تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران

علی اسماعیلی[1]
جلال ثناقربانی[2]

تاریخ دریافت:۱۳۹۶/۰۹/۲۰ تاریخ پذیرش:۱۳۹۶/۱۲/۲۲

چکیده:

جایگاه خاص جمهوری اسلامی ایران در ترتیبات منطقه‌ای و نظام بین‌الملل سبب شده تا نظام سلطه، چالش‌های متنوعی به‌خصوص در مسائل نوظهوری مانند رسانه‌های جمعی و فضای سایبری برای تحدید قدرت ملی آن ایجاد نماید. در فضای تکثر و تنوع چالش‌ها و فرصت‌ها، نظام تصمیم‌ساز کشور در دانشگاه‌ها و مراکز مطالعاتی، علاوه بر طراحیِ روش‌های مقابله با چالش‌های کنونی، مؤظف هستند تصویری از موانع، آسیب‌ها و فرصت‌های پیش‌رو در حوزه‌های مختلف احصاء و سناریوهای محتمل پیش-رو و سناریوی مطلوب نظام اسلامی را پیش روی تصمیم‌گیران اصلی کشور قرار داد.

این پژوهش با هدف سناریوپردازی و تبیین نسبتِ میان آینده‌های محتمل و مطلوب تهدیدات سایبری علیه جمهوری اسلامی ایران صورت گرفته و با بهره‌گیری از روش پژوهش آمیخته؛ سعی دارد علاوه بر شناسایی آینده‌های محتمل، فضای مطلوب نظام جمهوری اسلامی ایران در حوزه فضای سایبر را نیز تبیین و بسترهای تجمیع نیروها در جهت نیل به چشم‌انداز مطلوب نظام را به لحاظ ذهنی فراهم آورد.

پس از بررسی سناریوهای محتمل و مشخص کردن الگوهای شرایط مطلوب (اسناد بالادستی و فرمایشات امام خامنه‌ای (مدظله‌العالی)) نتیجه‌گیری شد که سناریوی مطلوب جمهوری اسلامی ایران؛ جزء سناریوهای محتمل نیست؛ این بدان معناست که روندهای کنونیِ فضای سایبر، به سمت الگوی مطلوب نظام اسلامی حرکت نمی‌کند و در صورتی که عزم عمومی برای ایجاد روندها، استفاده از فرصت‌ها و مقابله با چالش‌ها نباشد؛ انتخاب آینده نظام در فضای سایبر، انتخاب بین بد و بدتر خواهد بود.

کلیدواژه‌ها: فضای سایبری، سناریونویسی، سناریوی محتمل، سناریوی مطلوب، تهدیدات سایبری

۱- دانشجوی دکتری مدیریت راهبردی امنیت فضای سایبر دانشگاه عالی دفاع ملی(نویسنده مسئول) a.esmaily@sndu.ac.ir
۲- دانشجوی دکترای مطالعات انقلاب اسلامی- پژوهشکده امام خمینی و انقلاب اسلامی

مقدمه:

در شرایطی که زیرساخت‌ها و حوزه‌های حیاتی و حساس کشور به‌شدت به فضای سایبر وابسته شده؛ نشانه‌هایی از تلاش آمریکا، رژیم صهیونیستی، عربستان سعودی و سایر بازیگران دولتی و غیردولتی برای استفاده از آن در شکل‌دهی به تهدیدات متکثر و هوشمند علیه جمهوری اسلامی ایران مشاهده می‌شود.

با توجه به ماهیت فضای سایبر که امکان پیش‌بینی بسیط و خطی از تهدیدات آینده را تقریباً غیرممکن کرده، احتمال غافلگیریِ کنشگران منفعل و محافظه‌کار در مقابل تهدیدات آتی بسیار بالا ارزیابی می‌شود. در این شرایط، مقابله با تهدیدات پیش‌رو و استفاده از فرصت‌های احتمالی، نیازمند ایجاد آمادگی نرم‌افزاری و سخت‌افزاری برای مقابله با چالش‌های آتی است. در این چارچوب، تصویرسازی از آینده، جلوگیری از تحقق آینده نامطلوب و تلاش برای شکل‌گیری روندهای مطلوب دستور کار مهمی برای نظام‌های حکومتی است که ادعای حکمرانی مطلوب دارند. در این معنا، ایجاد سازوکارهای لازم برای بازیگریِ فعال در شکل‌دهی به آینده فضای سایبر، نیازمند تصویرسازی از آینده‌های محتمل پیش رو در ابعاد تهدیدات و فرصت‌های پیش‌رو است.

بیان مسئله: در گذشته شاهد نوعی یکنواختی در فرایندها و رویدادها بودیم که در آن پیوستگی عجیبی در سیر حوادث وجود داشت و عناصر شگفتی‌ساز به‌ندرت اتفاق می‌افتاد؛ اما ارزیابی روندهای حاکم بر فضای سایبری، تأییدی بر وجود روندهای متقاطع، متکثر، جهش یابنده و افول یابنده و به‌طور کلی کثرت عوامل ضعیف تغییر و شگفتی سازها است.

برخلاف روندهای کلاسیک، روندهای کنونی و پیش‌رو، مملو از عدم قطعیت‌ها، پیچیدگی‌ها و تکثر منابع تأثیرگذار بر ساخت آینده است. نماد بارز ویژگی‌های فوق را می‌توان در فضای سایبر دید و یا به تعبیری دیگر، بیان داشت که فضای سایبر علت اصلی این همه پیچیدگی و عدم قطعیت است. اهمیت این مسئله تا بدان جا مورد تأکید قرار گرفته که در ادبیات جدید سیاسی و امنیتی ناتو و وزارت دفاع آمریکا؛ از این فضا به‌عنوان قلمرو پنجم نبردهای نظامی – اطلاعاتی نام برده شده است (kevin benedict,2011).

جمهوری اسلامی ایران به جهت حفاظت از ارزش‌های اساسی، زیرساخت‌های حیاتی و در نهایت حفظ و ارتقاء منافع و امنیت ملی در این به‌اصطلاح قلمرو پنجم نبردهای نظامی- اطلاعاتی،

از یک‌سو باید برای تهدیدات فعلی چاره‌ای بیاندیشد تا ثبات کنونی حفظ شود و از سوی دیگر تصویر روشنی از آینده‌های محتمل این فضا و تهدیدات متصوره از آن داشته باشد تا بتواند بر تهدیدات آینده غلبه و در صورت امکان مطلوبیت‌های خود را در آن ایجاد نماید.

این دستور کار مهم، نیازمند شناسایی تهدیدات آینده، سناریوهای محتمل پیش‌رو و تعیین نسبت آن با سناریوی مطلوب جمهوری اسلامی ایران در این فضا است. این تصویرسازی، کمک خواهد کرد تا بستر تأثیرگذاری ذهنی و روانی بر تصمیم‌سازان و تصمیم‌گیران کشور برای تحقق بازیگریِ فعالانه و اجتناب از حضور منفعلانه در فضای سایبر ایجاد شود. نکته مهم آنکه سناریوی مطلوب (که در بعضی از ادبیات آینده‌پژوهی به آن چشم‌انداز نیز اطلاق می‌شود) باید با نگاه به رسالت انقلاب اسلامی و ایجاد تمدن نوین اسلامی طراحی شود اما سناریوهای محتمل با نگاهی واقع‌بینانه طراحی و تبیین گردد.

اما نکته مهم اینجاست که در شرایطی که طراحی سناریو مطلوب نظام اسلامی در کنار شناسایی سناریوهای محتمل از نیازهای اساسی نظام مدیریت تهدیدات فضای سایبر جمهوری اسلامی ایران می‌باشد، اما چیستی و مؤلفه‌های سناریوهای محتمل و مطلوب و رابطه میان آن‌ها به صورتی روشمند و قابل ارزیابی به تصمیم گیران کشور ارائه نشده است. این پژوهش با هدف رفع این خلاء، به سناریوهای محتمل و سناریوی مطلوب در فضای سایبر و تبیین نسبت آنان می‌پردازد.

اهمیت و ضرورت تحقیق: کشورهای پیشرو در حوزه سایبر سعی در شناسایی تهدیدات و فرصت‌های آینده فضای سایبر دارند و از هم‌اکنون در سطوح مختلف راهبردی و عملیاتی، سناریوهای مختلفی را متناسب با نیازمندی‌ها و الگوهای حاکم بر کشورهای خود طراحی نموده‌اند. به‌عنوان نمونه مؤسسه تحقیقاتی رند، مؤسسه تحقیقاتی میتری همچنین سندیا ازجمله مؤسسات آمریکایی متعلق به نهادهای امنیتی – نظامی آمریکا هستند که نسبت به ارائه تصاویری از آینده فضای سایبر و آینده مطلوب خود اقدام کرده‌اند.

اگر جمهوری اسلامی ایران نیز بخواهد از ارزش‌های اساسی، زیرساخت‌های حیاتی، اطلاعات ارزشمند ملی در جهت حفظ و ارتقای امنیت ملی خود محافظت نماید و به‌عنوان بازیگری فعال به ایفای نقش خود بپردازد؛ باید تصویر درستی از وضعیت خود، محیط پیرامونی و عوامل تأثیرگذار بر آینده داشته باشد تا بتواند ساخت آینده را در جهت تحقق اهداف خود برنامه‌ریزی کند و این

مستلزم شناخت از آینده‌های محتمل و روندهای تأثیرگذار بر آن است. اهمیت این پژوهش نیز در این چارچوب معنی پیدا می‌کند یعنی تلاش برای فهم آینده و ساخت آینده مطلوب.

