فصلنامه مطالعات راهبردی فضای سایبر
سال دوم، شماره چهارم، پائیز ۱۴۰۲
مقاله سوم از صفحات ۹۶-۶۳

مدل مفهومی هوشمند مداری در فضای سایبری

آریان حامد[۱] اوژن کریمی[۲]

تاریخ دریافت: ۱۴۰۰/۱۱/۱۰ تاریخ پذیرش: ۱۴۰۱/۰۲/۳۰

چکیده

امروزه، قدرت هوشمند به‌عنوان عامل کاربردی و یک اهرم فشار قابل‌اطمینان از سوی دولت‌ها معرفی‌شده است. قدرت هوشمند با توجه به سیر تکاملی بودن خود نیازمند سامانهٔ حمایتی همه‌جانبه برای پیشبرد اهداف می‌باشد و برای حرکت روبه‌جلوی خود در نظام‌های بین‌المللی نیازمند حمایت کننده‌ای قوی دارد تا بتواند با توجه به رابطه مداری‌های بین‌المللی اهداف خود را پیش ببرد. این حمایت‌کننده قوی فضای سایبری می‌باشد. ادبیات در حوزه‌های مشترک امنیت سایبری و قدرت هوشمند هنوز در دوران اولیهٔ رشد خود به سر می‌برد.

این پژوهش براساس اهداف توسعه‌ای و ازنظر روش گردآوری داده‌ها، از نوع همبستگی می‌باشد، به این دلیل که پژوهشگر درصدد یافتن رابطه‌ای بین دو متغیر قدرت هوشمند و فضای سایبری، تعریف مکانیسم‌های هوشمندانه فضای سایبری و به‌دست آوردن ساختاری جامع از روابط متقابل قدرت هوشمند و فضای سایبری می‌باشد. در این پژوهش از منابع کتابخانه‌ای و پژوهش‌های میدانی بهره برده شده است و ازنظر هدف، صورت توسعه‌ای – کاربردی و ازنظر گردآوری داده‌ها توصیفی می‌باشد. این پژوهش به بررسی عوامل هوشمند در فضای سایبری پرداخته و رابطه‌ای سامانمند میان جنبه‌های مختلف این دو عامل را موردبررسی قرار داده است. عوامل قدرت هوشمند و فضای سایبری شناسایی گردید. مدل مفهومی نهایی براساس مؤلفه‌های به‌دست‌آمده طراحی گردید.

کلیدواژه‌ها: قدرت هوشمند، فضای سایبری، روابط متقابل، مدل مفهومی.

۱. کارشناسی ارشد مدیریت فناوری اطلاعات، نویسنده مسئول aryanhamed110@gmail.com
۲. عضو هیئت‌علمی دانشگاه پیام نور، karimi.oj@gmail.com

مقدمه

قدرت نمادی از پویایی سازمانی در رشته‌های مختلف کاری چه در سطح داخلی و چه در سطح بین‌المللی می‌باشد که بنابر شرایط امکان تغییر آن وجود دارد. قدرتی که ورای قدرت هنجاری و مادّی بشری بوده و بتواند در مسیر راهبردهای موردنظر گام بردارد. عاملی که به‌صورت سامانمند و کاملاً آگاهانه بستری را فراهم سازد که در آن قدرت از یک‌سو و مفهومی به نام سایبریسم از سوی دیگر در محل تلاقی خود باعث پدید آمدن عواملی شوند تا بتوانند به‌وسیله آن‌ها هوشمند مداری را در جهت اهداف موردنظر شناسایی نمایند. در فضای اطلاعاتی امروزی بیشتر فعالیت‌های انرژی مدار فرهنگی، اقتصادی و دیپلماسی و اجتماعی و... در فضای سایبر[1] صورت می‌پذیرد. سایبریسم و فضای سایبر فضای تعاملی با کارکردی پویا و میزان دسترسی متفاوت نبست به فعالیت‌ها می‌باشد (رادو،۲۰۱۳: ۳۲-۳٤). پژوهش پیش رو این نکته را در نظر می‌گیرد که چه عوامل و پروتکل‌هایی از قدرت هوشمند[2] در فضای سایبری به کار گرفته شوند تا بتوان با توجه به‌ضرورت حفظ امنیت در فضای اطلاعاتی موردنظر، هوشمند مداری را پیاده‌سازی نمایند (استیونس، ۲۰۱۵: ۲۰-٤۱).

بیان مسئله: مسئله اصلی و سؤال کلیدی در این پژوهش بر این اساس مطرح می‌شود که با توجه به رشد روزافزون فضای سایبری و پیدایش هوشمند مداری قدرت و با توجه به اینکه در راستای اعمال سیاست‌های هوشمندانه در فضای سایبری عوامل ارتباطی قدرت هوشمند با فضای سایبری برحسب مؤلفه‌های به‌وجود آمده بین قدرت هوشمند و فضای سایبری چیست؟ اولین دلیل اهمیت قدرت هوشمند در فضای سایبری، شناسایی عوامل قدرت هوشمند در فضای سایبری می‌باشد و منظور این است که عواملی را موردبررسی قرار دهیم که تأثیر مستقیمی بر عملکرد یگانگی قدرت هوشمند در فضای سایبری را دارا می‌باشند. دومین دلیل، منابع به‌کار گرفته‌شده چه از بعد اجتماعی و معنوی، اقتصادی،

1. Cyber Space
2. Smart Power

فرهنگی سیاسی می‌باشد. سومین دلیل اهمیت قدرت هوشمند در فضای سایبری نادیده گرفتن عوامل غیرجنگی به‌عنوان منابع رشد یک کشور می‌باشد. قدرت هوشمند از ابزار ترکیبی از اقتصادی و دیپلماتیک و توسعه، ابزار قانونی و نظامی جهت دستیابی به اهداف سیاست خارجی می‌باشد (یی کوانگ هنگا و لی کوان یو، ٢٠١٥: ٢٨٤).

اهمیت و ضرورت پژوهش

صرف‌نظر از اینکه موضوع سایبر و امنیت سایبری[1]در دیدگاه کشوری و بین‌المللی موردبررسی قرارگرفته است با این وجود بررسی‌های نشان می‌دهد که آن‌طور که باید و شاید به مقولهٔ سایبر از دیدگاه جزئی‌نگری پرداخته نشده است. اگر بخواهیم ملاک عمل را بر پایه مقالات فارسی معتبر قرار دهیم، به این موضوع می‌رسیم که موضوع سایبر در حوزه جنگ[2]و تهدیدات[3]بیشتر مورد بررسی قرارگرفته و درواقع همه آن‌ها بینش یکسانی نسبت به موضوع سایبر دارند. لزوم پیشروی هدف در این نوع روابط، پیاده‌سازی ساختاری هوشمندانه می‌باشد که می‌توان در مسیر شکوفایی قدم برداشته و قدرت واقعی برای پیاده‌سازی اهداف طرف‌های رودررو را نشان دهد.

پیشینهٔ پژوهش

صرف‌نظر از اینکه موضوع سایبر و امنیت سایبری در دیدگاه کشوری و بین‌المللی مورد بررسی قرارگرفته است با این وجود بررسی‌های نشان می‌دهد که به مقوله سایبر از دیدگاه جزئی نگری پرداخته نشده است. اگر بخواهیم ملاک عمل را بر پایه مقالات فارسی معتبر قرار دهیم به این موضوع می‌رسیم که موضوع سایبر در حوزه جنگ و تهدیدات بیشتر مورد بررسی قرارگرفته و همه آن‌ها خودآگاه و ناخودآگاه بینش یکسانی نسبت به موضوع سایبر دارند. دربارهٔ مقالات بین‌المللی و نظریه پردازانی که بر روی موضوع قدرت

1. Cyber Security
2. War Area
3. Treats

هوشمند پرداخته‌اند می‌توان از جوزف نای، سوزان ناسل و ریچارد آرمیتاژ نام برد که مهم‌ترین نظریه پردازان درزمینهٔ قدرت هوشمند می‌باشند.

اهداف پژوهش

موضوع این پژوهش شناسایی عوامل هوشمند در فضای سایبری می‌باشد؛ بنابراین هدف این پژوهش به‌دست آوردن راهکارهای هوشمندانه ترکیبی به‌وسیله عوامل قدرت هوشمند و فضای سایبری در فضایی هوشمندانه می‌باشد. اهداف این پژوهش به شرح زیر می‌باشد:

- تعریف مکانیسم هوشمندانه فضای سایبری با استفاده از عوامل تأثیرگذار.
- تعریف مکانیسم‌های غیرجنگی برای افزایش کاربری امنیت در فضای سایبر.
- به‌دست آوردن ساختاری جامع از روابط متقابل قدرت هوشمند و فضای سایبری.

مبانی نظری

قدرت: قدرت توانایی تأثیرگذاری بر دیگران برای دستیابی به نتایجی است که می‌خواهد و می‌تواند با اجبار، پرداخت یا جاذبه انجام شود (نای، ۲۰۱۲: ۱۵۱). قدرت برمی‌انگیزاند، امری را تسهیل ساخته و یا دشوار می‌سازد محدودیت ایجاد کرده یا امروز نهی می‌کند. قدرت ازنظر بنکلر ظرفیت وجودی برای تغییر رفتارها باورها و نتایج و یا مخالفت برخی نهادهای دیگر می‌باشد. شرکت‌های بزرگ و دولت‌ها مکان اولیه برای قدرت‌های متمرکز در جامعه معاصرمی باشند (بنکلر و یوچای، ۲۰۱٦: ۲۰-۱۹).

در مباحث قدرت، سه یا چهار بعد از ابعاد مانند قدرت، بالای قدرت، به سمت قدرت، با قدرت یکی از پایه‌های اصلی تحلیل علمی را تشکیل می‌دهد. قدرت، حاصل موقعیت در شبکه بوده و به‌طورمعمول به عامل اجازه استخراج سهام بیشتری از منابع مشترک را می‌دهد (هوگارد، ۲۰۱۲: ۳۵۳). از موضوعات مهمی که در قدرت مورد بررسی قرار می‌گیرد، مقوله جهانی شدن می‌باشد که هدفمندی قدرت را تحت تأثیر خود قرار داده و

جنبه جدیدی از قدرت که قدرت هوشمند می‌باشد را معرفی می‌نماید (پترس، ٢٠١٦: ١-٣). در نظر پژوهشگران قدرت سخت نوعی از قدرت است که مهم می‌باشد. کتاب مشهور رابرت کگان به نام بهشت و قدرت بر قدرت سخت متمرکز می‌باشد. به‌نظر کگان قدرت توسط ارتش ارزیابی می‌شود و توانایی برای رسیدن به نتایج مطلوب قدرت یکی از راه‌های انجام این عمل می‌باشد. می‌توان قدرت دولت را توسط ارتش اندازه‌گیری نمود (پترسون، ٢٠٠٨: ٣٤٩-٣٤٠).

