Archive of SID

فصلنامهٔ علمی راهبرد دفاعی، سال هجدهم، شمارهٔ ٦٩، بهار ١٣٩٩

فرمانده معظم کل قوا: «سعی کنیم عناصر قدرت را در داخل جمهوری اسلامی افزایش بدهیم. ... باید روزبه‌روز این قدرت دفاعی افزایش پیدا کند، و البتّه میکند؛ به کوری چشمشان، روزبه‌روز هم افزایش پیدا خواهد کرد» (١٣٩٦/٠٧/٢٦)

مقالهٔ پژوهشی: معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران

بهزاد ربیعی[1]، شهرام علی یاری[2] و محمد مردانی شهربابک[3]

تاریخ دریافت: ٩٨/٠٨/٠٥ تاریخ پذیرش: ٩٨/١١/٠٥

چکیده

مروزه قدرت سایبری دفاعی برای یک سازمان نظامی در کشور اهمیت ویژه‌ای دارد. با توجه به اینکه چهار حوزهٔ زمین، دریا، هوا و فضا از فضای سایبری برای انجام بهتر و کاراتر عملیات‌های خود بهره می‌برند؛ یک الگوی ارزیابی قدرت سایبری برای سازمان دفاعی می‌تواند بینش صحیحی از متغیرهای اثرگذار بر قدرت سایبری دفاعی را در اختیار مدیران و تصمیم‌گیران این حوزه قرار دهد. هدف از این مقاله، شناسایی و الگوسازی مؤلفه‌های ارزیابی قدرت سایبری، برای یک سازمان دفاعی است که درنهایت ٥ مؤلفه، ٢٦ شاخص و ٧٨ سنجه برای اندازه‌گیری معرفی گردیده است. الگوی معرفی شده با مطالعهٔ الگوهای ارزیابی سایبری و برنامه‌های راهبردی ملی سایبری، مؤلفه‌های قدرت سایبری دفاعی استخراج گردیده، و با استفاده از روش الگوسازی معادلات ساختاری با رویکرد کمترین مربعات جزئی با سنجه‌های تکوینی، کشف و تعیین اعتبار شده است. فن (تکتیک) نامبرده شده از داده‌های تجربی (قضاوت خبرگان) برای الگوسازی استفاده می‌نماید. روش تحلیل در این نوع الگوسازی تحلیل آماری است که ارتباط و اهمیت مؤلفه‌های الگو را با استفاده از آزمون‌های مختلف و دقیق آماری موردسنجش قرار می‌دهد. نتایج سطوح معناداری سنجه‌های (سؤال‌های تحقیق) هر سازهٔ اصلی (ابعاد) و فرعی (مؤلفه‌ها) به میزان حداقل ٩٠٪ تا حداکثر بیش از ٩٩٪ (نزدیک به ١) را نشان می‌دهد. این مقادیر برای معناداری اتصال سازه‌های اصلی به یکدیگر و اتصال سازه‌های فرعی به اصلی نیز برقرار می‌باشد. همچنین مقادیر R^2 برای سازه‌های اصلی نشان‌دهنده تبیین واریانس توسط متغیرهای پیش‌بین و حد مطلوب کسب شده برای آنها می‌باشد. بنابراین اعتبار متغیرهای انتخاب شده و الگوی ترسیم شده برای آنها (روابط و چگونگی اثرگذاری متغیرها) تأیید گردیده است.

واژگان کلیدی: قدرت سایبری، سازمان دفاعی، الگوسازی معادلات ساختاری، ارزیابی قدرت سایبری دفاعی.

١. دانش آموختهٔ کارشناسی ارشد مهندسی صنایع- مدلسازی سیستم‌های کلان در دانشگاه جامع امام حسین(ع)، تهران، ایران (نویسندهٔ مسئول)- behzaderabbiee@gmail.com

٢. دانشیار دانشکدهٔ مهندسی صنایع دانشگاه جامع امام حسین(ع)، تهران، ایران- shaliyari@ihu.ac.ir

٣. دانشیار دانشکدهٔ مهندسی صنایع دانشگاه جامع امام حسین(ع)، تهران، ایران- mardani@ihu.ac.ir

www.SID.ir

Archive of SID

مقدمه

وابستگی و اتصال عناصر کشورها از طیف خانواده‌ها، سازمان‌های خصوصی و دولتی، به‌ویژه زیرساخت‌های حیاتی به اینترنت، و تنوع بازیگران مخرب امکان آسیب‌پذیری را در برابر فعالیت‌های مخرب سایبری ایجاد می‌نماید. (Hathway, et.al, 2015:8) کیفیت حضور یک کشور در صحنهٔ بین‌المللی با بحث «قدرت ملی» آمیخته شده و دارای ابعاد گوناگونی شامل زمین، دریا، هوا و فضاست. در سال‌های اخیر قدرت سایبری به‌عنوان بعد پنجم قدرت ملی معرفی شده است. «ارگانسکی» قدرت را به‌عنوان «توانایی کشورها در اثرگذاری بر رفتار دیگر کشورها... .»، و «نای» قدرت را به‌عنوان «قابلیت و توانایی یک نهاد در اثرگذاری بر دیگر نهادها برای به‌دست آوردن نتیجهٔ موردنظر و حتی وادار ساختن یک نهاد بر انجام کاری...» تشریح می‌کنند.(Rowland, et.al, 2014:2) اما به عقیدهٔ برخی صاحب‌نظران تنها شکل مهم قدرت تا سال ۲۰۲۰ «قدرت نظامی» خواهد بود.(Treverton, et.al, 2005:26) یک کشور را می‌توان به‌عنوان یک «سیستم سیستم‌ها[1]» درنظر گرفت که نهادهای آن نقش «سیستم‌های» جزء (کوچکتر) را دارند.(Walden, et.al, 2015:127-145) قدرت یک ملت از برآیند سازمان‌ها یا نهادهای آن کشور پدید می‌آید که نهادهای نظامی مؤثرترین آنها در قدرت ملی به‌شمار می‌روند.(Rowland, et.al, 2014:5-7) در نتیجه انتخاب مؤلفه‌های قدرت سایبری یک سازمان دفاعی می‌تواند از مؤلفه‌های قدرت سایبری ملی مطابق با هدف‌ها و مأموریت‌های تعریف شده برای آنها صورت پذیرد. برنامه‌های راهبردی سایبری ملی نیز می‌تواند منبع قابل توجه دیگری برای استخراج مؤلفه‌های قدرت سایبری باشد.(Cate, 2015:33) انتخاب یک راهبرد می‌تواند به ایجاد یک مؤلفه قدرت منجر شود.(Freedman 2015:184-203)

1. System of systems (SOS)

www.SID.ir

Archive of SID

۱. کلیات

۱-۱. بیان مسئله

امروزه منافع فضای مجازی، اداره و توسعهٔ حوزه‌های سایبری ملی و به‌ویژه حوزهٔ نظامی جزو موضوع‌های دارای اهمیت بالا در دنیا به‌شمار می‌رود.(زرقانی، ۸۹:۱۳۸۷)؛ (Hunker, 2010:63-70)؛(Klimburg et. al, 2012:13-16) عدم وجود الگوهای ارزیابی به‌منظور اندازه‌گیری قدرت سایبری باعث عدم آگاهی از میزان قابلیت‌های دفاعی در حوزهٔ سایبر گردیده است. اگر نتوانیم چیزی را ارزیابی و اندازه‌گیری کنیم، قادر به مدیریت آن نخواهیم بود.(Drucker, 2006:34) عدم ارزیابی، درنهایت منجر به مدیریت ناکارآمد حوزهٔ دفاع سایبری می‌گردد؛ این موضوع به‌ویژه در نهادهای نظامی می‌تواند خطرهای جدی را متوجه کشور نماید. درواقع مسئلهٔ اصلی تحقیق آن است که چگونه و براساس چه ابعاد، مؤلفه‌ها و سنجه‌هایی می‌توان قدرت سایبری یک سازمان دفاعی را اندازه‌گیری نمود.

