲۳) و اعتقاد دارند که انسان‌ها، قابلیت یادگیری داشته و تعلیم‌پذیرند و باید رفتار و عملکرد ناهنجار و غیراخلاقی خود را بر اساس موازین اخلاقی و انسانی تغییر دهند(کلومبیس و ولف، ۱۳۷۵: ۵۱).
لیبرالیسم (رویکرد ارتباطات)	معتقدند که ارتباطات، سه اثر مهمِ هماهنگی مطمئن بین تلاش‌ها و انتظار انسان‌ها برای اهداف جامعه، ارتقاء سطح همکاری و محدود نشدن به سطوح تهدید را بر روابط بین‌الملل دارند(دویچ، ۱۳۷۵: ۸۳۲) و ارتباطات بین‌المللی به مذاکرات بین‌المللی، مذاکرات بین‌المللی به همکاری بین‌المللی و همکاری بین‌المللی به همگرایی بین‌المللی می‌انجامد.
لیبرالیسم (نظریه کارکردگرایی)	کارکردگرایی با نام «دیوید میترانی[1]» در پیوند است و از دید وی، ریشه‌های همکاری بین‌المللی در قلمروی وابستگی متقابل کارکردی بوده و همکاری میان دولت‌ها به علت مشکلات فنی فراوان و عدم توانایی سیاستمداران برای حل آن‌ها، اجتناب‌ناپذیر است(عبدالله خانی، ۱۳۸۳: ۱۲۳) و بر این اساس، دولت‌ها وارد همکاری می‌شوند و نهادهایی شکل داده و اقتدار خود را در این حوزه‌ها به این نهادها انتقال می‌دهند(مشیرزاده، ۱۳۹۴: ۶۰).
لیبرالیسم (نظریه نوکارکرگرایی)[2]	موضوعات مربوط به رفاه و راهکار خارجی و دفاعی برای کنشگران را برجسته‌تر دانسته (همان، ص ۱۶۵) و هر اقدامی برای همکاری در یک بخش را مستلزم همکاری در بخش‌های دیگر می‌دانند و معتقدند همکاری از یک بخش به بخشی دیگر سرریز می‌کند. عکس آن را نیز صحیح می‌دانند، یعنی بروز مشکل در یک بخش می‌تواند همکاری در بخش‌های دیگر را نیز مختل کند (همان، ص ۶۳).
لیبرالیسم (نظریه صلح دموکراتیک)	اعتقاددارند، چشم‌اندازهای همکاری اقتصادی و سیاسی و حفظ آن در میان دموکراسی‌های توسعه‌یافته، قوی‌تر است، چراکه این دولت‌ها گسترده‌ترین دامنه منافع مشترک سیاسی، نظامی و اقتصادی رادارند (مستقیمی، ۱۳۸۵، ص ۳۷۵). از دیدگاه این نظریه، برای دستیابی به صلح و ثبات، باید نظام‌های سیاسی لیبرال دموکراتیک ایجاد کرد زیرا به‌ندرت در بین آن‌ها جنگ رخ خواهد داد(فیروزآبادی، ۱۳۸۱: ۹۵).
نو لیبرالیسم	نظام بین‌الملل را آنارشیک و فاقد یک مرجع و اقتدار مرکزی می‌دانند و به وجود عنصر ناسازگاری و درگیری در همکاری اعتقاد دارند و آن را بخش جدایی‌ناپذیر عملکرد دولت‌ها می‌دانند(عسگرخانی، ۱۳۸۳: ۴۴). بزرگ‌ترین مانع همکاری را مسئله تقلب دیگران می‌دانند و معتقدند که با اتخاذ راهبردهای تعامل بین کشورها و پیوند موضوعی از یک طرف و تأسیس نهادها و رژیم‌های بین‌الملل از طرف دیگر، می‌توان بر مشکل فریب‌کاری و عهدشکنی غلبه کرد(مشیرزاده، ۱۳۹۴: ۶۶) و علی‌القاعده، افزایش در وابستگی متقابل باعث تقویت این تأثیر می‌شود(ونت، ۱۳۸۴: ۵۰۳).

1.David Mitrany
2. Neofunctionalism

دیدگاه	مختصری از نظرات در خصوص همکاری بین‌المللی
نظریه رژیم‌های بین‌المللی	رژیم‌های بین‌المللی را مجموعه‌ای از اصول، قواعد، هنجار و رویه‌های تصمیم‌گیری می‌دانند(Krasner, 1983: 2) که با تقسیم هزینه‌ها و تسهیل دیپلماسی بین دولت‌ها، ایجاد نظم نموده(عسگرخانی، ۱۳۸۳: ۷۴) باعث کاهش عدم اطمینان و عدم قطعیت[1] در نظام بین‌الملل شده(مشیرزاده، ۱۳۹۴: ۶۸) و دولت‌ها را وادار به اعتمادسازی و امنیت‌سازی می نماید(عسگرخانی، ۱۳۸۳: ۴۴).
رئالیسم	خشونت و منازعه را امری غریزی در سرشت انسان و قدرت‌طلبی در روابط بین‌الملل را امری طبیعی می‌دانند و معتقدند تأمین آن، حتی با توسل به زور و جنگ نیز جایز است(فیروزآبادی، ۱۳۸۱: ۸۷) زیرا، دولت‌ها تنها به‌وسیله قدرت می‌توانند از خود محافظت کرده و رفاه اتباع خود را ارتقاء بخشند(دویچ، ۱۳۷۵: ۲۴۴) و با افزایش وابستگی متقابل، کشورها در مقابل یکدیگر آسیب‌پذیرتر می‌شوند و احساس عدم امنیت به وجود می‌آید (مستقیمی، ۱۳۸۵: ۶۰) و دو عامل عمده ملاحظات مربوط به دستاوردهای نسبی و نگرانی از فریب در چشم‌انداز رئالیست‌ها مانع همکاری می‌شود (Lynn-Jones, 1995: 660).
نورئالیسم	معتقدند که نظام بین‌الملل آنارشیک بوده و یک اقتدار مرکزی در نظام بین‌الملل وجود ندارد و این امر، سه الگوی رفتاری، بی‌اعتماد و سوءظن، تضمین بقا و ادامه حیات و تلاش برای به حداکثر رساندن قدرت نسبی در روابط بین‌الملل ایجاد می‌کند(فیروزآبادی، ۱۳۸۱: ۹۹) و باعث می‌شود که کشورها، از ترس استثمار شدن در آغاز و ادامه همکاری با کشورهای دیگر، محتاط بوده و سودهای اقتصادی را تابع منافع سیاسی قرار دهند و دولت‌ها به دنبال حفظ خودمختاری‌شان باشند (Neuss, 2007: 107).
مکتب انگلیسی	اصل بنیادین سیاست جهانی را قواعد دانسته و قواعد همزیستی (شرایط حداقل برای همزیستی) را مقدم بر قواعد همکاری می‌دانند(مشیرزاده، ۱۳۹۴: ۱۴۴) و معتقدند، هر نظمی در نظام بین‌الملل ناشی از عوامل مادی است (نه فرهنگی)(ونت، ۱۳۸۴: ۳۶۸) و نهادهای بین‌المللی، ابزاری برای برقراری و تداوم بخشیدن به همکاری میان دولت‌ها در انجام کارکردهای سیاسی هستند(مشیرزاده، ۱۳۸۳: ۵۹۳).
مارکسیسم	سطح حقیقی تحلیل مارکسیست‌ها را می‌توان نظام جهانی سلطه و وابستگی دانست. معتقدند که کشورهای سرمایه‌داری مدرن، ضرورتاً در منازعه و مناقشه با یکدیگرند تا قلمروهای اقتصادی خود را گسترش دهند. اقتصاد را زیربنا و سایر پدیده‌های اجتماعی را روبنای آن تصور نموده و کمتر به مناسبات میان دولت‌ها و بیشتر به جهان‌گیر شدن مناسبات اقتصادی و اجتماعی توجه دارند(طیب، ۱۳۹۵: ۳) و طبق نظریه مارکسیستی ارتدوکسی[2]، سرمایه‌داری را علت بنیادی و اساسی تعارض و کشمکش در عرصه بین‌المللی می‌دانند(ام. والت و مهدویان، ۱۳۸۵).
نظریه	به دلیل گرفتار شدن در بحث‌های فرانظری هستی‌شناختی و معرفت‌شناختی، لزوم تلاش برای