قدرت سخت[1]: قدرت سخت در نظر برخی از محققان، تنها نوع قدرت بوده که مهم می‌باشد. برای مثال، بحث رابرت کگان درباره قدرت در کتاب مشهور او بهشت و قدرت به شدت بر قدرت سخت متمرکز است. ازنظر کگان قدرت توسط ظرفیت ارتش ارزیابی می‌گردد و توانایی رسیدن به نتایج مطلوب را با یکی از راه‌های موجود دارد (کیگان، ٢٠٠٤ و ٢٠٠٣). قدرت سخت ظرفیتی برای ناگزیر کردن آن‌ها برای انجام کار می‌باشد و راهبرد آن در مداخله نظامی، دیپلماسی و تحریم‌های اقتصادی برای به اجرا درآوردن منافع ملی تمرکز دارد. در نگارش دانشگاهی یک روش نئورئالیستی می‌باشد که تمایل به تأکید بر قدرت سخت در مورد دولت‌ها دارد (ویلسون، ٢٠٠٨: ١١٤). قدرت سخت به توانایی اقتصادی و نظامی یک کشور برای تحمیل ارزش‌ها اشاره دارد (کاشی‌ام و عبدالا: ٢٠١٢) قدرت سخت یک عنصر ناشناخته و دردناک باقی می‌ماند و در محیط بی‌ثبات است (شر ٤، ٢٠١١: ١١).

قدرت نرم[2]: مفهوم «قدرت نرم»، توسعه‌یافته درزمینهٔ روابط بین‌الملل، توسط متخصصان ارتباطات متعدد به‌عنوان یک روش برای توضیح چگونگی محصولات فرهنگی کشور می‌تواند جذابیت کلی آن و درنتیجه تأثیر آن درصحنه جهانی را به دست آورد. دولت‌ها این ایده را در تلاش‌های خود در «دیپلماسی عمومی»[3] پذیرفته‌اند که اشاره به ارتباطی است که به‌سوی مردم خارجی به‌عنوان مخالف دولت‌های دیگر مطرح می‌شود (جورج، ٢٠١٦: ١). جاشوا رامو کوپر استدلال می‌کند که قدرت نرم یکی از آن ایده‌های زیبا و

1. Hard Power
2. Soft Power
3. Public Diplomacy

علمی است که بسیاری از آزمایش‌های سیاست خارجی را شکست داد و استدلال می‌کند که «ارتش توسط حتی عمیق‌ترین رابطه فرهنگی متوقف نشده است (نای، ۲۰۱۲: ۱۵۲–۱۵۱). قدرت نرم، زمینه را که در آن کشورهای دیگر تصمیماتی در اختیار دارند که به منافع کشورهای قدرت نرم لطمه می‌زند، تنظیم می‌کند و شرایط کشورهای هدف را داوطلبانه انجام می‌دهد (گالارتی، ۲۰۱۱: ۳۰–۲۵). قدرت سخت و نرم با یکدیگر در ارتباط می‌باشند، به این دلیل که هر دو توانایی رسیدن به هدف با توانایی تأثیر بر رفتار دیگران را دارند. قدرت سخت و نرم‌افزاری تقویت می‌شود و گاهی با یکدیگر هم تداخل پیدا می‌کنند. قدرت نرم به تنهایی خوب نبوده و همیشه بهتر از قدرت سخت نمی‌باشد (نای، ۲۰۰٦: ٤–۳). قدرت سخت، به‌طور عمده ناگزیر از پیروی از منابع قدرت ملموس می‌باشد – روش‌های مستقیم‌تر (از طریق استفاده نمادین). درحالی‌که قدرت نرم آن را از طریق سیاست‌ها، کیفیت‌ها و اقداماتی که کشورها را به دیگر ملل جذاب می‌کند از طریق روش‌های غیرمستقیم، پرورش می‌دهد (گالاروتی، ۲۰۱٤: ۸–٤).

قدرت هوشمند: قدرت هوشمند به معنی شناخت نقاط قوت و محدودیت هر ابزار است. مفاهیم دقیق و تعاریف قدرت هوشمند ضروری هستند؛ اما طراحی و اجرای قدرت هوشمند همواره در یک زمینهٔ سازمانی عملی صورت می‌گیرد. یکی از چالش‌های اطلاعات فنّاوری بحرانی امروزی در قدرت هوشمند این است که دولت‌ها و افراد فنّاوری را به‌عنوان خوب و بد به کار می‌برند؛ بنابراین سیاست گزاران به‌طور مداوم نیاز به باقی ماندن در بازی‌های سیاستی جهت ماندن در فضای اینترنتی مربوطه دارند (سریان، ۲۰۱۵: ۱۹–۱٤). هر مذاکره‌ای در رابطه با دستیابی به قدرت هوشمند باید با پذیرفتن اینکه طبقه‌بندی نهادی فعلی یک توده سنگین و بزرگ را تشکیل می‌دهد، آغاز گردد، پیگیری همکاری قدرت هوشمند به معنی شناسایی تفاوت‌های فرهنگی و ترکیب کردن و تعدیل نمودن عملیات بین‌المللی اصلاح‌شده می‌باشد. لازمه دستیابی به قدرت هوشمند، ترکیب ماهرانه عوامل مفهومی، نهادی و سیاسی می‌باشد که به یک جنبش اصلاحات می‌انجامد که بتواند نوآوری‌های سیاست خارجی را در آینده حفظ کند (ویلسون، ۲۰۰۸: ۱۱۲–۱۱۱).

اولین قدم به قدرت هوشمند و راهبردهای تبدیل قدرت مؤثر درک کامل طیف وسیعی از منابع انرژی و مشکلات ترکیب آن‌ها در زمینه‌های مختلف است (نای، ٢٠١١: ٢٠). قدرت هوشمند مورد ارزیابی قرار می‌گیرد و یک راهبرد غیراجباری بوده که هدف آن جذب «دیگران» به مجموعه‌ای از اهداف و ارزش‌ها یا دستور کار موردنظر است. یکی از ویژگی‌های قدرت هوشمند این است که ارتش به‌عنوان یک منبع نرم و قدرت سخت دیده می‌شود. قدرت هوشمند یک ایده می‌باشد که در آن بازیگر می‌تواند ترکیب مختلفی از قدرت سخت و نرم به‌عنوان انگیزه یا تهدید، به‌عنوان یک راهبرد که دیگران را به پذیرش ارزش‌ها تشویق نموده و خود را با سیاست‌های لازم هماهنگ نمایند را طراحی می‌نمایند. قدرت هوشمند نقطه پایانی نداشته، یک پویایی که به‌طور پیوسته درحالی‌که تغییراست می‌باشد (ادی و پائولاین، ٢٠١٦: ٣٢٤-٣٢٣).

هنگامی‌که عمل نمودن به قدرت سخت موجب ضعیف شدن قدرت نرم می‌گردد رهبری را با مشکل روبرو می‌سازد. توانایی ترکیب مفید و مؤثر قدرت نرم و سخت قدرت هوشمند را به وجود می‌آورد (نای و آرمیتاژ، ٢٠٠٧). استفاده از مفهوم قدرت جهانی به‌وسیله این واقعیت که به‌طور تقریبی با قدرت هوشمند مترادف می‌باشد، تضعیف شده و با کاربری قدرت سخت و نرم ترکیب‌شده است. قدرت هوشمند به‌طور صرف برای تصمیم‌گیری اینکه ترکیبی کیمیاگرانه از بهترین ابزار کاری برای هر وضعیت امنیتی که در آن قرار دارد، می‌باشد که حداقل این‌گونه باید باشد. به همان اندازه ابعاد جنجالی وجود دارد که قدرت و ارزش‌ها آن را برآورده می‌کنند (تانا و سنگ، ٢٠١٥: ٣٣٣-٣٣٢). درحالی‌که قدرت نرم و اجزای قدرت سخت‌افزاری قدرت هوشمند به طریقی تقریباً معکوس متفاوت است، در توانایی برابر نیست (رستیک و راجاراتنام، ٢٠١٦: ٣٩١).

قدرت هوشمند نشان می‌دهد بیشتر کشورها به شدت مایل به استفاده از طیف وسیعی از ابزارهایی می‌باشند که در اختیارشان است مانند ابزار مدارس، اقتصادی، نظامی، سیاسی، قانونی و فرهنگی و ابزار مناسب را متناسب و یا ترکیبی از ابزارها را متناسب با هر موقعیتی به کار می‌برند (فنگ، ٢٠١٦: ٧). قدرت سخت با ابزار نظامی مرتبط است؛ اما قدرت سخت

را می‌توان در روش‌های نرم‌تر برای تولید قدرت هوشمند استفاده کرد. تقویت توانایی نظامیان ضعیف خارجی نمونه‌هایی از کاربرد نرم‌افزاری قدرت سخت نظامی است (مارینو و برین، ۲۰۰۹: ۲). آلمانی‌ها توانسته‌اند قدرت سخت و نرم را دریک آمیختگی از قدرت با یکدیگر ترکیب نموده که این امر نشان می‌دهد که نای و آرمیتاژ به چه صورتی ازقدرت هوشمند نام می‌برند (پترسون، ۲۰۰۸: ۳۵۰). قدرت هوشمند برای مقابله با مشکلات کشور نمی‌باشد و درباره جدید سازی رهبری می‌باشد که خود را با اجرا و پاسخگویی تطبیق داده و در راهبرد و نفوذ آمریکا دردنیای درحال تغییر به چشم می‌خورد (آرمیتاژ و نای، ۲۰۰۸: ۳).

عوامل قدرت هوشمند و رویکردهای آن

استراتژی: راهبردهای قدرت هوشمند باید از موضع مخاطبان، نه کسانی که آن را گسترش می‌دهند، نگاه کنند و انعطاف‌پذیر باشند (ادی،۲۰۱٦: ۳۲۸). راهبرد قدرت هوشمند منابع قدرت سخت و نرم را ترکیب می‌کند؛ دیپلماسی عمومی دارای تاریخچهٔ طولانی به‌عنوان وسیله‌ای برای ارتقاء قدرت نرم کشور است و برای برنده شدن در جنگ سرد ضروری است. راهبرد ارتباطات نمی‌تواند کار کند، درصورتی‌که علیه سیاست متوقف شود، اقدامات با صدای بلندتر از کلمات صحبت می‌کنند و دیپلماسی عمومی که فقط پنجره پوشیدن برای نمایش قدرت سخت است بعید است موفق باشند (نای، ۲۰۰۸: ۱۰۲–۹٤).

مؤلفه‌های هوشمند مدار راهبرد

ابزار مدیریتی[1]: به‌عنوان یک ابزار مدیریت، توجه به یکپارچگی چارچوب‌ها و روش‌هایی که از تصمیم‌گیری در مورد بهبود بهره‌وری اقتصادی بهره می‌برند، موردتوجه قرارگرفته است. نویسندگان پیشنهاد می‌کنند که استفاده از فرایندها که بر اساس سلسله‌مراتب است، یک عنصر ضروری از ابزارها باشد. هدف رویکرد طراحی ابزار

1. Management Tool

مدیریت مطالعه موردی است که چگونه ابزارهای مشابه را توسط تمرین کنندگان توسعه داد (لیتسب و برزیلو، ۲۰۱۷: ۵۰۵). ابزارهای مدیریت مرجع محصولاتی هستند که به کاربران هدایت می‌شوند که هدف آن ایجاد یک پایگاه اطلاعاتی کتابشناختی بزرگ است که از فعالیت‌های علمی آن‌ها پشتیبانی می‌کند. ابزارهای مرجع مدیریت سامانهٔ اطلاعاتی جهانی غنی‌شده توسط تعامل اجتماعی کاربران را ایجاد می‌نماید (اورتگا، ۲۰۱٦: ٦٥).