۱-۲. اهمیت و ضرورت تحقیق

امروزه با توجه به کاربرد گستردهٔ فضای دیجیتال در عملیات‌ها و انجام برنامه‌های سازمان‌های دفاعی، تهدیدهای سایبری به یکی از چالش‌های اولویت‌دار تبدیل شده است؛ و قدرت نظامی (دفاعی) در حیطهٔ فضای سایبری از اهمیت ویژه‌ای برخوردار می‌باشد.(Gehem, et.al, 2015:117-122) «نایجل اینکستر»[1] لازمهٔ مدیریت بر فضای سایبر را توانمندی در اندازه‌گیری آن و به‌دست آوردن معیارهایی برای ارزیابی می‌داند. (Inkster, 2017:27-34) بالابردن قابلیت‌های دفاعی در حوزهٔ سایبر نیازمند درک صحیح از متغیرهای اثرگذار قدرت سایبری برای برنامه‌ریزی و تصمیم‌گیری در شرایط مناسب است.(شهلائی، ۱۳۹۵:۳-۱) یک الگوی ارزیابی کارآمد ابزار مناسبی برای پایش نقاط ضعف و قوت یک سازمان دفاعی و ارائهٔ آگاهی به سیاست‌گذاران و برنامه‌ریزان از وضع موجود

1. Nigel Inkster

www.SID.ir

Archive of SID

است.(Gehem, et.al, 2015:117-122) بنابراین دستیابی به الگوی ارزیابی قدرت سایبری یک سازمان دفاعی دارای اهمیت بوده و ضروری می‌باشد.

۱-۳. پیشینهٔ تحقیق

(۱) «رابرت ببر»[1] قدرت سایبری را تشکیل یافته از یک ساختار بومی و متغیرهای نظام‌مند در محیط راهبردی عملیات، شامل ابزارهای راهبردی، عملیاتی، راهکنشی (تاکتیکی) و فنی(تکنیکی) می‌داند.(Bebber, 2017:426-436)

(۲) «استوارت استار»[2] در نظریهٔ سه سطحی قدرت سایبری، الگوی هرمی قدرت سایبری را دارای سه سطح: توانمندسازی، سطوح قدرت و زیرساخت سایبری معرفی نموده و خطر و فرصت سازمان‌ها را نیز در سه سطح: راهبردی، عملیاتی و راهکنشی قرار می‌دهد.(Starr, 2013:38-49)

(۳) «مؤسسهٔ بوزآلن همیلتون»[3] در یک تحقیق گسترده متغیرهای قدرت سایبری را در سطح ملی شامل ٤ مؤلفه اصلی چارچوب قانونی و حقوقی، بافت اقتصادی و اجتماعی، زیرساخت فناورانه و کاربری صنعت، ۱۹ مؤلفه فرعی و۳۰ مؤلفه برای ابعاد سنجه‌ها معرفی نموده و ۱۹ کشور را مورد ارزیابی قرار داده است. این نهاد همچنین در یک کار تحقیقاتی دیگر «مسیر دستیابی به قدرت سایبری» را یک پیکرهٔ واحد معرفی نموده که از ایجاد توانمندی در سه حوزهٔ کلان دولت، کسب و کار و جامعه مدنی به‌وجود آمده و بر عناصر بنیادینی چون نوآوری، تحقیق، توسعه، آموزش و تمرین و قانون و سیاست متکی است.(Booz Allen Hamilton, 2011:2-11)

(٤) «نیل رابینسون[4] و دیگران» در تحقیقی که برای اتحادیه اروپا انجام داده‌اند، قابلیت‌های نظامی سایبری را توانمندی و قدرت در رهنامه، سازمان، آموزش، پشتیبانی و

1. Robert “Jake” Bebber
2. Stuart H. Starr
3. Booz Allen Hamilton Inc
4. Neil Robinson

www.SID.ir

Archive of SID

تدارکات، نیروهای انسانی توانمند، رهبری، تسهیلات و قابلیت‌های همکاری معرفی نموده‌اند.(Robinson, et.al, 2013:13-20)

(٥) «یله ون هاستر»[1] چارچوب تحلیلی قدرت سایبری را با تعیین قابلیت و ظرفیت‌های سایبری در بافت ٤ ابزار معروف قدرت شامل سیاسی، اقتصادی، اطلاعاتی و نظامی ترسیم و معرفی می‌کند.(Haaster, 2016:7-2)

(٦) «جیل رولند»[2] ویژگی‌های قدرت سایبری در یک نهاد سایبری را قابلیت تداوم (شامل عقیده (ایدئولوژی)، بدنهٔ سیاسی، و زیرساخت و ساختار) و دارای ابعاد قدرت (شامل دیپلماتیک، اطلاعاتی، اقتصادی و نظامی)، مقاوم و مصر، انعطاف‌پذیر و تاب‌آور، و با وابستگی‌های متقابل دانسته است.(Rowland, et.al, 2014:5-11)

(٧) «لیور تابانسکی»[3] مؤلفه‌هایی چون راهبرد کلان ملی، راهبرد نظامی، راهکنش‌ها (تاکتیک‌ها) و عملیات راهبردی، سطح دانشگاه‌ها، تحقیق و توسعه و نوآوری در کسب‌وکار، صادرات صنایع امنیت سایبری، سیاست‌های سایبری ملی رسمی و تجربه و نوآوری دفاعی را معرفی می‌کند.(Tabansky, 2016:51-63)

(٨) «خداداد هلیلی و همکاران» ویژگی‌ها و ابعاد قدرت سایبری را شامل: ویژگی‌های اساسی، ویژگی‌های کارکردی، ویژگی‌های مورد انتظار ، پیامدها و دستاوردهای موردانتظار معرفی نموده‌اند.(هلیلی و همکاران، ١٣٩٧:١٩)

(٩) «جمشید نصرت‌آبادی و همکاران» ٣ بعد شامل: آفند، پدافند و تاب‌آوری، و ١١ مؤلفه و ٥٥ شاخص را ارائه می‌دهند.(نصرت‌آبادی و همکاران، ١٣٩٧:١٩٢)

(١٠) «رضا تقی‌پور و علی اسماعیلی» الگوی دفاع سایبری را با ٣ بعد: بازدارندگی، پدافند و برگشت‌پذیری، و ١٠ مؤلفه و ٣٢ شاخص معرفی می‌نمایند.(تقی‌پور و اسماعیلی، ١٣٩٧:١٩٣) همان‌گونه که بررسی شد، تحقیقی درخصوص ارزیابی قدرت سایبری دفاعی در کشور انجام نشده است.

1. Jelle van Haaster
2. Jill Rowland
3. Livor Tabansky

www.SID.ir

Archive of SID

۱-٤. سؤال‌های تحقیق

۱-٤-۱. سؤال اصلی

الگوی مناسب برای ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران چیست؟

۱-٤-۲. سؤال‌های فرعی

(۱) مؤلفه‌ها، شاخص‌ها و سنجه‌های اندازه‌گیری قدرت سایبری دفاعی در ج.ا.ایران چه هستند؟

(۲) الگوی مسیری (چگونگی اثرگذاری و ارتباط) مؤلفه‌ها، شاخص‌ها و سنجه‌های اندازه‌گیری قدرت سایبری یک سازمان دفاعی در ج.ا.ایران به چه صورت است؟

۱-۵. هدف‌های تحقیق

۱-۵-۱. هدف اصلی

معرفی الگویی برای ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا.ایران.

۱-۵-۲. هدف‌های فرعی

(۱) شناخت و انتخاب مؤلفه‌ها، شاخص‌ها و سنجه‌های اندازه‌گیری قدرت سایبری یک سازمان دفاعی در ج.ا.ایران؛

(۲) ترسیم الگوسازی مسیری (چگونگی اثرگذاری و ارتباط) مؤلفه‌ها، شاخص‌ها و سنجه‌های اندازه‌گیری قدرت سایبری یک سازمان دفاعی در ج.ا.ایران.