1.Uncertainty
2.Orthodox Marxist Theory

دیدگاه	مختصری از نظرات در خصوص همکاری بین‌المللی
انتقادی	تبیین روابط بین‌الملل بی‌توجه است (مشیرزاده، ۱۳۹۴: ۲۲۹، ۲۴۹) و ضمن تلاش برای تضعیف گفتمان امنیتی سلطه‌جویانه، خواهان نظامی هستند که از طریق ارتباطات متقابل و نیرومند هدایت شود و در آن مفاهیمی مانند حقوق و تعهدات (به‌عنوان عوامل زمینه‌ساز همکاری) جایگزین قدرت و زور شده باشد (عبدالله خانی، ۱۳۸۳: ۲۴۰–۲۳۸).
فمینیسم	معتقدند، در رشته روابط بین‌الملل آگاهی جنسیتی وجود ندارد و در عمل باید، مشارکت زنان در تمام جنبه‌های روابط خارجی بیشتر شود و تحلیل روابط بین‌الملل نسبت به جنسیت به‌عنوان برساخته‌ای اجتماعی حساس باشد و درواقع، زمانی که جهان حقیقتاً مادرسالارانه باشد، کمتر مستعد درگیری است و نسبت به جهانی که اکنون ساکن آن هستیم، بیشتر مسالمت‌جویانه و در پی همکاری است(مشیرزاده، ۱۳۹۴: ۳۰۷).
سازه‌انگاری	سیاست بین‌الملل را بر اساس یک هستی‌شناختی رابطه‌ای می‌بینند و به عوامل فکری مانند فرهنگ، هنجارها و انگاره‌ها بهاء می‌دهند (ونت، ۱۳۸۵: ۶۳) و به سه گزاره، اهمیت ساختارهای هنجاری یا عقیدتی به‌اندازه ساختارهای مادی، هویت بازیگران در ساختارهای غیرمادی و ایجاد عوامل و ساختارها متقابل، تأکید دارند (کلومبیس و ولف، ۱۳۷۵: ۵۳–۵۱) و معتقدند با ایجاد هنجارهای مشترک، کشورها با یکدیگر همکاری خواهند کرد و جهان سیاست، صلح‌آمیزتر خواهد شد (Mearsheimer, 1994, pp. 10-12) و فرهنگ هم می‌تواند به تعارض یا همکاری قوام بخشد (ونت، ۱۳۸۴: ۳۶۶).
پست مدرنیسم	تلاش دارند تا نشان دهند که هویت خودی از طریق اعمال دیگران شکل می‌گیرد و در شکل‌گیری آن نیز، زبان را مهم دانسته (عبدالله خانی، ۱۳۸۳: ۲۱۶) و به پنج گزاره، نفی پایان تاریخ بودن مدرنیسم، انتخابی بودن و برساخته بودن هر آنچه هست، نقش باورها و رفتارها به‌عنوان خالق واقعیت‌ها، رها نبودن تحقیق علمی از ارزش‌ها و نقش زبان و چارچوب‌های مفهومی در خلق شیوه‌های زندگی و قائل شدن فرآیند هویت‌یابی و برساخته شدن هویت به‌عنوان شکلی از قدرت، تأکید دارند (مشیرزاده، ۱۳۹۴، صص ۲۶۹–۲۶۷).

حملات سایبری

در یک تعریف مفهومی، فضای سایبر را می‌توان دنیایی شکل‌گرفته در امتداد دنیای واقعی دانست که در آن، افراد از طریق شبکه‌های متعدد، بدون محدودیت زمان و مکان، با یکدیگر در ارتباط بوده و به دادوستد اطلاعات می‌پردازند (غلامحسین‌زاده، ۱۳۹۳). وزارت دفاع آمریکا، فضای سایبری را «یک دامنه سرتاسری[1] در محیط اطلاعاتی؛ شامل

1.Global Domain

شبکه‌های مرتبط به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، دستگاه‌های کامپیوتری، پردازنده‌ها و کنترل‌گرهای توکار[1]»، تعریف نموده است (Joint Publication, 2016: 58) ، ولی بهترین تعریف را می‌توان تعریف مشترک آمریکا و روسیه؛ یعنی «یک رسانه الکترونیکی که از طریق آن اطلاعات تولیدشده، منتقل‌شده، دریافت‌شده، ذخیره‌شده، پردازش‌شده یا حذف می‌شوند»، دانست (Godwin, Kulpin, Rauscher, & Yaschenko, 2014: 17) و به زبان ساده می‌توان گفت: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوهای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود، به‌گونه‌ای زنده و مستقیم در آن روی می‌دهد» (قادری حاجت و نصرتی، ۱۳۹۱: ۹۱). فضای سایبر جمهوری اسلامی ایران را نیز می‌توان، مجموعه‌ای از ارزش‌ها، منافع و دارایی‌های ملّی در راستای اهداف جمهوری اسلامی ایران دانست که محدود به مرزهای جغرافیایی نیست. از منظر ژئوپلیتیک می‌توان ویژگی‌های مدیریت و کنترل، هویت، هم‌گرایی و همکاری، رقابت و ستیز، شکاف توسعه، تولید قدرت، حاکمیتی ملی را برای فضای مجازی برشمرد (حافظ‌نیا، ۱۳۹۰: ۴).

سرمایه‌های ملی سایبری کشور در فضای مجازی، در دو گروه دارایی مادی (زیرساخت، سازه و سامانه‌های سایبری، محتوا، داده و اطلاعات سایبری) و معنوی (فردی و جمعی/ملی) دسته‌بندی می‌شوند که می‌توانند به یک شخص، گروه و یا کل جامعه تعلق داشته باشند (جلالی فراهانی، ۱۳۹۰: ۳۸). هرگونه ضعف و نقص در رویه‌های امنیتی، آسیب‌پذیری‌هایی را به وجود می‌آورد (آسیب‌پذیری سایبری) و زمینه‌ساز حملاتی همچون دسترسی غیرمجاز، تخریب، افشاء، تغییر اطلاعات، اختلال، ممانعت از ارائه سرویس و غیره خواهد شد و مهاجمین نیز از آن طریق، سرمایه‌های ملی سایبری کشور را مورد تهاجم قرار می‌دهند (حمله سایبری)(کمیته دائمی پدافند غیرعامل کشور، ۱۳۹۴: ۱).

جهان در دهه آتی با تغییرات فوق‌العاده‌ای در رشد عناصر مشترک روبه‌رو خواهد بود. یکی از این عناصر مشترک، فضای سایبری است و معنای این رشد، کاربران بیشتر،

1. Embedded Processors and Controllers

تجهیزات بیشتر، اتصال بیشتر و اطلاعات بیشتر خواهد بود. شرکت مایکروسافت در سال ۲۰۱۴، آینده‌پژوهی خود را با عنوان «فضای سایبری ۲۰۲۵، تصمیم‌گیری‌های امروز، زمینه‌ساز آینده»[1] منتشر نمود و در آن، تغییرات جهان آنلاین، فرصت‌های ناشی از همکاری و نوآوری و غیره را بیان و مجموعه‌ای از سناریوها و چارچوب‌ها را جهت ارزیابی تصمیم سیاست‌گذاران، رهبران کسب‌وکار و سایر تصمیم‌سازان ارائه کرد (Burt, Kleiner, Nicholas, & Sullivan, 2014). مرکز ملی فضای مجازی کشور نیز، ضمن مبنا قرار دادن آینده‌پژوهی فوق، گزارشی با عنوان «فضای مجازی ۲۰۲۵» در سال ۱۳۹۶ منتشر نمود (مرکز ملی فضای مجازی، ۱۳۹۶). طبق مستندات فوق تا سال ۲۰۲۵، بیش از ۹۱ درصد مردم کشورهای توسعه‌یافته و نزدیک به ۷۵ درصد اقتصادهای نوظهور از اینترنت استفاده خواهند کرد و وابستگی به اینترنت نه‌فقط یک مفهوم بلکه، واقعیتی جدید خواهد بود. پیش‌بینی تهدیدات سایبری سال ۲۰۱۹ توسط شرکت‌ها و صاحب‌نظران امنیت سایبری را نیز باید مورد توجه قرار داد (۰):

جدول (۲-۲): مهم‌ترین تهدیدات سایبری سال ۲۰۱۹ در پیش‌بینی‌های انجام‌شده توسط شرکت‌ها و صاحب‌نظران امنیت سایبری

شرکت و مؤسسه	پیش‌بینی مهم‌ترین تهدیدات سایبری سال ۲۰۱۹	مرجع
Symantec	– افزایش بهره‌برداری از شبکه اینترنت نسل پنجم (5G) و سرعت بالای انتقال داده در آن – استفاده از اینترنت اشیاء در زیرساخت حیاتی، موجب حملات مخرب در انرژی و نظام بانکی	(هواشناس، ۱۳۹۷)
McAfee	– تمرکز و مشارکت در فعالیت‌های زیرزمینی سایبری و گسترش اقتصاد بازار انحصاری. – حمله استخراج پنهانی داده‌ها[2] از فضای ابری و تلاش برای اخاذی در رقابت بین برندها	(McAfee Labs, 2018)

1.Cyberspace2025 Today’s decisions, Tomorrow’s Terrain, navigating the future of cybersecurity policy

