فصلنامه علمی مطالعات دفاع مقدس
دوره ۷، شماره ۳، شماره پیاپی (۲۷)، پاییز ۱٤۰۰، ص ۲۰۷ ـ ۱۸۱

مقاله پژوهشی **DOR: 20.1001.1.25883674.1400.7.3.8.8**

الگوی راهبردی جلوگیری از امنیتی شدن پدیده‌های متاثر از فضای سایبر

حسن محمدی منفرد[۱]، مهدی عزیزی مهماندوست[۲]، محمدرضا موحدی صفت[۳]، محمد حسن انتظاری[٤]

تاریخ دریافت: ۱۴۰۰/۰۲/۲۵ تاریخ پذیرش: ۱۴۰۰/۰۶/۰۱

چکیده: جریان سلطه در ادامه تقابل دائمی خود با نظام مقدس جمهوری اسلامی ایران به موازات فضای واقعی، راهبرد تضعیف پشتوانه مردمی نظام را از طریق فضای سایبر، و با بکارگیری فناوری‌های اجتماعی برای خود ترسیم نموده است. دستگاه های متولی در جمهوری اسلامی ایران باید با شناخت مناسب و به هنگام در مواجهه با پدیده‌های متاثر از فضای سایبر، اقدام بایسته را انجام دهند. برای این کار نیاز به الگو است. هدف و سؤال اصلی پژوهش حاضر معرفی الگویی راهبردی برای جلوگیری از امنیتی شدن پدیده‌های متاثر از فضای سایبر می باشد. پژوهش از نظر هدف کاربردی و از حیث روش، ترکیبی یا آمیخته است. جامعه آماری، در بخش کیفی شامل تعداد ده نفر از خبرگان و اساتید دانشگاهی در حوزه فضای سایبری و مدیریت بحران هستند که با استفاده از روش نمونه گیری هدفمند و اصل اشباع نظری انتخاب شدند. همچنین در بخش کمی تعداد ۱۳۰ نفر شامل مدیران و کارشناسان سطوح مختلف دستگاه‌های متولی با استفاده از روش طبقه‌ای تصادفی انتخاب شدند. داده‌ها در بخش کیفی با استفاده از مصاحبه عمیق و در بخش کمی با پرسشنامه محقق ساخته که روایی و پایایی(۷۹/.) آن نیز تأیید شد، گردآوری شدند. نتایج نشان داد، مؤلفه‌های الگوی راهبردی مذکور ۲۰ مؤلفه در ٤ بعد شامل: حکمرانی سایبری، اشراف اطلاعاتی سایبری، مدیریت امنیت سایبری و عوامل کلان محیطی می باشند.

واژگان اصلی: امنیتی شدن پدیده‌ها، حکمرانی سایبری، اشراف اطلاعاتی سایبری، مدیریت امنیت سایبری، عوامل کلان محیطی.

۱. دانش آموخته دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران (نویسنده مسئول). h.mohammadi@sndu.ac.ir
۲. دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران.
۳. استادیار مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران.
٤. استادیار مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران.

مقدمه

مهم «انّ اَخَا الحَرب اَلاَرِق ومَن نام لَم یَنُم عَنهُ» آن کس که همواره با جنگ همراه است، هرگز به خواب نمی رود و کسی که بخوابد، دشمن در مقابل او بیدار است (نهج البلاغه، نامه ٦٢). امام خامنه ای (مدظله العالی) در مورد ضرورت توجه به فضای سایبر می فرمایند «اهمیت فضای سایبر به اندازه خود انقلاب اهمیت دارد» همچنین می فرمایند "این فضا مثل یک رود خانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می شود فرصت. اگر رهایش کنیم و برنامه ای برای آن نداشته باشیم می شود یک تهدید". این تاکید معظم له مشخص می نماید که پرداختن به فضای سایبر و تبیین نقش وکارکردها ی آن از اهمیت بسیار بالایی برخوردار است. چراکه فضای سایبر به عنوان پدیده ای اجتماعی، دارای ابعاد گسترده می باشد که مهمترین موضوع آن، توجه به تغییرات بنیادینی می باشد که در نظام مدیریت و حکمرانی اجتماعی بوجود آورده است. این تغییرات تا به آنجا می باشد که در نظام حکمرانی کشورهای توسعه یافته، دولت ها همه عملکردهای خود را به این فضا منتقل نموده اند. در این میان، امروزه ما شاهد ظهور طیف گسترده‌ای از فناوری‌های اجتماعی هستیم. برای مثال، شبکه‌های اجتماعی (فیسبوک، لینکداین،[1] واتسَپ،[2] اینستاگرام،[3] اسنپ‌چت[4] و غیره) و بسیاری برنامه‌های جدید وب‌محور، نشان‌دهنده‌ی تغییری اساسی در شیوه‌ی تعامل اجتماعی و حرفه‌ای بسیاری از ما انسان ها می باشد. پیشرفت های حوزه فناوری اطلاعات و ارتباطات به عنوان پیشران‌های اصلی فناوری‌های اجتماعی از یک طرف و شیوه‌ی استفاده‌ی ما از این فناوری ها به عنوان اعضای جامعه، در حال ایجاد دگرگونی‌های اساسی است. فرایندی که برخی از صاحب‌نظران این حوزه از آن به انقلاب «سکویی»[5] یاد می‌کنند(پارکر، ٢٠١٦: ٢٤١). جمهوری اسلامی ایران در عمل، در مسیر جامعهٔ اطلاعاتی حرکت کرده و روز به روز بر شتاب آن افزوده می شود، طبق پایش انجام شده در سال ١٣٩٩، ٧٣,٦ درصد از افراد بالای ١٨ سال کل کشور اعلام کردند در حال حاضر از رسانه‌های اجتماعی مجازی استفاده می کنند. ٦٤,١ درصد از افراد بالای ١٨ سال از پیام‌رسان واتس‌اپ استفاده می‌کنند. اینستاگرام با ٤٥,٣ درصد در رتبه دوم و تلگرام با ٣٦,٣ درصد در رتبه سوم قرار دارد. پیام‌رسان ایتا با ٤,٨ درصد و

1. LinkedIn
2. Whatsapp
3. Instagram
4. Snapchat
5. Platform

پیام‌رسان سروش با ٤ درصد و بله با ٤ درصد در رتبه‌های اول تا سوم پیام‌رسان‌های ایرانی هستند(مرکز افکارسنجی دانشجویان ایران[1]، ۱۳۹۹). از طرفی، امروزه جهان در حال تجربه نوینی از ضریب نفوذ فضای سایبر و بکارگیری فنآوری های اجتماعی است که در آن تلاش می‌شود از قابلیت برقراری ارتباط متقابل در فضای سایبر، برای هدایت منابع انسانی جوامع و به منظور تأثیرگذاری بر بینش و کنش های رفتاری آنان در راستای منافع مالکان خود استفاده بهینه شود. این راهبرد در صورت موفقیت می‌تواند از ظرفیت ها و قابلیت های این مخاطبین، در جهت ساماندهی، سازماندهی و هدایت جوامع استفاده کند. در واقع با تکیه بر همین راهبرد اساسی، در چند سال گذشته با استفاده از سرمایه‌های انسانی و اجتماعی، از اقشار مختلف جامعه ی انسانی برای ایجاد تغییرات هدفمند در کشورها به خوبی استفاده شده است. نتایج تحقیقات مختلف بیانگر آن است که می توان از ظرفیت فناوری های اجتماعی در بسیاری از سطوح فردی و اجتماعی به منظور شناسایی مسائل و نیازهای اجتماعی، برقراری روابط اجتماعی و رهنمون سازی افراد در مسیر دستیابی به اهداف استفاده نمود (محمدی منفرد و مهدی نژاد نوری، ۱۳۹۹: ۲۱٦). با توجه به مجموع کنش‌ها و واکنش‌های فوق، مشخص می‌شود: عدم ساماندهی و مدیریت یکپارچه فضای سایبری کشور و اعمال سیاست‌های مقطعی و سلیقه‌ای برای کشور خطرناک بوده و زمینه بهره برداری معاندین جمهوری اسلامی ایران را در امنیتی نمودن پدیده ها که همواره به عنوان یکی از راهبردهای آنها در جنگ نرم می باشد را فراهم می نماید. لذا این مقاله در راستای معرفی الگویی راهبردی برای جلوگیری از امنیتی شدن پدیده های متاثر از فضای سایبر در جمهوری اسلامی ایران، نخست به طرح موضوع پرداخته و سپس مفاهیم پدیده ها، فضای سایبر و فرآیند امنیتی شدن را توصیف، و در ادامه با مراجعه به پیشینه تحقیق، تجربه سایر کشورها، خبرگان موضوع و ادبیات مرتبط در سطح داخل و خارج ضمن تبین مساله، ابعاد و مؤلفه های الگوی مذکور را ارائه می نماید.

ضرورت و اهمیت تحقیق

انجام این تحقیق از آن جهت حائز اهمیت است که با ارائه الگوی راهبردی مواجهه با پدیده های متاثر از فضای سایبر، مزیت های زیر حاصل می گردد.

۱. توسعه مرزهای دانشی شناخت فضای سایبر در حوزه کاربردها، مخاطرات و تهدیدات آن.

۲. درک مشترک و همگرایی سیاست گذاران فضای سایبر در کشور و ارائه یک چارچوب جامع برای تدوین راهبرد.

[1] . http://ispa.ir/Default/Details/fa/2288

۳. زمینه‌ساز گفتمان سازی و توسعه مرزهای دانشی برای انجام فعالیت علمی و پژوهشی درآینده.
٤. تعیین معیار و شاخص مناسب برای ارزیابی اقدامات عملیاتی در این حوزه.