۱-٦. روش تحقیق

با توجه به کاربرد روش‌های چندمتغیره سطح بالا، در این تحقیق از الگوسازی معادلات ساختاری استفاده شده است.(Hair, et.al, 2017:2-4) روش نمونه‌برداری نیز خوشه‌ای انتخاب گردید. به‌منظور گردآوری داده‌های تحقیق پرسشنامه‌ای تهیه گردید که شامل ۵ مؤلفه اصلی تحقیق و ۲٦ مؤلفه فرعی و در مجموع این ۳۱ مؤلفه، هریک دارای سه معرف (سنجه) است. پرسشنامه‌ها بین ۵ مرکز پژوهشی نظامی مرتبط با موضوع‌ها و چالش‌های

www.SID.ir

Archive of SID

فضای سایبری توزیع گردید. در مجموع ۵۹ پرسشنامه توزیع گردید کـه تمـامی آنهـا قابـل استفاده است.

جدول شمارهٔ (۱): ویژگی‌های نمونه آماری تحقیق

سطح تحصیلات					
کارشناس	٪۷	کارشناسی ارشد	٪۳۷	دکترا	٪۵٦
سن پاسخ‌دهندگان					
کمتر از ۳۵ سال	٪٤۳	۳٦ – ٤۰ سال	٪۲٦	٤۰ سال به بالا	٪۳۱
تجربهٔ کاری					
کمتر از ۵ سال	٪٤۲	۵–۱۰ سال	٪۱۹	بیش از ۱۰ سال	٪۳۹

۱-٦-۱. آزمون‌های ارزیابی الگوی اندازه‌گیری و الگوی ساختاری

باتوجه به الگوی اندازه‌گیری و الگوی ساختاری ۷ آزمون باید انجام گیـرد. (Hair, et.al, 2017:118-203) این آزمون‌ها در الگوی اندازه‌گیری عبارتند از:

(۱) روایی قانونی معرف‌ها.(Diamantopoulos,et.al, 2001:270,Burke,et.al, 2003: 214)

(۲) ارزیابی روایی همگرا.(Chin, 1998: 306, Hair, et.al, 2017:121)

(۳) ارزیابی همخطی معرف‌ها.(Hair, et.al, 2017:123, Garson, 2016:15)

(٤) ارزیابی معناداری و تناسب معرف‌هـای ترکیبـی یـا معنـاداری وزن‌هـا. (Hair, et.al, 2017:126, Garson, 2016:17)

و آزمون‌های الگوی ساختاری عبارتند از:

(۱) ارزیابی الگوی سـاختاری بـرای روابـط همخطـی. (Hair, et.al, 2017:168, Garson, 2016:21)

(۲) ارزیابی معناداری و تناسب روابط الگوی ساختاری. (Hair, et.al, 2017:170, Garson, 2016:29)

(۳) ارزیابی سطح ضرایب تعیین R^2.(Hair, et.al, 2011:174, Henseler, et.al, 2010:93)

www.SID.ir

Archive of SID

۲. ادبیات و مبانی نظری تحقیق

۲-۱. مفاهیم

۲-۱-۱. سایبر

کلمه «سایبر»[1] برای ارجاع به علم سایبرنتیک[2] انتخاب و استفاده شده است. اصطلاح «سایبرنتیک» نخستین بار در سال ۱۹٤۸ توسط «نوربرت وینر»[3] در کتاب «کنترل و ارتباط در حیوان و ماشین» تعریف شد. ریشهٔ این کلمه، فعل یونانی «Kubernao» است؛ که به‌معنی راندن، رهبری و هدایت کردن می‌باشد.(Kramer&et. al, 2009:21) انجمن علوم دفاعی آمریکا واژهٔ «سایبر» را برای اتوماسیون دیجیتالی که توسط صنایع پایهٔ وابسته به آن مورد استفاده قرار می‌گیرد، به‌کار می‌برد؛ که شامل سامانه‌های سلاح و برنامه‌های اساسی آنها، سامانه‌های فرمان، ارتباطات و واپایش، جاسوسی، نظارت و شناسایی، تدارکات و نظام‌های منابع انسانی، تلفن همراه و ارتباط‌دهندگان متحرک و همچنین نظام‌های زیرساختی ثابت است.(Kramer&et. al, 2009:22)

۲-۱-۲. قدرت سایبری

«کوهل» قدرت سایبری را به‌عنوان «قابلیت یا توانایی استفاده از فضای مجازی برای ایجاد مزیت‌ها و تأثیر بر رویدادها در سراسر محیط عملیاتی (زمین، دریا، هوا، فضا و فضای سایبری) و در تمام ابزارهای قدرت» (دیپلماسی، اطلاعات، ارتش و اقتصاد) عنوان می‌کند.(Kuehl, 2009:29) «شلدون» تاکید می‌کند که فضای سایبری می‌تواند بر تمام حوزه‌ها «به‌طور کامل و همزمان» اثر گذارد.(Sheldon, 2012:211) «نای» بیان می‌دارد: «قدرت سایبری وابسته به منابعی است که ویژگی‌های حوزهٔ فضای سایبری را تعیین می‌نماید». او قدرت را توانایی دستیابی به نتایج موردانتظار از راه ابزارها و امکانات در فضای سایبری و دیگر حوزه‌ها معرفی می‌کند.(Nye, 2011:8)

1. cyber
2. cybernetics
3. Norbert Wiener

www.SID.ir

Archive of SID

۲-۱-۳. روش‌های ارزیابی قدرت ملی

اندازه‌گیری قدرت ملی شامل دو روش تک‌متغیره و چندمتغیره است. در رویکرد تک‌متغیره قلمرو، جمعیت، تولید ناخالص داخلی، کارکنان نیروهای مسلح، هزینه‌های نظامی و مصرف منابع و انرژی به عنوان واضح‌ترین و قابل دسترس ترین برای نشان دادن قدرت در نظر گرفته شده‌است (Hohn, 2014: 68-99, Hafeznia, et. al, 2008:235)، شاخص‌های تک‌متغیره دارای سادگی هستند، با این حال به یک جنبهٔ ویژه از قدرت ملی محدود می‌شوند و به‌طور معمول نمی‌توانند جنبه‌های مختلف یک کشور را بیان نمایند.(Kadera&Sorokin, 2004:213)؛ بنابراین بهتر است، برای پوشش تمام حوزه‌ها و ابعاد قدرت از شاخص‌های متنوع و مناسبی در هر حوزه استفاده شود.(Liao, et. al, 2015:1674)

۲-۱-٤. ارزیابی قدرت سایبری

با توجه به مطالب بیان شده می‌توان اذعان نمود قدرت سایبری بخشی از قدرت ملی است. ارزیابی قدرت سایبری از روش‌های ارزیابی قدرت ملی تبعیت می‌نماید، بنابراین می‌تواند شامل تک‌متغیره و چندمتغیره باشد. در ارزیابی قدرت سایبری با استفاده از یک الگوی چندمتغیره شکاف بین وضع موجود و وضع مطلوب مشخص شده و منجر به راهکارهایی برای بهبود وضع موجود خواهد شد.