2.Data Exfiltration Attacks

شرکت و مؤسسه	پیش‌بینی مهم‌ترین تهدیدات سایبری سال ۲۰۱۹	مرجع
Kaspersky	– بروز تهدیدهای قدیمی توسعه‌یافته (حلقه‌های منفی) توسط خودکارسازی و هوش مصنوعی – بروز برخوردهای تلافی‌جویانه عمومی (دست‌کم گرفتن سطح تهدیدات عمومی)	(Diaz, 2018)
AT&T	– خودکارشده فرایند امنیت سایبری و بحران استعدادهای امنیت سایبری – دستگاه‌های تلفن همراه به‌عنوان تهدید سایبری و سرقت رمزها	(AT&T Business Editorial Team, 2019)
IBM	– ارتباطات به‌طور فزاینده‌ای گسترش خواهد یافت – گسترش هوش مصنوعی کوانتومی و افزایش اعتماد به هوش مصنوعی	(Barlow, 2018)
RSA Security	– گسترش ابزارهای امنیتی پیچیده مبتنی بر هوش مصنوعی و گسترش تهدید باج‌افزارها – استقرار نهایی ابزار پیشرفته پیشگیری از نفوذ و عدم توجه به ضرورت اخذ پشتیبان اطلاعات	(RSA Security, 2019)
Trend Micro	– افزایش حجم و پیچیدگی تهدیدات و حملات سایبری، با تکیه بر آسیب‌پذیری‌ها – هماهنگ‌سازی فرایندهای فناوری اطلاعات، باید مورد توجه قرار گیرد	(اخبار رسمی، ۱۳۹۷) (Trend Micro, 2019)
Sophos	– بدافزارها در صدر تهدیدات سایبری و افزایش احتمال به خطر افتادن امنیت اینترنت اشیاء – تهدید رو به رشد و مداوم نرم‌افزارهای مخرب تلفن همراه بر اثر کمپین‌های مخرب غیرمعمول	(Sophos, 2019)
Nuvias Group	– افزایش جرائم سایبری، جاسوسی و خرابکاری از سوی کشورها – ناامنی فناوری ابری و اینترنت اشیاء توسط بدافزار و رمزهای عبور ضعیف	(فراست، ۱۳۹۷)
Tech Native	– تهدید باج افزارها، اینترنت اشیاء و افزایش حملات سایبری به سیستم‌عامل مکینتاش – گسترش تهدیدات نامرئی[1] و ضرورت مبارزه با آن‌ها (دخالت در رقابت‌های انتخاباتی اروپا)	(Arsene, 2018)

1.Invisible Threats

شرکت و مؤسسه	پیش‌بینی مهم‌ترین تهدیدات سایبری سال ۲۰۱۹	مرجع
CSO staff	– فناوری‌های تهاجمی و دفاعی گسترش یافته و دامنه و پیچیدگی حملات افزایش خواهد یافت – حملات فیشینگ گسترش خواهد یافت. باج‌افزارها، پنهان ولی ویران‌کننده‌اند	(CSO staff, 2018)
Forbes Technology Council	– رخداد جنگ سایبری در بین ملل و افزایش حملات سایبری به زنجیره‌های تأمین – سازمان‌های امنیتی، هدف اول برای مهاجمان سایبری خواهند بود	(NeSmith, 2018)
MIT Technology Review	– حملات و دفاع مبتنی بر هوش مصنوعی و حمله از طریق ابررایانه – هک کردن قراردادهای هوشمند و شکستن رمزگذاری‌ها توسط رایانه‌های کوانتومی	(Giles, 2019)
FireEye	– ضعف در زنجیره تأمین و گسترش جرائم و سایر تهدیدهای مرتبط با صنعت هوایی – ادامه نقص‌های فقدان هویت و مسئولیت‌پذیری و گسترش توجه مهاجمان به فضای ابری	(Greenberg, 2018)
Forcepoint	– ایجاد اختلال در اینترنت اشیاء صنعتی در مقیاس بزرگ و سرقت مشخصات چهره کاربران – افزایش استفاده از سایبر برای ایجاد اختلال در دولت، زیرساخت‌های حیاتی و صنایع حیاتی	(Raffael, 2018)
Beyond Trust	– تمرکز سیستم‌های کنترل صنعتی و افزایش استفاده از هوش مصنوعی در حملات سایبری – زنجیره‌های تأمین در خطر بوده و حمله به آسیب‌پذیری‌های آشکار و پنهان ادامه خواهد داشت	(Bradshaw, 2018)
Barracuda MSP	– افزایش حملات سایبری به فضای ابری افزایش داشته و تهدید امنیت ایمیل ادامه می‌یابد – دولت‌ها، برای کمک به امنیت فضای ابری، به بخش خصوصی توجه خواهند کرد	(Barracuda MSP, 2018)
kaliboys (گروه ایرانی)	– تهدید مؤسسات مالی و شبکه شرکت‌ها و آسیب‌پذیری بیشتر سیستم‌های دیجیتال – ادغام مجرمان سایبری و تهدید شبکه‌های تلفن همراه و دستگاه‌های کنترل صنعتی	(وفایی، ۱۳۹۸)

به گزارش انتخاب، بسیاری از درگیری‌های بین‌المللی سال ۲۰۱۹ می‌تواند تابعی از حملات سایبری سال ۲۰۱۸ باشند (انتخاب، ۱۳۹۷). پژوهشگران مؤسسه سوفوس معتقدند، باج‌افزارها شاخص‌ترین و گسترده‌ترین حملات سایبری سال ۲۰۱۸ بوده و مجرمین توانسته‌اند با استفاده از باج‌افزارهایی همچون WannaCry،Dharma و SamSam، میلیون‌ها دلار به سرقت ببرند و موفقیت‌های مالی آن‌ها، احتمال ادامه این نوع حملات در سال ۲۰۱۹ را بیشتر خواهد کرد (Sophos, 2019). از دیدگاه مک‌آفی، اگرچه در سال ۲۰۱۸ شاهد ظهور باج‌افزارهایی همچون GandCrab و SamSam بوده‌ایم ولی بازهم باید خوشحال باشیم که فضای سایبری هنوز در تسلط کامل باج‌افزارها قرار نگرفته است (McAfee Labs, 2018).

نشریه بین‌المللی تجارت «اکونومیست»، جنگ تجاری چین و آمریکا، رکود اقتصاد جهانی، پیامدهای خروج بریتانیا از اتحادیه اروپا، تحریم‌ها علیه ایران و تهدیدات سایبری را، پنج تهدید کلیدی برای اقتصاد جهانی در سال ۲۰۱۹ برشمرده است (خاک‌پور، ۱۳۹۷) و در میان تهدیدات و حملات امنیتی نوظهور علیه نظام مقدس جمهوری اسلامی ایران، دو حمله تروریسم سایبری و نقض حقوق بشر قابل توجه بیشتری است (علیزاده و موسوی، ۱۳۹۴: ۱۶)؛ لذا، توجه به حملات سایبری و اتخاذ تمهیدات دفاعی در مقابل آن‌ها، از اهمیت بالایی برخوردار است.

دفاع سایبری

دفاع، در لغت‌نامه معین، از دستبرد دشمن حفظ کردن، بازداشتن، پس زدن (معین، ۱۳۸۲: ۵۳۰) و در لغت‌نامه دهخدا، دور کردن از کسی، دفع کردن از کسی، یاوری و حمایت کردن کسی از دستبرد دشمن (دهخدا، ۱۳۷۷: ۱۰۹۴۰) معنی شده است. در قرآن کریم، بارها به رعایت عدالت و عدم تجاوز از حدود معقول و انسانی در مقابل دشمنان تأکید شده است (سوره بقره: آیه ۱۹۰). حضرت امام خمینی(ره)، در باب دفاع همه‌جانبه فرمودند: «اگر بر کشوری ندای دل‌نشین تفکر بسیجی طنین اندازد، چشم طمع دشمنان و جهان‌خواران از آن دور خواهد گردید و

الا هر لحظه باید منتظر حادثه باشیم»[۱]. حضرت امام خامنه‌ای(مدظله‌العالی) فرموده‌اند، «دفاع یک وظیفه عقلی، انسانی و اسلامی است. پس باید آماده بود. روزبه‌روز باید آمادگی‌تان را بیشتر کنید و آموزش‌ها را پیش ببرید، سازمان‌دهی منظم مبتنی بر حفظ انضباط کامل و رعایت مقررات است»[۲].

در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل گرفته است. سهم درآمد حاصل از کسب‌وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیر یافته و از میان شاخص‌های تعیین‌شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. به‌عبارت‌دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، به‌طور مستقیم زندگی شهروندان را به مخاطره خواهد انداخت. جنگ سایبری (رایاجنگ یا نبرد مجازی)، به‌نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در فضای سایبری جاری سازند. عصر اطلاعات و زیرساخت‌های آن‌ها مصادیق جنگ و دفاع را دستخوش تغییر نموده است؛ یعنی، اگر قائل باشیم که زمین، دریا و هوا سه بعُد جنگ زمینی، دریایی و هوایی و جنگ‌های فضایی بُعد چهارم جنگ است، بدین منوال جنگ‌های سایبری نیز بُعد پنجم جنگ می‌توانند در نظر گرفته شوند (ایمانی، ۱۳۹۰: ۳۰۰).

---

۱. صحیفه نور، ج ۲۱، ۵۲

۲. دیدار با کارکنان نهاجا در روز نیروی هوایی – ۱۳۶۹/۱۱/۱۹

دفاع سایبری یک سامانه یکپارچه برای پیاده‌سازی همه اقدامات مرتبط با فناوری اطلاعات و ارتباطات و امنیت اطلاعات، قابلیت‌های گروه پاسخگویی حوادث رایانه‌ای[1] و عملیات شبکه‌ای رایانه‌ای[2]، همچنین پشتیبانی از قابلیت‌های فیزیکی نظامی (Grafik, 2013: 21) شامل بخش‌های محافظت، کشف، پاسخ و بازیابی است (ACST–Strategy-CyberSecurity, 2014: 18). نقاط ضعف اصلی دفاع سایبر را می‌توان بررسی هویت و مکان مهاجم، شناسایی نیت مهاجم، تشخیص حمله‌های از قبل طراحی‌شده، بررسی و ارزیابی تلفات بعد از حادثه یا جنگ، برشمرد (ویکی‌پدیا، دانشنامه آزاد، ۲۰۱۸). برای داشتن دفاع سایبری همه‌جانبه و یکپارچه در سراسر کشور، بایستی چهار دسته توانمندی‌ها راهبردی، علمی، فناورانه و عملیاتی را در کشور تولید کرده و یا تقویت نماییم (اسکندری، ۱۳۹۳: ۸۵). به‌طورکلی، هر اقدام مجرمانه در فضای سایبری، مجموعه اعمالی است که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای سایبری انجام شده و ابتدا، عملیات شناسایی و پویش سامانه هدف انجام شده و سپس تلاش برای دسترسی به سامانه صورت می‌گیرد. سپس ارتقاء حقوق دسترسی جهت دست یافتن به اهداف مورد نظر انجام و توسط آن، صدمه، سرقت اطلاعات یا هر اقدام مجرمانه دیگر انجام می‌شود (حتی نصب هر ابزار لازم دیگری برای حفظ دسترسی به سامانه در آینده). درنهایت نیز ضمن انجام مخفی‌کاری لازم برای عدم به‌جا ماندن ردپا و آثار جرم یا حمله، یورش مورد نظر به سامانه انجام شده و به تثبیت مواضع در سامانه هدف پرداخته می‌شود (حسینی و ظریف‌منش، ۱۳۹۲: ۴۸).