همچنین ضرورت انجام این تحقیق با رویکرد سلبی با توجه به این مورد است که باعث عدم توجه به بروز چالش‌های بنیادین در امورحاکمیتی و حکمرانی سایبری کشور خواهد شد و ضمن ایجاد موضع انفعالی در تصمیم‌سازی، باعث افول قدرت تصمیم گیری برای مدیران، در حوزه مواجهه فعال با مخاطرات و تهدیدات این فضا می شود. در راستای نیل به موارد یاد شده هدف و سؤال اصلی تحقیق، دستیابی به الگوی راهبردی مواجهه با پدیده‌های امنیتی متاثر از فضای سایبر در جمهوری اسلامی ایران می‌باشد. این هدف می‌تواند برای سیاستگذاران، برنامه ریزان و مسئولان نوعی چشم انداز و نقشهٔ راه باشد.

پیشینه پژوهش

احمدی مقدم و عابدی (۱۳۹۹) در تبیین «نابرابری های اجتماعی و امنیتی شدن پدیده های اجتماعی» به این نتیجه رسیدند که ارتباط مستقیم و موثری بین نابرابری های اجتماعی و امنیتی شدن پدیده های اجتماعی وجود دارد. لذا نظام اجتماعی برای مدیریت تهدیدهای امنیتی، باید فرصت های برابری را برای شهروندان در جامعه ایجاد کند، تا با جلب رضایت آن ها مانع از بروز نابسامانی های اجتماعی شده و امنیت را تضمین نماید.

کِلی شیرکی[1] (۲۰۰۸) در کتاب «همه می‌آیند: قدرت سازمان‌دهی بدون سازمان» نشان می‌دهد که فضای سایبر، توانایی جامعه در ایجاد ارتباط، بسیج و تأثیر دهی تغییر را به شکلی چشم‌گیر اصلاح کرده است. او بیان می‌کند که فناوری های نوین به همه اجازه می‌دهد که عملکرد اجتماعی بزرگ‌تر از گذشته داشته باشند، «آن‌ها را قادر به ساختن انواع جدید گروه می‌کند» و به این گروه‌ها اجازه می‌دهد تا قدرت و نفوذ فراوان در حوزه‌هایی داشته باشند که عموماً به روی آن‌ها بسته است.

نتایج حاصل از پژوهش موسسه‌ی راهبرد معاصر (۱۳۹۷) با هدف بررسی« نقش فضای سایبر در اغتشاشات دی ماه ۹۶ در جمهوری اسلامی ایران» حاکی از آن است که نقش فضای سایبری در شکل گیری اغتشاشات آن زمان بسیار پررنگ است. نتایج این تحقیق در قالب پنج دسته عوامل علّی، عوامل بستر، عوامل مداخله‌گر، راهبردها و پیامدها استخراج شده است به طوریکه در عوامل علّی، تأثیر روانی

[1]. Clay Shirky

رسانه‌ها بر افکار عمومی، در عوامل بستر، انفعال در مدیریت فضای سایبری و در عوامل مداخله‌گر، تأثیر فضای سایبری، جزو عواملی بوده اند که توسط کارشناسان مورد اشاره قرار گرفته اند.

واگنر[1] و همکاران (۲۰۱۹)، به اشتراگ گذاری اطلاعات تهدیدات فضای سایبری را به عنوان یکی از روش های خنثی کردن افزایش مداوم حملات سایبری معرفی نمودند. در این تحقیق به بررسی آئین نامه و روش‌هایی پرداختند که از یک روند اشتراک‌گذاری اطلاعات در مورد تهدیدات فضای سایبری پشتیبانی می کند.

یافته‌ها و نتایج مطالعه ی اندرسون[2] (۲۰۱٤) با عنوان « زندگی دیجیتالی در سال ۲۰۲۵ و اینکه چگونه فضای مجازی جامعه را در آینده تغییر خواهد داد» بیانگر شکل‌گیری «فضای مجازی، عظیم و ناپیدا است». در این جامعه، بهبود واقعیت از طریق فن‌آوری‌های پوشیدنی و کاشتنی در بدن، اختلال در الگوهای کاری موجود و جاری؛ و «برچسب‌گذاری، قرار دادن در پایگاه داده و نقشه‌کشی تحلیلی هوشمند در حوزه‌های فیزیکی و اجتماعی» اتفاق خواهد افتاد.

براساس مطالعات به عمل آمده در خصوص اسناد نزدیک به موضوع مورد مطالعه که در گذشته انجام شده است پژوهشی که مستقیماً به تدوین الگوی راهبردی مواجهه با پدیده های امنیتی فضای سایبر پرداخته باشد انجام نشده است. بدیع بودن این تحقیق در قالب الگوی راهبردی برای نخستین بار در حوزه مواجهه با پدیده های امنیتی متاثر از فضای سایبر با بهره گیری از گفتمان مقام معظم رهبری(مدظله العالی)، اسناد بالادستی و انجام مصاحبه و مستندسازی نظرات خبرگان، دارای اهمیت بسزایی است و از آنجا که تاکنون در این خصوص اقدامی نشده است، این تحقیق دارای نوآوری می باشد و انجام آن ضرورت دارد.

مبانی نظری

پدیده

پدیده عبارت است از اتفاقات اجتماعی پیرامونی، که قابل درک اند و هویت مشخصی دارند. پدیده ها اصولا آن هنگام قابل شناسایی هستند که از ذات(درون) خود خارج می شوند و به حالت یک اثر در بیرون نمود پیدا می کنند. هایدگر پدیده را به معنای هرگونه دلالت، نماد، نشانه و سمبل در بنیاد صوری

[1] . Wagner
[2] . Janna Anderson

خویش معرفی کرده است(هایدگر،۱۳۸۰: ۷۸). مدل های مختلف از زوایای گوناگون به توصیف پدیده ها پرداخته اند. رمضانی و همکاران یک دسته بندی جامع برای توصیف پدیده ها به شرح جدول(۱) ارائه نموده است.

جدول(۱): مدل تحلیلی توصیف جامع یک پدیده در ابعاد مختلف (رمضانی و همکاران،۱۳۹۵ : ۱۵۲)

مدل تحلیلی توصیف جامع یک پدیده در ابعاد مختلف		
ردیف	**معیار و تحلیل پدیده**	**گونه**
۱	ماهیت پدیده	سیاسی، اقتصادی، نظامی، اجتماعی، زیست محیطی، فناورانه و ...
۲	سطح پدیده	فردی، اجتماعی، ملی،منطقه ای، بین المللی و جهانی
۳	جغرافیای پدیده	داخلی – خارجی
٤	تقارن پدیده	متقارن – نامتقارن
٥	پیچیدگی	بسیط – پیچیده
٦	هویت پدیده	مادی – معنوی
۷	جنس پدیده	عینی – ذهنی
۸	کانون پدیده	بازیگران – ساختاری
۹	انگیزه پدیده	عمدی – غیر عمدی

امنیتی شدن

امنیتی شدن به معنای خروج پدیده ها و یا موضوعات از وضعیت عادی به وضعیت فوق العاده می باشد یعنی، خارج شدن پدیده ها از حوزه سیاست های عادی یا سیاست های عمومی و وارد شدن آنها به حوزه امنیتی، که الزاماً ربطی به وجود تهدید حقیقی ندارد و می تواند از معرفی آن موضوع به عنوان تهدید نشأت گیرد. (عبداله خانی، ۱۳۸۵: ٤٤۹). چنانچه بازیگر امنیتی ساز، پدیده ای را امـنیتی نماید و مخاطب وی نیز آن را بپذیرد، آن پدیده امنیتی شده است. بنابراین آنچه در این میان نقش دارد، ذهن، ادراک و نگرش بازیگر و مخاطب مـی باشد(همان، ٤۹٤). بالزاک[1] با استفاده از مفهوم کنش کلامی[2](عمل به گفتار) عنوان می کند که مفهوم امنیتی شدن زمانی بهتر فهمیده می شود که آن را رویه ای راهبردی و عملگرایانه تصور کنیم که درون یک وضعیت و به

[1] .Balzaq
[2] .Speech Act

عنوان بخشی از آن روی می دهد و سه مؤلفه محیط و زمینه رویداد، ویژگیهای فرهنگی ـ روانی کارگزار سیاسی و مخاطب را در برمی گیرد. در این چارچوب، قدرت شنونده و گوینده در یک روند تعاملی دارای اهمیت می باشد (بالزاک، ۲۰۰۵: ۱۷۳). در نظریه امنیتی شدن، کنش کلامی موفقیت آمیز، از طریق درک بین الاذهانی در درون یک جامعه سیاسی شکل می گیرد (استریتزل[1]، ۲۰۰۷ : ۳۵). برای امنیتی شدن موضوعات، چهارچوبی امنیتی وجود دارد که از سه مفهوم اساسی و مرتبط، به شرح زیر تشکیل می شود:

۱- شکل: از نظر شکلی امنیتی شدن به طور مشخص با تمرکز بر گفتار بازیگران مسلط تعریف می شود که این بازیگران
اغلب رهبران سیاسی می باشند.

۲- محتوی: مفاهیم و محتوای عمل امنیتی شدن به طور دقیقی بر تمرکز کردن بر زمان شروع این فرآیند تعریف شده و با ایجاد پتانسیلی برای موضوعات امنیتی توسعه آن را سبب می شود.