۲-۱-۵. ویژگی‌ها، هدف‌ها و مأموریت‌های سازمان دفاعی (سایبری)

سازمان نهادی مستقل است که مأموریت ویژه دارد؛ و می‌تواند با نیت انتفاعی یا غیرانتفاعی تأسیس شده باشد. مأموریت یک سازمان دفاعی حفظ امنیت و دارایی‌های ملی و حکومتی در برابر تهدیدهاست. سازمان‌های دفاعی به بخش‌هایی گفته می‌شود که به تولید کالا و خدمات و فناوری برای مصرف نهایی در نیروهای مسلح دولتی در زمان صلح یا نیازهای درحال افزایش زمان جنگ یا موقعیت اضطراری بپردازد و به‌طورمشخص یک سازمان غیردفاعی چنین وظیفه‌ای ندارد، و می‌تواند هر محصولی غیر از نظامی یا دفاعی داشته باشد.(احمدی و همکاران، ۱۳۹٦:۳) سازمان نظامی دارای یک نظام سلسله‌مراتبی است که تلاش می‌کند با استفاده از سازماندهی تشکیلات داخلی، کسب منابع مورد نیاز و مدیریت

www.SID.ir

Archive of SID

عوامل خارجی اثرگذار بر سازمان، در دو زمینهٔ اصلی کارکردی «نظامی و علمی» در به‌دست آوردن هدف‌ها و مأموریت‌ها و خروجی‌های نظام‌مند خود اثربخشی لازم را داشته باشد.(ساعی و اکبرزاده، ۱۳۸۹:۳۵-۳٤) یک سازمان دفاعی یا نظامی دارای مأموریت‌های گسترده‌ای در بخش‌های مختلف عملیاتی و رزمی، فرماندهی و کنترل، فناوری، ساخت و نگهداری تجهیزات، ادوات نظامی و پشتیبانی و خدمات اداری و مالی است.(دهقانی پوده و پاشایی هولاسو، ۱۳۹٦:۲۱) سازمان دفاعی دارای مدیریت و نگرش نظام‌مند بر ادارهٔ امور، برنامه‌ریزی، بهینه‌سازی و نظارت بر وظایف است. ملزم به در اختیار داشتن ابزار و تجهیزات و فناوری‌های نوین و تلاش برای تحقیق، توسعه و نوآوری در تمامی ابعاد مأموریتی خود و مجاز بر به‌کارگیری خشونت و جنگ‌افزار بر دشمن می‌باشد.(رجبی مسرور و همکاران، ۱۳۹۷:۱۹-۱۷) سازمان دفاعی سایبری، سازمانی است که بخش‌ها و نیروهای آن، وظیفهٔ ایجاد آمادگی و توانمندی دفاعی از راه افزایش قابلیت‌ها و مهارت‌های پاسخ به تهدیدهای سایبری که از فضای سایبری (مجازی)[1] سرچشمه می‌گیرد را دارند. به‌روز شدن نیروهای مسلح در عصر حاضر ضروری است. وجود قابلیت دفاع سایبری برای نهادهای هر کشوری لازم است تا امنیت ملی در ابعاد گوناگون فضای سایبری تضمین شود.(Hathway, et.al, 2015:11)

۲-۲. الگوهای ارزیابی در حوزهٔ فضای سایبر

براساس جستجوهای به‌عمل آمده ۸ الگوی شناخته شده بین‌المللی ارزیابی سایبری مورد مطالعه و بررسی قرار گرفتند. این الگوها از مهم‌ترین و مشهورترین الگوهای ارزیابی در این حوزه می‌باشند که در دنیا معرفی و به‌کار گرفته شده‌اند. تعداد معیارهای معرفی شده با توجه به سه سطح مؤلفه‌ها، شاخص‌ها و سنجه‌ها در جدول شمارهٔ (۲) ارائه گردیده است:

۱. تفاوت معنایی برای «سایبری» و «مجازی» وجود ندارد، مگر وقتی که نیروهای نظامی یک کشور کلمهٔ سایبری را به جای مجازی به‌عنوان یک محیط عملیات به کار می‌برند.

www.SID.ir

Archive of SID

جدول شمارهٔ (٢) : الگوهای سایبری بررسی‌شده تحقیق

ردیف	الگوی ارزیابی	مؤلفه	شاخص	سنجه
١	شاخص قدرت سایبری[1] (Booz Allen Hamilton Inc, 2011)	٤	١٩	٣٠
٢	مسیر دستیابی به قدرت سایبری[2] (Booz Allen Hamilton Inc, 2011)	٥	١٠	٢١
٣	شاخص آمادگی سایبری[3] (Hathway, et.al, 2015:8)	٧	٥٨	–
٤	شاخص امنیت و پروفایل سلامت سایبری[4] (Zhang, 2014)	٦	٢١	–
٥	شاخص امنیت سایبری جهانی[5] (Minges, 2017)	٥	٢٤	–
٦	الگوی بلوغ امنیت سایبری[6] (Oxford Martin School, 2016)	٥	٢٤	٥٣
٧	الگوی بلوغ سایبری در منطقه آسیا و اقیانوسیه[7] (Feakin, 2016)	٥	١١	١٧
٨	الگوی بلوغ قابلیت امنیت سایبری[8] (Christopher, 2014)	١٠	–	–
٩	الگوی قابلیت‌های نظامی دفاع سایبری[9] (Oxford Martin School, 2016)	٨	٥٣	–

به‌منظور انتخاب کشورها برای بررسی برنامه‌های راهبردی، از رده‌بندی یک مؤسسه مشهور به نام «مرکز مطالعات راهبردی هِگ[10]» استفاده گردید. این مؤسسه با یک الگوی مناسب، میانگین رده‌بندی هر کشور را به‌طورکلی مورد محاسبه قرار داده است. (Gehem, et. al, 2015:71) ١٤ کشور که به ترتیب رتبه‌های ١ تا ١٤ را در این رده‌بندی به‌دست آورده‌اند، عبارتنداز: آمریکا، انگلیس، هلند، فنلاند، آلمان، استرالیا، کانادا، رژیم اشغالگر قدس، ژاپن، فرانسه، سوئد، کره جنوبی، اتریش و دانمارک. (TheNATO Cooperative Cyber Defence Centre of Excellence)

1. Cyber power index
2. The road to cyber power
3. Cyber Readiness Index
4. Global Cybersecurity Index & Cyberwellness Profiles
5. Global Cybersecurity Index (GCI)
6. Cybersecurity Capacity Maturity Model (CMM)
7. Cyber maturity in the Asia-Pacific region
8. Cybersecurity Capability Maturity Model (C2M2)
9. Stocktaking study of military cyber defence capabilities
10. The Hague Centre for Strategic Studies

www.SID.ir

Archive of SID

۳. یافته‌های تحقیق و تجزیه‌وتحلیل آنها

۳-۱. شناسایی ابعاد و مؤلفه‌ها

با مطالعه تطبیقی منابع بیان شده مؤلفه‌ها و شاخص‌های زیر استخراج گردید.

جدول شمارهٔ (۳) : مؤلفه‌های مشترک به‌دست آمده از الگوها و برنامه‌های راهبردی سایبری

ردیف	مؤلفه‌ها	منابع
۱	پاسخ به حادثه (عملیات سایبری) و امنیت	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016, Christopher, 2014)
۲	قانون و مقررات، جرائم سایبری	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016)
۳	اقتصاد دیجیتال، صنعت، دیپلماسی	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Oxford Martin School, 2016, Feakin, 2016)
٤	برنامهٔ راهبردی، رهنامه، حاکمیت و ساختار	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016, Christopher, 2014)
۵	تحقیق و توسعه، و استانداردها	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016, Christopher, 2014)
٦	مدیریت منابع انسانی و آموزش	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016, Christopher, 2014)
۷	زیرساخت‌ها، منابع و امکانات	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Oxford Martin School, 2016, Feakin, 2016)
۸	اجتماع و فرهنگ	(Booz Allen Hamilton Inc, 2011Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016)
۹	همکاری‌ها (ملی و بین‌المللی)	(Booz Allen Hamilton Inc, 2011, Hathway, et.al, 2015: 8, Zhang, 2014, Minges, 2017, Oxford Martin School, 2016, Feakin, 2016, Christopher, 2014)