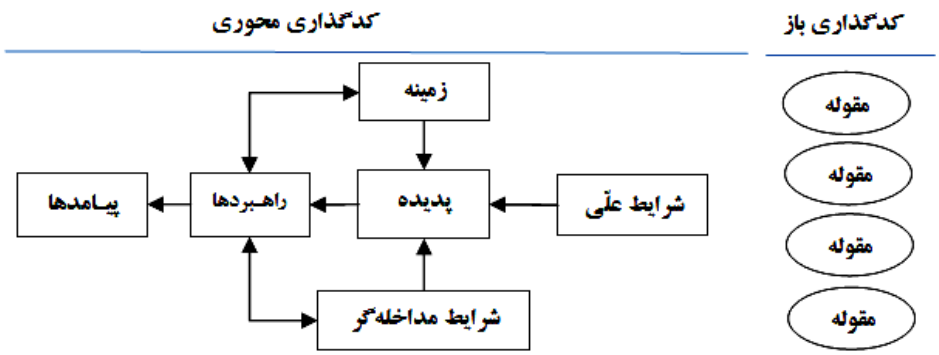
روش‌شناسی تحقیق

در پژوهش توسعه‌ای حاضر، ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی از طریق جمع‌بندی مبانی نظری جمع‌آوری و مطالعه شده و احصاء و تأثیر آن‌ها بر تقویت دفاع سایبری کشور (ابعاد، مؤلفه‌ها و شاخص‌های احصاءشده در مقاله پژوهشی دیگر) بررسی و

1. CERT
2. CNO: Computer network operation

مدل مفهومی مربوطه ترسیم می‌گردد. روش‌های متعددی برای بررسی داده‌های کیفی (کلیه مفاهیم استخراج‌شده از مستندات و مبانی نظری که با معیارهای کمی و عددی قابل بررسی نیست) وجود دارد که بسته به نوع تحقیق و موردکاوی مربوطه، از هر یک از آن‌ها استفاده می‌شود (حاجیلو، ۱۳۸۳: ۵۶) و یکی از مهم‌ترین آن‌ها، گراندد تئوری یا نظریه‌پردازی داده‌بنیاد[1] است (پدیده را از پنج محور یا بُعد مورد شناسایی قرار می‌دهد)، انطباق بیشتری با مطالبات پژوهش حاضر دارد. در پژوهش حاضر، به پیشنهاد اشتراوس و کوربین در کتاب «کشف نظریه داده بنیاد» (۱۹۶۷)، سه فن کدگذاری باز، کدگذاری محوری (شرایط علّی[2]، زمینه[3]، پدیده یا مقوله‌محوری[4]، شرایط مداخله‌گر[5]، راهبردها[6] و پیامدها[7]) و کدگذاری انتخابی (مرادی، ۱۳۹۵) توسط نرم‌افزار مکس کیودا ۲۰۱۸ (آنالتیک پرو[8]) مورد استفاده قرار می‌گیرد. طبق روش فوق، کلیه مستندات پژوهش در نرم‌افزار مکس کیودا درج و ضمن مطالعه، مفاهیم قابل توجه استخراج و کدگذاری می‌شود (کدگذاری باز) و با دسته‌بندی کدهای مرتبط و کدگذاری کلان‌تر آن‌ها در چندین مرحله، مقوله‌های به‌دست‌آمده، در محورهای شرایط علّی، زمینه، شرایط مداخله‌گر، راهبردها و پیامدها، شکل (۳-۲) ساماندهی می‌شود (کدگذاری محوری) و با سناریوپردازی و تفسیر نتایج، مدل مفهومی مورد نظر استخراج می‌گردد (کدگذاری انتخابی).

1.Grounded Theory
2.Causal Conditions
3.Context
4.Core Category or Phenomenon
5.Intervening Conditions
6.Strategies
7.Consequences
8.MAXQDA 2018 Analytics Pro



شکل (۳-۲): کدگذاری محوری (Creswell, 2013: 428)

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

در این مرحله، با تجزیه‌وتحلیل یافته‌ها باید ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی و دفاع سایبری را شناسایی نماییم تا درنهایت، تأثیر همکاری بین‌المللی در تقویت دفاع سایبری احصاء گردد.

شناسایی ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی

طبق روش نظریه‌پردازی داده‌بنیاد (در سرفصل روش‌شناسی تحقیق تشریح گردیده است)، کلیه مستندات جمع‌آوری‌شده در خصوص همکاری بین‌المللی را در نرم‌افزار مکس کیودا درج و با استخراج و کدگذاری مفاهیم قابل توجه، در مجموع ۲۹۹ مفهوم پایه استخراج (کدگذاری باز) و با دسته‌بندی (خوشه‌بندی) کدهای مشابه و نزدیک به هم ۴۱ مقوله قابل توجه (مفهوم یا کدهای جامع‌تر)، استخراج گردید (شاخص‌ها) و با ادامه مقوله‌سازی‌های پی‌درپی مقوله‌های فوق، در مجموع ۱۶ مقوله کلان یا مؤلفه احصاء گردید تعداد مفاهیمی که با اتکا به آن‌ها، عناوین شاخص و مؤلفه تعریف گردیده‌اند، در ستون «مفاهیم» آورده شده است (۰).

جدول (۴-۱): احصاء شاخص‌ها و مؤلفه‌های همکاری بین‌المللی (تحصیل محقق)

ردیف	شاخص‌ها	مفاهیم	مؤلفه‌ها	مفاهیم
۱	انتخاب ویژگی‌های امنیتی مشترک	۴	ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل	۲۷
۲	ارتقاء دیپلماسی کشور در قالب دیپلماسی اسلامی و ارزشی ایران	۵		
۳	جایگزینی حقوق و تعهدات به‌جای قدرت و زور در روابط بین‌الملل	۵		
۴	تحقق آرمان‌های بزرگ و ملی کشور	۹		
۵	بازنگری مداوم دولت‌ها به منافع ملی کشور خود	۳	وابستگی متقابل منافع ملی کشور با منافع ملی سایر کشورها	۵۰
۶	لزوم گسترش مناسبات اقتصادی، اجتماعی و سیاسی کشورها	۵		
۷	نپذیرفتن تعدی و تجاوز به کشور	۷	وقوع مداوم جنگ در جهان و لزوم دفاع قاطع از کشور و مظلومان جهان	۲۱
۸	بیداری اسلامی و مخالفت جدی با نظام سلطه	۱۲		
۹	برقراری امنیت و تعادل قدرت قدرت‌ها	۲	رفع دغدغه کشورها در دستیابی به امنیت بین‌المللی	۳۷
۱۰	بقاء و ادامه حیات کشور	۳		
۱۱	تعریف دقیق منافع مشترک و سهم کشورها در آن	۲	شناخت دقیق محیط همکاری و منابع در دسترس	۲۵
۱۲	تعیین دقیق و صریح اهداف مشترک و پایبندی صادقانه به آن‌ها	۳		
۱۳	ایستادگی و مقاومت در نیل به اهداف	۲		
۱۴	تعاملات سیاسی و بین‌المللی بر اساس قواعد اخلاقی	۷	همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاقی	۲۰
۱۵	احترام و پایبندی به عهد و پیمان	۴		
۱۶	دوست داشتن تمام انسان‌ها و مهرورزی به آن‌ها	۴		
۱۷	وابستگی متقابل کارکردی و اقتصادی کشورها	۱۶	همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها	۴۶
۱۸	همکاری جهانی طبق اندازه و توان اقتصادی	۱۶		
۱۹	تداوم همکاری جهت حفظ منافع ملی	۸		
۲۰	سیاست‌های دفاعی کشورها	۱۸	سوابق همکاری و مشارکت در جامعه هدف	۳۳
۲۱	سرایت یا سرریزی در تداوم همکاری	۵		
۲۲	منازعه‌آمیز بودن روابط کشورها به علت ناهماهنگی منافع	۱۶	آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد	۵۱
۲۳	نگرانی کشورها از تعادل قوا در سطح بین‌المللی	۲۱		