۳- ماهیت: محوری ترین نکته چهارچوب امنیتی شدن، مفهوم ماهیت عملی است که توسط بازیگر تعریف شود. این عمل صرفاً در قالب اصطلاحات و طرح تهدیداتی که به منظور امنیتی شدن توسط شخص امنیتی ساز به کار می رود، انجام می شود. اهمیت اصلی در این مفهوم تمرکز بر هدف هنجاری و یا بیان ارزشهای اصلی است که در قالب و چهارچوبی خاص فهمیده می شود(مک دونالد[2]،۲۰۰۸: ٥٦٤). مهم ترین عناصر اصلی در نظریه امنیتی شدن عبارتند از:

۱- بازیگر امنیتی‌ساز

بازیگر امنیتی ساز بازیگری است که اقدام به امنیتی کردن یک موضوع خاص می‌کند. این بازیگر بایستی از سرمایه اجتماعی کافی برخوردار بوده و در موقعیت اقتدار نیز باشد. (بوزان، ۱۳۷۸: ۵۵).

۲- کنش گفتاری:

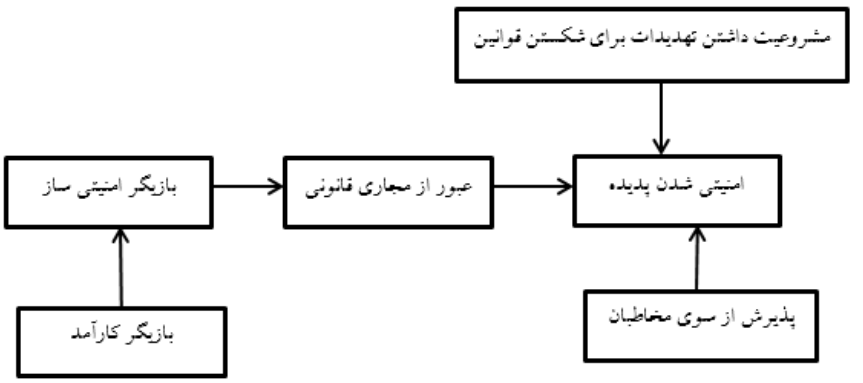
به طور کلی موفقیت در امنیتی ساختن هر پدیده به کاربرد موفقیت آمیز قواعد سازنده هر اقدام گفتاری بستگی دارد. در این زمینه بایستی به توان متفاوت بازیگران امنیتی ساز برای بیان ادعای مؤثر و نهایتاً پذیرفته شدن این ادعا از سوی مخاطب اشاره کرد (همان، ۵۵). به عبارت دیگر امنیتی کردن موضوعات به عنوان مجموعه‌ای از گفتارها تلقی می‌شود که اجزای این گفتار می‌تواند شامل

[1] .Stritzel
[2] . Mcdonald

ادعا کردن، هشدار دادن و یا ایجاد تقاضا از سوی بازیگر امنیتی ساز باشد (وری، ۲۰۰۸: ۷۵).

۳- مخاطب:

مرحله نهایی فرایند امنیتی ساختن، پذیرش مخاطب است؛ به عبارت دیگر امنیتی شدن وقتی کامل می‌شود که از سوی مخاطب مورد پذیرش قرار گیرد. خود این پذیرش می‌تواند آمیزه‌ای از زور و یا رضایت باشد. در همین زمینه می‌توان این گونه بیان کرد که هر چقدر بحران ایجاد شده و موضوع امنیتی شده مخاطب را در مورد آسیب پذیری اش دچار حساسیت بیشتری کند، آن گاه سخنان هشداردهنده بازیگر امنیتی ساز پاسخ مناسب مخاطب را ایجاد کرده و فرایند امنیتی شدن موفق آمیزتر خواهد بود. بدین ترتیب موفقیت امنیتی شدن تا حد زیادی به توانایی بازیگر امنیتی ساز در شناخت احساسات، نیازها و منافع مخاطب و همچنین ایجاد درک و آگاهی مشترک و متقابل میان بازیگر امنیتی ساز و مخاطب بستگی دارد. بر این اساس چالش اصلی یک بازیگر امنیتی ساز متقاعد ساختن مخاطب است؛ بنابراین می‌توان این گونه بیان کرد که امنیتی ساختن، مخاطب محور است (عبدالله خانی، ۱۳۸۹: ۳۱۶).



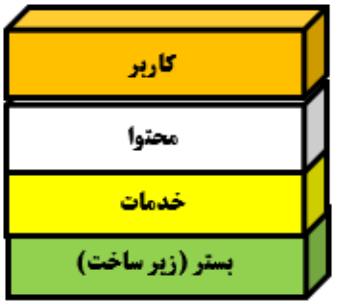
شکل(۱) ترسیم نمای کلی از امنیتی شدن پدیده‌ها (عبدالله خانی، ۳۱۷:۱۳۸۹)

هستی شناسی فضای سایبر

اصطلاح فضای سایبر، نخستین بار توسط ویلیام اف گیبسون[1]در رمان علمی – تخیلی «برنینگ کروم»[2] در سال ۱۹۸۲ به‌کار برده شد و به رغم معرفی، اصطلاحی مبهم باقی ماند(گیبسون ،۲۰۰۳:

1. William F. Gibson
2. Burning Chrome

۲۲٤). طی سالهای اخیر، تعاریف زیادی برای این واژه در اسناد راهبردی کشورها ارائه و به مرور تکمیل شده است. به طور کلی فضای سایبر عبارت است از « فضایی، برآمده از شبکه های وابسته به یکدیگر، اعم از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های جاگذاری شده، کنترل کننده های صنایع حیاتی، محیط تولید، پردازش، ذخیره سازی، ارسال، دریافت، امحاء، بازیابی و بهره برداری از اطلاعات می باشد» (تقی پور، ۱۳۹۸: ۲۹). از سوی دیگر فضای سایبر، تعاملات و اثر متقابل این محیط و انسان را نیز در بر می گیرد. شورای عالی فضای مجازی به منظور ترسیم این فضا، یک مدل چهار لایه ای برای فضای سایبری کشور به شرح شکل (۲) ارائه نموده است.



شکل (۲): مدل چهار لایه ای فضای سایبر (مرکز ملی فضای مجازی، ۱۳۹٦)

لایه زیرساخت: این لایه برای ذخیره سازی، انتقال و پردازش اطلاعات در فضای سایبر مورد استفاده قرار می گیرد.

لایه خدمات: به سرویس ها و یا خدماتی که در فضای سایبر ارائه می گردد، اشاره دارد.

لایه محتوا: به محتوا و اطلاعات ارجاع دارد که در فضای سایبری وجود داشته و ابزارهایی که برای دستیابی و پردازش این اطلاعات مورد استفاده قرار می گیرند

لایه انسانی/اجتماعی: به ارتباطات و تعامل های بین کاربران در فضای سایبر و اطلاعاتی که به اشتراک می گذارند اشاره دارد. البته هرکدام از این لایه های فضای سایبر از اجزایی تشکیل شده اند که در جدول(۲) به آن اشاره شده است.

جدول(۲): اجزای تشکیل دهنده لایه های فضای سایبر (تقی پور و دیگران،۱۳۹۸: ۱٦)

ردیف	عنوان لایه	اجزاء تشکیل دهنده لایه
۱	زیر ساخت	زیر ساخت داده/ زیر ساخت های اطلاعاتی و محتوایی/ شبکه (ساختار، معماری و پیکربندی، عملیات و اجزاء، منابع و تجهیزات)/ زیر ساخت های

		نرم افزاری و پردازشی/ زیر ساخت های کاربردی و خدماتی/ زیر ساخت های رایانشی/ زیر ساخت های پایه/ زیرساخت های ذخیره و پشتیبان گیری
۲	**محتوا**	داده ها و اطلاعات حساس مراکز داده – اطلاعات کنترل و پایش در دیسپچینگ ها – اطلاعات موجود در سامانه های بانکداری الکترونیکی، سامانه های حوزه سلامت، سامانه های ارتباطی و حمل و نقل، سامانه های خدمات دولت الکترونیک، سامانه های خدمات حقوقی و قضایی و ....
۳	**خدمات**	نرم افزارهای پردازشی و برنامه های کاربردی، خدمات شبکه محوری، نرم افزارهای پایه
٤	**کاربر**	نیروی انسانی دارای دسترسی به اطلاعات حساس در مراکز داده، دسترسی به ساختار دیسپچینگ های ملی، افراد دارای دسترسی به سامانه های بانکداری الکترونیکی، سامانه های ناوبری، ارتباطی، کنترلی حوزه حمل و نقل، سامانه های پرونده الکترونیک سلامت، خدمات دولت الکترونیک، سامانه های خدمات حقوقی و قضایی و ....

نحوه تاثیر فضای سایبر بر انواع پدیده ها

رشد ضریب نفوذ فضای سایبر و تولید کلان داده ها، پیامدهای گسترده ای برای جوامع در حوزه های گوناگون اجتماعی، سیاسی، فرهنگی و امنیتی داشته و دارد. چرا که در این فضا داده ها مدیریت شده و از آن به عنوان بستر و پشتیبانی در تحلیل های فردی و اجتماعی استفاده می شود به طوریکه: دو نتیجه‌ی عمده‌ی مدیریت فضای سایبر و کلان داده‌ها های موجود در آن را به شرح زیر می توان برشماری نمود:

۱- توانایی ردگیری (مردم، چیزها، رفتارها و غیره)

۲- توانایی پیش‌بینی رفتارها و وقایع .