فعالیت[1]: فعالیت به مجموعه‌ای از عملکردهایی گفته می‌شود که در رابطه با پیشبرد اعمال ساختاریافته و گستردگی ساختاری صورت می‌پذیرد. این مجموعه عملکردها در صورتی به سرانجام می‌رسد که بتوان بیان درستی ازآنچه درباره پیوستگی اعمال انجام‌شده در رابطه با وضعیت‌های به وجود آمده، پیش می‌آید داشت. این پیوستگی را چگونه می‌توان بیان نمود. سطوح فعالیت بسته به زمان و نوع فعالیت انجام‌شده و در حال انجام فرق می‌کند. دو نوع اصلی فعالیت ازلحاظ میزان تأثیر گزاری و تأثیرپذیری وجود دارد که به فعالیت‌های داخلی و بین‌المللی مشهور می‌باشند. فعالیت‌های داخلی آن دسته از فعالیت‌هایی می‌باشد که پایه و اساس هر فعالیتی را تشکیل می‌دهد که به‌عنوان فعالیت‌های درون تیمی سیاسی معرفی می‌گردند.

تصمیم[2]: تصمیم‌گیری‌ها در جهت نظم دادن به کار می‌روند. به این دلیل که می‌توانند تغییرات از پیش تعیین‌شده را بر مبنای ورود و خروج‌های مشخص، پیدا نموده و بر اساس سیاست‌های از پیش تعریف‌شده در نظام‌های جهانی، راهکاری را در جهت برآورده ساختن نیازهای امنیتی به کار ببندند. تصمیم‌گیری فرایندی نیمه‌خودکار بوده که بر اساس روش‌های مطالعاتی مربوط به هر سیستم فرق می‌کند و می‌تواند اصول متفاوتی را داشته باشد. این اصول همواره حفظ‌کننده منافع خویش بوده و برای آن مبارزه می‌کنند. روش‌های امنیتی در این نوع اصول پایدار نبوده و بسته به شرایط ممکن است تغییر پیدا نماید. این

1. Activity
2. Decision

تغییرات پی در پی ممکن است زیان‌هایی را متوجه سامانه‌های اطلاعاتی دولت‌ها در رده‌های امنیتی سطوح بالا قرار دهد.

کنترل[1]: کنترل شاید در بیشتر موارد به‌عنوان یک واژه کلیدی در سطح عمومی به‌کاررفته باشد. از این نظر به آن واژه کلیدی گفته می‌شود که می‌تواند توانایی برقراری چیدمانی خاص و یکتا را برای هر یک از سامانه‌های پیش‌رونده در فرایند راهبری مسیر هدف داشته باشد. قدرت‌طلبی نقش مهمی را ایفا می‌نماید و بر اساس آن می‌توان راهبردی را جهت محافظت از سامانه‌های کنترل پیاده‌سازی نمود. نقش قدرت در کنترل، نقشی مدیریتی می‌باشد که بر اساس ساختاری هوشمند عمل می‌نماید. این رفتار، سامانه‌ای را می‌طلبد که بتواند با توجه به نیازهای امنیتی کنترل از آسیب رساندن به روابط جلوگیری نموده و بیگانگی را در نمادهای کنترل از بین ببرد. قدرت هوشمند نیاز به کنترل هوشمندانه‌ای دارد که توسط رهبر اجرایی اجرا می‌شود (فرای، ۲۰۱٤: ۳۱).

مؤلفه‌های هوشمند مدار کنترل

اثربخشی و کارایی: کارایی مربوط به «انجام درست‌کار» برای دستیابی به حداکثر خروجی است، درحالی‌که کارایی مربوط به «انجام کارهای مناسب» با انجام اقدامات لازم برای دستیابی به اهداف پروژه است. برآیی و اثربخشی هر دو برای تأمین موفقیت پروژه تضمین‌شده اهمیت دارد، کارایی معیارهای موفقیت کوتاه‌مدت است، درحالی‌که کارایی معیارهای موفقیت درازمدت است (مقبول، ۲۰۱۸: ۱۳-٦). اثربخشی قدرت هوشمند، به‌عنوان ترکیبی از دو طرف، قدرت سخت، چسبنده و نرم، بر اساس مفاهیم اعتماد عمومی در کشورهای دریافت کننده سنجیده می‌شود (ادی و پائولین، ۲۰۱٦: ۳۲٤).

قوانین و مقررات: در یک کشور که قانون حاکمیت اساسی داشته باشد، قدرت هوشمند در زمینه‌های قانونی و بین‌المللی موفق عمل می‌کند. باید یک پارادایم قانونی جهت همگام‌سازی‌های کامل قدرت هوشمند وجود داشته باشد. قانون این قابلیت را دارد که به‌عنوان یک ابزار قدرت هوشمند در مبارزه با تهدیدات نامتقارن به کار گرفته شود

1. Control

(امنیت عمومی ۲۰۰۹). قانون را می‌توان از این منظر طبقه‌بندی نمود که در چه مواردی امکان استفاده درست و تأثیرگذار از قانون وجود دارد. می‌توان ازنظر استفاده از قانون آن را به دو نوع قانون سخت و قانون نرم طبقه‌بندی نمود که در قوانین بین‌المللی استفاده می‌شوند. قانون سخت اشاره به قوانین به هم پیوسته‌ای مانند قطعنامه‌های شورای امنیت سازمان ملل متحد و قواعد عرفی حقوق بین‌الملل دارد (استراتون، ۲۰۰۹: ۷-۲).

مشارکت[1] در طول تاریخ افراد برای به دست آوردن مشارکت دموکراتیک و به دست آوردن نتایج جنگیدند. باید به این نکته اذعان داشت که به دست آوردن ابزاری که بتواند نتیجه‌های مطلوب را استخراج نماید، امری بسیار دشوار می‌باشد. یکی از ویژگی‌های مشارکت سیاسی امروز یک آرایه در حال گسترش از فعالیت‌های سیاسی فراتر از اشکال انتخاباتی مشارکت سیاسی می‌باشد (مارتین، ۲۰۱۲).

نوآوری[2]

نوآوری همانند خلاقیت نیروی محرّکه قرن بیست و یکم می‌باشد. اقتصاد جهانی به‌طور فزاینده‌ای شکل می‌گیرد و به‌وسیله نوآوری‌های فردی و سازمانی بهبودیافته است. نوآوری می‌تواند جدید باشد یا موجودیت جدیدی را قبول کند و باید به‌عنوان فرآیند سیستم ایدئال در نظر گرفته شود که ایده خلاقانه توسط محیط شکل‌گرفته و محیط با نوآوری تغییر می‌یابد (مای فیلد، ۲۰۱۱: ۱). نوآوری تبدیل به یکی از موضوعات مهم در لغت‌نامه مدیریتی رفتار شده است (کوزینتز و همتزبرگر و چائو، ۲۰۰۸: ٣٤).

سازمان‌های عمومی سیاست‌های نوآوری را به‌عنوان ابزاری برای تأثیر گزاری بر روند نوآوری استفاده می‌نمایند. امّا ابزارهای سیاست نوآوری به‌طورمعمول با یکدیگر ترکیب‌شده‌اند که حاکی از آن می‌باشد که تأثیرات مکمل یا متعادل‌کننده‌ای در سامانه‌های نوآوری دارد (بوراس و اکوئیست، ۲۰۱۳: ۱).

1. Participation
2. Innovation

سیاست نوآوری مانند سیاست دولت نشان دهنده سلسله‌مراتب کنترلی می‌باشد که عوامل آن را توضیح می‌دهد. اثرات سیاست بستگی به جزئیات و بسیاری از عواملی که ممکن است مانند دیگر عوامل توجیه‌ناپذیر باشند. تا زمانی که اثرات مورد ارزیابی قرار بگیرند توجه سیاست‌گزاران در جای دیگری بوده و روایت‌هایی که سیاست را توجیه می‌کند، به دست فراموشی سپرده شده‌اند (لِین و لیئوا و آداری، ۲۰۱۱: ۸٦-۸۳).

مؤلفه‌های هوشمند مدار نوآوری

ارتباطات بین‌المللی[1]: ارتباطات شامل تبادل اطلاعات، افکار، ایده‌ها و احساسات می‌باشد و از طریق فرایندها و روش‌های مختلف بسته به سبک‌های مورد استفاده رخ می‌دهد. هر روش ارتباطی پتانسیل‌ها، محدودیت‌ها، مشکلات و فرصت‌های خود را دارد (پاسادئوس وکفالاکی: ۲۰۱۲). هنگامی‌که ما درباره ارتباطات بین‌المللی و یا ارتباطات در روابط بین‌المللی صحبت می‌کنیم، درواقع به هفت بعد این مسئله می‌پردازیم که عبارت‌اند از فنّاوری، ارتباطات از راه دور، محصولات فرهنگی اخبار، پست الکترونیکی، ارتباطات فرهنگی و زبان. این هفت بعد مربوط به فعالیت‌های سیاسی ارتباطات بین‌المللی می‌باشند شامل سازمان‌های بین‌المللی ارتباطات، قوانین ارتباطات بین‌المللی، اجلاس‌های بین‌المللی فعالیت‌های سیاسی، عملکردها و سیاست‌های آن‌ها می‌باشد (آلین و پاکوستا، ۲۰۱۲: ۲).

فضای سایبری: یکی از مشکلات کلیدی کاربران فضای سایبری این است که در حال عبور از مرزهای سریع اما غافلگیرکننده و قانونی، غیرقانونی و اخلاقی و مذهبی می‌باشند. برای کسانی که در دنیای سایبری جستجو می‌نمایند، در بیشتر اوقات نشانه‌هایی مشخص از زمانی است که از مرزهای جغرافیایی عبور کرده‌اند و نمادها چنین تفاوت‌هایی را شناسایی می‌کنند. در فضای سایبری، می‌تواند در مرزهای جغرافیای حرکت نمود، بدون اینکه از واقعیت آگاه باشد (گیلام و وارتانانس،۲۰۱۳: ۲۰۳). یک راه برای درک فضای سایبری به‌طورکلی و حملات سایبری به‌طور خاص، در نظر گرفتن آن به‌عنوان سه لایه می‌باشد که عبارت‌اند از: لایه فیزیکی، لایه ترکیبی بالاتر از فیزیکی، لایه معنایی که بالاتر از

1. International Communication

همه قرارگرفته است. همه سامانه‌های اطلاعاتی در لایه فیزیکی که شامل جعبه‌ها و گاهی سیم‌ها می‌باشند، باقی می‌مانند. فضای سایبری توسط مقامات محافظت می‌شود (لیبیکی، ۲۰۰۹: ۱۳-۱۲). فضای سایبری که به آن سریع‌ترین فضای فناوری اطلاعات در طول تاریخ بشر نیز گفته می‌شود، در کاربردهای جدید و در حجم‌های بزرگی از داده‌ها در حال ظهور بوده و فرصت‌های بالقوه‌ای را از طریق سامانه‌های اقتصادی برای بهبود سامانه‌های سایبری به کار می‌بندد (فیشر، ٢٠١٤: ٦).