ردیف	شاخص‌ها	مفاهیم	مؤلفه‌ها	مفاهیم
۲۴	تدوین چشم‌انداز همکاری اقتصادی و سیاسی قوی	۵	تدوین منشور و قوانین حاکم بر همکاری	۱۵
۲۵	بهره‌گیری از نظریه‌های بین‌المللی	۴		
۲۶	برخورداری از صلاحیت‌های دیپلماتیک	۱۱	تدوین و به‌کارگیری دیپلماسی مشترک تعاملی کارآمد و قوی – بسیجی	۵۲
۲۷	برخورداری از خصلت‌های بسیجی	۱۶		
۲۸	چارچوبی برای حل اختلاف عادلانه با رعایت اصول اخلاقی	۸		
۲۹	پایبندی به موازین شرع در دیپلماسی، رفتارهای فردی و اجتماعی	۳		
۳۰	ایجاد همکاری، توسط رژیم‌های بین‌الملل	۴	تقویت رژیم‌ها و نهادهای بین‌المللی	۲۸
۳۱	تداوم بخشیدن به همکاری، توسط نهادهای بین‌المللی	۴		
۳۲	تلاش و گفتگو برای تضعیف گفتمان‌های امنیتی سلطه‌جویانه	۶	اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی	۵۷
۳۳	ایجاد و تقویت حس مقاومت در برابر نظام سلطه و استکبارستیزی	۱۶		
۳۴	تغییر تفکر در روابط بین‌الملل	۱۶		
۳۵	تقویت نهادها و رژیم‌های بین‌الملل	۱۰		
۳۶	تأمین امنیت و منافع ملی کشورها	۴	ارتقاء امنیت و ثبات بین‌المللی و تأمین منافع ملی کشورها	۱۳
۳۷	توسعه پایدار در سطح بین‌المللی	۲		
۳۸	ایجاد هویت جمعی با همکاری‌های اجتماعی	۲	گسترش روابط بین‌المللی بر اساس مبانی اسلامی و انسانی	۱۵
۳۹	گسترش روابط محترمانه و همه‌جانبه بر اساس احکام اسلامی	۷		
۴۰	راه‌اندازی پایگاه اطلاعاتی	۲	یکپارچه‌سازی ابزارها جهت تحقق همکاری بین‌المللی	۱۴
۴۱	منابع، ابزار و ساختارها	۲		
	جمع	**۲۹۹**		**۵۰۴**

طبق روش، ابعاد یک پدیده را می‌توان از پنج بُعد یا محور شرایط علّی، زمینه، شرایط مداخله‌گر، راهبردها (کنش‌ها و برهم‌کنش‌ها) و پیامدها مورد توجه قرار داد لذا با دسته‌بندی و خوشه‌بندی مؤلفه‌ها در پنج محور فوق ۰، مقوله‌های کلان یا ابعاد، دلایل لزوم همکاری بین‌المللی (شرایط علی)، محیط و منابع لازم جهت همکاری بین‌المللی

(زمینه)، روابط و منافع اثرگذار در همکاری بین‌المللی (شرایط مداخله‌گر) و ساختارها و فرایند همکاری بین‌المللی (کنش و برهم‌کنش (راهبردها)) و پیامدهای حاصل از همکاری بین‌المللی (پیامدها) احصاء گردید (با اتکا به جمعاً ۵۲۴ مفهوم احصاء شده).

جدول (۴-۲): مؤلفه‌ها و ابعاد همکاری بین‌المللی (تحصیل محقق)

ردیف	مؤلفه‌ها	ابعاد	مفاهیم
۱	ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل	بُعد ۱: دلایل لزوم همکاری بین‌المللی (شرایط علی)	۱۳۵
۲	وابستگی متقابل منافع ملی ج.ا.ایران با منافع ملی سایر کشورها		
۳	وقوع مداوم جنگ در جهان و لزوم دفاع قاطع از کشور و مظلومان جهان		
۴	رفع دغدغه کشورها در دستیابی به امنیت بین‌المللی		
۵	شناخت دقیق محیط همکاری و منابع در دسترس	بُعد ۲: محیط و منابع لازم جهت همکاری بین‌المللی (زمینه)	۹۹
۶	همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاقی		
۷	همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها		
۸	سوابق همکاری و مشارکت در جامعه هدف	بُعد ۳: روابط و منافع اثرگذار در همکاری بین‌المللی (شرایط مداخله‌گر)	۸۶
۹	آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد		
۱۰	تدوین منشور و قوانین حاکم بر همکاری	بُعد ۴: ساختارها و فرایند همکاری بین‌المللی (کنش و برهم‌کنش (راهبردها))	۱۵۳
۱۱	تدوین و به‌کارگیری دیپلماسی مشترک تعاملی کارآمد و قوی (روحیه بسیجی)		
۱۲	تقویت رژیم‌ها و نهادهای بین‌المللی		
۱۳	اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی		
۱۴	ارتقاء امنیت و ثبات بین‌المللی و تأمین منافع ملی کشورها	بُعد ۵: پیامدهای حاصل از همکاری بین‌المللی (پیامدها)	۵۱
۱۵	گسترش روابط بین‌المللی بر اساس مبانی اسلامی و انسانی		
۱۶	یکپارچه‌سازی ابزارها جهت تحقق همکاری بین‌المللی		
	جمع		**۵۲۴**

شناسایی ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور

رضا تقی‌پور و علی اسماعیلی (۱۳۹۷)، در مقاله‌ای با عنوان «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران»، ضمن تحلیل محتوای تعاریف دفاع و دفاع سایبری، اسناد بالادستی و مطالعات تطبیقی، کلیدواژه‌های مهم را استخراج کردند و با دریافت اجماع نظر نخبگان از طریق تکنیک دلفی، سه کلیدواژه بازدارندگی، پدافند و برگشت‌پذیری را به‌عنوان ابعاد دفاع سایبری ارائه نمودند و با واکاوی اطلاعات مرتبط در حکم تشکیل شورای عالی فضای مجازی، قانون اساسی جمهوری اسلامی ایران (اصول ۱۷۰،۱۱۱،۱۱۲)، سند راهبردی پدافند سایبری کشور، قوانین بین‌المللی منشور سازمان ملل متحد و استراتژی امنیت و دفاع سایبری اتحادیه اروپا، آمریکا، انگلیس، کره جنوبی، ترکیه و اردن، مؤلفه‌ها و شاخص‌های مرتبط را احصاء و ارائه نمودند (تقی‌پور و اسماعیلی، ۱۳۹۷: ۱۹۷) که در پژوهش حاضر مورد پذیرش قرار گرفته و توسعه داده خواهد شد.

جدول (۴-۳): ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری (تقی‌پور و اسماعیلی، ۱۳۹۷: ۱۹۷)

ابعاد	مؤلفه‌ها	شاخص‌ها
۱. قابلیت بازدارندگی	ثبات نظر	ثبات دیدگاه
	اعتبار	اثبات توانمندی، اراده اقدام سایبری
	قابلیت	تضعیف توانمندی دشمن، ارتقاء توانمندی خودی
	ارتباط	ضمنی، صریح
۲. قابلیت پدافند	پدافند غیرعامل	پوشش، اختفاء، استتار، پراکندگی، فریب، موانع، جابه‌جایی، مستحکم‌سازی، حسگر
	پدافند عامل	سلاح سایبری
۳. قابلیت برگشت پذیری	مقاومت	آسیب، اختلال
	قابلیت اطمینان	بازدید دوره‌ای، تجهیزات بومی، آزمون نفوذ، آستانه ریسک‌پذیری
	افزونگی	سخت‌افزار، نرم‌افزار، نیروی انسانی
	پاسخ و بازیابی	حفاظت از زیرساخت‌ها، کاهش اثر بحران، بازگشت به حالت عادی، بازسازی، ترمیم، توان‌بخشی

نتیجه‌گیری و پیشنهاد

در پژوهش حاضر، با مطالعه نتایج پژوهش‌های قبل در خصوص دفاع سایبری کشور و فرایندهای آن، این مسئله در ذهن شکل گرفت که همکاری بین‌المللی چه تأثیری بر دفاع سایبری کشور داشته باشد و ضمن شناخت اهمیت و ضرورت پژوهش در این خصوص، سه سؤال فرعی کلیدی «ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی کدام‌اند؟» و «ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور کدام‌اند؟» و «تأثیر همکاری‌های بین‌المللی بر دفاع سایبری کشور چگونه است؟» مدنظر قرار گرفت. به‌منظور پاسخگویی به سؤالات فوق، ضمن جمع‌آوری مبانی نظری مرتبط، به جستجو و شناسایی ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور پرداخته (۰ و ۰) و از طرف دیگر، دیدگاه‌های مختلف در خصوص همکاری بین‌المللی مورد مطالعه قرار گرفت و با تجزیه‌وتحلیل کیفی یافته‌ها به روش نظریه‌پردازی داده‌بنیاد (گراندد تئوری)، ابعاد، مؤلفه‌ها و شاخص‌های همکاری بین‌المللی احصاء گردید (۰).

طبق عنوان پژوهش، عواملی از همکاری بین‌المللی باید مورد توجه قرار گیرد و در مدل مفهومی لحاظ گردد که موجب تقویت دفاع سایبری کشور شود؛ بنابراین، عوامل دفاع سایبری کشور (۰) را باید به‌عنوان پیامدهای حاصل از همکاری بین‌المللی در نظر گرفت (طبق مرحله سوم روش نظریه‌پردازی داده‌بنیاد – کدگذاری انتخابی) و عوامل همکاری بین‌المللی را طبق محورهای دلایل لزوم همکاری (شرایط علی)، محیط و منابع لازم برای همکاری (زمینه لازم)، روابط و منافع اثرگذار (شرایط مداخله‌گر)، راهبردها یا کنش و برهم‌کنش قابل توجه (طبق روش پژوهش)، مورد توجه قرار داد (۰).