با توجه به اینکه دشمنان و رقبای جمهوری اسلامی ایران هریک در تلاش‌اند تا با تأثیرگذاری بر روندهای سازنده آینده؛ تصویر مطلوب خود از فضای سایبر را عملیاتی نمایند؛ ایران نیز باید با شناسایی آینده‌های محتمل، بکوشد ضمن جلوگیری از وقوع سناریوی نامطلوب؛ سناریوی مطلوب خود را در این فضا ایجاد نماید. ضرورت این پژوهش آنجاست که در صورت عدم توجه به پژوهش‌هایی از این دست، جمهوری اسلامی ایران را باید بازیگری منفعل در آینده به‌حساب آورد که دچار غافلگیری‌های متعدد در فضای سایبر شده است.

امام خامنه‌ای (مدظله‌العالی) در مورد لزوم تحقق سناریوی مطلوب نظام اسلامی در حوزه‌های مختلف چنین می‌فرمایند:

«ما اجازه نمی‌دهیم که آینده، جدای از اراده و خواست ما به جهتی حرکت کند، ما می‌خواهیم اراده خود را در آینده دخیل کنیم، این هم خاصیت انسان مؤمن به اهداف است» (امام خامنه‌ای: ۱۳۶۸/۵/۱۸).

اهداف تحقیق

هدف اصلی: تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران

اهداف فرعی:

- تبیین و شناخت عدم قطعیت‌های تأثیرگذار بر ساخت آینده فضای سایبر جمهوری اسلامی ایران
- تبیین و شناخت پیشران‌های تأثیرگذار بر ساخت آینده فضای سایبر جمهوری اسلامی ایران

سؤالات تحقیق:

سؤال اصلی: نسبت میان سناریوهای محتمل و مطلوب تهدیدات سایبری علیه جمهوری اسلامی ایران چیست؟

سؤالات فرعی:

- عدم قطعیت‌های تأثیرگذار بر ساخت آینده فضای سایبر جمهوری اسلامی ایران کدام است؟
- پیشران‌های تأثیرگذار بر ساخت آینده فضای سایبر جمهوری اسلامی ایران کدام است؟

روش‌شناسی

در انجام این پژوهش؛ چهار مرحله طی شده است.

مرحله اول مطالعات توصیفی: بر اساس تکنیک خوشه‌بندی در تحلیل محتوا؛ اسناد بالادستی، مبانی نظری، فرمایشات امام خامنه‌ای (مدظله‌العالی)، مطالعات تطبیقی، روندهای فناوری اطلاعات و ارتباطات؛ مورد خوشه‌بندی و تحلیل و بررسی قرار گرفت. در این مرحله استخری از کلیدواژه-ها به دست آمد که بر اساس بیشترین فراوانی، پیش‌نیازهای سناریونویسی استخراج گردید.

مرحله دوم؛ با تکنیک دلفی، پیش‌نیازهای استخراجی برای استفاده در سناریونویسی در مصاحبه با خبرگان، مورد تأیید آنان قرار گرفت.

در مرحله سوم، پرسشنامه پژوهش طراحی و در مرحله چهارم بار دیگر پنل خبرگان پژوهش شکل گرفت و با دعوت از خبرگان، روندها، پیشران‌ها وعدم قطعیت‌های مزدوج (دوبه‌دو)؛ (بر اساس ارائه مؤلفه‌های به دست آمده در سه مرحله قبل) به تأیید خبرگان پژوهش، رسید. در نهایت سناریوهای محتمل و مطلوب ترسیم گردید.

این پژوهش که به روش آمیخته صورت گرفته و از نظر نوع؛ پژوهشی کاربردی می‌باشد. از منظر قلمرو، پژوهش سناریوهای ایران و غرب به‌خصوص آمریکا را مورد بررسی قرار می‌دهد.

جامعه آماری و حجم: اعضای جامعه آماری این پژوهش شامل دو گروه هستند: متخصص فضای سایبر و تهدیدات سایبری و متخصص دانش راهبردی. از میان این دو گروه، به روش نمونه‌گیری هدفمند و در دسترس تعداد ۷۰ نفر انتخاب و مورد پرسش قرار گرفته‌اند.

پیشینه شناسی تحقیق:

پژوهش‌های مستقل درباره فضای سایبر را می‌توان به چند دسته تقسیم کرد: تعدادی از پژوهش‌های صورت گرفته در رابطه با فضای سایبر به مزیت‌ها، کارکردها و دستاوردهای این فضا پرداخته‌اند. در این رابطه می‌توان به آثاری مانند «روزنامه در فضای سایبر؛ جامعه اطلاعاتی و آزادی بیان» نوشته یونس شکرخواه، مقاله «اینترنت و توسعه سیاسی: حوزه عمومی در فضای سایبرنتیک» نوشته آقای محمدقلی میناوند و مقاله «تأثیر سایبر دیپلماسی آمریکا بر دیدگاه کاربران سایبری ایران» نوشته آقایان طباطبایی، سیدمحمد؛ سلیمی، حسین؛ موحدیان، احسان اشاره نمود.

تعداد قابل توجهی از پژوهش‌ها درباره فضای سایبری معطوف به آسیب‌پذیری‌ها و تهدیدات متصور از این ناحیه است. این آثار در زمینه‌های جنگ سایبری، امنیت، هویت، مرز و سایبر تروریسم به نگارش درآمده‌اند. برای نمونه می‌توان مقاله سنجش تهدیدات سایبری آقایان عبداله-خانی و حسینی که به دنبال پاسخ به این سؤال است که وضعیت و میزان تهدیدات خطرناک امنیتی سایبری در چه حدی است؟ پروژه تحقیقاتی با عنوان «الزامات جنگ‌های نوین در فضای سایبری» به کوشش جمعی از محققین مرکز آینده‌پژوهی علوم و فناوری دفاعی وزارت دفاع و پشتیبانی نیروهای مسلح، پایان‌نامه آقای مصطفی اصلانی‌مقدم با عنوان «جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران» و پژوهش «تأثیر جهانی‌شدن بر مرزها و اشاعه مرزها در فضای سایبر» نوشته هادی ویسی و نیز مقاله «بهره‌برداری داعش از فضای سایبری» نوشته سیدعباس عراقچی و شاهین جوزانی کهن اشاره نمود.

همچنین تعداد قابل ملاحظه‌ای از پژوهش‌های خارجی نیز در این حوزه انتشار یافته است، به‌عنوان نمونه شاخصه‌های تهدیدات سایبری توسط مؤسسه سندیا (Sandia,2012)، ارزیابی تهدیدات سایبری و همچنین متدولوژی ارزیابی و اصلاح تهدیدات سایبری توسط مؤسسه میتری (The MITRE Corporation,2012).

در یک جمع‌بندی از پیشینه تحقیق می‌توان مشخص کرد که فقدان بررسیِ سناریوهای محتمل فضای سایبر برای جمهوری اسلامی ایران، از مهم‌ترین نقاط ضعف ادبیات تحقیق است که در مورد آن خلاء جدی وجود دارد. در این چارچوب، نوآوری این مقاله، تبیین و بررسی سناریوهای محتمل فضای سایبر با نگاهی آینده‌پژوهانه است. شاید مهم‌ترین بخش این نوآوری، مشخص کردن سناریوی مطلوب نظام جمهوری اسلامی ایران در میان سناریوهای محتمل است تا بتوان نسبت میان این دو را درک کرد و برای ترمیم شکاف میان سناریوی محتمل و سناریوی مطلوب از هم‌اکنون به فکر طراحی و برنامه‌ریزی کلان و بلندمدت بود.

ادبیات و مبانی نظری پژوهش

مفهوم شناسی:

سناریونویسی: واژه سناریو از هنرهای نمایشی گرفته شده است. هرمان کان اولین بار در سال ۱۹۵۰ واژه سناریونویسی را در مطالعات آینده‌پژوهی برای برنامه‌ریزی مطالعات راهبردی و نظامیِ مؤسسه رند به کار برد. سناریوها از آینده‌های محتمل و مطلوب تصویری را ارائه می‌نمایند (پدرام،

۱۳۸۸: ۱۴۳).

به ترتیب فراوانی، آینده‌ها شامل، آینده‌های ممکن، باورکردنی، محتمل و مطلوب (مرجح) است. یک سناریوی خوب، به صورتی باورپذیر، با انسجام درونی، جذابیت و کاربردی بودن در فرآیند تصمیم‌گیری کلان، ارتباط میان گذشته و آینده را برقرار و به شکل‌گیری چالش‌های آینده اشاره می‌نماید. سناریونویسی با تمرکز بر شناسایی چالش‌ها و فرصت‌ها؛ به تبیین آینده‌های محتمل‌تر و مطلوب می‌پردازد (Wendell Bell 2008, 431).