عوامل فضای سایبری و رویکردهای آن

امنیت سایبری[1]: امنیت سایبری به حفاظت از شبکه‌ها و سامانه‌های اطلاعاتی در برابر اشتباهات انسان، بلایای طبیعی، مشکلات فنی و یا حملات مخرب می‌پردازد. امنیت سایبری بخشی از یک تحول بسیار گسترده در جامعه‌ای که توسط فناوری اطلاعات و ارتباطات هدایت می‌گردد و در آن اتصالات دیجیتالی فزاینده اشاره به افزایش سرعتی که افراد، فرایندها و اشیاء در اتصال به اینترنت دارند، می‌نماید. امنیت سایبری تلاشی را در حفظ دسترسی و یکپارچگی شبکه و زیرساخت و محرمانه بودن اطلاعات موجود در آن انجام می‌دهد (کمیسیون اروپا،٢٠١٦).

امنیت سایبری وضعیتی است که در آن فضای سایبری به‌وسیله رویدادهای تصادفی یا داوطلبانه که شامل مالکیت و انتقال داده‌ها و تخریب غیرقانونی و یا مسدود نمودن سامانه‌های اطلاعات در زیر سایه اقدامات امنیتی مناسب محافظت می‌شود. این اقدامات شامل ممیزی ایمنی، مدیریت به‌روزرسانی امنیتی، روش‌های احراز هویت، تجزیه‌وتحلیل خطر، تشخیص و پاسخ به حوادث و حملات، کاهش اثرات، بهبود اجزای در معرض حمله، آموزش‌وپرورش شخصی و افزایش امنیت فیزیکی که سامانه‌های اطلاعات و ارتباطات در آن قرار می‌گیرند (آنجلینی و آکوری و بالدونی و همکاران، ۲۰۱۳).

بر طبق تعاریف کاولتی و سافر، عدم وجود یک تهدید از طریق فناوری اطلاعات و ارتباطات و شبکه‌ها می‌باشد. مازن و وابر امنیت سایبری ر ادر ابعاد جهانی به‌عنوان یک

1. Cyber Security

عامل جدید برای مبارزه علیه تروریسم می‌دانند (استیونس، ۲۰۱۵: ٤١-۲۰). سیاست‌گذاران امنیتی زمانی به فضای سایبری توجه می‌کنند که مورد تهدید واقع شوند برای اولین بار با توجه به پیدایش شبکه‌های جهانی نوظهور بازیگران می‌توانند حملاتی را برای قربانیان خود طرح‌ریزی نمایند که برای مقابله با این‌گونه تهدیدات با قوانین قضایی ضعیف مواجه می‌شویم (وامالا، ۲۰۱۱). چالش‌های فنی و سازمانی مطرح‌شده درباره امنیت سایبری بسیار گسترده می‌باشند و تنها می‌توان از طریق یک راهبرد منسجم و در نظر گرفتن نقش‌های مختلف در چارچوب‌های بین‌المللی می‌توان به این مهم دست پیدا نمود (آی تی یو، ۲۰۱۰). این آسیب پذیری که بیشتر فضای سایبری را تهدید می‌کند، در داشته‌های زیر ساختی اطلاعاتی و ساختارهای پشتیبانی خارجی پدیدار می‌گردد. به‌طورکلی دشمنان و مدافعان می‌توانند اقدامات مثبت و منفی خود را در فضای سایبری و همچنین در دیگر موارد مانند حوزه‌های دیپلماتیک، اطلاعاتی، نظامی و اقتصادی به اجرا بگذارند (ریسا و باتس و شنویا،۲۰۱۱: ۵۸). بسیاری از مسائل به وجود آمده امنیت سایبری در طبیعت اقتصادی می‌باشند و مداخله‌هایی که انگیزه‌ها و شکست‌های ذینفعان را همتراز می‌نماید می‌تواند به بهبود وضعیت امنیت سایبری کمک نماید. سیستم در بیشتر مواقع با شکست مواجه می‌شود به این دلیل که سازمان‌هایی که از آن‌ها دفاع می‌کنند نمی‌توانند شکست را تحمل نمایند. سیاست باید مسئولیت‌ها را اختصاص دهند به‌طوری‌که احزاب در یک موقعیت برای رفع مسائل تمایل به انجام این کار داشته باشند (مور، ۲۰۱۰). در تقابل زمین، هوا، دریا و فضا فضای سایبری در مقابل مشکلات منحصربه‌فردی قرار می‌گیرد. با توجه به حضور شبکه‌ها در تمام نقاط، متصدیان تهدید می‌توانند حملاتی مضطرب کننده علیه قربانیان را در حوزه‌های اجرایی و با قوانین ضعیف به اجرا بگذارند (وامالا،۲۰۱۱: ١٤). اقدامات اجرایی و قانون‌های پیشنهادی تا حد زیادی برای رسیدگی به جهات مخالف در امنیت فضای سایبری طراحی شده‌اند: جلوگیری از بلایای مبتنی بر سایبر و جاسوسی، کاهش اثرات حملات موفقیت‌آمیز، بهبود همکاری داخلی و مبارزه با جرائم اینترنتی. چالش‌های سخت‌تری درزمینهٔ طراحی، انگیزه، اجماع و محیط‌زیست وجود دارد: پیش‌بینی

نمی‌باشند (فیشر، ٢٠١٦: ١٢). جایگزینی برای مطالعات عملیات واقعی را می‌توان با تمرینات آموزشی عملیات سایبری پیدا نمود. این محیط‌ها ممکن است ابزاری برای فعالیت شرکت‌کنندگان، استفاده از ابزار نرم‌افزاری و موفقیت در انجام اهداف و فعالیت‌ها باشد (ابوت و مک کلین و اندرسون و نائور و فورسیته، ٢٠١٤: ٧-٥). کاربران درک مطمئنی از تأثیرات مثبت و منفی امنیت سایبری دارند.

فرایند امنیت سایبری تبدیل به یک موضوع انسانی شده است و نیاز کنترل‌های فنی بیشتری دارد. تحقیق در مورد فرهنگ سایبری به دو بخش نظرگاه فنی و نظرگاه متمرکز انسانی می‌باشد. دیدگاه انسانی بر عوامل انسانی که به‌طور اساسی با رفتار انسانی تعامل دارد، تأکید می‌ورزد (کازا و سولمز و گروبلر و وورن، ٢٠١٧: ٤). امنیت فضای سایبری به یکی از مهم‌ترین حوزه‌های سیاست جهانی قرن بیست و یکم و یک عصر رقابت شدید سیاسی تبدیل شده است (رادو،٢٠١٣: ٣٢). در بیشتر موارد روش‌های به کار گرفته شده در دسترس عموم نبوده و دارای ارزیابی پیچیده‌ای می‌باشد تحولات اخیر از روش‌های قوی‌تر از تمرکز اندازه‌گیری در شرکت‌های فردی و سازمان‌ها و نه درکل شبکه ارزشی خواهد بود (دوتن، بائر و ویلیام، ٢٠١٦: ١٢-٧).

مؤلفه‌های امنیتی فضای سایبری

شناسایی[1]: بسیاری از سازمان‌ها نیاز به یک کمک حرفه‌ای دارند تا بتوانند پاسخی سریع به یک حادثه امنیتی بدهند. شناسایی سازمان‌هایی که دسترسی‌های موردنظر را داشته و کارشناسان واجد شرایط که بتوانند اطلاعات حساس شرکت‌های بزرگ را با بهترین شرایط محافظت نمایند کار دشواری می‌باشد (کرسی وگلوور، ٢٠١٣: ٤). امنیت سایبری به شناسایی و ارزیابی و حل‌وفصل تهدیدات سایبری به‌منظور کاهش خطرات سایبری و از بین بردن اثرات حملات سایبری، تروریسم سایبری و جاسوسی سایبری با افزایش

1. Authentication

محرمانگی، یکپارچگی و در دسترس بودن داده‌ها و سامانه‌های اطلاعاتی و زیرساخت اطلاعات و ارتباطات می‌پردازد (ناوراتی، ۲۰۱٤: ۵).

تجزیه و تحلیل[1]: سازمان‌هایی که در آن‌ها امنیت سایبری رعایت و اجرا می‌گردد، دارای ساختار یکپارچه بوده که به‌جای تهدید در خط مقدم از شیوه‌های راهبردی، تاکتیکی و عملیاتی استفاده می‌نماید. معماران مهندسان و تحلیلگران پایبند به یک روش مشترک می‌باشند که شامل تجزیه‌وتحلیل خطر و اطلاعات تهدید در سرتاسر سامانه‌های در حال توسعه و فرایندهای عملیاتی می‌باشد. فناوری‌های سایبری نشان دهنده یکی از چالش‌های مهم برای امنیت ملی امروزه بسیاری از کشورها می‌باشند. تحلیل گران امنیت سایبری به شناسایی و طبقه‌بندی و کاهش حملات سازمان‌یافته به مرزهای سازمانی و ملی می‌نمایند (جاسلین و چود هری و هاگلین، ۲۰۱۳: ۱). استفاده از فناوری اطلاعات در سرتاسر جهان و به‌طور فزاینده‌ای در جوامع مرکزی در حال گسترش می‌باشد. در آینده وابستگی سایبری رشد پیدا نموده و به‌عنوان فضای سایبری بیشتر و بیشتر آسیب پذیر می‌گردد. این همان چیزی است که مشارکت بخش دولتی و خصوصی به اجرا و حمایت در برابر حملات سایبری می‌پردازند و آینده در زیرساخت‌های ملی و حیاتی مانند برق و شبکه‌های ارتباط از راه دور می‌باشد که همیشه مستعد ابتلا به اختلال می‌باشند (استال و تسیر، ۲۰۱۱: ۷). امنیت سایبری یک مسئله رو به رشد برای سازمان‌ها ازجمله فرودگاه‌ها می‌باشد. درحالی‌که خطرپذیری سنتی زیر ساخت فناوری اطلاعات در بیشتر موارد برجسته می‌باشند، بیشتر فرودگاه‌ها بیشتر بر سامانه‌های کنترلی که خطراتی را که کمتر آشکار می‌باشند اتکا می‌کنند (مورفی و سوکاریه، ۲۰۱۵: ۷).

دفاع سایبری[2]: با وجود سابقه فعالیت حملات سایبری، دفاع سایبری یک مفهوم جدید محسوب می‌گردد. به این خاطر که دولت‌ها ساختار جدیدی را برای ارائه دفاع سایبری و امنیت سایبری به‌طور گسترده به کار گرفته‌اند. هر کشوری که در این زمینه ترکیبی از

1. Analyze
2. Cyber Defense

سامانه‌های دولتی، خصوصی و نظامی را فراهم سازد در این زمینه فعال می‌باشد (گیلز و هارتمن: ۲۰۱۵). دفاع‌های سایبری که امروزه استفاده می‌شوند، در مقابل بیشتر اشکال حملات سایبری تأثیرگذار نمی‌باشند. دفاع سایبری طیف گسترده‌ای از فعالیت‌هایی است که افراد را قادر می‌سازد خود را در برابر حملات محافظت نموده و یک پاسخ به تهدیدهای درحال رشد بدهند. تعامل در این زمان شامل تجزیه و تحلیل فنی و بررسی‌های مورد نظرتا اطمینان حاصل شود که می‌توان از نقشه‌های امنیتی و دفاعی مورد نظر استفاده نموده و بتوان از مسیرهای حمله محافظت نمود (ابوت و مک کلین و اندرسون و نائور و سیلوا و فرسیته، ۲۰۱۵: ۵۰۸۹).