مدل فرایندی تأثیر همکاری بین‌المللی بر دفاع سایبری کشور

طبق مدل فرایندی فوق، به دلایلی همچون ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل (حوزه فضای سایبر)، وابستگی متقابل منافع ملی کشور با منافع ملی سایر کشورها، وقوع مداوم جنگ در جهان و 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 باید شکل بگیرد و در این راستا 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 سایبری 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.

پاسخ به سؤال اصلی و ارائه مدل مفهومی

در نتیجه‌گیری نهایی به‌منظور پاسخگویی به سؤال اصلی پژوهش (مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور چگونه است؟)، با شناخت همکاری بین‌المللی و دفاع سایبری کشور در مراحل قبل، تأثیر آن‌ها نیز مورد بررسی قرار گرفت و نتایج طبق ۰ احصاء گردید (به‌عنوان مثال، ارتقاء جایگاه نظام جمهوری اسلامی

ایران در نظام بین‌الملل، بر مؤلفه قابلیت از بُعد بازدارندگی دفـاع سـایبری کشـور اثـرگـذار بوده و می‌تواند موجب تضعیف توانمندی دشمن و ارتقاء توانمندی خودی گردد).

جدول (۵-۱): تأثیر همکاری بین‌المللی بر دفاع سایبری کشور

مؤلفه‌های دفاع سایبری / مؤلفه‌های همکاری بین‌المللی	ثبات نظر	اعتبار	قابلیت	ارتباط	پدافند غیرعامل	پدافند عامل	مقاومت	قابلیت اطمینان	افزونگی	پاسخ و بازیابی
ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل			*							
وابستگی متقابل منافع ملی ج.ا.ایران با منافع ملی سایر کشورها					*					
وقوع مداوم جنگ در جهان و لزوم دفاع قاطع از کشور و مظلومان جهان		*								
رفع دغدغه کشورها در دستیابی به امنیت بین‌المللی						*				
شناخت دقیق محیط همکاری و منابع در دسترس								*		
همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاقی				*						
همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها										*
سوابق همکاری و مشارکت در جامعه هدف									*	
آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد	*									
تدوین منشور و قوانین حاکم بر همکاری							*			
تـدوین و بـه‌کـارگیری دیپلماسـی مشـترک تعـاملی کارآمـد و قـوی (روحیه بسیجی)				*						
تقویت رژیم‌ها و نهادهای بین‌المللی	*									
اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی				*						
ارتقاء امنیت و ثبات بین‌المللی و تأمین منافع ملی کشورها										*
گسترش روابط بین‌المللی بر اساس مبانی اسلامی و انسانی			*							
یکپارچه‌سازی ابزارها جهت تحقق همکاری بین‌المللی					*					

با تلفیق نتایج فوق و دفاع سایبری، ابعاد، مؤلفه‌ها و شاخص‌های (عواملی که مـی‌توانـد بر مؤلفه‌ها اثرگذار باشد) همکاری بین‌المللی با رویکرد دفاع سایبری کشور طبق ۰ احصـاء گردید.

جدول (۵-۲): ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری (تقی‌پور و اسماعیلی، ۱۳۹۷: ۱۹۷)

ابعاد	مؤلفه‌ها	شاخص‌های اثرگذار
۱. قابلیت بازدارندگی	ثبات نظر	آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد - تقویت رژیم‌ها و نهادهای بین‌المللی
	اعتبار	وقوع مداوم جنگ در جهان و لزوم دفاع قاطع از کشور و مظلومان جهان
	قابلیت	ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل - گسترش روابط بین‌المللی بر اساس مبانی اسلامی و انسانی
	ارتباط	همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاق - تدوین و به‌کارگیری دیپلماسی مشترک تعاملی کارآمد و قوی (روحیه بسیجی) - اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی
۲. قابلیت پدافند	پدافند غیرعامل	وابستگی متقابل منافع ملی ج.ا.ایران با منافع ملی سایر کشورها - یکپارچه‌سازی ابزارها جهت تحقق همکاری بین‌المللی
	پدافند عامل	رفع دغدغه کشورها در دستیابی به امنیت بین‌المللی
۳. قابلیت برگشت پذیری	مقاومت	تدوین منشور و قوانین حاکم بر همکاری
	قابلیت اطمینان	شناخت دقیق محیط همکاری و منابع در دسترس
	افزونگی	سوابق همکاری و مشارکت در جامعه هدف
	پاسخ و بازیابی	همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها - ارتقاء امنیت و ثبات بین‌المللی و تأمین منافع ملی کشورها

نتایج نشان داد که همکاری بین‌المللی از سه بُعد می‌تواند بر دفاع سایبری کشور اثرگذار باشد:

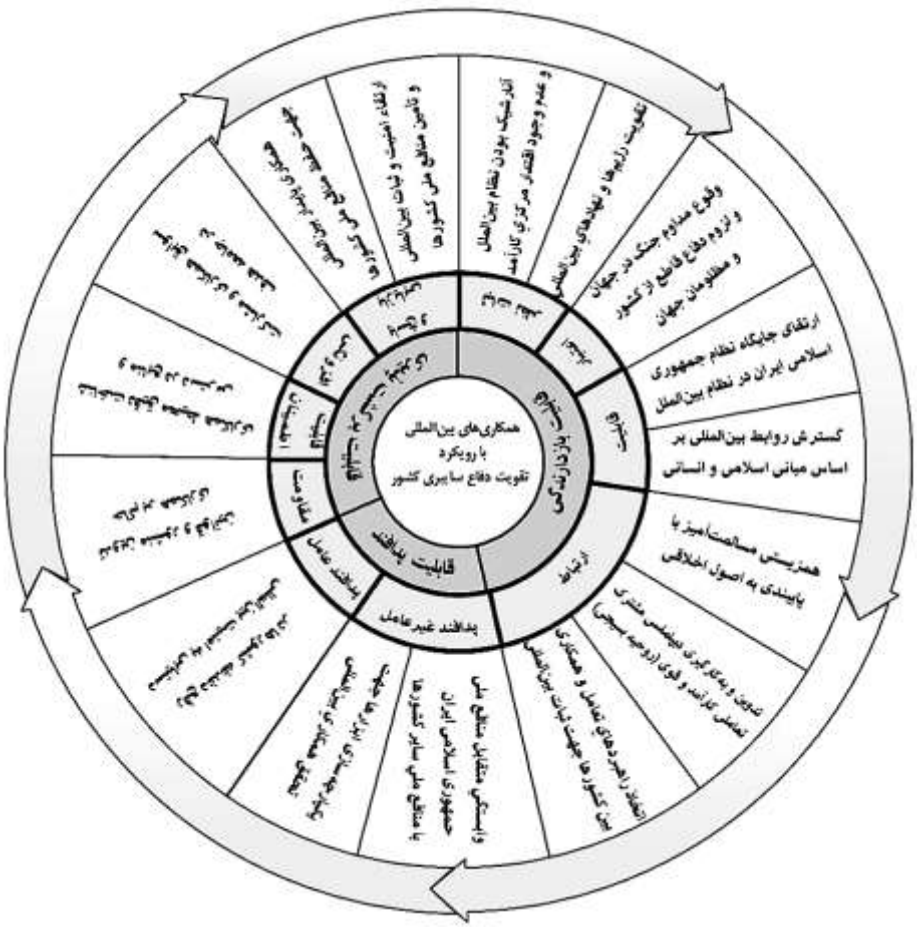
- تأمین قابلیت بازدارندگی:
  - ثبات نظر و ثابت ماندن در دیدگاه‌ها و استحکام در مواضع: تقویت رژیم‌ها و نهادهای بین‌المللی باعث تقویت این مؤلفه می‌گردد ولی آنارشیک بودن نظام بین‌الملل و عدم وجود اقتدار مرکزی کارآمد اثرات منفی بر این مؤلفه خواهد داشت.
  - کسب اعتبار بین‌المللی در حوزه دفاع سایبری: به دلیل وقوع مداوم جنگ در جهان و لزوم دفاع قاطع از کشور و مظلومان جهان باید توجه ویژه‌ای به این مؤلفه داشته باشیم.
  - تقویت توانایی و قابلیت بازدارندگی در حوزه سایبر کشور: با گسترش روابط بین‌المللی بر اساس مبانی اسلامی و انسانی و ارتقاء جایگاه نظام جمهوری اسلامی ایران در نظام بین‌الملل تقویت می‌یابد.

- برقراری ارتباط صریح یا ضمنی با دشمن به‌منظور بازدارندگی: همزیستی مسالمت‌آمیز با پایبندی به اصول اخلاق، تدوین و به‌کارگیری دیپلماسی مشترک تعاملی کارآمد و قوی (روحیه بسیجی) و اتخاذ راهبردهای تعامل و همکاری بین کشورها جهت ثبات بین‌المللی تأثیر به‌سزایی در تقویت این مؤلفه خواهند داشت.