تهدیدات سایبری: هر رویداد یا واقعه باقابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشا، تغییر اطلاعات و یا ممانعت از ایجاد اختلال در ارائه خدمت (سند راهبردی پدافند سایبری کشور:۱۳۹۰).

تعریف عملیاتی سناریوهای فضای سایبری: تصویرسازی از تهدیدات و روند تحولات آتی فضای سایبر مبتنی بر ویژگی‌های فضای سایبر مطلوب جمهوری اسلامی ایران.

سناریونویسی در مورد آینده فضای سایبر: سناریونویسی از مهم‌ترین کار ویژه‌های نهادهای ملی در حاکمیت‌های مدرن و هدف غایی آن شناسایی محتمل‌ترین آینده‌ها و تحقق سناریوهای مطلوب و پیشگیری از وقوع سناریوهای است.

آینده‌ها به‌صورت منطقی می‌تواند شامل آینده‌های ممکن، آینده‌های باورکردنی، آینده‌های محتمل و در نهایت آینده‌های مرجح و مطلوب باشد (عاشوری، حسینی ۱۳۹۳: ۴۶).

سناریوهای مشارکت کننده در تصمیم‌سازی و تصمیم‌گیری، باید محدود به سه آینده (در شرایط خاص چهار آینده) محتمل از بی‌نهایت آینده ممکن و باورکردنی باشد و بر این اساس است که سناریونویسی می‌کوشد سه آینده ممکن شامل محتمل‌ترین وضعیت، بدترین وضعیت (تهدید و آسیب) و بهترین وضعیت (قوت و فرصت) را پیش‌روی مراجع تصمیم‌گیر بگذارد.

در این پژوهش، با شناسایی زوج‌هایی از عدم قطعیت‌های اصلی مؤثر بر آینده فضای سایبر، نموداری دکارتی از دو عدم قطعیت رسم و از طریق آن در قالب چهار قسمت اصلی، سه سناریوی محتمل‌ترین، بهترین و بدترین آینده متصوره برای فضای سایبر شناسایی و تبیین خواهد شد. با توجه به شیوه تبیین نموداری، آینده‌های محتمل مختلفی وجود خواهند داشت که قطعاً از دید ما

برخی مطلوب و مرجح و برخی دیگر نامطلوب خواهند بود. آینده‌های مرجح بیشتر از آنکه دانش شناختی باشند؛ از نوع برانگیزاننده و برآمده از قضاوت‌های ارزشی بازیگران عرصه سیاسی اجتماعی خواهند بود (همان، ۴۴). به دلیل تعدد بازیگران و تفاوت و حتی تضاد میان قضاوت‌های ارزشی آنان، تناقض میان آینده‌های مرجح بازیگران اصلی (در این پژوهش جمهوری اسلامی ایران و آمریکا) است که کنش‌ها و تضادهای صحنه فضای سایبر را موجب می‌شود.

تجربه سایر کشورها در طراحی وضع مطلوب خود نشان می‌دهد، آنان با استفاده از روش‌ها و الگوهای مدیریت راهبردی از جمله تدوین چشم‌انداز، دکترین، بیانیه ارزش‌ها و به‌طورکلی مطلوبیت‌های راهبردی سعی در گفتمان‌سازی بر پایه اسناد بالادستی می‌کنند تا زیرمجموعه‌های آن کشورها با بهره‌گیری از آن موارد نسبت به تدوین راهبرد یا همان مرحله گذار از وضع موجود به وضع مطلوب به هم‌افزایی و همگرایی تلاش‌ها برسند. سناریوی مطلوب این پژوهش بر اساس تحلیل محتوای فرمایشات امام خامنه‌ای (مدظله‌العالی) می‌باشد. بر این اساس با شناسایی آینده‌های محتمل، نسبت این آینده‌ها با آینده مطلوب مدنظر حاکمیت جمهوری اسلامی ایران که منبعث از فرمایشات امام خامنه‌ای (مدظله‌العالی) است تبیین و ارزیابی خواهد شد؛ بنابراین مهم‌تر از تصویری که «دیگران»، از فضای سایبر ارائه می‌نمایند؛ تصویری است که «ما» به‌عنوان جمهوری اسلامی ایران؛ از این فضا و مطلوبیت‌های آن داریم و برای تحقق آن باید تلاش کنیم.

گام‌های سناریونویسی در این پژوهش: سناریونویسی اقدامی گام به گام است که بر اساس نظر پیتر شوارتز در کتاب هنر دورنگری، هفت گام اصلی دارد؛ اما در این پژوهش با توجه به الگوی بومی شده‌ای که علی ستاری‌خواه در کتاب آینده‌پژوهی و سناریونویسی کاربردی ارائه داده؛ گام‌های سناریونویسی زیر صورت گرفته است:

- گام صفر: ایجاد تمهیدات لازم
- گام یک: شناسایی بازیگران (بخش قلمرو تحقیق)
- گام دوم: شناسایی مؤلفه‌ها و عوامل تأثیرگذار (جدول شماره یک)
- گام سوم: شناسایی پیشران‌ها (بخش بررسی فناوری¬های برهم زن)
- گام چهارم: شناسایی عدم قطعیت‌ها (جدول شماره یک)
- گام پنجم: ترسیم اصول فضای مطلوب (چشم‌انداز) بررسی اسناد بالادستی و فرمایشات امام خامنه‌ای (مدظله‌العالی)

- گام ششم: تعیین عدم قطعیت‌های کلیدی (تعیین عدم قطعیت‌های مزدوج در شکل شماره یک و دو)
- گام هفتم: سناریونویسی
- گام هشتم: ارزیابی سناریوها و تبیین نسبت میان آن‌ها (بخش نتیجه‌گیری)

بایسته‌های سناریوی مطلوب فضای سایبر برای جمهوری اسلامی ایران

اسناد بالادستی نظام جمهوری اسلامی ایران: با توجه به اهمیت فضای سایبر از ابعاد گوناگون آن و خصوصاً توجه به تنوع کاربردها و تهدیدات موجود و آتی، لازم است بر اساس اسناد بالادستی ویژگی‌های فضای مطلوب سایبری جمهوری اسلامی ایران استخراج گردد. مطالعه مستندات موجود سیاست‌ها، قوانین و مقررات کشور و به‌ویژه چشم‌انداز بیست‌ساله، سند افتا، سیاست‌های کلی نظام در حوزه افتا، احکام مرتبط با توسعه فتا در برنامه توسعه اقتصادی، اجتماعی و فرهنگی و سایر اسناد مرتبط در دسترس، شالوده اصلی این پژوهش را شکل می‌دهد در این راستا و در تکمیل فعالیت‌های مرتبط با این مسئله یکی از مراجع معتبر در دستیابی به شناخت تهدیدات فضای سایبر می‌باشد. لذا آن دسته از قوانین، آیین‌نامه‌ها و اسناد بالادستی کشور که به‌نوعی به فضای سایبر کشور مرتبط می‌شوند، شناسایی، جمع‌آوری شده‌اند که برخی از مهم‌ترین کلیدواژه-های مورد استفاده از آن در جدول شماره ۱ درج شده است. مهم‌ترین این اسناد، شامل موارد زیر بوده است:

- سند چشم‌انداز ۲۰ ساله جمهوری اسلامی ایران با هدف تعیین چشم‌انداز کلی نظام جمهوری اسلامی ایران
- حکم امام خامنه‌ای(مدظله‌العالی) در تشکیل شورای عالی فضای سایبری برای ایجاد نقطه کانونی متمرکز در سیاست‌گذاری و تصمیم‌گیری در کشور
- سیاست‌های کلی نظام در حوزه فتا ابلاغی امام خامنه‌ای (مدظله‌العالی) با هدف تعیین خط‌مشی و جهت‌گیری نظام اسلامی در بخش فناوری اطلاعات و راهنمایی دستگاه‌های اجرایی، قانون‌گذار و نظارتی در بخش فتا
- (سند افتا) امنیت فضای تولید و تبادل اطلاعات کشور با هدف پرداختن به امنیت فضای تولید و تبادل اطلاعات به‌عنوان یک ضرورت و اولویت کشور به‌منظور تعیین نقش حاکمیت، جهت‌دهی فعالیت‌های اجرایی و هماهنگی، نظارت و هدایت بخش‌های

درگیر موضوع فوق و ایجاد نظامی منسجم در سطح ملی

- نظام جامع فناوری اطلاعات کشور ابلاغی دولت جمهوری اسلامی ایران با هدف کمک به توسعه نظام‌مند فناوری اطلاعات کشور در رسیدن به اهداف چشم‌انداز ۲۰ ساله نظام جمهوری اسلامی ایران

فرمایشات امام خامنه‌ای (مدظله‌العالی): در این بخش از پژوهش، با تبیین فرمایشات معظم له در خصوص ویژگی‌ها و اهمیت این فضا در راستای ایجاد فضای سایبر مطلوب که از ضرورت‌های اساسی این پژوهش می‌باشد، تلاش می‌شود طبق الگوی مدیریت راهبردی؛ فرمایشات امام خامنه‌ای (مدظله‌العالی) مورد تحلیل محتوای قرار گیرد و موارد ذیل به‌عنوان فرمایشات کلیدی و راهگشای مدیریت این فضا و همچنین یکی از ارکان اصلی مبانی نظری این پژوهش استخراج گردید.