به عنوان مثال داده‌های به دست‌آمده از مچ بند های سلامت و ساعت های هوشمند می‌تواند به بیمه‌گران در خصوص امید به زندگی افراد اطلاعات بی‌شماری ارائه کند، یا این که اطلاعات به‌دست‌آمده از وسایل موجود در «خانه‌های هوشمند[1]» به همراه داده‌های جی‌پی‌اس[2] می‌تواند در

[1]. smart home
[2]. GPS

مورد تخلیه بودن خانه اطلاع رسانی کند. دغدغه‌ی مهم دیگر در خصوص محیط کلان داده‌ها مفهوم حباب‌های فیلتری و تمایز[1] است. الگوریتم‌هایی که از داده‌های پیشین استفاده می‌کنند به کاربران دیجیتالی این تجربه‌ی آنلاین ویژه را می‌دهند که اثر «حباب پالایه‌ای[2]» را ایجاد کنند، اثری که به‌واسطه‌ی آن محتوا، تبلیغات و حتی اخبار برای هر فردی پالایه می‌شود. اگرچه منافع بسیاری در این عمل وجود دارد ولی ممکن است مضراتی همچون تفاوت‌های وخیم سیاسی و فرهنگی در جوامع و یا حتی تبعیض قیمتی ناخواسته برای برخی گروه‌های مشتری پیش آید. شرکت‌ها در حال حاضر از داده‌های به دست‌آمده از خریدهای مشتریان و رفتار اینترنتی آن‌ها برای طراحی و بازاریابی محصولات و خدمات به افراد استفاده می‌کنند. جناح‌های سیاسی نیز می‌توانند از چنین داده‌هایی برای پیشبرد «هدف گذاری جزئی» بر روی رأی دهندگان استفاده کنند. مسئله‌ی هشدار دهنده تر توانایی پیش‌بینی است (سادیلک[3] و کروم[4]، ۲۰۱۲: ۱۱۵). و در آینده این توان پیش‌گویانه‌ی داده‌ها با پیشرفت در پردازش رایانه ای و هوش مصنوعی قطعا افزایش خواهد یافت.

بررسی های موسسه گارتنر نشان می دهد شکل گیری اینترنت رفتارها مهم ترین روند فناورانه سال ۲۰۲۱ است. اینترنت رفتارها[5] با توجه به استفاده انسان ها از انبوهی از وسایل الکترونیک هوشمند مانند گوشی، ساعت ها و مچ بندهای هوشمند و غیره شکل می گیرد. ردگیری لحظه به لحظه زندگی انسان ها و کسب اطلاع از موقعیت مکانی و حالات چهره اشخاص و سلائق افراد و مرتبط کردن این داده ها به موقعیت جغرافیایی آنها باعث می شود تا تصویری دقیق از رفتارها و حالات روحی و روانی انسان ها به صورت آنی به دست آید. بر اساس بررسی گارتنر تا سال ۲۰۲۵ نیمی از جمعیت جهان در معرض برنامه های تجاری یا دولتی مبتنی بر اینترنت رفتارها قرار می گیرند. گارتنر هشدار داده که مشکلات اخلاقی و اجتماعی ناشی از همه گیر شدن اینترنت رفتارها غیرقابل انکار است (مؤسسه گارتنر، ۲۰۲۰).

در این تحقیق از منظر عملیاتی، فضای سایبر دارای تاثیراتی بر انواع پدیده ها در سطح جامعه می باشد. که در ادامه فرآیند و نحوه چگونگی این تاثیر گذاری بر کنش گران فضای سایبر بیان خواهد شد.

1. discrimination
2. filter bubble
3. sadilek
4. krumm.
5. IOB

الف) ارتقاء آگاهی اجتماعی

فضای سایبر زیرساخت کارآمدی برای ایجاد کثرت گفتمانی و پویایی زندگی روزمره شده اند که با تولید و توزیع محتوای جدید و کاربردی، فراتر از نظام آموزشی راکد و رسانه های رسمی و سنتی عمل نموده و موجبات افزایش آگاهی های اجتماعی را فراهم می آورند.

ب) توانمندی ارتباطی

فضای سایبر بستری مناسب برای تولید، گزینش و توزیع محتوای ارتباطی توسط همگان است که موجب کمرنگ شدن «مخاطب» و هویت یافتن «کاربر« است». از طریق این فضا، مسیرهای ارتباطی جدید شکل گرفته و روابط اجتماعی، سیاسی و فرهنگی تسهیل شده است. ارتباطات مجازی با ایجاد استقلال ارتباطی از رسانه های جریان اصلی، روابط سیاسی و اجتماعی و فرهنگی کاربران را تسهیل می کنند و به تبع آن، افزایش انعطاف و انطباق فرهنگی ارتباطگران را سبب می شوند.

ج) توانمندی اقتصادی

بخش مهمی از اشتغال جدید، نوآوری و کارآفرینی در بستر فضای سایبر محقق شده است و به عنوان رسانه تأثیرگذار در معرفی تجارت و کسب وکار ایرانیان است. این فضا، زمینه مناسبی برای معرفی کسب و کار شده اند و در این میان خانم ها پیشتازند. جوانان و زنان، پیشتاز بهره گیری از تلگرام و اینستاگرام در معرفی کسب وکار خود هستند. آنان با استفاده از ظرفیتهای مجازی توانمندی اقتصادی خود را ارتقا می دهند.

د) اصلاح برخط[1] اجتماعی و سیاسی

رویدادهای زیادی در سالهای پیش از ظهور و فراگیری فضای سایبر اتفاق می افتاد اما با دروازه بانی رسانه رسمی مواجه می شد؛ حداقل نتیجه آن عدم اطلاع شهروندان از آن وقایع بود. در سالهای اخیر وقایع با پوشش گسترده در فضای سایبری به اطلاع شهروندان می رسند؛ به طوریکه بسیاری از این رویدادها زمینه مناسبی برای گفتگوهای ملی شده اند. به واسطه فضای سایبر مواردی چون محیط زیست، گورخواب ها، کارتن خواب ها، حادثه پلاسکو و آتشنشانان، اشتباهات مدیران و مسئولان، املاک و فیشهای نجومی مورد توجه و نقد جامعه قرار گرفت. برجسته شدن موضوع پلاسکو در شبکه های اجتماعی مقدمه ای بر حساس شدن جامعه در ایجاد

[1] . Online

و افزایش تاب آوری اجتماعی بود (ایلالی و بروجردی علوی،۱۳۹۷: ۹۱-۸۹).

بازیگران فضای سایبر برای امنیتی کردن پدیده‌ها

فضای سایبری به‌عنوان جدیدترین عرصه منازعات راهبردی، دارای ویژگی هایی نظیر بدون مرز بودن این فضا، وجود بازیگران متعدد و گوناگون اعم از دولتی و غیردولتی شامل گروه های تروریستی، شرکت های چندملیتی، رسانه ها هکرها و غیره و مشخص نبودن منشاء بسیاری از حملات سایبری اعم از امواج فرهنگی و یا تهاجمات خرابکارانه و اخلالگر می باشد.

تا پیش از پایان جنگ سرد دولت ها یگانه بازیگران عرصه قدرت و حاکمیت بودند، اما با وقوع تحولات جدید که یکی از آنها گسترش ارتباط انسان ها و جوامع با یکدیگر از طرق مختلف بود، مفهوم مرزهای سیاسی قلمرو جغرافیایی کشورها کمرنگ شد و به تبع آن قدرت دولت ها کمتر از سابق گردید. تحول دیگری که در این زمینه اتفاق افتاد، ورود بازیگران جدید به عرصه قدرت، نظیر رسانه ها و شرکت های چند ملیتی بود که باعث شد قدرت دولت ها نسبت به سابق کم شود. گسترش اینترنت و به تبع آن فضای سایبری هم باعث تشدید این وضعیت شده است. بنابراین با توجه به نکات یاد شده، وجود عواملی چون بازیگران متعدد و بدون مرز بودن فضای سایبری بهتر درک می شود. در عرصه سایبری و در امنیتی شدن پدیده ها به طور کلی بازیگران مهمی نظیر بازیگران دولتی و یا غیردولتی حضور دارند. از جمله بازیگران دولتی می توان به آمریکا، روسیه، چین، عربستان سعودی، رژیم صهیونیستی، اتحادیه اروپا و جمهوری اسلامی ایران اشاره نمود که به نقش فضای سایبر برای ورود به عرصه های درگیری و تقابل (عملیات روانی در فضای سایبر) توجه نموده و در سطح بین المللی داری نقش و فعالیت می باشند. در بررسی محیط بیرونی (عرصه بین المللی) بازیگران به ظاهر غیر دولتی علیه جمهوری اسلامی ایران فعالیت دارند که دارای پشتیبانی های گسترده ای از سوی دولت های متخاصم و رقیب هستند.

فضای سایبر به شدت آسیب پذیر است و در سطح ملی می تواند از سوی عوامل بیرونی یا درونی مورد تهدید جدی قرار گرفته و صدمه ببیند که این خسارت متوجه حاکمیت، سازمان ها و نهاد های دولتی، موسسه ها، بانک ها و در نهایت شهروندان خواهد گردید بنابر این امنیت فضای سایبری یکی از مولفه های امنیت ملی است که باید به طور جدی مورد توجه قرار گرفته و به صورت پیوسته مورد ارزیابی واقع شود. (راهنمای تدوین راهبرد ملی امنیت سایبری، ۱۳۹۵: ۱۱). در جدول(۳) برخی از آسیب پذیری ها و تهدیدات فضای سایبر بیان شده است.