مؤلفه‌های مناسب برای قدرت سایبری یک سازمان دفاعی با توجه به تعریف، مأموریت و هدف‌های سازمان دفاعی و همچنین قراردادن مؤلفه‌ها در معرض قضاوت خبرگان حوزهٔ دفاع سایبری در جلسه‌های مصاحبهٔ حضوری و در برخی موارد پرسشنامه‌ای، مؤلفه‌ها و شاخص‌های جدول شمارهٔ (٤) انتخاب گردید. چگونگی ارتباط و پسینی و پیشینی بودن (تقدم و تأخر) مؤلفه‌ها در الگوی مسیری در شکل شمارهٔ (۱) ارائه گردیده است.

www.SID.ir

Archive of SID

جدول شمارهٔ (٤): ابعاد، مؤلفه‌ها و سنجه‌های اندازه‌گیری استخراج شده

سازه‌های اصلی (مؤلفه‌ها)	سازه‌های فرعی (شاخص‌ها)	معرف‌ها (سنجه‌های اندازه‌گیری)
١- (A00) برنامهٔ راهبردی و رهنامهٔ سایبری	(A1) راهبرد کلان سازمانی	(a1) یکی از ارکان اصلی راهبرد کلان (کلی) سازمان
		(a2) هم‌راستایی و هماهنگی با دیگر موضوع‌های راهبردی
		(a3) تعیین و ارزیابی تأثیرات بر دیگر راهبردها
	(A2) سیاست‌های‌کلی و راهبردهای دفاعی نهادهای حفاظتی و امنیتی سازمان	(a4) محور اصلی سیاست‌گذاری امنیتی کلان در نگاه مدیران ارشد
		(a5) برگزاری و مستندسازی جلسه‌های منظم شناسایی تهدیدهای ویژه
		(a6) ارزیابی دقیق از آگاهی افراد از درک تهدیدهای سایبری و سطح مهارت در برخورد با تهدیدها
	(A3) سازوکار توسعه دکترین نظامی سایبری	(a7) سازوکار معین شناخت و توسعه ابعاد مختلف رهنامه
		(a8) مستندنگاری ساختار نظامی، تجهیز فنی نیروها، تمرین‌ها و ابزارهای هدایت عملیات
		(a9) تبیین اثربخش ابعاد مختلف رهنامهٔ دفاعی سایبری: عملیات شبکهٔ کامپیوتری و رهنامهٔ بازدارندگی سایبری
	(A4) برنامه راهبردی قدرت سایبری دفاعی	(a10) تحلیل محیطی قوی در طرح و برنامهٔ راهبردی
		(a11) پوشش کامل از محورهای اساسی امنیتی و قدرت دفاعی در طرح و برنامهٔ راهبردی
		(a12) تبیین مناسب ابعاد طرح و برنامهٔ راهبردی سایبری
	(A5) تخصیص منابع	(a13) تعیین انواع منابع و نقش و اثر هر یک در دستیابی به هدف‌ها و مأموریت‌ها
		(a14) سازوکار ایجاد ارزش از منابع و ارزیابی بهره‌وری
		(a15) کفایت مقدار و تنوع منابع و امکانات
	(A6) سازوکار ارزیابی و به‌روز رسانی راهبردها و برنامه‌ها	(a16) سازوکار ارزیابی و به‌روزرسانی راهبردها و برنامه‌ها
		(a17) مشارکت تمام افراد در تدوین و به‌روز رسانی سازوکار ارزیابی و به‌روز رسانی راهبردها و برنامه‌ها
		(a18) تبیین اثربخش راهبردها، برنامه‌ها و سیاست‌های جدید در تمامی سطوح سازمان و برای تمامی افراد

www.SID.ir

Archive of SID

سازه‌های اصلی (مؤلفه‌ها)	سازه‌های فرعی (شاخص‌ها)	معرف‌ها (سنجه‌های اندازه‌گیری)
۲- (B00) تامین و توسعه زیر ساخت‌ها	(B1) واحدهای سازمانی در اجرای راهبردها و برنامه‌ها	(b1) طراحی ساختار سازمانی مناسبی برای اجرای راهبردها و برنامه‌های دفاع سایبری
		(b2) تعیین رسمی و مستند نقش‌ها، مسئولیت‌ها و اختیارات مشخص برای اجرای برنامه‌های سایبری
		(b3) تعیین، ارزیابی و واپایش فرایندهای اجرایی، ارتباطی و تعاملات هریک از واحدهای سازمانی در رابطه با برنامه‌ها
	(B2) واحدها و گروه‌های پاسخ به حوادث	(b4) ضرورت ایجاد واحدهای پاسخ به حوادث از دیدگاه مدیران ارشد
		(b5) تأثیر بالا از فعالیت‌های گروه‌های پاسخ به حوادث
		(b6) برنامه‌ریزی مدون و طرح کلی، ساختارها و فرایندهای واحدهای پاسخ به حوادث
	(B3) مرکز توسعه و آزمایش قابلیت‌های تهاجمی سایبری	(b7) برنامه‌ریزی رسمی، ساختارها و فرایندهای یک مرکز برای توسعه و آزمایش قابلیت‌های تهاجمی سایبری
		(b8) برنامه اختصاصی تولید سلاح‌ها و تجهیزات تهاجمی بازدارنده و جدید سایبری
		(b9) طراحی یک نظام جامع از روش‌ها و ابزارهای پایش و تحلیل سلاح‌های سایبری (همگامی با جهان)
	(B4) آزمایشگاه تست سخت‌افزارها و نرم‌افزارهای رایانه‌ای	(b10) تعیین معیارهای کارآمد برای ارزیابی امنیتی در سند «راهنمای آزمایشگاه‌ها»
		(b11) ارزیابی امنیتی بر اساس استانداردها و آیین‌نامه‌ها
		(b12) سیاست‌های مناسب در حفاظت از تمامی ابعاد وظایف و مأموریت‌های آزمایشگاه تست
	(B5) مرکز مستقل تحقیق و توسعه و آینده‌پژوهی	(b13) تدوین کتاب راهنمای (هندبوک) اختصاصی از روش‌ها و ابزارهای تحقیق، توسعه و آینده‌پژوهی
		(b14) چهارچوب تحلیلی انطباق راهبردها و نقاط تمرکز مرکز بر تغییرهای مسئله‌ساز قدرت سایبری
		(b15) تدوین شاخص‌های اثربخشی، کارایی و تحقق هدف‌ها و مأموریت‌های مرکز

www.SID.ir

Archive of SID

سازه‌های اصلی (مؤلفه‌ها)	سازه‌های فرعی (شاخص‌ها)	معرف‌ها (سنجه‌های اندازه‌گیری)
٣- (C00) مدیریت فرایندهای عملیات سایبری	(C1) شناسایی	(c1) تدوین فهرست کاملی از دارایی‌های سازمانی، انواع و میزان آسیب‌پذیری‌های آنها در سازمان
		(c2) تعیین، مستندسازی و اندازه‌گیری اثر تهدیدها و آسیب‌ها بر کارکردها و وابستگی‌ها
		(c3) اولویت‌بندی تمامی مأموریت‌های سازمانی، هدف‌ها، صاحبان منافع و فعالیت‌های سازمانی
	(C2) مدیریت و ارزیابی خطرها	(c4) تعیین سیاست‌های قدرت دفاع سایبری، و همراستاسازی نقش‌ها و مسئولیت‌های داخلی و شرکای خارجی
		(c5) تمرکز بر خطرهای سایبری به‌وسیلهٔ فرایندهای حاکمیت مدیریت مخاطرهٔ یکپارچه
		(c6) چارچوب مدیریت و ارزیابی خطرهای سایبری، مبتنی بر حمایت کامل مدیران ارشد
	(C3) حفاظت	(c7) مدیریت کارآمد شناسایی، اعتبارسنجی و دسترسی به دارایی‌ها و تسهیلات
		(c8) مدیریت تضمین امنیت و انعطاف‌پذیری نظام‌ها و دارایی‌ها، مطابق با سیاست‌ها و رویه‌ها
		(c9) مستندسازی و اجرای پرونده‌های ممیزی/ ثبت
	(C4) کشف	(c10) تدوین و بهبود مداوم فرایندها و نقش‌ها برای کشف
		(c11) سازوکار رسمی تحلیل رویدادها و ارزیابی حفاظتی
		(c12) نظام پایش کارآمد از کارکنان غیرمجاز، اتصالات، دستگاه‌ها، نرم‌افزارها و اسکن‌های آسیب‌پذیر
	(C5) پاسخ	(c13) تدوین، اجرا و نگهداری- تعمیرات فرایندهای پاسخ به‌موقع و کشف رویدادهای سایبری
		(c14) فعالیت‌های مدون برای پیشگیری از گسترش یک رویداد، کاهش اثرهای آن و ریشه‌کن شدن حادثه
		(c15) به‌روز رسانی راهبردها و فعالیت‌های پاسخ با یکپارچه‌سازی تجربه‌های کشف و پاسخ گذشته
	(C6) بازیابی	(c16) تدوین، اجرا و نگهداری- تعمیرات فرایندهای بازیابی برای