- تأمین قابلیت پدافند:
  - پدافند غیرعامل (ارتقاء پوشش، اختفاء، استتار، پراکندگی، فریب، موانع، جابه‌جایی، استحکام و غیره): وابستگی متقابل منافع ملی ج.ا.ایران با منافع ملی سایر کشورها لازمه یکپارچه‌سازی ابزارها جهت تحقق همکاری بین‌المللی بوده و برآیند آن‌ها باعث تقویت این مؤلفه خواهد شد.
  - پدافند عامل (تجهیز سلاح و جنگ‌افزار سایبری کشور): رفع دغدغه کشورها در دستیابی به امنیت بین‌المللی باعث می‌گردد که این مؤلفه همیشه در حالت ارتقاء و تقویت مداوم قرار داشته باشد.
- تأمین قابلیت برگشت‌پذیری (تاب‌آوری):
  - رفع آسیب‌پذیری‌های سایبری و مقاومت در مقابل اختلالات: تدوین منشور و قوانین حاکم بر همکاری می‌تواند زمینه‌ای را برای کاهش تنش‌ها و اختلالات ایجاد کند و به دنبال آن بهتر به این مؤلفه در کشور پرداخته شود.
  - بازدید دوره‌ای، تجهیزات بومی، تست نفوذ و کنترل آستانه پذیرش ریسک جهت ارتقاء قابلیت اطمینان: شناخت دقیق محیط همکاری و منابع در دسترس می‌تواند کمک شایانی به پیشبرد اهداف این مؤلفه داشته باشد.
  - ایجاد افزونگی (در دسترس بودن سخت‌افزار، نرم‌افزار و نیروی انسانی به‌منظور جایگزینی سریع جهت تداوم خدمات): جمع‌آوری و شناخت سوابق همکاری و مشارکت در جامعه هدف می‌تواند نقش مؤثری را در این مؤلفه ایفاء نماید.

- پاسخ سریع به حملات و حفاظت از زیرساخت‌ها، کاهش اثر بحران، بازیابی، بازسازی، ترمیم و توان‌بخشی سریع: همکاری پایدار بین‌المللی جهت حفظ منافع ملی کشورها و ارتقاء امنیت و ثبات بین‌المللی و تأمین منافع ملی کشورها می‌تواند توان پاسخگویی و سایر اهداف این مؤلفه را تقویت نماید.

با تجمیع یافته‌ها در یک مدل خورشیدی[1]، مدل مفهومی همکاری بین‌المللی با رویکرد تقویت دفاع سایبری کشور طبق ۰ ترسیم گردید.



شکل (۵-۲): مدل مفهومی همکاری بین‌المللی با رویکرد تقویت دفاع سایبری کشور

1.Sun Burst

پیشنهادها

بر اساس نتایج حاصل از پژوهش، پیشنهادهای زیر ارائه می‌گردد:

۱) توجه ویژه به شناخت دقیق منافع ملی کشور در فضای سایبر و دفاع از آن‌ها در مقابل حملات سایبری

۲) توجه ویژه به شناسایی آسیب‌پذیری‌های کشور در فضای سایبر و رفع سریع آن‌ها در راستای تقویت دفاع سایبری کشور

۳) توجه ویژه به شناسایی عوامل اثرگذار در ارتقاء توان بازدارندگی کشور در فضای سایبری.

۴) توجه ویژه به شناخت دقیق محیط و زمینه همکاری بین‌المللی جهت تقویت دفاع سایبری کشور

۵) توجه ویژه به سیاست‌گذاری متمرکز اقدامات حوزه دفاع سایبری کشور و نگاشت نهادی تکالیف و فعالیت‌ها

در طی پژوهش، مواردی مشاهده شد که می‌تواند زمینه مطالعاتی مناسبی برای پژوهش‌های آتی باشد که به‌اختصار عبارت‌اند از:

۶) مطالعه تطبیقی همکاری‌های بین‌المللی انجام‌شده در خصوص دفاع سایبری کشورها.

۷) مطالعه تطبیقی اقدام سازمان‌های بین‌المللی در خصوص ارتقاء قدرت دفاع سایبری کشورها.

۸) طراحی نظام مقابله با تهدیدات و حملات سایبری در شرایط عادی، ویژه امنیتی و جنگی.

۹) معماری وظایف و نگاشت نهادی ساختارهای ملی در همکاری‌های بین‌المللی برای تقویت توان دفاع سایبری کشور.

فهرست منابع ومآخذ

الف. منابع فارسی

- قرآن کریم
- کتب و بیانات حضرت امام خمینی (رحمه الله علیه(
- کتب و بیانات حضرت امام خامنه‌ای (مدظله‌العالی(
- اخبار رسمی (۱۳۹۷)، ترندمیکرو پیش‌بینی آینده تهدیدات سایبری در سال ۲۰۱۹ را منتشر کرد [اخبار رسمی]. از ترندمیکرو-https://news.akhbarrasmi.com/news/13971022339626094/ پیش‌بینی آینده تهدیدات سایبری در سال ۲۰۱۹ را منتشر کرد .
- اسکندری، حمید (۱۳۹۳)، دانستنی های پدافند غیرعامل: دوره عمومی مدیران و کارکنان دستگاه‌های اجرایی، بوستان حمید.
- اسماعیلی، محسن و بالایی، حمید (۱۳۹۲)، «الگوی راهبردی تأمین امنیت ملّی جمهوری اسلامی ایران»، فصلنامه پژوهش‌های راهبردی سیاست، جلد ۲، شماره ۵.
- ام. والت، استفان و مهدویان، حسن (۱۳۸۵)، روابط بین الملل: یک جهان، چندین تئوری [تخصصی]. از http://www.bashgah.net/fa/content/show/20215.
- انتخاب (۱۳۹۷)، شطرنج سایبری سال ۲۰۱۹ آغاز شد / پیش‌بینی کیش‌ومات‌های دنیای مجازی [آی تی و فناوری]. از شطرنج سایبری سال ۲۰۱۹ /https://www.entekhab.ir/fa/news/450142 آغاز شد پیش‌بینی کیش‌ومات‌های دنیای مجازی.
- ایمانی، هادی (۱۳۹۰)، جنگ‌های سایبری و مشکل یافتن منشأ آن‌ها- مطالعه موردی استاکس نت، مقاله ارائه‌شده در نخستین همایش ملی دفاع سایبری، نخستین همایش ملی دفاع سایبری.
- تقی‌پور، رضا و اسماعیلی، علی (۱۳۹۷)، «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران»، فصلنامه امنیت ملی، ۳۰.
- تقی‌پور، رضا؛ کارگری، مهرداد؛ لطیفی، میثم؛ فرجی‌پور، محمدرضا؛ محمدی، علی؛ صنیعی، محمدحسین؛ ... و یزدانی، سعید (۱۳۹۷)، طراحی نظام دفاع سایبری کشور و تدوین الزامات تحقق آن (پایان‌نامه دکتری)، دانشگاه عالی دفاع ملی، تهران.
- جلالی فراهانی، امیرحسین (۱۳۹۰)، بایسته های حقوق دفاع مشروع سایبری، مقاله ارائه‌شده در نخستین همایش دفاع سایبری، نخستین همایش دفاع سایبری.
- جمالی، حسین (۱۳۸۲)، تاریخ و اصول روابط بین الملل (ج ۱)، قم - ایران: سپاه پاسداران انقلاب اسلامی، نمایندگی ولی‌فقیه، مرکز تحقیقات اسلامی.

- حاجیلو، حسین‌علی (۱۳۸۳)، «معرفی روش‌های تحلیل داده‌های کیفی با تأکید بر روش تحلیل محتوا»، مدیریت فردا، ۲، شماره‌های ۸-۷.
- حافظ نیا، محمدرضا (۱۳۹۰)، «مفهوم سازی ژئوپلیتیک اینترنت و فضای مجازی»، ژئوپلیتیک، شماره ۲۱.
- خاک‌پور، مرتضی (۱۳۹۷)، بزرگ‌ترین خطرات سایبری برای تجارت‌ها در سال ۲۰۱۹ [سایبربان]. از بزرگ ترین خطرات سایبری برای تجارت ها در https://www.cyberbannews.com/ سال ۲۰۱۹.
- دهخدا، علی‌اکبر (۱۳۷۷)، لغت‌نامه دهخدا (ج ۱۴)، تهران: مؤسسه انتشارات و چاپ دانشگاه تهران.
- دویچ، کارل (۱۳۷۵)، نظریه‌های روابط بین‌الملل، ترجمه وحید بزرگی، ج دوم، تهران: انتشارات جهاد دانشگاهی.
- ربیعی، علی (۱۳۹۳)، «امنیت ملی، مفهومی در حال تکوین»، اطلاعات سیاسی اقتصاد، شماره‌های ۱۹۸-۱۹۷.
- روشندل، جلیل (۱۳۹۴)، امنیت ملی و نظام بین‌المللی، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- زمانی، سید قاسم و پیری، حیدر (۱۳۹۱)، «کارکرد منافع ملی حیاتی در حوزه‌های انسانی حقوق بین‌الملل: حقوق بشردوستانه»، حقوقی دادگستری، شماره ۷۹.
- طیب، علیرضا (۱۳۹۵)، مارکسیسم، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- عبدالله خانی، علی (۱۳۸۳)، نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۱)، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌الملل ابرار معاصر تهران.
- عسگرخانی، ابومحمد (۱۳۸۳)، رژیم های بین المللی، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌الملل ابرار معاصر تهران.
- علیخانی، علی‌اکبر (۱۳۹۰)، «مبانی و اصول روابط بین‌الملل در اسلام»، پژوهش‌های روابط بین‌الملل، جلد ۱، شماره ۱.
- علیزاده، کریم و موسوی، علیرضا (۱۳۹۴)، تحلیلی بر امنیت ملی و تأمین آن در قانون اساسی، مقاله ارائه‌شده در نخستین کنگره بین‌المللی حقوق ایران.
- غفرانی، لیلا (۱۳۹۱)، روابط بین الملل و سیاست خارجی مبتنی بر صلح از دیدگاه امام خمینی(ره) (ج ۱، ص ۷)، مقاله ارائه‌شده در همایش ملی حقوق بین‌الملل در آیینه علوم روز.
- غلامحسین زاده، زهره (۱۳۹۳)، «فضای سایبر: رویکردهای مفهومی»، ماهنامه گفتمان علم و فناوری، جلد ۱، شماره ۶، صص ۲۷۱-۲۵۵.