ویژگی‌های فضای سایبر در بیانات امام خامنه‌ای (مدظله‌العالی):

- ✓ فرصت و ظرفیت هدایت بشر (امام خامنه‌ای (مدظله‌العالی): ۱۳۹۱/۷/۱۹)
- ✓ پیشران تحول در زندگی انسان (امام خامنه‌ای (مدظله‌العالی): ۱۳۹۶/۶/۱۴)
- ✓ قدرت نرم فضای سایبر (امام خامنه‌ای (مدظله‌العالی): ۱۳۹۴/۴/۱۶)
- ✓ سیاست‌های مدیریت فضای سایبری در بیانات معظم له
- ✓ مواجهه هوشمندانه و مقتدرانه با تحولات پرشتاب این عرصه، برای استفاده از فرصت‌ها مقابله با آسیب‌ها و تهدیدات آن.
- ✓ حضور فعال و تأثیرگذار در فضای سایبری، تمرکز در تصمیم‌گیری، جدیت در اجرا بدون از دست دادن زمان، هماهنگی میان دستگاه‌ها و پرهیز از موازی کاری و تعارض.
- ✓ کسب جایگاه برتر منطقه در توسعه دولت الکترونیک در بستر شبکه ملی اطلاعات.
- ✓ توسعه محتوی در فضای سایبری بر اساس نقشه مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی (همان).
- ✓ تکمیل و توسعه شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی
- ✓ حضور مؤثر و هدفمند در تعاملات بین‌المللی فضای سایبری (امام خامنه‌ای (مدظله‌العالی): ۱۳۹۴/۴/۱۶).

راهبردهای مدیریت فضای سایبر در کلام امام خامنه‌ای (مدظله‌العالی)

- ✓ ارتقاء جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی ... در جهت شکل‌دهی به قوانین مرتبط با فضای سایبری در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه. (همان)
- ✓ تسریع در راه‌اندازی شبکه ملی اطلاعات و نظارت مستمر بر مراحل آن. (همان)
- ✓ اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه، حفظ حریم خصوصی و مقابله با نفوذ. (همان)
- ✓ ترویج هنجارها، ارزش‌ها و سبک زندگی اسلامی ایرانی و ارتقای فرهنگ کاربری (همان)

بررسی اسناد بالادستی کشورهای غربی در مورد سناریوهای پیش روی فضای سایبر: با توجه به اینکه راهبرد نویسی و شناخت آینده با هدف تحقق فضای مطلوب صورت می‌گیرد؛ اسناد راهبردی کشورها صرفاً برای شناخت آینده به نگارش درنیامده است؛ بلکه هدف اصلی آن ساخت آینده مطلوب در پرتو شناخت آینده‌های محتمل است؛ بنابراین برای شناخت آینده‌های محتمل و آینده مطلوب رقبا بررسی این اسناد امری لازم و حیاتی است.

راهبرد بین‌المللی آمریکا برای فضای سایبر: در این سند هدف ایالات‌متحده آمریکا به‌صورت بین‌المللی؛ ارتقاء زیرساخت ارتباطی و اطلاعاتی باز، سازگار، امن و پایدار که پشتیبان کسب‌وکار و تجارت، تقویت‌کننده امنیت بین‌الملل و همچنین تقویت‌کننده آزادی بیان و خلاقیت باشد را انجام خواهد کرد. در بخش ارزش‌ها بر حق دفاع مشروع و در بخش سیاست‌های ابلاغی این سند بر آماده شدن برای چالش‌های امنیتی قرن ۲۱، ایجاد و ارتقاء ائتلاف نظامی برای مقابله با تهدیدات بالقوه در فضای سایبری و گسترش همکاری فضای سایبری با متحدان و شرکاء برای افزایش امنیت دسته‌جمعی تأکید شده است. در این سند، لزوم حفظ حاکمیت آمریکا بر اینترنت از طریق ارتقای زیرساخت مؤثر و فراگیر مورد توجه قرار گرفته است (International strategy for cyber space,2011).

سند امنیت فضای سایبری؛ وزارت امنیت داخلی آمریکا: وزارت دفاع آمریکا به فضای سایبری به‌منزله یک قلمرو عملیاتی نگاه کرده و خود را برای استفاده هرچه تمام‌تر از پتانسیل‌های آن، سازمان‌دهی، آماده‌سازی و تجهیز می‌کند. با این‌که فضای سایبری توسط انسان ساخته شده است،

این فضا همانند زمین، دریا، هوا و فضا قلمرو مناسبی برای فعالیت‌های وزارت دفاع آمریکا است (US cyber security strategy, DHS,2014).

راهبرد امنیت سایبری انگلیس: چشم‌انداز ارائه شده در این سند برای انگلستان؛ ایجاد ارزش‌های بزرگ اقتصادی و اجتماعی از فضای سایبری پر جنب‌وجوش و انعطاف‌پذیر و امن و افزایش رفاه موجبات ارتقاء امنیت ملی، پیشرفت و یک جامعه قوی را فراهم آورد. در حوزه ارزش‌های ارائه شده در سند، رویکرد دولت انگلیس به امنیت ملی به‌طور مشخص مبنی بر ارزش‌هایی همچون حقوق بشر، حکومت قانون، دولت پاسخ‌گو، عدالت، آزادی، تساهل و ایجاد فرصت‌های برابر برای همگان عنوان شده است. در اهداف سند نیز مقابله با جرائم اینترنتی، ایجاد انعطاف‌پذیری پایداری نسبت به حملات اینترنتی و ایجاد توانایی بالاتر برای حفاظت از منافع ملی در فضای سایبری با تمرکز مضاعف بر منابع موجود انگلیس و کمک به شکل دادن به فضای سایبری باز و حمایت از جوامع باز عنوان شده است (UK cyber security strategy, 2016).

راهبرد امنیت فضای سایبر اتحادیه اروپا: در این سند در حوزه ارزش‌ها بر ترویج آزادی بر خط و ایجاد اطمینان از توجه به حقوق اساسی و تشویق ارزش‌های اتحادیه و در حوزه سیاست‌ها بر محافظت فضای سایبر از وقایع و فعالیت‌های بدخواهانه و تأمین جامعیت و امنیت اطلاعات تأکید شده است (Cybersecurity Strategy of the European Union,2013).

مطالعه تطبیقی اسناد بالادستی کشورها؛ تناقض چشم‌انداز مطلوب جمهوری اسلامی ایران با جبهه استکبار: در مطالعه تطبیقی آشکار گردید که کشورهای تأثیرگذار در این فضا این حوزه را جزئی از حوزه‌های قدرت و قلمرو عملیاتی در نظر گرفته‌اند، فلذا امنیت این حوزه را در درون توسعه آن طراحی نموده‌اند و به‌غیراز آمریکا، دیگر کشورها اسناد بالادستی در حوزه راهبری استراتژیک این فضا نداشته‌اند و تماماً اسناد توسعه و مدیریت این فضا را در اسناد راهبردی امنیت و دفاع ذکر نمودند. اما از آنچه در بررسی اسناد بالادستی و فرمایشات مقام معظم رهبری به دست آمد، می‌توان این‌گونه نتیجه‌گیری کرد که به‌طور کلی می‌توان پارادایم و گفتمان مطلوب نظام اسلامی برای فضای سایبر با آنچه نظام سلطه در حال طراحی آن می‌باشند در تعارض است. دو پارادایم اصلی در راهبری فضای سایبر را می‌توان این‌گونه تصور نمود:

پارادایم لیبرال دموکراسی که معتقد است اساساً رسانه مدرن متعلق به جهان مدرن است و امر قدسی در پیچیدگی‌های جهان مدرن، قابل دوام نیست. اصلاً عرصه مدرن، عرصه مفاهیم قدسی

نیست. ادعای آن‌ها این بود که هیچ روزنه روشنی برای مداخله در روند و مضمون فضای رسانه‌ای جدید و مواجه با این نظم سیاسی و اقتصادی جهان وجود ندارد و ممکن نیست کسانی با گفتارهای قدسی و انقلابی، یعنی هم در جهت براندازی نظم حاکم بر جهان و هم با نیروی معنوی – دینی برای ساختارشکنی نظم سکولار که حاکم بر سیاست و اقتصاد در جهان بود، وارد میدان شوند.

در پارادایم دوم که پارادایم انقلاب اسلامی است ضرورت بهره‌گیری از فضای سایبری منطبق بر شعارهای اصلی آن پارادایم یعنی «استقلال، آزادی، جمهوری اسلامی» و «نه شرقی، نه غربی، جمهوری اسلامی» آشکار است. این شیوه جدید از تفسیر شعارهای عمیق و راهبردی انقلاب اسلامی متناسب با شکل‌گیری نوعی جدید از فضای زندگی یعنی فضای سایبری رویکردی مهم در نحوه مدیریت فناوری را به دنیا معرفی خواهد کرد.