www.SID.ir

Archive of SID

سازه‌های اصلی (مؤلفه‌ها)	سازه‌های فرعی (شاخص‌ها)	معرف‌ها (سنجه‌های اندازه‌گیری)
		اطمینان از بازگرداندن به موقع نظام‌ها در رویدادها
		(c17) طرح و برنامه مدون بازیابی در طول و پس از حادثه
		(c18) بهبود مداوم برنامه‌ریزی و پردازش بازیابی به‌وسیلهٔ ترکیب درس‌های آموخته‌شده با فعالیت‌های آینده
	(C7) گردش اطلاعات و ارتباطات	(c19) قابلیت اطمینان کارکنان از نقش خود و ترتیب انجام عملیات، در هنگام یک پاسخ موردنیاز
		(c20) هماهنگی فعالیت‌های واکنش و بازسازی با ذینفعان داخل و خارج سازمان
		(c21) اشتراک‌گذاری داوطلبانه اطلاعات با صاحبان منافع خارجی در جهت رسیدن به آگاهی موقعیتی امنیت سایبری گسترده‌تر
	(C8) تدوین استانداردهای سطح سازمان	(c22) تدوین رسمی استانداردها با گرفتن بازخورد کافی از همه صاحبان منافع
		(c23) به‌روز رسانی استانداردها در بازه‌های زمانی مشخص
		(c24) سازوکار قوی تدوین استانداردهای بومی
٤- (D00) مدیریت سرمایه‌های انسانی	(D1) جذب و استخدام متخصصین و نخبگان	(d1) قابلیت جذب بهترین متخصصان و نخبگان
		(d2) ایجاد تحرک و پویایی به‌وسیلهٔ سیاست‌ها در نیروها
		(d3) مسیر شغلی معین، انگیزشی و مطلوب
	(D2) آموزش و ارتقای توانمندی‌ها	(d4) برنامهٔ آموزشی مدون و منظم، الزام‌های دانش سایبری
		(d5) ارزیابی کارایی و اثربخشی برنامه‌های آموزشی
		(d6) بستهٔ متنوع از امکانات آموزشی باتوجه به مجموعه‌ای از روش‌های مختلف (سنتی و نوین) آموزشی
	(D3) نگهداری و مسیر شغلی معین و انگیزشی	(d7) تعریف مناسب، انگیزشی و موردپسند ساختارهای ارتقا و ترفیع کارکنان
		(d8) بسترسازی مناسب برای به کارگیری ساختارها و فرآیندهای تعریف شده مربوط به ارتقای شغلی
		(d8) جبران خدمت مناسب و شایسته کارکنان سازمان

www.SID.ir

Archive of SID

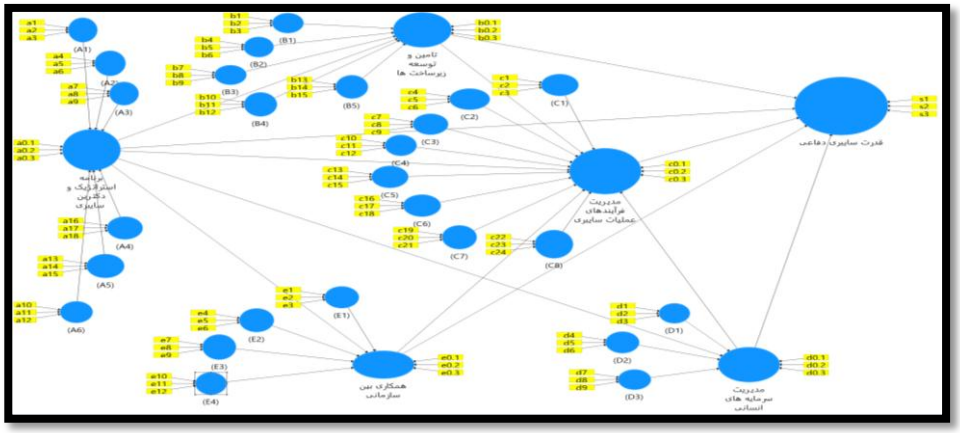
سازه‌های اصلی (مؤلفه‌ها)	سازه‌های فرعی (شاخص‌ها)	معرف‌ها (سنجه‌های اندازه‌گیری)
٥- (E00) همکاری بین سازمانی	(E1) هیئت مدیره همکاری بین سازمانی برای تمرینات سایبری	(e1) سازماندهی یک هیئت مدیره با توانمندی‌های لازم
		(e2) تدوین، مستندسازی و توسعه رویه‌ها، دستورالعمل‌ها و سیاست‌های اجرایی هیئت مدیره تمرین‌های سایبری
		(e3) سازوکار رسمی و نظام‌مند دریافت بازخوردهای مناسب
	(E2) چارچوب مدون همکاری رسمی و غیر رسمی با دیگر سازمان‌ها	(e4) فهرست همکاران سازمانی بالقوه، سطح توانمندی‌ها، هدف‌ها و زمینه‌های همکاری راهبردی، راهکنشی و فنی (تکنیکی)
		(e5) برنامهٔ رسمی و مدون راهبردی برای همکاری‌ها
		(e6) سازوکار و روش مناسب انتخاب انواع تمرین‌ها، عملیات‌های مشترک و شرکای عملیاتی دوجانبه و چندجانبه
	(E3) تدوین استانداردهای امنیتی و دفاعی سایبری بومی با مشارکت شرکا	(e7) فرایندهای رسمی برای تدوین استانداردهای موردنیاز
		(e8) قوانین و سیاست‌های الزام‌آور در تعهد به استفاده از استانداردهای تصویب شده در میان سازمان‌های همکار
		(e9) سازوکار رسمی با دخالت دادن تمام صاحبان منافع برای اصلاح، به‌روز رسانی و بومی‌سازی استانداردها
	(E4) تدوین سازوکارآموزش و اعطا گواهینامه‌های حرفه‌ای	(e10) برنامهٔ آموزشی مدون و منظم، و مسابقه‌های علمی بین‌گروهی در ارتباط با موضوع‌های سایبری
		(e11) ارزیابی و اندازه‌گیری کارایی و اثربخشی برنامه‌های آموزشی
		(e12) اعطای گواهینامه‌های حرفه‌ای ملی و بین المللی

۳-۲. ترسیم و طراحی الگوی مسیری

مؤلفه‌های قدرت سایبری در نرم افزار «اسمارت پی.ال.اس ۳» الگوسازی گردید (شکل شمارهٔ ۱). دایره‌های بزرگ‌تر با شماره‌های ۱ تا ۵ مؤلفه‌های قدرت سایبری هستند. دایره‌های کوچکتر متصل به مولفه‌ها شاخص‌ها و مستطیل‌های کوچک متصل به هرشاخص سنجه‌های اندازه‌گیری می‌باشند. سازهٔ هدف الگو بزرگ‌ترین دایره در انتهای سمت راست، قدرت سایبری دفاعی است.

www.SID.ir

Archive of SID



شکل شمارهٔ (۱) : الگوی طراحی‌شده با نرم‌افزار SMART-PLS

۳-۳. جداول نتایج آزمون‌ها

باتوجه به حجم زیاد نتایج آزمون‌ها به‌منظور جلوگیری از طولانی شدن مقالهٔ حاضر، خلاصه نتایج ارائه می‌گردد. نتایج تفصیلی در منبع بیان‌شده موجود می‌باشد. کلیهٔ آزمون‌ها اندازهٔ قابل قبول را به‌دست آوردند.