جدول(۳): تهدیدات و آسیب پذیری های فضای سایبر(محمدی منفرد و مهدی نژاد نوری،۱۳۹۹)

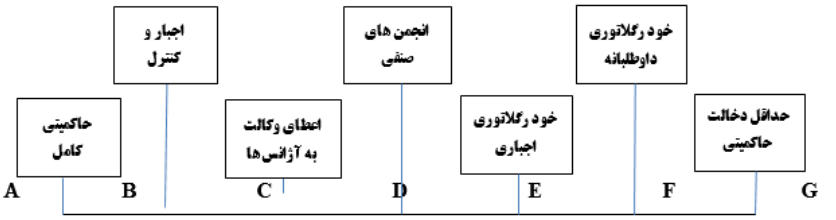
ردیف	لایه	تهدیدات
۱	**زیر ساخت**	تخریب یا تصاحب زیر ساخت های ارتباطی(محیط انتقال و توزیع)، اطلاعاتی و مدیریت شبکه، نقض حریم خصوصی با فراگیر شدن اینترنت همه ی اشیاء- تسری یافتن تهدیدات با توجه به بستر شبکه ای فضای سایبر
۲	**محتوا**	حملات منع خدمات توزیع یافته – حملات ویروسی- حملات علیه دسترس پذیری – مهندسی اجتماعی – داده های رمز نگاری نشده – باج افزارها (زینگ گائو و دیگران،۲۰۱۸). انگاره سازی وهنجارسازی معارض در جامعه - شبیه سازی الگوهای رفتاری جامعه - ایجاد محدودیت در دسترسی به اطلاعات - افکار سنجی جامعه - فضا سازی کاذب و پخش شایعات - تصویر سازی امنیتی از جامعه - پایش وکنترل اجتماعی به صورت متمرکز
۳	**خدمات**	اختلال در زیر ساخت های مجموعه های خدمت رسان اجتماعی از قبیل (بانک ها، پالایشگاه ها، نیروگاه ها ، سدها ، شبکه های حمل و نقل و ترافیک ، شبکه های توزیع برق، اب ، گاز و...).- انهدام و یا آسیب رسانی به تاسیسات صنعتی کشور (پالایشگاه ها نیروگاه ها و ...) با نفوذ در سیستم های رایانه ای و کنترلی آنها- ممانعت از استفاده از برخی سرویس های فضای سایبر به بهانه تحریم ها- قطع ارتباط با مراکز نگهداری داده در مواقع حساس و ضروری
٤	**کاربر**	جعل هویت و کلاه برداری - امکان توانایی رهگیری افراد در فضای سایبر - امکان پیش بینی رفتار افراد - انجام عملیات های روانی و ادراکی - ورود غیر قانونی به حریم خصوصی افراد - شبکه سازی وگروه سازی معارضین در سطح جامعه - بستری مناسب و تسهیل کننده برای فعالیت های تروریسم سایبری - تضعیف سرمایه های اجتماعی - جعل هویت در فضای سایبر و شیوع زندگی آواتاری - ذائقه سازی و تغییر سبک زندگی بخصوص در جوامع شرقی - جهانی سازی فرهنگی و تسخیر فضای اجتماعی کشورها

حکمرانی در فضای سایبر در سطح بین الملل

از زمان پیدایش فضای سایبر و ورود این پدیده به حوزه اجتماعی، بحث حمرانی در این فضا یکی از چالش های جدی محسوب می گردد. چرا که شیوه حکمرانی و قانون گذاری در این فضا

بر اساس نوع نگرش دولت ها به فضای سایبر می باشد. رویکرد دولت ها به مقوله امنیت فضای سایبر متفاوت می باشد و همان طور که در شکل(۳) نشان داده شده، می تواند یکی از حالت های زیر باشد:

کاملا حاکمیتی(حفاظت کامل حاکمیت از فضای سایبر)، اجبار نمودن رعایت استاندارد های تامین امنیت فضای سایبر از جانب دولت و کنترل و نظارت بر اجرای آن، استاندارد سازی و اجرای امنیت فضای سایبری توسط آژانس های عمومی، اعمال امنیت و حفاظت توسط انجمن های صنفی، اجرای ملاحظات امنیتی توسط بخش خصوص و تصدیق آن توسط حاکمیت و ایجاد چارچوب قانونی توسط حاکمیت و حداقل دخالت انجام می شود (ماین[1]،۲۰۱۵: ۱۵).



شکل(۳): رویکردهای مختلف دولت ها در امنیت سایبری(ماین،۲۰۱۵: ۱۵)

با توسعه و گسترش فضای سایبری، اکنون حجم بالایی از کارها و داد و ستد های اقتصادی، فرهنگی، اجتماعی و دفاعی در کلیه سطوح اعم از فردی، دولتی و بخش خصوصی در این فضا انجام می شود. به عبارتی، وجوه مختلف زندگی شهروندان به گونه ای روشن با این فضا درآمیخته و هر گونه ناامنی و چالش در این فضا به طور مستقیم یا غیر مستقیم بر زندگی و رفتار شهروندان تاثیر خواهد گذاشت. (راهنمای تدوین راهبرد ملی امنیت سایبری، ۱۳۹۵: ۱۰). بر این اساس موضوع حکمرانی در فضای سایبر عموما معطوف به سیاست های اعمال امنیت و تبعات ناشی از ناامنی در این فضا در سطح جامعه می باشد. لذا دولت ها برای ارزیابی صحیح امنیت در فضای سایبری ناچار بودند که از یک چارچوب برای امنیت سایبری استفاده نمایند. چنین چارچوبی شامل مجموعه فعالیتهای اصلی بخش دولتی و خصوصی برای تضمین سطح قابل قبولی از امنیت سایبری است. جدول (۵) فعالیت نهادهای بین المللی را در این حوزه به تصویر کشیده است.

[1] .Min

جدول(۵): چارچوب های امنیت سایبری نهادهای بین المللی

ردیف	شاخص	عنوان چارچوب	سازمان مرجع	سال انتشار	ابعاد اصلی چارچوب امنیت سایبری
۱	ITU	چارچوب امنیت سایبری اتحادیه بین المللی مخابرات	اتحادیه بین المللی مخابرات راه دور	۲۰۱۸	۱- حقوقی و قانونی ۲- سازماندهی ۳- ظرفیت سازی ٤- فنی ۵- همکاری ها
۲	CTO	چارچوب ارزیابی امنیت سایبری سازمان مخابرات کشورهای مشترک المنافع	سازمان مخابرات کشورهای مشترک المنافع	۲۰۱۵	۱- چارچوب قانونی، مقررات گذاری و نظارت ۲- ظرفیت سازی ۳- آگاهی رسانی ٤- قابلیت های فنی بومی ۵- واکنش به حوادث
۳	ENISA	شاخص ارزیابی امنیت سایبری اتحادیه اروپا	اداره امنیت شبکه و اطلاعات اتحادیه اروپا	۲۰۱٤	۱- سیاست ها و ظرفیت های دفاع سایبری ۲-تاب آوری سایبری ۳- مقابله با جرایم سایبری ٤- حمایت از صنعت در زمینه امنیت سایبری ۵- امن سازی زیرساخت های اطلاعاتی حیاتی
٤	CMM	مدل بلوغ امنیت سایبری دانشگاه آکسفورد	دانشگاه آکسفورد	۲۰۱٤	۱- تدوین سیاست و راهبرد سایبری ۲-تشویق فرهنگ مسئولیت پذیری سایبری در جامعه ۳ -ایجاد مهارت های سایبری در نیروی کار و کار فرمایان ٤ -ایجاد چارچوب های مؤثر قانونی و نظارتی ۵ - کنترل ریسک از طریق

					سازماندهی، استانداردها و فناوری
۵	CRI	شاخص آمادگی سایبری موسسه پوتومک	وسسه پتو ماک	۲۰۱۵	۱- راهبرد ملی؛ ۲- واکنش به حوادث سایری ۳- جرایم الکترونیکی و الزامات قانونی؛ ٤- به اشتراک گذاری اطلاعات؛ ۵- سرمایه گذاری در تحقیقات و توسعه؛ سایبری ٦- دیپلماسی و تجارت ۷- دفاع و پاسخ به بحران
٦	ASPI	چارچوب ارزیابی بلوغ سایبری در منطقه آسیا - اقیانوسیه	موسسه خط مشی گذاری راهبردی استرالیا	۲۰۱۷	۱- حکمرانی ۲- جرایم سایبری مالی ۳- نظامی نیروی ٤-اقتصاد و تجارت دیجیتال ۵- تعامل اجتماعی
۷	EGA	شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک	آکادمی حکمرانی الکترونیک	۲۰۱۸	۱ - سیاست و خط مشی سایبری ۲-اطلاع رسانی تهدیدات سایری ۳-آموزش و تربیت امنیت سایبری ٤ -مشارکت در امنیت جهانی سایبری ۵-حمایت از خدمات دیجیتال ٦ - حمایت از خدمات حیاتی ۷-شناسایی و اعتماد الکترونیکی ۸-محافظت از اطلاعات شخصی ۹- تیم واکنش به حوادث سایبری ۱۰-مدیریت بحران سایبری ۱۱- پلیس مبارزه با جرایم

					سایبری ۱۲- عملیات سایبری نظامی

وضعیت موجود کشور جمهوری اسلامی ایران در حوزه امنیت سایبری

مرکز مدیریت راهبردی افتا در سال ۱۳۸۷ الگوی ارزیابی و تحلیل وضعیت امنیت فضای تبادل اطلاعات کشور را ارائه نمود که در این الگو، وضعیت امنیت فضای تبادل اطلاعات (افتا) کشور، از منظر ٤ بعد سیاسی، اقتصادی، اجتماعی/ فرهنگی و فناورانه، مورد توجه قرارگرفته است و با استفاده از ٦٤ مؤلفه و مجموعاً ٤١٥ شاخص، موردسنجش، ارزیابی و تحلیل قرار می گیرد.