بنابراین آنچه در این پژوهش به‌عنوان فضای سایبر مطلوب جمهوری اسلامی ایران. تعریف و تبیین می‌شود، مبتنی بر پارادایم انقلاب اسلامی است. این بدان معنی است که زندگی در فضای سایبری استمرار همین زندگی عینی است در بستر فناوری اطلاعات و ارتباطات، فلذا می‌بایست مبتنی بر فرآیند تحقق تمدن نوین اسلامی راهبری شود. سناریوهای محتمل نیز مبتنی بر روندهای فضای سایبر و متغیرهای تأثیرگذار بر آن ساماندهی و تصویرسازی می‌گردد.

سناریوی مطلوب در چارچوب پارادایم انقلاب اسلامی و الگوی اسلامی – ایرانی پیشرفت

در بینش حکیمانه مقام معظم رهبری (مدظله‌العالی) پیشرفت با توسعه غربی ماهیتاً متفاوت هست. ایشان در تبیین این مفهوم اظهار داشتند: «توجه داشته باشیم که مراد ما از پیشرفت، پیشرفت با الگوی غربی نیست. دستور کار قطعی نظام جمهوری اسلامی، دنبال کردن الگوی پیشرفت ایرانی- اسلامی است. ما پیشرفت را به شکلی که غرب دنبال کرد و پیش رفت، نمی‌خواهیم» (امام خامنه-ای (مدظله‌العالی): ۱۳۹۲).

همان‌طور که امام خامنه‌ای (مدظله‌العالی) فرمودند: هدف والا و میانی الگوی اسلامی- ایرانی پیشرفت تحقق تمدن نوین اسلامی است که این الگو می‌بایست سرمشق تمام اسناد بالادستی حتی سند چشم‌انداز باشد. راهبری فضای سایبری نیز از این اصل مستثنی نیست. این بدان معنی است که فضای سایبر مطلوب به‌نوبه خود می‌بایست متضمن تحقق تمدن نوین اسلامی باشد.

روندهای تأثیرگذار بر آینده فضای سایبری:

- ✓ ساختار اینترنت
- ✓ نوآوری‌های روزافزون
- ✓ درهم آمیختگی و نفوذ وسیع
- ✓ موانع بر سر راه امنیت کامل در سایبری

مهم‌ترین عنصر برای شناخت عدم قطعیت‌های آینده در فضای سایبر این است که بدانیم اصولاً فضای کاملاً امن در این حوزه امری موهوم است. این سه عامل ایجاد ناامنی در فضای سایبر موانعی را برای امنیت ایجاد کرده که حتی صاحبان اصلی اینترنت نیز باید با آن‌ها دست و پنجه نرم کنند تا بتوانند سیاست‌های مناسبی در جهت مقابله با آن‌ها اتخاذ کنند. مهم‌ترین این موانع در ادامه بررسی می‌شوند.

- ✓ سرعت و از میان رفتن فاصله‌ها
- ✓ بزرگی حجم و سختی
- ✓ دسترسی آسان و بدون مانع
- ✓ نبود شفافیت
- ✓ هنجارهای رفتاری غیرواضح
- ✓ احاطه حمله و یورش

پیشران‌های فضای سایبر: با بررسی مؤسسات آینده‌پژوهی مانند گارتنر، آی بی ام، پیو که به معرفی فناوری‌های نوظهوری می‌پردازد؛ موارد زیر به‌عنوان روندهای مهم تأثیرگذار بر ساخت آینده، احصاء شده است:

- ✓ رایانش ابری
- ✓ خودکارسازی و هوش مصنوعی
- ✓ دستگاه‌های قابل حمل
- ✓ ساختار اینترنت
- ✓ تهدیدات نوظهور
- ✓ حمله به زیرساخت‌های حیاتی
- ✓ رایانش موبایلی

- ✓ اعتماد به زیرساخت‌ها مانند کلید عمومی
- ✓ ابر دیتاها
- ✓ اینترنت اشیا
- ✓ سایبری سازی‌ها (Gartner,2014).

سناریوهای تهدیدات سایبری:

همان‌طور که ذکر شد برای بررسی سناریوهای تهدیدات سایبری می‌بایست سناریوهای ما و دیگران (دشمن) مورد تحلیل و کاوش قرار گیرد. شناخت عدم قطعیت‌ها، پیشران‌ها و مؤلفه‌های مؤثر بر فضای سایبر بر اساس الگوی تحرکات تهدیدگر و فعالیت‌های خودی مورد احصا قرار گرفت که نمونه‌ای از آن در جدول زیر ارائه شده است.

جدول شماره ۱ کلیدواژه‌های مرتبط با تهدیدات سایبری

مفهوم	ارجاع	منبع
نفوذ	مبانی نظری– دشمن‌شناسی	امام خامنه‌ای (مدظله‌العالی) در دیدار با مدرسان، فضلا و طلاب حوزه علمیه مشهد ۶۸/۴/۲۰
	مبانی نظری– روندهای فناوری در فضای سایبر	World Future Society, 2014
	ادبیات تحقیق– تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق– تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
منشأ	مبانی نظری– دشمن‌شناسی	امام خامنه‌ای (مدظله‌العالی) در دیدار گروه کثیری از بسیجیان سراسر کشور ۷۵/۸/۳۰
	ادبیات تحقیق– تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
	مبانی نظری – طبقه‌بندی تهدیدهای سایبری در گزارش کنگره آمریکا	USGAO,2010
	مبانی نظری– دسته‌بندی هوارد از حمله سایبری	Cohen,2009
	مطالعه تطبیقی– انگلیس	Uk cyber security 2014
هم‌پیمانان	ادبیات تحقیق– تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
دانش تخصصی فضای مجازی	مفاهیم و ادبیات تحقیق– ژئوپلیتیک فضای سایبر	احمدی پور– ابعاد ژئوپلیتیک فضای سایبری در عصر فناوری اطلاعات–۹۱
	ادبیات تحقیق– تاریخچه و مفاهیم	Sandia, 2012, cyber metrics

دانش جنبی	ادبیات تحقیق- تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
تمایل		
مفهوم	**ارجاع**	**منبع**
پافشاری	مفاهیم و ادبیات تحقیق – سازمان معنایی تهدید	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
	ادبیات تحقیق- تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
	مفاهیم و ادبیات تحقیق- شاخص انگیزه در طبقه‌بندی تهدیدات	افتخاری، اصغر -۱۳۹۲- برآورد تهدید رویکردی نظام واره
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
زمان	مفاهیم و ادبیات تحقیق – سنجش شدت تهدیدات	افتخاری، اصغر -۱۳۹۲- برآورد تهدید رویکردی نظام واره
	ادبیات تحقیق- تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
سابقه تهدید	ادبیات تحقیق- تاریخچه و مفاهیم	The MITRE Corporation,2012
قابلیت /توانایی	مفاهیم و ادبیات تحقیق- ظرفیت‌های درونی	افتخاری، اصغر -۱۳۹۲- برآورد تهدید رویکردی نظام واره
	ادبیات تحقیق- تاریخچه و مفاهیم	The MITRE Corporation,2012
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
احتمال موفقیت	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
شدت تهدید سایبری	مبانی نظری – تقسیم‌بندی سازمان پدافند غیرعامل	ارزیابی تهدیدات سایبری – سازمان پدافند غیرعامل
	ادبیات تحقیق- تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
نهان‌کاری	مبانی نظری – مطالعه تطبیقی آمریکا	America ‘s cyber future 2011
	ادبیات تحقیق- تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
جذابیت	ادبیات تحقیق- تاریخچه و مفاهیم	America ‘s cyber future 2011
	ادبیات تحقیق- تاریخچه و مفاهیم	آیین‌نامه فنی سایبری، پدافند غیرعامل ۱۳۸۸
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
تبعات منفی	ادبیات تحقیق- تاریخچه و مفاهیم	The MITRE Corporation,2012
	مبانی نظری – دشمن‌شناسی	مقام معظم رهبری (مدظله‌العالی)- در مراسم بیعت مردم زنجان ۶۸/۴/۱۵

	ادبیات تحقیق- تاریخچه و مفاهیم	آیین‌نامه فنی سایبری، پدافند غیرعامل ۱۳۸۸
	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
تمایل	ادبیات تحقیق- تاریخچه و مفاهیم	The MITRE Corporation,2012
تمایل	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل ۱۳۹۱
افشا	ادبیات تحقیق- تاریخچه و مفاهیم	The MITRE Corporation,2012
آسیب‌پذیری		
مفهوم	**ارجاع**	**منبع**
بازدارندگی	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
بازدارندگی	ادبیات تحقیق- تاریخچه و مفاهیم	جمعی از محققین، ۱۳۹۵
بازدارندگی	ادبیات تحقیق- تاریخچه و مفاهیم	سیاست‌های کلی نظام در حوزه پدافند غیرعامل
بازدارندگی	ادبیات تحقیق- تاریخچه و مفاهیم	سند چشم‌انداز ایران در ۱۴۰۴- ۱۳۸۲
بازدارندگی	ادبیات تحقیق- تاریخچه و مفاهیم	نظام جامع فناوری اطلاعات- ۱۳۸۶
ظرفیت انطباق	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
ظرفیت انطباق	ادبیات تحقیق- تاریخچه و مفاهیم	حکم امام خامنه‌ای (مدظله‌العالی) در تشکیل شورای عالی فضای مجازی
تاب‌آوری	ادبیات تحقیق- تاریخچه و مفاهیم	جمعی از محققین، ۱۳۹۵
تاب‌آوری	ادبیات تحقیق- تاریخچه و مفاهیم	سیاست‌های ابلاغی مقام معظم رهبری(مدظله‌العالی) در حوزه فتا
تاب‌آوری	ادبیات تحقیق- تاریخچه و مفاهیم	The DOD cyber strategy, 2015
تاب‌آوری	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
تاب‌آوری	ادبیات تحقیق- تاریخچه و مفاهیم	جمعی از محققین، ۱۳۹۵
پیامد تهدید سایبری		
مفهوم	**ارجاع**	**منبع**
عمق تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
عمق تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
عمق تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	باری بوزان ۱۳۷۸
شدت تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
شدت تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	باری بوزان ۱۳۷۸
گستره تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	عبدالله خانی، علی – ۱۳۸۶- تهدیدات امنیت ملی
گستره تهدید سایبری	ادبیات تحقیق- تاریخچه و مفاهیم	باری بوزان ۱۳۷۸

بنا بر مفاهیم به دست آمده از جدول فوق سناریو بر اساس دو عدم قطعیت «منابع» و «تمایل» ناظر به تحرکات سایبری دشمن است و سناریو بر اساس دو عدم قطعیت «آسیب‌پذیری دارایی» و «پیامد تهدیدات » نیز ناظر به اقدامات طرف خودی (تهدید شونده) است.