مؤلفه‌های دفاعی فضای سایبری

شناسایی معیارها: معیارها در دفاع سایبری عواملی می‌باشند که بر اساس میزان و گستردگی استفادهٔ سازمان‌ها و دولت‌ها می‌توانند طراحی و پیاده سازی و اجرا گرند. معیارها وزن دفاع را مشخص می‌نمایند بدین معنی که می‌توانند با استفاده از پیوندهای دوگانه و یا چندگانه بر اساس ترتیب استفاده در موقعیت زمانی و مکانی خاص خود قرار گرفته و بر اساس اولویت بندی‌های از پیش تعیین شده مورد استفاده قرار گیرند. این اولویت بندی‌ها به دو قسمت تقسیم می‌شوند. اولویت‌های زمانی و اولویت‌های مکانی. اولویت‌های مکانی نوعی از اولویت می‌باشد که بر اساس موقعیت‌های به وجود آمده در سامانه‌های دفاعی در سازمان‌ها و دولت‌ها می‌توانند سیستم یکسان سازی فیزیکی معیارها را با یکدیگر همگون سازند. اولویت‌های زمانی نوعی از اولویت می‌باشند که بر اساس موقعیت‌های به وجود آمده روابط بین‌المللی بتوانند ازنظر زمانی ساختار دفاعی را به گونه‌ای برنامه ریزی نمایند که اولویت‌های دفاعی رعایت گردند.

سنجش راهبردی[1] به منظور جمع آوری و به کار بردن اهرم نفوذ هوشمند در جهت ساخت یک برنامه دفاع سایبری تهدید گرا یک سازمان باید جنبه‌های برنامه‌های سایبری را

1. Strategic Assessment

در نظر بگیرد (بُینی و کُنُلی و اسکروپکا و کروگر و سامرز، ۲۰۱۵: ۸-٤). سنجش راهبردی بر اساس مؤلفه‌های به دست آمده از بررسی‌های به عمل آمده در محدوده‌های امنیتی جهت به کارگیری سامانه‌های بهینه سازمانی و بین‌المللی طراحی و به کار گرفته شده است که می‌توان توسعه‌های امنیتی در سطح وسیعی ایجاد نمود.

خطرپذیری (ریسک)[1] خطرپذیری سایبری یک اصطلاح مشترک در بسیاری از نشریات و رسانه‌ها می‌باشد. در وسیع‌ترین مفهوم خطر سایبری به‌عنوان بهترین درک خطر انجام کسب و کار در محیط سایبری می‌باشد؛ مانند یک اصطلاح گسترده که ممکن است غیرکاربردی باشد، مفهوم خطرپذیری سایبری در برابر تعریف خطرپذیری‌ها ضروری هست. این خطرپذیری‌ها ممکن است از برخی از منابع که پیش‌بینی‌نشده می‌باشند سرچشمه گیرند و اثرات آن‌ها می‌تواند متفاوت بوده و می‌تواند در تعدادی از راه‌های کسب‌وکار تأثیرگذار باشد. حمله به زیرساخت‌های حیاتی مانند سامانه‌های کنترل صنعتی شدید بوده و عواقب گسترده‌ای داشته باشد (سی آر سی، ۲۰۱٤). ارزیابی خطرپذیری امنیت اطلاعات باید یک محدوده تعریف روشن که شامل ارزیابی روابط خطرپذیری با نواحی دیگر باشد، داشته باشد. ارزیابی خطرپذیری باید به‌صورت دوره‌ای و یا زمانی که هر تغییری در مورد سامانه‌های اطلاعاتی سازمان‌ها وجود دارد، باشد (پهری و ادریس، ۲۰۱۰: ۱۲). ارزیابی خطرپذیری امنیت سایبری بر تمرکز و بر اساس رویکرد ارزیابی خطرپذیری کسب‌وکار بوده است. بااین‌حال با توجه به یک محیط دفاعی معین، خطرپذیری امنیت سایبری نیاز به ارزیابی کلی بیشتر، تحلیلگر فناوری اطلاعات و پدافندی و مهاجم دارد. اجرای موفقیت‌آمیز ارزیابی کلی خطرپذیری امنیت سایبری نیازمند توسعه معیارهای اندازه‌گیری برای ویژگی‌های امنیت اطلاعات ازجمله محرمانه بودن، صداقت و در دسترس بودن را دارد. در توسعه ارزیابی خطرپذیری امنیت سایبری، آزمایشگاه تحقیقاتی ارتش امنیت سایبری، تعاملی را جهت ایجاد چارچوبی برای ارزیابی خطرپذیری امنیت سایبری و دفاع پیشگیرانه انجام می‌دهد (هنشلا و کازینا و هافمنب و کلیک، ۲۰۱۵:

1. Risk

١١١٨). یک رویکرد پیشگیرانه مانند به وجود آوردن فعالیت‌های آموزشی برای کارکنان، توسعه و پیاده‌سازی روش کار رسمی برای به دست آوردن استانداردها و ابزارها، سیستم کنترل داخلی و ارزیابی‌های دوره‌ای می‌تواند به سازمان در جهت کاهش تأثیرگذار اثرات قابل‌توجهی از حوادث امنیتی که می‌تواند در آینده رخ دهد و به‌طور کامل از بین نمی‌روند، یاری رساند (استرویی و روسو، ٢٠١١: ٢٣٠-٢٢٩).

ارزیابی اجازه تعیین سطح قابل قبولی از خطرپذیری را خواهد داد و مدیریت مناسبی را برای کنترل خطرپذیری بالقوه برای اطلاع‌رسانی سامانه‌ها و شبکه‌ها و اهمیت اطلاعات محافظت شده اتخاذ می‌نماید. به دلیل اتصالات سامانه‌های اطلاعاتی، ارزیابی خطرپذیری باید شامل توجه به آسیب احتمالی که ممکن است به‌وسیله دیگران انجام شود باشد (رامساروپ، ٢٠٠٣: ١٤). ارزیابی جامع از خطرپذیری امنیت سایبری دارای عوامل پیچیده چند جزئی و چند سطحی شامل سخت‌افزار، نرم‌افزار، محیط‌زیست و عوامل انسانی هست. به‌عنوان بخشی از تلاش‌های موردنظر در رابطه با ایجاد مدل ارزیابی تعیین عوامل انسانی که رفتار انسانی را شامل می‌شود احتیاج به درک چگونگی رفتار کاربران، مدافعان و مهاجمان تأثیرگذار بر روی خطرپذیری امنیت سایبری دارد (هنشلا و کاینسا و هُفمِنب و کِلِیک، ٢٠١٥: ١١١٨). چالش‌های زیادی در امن کردن تهدید در فضای سایبری وجود دارد. ماهیت امنیت سایبری به‌عنوان یک مسئله امنیت ملی مبهم بوده پتانسل مبهمی برای وضع دشوار امنیتی در دامنه وجود دارد (هِیر، ٢٠١٥: ٢). برای مدیریت امنیت سایبری و خطرپذیری، سازمان باید الزام و تعهدی را در تمام سطوح برای حفظ امنیت و حریم خصوصی خطرپذیری و با ترکیب کردن این خطرپذیری‌ها با خطرپذیری‌های دیگر به‌عنوان بخشی از راهبرد اولویت‌بندی و پرداختن به چالش‌های خطرپذیری حاضر و آینده صورت پذیرد (پرودی، ٢٠١٦: ٧).

مؤلفه‌های خطرپذیری سایبری

واکنش‌های اجتماعی:[1] خطرپذیری‌های سایبری در محیط‌های بین‌المللی بازتاب‌های گسترده‌ای بخصوص در سطح اجتماعی هر کشوری دارد. این بازتاب‌های گسترده به‌طورمعمول در سطوح جوامع با ارتباطات داخلی و بین‌المللی نمود خاصی پیدا می‌کند تا جایی که بتوان از آن به‌عنوان یکی از عوامل تعیین‌کننده برتری اجتماعی از نگاه فردی و درنتیجه برتری بین‌المللی از نگاه روابط متقابل نام برد. مطالعه سامانه‌های سایبری اجتماعی یک چارچوبی از سیاست‌های رسیدگی فوری به تهدیدات سایبری و چالش‌های آن هست که این چالش‌ها منفعت‌های اجتماعی را در نوآوری‌های فنی افزایش می‌دهد.

عدم موفقیت: عدم موفقیت در خطرپذیری سایبری به عواملی گفته می‌شود که باعث بر هم زدن سامانه‌های تعاملی سایبری در مواجهه با خطرپذیری امنیتی می‌گردد. سیستم تعاملی در خطرپذیری سایبری به مجموعه‌ای از عامل‌های کنترل‌کننده در امنیت سایبری گفته می‌شود که روابطی را بر پایه اصول همگرایی تنظیم نموده تا بتواند سیستم امنیت سایبری را در راستای منافع پیش روی آن به جلو حرکت داده و خطرپذیری سایبری را به کمترین میزان ممکن برساند. عدم موفقیت با بررسی عامل‌های خطرپذیری پذیر مورد آزمایش قرار می‌گیرد.

جاسوسی سایبری:[2] جاسوسی سایبری اشاره به استفاده از قلمرو سایبری بیشتر از طریق نرم‌افزارهای مخرب یا هک کردن مانند فیشینگ کیت به سرقت، آزار و اذیت، جمع‌آوری اطلاعات و یا شناسایی توانایی مهاجمان شبکه را دارد. جاسوسی سایبری توسط دولت‌ها، بازیگران غیردولتی و افراد صورت می‌پذیرد (کوهن و فدریچ، ۲۰۱۵). جاسوسی یک فرم قدیمی از کسب و کار دولتی هست که از طریق فضای سایبری روند ساده‌تری را در پیش‌گرفته است. در جاسوسی سایبری، حضور فیزیکی لازم نمی‌باشد (سوئن و اَبمان، ۲۰۱٤: ٤). جاسوسی سایبری مانند انواع دیگر جاسوسی‌ها، برای یک فعالیت مشروع برای یک

1. Social Reactions
2. Cyber Espionage

کشور مستقل برای عمل نمودن در برابر یکدیگر در نظر گرفته‌شده است ظهور فضای سایبری ماهیت جاسوسی را تغییر داده است. علاوه بر این جاسوسی سایبری می‌تواند در مقابل اهداف بسیاری از کشورهای جهان هدایت شود. هنجارهای حول جاسوسی سایبری از جاسوسی‌های سنت گرایانه دولت _ دولت ناشی می‌شوند. به‌طور تقریبی هر کشوری با منابع و توانایی‌های فنی برای انجام کارها، جاسوسی سایبری را هم در حول فضای سایبری هم و در حول مجموعه‌های هوشمند انسانی انجام می‌دهد (کلارک، ۲۰۱۵).

مؤلفه‌های جاسوسی فضای سایبری

جاسوسی سایبری اقتصادی[1]: جاسوسی اقتصادی سایبری اسرار کسب و کار تجاری شرکت‌ها و نهادهای دولتی و غیردولتی را تحت تأثیر خود قرار داده و تفاوت زیادی با جاسوسی صنعتی به خاطر فعالیت‌ها مالی دولتی دارد. تعیین کمیت تلفات جاسوسی اقتصادی کار دشواری هست. اثرات جاسوسی اقتصادی به‌طور کامل منفی بوده و دولت‌ها میان کشورها را مورد هدف قرار داده و مانع به وجود آمدن یک سیستم کسب و کار رقابتی در بستر امنیتی فضای سایبری شده و در اقتصاد رقابتی کشورها امری رایج می‌باشد (دنیلسون و ای‌ای، ۲۰۰۹: ۵۰۷-۵۰٤). اگرچه عوامل مختلف می‌تواند عدم واضح بودن قوانین وضع‌شده درباره جاسوسی سایبری اقتصادی را مشخص نموده و مکانیزمی برای انجام فعالیت‌ها به کار گیرد تا مانع به وقوع پیوستن چنین خساراتی گردد که در برخی از مواقع قابل جبران نمی‌باشند (اسکینر و پاراجُن، ۲۰۱٤).