جدول (٦): مؤلفه های الگوی ارزیابی و تحلیل وضعیت افتا کشور

ردیف	بعد	مؤلفه ها
۱	سیاسی	وضعیت خط مشی ها و طرح های کلان وضعیت قوانین و مقررات افتا وضعیت ساختارهای اجرایی (دولتی) افتا
۲	اجتماعی و فرهنگی	وضعیت کاربری افتا وضعیت منابع انسانی مولد در حوزه افتا وضعیت فرهنگ افتا وضعیت ناهنجاریهای اجتماعی مرتبط با افتا
۳	اقتصادی	وضعیت گردش مالی دولت در حوزه افتا وضعیت تولید افتا کشور وضعیت تقاضای افتا در کشور وضعیت سرمایه گذاری درزمینه افتا
٤	فناورانه	وضعیت زیرساختهای فنی افتا وضعیت توانمندیهای فناورانه افتا وضعیت زیرساختهای ارتقاء توانمندیهای فناورانه افتا

همچنین بر اساس بررسی های بعمل آمده توسط نهادهای بین المللی امنیت سایبری، کشور جمهوری اسلامی ایران دارای نقاط قوت و ضعف در این حوزه به شرح زیر می باشد.

نقاط قوت: وجود نظامات، قوانین و اسناد متعدد در حوزه امنیت سایبری، تقسیم کار ملی(نظام ملی پیشگیری و مقابله با حوادث فضای سایبری)، مشارکت بین المللی و همکاری ملی، تحقیق و

توسعه، وجود نهاد های پاسخگو، تیم های متعدد، مراجع و تیم های دولتی و خصوصی برای پیشگیری و تشخیص و واکنش (شاخص امنیت سایبری جهانی[1]، ۲۰۱۷).

نقاط ضعف: فقدان نقشه راه برای فناوری های نوین، مانند زنجیره بلوکی، رایانش ابری، ضعف در تعیین سنجه های امنیت سایبری، ضعف در دیپلماسی سایبری(فقدان قراردادهای دو یاچند جانبه)، ضعف در ظرفیت سازی(مانند عدم استقرار زیست بوم فناوری های نوین در زیرساخت های ملی)، ضعف در آموزش، ضعف در عملیات پدافندی به هنگام، داشتن سطح متوسط امنیت سایبری، ضعف در استانداردهای سازمانی و صنفی(شاخص امنیت سایبری جهانی، ۲۰۱۷).

سرانجام پس از مباحث محیط شناسی و مطالعه اسناد بالادستی، مدل ها، رویکرد های بین المللی، اسناد راهبردی امنیت سایبری سایر کشورها و مصاحبه با خبرگان حوزه های امنیتی، حقوقی و فضای سایبر، ابعاد و مؤلفه های الگوی راهبردی مواجهه با امنیتی شدن پدیده ها ی متاثر از فضای سایبر به صورت جدول (۷) پیشنهاد می گردد.

جدول(۷) ابعاد و مؤلفه های الگوی مواجهه با امنیتی شدن پدیده ها

ردیف	بعد	مؤلفه
۱	حکمرانی سایبری	سیاستگذاری، نگاشت نهادی، ظرفیت سازی، دیپلماسی سایبری، تدوین قوانین، مقررات و نظامات
۲	اشراف اطلاعاتی	رصد و پایش مستمر فضای سایبر در سطح ملی و بین المللی، داده کاوی و تحلیل هوشمند اطلاعات، توجه به روند فناوری های نوظهور، تسلط بر فنون روز، جلوگیری از رصد و نفوذ دشمن
۳	مدیریت امنیت سایبری	امنیت زیر ساخت، امنیت محتوی، امنیت خدمات و امنیت کاربران
٤	عوامل کلان محیطی	فناوری های برهم زن سایبری، عوامل علی پدیده ها، عوامل بستر ساز پدیده ها و عوامل و شرایط مداخله گر پدیده ها

حکمرانی: در اسناد سایبری کشورهای مختلف در حوزه حکمرانی سایبری مباحث سیاستگذاری، راهبری، نگاشت نهادی، ظرفیت سازی، همکاری های سایبری به چشم می خورد. در جمهوری اسلامی ایران به دلیل تقابل راهبردی با نظام سلطه از یک طرف و سوء استفاده ایالات متحده آمریکا از اعمال حکمرانی یک جانبه سنتی بر فضای سایبر در جهت برآورده ساختن منافع استکباری خود، بیش از

[1] .Global Cybersecurity Index (GCI)

هـر دولت دیگری از تهدیدات شناختی پدیده سایبر به اندازه تهدیدات فنی و زیر ساختی آن نگران اسـت. بـه همین دلیل انتقال پارادایمی از (حکمرانی اینترنت) به معنای حکمرانی صرفاً در لایه زیرساخت به حکمرانی (دیجیتال جامع) به معنای حکمرانی در لایه محتوا، خدمات و کاربران با تقویت مکانیزم های حکمرانی در زمینه امنیت سایبری، حریم خصوصی، حفاظت از داده های شخصی و فرآیند تولید و مصرف داده به عنوان یک ضرورت می باشد. لذا در این تحقیق پس از انجام مصاحبه با خبرگان، مؤلفه های، سیاستگذاری، نگاشت نهادی، ظرفیت سازی، دیپلماسی سایبری، تدوین قوانین، مقررات و تدوین نظامات به عنوان مؤلفه های بعد حکمرانی سایبری مورد تاکید قرار گرفتند.

اشراف اطلاعاتی: اشراف اطلاعاتی از نظر اصطلاحی عبارت است از: مجموعه اقداماتی که در اثر اجرای آن یک سازمان قابلیت احاطه و تسلط کامل بر روند گذشته، حال و آینده وقایع و حوادث حوزه پیرامونی (قلمرو) آن داشته باشد، به نحوی که بتواند در جهت پیشگیری و مقابله با تهدیدات و آسیب های مرتبط با آن و همچنین تولید فرصت ها، اقدام لازم و به موقع را به عمل آورد (جمشیدیان، ۱۳۸۸: ۳۳). عبیری و ولوی در مقاله ای با عنوان ارائه الگوی راهبردی مدیریت فضای سایبر جمهوری اسلامی ایران بر اساس اوامر و تدابیر حضرت امام خامنه ای(مدظله العالی)، اشراف اطلاعاتی را شامل مؤلفه های: اشراف در سطح ملی و بین المللی، توجه به روند فناوریهای نوظهور، تسلط بر فنون روز، تسلط راهبردی بر فضای مجازی، جلوگیری از رصد و نفوذ دشمن برشماری کرده اند(عبیری و ولوی، ۱۳۹۷: ۱۸۵). در این تحقیق پس از انجام مصاحبه با خبرگان، مؤلفه های، رصد و پایش مستمر فضای سایبر در سطح ملی و بین المللی، داده کاوی و تحلیل هوشمند اطلاعات، توجه به روند فناوری های نوظهور، تسلط بر فنون روز، جلوگیری از رصد و نفوذ دشمن مورد تاکید قرار گرفتند.

مدیریت امنیت: با توجه به اینکه تمامی اجزاء یا موجودیت های حاضر در فضای سایبر، نیازمند تأمین ساز و کارهای امنیتی می باشند، امنیت فضای سایبری نیز مانند ساختار نمایش داده شده برای لایه های تشکیل دهنده این فضا در قالب چهار سطح با عناوین امنیت زیر ساخت، امنیت محتوی، امنیت خدمات و امنیت کاربران، قابل طبقه بندی است.

عوامل محیطی کلان: متغیرهای محیطی (غیر قابل کنترل) و متغیرهای قابل کنترل:

یکی دیگر از متغیرهای موثر بر امنیتی شدن پدیده های متاثر از فضای سایبر که از مصاحبه های خبرگی بدست آمد، عوامل محیطی کلان است. این عوامل فیزیکی و ذهنی مربوط به محیط، بر پدیده ها تأثیرات مختلفی دارند و می توانند نقش سلبی و یا ایجابی در امنیتی کردن پدیده ها

ایفا کنند. عوامل محیطی لزوماً در اختیار و کنترل مدیران سطوح مختلف نیستند و از آنجا که قابل دستکاری نیستند، ممکن است در اجرا و اعمال تدابیر مدیریتی مشکلاتی را به وجود آورند. بر این اساس، پس از طرح موضوع با خبرگان جامعه آماری تحقیق ، توجه به فناوری های برهم زن سایبری، عوامل علی پدیده ها، عوامل بستر ساز پدیده ها و عوامل و شرایط مداخله گر پدیده ها به عنوان مؤلفه های بعد عوامل محیطی کلان مورد تاکید قرار گرفتند.