عدم قطعیت‌های فوق که مبنای سناریونویسی در این تحقیق است؛ در چند مرحله به دست آمد. ابتدا روندها و پیشران‌های مؤثر بر موضوع تحقیق، خوشه‌بندی و بر اساس نمره‌دهی جامعه آماری پژوهش، تعیین اولویت شد. در مرحله بعد با دعوت از خبرگان، از مؤلفه‌های به‌دست‌آمده، زوج‌هایی از عدم قطعیت که قابلیت سناریونویسی را داشته باشند؛ استخراج گردید.

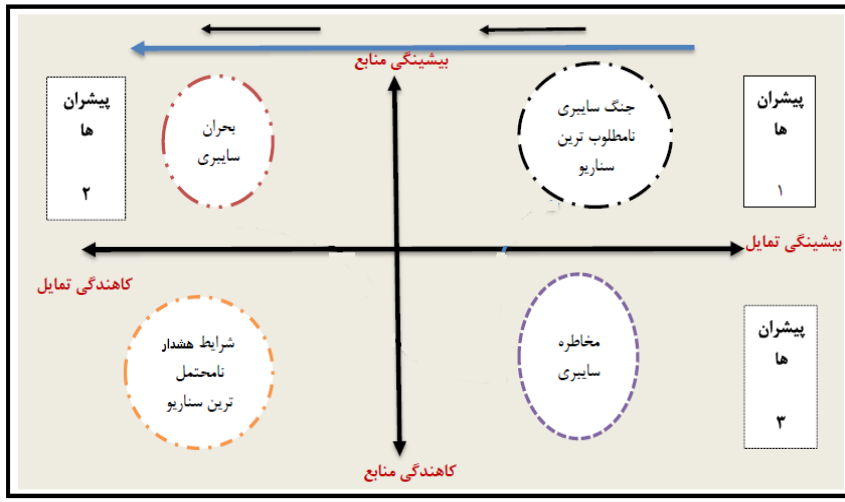
هرچند سناریوهای این دو حوزه به این دلیل به‌صورت مستقل با نخبگان پژوهش به بحث گذاشته شد؛ به‌تنهایی نیز قابل فهم و تجزیه تحلیل است و هرکدام هویت مستقل دارند؛ اما در نگاه کلان ارزیابی تهدیدات سایبری باید یک رابطه دو سویه متأثر از هم را نیز در نظر گرفت. این دو، رابطه تعاملی با یکدیگر داشته و با یکدیگر معنی کامل‌تری می‌یابند و در کنار هم بهتر فهمیده می‌شوند. مثلاً، افزایش آسیب‌پذیری دارایی‌ها بر تمایل دشمن برای بهره‌برداری از تهدید تأثیر افزایشی خواهد داشت و یا اینکه پیامدهای تهدید، عنصر تأثیرگذاری در انجام یا عدم انجام تهدید خواهد بود.

سناریوهای تحرکات دشمن (تهدیدگر)

با توجه به اینکه «ما» بر متغیرهای اصلی حوزه دشمن که شامل منابع و تمایل دشمن برای انجام تهدید سایبری است، امکان تأثیرگذاری نسبی داریم، بررسی سناریوهای این بخش علاوه بر اهمیت ذاتی موضوع، جهت کمک به حوزه خودی و همچنین واکنش لازم و تأثیر غیرمستقیم بر متغیرهای منابع و تمایل اهمیت حیاتی دارد. در اینجا دو نکته قابل ذکر است:

اول آنکه با توجه به اینکه فضای سایبر آمیخته با عدم قطعیت است لذا چرخه سناریویی را شاهد خواهیم بود که احتمال تغییر یک سناریو به سناریوی دیگر را فراهم می‌کند.

دوم آنکه نامحتمل‌ترین سناریو یا همان سناریو مطلوب وجود خارجی نخواهد داشت. چراکه در شرایط تقاطع دو عدم قطعیت کاهندگی تمایل و کاهندگی منابع تهدیدگر روی خواهد داد.



(شکل ۱) سناریوهای تهدیدات سایبری مبتنی بر جدول شماره ۱

سناریوی شماره یک جنگ سایبری: (نامطلوب‌ترین سناریو)

این ابر سناریو که زیرسناریوهای متعددی ذیل آن تعریف می‌شود در شرایط میل عدم قطعیت‌های تمایل و منابع تهدیدگر به سمت بیشینگی، تحقق می‌یابد. در این شرایط موجودیت نظام سیاسی، تمامیت ارضی و بقاء جمعیت کشور مورد هدف دشمن قرار دارد. پیشران‌های نامطلوب‌ترین سناریو در حوزه دشمن شامل موارد زیر است:

- افزایش روزافزون تخاصم استکبار جهانی با نظام اسلامی (بیشینگی تمایل)
- کاهش شاخصه‌های پدافند غیرعامل در فضای سایبری (بیشینگی تمایل)
- افزایش تنیدگی فضای سایبر با ابعاد زندگی بشری (بیشینگی منابع)
- نفوذ دشمن در بدنه مدیریت راهبردی فضای سایبر به‌منظور انفعال در راهبری این فضا (بیشینگی منابع)

سناریوی شماره دو بحران سایبری: (سناریوی محتمل)

در شرایط قرار گرفتن در موقعیت‌های بیشینگی منابع و کاهندگی تمایل شاهد ابر سناریوی بحران سایبری خواهیم بود. پیامدهای این وضعیت کمتر از جنگ سایبری خواهد بود. پیشران‌های این سناریو عبارتند از:

- افزایش توان بازدارندگی سایبری و دفاع فعال جمهوری اسلامی ایران (کاهندگی تمایل)

- مشغولیت بین‌المللی استکبار جهانی به دستورکارهایی غیر از موضوع ایران (کاهندگی تمایل)
- بهره‌گیری از فناوری‌های برهم زن از سوی دشمن در افزایش دسترسی به زیرساخت‌های حیاتی (بیشینگی منابع)
- به دست گرفتن مدیریت فضای سایبری از سوی جریان‌های لیبرال داخل کشور (بیشینگی منابع)

البته در همه سناریوها جمع‌آوری اطلاعات از شاخصه‌های فعالیت دشمن می‌باشد، اما در این سناریو این مهم برجسته‌تر می‌باشد. آنچه در این سناریو باید مدنظر راهبران فضای سایبری باشد توجه جدی به شگفتی‌سازها و علائم ضعیف تغییر است، مانند تحولات اجتماعی و موج‌های انحرافی حاصل از آن مانند آنچه در فتنه سال ۸۸ شاهد بودیم. یا جنگ‌های نیابتی جمهوری اسلامی ایران با رژیم اشغالگر صهیونیستی که تمایل تهدیدگران غربی را بیشتر خواهد کرد.

سناریوی شماره سه مخاطره سایبری:

این سناریو محصول تقاطع دو عدم قطعیت بیشینگی تمایل و کاهندگی منابع است. در این شرایط احتمال بهره‌برداری یک تهدید سایبری، از آسیب‌پذیری سایبری موجود دریک سرمایه سایبری بالا است. پیشران‌های این سناریو عبارتند از:

- امن‌سازی زیرساخت‌های داخلی (کاهندگی منابع)
- ایجاد نهادهای بین‌المللی و همچنین قانون‌گذاری برای پیگیری جرائم سایبری از سوی جبهه استکبار (مانند شورای امنیت سازمان ملل) (بیشینگی تمایل)

سناریوی شماره چهار هشدار سایبری:

این سناریو محصول تقاطع دو عدم قطعیت کاهندگی منابع و کاهندگی تمایل می‌باشد. آنچه اهمیت دارد آنکه این شرایط به دلیل تخاصم دائمی جمهوری اسلامی ایران با نظام سلطه شرایط تحقق را پیدا نخواهد کرد و ما همیشه ضریبی از تمایل و منابع را در حوزه دشمن شاهد خواهیم بود. ممکن است شرایط این سناریو بیشتر در ارتباط با کشورهای غیرمتخاصم با ایران مانند کره جنوبی باشد.