جاسوسی سایبری نظامی[2]: گرچه بسیاری از کشورهای دنیا از جاسوسی سایبری استفاده نموده و آن را در برنامه‌های خود به کار می‌بندند ایالت متحده آمریکا، روسیه و چین شامل پیشرفته‌ترین جاسوسان سایبری می‌باشند. این دستورالعمل‌های امنیتی که به‌عنوان پایه‌های جاسوسی نظامی سایبری به‌کاربرده می‌شوند مانند راهبردها، آموزه‌ها،

1. Economic Cyber Espionage
2. Military cyber espionage

روش‌ها و پروتکل‌هایی برای جنگ سایبری، به‌عنوان سمبل‌های آماده‌سازی جنگ سایبری مانند آموزش کارکنان نظامی در دفاع سایبری به‌عنوان بخشی از عملیات نظامی معمولی می‌باشند (رابینستِین، ۲۰۱٤: ۲). عناصر مشترک در دکترین نظامی شامل استفاده از قابلیت سایبری برای شناسایی و عملیات اطلاعاتی حملات سایبری و به‌عنوان مکمل عملیات جنگ و ارتباطات الکترونیکی می‌باشند (لوییس وتیملین، ۲۰۱۱: ۳).

جاسوسی سایبری صنعتی[1]: جاسوسی سایبری صنعتی توسط جرائم سازمان‌یافته و شرکت‌های بزرگ برای به دست آوردن اطلاعات و یا مالکیت معنوی به‌طورمعمول برای استفاده اقتصادی می‌باشد. جاسوسی سایبری بیشتر به سمت تأثیرپذیری اقتصادی، سیاسی و اجتماعی سوق داده می‌شود؛ اما پیامدهای امنیت ملی با تلفیق جاسوسی در دولت وجود دارد که به سامانه‌های اطلاعاتی ارتباط پیدا نموده است. شاید جای تعجب نباشد که دنیای جاسوسی صنعتی در دید عمومی قرار می‌گیرد و انگیزه کمی برای شرکت‌هایی که دچار نقض هوشمندی در جهت برطرف کردن مشکلات عمومی خود شده‌اند (کابای، ۲۰۰۸: ۳).

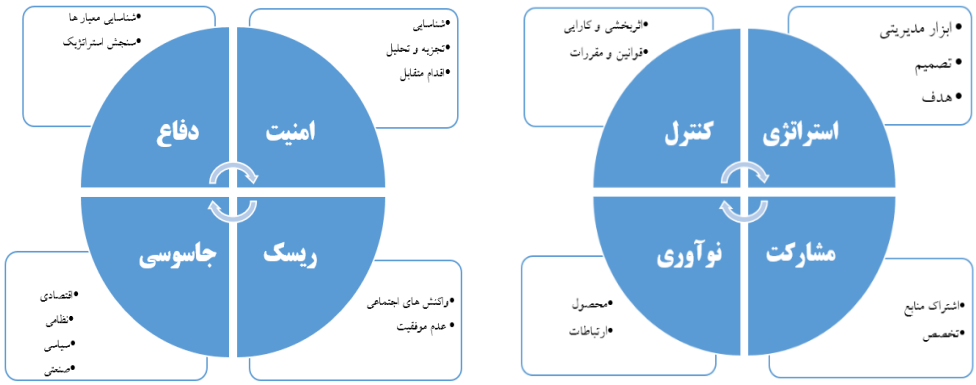
جاسوسی سایبری سیاسی[2]: جاسوسی سایبری یک واقعیت زندگی در سیاست بین‌المللی هست که هیچ رهبر سیاسی نمی‌تواند بدون آن زندگی کند. درحالی‌که رهبران سیاسی دانا به‌خوبی می‌دانند که موانع ذاتی در بازی فریب متقابل جاسوسی رسیدن به حد بالایی از جاسوسی را می‌طلبد (کورمیا، ۲۰۰۹: ۳).

روش تحقیق

روش تحقیق ازنظر هدف به‌صورت توسعه‌ای – کاربردی و ازنظر گردآوری داده‌ها توصیفی می‌باشد و عوامل توسعه‌ای قدرت هوشمند و فضای سایبری به‌عنوان عوامل کلیدی موفقت در ایجاد ساختاری مناسب و هماهنگ شناخته می‌شوند. روش گردآوری اطلاعات مورد نیاز در مرحله نگارش ادبیات، مقالات علمی، کتاب‌ها و پایگاه‌های علمی

1. Industrial Cyber Espionage
2. Political Cyber Espionage

معتبر می‌باشند. روشی که برای پیشبرد این تحقیق به‌کاررفته است، روش تحقیق ترکیبی هست که بر اساس ترکیب دو نوع تحقیق کمی و کیفی در نظر گرفته‌شده است. این پژوهش به بررسی عوامل هوشمند در فضای سایبری پرداخته و رابطه‌ای سامانمند میان جنبه‌های مختلف این دو عامل را مورد بررسی قرار می‌دهد. نوع تحقیق ازنظر اجرا «پیمایش دلفی کلاسیک» می‌باشد. به دلیل اینکه عوامل ازنظر کاربردی عاملی قدرت هوشمند و فضای سایبری مورد بررسی قرار نگرفته بودند به‌صورت مدل‌های جداگانه مورد بررسی و به‌صورت کلی در مدل مفهومی نهایی قرار گرفتند. جامعه آماری شامل خبرگان و صاحب‌نظران حوزه سایبری و قدرت هوشمند که دارای تحصیلات دانشگاهی هوانوردی و مدیریت دولتی، علوم سیاسی و روابط بین‌الملل می‌باشند، استفاده‌شده است.



شکل شمارهٔ ١: مدل مفهومی فضای سایبری و قدرت هوشمند

در این پژوهش از طیف لیکرت هفت گزینه‌ای و دلفی ٤ مرحله‌ای استفاده شده است. در مرحله اول یافته‌های میدانی و کتابخانه‌ای و تجربیات و نوآوری‌های به دست آمده پژوهشگر و خبرگان و صاحبنظران مورد بررسی قرارگرفته و عواملی که کمینه ٦٠ درصد را به دست آوردند، در مرحله بعدی مورد بررسی قرار گرفتند (جدول‌های ١ و ٢).

جدول شماره ١:

عوامل قدرت هوشمند	مرحله اوّل		مرحله دوّم		مرحله سوّم		مرحله چهارم	
عامل	میانگین	رتبه	میانگین	رتبه	میانگین	رتبه	میانگین	رتبه

مشارکت	٦,٥٨	١	٦,٦١	٤	٦,٧١	٤	٦,٥٨	٣
کنترل	٦,٥٧	٢	٦,٦٤	٣	٦,٧٤	٣	٦,٥٤	٤
راهبرد	٦,٣٣	٣	٦,٧١	١	٦,٧٨	١	٦,٦٤	١
نوآوری	٦,٣	٤	٦,٦٨	٢	٦,٧٥	٢	٦,٥٨	٣
ابزار مدیریتی	٥,٠٣	٥	–	–	–	–	–	–
تصمیم گیری	٤,٨٩	٦	–	–	–	–	–	–
آینده نگری	٤,٨٣	٧	–	–	–	–	–	–
حمله نرم	–	–	٥,٨٨	٥	–	–	–	–
حمله هوشمند	–	–	٥,٧٩	٦	–	–	–	–
مدیریت زمان هوشمند	–	–	–	–	٦,٤	٥	٦,٦١	٢
فعالیت	–	–	–	–	٥,٦٩	٦	–	–
تصمیم گیری	–	–	–	–	٥,٦٧	٧	–	–
اثربخشی و کارایی	–	–	–	–	٥,٦٥	٨	–	–
تفکر	–	–	–	–	٥,٦	٩	–	–

جدول شماره ۲: عوامل فضای سایبری

عوامل فضای سایبری	مرحله اوّل		مرحله دوّم		مرحله سوّم		مرحله چهارم	
عامل	میانگین	رتبه	میانگین	رتبه	میانگین	رتبه	میانگین	رتبه
جاسوسی	٦,٤	١	٦,٧١	٣	٦,٧٥	٢	٦,٦٤	٣
امنیت	٦,٣١	٢	٦,٦٨	٤	٦,٧١	٣	٦,٧٥	١
خطرپذیری	٦,٢٦	٣	٦,٧٨	١	٦,٨١	١	٦,٧٥	١
دفاع	٦,٢٣	٤	٦,٧٥	٢	٦,٦٨	٤	٦,٦٨	٢
تهدید	٥,٩	٥	–	–	–	–	–	–
حملات سایبری	٥,٣٧	٦	–	–	–	–	–	–
فضای سایبری هوشمند	–	–	٦,٢٩	٥	٦,٢٩	٥	٦,٧٥	١
اقدام متقابل	–	–	٥,٤٢	٦	–	–	–	–
مهارت سایبری	–	–	–	–	٥,٩٢	٦	–	–
واکنش‌های اجتماعی	–	–	–	–	٥,٤٢	٧	–	–

تجزیه و تحلیل آماری

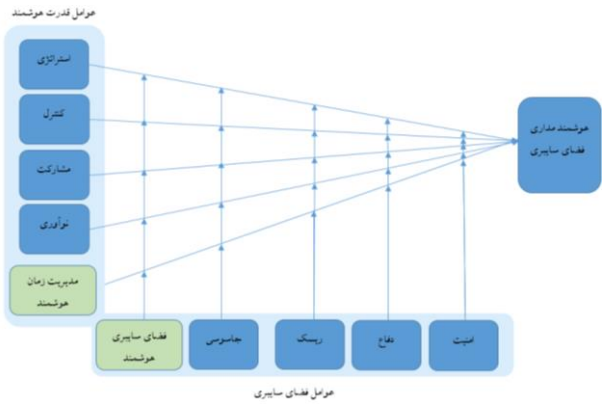
در این پژوهش برای تجزیه و تحلیل داده‌ها از نرم‌افزار Smart PLS, SPSS استفاده شده است که با کمک آمارهای توصیفی و استنباطی داده‌های به دست آمده مورد تجزیه و تحلیل قرار می‌گیرند. برای تجزیه و تحلیل داده‌ها و آزمون فرضیه‌های پژوهش از

روش‌های آمار استنباطی استفاده می‌شود. برای سنجش پایایی مدل از آلفای کرونباخ و پایایی مرکب استفاده شده است. از آنجایی که مقادیر بارهای عاملی بیش از ۰,۷ می‌باشد و به دلیل اینکه تعداد کارشناسان خبره کم بوده است، روایی مدل پژوهش تأیید گردید. سپس با استفاده از محاسبه میانگین واریانس استخراج شده روایی همگرای متغیرها مورد تأیید قرار گرفت (جدول شمارهٔ ۳).