روش‌شناسی تحقیق

با توجه به موضوع و هدف تحقیق که به دنبال ارائه الگوی جلوگیری از امنیتی شدن پدیده های متاثر از فضای سایبر در راستای صیانت از امنیت داخلی است و نتایج آن، زمینه ایجاد وفاق در فرآیند تصمیم‌سازی و تصمیم‌گیری برای مدیران دستگاه های متولی را فراهم می‌نماید. بنابراین تحقیق حاضر بر اساس هدف در زمره انواع تحقیقات کاربردی قرار می‌گیرد. از طرفی این تحقیق با بررسی ادبیات جهانی و شرایط و اقتضائات بومی تلاش می‌نماید تا ادبیات موجود در این حوزه را توسعه و نیز ادبیات جدیدی را تولید نماید بنابراین توسعه ای نیز است. این تحقیق از نظر نوع، کاربردی – توسعه ای می‌باشد. روش تحقیق در این پژوهش از نظر ماهیت و نحوه گردآوری داده های آن، توصیفی، پیمایشی است. رویکرد مورد استفاده در این پژوهش ترکیبی و یا آمیخته (کیفی– کمی) است. برای رسیدن به اهداف تحقیق، در ابتدا با مطالعه کتابخانه ای اسناد بالادستی، مدل ها، رویکرد های بین المللی، اسناد راهبردی امنیت سایبری سایر کشورها مورد بررسی قرار گرفته و گزاره های نامرتبط که با شرایط مورد مطالعه همخوانی ندارند حذف شد. سپس از ابزار مصاحبه عمیق نیمه ساختار یافته تا حد اشباع نظری بهره گرفتیم تا پس از تجزیه و تحلیل، ابعاد، و مؤلفه های این پژوهش استخراج و ارائه شود. سرانجام بر اساس نتایج خروجی حاصل از مطالعات مرحله اول، گزاره های مورد نظر برای طراحی ابزار سنجش در مرحله دوم (مطالعه کمی) فراهم و با استفاده از ابزار پرسشنامه و نظر خواهی از جامعه نمونه آماری مرتبط با موضوع پژوهش، بهره گیری و نهایتا الگوی پژوهش با استفاده از تحلیل عاملی طراحی شد. در این قسمت برای تحلیل داده ها از نرم افزار Amoss استفاده شد.

حجم نمونه و روش نمونه‌گیری

با توجه به این که در این تحقیق از روش گلوله برفی با انتخاب هدفمند استفاده شده، نمونه برداری تا حصول اشباع نظری ادامه یافت. لذا در مرحله ی نخست تحقیق با تعداد ۱۰ نفر شامل

۵ نفر از اعضای هیئت علمی دانشگاه و ۵ نفر از مدیران ارشد فضای سایبر آشنا با مباحث سایبری، امنیتی و حقوقی در سازمان‌های متولی مصاحبه بعمل آمد.

در مرحله ی دوم برای اعتبار سنجی ابعاد و مؤلفه های احصاء شده از جمع بندی ادبیات تحقیق و مصاحبه خبرگان، تعداد۱۳۰ پرسشنامه که به تایید صاحبنظران رسیده بود بین جامعه ی آماری تحقیق متشکل از متخصصان، اساتید و صاحبنظران این حوزه توزیع و پس از جمع آوری تعداد ۱۱۷ پرسش نامه، نتایج آن مورد بهره برداری قرار گرفت.

روایی و پایایی تحقیق

به منظور بررسی روایی ابزار تحقیق (مصاحبه و پرسش نامه) و الگوی تحقیق از روایی صوری و روایی محتوایی استفاده شده است. به منظور تضمین روایی محتوایی و ارزیابی میزان هماهنگی محتوای ابزار اندازه گیری با هدف مورد نظر از قضاوت افراد خبره و متخصص در این زمینه استفاده و مورد تائید قرار گرفته است. پایایی تحقیق نیز با بررسی پایایی ابزار تحقیق مشتمل بر مصاحبه و پرسش نامه بررسی شده است. به گونه ای که برای بررسی پایایی مصاحبه های انجام شده، سؤالات مصاحبه در زمان های مختلف ارائه شد و با مقایسه پاسخ های دریافتی، پایایی یا همان تکرار پذیری بدست آمد. همچنین برای مشخص شدن میزان پایایی پرسش نامه تحقیق، با استفاده از نرم افزار SPSS ضریب آلفای کرونباخ محاسبه و مقدار آن ۷۹/ محاسبه شد. که بیانگر پایایی قابل قبول بود.

یافته‌های پژوهش

در بخش تحلیل داده های کیفی پژوهش، از تحلیل مضامین استفاده شده و نتایج حاصل از مصاحبه برای هر پرسش پس از تحلیل محتوا، توسط محقق در قالب جدولی که بیانگر ابعاد اصلی پژوهش می باشد درج و مفاهیم اولیه‌ای که از تحلیل محتوا حاصل شده، ارائه و در نهایت ۲۰ مؤلفه استخراج و ثبت گردید. در مرحله بعد مؤلفه‌های بدست آمده در قالب ٤ بعد دسته بندی شد. سرانجام داده های بدست آمده مورد تحلیل قرار گرفت: برای این منظور، از تحلیل عاملی استفاده شده است. در تحلیل عاملی، قبل از دسته بندی عاملی بر روی داده ها، از آزمون مقدماتی کایزر- مایز و آزمون بارلت برای تشخیص اینکه تعداد داده های مورد نظر برای تحلیل عاملی مناسب می باشد مطابق جدول (۸) استفاده شد.

در تحلیل عاملی، اگر مقدار بار عاملی کمتر از۰/۳ باشد نشان دهنده مقیاس ضعیف بوده و باید از

مدل حذف شود. بارهای عاملی بین ۰/۳ تا ۰/٦ نشان می دهند که متغیر مشاهده شده مقیاس متوسطی بوده و برای ادامه آنالیز کفایت می کند. مقادیر بزرگتر از ۰/٦ نیز نشان می‌دهند که متغیر مشاهده پذیر مقیاس قابل اطمینان برای محاسبه متغیر پنهان است. در کل مقادیر بارهای عاملی بزرگتر از ۰/٤ را می توان در مدل حفظ کرد(داوری و رضا زاده،۱۳۹۲ :٤٧).

جدول(۸): نتایج تحلیل عاملی اکتشافی ابعاد اصلی

ابعاد	تعداد مؤلفه ها	واریانس	آزمون کایزر- مایز و بارلت
حکمرانی سایبری	٦	۷۰/٤۰	Barttlett=230/252 , KMO=0/81
اشراف اطلاعاتی	٦	۷۲/۳۰	Barttlett=212/356 , KMO=0/89
مدیریت امنیت سایبری	٤	۷۳/۲۳	Barttlett=119/464 , KMO=0/83
عوامل کلان محیطی	٤	٦۷/۱۵	Barttlett=230/252 , KMO=0/91

همان گونه که در جدول(۸) ملاحظه می شود. مقدار آزمون آزمون کایزر- مایز و بارلت در کلیه ابعاد بالای ۰/٦ می باشد لذا بیانگر این است که تحلیل عاملی برای این داده ها مناسب می باشد. بنابراین ابعاد و مؤلفه های احصاء شده در بخش کیفی، مبنای تحلیل آماری قرار گرفتند. و در ادامه نتایج تحلیل عاملی اکتشافی بر اساس جدول(۸) و (۹) احصاء شدند.

جدول (۹): نتایج تحلیل عاملی اکتشافی ابعاد اصلی و تعین بار عاملی

بعد	بار عاملی	ضریب تعین R^2	مقدار t
حکمرانی سایبری	۰/۹۱	۰/۵۲	۱۱/۰۱
اشراف اطلاعاتی	۰/۸۹	۰/٤۸	۱۰/۰۳
مدیریت امنیت سایبری	۰/۸۷	۰/٤۵	۸/٦۵
عوامل کلان محیطی	۰/۸٤	۰/٤٦	۹/۷۵

جدول (۱۰): نتایج تحلیل عاملی اکتشافی مدل مفهومی

ابعاد	مؤلفه	بار عاملی
حکمرانی سایبری	سیاستگذاری	**۰/۹۳**
	نگاشت نهادی	**۰/۸۹**
	ظرفیت سازی	**۰/۷٤**
	دیپلماسی سایبری	**۰/۸۵**
	قانون و مقررات گذاری	**۰/۹٤**

	تدوین نظامات	۰/۸۱
اشراف اطلاعاتی	رصد و پایش مستمر فضای سایبر در سطح ملی	۰/۷۸
	رصد و پایش مستمر فضای سایبر در سطح بین المللی	۰/۵۸
	داده کاوی و تحلیل هوشمند اطلاعات	۰/۸۹
	توجه به روند فناوری های نوظهور	۰/۶۳
	تسلط بر فناوری های اجتماعی	۰/۸۹
	جلوگیری از رصد و نفوذ دشمن	۰/۶۸
مدیریت امنیت سایبری	امنیت زیرساخت	۰/۶۳
	امنیت محتوی	۰/۹۶
	امنیت خدمات	۰/۸۴
	امنیت کاربران	۰/۸۳
عوامل کلان محیطی	فناوری های برهم زن سایبری	۰/۶۲
	عوامل علی پدیده ها	۰/۸۹
	عوامل بستر ساز پدیده ها	۰/۸۲
	عوامل و شرایط مداخله گر پدیده ها	۰/۷۷

اطلاعات جدول(۱۰) نشان می دهد که تمام مؤلفه ها دارای مقادیر بارهای عاملی بزرگ تر از ۰/۶ دارند و از اعتبار لازم برخوردار می باشند. بعد از ارائه الگوی نهایی مذکور، برازش الگو مورد بررسی قرار گرفت. برای این منظور از شاخص نیکویی برازش[1] استفاده شد. از آنجا که مقدار شاخص نکویی برازش مدل برابر عدد ۰/۹۴ محاسبه شد و از عدد مورد قبول آن یعنی (۰/۹) بیشتر است. لذا بیانگر این است که الگوی بدست آمده از شاخص های انطباق بسیار خوبی بر خوردار بوده و مناسب بودن الگوی پژوهش را نشان می دهد. یعنی اینکه الگوی ارائه شده بر اساس مبانی نظری و یافته های بخش کیفی، دارای برازش لازم بوده و کلیت آن مورد تائید است.