تصمیم‌سازان و تصمیم‌گیران باید شرایط لازم برای تحقق سناریو شرایط هشدار را فراهم کنند. به عبارت دیگر چرخه تغییرات را به کاهندگی تمایل و کاهندگی منابع سوق دهند. آنچه باید مورد

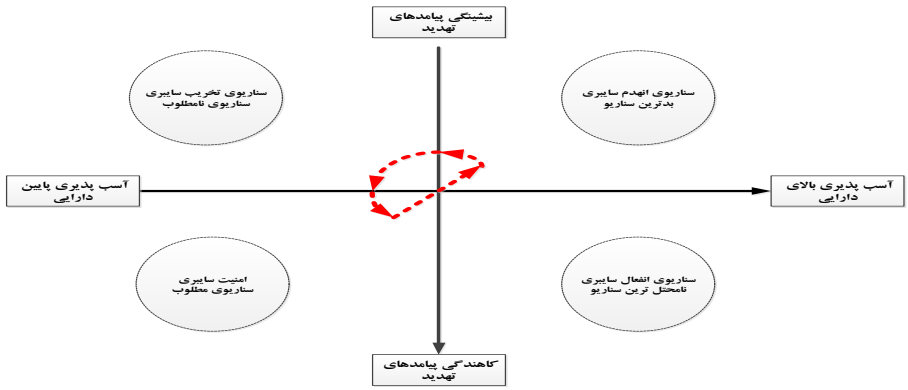
توجه قرار گیرد آنکه ضرورتاً سناریوها به‌صورت تدریجی تحقق پیدا نمی‌کنند و ممکن است ناگهانی محقق شوند.

تحلیل سناریوهای تهدیدگر:

سناریوی شماره ۱ در شکل ۱ که بیشینگی منابع و تمایل با هم تقاطع داشتند، سناریوی جنگ سایبری را داشتیم. در شرایط بیشینگی آسیب‌پذیری دارایی‌ها و پیامد تهدید نیز همین‌طور سناریوی جنگ سایبری قابل تصور است. بالعکس در شرایط کاهندگی تمایل و منابع (سناریوی شماره ۳) در شکل ۱ وضعیت هشدار داشتیم که به‌صورت هم‌عرضی این سناریو با سناریویی که ناشی از تقاطع دو عدم قطعیت کاهندگی آسیب‌پذیری و پیامد تهدید است هم‌راستا می‌باشد.

سناریوهای حوزه خودی (تهدید شونده): همان‌گونه که ذکر شد سناریو بر اساس دو عدم قطعیت «آسیب‌پذیری دارایی» و «پیامد تهدیدات» نیز ناظر به اقدامات طرف خودی (تهدید شونده) است. از منظر ارائه الگوی عملکردی به تصمیم گیران کشور، با توجه به تأثیرگذاری بالای اقدامات جبهه خودی بر متغیرهای این عرصه؛ سناریوهای این بخش نقش مهمی در خروج از انفعال در مقابل تهدیدات خواهد داشت.

پیش‌بینی آینده نحوه برخورد تهدید سایبری با دارایی‌ها مستلزم بررسی آسیب‌پذیری‌های دارای سایبری و همچنین پیامد تحقق آن تهدیدات می‌باشد، چراکه تهدیدات به خودی خود و فارغ از محیط دارایی‌ها فاقد خطر می‌باشند. لذا می‌بایست بر اساس شاخص‌های آسیب‌پذیری دارایی‌ها و پیامد تحقق تهدیدات، اطلاعات جمع‌آوری و مورد تحلیل قرار گیرد.



شکل شماره ۲- سناریوهای حوزه خودی برگرفته از جدول شماره ۱

سناریوی اول؛ بدترین سناریوی ممکن (برخورد منفعلانه با تهدیدات متصوره)

در حوزه ارزیابی تهدیدات، سناریوی فرضی اول حاصل تقاطعِ دو عدم قطعیت بیشینگی پیامد تهدید و آسیب‌پذیری بالای دارایی می‌باشد. تحقق این سناریوی فرضی به این معناست که تهدیدات بیرونی قابلیت اعمال بالایی بر دارایی سایبری ما خواهد داشت. و در نقطه مقابل اقدام عاجل و بازدارنده‌ای از سوی ما نیز متصور نیست.

تحقق این سناریو بدان معناست که در حوزه دارایی‌های سایبری پدافند غیرعامل جدی گرفته نشده است و دارایی‌های ما امکان تاب‌آوری و بازیابی (انطباق) در مقابل تهدیدات متصوره را ندارند. با توجه به هم‌ارز بودن سناریوهای طرف خودی و سناریوهای دیگران؛ باید در تطبیق این دو سناریو گفت که سناریوی اول بر افزایش تمایل دشمنان تأثیر جدی دارد و در جدول محاسباتی آنان؛ به افزایش مطلوبیت حمله سایبری منجر خواهد شد.

برای جلوگیری از انفعال سایبری، (در صورت وقوع این سناریو؛ غیرقابل اجتناب است) باید مؤلفه‌هایی که این وضعیت را ایجاد می‌کند؛ قبل از تحقق تهدید؛ ارتقاء یابند. پدافند غیرعامل، تاب‌آوری و امکان بازیابی سه مؤلفه اصلی برای جلوگیری از تحقق این سناریو می‌باشد.

سناریوی دوم: هشدار سایبری

در سناریوی فرضی دوم؛ تقاطع کاهندگی آسیب‌پذیری با بیشینگی پیامد تهدیدات؛ ما با شرایطی روبرو هستیم که مشکل اصلی نه در پدافند غیرعامل؛ بلکه در تاب‌آوری و قدرت بازیابی است؛ بنابراین تحقق این سناریو هرچند بدترین سناریو نخواهد بود؛ اما در نوع خود سناریوی نامطلوبی به حساب می‌آید.

سناریوی سوم: وضعیت عادی (مطلوب‌ترین سناریو)

در سناریوی سوم که حاصل تقاطع کاهندگی آسیب‌پذیری و کاهندگی پیامد تهدیدات است؛ با وضعیت عادی در فضای سایبر روبرو هستیم. در این بخش با توجه به فقدان تهدید؛ مشکل فقط تاب‌آوری است. واقعیت آن است که سناریوی سوم؛ در شرایط فعلی روابط جمهوری اسلامی ایران با نظام سلطه، سناریوی غیرمحتملی محسوب می‌شود. این سناریو بیشتر برای کشورهایی مانند سوئیس، سوئد و فنلاند موضوعیت دارد که اولاً در روابط خارجی خنثی و تابع روندهای نظام بین‌الملل عمل می‌کنند و ثانیاً توانایی فنی لازم برای افزایش استانداردهای لازم در پدافند غیرعامل و بازیابی را دارند.

سناریوی چهارم؛ انفعال سایبری: غیرمحتمل‌ترین سناریو

سناریوی چهارم که حاصل تقاطع بیشینگی آسیب‌پذیری و کاهندگی پیامدهای تهدیدات است؛ شرایطی است که در آن علی‌رغم ضعف جدی در مؤلفه‌های پدافند غیرعامل، تاب‌آوری و بازیابی شاهد وقوع تهدیدات جدی نخواهیم بود. این سناریو بیشتر برای دولت‌های دست نشانده مانند عربستان موضوعیت دارد که علی‌رغم آسیب‌پذیری بالا از جانب نظام سلطه، به دلیل آنکه در موضع اتحاد و دست نشاندگی با آنان قرار دارد؛ با تهدیدات سایبری روبرو نیست. با توجه به حجم دشمنی‌های علیه جمهوری اسلامی ایران این سناریو نیز سناریوی غیرمحتملی برای تبیین روندهای آتی ارزیابی تهدیدات سایبری علیه نظام اسلامی خواهد بود. در سناریوهای ارزیابی تهدیدات سایبری باید گفت که سناریوی ۳ و ۴ برای جمهوری اسلامی ایران موضوعیت ندارد؛ بنابراین در ارزیابی واقع‌بینانه، سناریوهای محتمل ۱ و ۲ به‌عنوان روندهای فعلی شناخته می‌شود.

نتیجه‌گیری:

نوآوری‌های سریع و مکرر، بازیگران مختلف را (اعم از تهدیدآفرین و تهدید شونده) در فضای عدم قطعیت قرار داده و شناسایی روندهای احتمالی آینده و پیش‌رانها را به امری حیاتی تبدیل کرده است. این پژوهش با شناسایی این متغیرها و عدم قطعیت‌ها، سناریوهایی برای مدیریت تهدیدات طراحی کرده است. در سناریوهای عنصر تهدیدگر (دشمن) سه سناریوی محتمل و یک سناریوی غیرمحتمل و در سناریوهای عنصر تهدید شونده (ما) نیز سه سناریوی محتمل و یک سناریوی غیرمحتمل مورد ارزیابی قرار گرفته است.