جدول شمارهٔ (۵): خلاصه نتایج آزمون‌های آماری الگو

آزمون	متغیر با کمترین مقدار	متغیر با بیشترین مقدار
روایی قانونی سنجه‌ها	توسط ۱۰ نفر از خبرگان به میزان ۱۰۰٪ تأیید گردید.	
هم‌خطی (VIF)	b8	a13
معناداری(t-value) اندازه‌گیری	a17	b7
روایی همگرا اندازه‌گیری (R^2Reflective)	E4	C5
R^2	E00	C00
هم‌خطی(VIF) ساختاری	D1 و E00 مرتبط با B00	E2 و B00 مرتبط با C00
معناداری(t-value) ساختاری	E4 مرتبط با E00	C6 و D00 مرتبط با C00

www.SID.ir

Archive of SID

شکل شمارهٔ (٢) : نمودار مفهومی الگوی قدرت سایبری

٤. نتیجه‌گیری

٤-١. جمع‌بندی

کیفیت حضور یک کشور در صحنهٔ بین‌المللی با بحث «قدرت ملی» آمیخته شده است؛ در سال‌های اخیر قدرت سایبری به‌عنوان بعد پنجم قدرت ملی معرفی شده است. عدم وجود الگوهای ارزیابی به‌منظور اندازه‌گیری قدرت سایبری باعث عدم آگاهی از میزان قابلیت‌های دفاعی در حوزهٔ سایبر گردیده است که درنهایت منجر به مدیریت ناکارآمد حوزهٔ دفاع سایبری

www.SID.ir

Archive of SID

می‌گردد؛ امروزه به‌منظور پاسخگویی سریع به تغییرهای محیطی فزاینده فضای سایبر به‌ویژه در موضوع دفاع نه تنها باید از الگوهای کارآمد پایش و ارزیابی قدرت دفاعی سایبری استفاده نمود، بلکه باید توانمندی لازم در ابعاد مختلف تهاجم و بازدارندگی را نیز به‌دست آورد، چرا که مهم‌ترین مأموریت یک سازمان دفاعی تأمین امنیت کشور است. پایش و ارزیابی مستمر قدرت دفاعی سایبری از سویی نقاط ضعف و حوزه‌های نیازمند بهبود را نمایان می‌سازد، و از سوی دیگر فرایندهای کسب توانمندی در قدرت تهاجمی سایبری را شکل می‌دهد. همچنین باتوجه به اهمیت تمرکز تصمیم‌گیری بر حوزهٔ سایبر، ایفای نقش فرماندهی سایبری توسط یک یا مجموعه‌ای از سازمان‌های دفاعی می‌تواند راهبرد هوشمندانه‌ای بوده و در میزان قابلیت اطمینان دفاعی کشور در محیط سایبر افزایش قابل توجهی ایجاد نماید.

این تحقیق همان‌گونه که در شکل شمارهٔ (۱) ارائه گردید، چنین بیان می‌دارد که ارزیابی قدرت سایبری در سازمان‌های دفاعی کشور می‌تواند از الگوی ارائه شده پیروی نماید. این الگو شامل ۵ مؤلفه، ۲۶ شاخص و ۷۸ سنجه اندازه‌گیری است که در مؤلفه‌ها، (C00) مدیریت فرایندهای عملیات سایبری، به‌عنوان مؤلفه اولویت‌دار و در شاخص‌ها، (D1) جذب و استخدام متخصصین و نخبگان، و در سنجه‌ها، (b8) برنامهٔ اختصاصی تولید سلاح‌ها و تجهیزات تهاجمی بازدارنده و جدید سایبری، به‌عنوان اولویت‌های قابل توجه در این حوزه مطرح می‌باشند. در ادامه بر اساس الگوی طراحی‌شده و شکاف وضعیت موجود پیشنهادهای اجرایی و تحقیقاتی ارائه شده است.

٤-۲. پیشنهادها

پیشنهادهایی در سطح عملیاتی سازمان‌های دفاعی:

(۱) به‌کارگیری یک چارچوب کلان بومی برای برنامه‌ریزی راهبردی و رهنامهٔ سایبری در بالاترین سطح سازمان، که شامل الگوی ارزیابی کمی اثربخشی، توسعه و به‌روزرسانی راهبردها، تخصیص منابع، برنامه‌های راهبردی بخشی و ارزیابی همگامی با دیگر راهبردها، و سازوکار توسعهٔ رهنامه باشد.

www.SID.ir

Archive of SID

(٢) استقرار نظام تحلیل و بررسی، پایش و توسعهٔ تولید و آزمایش سلاح‌های مدرن سایبری.

(٣) استخدام، ارتقای مسیر شغلی، آموزش و حفظ نخبگان و سرمایه‌های انسانی که می‌توانند بیشترین تأثیر را در محیط عملیات سایبری داشته باشند.

(٤) ایجاد سازوکارهای یکپارچه جهت شکل‌گیری فرایندهای متقن حکمرانی سایبری دفاعی و تدوین دستورالعمل‌های اجرایی آن.

(٥) به‌کارگیری نیروهای غیرنظامی سایبری در همکاری با نیروهای نظامی در نقش‌آفرینی در عملیات‌های مشترک.

پیشنهادهایی برای تکمیل یا ادامه تحقیقات در زمینهٔ پژوهش:

(١) تدوین نقشهٔ راه قدرت سایبری دفاعی برای مجموعه سازمان‌های سایبری ج.ا.ایران یا برای سازمان‌های دفاعی ایران.

(٢) تدوین برنامهٔ راهبردی و رهنامهٔ دفاعی قدرت سایبری ج.ا.ایران یا برای سازمان‌های دفاعی ایران.

٣ . تدوین چهارچوب عملیات سایبری سازمان‌های دفاعی ایران.

*****

www.SID.ir

Archive of SID

فهرست منابع

الف. منابع فارسی

۱. احمدی، اردشیر، علی‌یاری، شهرام، ندرتی، رضا (۱۳۹٦)، ارائه یک مدل برای شایستگی‌های پاسداری در سازمان دفاعی، ***فصلنامهٔ راهبرد دفاعی***، سال پانزدهم، شمارهٔ ۵۷.

۲. تقی‌پور، رضا و اسماعیلی، علی (۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، ***فصلنامهٔ امنیت ملی***، سال هشتم، شمارهٔ سی‌ام.

۳. دهقانی پوده، حسین و پاشایی هولاسو، امین (۱۳۹٦)، تحلیل تعامل عوامل موثر بر نوآوری سازمان‌های دفاعی با استفاده از رویکرد مدلسازی ساختاری و تفسیری (ISM)، ***فصلنامهٔ علمی-پژوهشی مدیریت نظامی***، شمارهٔ ۳.

٤. زرقانی، سید هادی (۱۳۸۷)، تحلیل و ارزیابی متغیرها و شاخص‌های قدرت نظامی، ***فصلنامهٔ راهبرد دفاعی***، سال ششم، شماره ۲۳.

۵. ساعی، علی و اکبرزاده، علیرضا (۱۳۸۹)، بررسی نقش فرهنگ سلسله مراتبی در اثربخشی سازمان‌های نظامی (مطالعه موردی: دانشگاه افسری امام علی(ع)، ***فصلنامهٔ علمی- پژوهشی مدیریت نظامی***، شمارهٔ ۳۹.