[1] .Comparative Fit Index (CFI)

نتیجه‌گیری

هدف تحقیق معرفی الگویی برای جلوگیری از امنیتی شدن پدیده ها در فضای سایبر است. محقق برای رسیدن به اهداف تحقیق در ابتدا ادبیات و موضوعات مهم و تأثیر گذار بر امنیتی شدن پدیده های در فضای سایبر مورد بررسی قرار گرفتند که در این خصوص اسناد بالادستی، مدل ها، رویکرد های بین المللی، اسناد راهبردی امنیت سایبری سایر کشورها مورد مطالعه قرار گرفته و با استفاده از پرسش نامه محقق ساخته مبتنی بر مصاحبه با خبرگان ابعاد و مؤلفه های الگوی راهبردی مواجهه با امنیتی شدن پدیده ها مورد شناسایی قرار گرفتند. در بخش کمی، پرسش نامه محقق ساخته ای که شامل ٤ بعد و ٢٠ مؤلفه بود به صورت طیف پنج گزینه ای لیکرت طراحی گردید و پس از نظر خواهی از جامعه نمونه آماری، نتایج گردآوری شده به وسیله روش های کمی آمار توصیفی مورد تجزیه و تحلیل قرار گرفتند. در این قسمت برای تحلیل داده ها از نرم افزار Amoss استفاده شد. نتایج این پژوهش نشان داد بنا بر نظر خبرگان، ابعاد حکمرانی سایبری، اشراف اطلاعاتی سایبری، مدیریت امنیت سایبری و عوامل کلان محیطی به ترتیب بالاترین ضریب اهمیت را در حوزه مواجهه با پدیده ها را دارا هستند.

بعد از ارائه الگوی نهایی مذکور، برازش الگو مورد بررسی قرار گرفت. برای این منظور از شاخص نیکویی برازش[1] استفاده شد. از آنجا که مقدار شاخص نکویی برازش مدل برابر عدد ٠/٩٤ محاسبه شد و از عدد مورد قبول آن یعنی (٠/٩) بیشتر است. لذا بیانگر این است که الگوی بدست آمده از شاخص های انطباق بسیار خوبی بر خوردار بوده و مناسب بودن الگوی پژوهش را نشان می دهد. یعنی اینکه الگوی ارائه شده بر اساس مبانی نظری و یافته های بخش کیفی، دارای برازش لازم بوده و کلیت آن مورد تائید است. نکته قابل توجه در نتایج بدست آمده، هم خوانی این نتایج با ادبیات تحقیق است.

الگوی معرفی شده برای حل مساله، دارای این ویژگی است که با توجه به سوابق پدیده های امنیتی در فضای سایبر و با پرداختن به اقدامات حکمرانی برای پیشگیری و جلوگیری از امنیتی شدن پدیده ها در صدد پاسخگویی به مساله است. لذا نگاه به آینده و انجام پیش بینی و ارائه راهکار های پیشگیرانه ویژگی این الگو می باشد. همچنین در این الگو، مواردی مانند نگاه سیستمی و نظام مند به استفاده هم افزا از کلیه دستگاه های متولی و نهادهای حاکمیتی، مدیریتی و عملیاتی نقش پر رنگی دارد.

[1] .Comparative Fit Index (CFI)

کتابنامه

امام خامنه‌ای(مدظله العالی)، مجموعه بیانات قابل دسترس در پایگاه www.khamenei.ir

احمدی مقدم، اسماعیل و عابدی، یونس (۱۳۹۹). «نابرابری های اجتماعی و امنیتی شدن پدیده های اجتماعی»، فصلنامه مطالعات دفاعی استراتژیک، دوره هیجدهم، شماره ۸۲، صص ۳۵۶-۳۳۷.

امیری، عبدالرضا(۱۳۹۱). مطالعه فرآیند و متغیرهای مؤثر بر امنیتی شدن بحرانهای اجتماعی درایران»، فصلنامه مطالعات مدیریت انتظامی، دوره هفتم، شماره۲ ، صص۲۳۷-۲۱۹.

ایلالی، سیدحسن و بروجردی علوی، مهدخت (۱۳۹۷). «پیامدهای زیست مجازی ایرانیان»، فصلنامه مطالعات رسانه های نوین، دوره چهارم، شماره ۱۶، صص ۱۱۰-۷۵.

بوزان، باری (۱۳۷۸). مردم، دولتها و هراس، تهران: پژوهشکده مطالعات راهبردی.

بوزان، باری (۱۳۷۹). «آشنایی با مکتب کپنهاک در حوزه مطالعات امنیتی(گفتگوی علمی بوزان با پژوهشکده مطالعات راهبردی)»، فصلنامه مطالعات راهبردی،دوره نهم، شماره۳، صص ۱۹-۹.

تقی پور، رضا و همکاران (۱۳۹۸). «الگوی راهبردی حفاظت سایبری از زیر ساخت های اطلاعاتی حیاتی ج.ا.ا»، فصلنامه امنیت ملی، دوره نهم، شماره ۳۴، صص ۴۳-۱.

جمشیدیان، هادی (۱۳۸۸). اشراف اطلاعاتی، پلیس اطلاعات و امنیت عمومی ناجا، تهران: انتشارات حدیث کوثر.

داوری، علی و رضا زاده، آرش (۱۳۹۲). مدل سازی معادلات ساختاری با نرم افزارPLS، تهران: انتشارات جهاد دانشگاهی

دشتی، محمد (۱۳۸۰). نهج البلاغه، قم: مؤسسه انتشارات مشهور، چاپ یازدهم.

رمضانی، حسینعلی (۱۳۹۵). «ارائه مدل جامع تحلیل پدیده های اجتماعی»، چاپ در مجموعه مقالات علمی - پژوهشی کنگره جهانی علوم انسانی اسلامی.

عبداله خانی، علی (۱۳۸۹). نظریه های امنیت، تهران: موسسه مطالعات و تحقیقات بین المللی ابرار معاصر تهران.

عبداله خانی، علی (۱۳۸۵). «بررسی و نقد نظریه امنیتی ساختن»، مجله مطالعات راهبردی، دوره نهم، شماره۳۳ ، صص ۵۱۱-۴۹۱

عبیری، داوود و ولوی، محمدرضا (۱۳۹۸). «ارائه الگوی راهبردی مدیریت فضای سایبر ج.ا.ا بر اساس اوامر و تدابیر حضرت امام خامنه ای (مدظله العالی)»، فصلنامه امنیت ملی، دوره نهم، شماره ۳۲، صص ۲۰۰-۱۷۱.

محمدی منفرد، حسن، مهدی نژاد نوری، محمد (۱۳۹۹). «بررسی تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران»، فصلنامه امنیت ملی، دوره دهم، شماره ۳۶، صص ۲۴۲-۲۱۳.

نای، جوزف (۱۳۹۰). آینده قدرت، ترجمه رضا مراد صحرایی، تهران: حروفیه.

هایدگر، مارتین (۱۳۸۰). در آمدی بر وجود و زمان، ترجمه منوچهر اسدی، آبادان: نشر پرسش.

Adam Sadilek and John Krumm, "Far Out: Predicting Long- Term Human Mobility, Association for the Advancement of Artificial Intelligence, 2012, http: / / research. microsoft. com / en - us / um / people / jckrumm/

Balzaq.T. (2005). The Three Faces of Securitization:Political Agency,Audience and Context, *European journal of International Relations*, vol.11.No.2

Clay Shirky, Here Comes Every body: The Power of Organ izing without Organizations(New York: Penguin Press, 2008), 11–21

Chui, M., Manyika, J., Bughin, J., Dobbs, R., Roxburgh, Ch., Sarrazin, H., Sands, G., Westergren, M. (2012). The Social Economy: Unlocking Value and Profuctivity Through Social Technologies, McKinsey Global Institute Report.

ENISA, (2018), " ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, ENISA Report ETL 2018

ENISA, (2015), "Critical Information Infrastructures Protection approaches in EU", Final Document, TLP Green, Version 1.

Janna Anderson and Lee Rainie, Digital Life in 2025(Washington, DC: Pew Research Center, 2014), 5, http: // www. pewinternet. org / files / 2014 / 03 / PIP _ Report _ Future _ of _ the _ Internet _ Predictions _ 031114.

KS Min, (2015), "An International Comparative Study on Cyber Security Strategy", International Journal of Security and Its Applications Vol.9, No.2 (2015), pp 13-20

Martin Koyabe, (2015), "Critical Information Infrastructure Protection A Commonwealth Perspective", ITU Workshop on "ICT Security Standardization for Developing Countries, pp 1-45

McKinsey Global Institute et al., *The Social Economy: Unlocking Value and Productivity Through Social Technologies* (McKinsey Global Institute, 2012).

McDonald,m. (2008), Securitization and Construction of Security, *European Journal of Inernational Relations*, vol 14(4).OECD, (2018), "Recommendation of the Council on the Protection of Critical Information Infrastructures", OECD/LEGAL/0361

Geoffrey Parker, Marshall Van Alstyne, and Sangeet Paul Choudary, P*latform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, 2016, https://www.overdrive.com/search?q=747D962F-32B3-4F05-9126-A09E659AB96C

Gibson, William, *Burning Chrome*, Eos Publishers, New York, NY, 2003 Edition, 224 pages and William Gibson, *Neruomancer*, 20th Edition, Ace Publishers, New York, NY, 2004, 384 pp. In the latter book, Gibson defined cyberspace as: "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts."

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589

Janna Anderson and Lee Rainie, Digital Life in 2025(Washington, DC: Pew Research Center, 2014), 5, http: // www. pewinternet. org / files / 2014 / 03 / PIP _ Report _ Future _ of _ the _ Internet _ Predictions _ 031114. pdf.

Stritzel.H. (2007).Towards a Theory of Securitization: Copenhagen and Beyobd. *European Journal of International Relations*, vol.13(3)