- فراست (۱۳۹۷)، مهم‌ترین چالش‌های پیش‌روی امنیت سایبری در سال ۲۰۱۹ [فراست- اطلاع‌رسانی امنیت اطلاعات]. از https://www.faraasat.com/news/6006/cybersecurity-predictions-for-2019/.
- فیروزآبادی، سید جلال دهقانی (۱۳۸۱)، «تحول نظریه های منازعه و همکاری در روابط بین‌الملل»، پژوهش حقوق و سیاست، شماره ۸.
- قادری حاجت، مصطفی و نصرتی، حمیدرضا (۱۳۹۱)، «فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار»، پژوهشنامه جغرافیای انتظامی، شماره ۲، صص ۱۱۴-۸۹.
- کانون تفکر سیاست خارجی (۱۳۹۷)، جمهوری اسلامی ایران و تهدیدهای نظامی- امنیتی منطقه‌ای و بین‌المللی [ایرنا]. از بین‌الملل/جمهوری اسلامی https://article.irna.ir/fa/c1_21976/ ایران و تهدیدهای نظامی- امنیتی منطقه‌ای و بین‌المللی.
- کلومبیس، تئودور و ولف، جیمز (۱۳۷۵)، رویکردهای مختلف در مطالعه سیاست، ترجمه وحید بزرگی، تهران: مؤسسه انتشارات جهاد دانشگاهی.
- کمیته دائمی پدافند غیرعامل کشور (۱۳۹۴)، سند راهبردی پدافند سایبری کشور، فرماندهی کل قوا- کمیته دائمی پدافند غیرعامل کشور.
- مرادی، محسن (۱۳۹۵)، کدگذاری داده‌ها در نظریه‌پردازی داده‌بنیاد (Grounded Theory) [علمی]. از html. کدگذاری داده‌ها در نظریه‌پردازی داده/http://analysisacademy.com/5209.
- مرکز ملی فضای مجازی (۱۳۹۶)، فضای مجازی در ۲۰۲۵ [شورای عالی فضای مجازی]. از http://majazi.ir/general_content/81611/swd_id/13825/unitWdId/53812/-فضای-مجازی-در-محتوای-عمومی=t?html.۲۰۲۵.
- مشیرزاده، حمیرا (۱۳۸۳)، «احیای مکتب انگلیسی در روابط بین‌الملل»، فصلنامه سیاست خارجی، شماره‌های ۱۸-۳.
- مشیرزاده، حمیرا (۱۳۹۴)، تحول در نظریه های روابط بین الملل، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- معین، محمد (۱۳۸۲)، فرهنگ فارسی معین (یک جلدی): بر اساس فرهنگ شش جلدی دکتر محمد معین، تهران: معین.
- هواشناس، رضا (۱۳۹۷)، پیش بینی سیمنتک از تهدیدات سایبری سال ۲۰۱۹ [سایبربان]. از پیش‌بینی سیمنتک از تهدیدات سایبری سال ۲۰۱۹/https://www.cyberbannews.com.
- وفایی، یوسف (۱۳۹۸)، ۱۰ تهدید امنیت سایبری در سال ۲۰۱۹ [kaliboys]. از https://kaliboys.com/top-10-cybersecurity-threats-in-2019/.

- ونت، الکساندر (۱۳۸۵)، جامعه و همکاری در روابط بین الملل، ترجمه بهرام مستقیمی، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- ونت، الکساندر (۱۳۸۴)، نظریه اجتماعی سیاست بین‌الملل، ترجمه حمیرا مشیری، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- ویکی‌پدیا، دانشنامه آزاد (۲۰۱۸)، جنگ مجازی [تخصصی]. از جنگ مجازی، ۱۹ اسفند ۱۳۹۷. https://fa.wikipedia.org/wiki/
- یوسفی، امیرمحمد حاجی (۱۳۸۲)، «سیاست خارجی ایران در قبال اسرائیل از دید نظریه‌های روابط بین‌الملل»، مطالعات خاورمیانه، شماره ۳۳.

الف. منابع انگلیسی

- Arsene, Liviu. (2018). 10 of the Biggest Security Predictions for 2019 – TechNative. Retrieved April 08, 2019, from https://www.technative.io/10-of-the-biggest-security-predictions-for-2019/
- AT&T Business Editorial Team. (2019). 5 cybersecurity trends to expect in 2019. Retrieved April 13, 2019, from https://www.business.att.com/learn/tech-advice/5-cybersecurity-trends-to-expect-in-2019.html
- Barlow, Caleb. (2018). IBM X-Force Security Predictions for the 2019 Cybercrime Threat Landscape. Retrieved April 08, 2019, from https://securityintelligence.com/ibm-x-force-security-predictions-for-the-2019-cybercrime-threat-landscape/
- Barracuda MSP. (2018). Predictions for 2019: Cybersecurity, Specialization and Overcoming Objections –. Retrieved April 12, 2019, from https://www.channelfutures.com/from-the-industry/predictions-for-2019-cybersecurity-specialization-and-overcoming-objections
- Bradshaw, Mike. (2018). BeyondTrust's Top 10 Security Predictions for 2019. Retrieved April 12, 2019, from https://www.globenewswire.com/news-release/2018/11/16/1653062/0/en/BeyondTrust-s-Top-10-Security-Predictions-for-2019.html
- Burt, David; Kleiner, Aaron; Nicholas, J. Paul; & Sullivan, Kevin. (2014). Cyberspace2025 Today's decisions, Tomorrow's Terrain, navigating the future of cybersecurity policy. Microsoft Corporation.
- Creswell, John W. (2013). Educational research: planning, conducting, and evaluating quantitative and qualitative research.
- CSO staff. (2018). 9 cyber security predictions for 2019 | CSO Online. Retrieved March 19, 2019, from https://www.csoonline.com/article/3322221/9-cyber-security-predictions-for-2019.html
- Diaz, Vicente. (2018). Kaspersky Security Bulletin 2018. Threat Predictions for 2019 |. Retrieved April 13, 2019, from https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878/

- Giles, Martin. (2019). Five emerging cyber-threats to worry about in 2019 - MIT Technology Review. Retrieved April 08, 2019, from https://www.technologyreview.com/s/612713/five-emerging-cyber-threats-2019/
- Godwin, James B.; Kulpin, Andrey; Rauscher, Karl Frederick; & Yaschenko, Valery. (2014). Critical Terminology Foundations 2. EastWest Institute and the Information Security Institute at the Moscow State University.
- Greenberg, Adam. (2018). Facing Forward: Cyber Security in 2019 and Beyond. Retrieved April 12, 2019, from https://www.fireeye.com/blog/executive-perspective/2018/11/facing-forward-cyber-security-in-2019-and-beyond.html
- Joint Publication. (2016). Department of Defense Dictionary of Military and Associated Terms 8 November 2010 (As Amended Through 15 February 2016). Joint Publication.
- Krasner, Stephen D. (1983). International regimes. Cornell University Press.
- Lukas, Carol; & Andrews, Rebecca. (2006). Four keys to collaboration success. fieldstone alliance, 1, 2011.
- Lyn Stoner, Jesse. (2013). Let's Stop Confusing Cooperation and Teamwork with Collaboration. Retrieved December 23, 2016, from http://seapointcenter.com/cooperation-teamwork-and-collaboration/
- Lynn-Jones, Sean M. (1995). Offense-defense theory and its critics. Security Studies, 4(4), 660–691.
- McAfee Labs. (2018). McAfee Labs 2019 Threats Predictions Report | McAfee Blogs. Retrieved March 19, 2019, from https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/
- Mearsheimer, John J. (1994). The false promise of international institutions. International security, 19(3), 5–49.
- NeSmith, Brian. (2018). Council Post: Cybersecurity Predictions For 2019. Retrieved April 08, 2019, from https://www.forbes.com/sites/forbestechcouncil/2018/12/28/cybersecurity-predictions-for-2019/#2e26aaf24a27
- Neuss, Beate. (2007). Kenneth N. Waltz, Theory of International Politics, New York 1979. In Schlüsselwerke der Politikwissenschaft (pp. 481–485). Springer.
- Raffael, Marty. (2018). 2019 Forcepoint Cybersecurity Predictions Report. Forcepoint.
- RSA Security. (2019). RSA Security 2019 Predictions: Rethinking Identity and Authentication. Retrieved April 12, 2019, from http://vmblog.com/archive/2019/01/14/rsa-security-2019-predictions-rethinking-identity-and-authentication.aspx#.XLDZV-gzZkg
- Sophos. (2019). Sophos releases 2019 cybersecurity threat report • InfoTech News. Retrieved April 09, 2019, from https://meterpreter.org/sophos-releases-2019-cybersecurity-threat-report/
- Trend Micro. (2019). Trend Micro Security Predictions for 2019. Trend Micro.