٦. شهلائی، ناصر (۱۳۹۵)، ابعاد و شاخص‌های ارزیابی قابلیت‌های علم و فناوری در سازمان‌های نظامی جمهوری اسلامی ایران، ***فصلنامهٔ راهبرد دفاعی***، سال چهاردهم، شمارهٔ ٥٤.

۷. رجبی مسرور، حسن، توفیق، علی‌اصغر، قاضی‌زاده فرد، سیدضیاءالدین (۱۳۹۷)، طراحی الگوی تصمیم‌گیری برون‌سپاری فعالیت‌های اجرایی پروژه‌های تحقیق و توسعه و انتخاب پیمانکار برون‌سپاری، ***فصلنامه راهبرد دفاعی***، سال شانزدهم، شمارهٔ ٦۳.

۸. نصرت‌آبادی، جمشید، لشگریان، حمیدرضا، مردانی شهربابک، محمد، موحدی‌صفت، محمدرضا (۱۳۹۷)، ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، ***فصلنامهٔ امنیت ملی***، سال نهم، شماره سی‌ویکم.

۹. هلیلی، خداداد، ولوی، محمدرضا، موحدی صفت، محمدرضا (۱۳۹۷)، شناسایی عوامل و مولفه‌های اثرگذار بر تدوین رهنامه قدرت سایبری ج.ا.ایران مبتنی بر سیاست‌های ابلاغی و اسناد بالا دستی، ***فصلنامه راهبرد دفاعی***، سال شانزدهم، شمارهٔ ٦۳.

ب. منابع انگلیسی

1. Bebber, Robert, (2017), Cyber power and cyber effectiveness: An analytic framework, ***Comparative Strategy***, 36:5.
2. Booz Allen Hamilton, (2011), Cyber power index: finding and methodology, An Economist Intelligence, ***Unit research program***.
3. Booz Allen Hamilton, (2011), The Road to Cyberpower, Seizing Opportunity While Managing Risk in the Digital Age.

www.SID.ir

Archive of SID

4. Cheryl Burke Jarvis, Scott B MacKenzie and Philip M Podsakoff, (2003). A Critical Review of Construct Indicators and Measurement Model Specification in Marketing and Consumer Research, ***Journal of Consumer Research***, vol. 30, , No. 2.
5. Cate, (2015), ***THE DEPARTMENT OF DEFENSE CYBER STRATEGY***, The secretary of defence, Washington DC.
6. Chin, (1998), The partial least squares approach to structural equation modeling, In G. A. Marcoulides (Ed.), ***Modern methods for business research*** (pp. 295-336).
7. Christophe, (2014), ***Cybersecurity Capability Maturity Model*** (C2M2), White House initiative, the U.S.Department of Energy (DOE) and Department of Homland Security (DHS), Version 1.1.
8. Diamantopoulos, Adamantios, and Winklhofer, Heidi, (2001), Index Construction with Formative Indicators: An Alternative to Scale Development", ***Journal of Marketing Research***, vol. 38, no.2.
9. Drucker, F. Peter, (2006), ***managing for results***, HarperBusiness; Reissue edition.
10. Feakin, (2016), ***CYBER MATURITY IN THE ASIA-PACIFIC REGION***, Australia, Australian Strategic Policy Institute.
11. Freedman, Lawrence, (2015), ***Strategy: A History***, Publisher: Oxford University Press.
12. Garson, (2016), ***Partial Least Squares Regression and Structural Equation Models***, Statistical Associates Blue Book Series, Kindle Edition.
13. Gehem, Maarten, Artur Usanov, Erik Frinking, Michel Rademaker, (2015), ***ASSESSING CYBER SECURITY: A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS***, The Hague Centre for Strategic Studies.
14. Haaster, Jelle, (2016), Assessing Cyber Power, ***8th International Conference on Cyber Con?*** ict, Faculty of Military Sciences.
15. Hafeznia, Mohammad Reza, Seyed Hadi Zarghani, Zahra Ahmadipor and Abdelreza Roknoddin Eftekhari (2008), Presentation a new model to measure national power of the countries, J**. *Appl. Sci***. 8, 230–240.
16. Hair Jr.Joseph F., Mary Wolfinbarger Celsi, Arthur H. Money, Phillip Samouel, (2011), ***Essentials of Business Research Methods***. Pub. Location: New York; second edition.
17. Hair and others, (2017), A PRIMER ON PARTIAL LEAST SQUARES STRUCTURAL EQUATION MODELING (PLS- SEM), 2nd Ed, ***Thousand Oaks***: Sage.
18. Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, (2015), ***CYBER READINESS INDEX 2.0***, Measuring and Assessing the Cybersecurity Challenge. Published by Potomac Institute for Policy Studies.
19. Henseler and Chin, (2010), A Comparison of Approaches for the Analysis of Interaction Effects Between Latent Variables Using Partial Least Squares Path Modeling, Taylor & Francis, ***Structural Equation Modeling***, 17.
20. Hohn, (2014), ***Geopolitics and the Measurement of National Power***, Ph.D. Thesis, university of Hamburg, Germany.
21. Hunker, (2010), Cyber War and Cyber Power Issues for NATO Doctorin, ***Research Division***, NATO Defence College, Rome, 62.

www.SID.ir

Archive of SID

22. Inkster, Nigel, (2017), Measuring Military Cyber Power, ***Survival***, 59:4, 27-34, DOI: 10.1080/00396338.2017.1349770
23. Kadera and Sorokin (2004), Measuring national power, Int. ***Interact***, 30.
24. Kramer, Franklin D., Stuart H. Starr, Larry K. Wentz (2009), ***Cyberpower and National Security***, 1st Edition. Published by: University of Nebraska Press, Potomac Books.
25. Kuehl, D, (2009), From cyberspace to cyberpower: defining the problem, in: F. Kramer, S. Starr, L. Wentz (Eds.), ***Cyberpower and National Security***, Potomac Books, Dulles, Virginia.
26. Liao, Hua, Weihua Dong, Huiping Liu and Yuejing Ge (2015), Towards Measuring and Visualizing Sustainable National Power—A Case Study of China and Neighboring Countries. ***ISPRS International Journal of Geo-Information,*** 4(3).
27. Minges, (2017), ***Global Cybersecurity Index (GCI)***, the Internatonal Telecommunication Union (ITU).
28. Nye, J, (2011), ***The Future of Power, Public Affairs***, Philadelphia, Pennsylvania.
29. Oxford Martin School, , (3/31/2016), ***Cybersecurity Capacity Maturity Model for Nations (CMM)***, Revised Edition.
30. Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez, (2013), ***Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*** Prepared for the European Defence Agency, Published by the RAND Corporation.
31. Rowland, Jill, Mason Rice, Sujeet Shenoi, (2014) The anatomy of a cyber power, ***International Journal of Critical Infrastructure Protection***. (7) 3–11.
32. Sheldon, J.B.. (2012). Toward a theory of cyber power: Strategic purpose in peace and war. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. 207-224. Starr, Stuart, (2011) Towards an Evolving Theory of Cyberpower, Series Cryptology and Information Security Series, ***Ebook,*** Vol 3.
33. Tabansky, Lior, (2016), Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy, ***8th International Conference on Cyber Conflict Cyber Power***, Blavatnik Interdisciplinary Cyber Research Center (ICRC) Tel Aviv Uni.
34. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) available at: https://ccdcoe.org/cyber-security-strategy- documents.html.
35. Treverton and Jones, (2005), Measuring National Power, ***RAND***, national security research division.
36. Walden, David D., R. Douglas Hamelin, Michael E. Krueger, (2015), ***Systems Engineering Handbook A Guide For System Life Cycle Processes and Activities***, Wiley, 4th edition. ISBN-13: 978-1118999400
37. Zhang, Shao Tong, Qin Chuan The, Aliya Abdul Razack, and Ineze Anni, (2014), ***Global Cybersecurity Index&Cyberwellness Profiles, a cooperative partnership between ABI Research and International Telecommunication Union (ITU)***, Switzerland.

www.SID.ir