جدول شماره ۳: محاسبات پایایی (آلفای کرونباخ، پایایی مرکب و میانگین واریانس استخراج‌شده)

متغیرهای اصلی	آلفای کرونباخ	پایایی مرکّب	عوامل مؤثر	AVE
قدرت هوشمند	۰,۹۳٤	۰,۹۵۰	کنترل، نوآوری، مشارکت، مدیریت زمان هوشمند، راهبرد	۰,۸۱۹
فضای سایبری	۰,۹٤٤	۰,۹۵۸	امنیت، جاسوسی، دفاع، خطرپذیری	۰,۷۹۱

همانگونه که در جدول شمارهٔ ۳ نشان داده ده است، ضریب همبستگی بین متغیر فضای سایبری و قدرت هوشمند ۰,٥٦٨ می‌باشد که این مقدار نشان دهنده رابطه مستقیم و مثبت میان دو متغیر است. از آنجایی که ضریب همبستگی محاسبه شده حالتی متقارن دارد، بدین ترتیب با تغییر جهت، تغییر در آن حاصل نمی‌گردد. برای اطمینان یک بار متغر هوشمند را به‌عنوان متغیر مستقل و فضای سایبری به‌عنوان متغیر وابسته در نظر گرفته شدند که تغییری در ضریب همبستگی ایجاد نگردید.



شکل شمارهٔ ۲: الگوی راهبردی هوشمند مداری در فضای سایبری

این عمل را می‌توان در رابطه با میزان (t) بارهای عاملی به دست آورد که مقدار بحرانی آن ۲,۷٦ می‌باشد و نشان می‌دهد بین این دو متغیر رابطه متقارن وجود دارد (شکل شمارهٔ ۳).

شکل شماره ۳: محاسبات ضریب همبستگی

مدل پژوهش

عواملی معرفی شده در مدل پژوهشی، برای اولین مرتبه می‌باشد که به‌عنوان عوامل قدرت هوشمند توسط نگارنده معرفی گردیده که با مطالعات کتاب‌ها، مقاله‌ها همایش‌ها و گزارش‌های امنیتی کشورهای گوناگون به دست آمده است. قدرت هوشمند از ٤ عامل راهبرد کنترل، مشارکت و نو آوری تشکیل شده که بر اساس میزان اطلاعات به دست آمده از روابط داخلی و بین‌المللی دولت‌ها و سازمان‌ها می‌توانند در فضای سایبری و محیط‌های وابسته (درونگرا و برونگرا) به فعالیت‌های از پیش تعیین شده و تعیین نشده خود بپردازند.

جدول شمارهٔ ٤: محاسبه مقادیر بارهای عاملی و t

عوامل پرسشنامه	بارهای عاملی	مقدار t	متغیرهای اصلی
دفاع	۰,۸۸۵	۲۲,٦۸۲	قدرت هوشمند
نوآوری	۰,۸۳٤	۱٤,۰,۸۳	
مشارکت	۰,۸۷۰	۱۸,۱۷۲	
مدیریت زمان هوشمند	۰,۹۳٤	٤۰,۲۲۸	

راهبرد	٠,٩٢١	٣٥,٤٣٣	
امنیت	٠,٨٦٤	٨٦,١٥٥	فضای سایبری
جاسوسی	٠,٨٦٤	٧٦,١٥٨	
دفاع	٠,٨٦٨	١٢,٨٨٤	
خطرپذیری	٠,٨٩٥	١١,٧٠	
فضای سایبری هوشمند	٤٢,٢٢١	٤٢,٢٢١	

نتیجه‌گیری

برای پاسخ به سؤالات پژوهش از آزمون فریدمن استفاده گردید. تمامی عوامل رتبه‌بندی شده گویای این مطلب هست که تمامی عوامل فضای سایبری شامل امنیت، دفاع و خطرپذیری، جاسوسی و فضای سایبری هوشمند در تمامی عوامل قدرت هوشمند تأثیرگذار می‌باشند. بدین معنی که بیشترین تأثیر را اوّل بر عامل کنترل، دوّم بر نوآوری، سوّم بر مدیریت زمان هوشمند و چهارم بر مشارکت و پنجم بر راهبرد دارد. با توجه به نتایج به‌دست‌آمده اولویت‌بندی عوامل فضای سایبری و قدرت هوشمند ارتباط معنی‌داری با یکدیگر دارند. در دنیای امروزی اهمیت تأثیرگذاری متقابل عوامل قدرت هوشمند و فضای سایبری بنا بر شرایط باید مورد بررسی و واکاوی قرار بگیرد تا بتوان بر اساس شرایط به دست آمده، روابط اقتضایی در دینای سایبری هوشمند را نمایان نمود (جدول‌های شمارهٔ ۵ و ٦).

جدول شماره ۵: محاسبات ضریب همبستگی

		امنیت	دفاع	خطرپذیری	جاسوسی	فضای سایبری هوشمند
	ضریب همبستگی	٠,٤٤٦	٠,٤٦٣	٠,٤٤٦	٠,٤	٠,٦١٣
راهبرد	سطح معنی‌داری	٠,٠١٤	٠,٠١	٠,٠١٤	٠,٠٢٩	٠
	ضریب همبستگی	٠,٣٥٤	٠,٣٥٦	٠,٣٥٤	٠,٢٨٩	٠,٥١٥
مشارکت	سطح معنی‌داری	٠,٠٤٥	٠,٠٤٣	٠,٠٤٥	٠,٠٢٢	٠,٠٠٤
	ضریب همبستگی	٠,٥١٢	٠,٥٨٢	٠,٥١٢	٠,٥٣٠	٠,٧٠٩
کنترل	سطح معنی‌داری	٠,٠٠٤	٠,٠٠١	٠,٠٠٤	٠,٠٠٣	٠
	ضریب همبستگی	٠,٣٢٧	٠,٣٦٥	٠,٣٢٧	٠,٤٦٣	٠,٤٩٩
نوآوری	سطح معنی‌داری	٠,٠٣٨	٠,٠٤٧	٠,٠٣٨	٠,٠١	٠,٠٠٥

	ضریب همبستگی	۰,۳۲۷	۰,۳٦٥	۰,۳۲۷	۰,۳۰۹	۰,٤۹۹
مدیریت زمان هوشمند	سطح معنی‌داری	۰,۰۲۸	۰,۰٤۷	۰,۰۲۸	۰,۰۰۷	۰,۰۰٥

جدول شمارهٔ ٦: محاسبات ضریب همبستگی (سطح معنی‌داری)

فضا / قدرت هوشمند	امنیت	رتبه	دفاع	رتبه	خطر پذیری	رتبه	جاسوسی	رتبه	فضای سایبری هوشمند	رتبه
کنترل	۳,۲٥	۱	۳,۳۰	۱	۳,۳	۱	۳,٤۳	۱	۳,٤	۱
نوآوری	۳,۱۷	۲	۳,۱۳	۲	۳,۰٥	۲	۳,۰۲	۲	۲,۹۸	۲
مدیریت زمان هوشمند	۳,۰۸	۳	۲,۹۷	۳	۲,۹۷	۳	۲,۹۳	۳	۳,۰۷	۳
مشارکت	۲,٦۷	٤	۲,۸۸	٤	۲,۸۸	٤	۲,۸٥	٤	۲,۸۲	٤
راهبرد	۲,۸۳	٥	۲,۹۷	٥	۲,۸۰	٥	۲,۷۷	٥	۲,۷۳	٥
χ^2	۱۸,۸۸۹		۸,۳٤۳		٦,۲۳٥		۸,۲٥٥		۹,۰۲۳	
درجه آزادی	٤		٤		٤		٤		٤	
سطح معنی‌داری	۰,۰۰۱		۰,۰۸		۰,۱۸۲		۰,۰۸۳		۰,۰٦۱	

عامل مشارکت قوی‌ترین ضریب همبستگی را با خطرپذیری و دفاع سایبری و ضعیف‌ترین همبستگی را با امنیت، عامل کنترل قوی‌ترین همبستگی را با جاسوسی و ضعیف‌ترین همبستگی را با امنیت، عامل نوآوری قوی‌ترین همبستگی را با امنیت و ضعیف‌ترین همبستگی را با فضای سایبری هوشمند، راهبرد قوی‌ترین همبستگی را با دفاع و ضعیف‌ترین همبستگی را با جاسوسی و مدیریت زمان هوشمند قوی‌ترین همبستگی را با امنیت و ضعیف‌ترین همبستگی را با عامل جاسوسی دارد (جدول شمارهٔ ۷).

جدول شماره ۷: روابط همبستگی

عامل قوی‌ترین همبستگی	ضعیف‌ترین همبستگی
مشارکت	خطرپذیری و دفاع
کنترل	جاسوسی
نوآوری	امنیت فضای سایبری هوشمند
راهبرد	دفاع جاسوسی
مدیریت زمان هوشمند	امنیت جاسوسی

عوامل فضای سایبری به‌صورت معنی‌دار در تمامی عوامل قدرت هوشمند اوّل بر عامل کنترل دوّم بر نوآوری، سوّم بر مدیریت زمان هوشمند، چهارم بر مشارکت و پنجم بر

راهبرد دارد. با توجه به نتایج به‌دست‌آمده از آزمون فریدمن اولویت‌بندی عوامل فضای سایبری و قدرت هوشمند ارتباط معنی‌داری با یکدیگر دارند. کنترل عاملی اصلی و قدرتمندی در میان عوامل قدرت هوشمند بوده و در ساختار امنیتی و بین‌المللی کشور و در مبادی ورودی و خروجی آن مانند فرودگاه بین‌المللی امام خمینی(ره) تصمیم‌گیری بر اساس عامل کنترل و توجه به این عامل درسی است گزاری‌های کلان کشوری می‌باشد. عوامل دیگری از قدرت هوشمند مانند نوآوری، مشارکت، راهبرد و مدیریت زمان هوشمند به‌عنوان عواملی از قدرت هوشمند در این پژوهش بیان‌شده‌اند که به‌وسیله این پژوهش معرفی و بیان شده‌اند.

پیشنهادها

با توجه به مطالب عنوان‌شده در طول پژوهش عوامل نوینی بر سر راه قدرت هوشمند قرار داده‌شده است که می‌تواند نقش بسزایی در هدف گزاری در ارتباطات بین‌المللی داشته باشد. تأثیرپذیری عوامل قدرت هوشمند و عوامل فضای سایبری روندی مثبت و مستقیم را طی می‌کند که این روند می‌تواند مهر تأییدی بر عوامل شناسایی‌شده قدرت هوشمند در فضای سایبری به‌صورت ترکیبی (همگرایی جمعی) بوده و همچنین عامل کنترل، مهم‌ترین عامل در میان عوامل تأثیرگذار قدرت هوشمند بر فضای سایبری هست. با توجه به خروجی‌های پرسشنامه، دو عامل به‌عنوان عواملی نوین در عرصه مدیریت قدرت هوشمند و فضای سایبری معرفی گشته و در مدل نهایی تحقیق آورده شدند. هدف اصلی در این پژوهش شناسایی، ترکیب و به‌کارگیری عوامل ازنظر سیاست گزاری‌های نوین می‌باشد. در پژوهش انجام شده، پژوهشگر تا آنجا که توانسته است تمامی جنبه‌های متغیرهای فضای سایبری و قدرت هوشمند را مورد بررسی و تجزیه و تحلیل قرار داده است؛ امّا به دلیل جدید بودن و ترکیبی بودن موضوع، دریچه‌های متعدّدی از سؤال‌های متفاوت به ذهن خطور می‌نماید. به همین دلیل می‌توان پژوهش‌های جدید و نوآورانه‌ای را پیاده‌سازی نمود. پژوهشگران می‌توانند با استفاده از عامل‌های شناخته‌شده در پرسشنامه‌های تکمیل‌شده توسط کارشناسان خبره عامل‌های ناشناخته را مورد پژوهش قرار دهند. این پژوهش در بعد

بین‌المللی و در حوزه فرودگاهی «فرودگـاه امـام خمینـی(ره)» صـورت پذیرفتـه اسـت کـه می‌توان با حمایت‌های انجام شده در تمامی ابعاد بین‌المللی که مربوط به‌تمـامی کشـورها می‌باشد، پیاده‌سازی نمود. نتایج به‌دست‌آمده می‌تواند مانند مرجعی برای تمامی کشـورها عمل نماید و قابل‌تعمیم برای تمامی جنبه‌های سایبریسم و هوشمند مداری باشد.