با بررسی سناریوهای محتمل و تبیین نسبت آن با سناریوی مطلوب جمهوری اسلامی ایران (که بر اساس تحلیل محتوای اسناد بالادستی و فرمایشات امام خامنه‌ای (مدظله‌العالی) به‌وسیله پنل نخبگان پژوهش، به دست آمده است) مشخص شد نه در حوزه تهدیدگر و نه در حوزه خودی، سناریوی مطلوب جمهوری اسلامی ایران در میان سناریوهای محتمل؛ نیست. این گزاره را در نظام تصمیم‌سازی راهبردی باید این‌گونه تفسیر کرد که روندهای کنونی فضای سایبر به سمت الگوهای ترسیم شده جمهوری اسلامی ایران حرکت نمی‌کند و باید با ایجاد عزم عمومی، استفاده از فرصت‌ها و مقابله با چالش‌ها، تغییر روندهای کنونی را در دستور کار قرار داد. به معنای دیگر برخورد منفعلانه با نوآوری‌های سریع و مکرر بستری مطلوب برای تهدیدگران جمهوری اسلامی

ایجاد خواهد کرد و در نقطه مقابل، تعامل فعالانه، ایجابی و مشارکتی در نوآوری‌های فضای سایبر زمینه‌های فرصت‌آفرین برای جمهوری اسلامی ایران در بر خواهد داشت.

در این میان نکته مهمی که نباید از آن غفلت کرد توسعه زیرساخت‌های غیربومی است که هم بر سناریوهای تهدیدگر (دشمن) و هم بر سناریوهای خودی (تهدید شونده) تأثیر معنی‌داری خواهد داشت و مؤلفه «منابع» را به نفع تهدیدگر خارجی و متغیر «آسیب‌پذیری دارایی‌ها» را به ضرر نیروی خودی تغییر خواهد داد.

منابع:

- امام خامنه‌ای (مدظله‌العالی)، ***مجموعه بیانات***، قابل دسترسی در: www.khamenei.ir
- امام خامنه‌ای (مدظله‌العالی)، ***حکم انتصاب اعضای جدید شورای عالی فضای سایبری برای یک دوره چهارساله***، (۱۳۹۶/۶/۱۴).
- امام خامنه‌ای (مدظله‌العالی)، ***دیدار رئیس و اعضای شورای عالی فضای سایبری***، (۱۳۹۴/۴/۱۶).
- ازغندی، علیرضا و روشندل، جلیل (۱۳۷۴)، ***مسائل نظامی و استراتژی معاصر***، تهران: انتشارات سمت.
- اسلاتر، ریچارد و همکاران (۱۳۶۷)، ***نواندیشی برای هزاره نوین***، مترجمان: عقیل ملکی فر، سیداحمد ابراهیمی، وحید وحیدی مطلق، مرکز مطالعات و برنامه‌ریزی استراتژیک، انتشارات مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- امیدوارنیا، محمدجواد (۱۳۸۲)، ***امنیت در قرن بیست و یکم***، تهران، نشر مطالعات سیاسی و بین‌المللی.
- بلیکی، نورمن (۱۳۹۳)، ***طراحی پژوهش‌های اجتماعی***، ترجمه حسن چاوشیان. تهران، نشر نی.
- بوزان، باری (۱۳۷۸)، ***مردم، دولت‌ها، هراس***، تهران، ترجمه و انتشارات پژوهشکده مطالعات راهبردی.
- پدارم (۱۳۸۸)، ***آینده‌پژوهی، مفاهیم و روش‌ها***، تهران، مرکز آینده‌پژوهی علوم و فناوری دفاعی.
- جمعی از محققین (۱۳۹۵)، ***طراحی نظام دفاع سایبری کشور و راهبردهای آن***، تهران، دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.
- جوزی‌خمس لویی، علی و جواهران، هدی (۱۳۹۲)، ***تحلیلی بر نقش پدافند غیرعامل در امنیت راهبردی کلان‌شهرها***، تهران، مجله اطلاعات جغرافیایی (سپهر). شماره ۸۷.
- حاجیانی، ابراهیم (۱۳۹۲)، ***اصول و مبانی روش‌های آینده‌پژوهی***، ناشر، دانشگاه امام صادق(ع).
- خزایی، سعید (۱۳۸۴)، ***دیده‌بانی، مبانی و مفاهیم***، مرکز آینده‌پژوهی علوم و فناوری دفاعی.

- طباطبایی، سیدمحمد؛ سلیمی، حسین؛ موحدیان، احسان (۱۳۹۵)، ***تأثیر سایبر دیپلماسی آمریکا بر دیدگاه کاربران مجازی ایران***، مطالعات رسانه‌های نوین.
- عبدالله خانی، علی (۱۳۸۶)، ***تهدیدات امنیت ملی***، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
- عراقچی، سید عباس و جوزانی کهن، شاهین (۱۳۹۶)، ***بهره‌برداری داعش از فضای مجازی***، فصلنامه روابط خارجی، شماره ۳۳.
- عاشوری ذبیح اله و حسینی محمدرضا (۱۳۹۳)، ***کاربرد روش‌های آینده‌پژوهی در بررسی مطالعاتی سازمان‌های حفاظت اطلاعات ن.م***، فصلنامه علمی- پژوهشی امنیت پژوهی شماره ۴۶.
- قاسمی، فرهاد (۱۳۸۶)، ***نگرشی بر طراحی مدل بازدارندگی سیاست خارجی ایران***، تهران، فصلنامه ژئوپلیتیک. سال سوم. شماره اول.
- قاسمی، فرهاد (۱۳۸۸)، ***الزامات تئوریک بازدارندگی منطقه‌ای جمهوری اسلامی ایران***، تهران، فصلنامه روابط خارجی. سال اول. شماره سوم.
- کرم نیا، رضا (۱۳۹۱)، ***ارائه الگوی راهبردی دفاعی بر اساس اندیشه دفاعی حضرت امام خمینی (ره)***، رساله دکتری، دانشگاه عالی دفاع ملی.
- قاسمی، فرهاد و کشاورز شکری، عباس (۱۳۸۸)، ***نگرشی به سیستم بازدارندگی منطقه‌ای در روابط بین‌الملل: مطالعه موردی ایران و آمریکا***، تهران، رهیافت‌های سیاسی و بین‌المللی. شماره ۲۰.
- ستاری‌خواه علی (۱۳۹۳)، ***آینده‌پژوهی و سناریونویسی کاربردی***، قرارگاه پدافند هوایی خاتم‌الانبیاء.
- ***سند امنیت فضای تولید و تبادل اطلاعات (افتا)***، هیئت وزیران، ۱۳۸۷.
- ***سند چشم‌انداز ۱۴۰۴ جمهوری اسلامی ایران***، مجمع تشخیص مصلحت نظام، ۱۳۸۲
- ***سند نظام جامع فناوری اطلاعات***، وزارت ارتباطات و فناوری اطلاعات، ۱۳۸۶
- ***سند راهبردی پدافند سایبری***، سازمان پدافند غیرعامل، ۱۳۹۰.
- شکرخواه، یونس (۱۳۸۴)، ***روزنامه‌نگاری سایبر، جامعه اطلاعاتی و آزادی بیان***، تهران: انتشارات ثانیه.
- میناوند، محمدقلی (۱۳۸۵)، ***اینترنت و توسعه سیاسی***، حوزه عمومی در فضای سایبرنتیک، پژوهش سیاست نظری.

- نجات‌پور، مجید. محمدی، مصطفی. اصغری، امید و شهریاری، حیدر (۱۳۹۱)، ***جنگ نرم و امنیت در فضای سایبر***، تهران، فصلنامه مطالعات راهبردی بسیج. سال پانزدهم. شماره ۵۴.
- Colarik Andrew, 2006, Cyber Terrorism Evolution Idea,Group Inc. IDEA GROUP PUBLISHING
- Do Hoon Kim, Taek Lee, Sung-Oh David Jung, Hoh Peter In, and Hee Jo Lee, (2007)Cyber Threat Trend Analysis Model Using HMM, Department of Computer Science and Engineering Korea University, Seoul, 136-701, Korea, IEEE
- Eid, Mahmoud, (2010), cyber-terrorism and Ethical journalism: need for Rationalism, *international journal of techno ethics*
- Jonse, Andrew, (2005), cyber terrorism, fact or fiction, *computer fraud &*
- International strategy for cyber space,2011 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- Gartner,2014, Gartner Top Predictions, http://www.gartner.com/it/content/2607600/2607616/november_6_top_ predicts_2014dplummer.pdf?userId=72895160 visit date: 2014-09-20
- Kevin Benedict, 2012, information operation, the fifth dimension of warfare,
- Neo Park,Won Hyung Park, (2012) Cyber Threat Prediction Model Using Security Monitoring System Event, Springer Netherlands
- Sandia, 2012, Cyber Threat Metrics, Sandia National Laboratories,
- The MITRE Corporation, 2012, "How Do You Assess Your Organization's Cyber Threat Level."
- The MITRE Corporation, 2010, "Cyber Threat Susceptibility Analysis (TSA) Methodology
- The DOD cyber strategy, 2015,accessible: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- US cyber security strategy, DHS,2014, https://www.dhs.gov/cybersecurity-overview
- UK cyber security strategy, 2016, https://www.gov.uk/government/publications/national-cyber-
- security-strategy-2016-to-2021
- Wendell Bell,2008, Foundations of Futures Studies, Volume 1: Human Science for a New Era, transaction publisher