فهرست منابع و مآخذ

- Cyber resilience , The cyber risk challenge and the role of insurance. (2014). CRC FORUM.
- Richard L. Armitage, J. S. (2007). CSIS COMMISSION ON SMART POWER. CSIS.
- Abbott, M. (2014). Log Analysis of Cyber Security Training Exercises. Elsevier, 5-7.
- Alleyne, M. D. (2012). International Communication And World Affairs. Journalism And Mass Communication, 2.
- Benkler. (2016). Degrees of Freedom, Dimensions of Power. MIT Press Journals, 19-20.
- Clarke, R. A.Securing Cyberspace Through International Norms. (2011).
- Cliff Joslyn, S. C. (2013). Massive Scale Cyber Traffic Analysis: A Driver for Graph Database.ACM. 1.
- D. Henshela, M. G. (2015). Trust as a human factor in holistic cyber security risk. 1118.
- D. Henshela, M. G. (2015). Trust as a human factor in holistic cyber security risk assessment. ScienceDirect, 1118.
- Danielson, M. E. ((2009)). Economic Espionage: A Framework for a Workable Solution. Minnesota Journal of Law, Science & Technology, 504-507.
- David A. Lane a, S. v. (2011). (2011). Innovation, sustainability and ICT. ELSEVIER, 83-86.
- Dealing With Today’s Asymmetric Threat to U.S, Global Security. Employing Smart Power. ((2009)).
- Dutton, J. M. (2016). The New Cybersecurity Agenda:Economic and Social Challenges to a Secure Internet. Michigan State University.
- Eadie, P. (2016). Counter-terrorism, Smart Power and the United States. GlobalPolicy, 328.
- Eadie, P. (2016). Counter-terrorism, Smart Power and the United States. 323-324.

- Eadie, P. (2016). Counter-terrorism, Smart Power and the United States. Global Policy, 324.
- Elena Ramona STROIE, A. C. (2011). Security Risk Management - Approaches and Methodology.. Informatica Economică,, 229-230.
- Ernest J. Wilson, I. (2008). Hard Power, Soft Power, Smart Power. The ANNALS of the American Academy of Political and Social Science. 111-122.
- european commission. Cybersecurity. (2016).
- Feng. (2016). China's Security Strategy towards East Asia.. The Chinese Journal of International Politics(OXFORD), 7.
- Fischer, E. A. (2014). Cybersecurity Issues and Challenges: In Brief. 1.
- Fischer, E. A. (2016). Cybersecurity Issues and Challenges. 12.
- Fry, R. (2014).. (2014). Smart Power and the Strategic Deficit. The RUSI Journal, 31.
- Gallarotti, G. M. (2011). Soft power: what it is, why it's important, and the conditions for its effective use. Journal of Political Power, 25-30.
- Gallarotti, G. M. (2011). Soft power: what it is, why it's important, and the conditions for its effective use. Journal of Political Power, 25-28.
- Gallarotti,G. M. (2014).Smart Power:Definitions,Importance,and Effectiveness Social Sciences, 4-8.
- George. (2016). Soft power: Media influence and its limits. 1.
- HARE, F. (2015). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?.. George Mason University, 2.
- Haugaard, M. (2012). reflections upon power over, power to,power with, and the four dimensions of power. Journal of Political Power. 353.
- Henga, Y.-K. (2015). Smart Power and Japan's Self-Defense Forces. 284.
- ITU. (2010). Understanding cybercrime: Phenomena, challenges and legal response.
- J.Wilson, E. (. (2008). Hard Power, Soft Power, Smart Power. The ANNAL Of American Academy of Politicalad Social Sciece, 114.
- James A. Lewis, K. T. (2011). (2011). Cybersecurity and Cyberwarfare.. CSIS, 3.
- Jason Creasey, I. G. (2013). Cyber Security Incident Response Guide. 4.
- Joseph S. Nye, J. (2008). Public Diplomacy and Soft Power. SAGE, 94-102.
- Kabay, M. E. (2008). Industrial Espionage. Network World Fusion Security. 3.
- KAGAN, R. (n.d.). OF PARADISE, AND P OWER. Vintage. 2003,2004.
- Kashiam, M. A. (2012). The Italian role in the Libyan spring revolution: is it a shift from soft to hard power? Routledge Taylor AndFrancis Group.

- Keir Giles, K. H. (2015). Cyber Defense:An International View. The United States.
- Kuromiya, H. (2009). STALIN’S GREAT TERROR AND ESPIONAGE. The National Council for Eurasian and East European Research. 3.
- Lampros Litosb, c (2017). Management tool design for eco-efficiency improvements in manufacturing.ScienceDirect, 505.
- Lee Gillam, A. V. (2012). Investigating Cyber Law and Cyber Ethics: Issues, Impacts, and Practices.. Information Science Reference, 79.
- Lee, G. (2009). A theory of soft power and Korea's soft power Strategy. Korean Journal of Defense Analysis, 211.
- Lee,G.A theory of soft power and Korea's soft power Strategy.Korean Journal of Defense Analysis. (2009) 211.
- LIBICKI, M. C. (2009). Cyber Deterence And Cyberwar. 12-13.
- Lindsley Boiney, J. C. (2015). Cyber Operations Rapid Assessment (CORA). 4-8.
- LuisOrtega, J. (2016). Reference Management Tools. Elsevier Ltd, 65.
- Maqbool. (2018). Efficiency and effectiveness of factors affecting renewable energy projects; an empirical perspective. 6-13.
- Marco Angelini. Maria Cristina Arcuri, R. B. (2013). Italian Cyber Security Report.
- Margarita Kefalaki, Y. P. (2012). Challenges in International Communication. Athens Institute for Education and Research, 1.
- Martin, A. (2012). Political participation among the young in Australia. Routledge.
- Martin, A. (2012). Political participation among the young in Australia Routledge.
- Mason Ricea, J. B. (2011). A signaling framework to deter aggression in cyberspace. ELSEVIER, 58.
- Mason Ricea, J. B. (2011). A signaling framework to deter aggression in cyberspace.. ELSEVIER, 58.
- MATTHEW S. COHEN, C. D. (2015). Israel and Cyberspace: Unique Threat and Response.. International Studies Perspectives Advance Access.
- Mayfield, M. (2011). Innovation. Elsevier, 1.
- Mkhoyan. (2016). Soft power, Russia and the former Soviet states: a case study of Russian language and education in Armenia. International Journal of Cultural Policy, 1.
- Moore, T. (2010). Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy.
- Navráti, D. (2014). National Cyber Security Strategy OF THE CZECH REPUBLIC. 20.

- Noluxolo Gcaza, R. v. (2017). Information & Computer Security.. EMERALD INSIGHT, 4.
- Nor'azuwa Muhamad Pahri, N. A. (2010). 3rd Party Information Security Assessment Guideline.CyberSecurity Malaysia, 12
- Nye, J. S. (2006). Soft Power, Hard Power and Leadership. 3-4.
- Nye, J. S. (2011). Power and foreign policy. Journal of Political Power, 20.
- Nye, J. S. (2012). China and soft power. Journal of International, 151-152.
- Nye, J. S. (2015). China and soft power. Routledge, 151.
- Patterson, W. R. (2008). Smart power in reunified Germany. pp.340-49. Journal of Power, 340-49.
- Peterson. (2008). Smart power in reunified Germany. Journal of Power, 350.
- Petress, K. (2016). Power: Definition, Typology, Description, Examples, and Implications. 1-3.
- Purdy, A. (2016). The Global Cyber Security Challenge. Huawei Technologies, 7.
- Radu. (2013). Negotiating meanings for security in the cyberspace. 32-34.
- Radu. (2013). Negotiating meanings for security in the cyberspace. Emerald Insight, 32-34.
- Radu. (2013). Negotiating meanings for security in the cyberspace. Emerald Insight, 32-34.
- Radu. (2013). Negotiating meanings for security in the cyberspace. Emerald Insight, 32-34.
- Ramsaroop, P. (2003). Cybercrime, Cyberterrorism, and Cyberwarfare. Technology and Health Services Delivery Health Services Organization Unit (THS/OS). 14.
- Randall J. Murphy, M. S. (2015). Guidebook on Best Practices for Airport Cybersecurity. 7.
- Resnick. (391). I Will Follow: Smart Power and the Management of Wartime Alliances.. Journal of Strategic Studies, 215.
- Richard L. Armitage, D. J. (2008). IMPLEMENTING SMART POWER: SETTING AN Agenda For National Security Reform. CSIS, 3.
- Robert G. Abbott, J. M. (2015).. (). Log Analysis of Cyber Security Training Exercises.ScienceDirect, 5089.
- Robert V. Kozinets, A. H. (2008). The Wisdom of Consumer Crowds: Collective Innovation in the Age of Networked Marketing. Journal of Macromarketing, 340.
- Rubenstein, D. (2014). Nation State Cyber Espionage and its Impacts. CSE, 2.
- Saroyan, D. (2015). SMART POWER. PUBLIC DIPLOMACY MAGAZINE,, 14-19.

- Sherr, J. (2011). Hard power in the Black Sea region: a dreaded but crippled instrument.. 11.
- SKINNER, C. P. An International Law Response to Economic Cyber Espionage.. (2014).
- Stall, S. T. (2011). The Future Of Cyber Security. 7.
- Stephen J. Mariano, C. B. (2009). US Army Africa: Smart Power in Action. Small Wars Journal, 2.
- Stevens. (2015). Cyber security, community, time. cyber security and the politic. 20-41.
- Stevens. (2015). Cyber security, community, time. Cyber Security and the Politics of Time. 21-40.
- Strategy, A. t. (2009). Lee, G.. Korean Journal of Defense Analysis, 1.
- Stratton, J. (2009). International law. 2-7.
- Susana Borrás, C. E. (2013). The choice of innovation policy instruments. 1.
- Tana, S. S. (2015). Mailed Fists and Velvet Gloves: The Relevance of Smart Power to Singapore's Evolving Defence and Foreign Policy. Journal Strategic Studies, 332-333.
- Understanding cybercrime: Phenomena, challenges and legal response.. (2010). ITU.
- Wamala, F. (2011). The ITU National Cybersecurity Strategy.
- Wamala, F. (2011). (2011). The ITU National Cybersecurity Strategy Guide. ITU.
- Wamala, F. (2011). The ITU National Cybersecurity Strtategy Guide. ITU.
- YONG-SOO EUN, J. S. (2014). Cyberwar: Taking Stock of Security and Warfare in the Digital Age. International Studies Perspectives, 4.