ISSN:2821-1588 htpps://www.jadm.khadu.ir

Journal of Air Defense Management
Volume 2, Issue 5
Spring 2023
P.P. 159-170

Research Paper

Explaining the Dimensions and Components of Cyber Resilience of Logistics and Defense Supply Chain

Hadi Baghbani[1], Amir Masood Saadatmand[2]

1. Assistant Prof., Shahid Sattari Aeronautical University of Sciences and Technology, Tehran, Iran. **E-mail: Baghbanihady@gmail.com**
2. PhD in Cyber Strategic Management, Faculty of Strategic Management, Supreme National Defense Universityh, Tehran, Iran. **E-mail: A.saadatmand@sndu.ac.ir**

bArticle Information

Received: 2023/01/02

Accepted: 2023/03/16

Keywords:

Resilience, Cyber, Logistics, supply Chain.

Corresponding Author: Hadi Baghbani

Email: *Baghbanihady@gmail.com*

Abstract

Background & Purpose: The strategic position of the Islamic Republic of Iran in the region and the international system and the failure of the domination system in the field of severe threats and its cost-effectiveness have caused a change in the strategy of the enemies of the Islamic system and the use of the available capacities in the cyberspace in order to confront has become the Islamic Republic of Iran. Based on this, the security and resilience of the cyber space as one of the components of national security and subsequently the cyber resilience of logistics and the supply chain of the armed forces in support of the battlefield and the continuation of the operations of the forces must be seriously considered. Its dimensions and components are evaluated and by identifying the strengths and weaknesses in different areas and by planning and presenting the necessary strategies, they will ultimately promote it. In this regard, the aim of this research is to achieve the dimensions and components of cyber resilience of logistics and the supply chain of the armed forces of the Islamic Republic of Iran.

Methodology: In order to extract the components of cyber resilience, the themes related to cyber resilience were done by studying the research literature and qualitative analysis of the existing documents, and then with the clustering technique and based on the frequency of repetition of words, the main components were initially recognized. and these components were modified through Delphi technique with the consensus of experts.

Findings: Based on this, by referring to scientific-research articles in this field and documents of international institutions, and by applying the clustering technique in content analysis and the Delphi method, four stages of the resilience event management cycle by adding the dimension of "discovery" to other dimensions. The concept of cyber resilience was confirmed, also the four domains of network-based war doctrine including physical, informational, cognitive and social were examined and finally by using the above definitions and creating a general matrix of criteria and evaluating their consequences during the stages and Different areas, dimensions and components of cyber resilience of logistics and defense supply chain were presented after the approval of cyber experts.

Conclusion: The results of this research can be used to identify and explain dimensions and components, produce literature, create consensus in decision-making and decision-making centers, strengthen and promote strategic thinking, smart methods to deal with increasing threats in the field of logistics resilience and defense chain.

Citation: Baghbani, Hadi and Saadatmand, Amir Masood.(2023). Explaining the Dimensions and Components of Cyber Resilience of Logistics and Defense Supply Chain. *Journal of Air Defense Management*, 2(5), 159-170.

ISSN:2821-1588 htpps://www.jadm.khadu.ir

فصلنامه علمی مدیریت دفاع هوایی
دورهٔ ۲، شمارهٔ ۵
بهار ۱۴۰۲
صص ۱۵۹-۱۷۰

مقاله پژوهشی

تبیین ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی

هادی باغبانی[۱]، امیر مسعود سعادتمند[۲]

۱. استادیار، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران. **رایانامه:** Baghbanihady@gmail.com

۲. دکتری مدیریت راهبردی سایبر، دانشکده مدیریت راهبردی، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران. **رایانامه:** A.saadatmand@sndu.ac.ir

اطلاعات مقاله

تاریخ دریافت:
۱۴۰۱/۱۱/۱۲

تاریخ پذیرش:
۱۴۰۱/۱۲/۲۵

کلیدواژه‌ها:
تاب آوری، سایبری، لجستیک، زنجیره تامین.

نویسنده مسئول:
هادی باغبانی

ایمیل:
Baghbanihady@gmail.com

چکیده

زمینه و هدف: موقعیت راهبردی جمهوری اسلامی ایران در منطقه و نظام بین‌الملل و ناکامی نظام سلطه در عرصه تهدیدهای سخت و هزینه‌بر بودن آن موجب تغییر راهبرد دشمنان نظام اسلامی و استفاده از ظرفیت‌های موجود در فضای سایبری به منظور تقابل با جمهوری اسلامی ایران گردیده است. بر این اساس امنیت و تاب‌آوری فضای سایبری به عنوان یکی از مولفه‌های امنیت ملی و متعاقب آن تاب‌آوری سایبری لجستیک و زنجیره تامین نیروهای مسلح در پشتیبانی از میدان نبرد و تداوم عملیات نیروها باید به طور جدی مورد توجه واقع شده، ابعاد و مولفه‌های آن مورد ارزیابی و با شناسایی نقاط قوت و ضعف در حوزه‌های مختلف و با برنامه‌ریزی و ارائه راهبردهای لازم، در نهایت موجب ارتقاء آن گردند. در همین راستا هدف این پژوهش دستیابی به ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین نیروهای مسلح جمهوری اسلامی ایران است.

روش‌شناسی: به منظور استخراج مولفه‌های تاب‌آوری سایبری، مضامین مرتبط با تاب‌آوری سایبری، با مطالعه ادبیات پژوهش و تحلیل کیفی اسناد موجود صورت پذیرفت و سپس با تکنیک خوشه‌بندی و بر اساس فراوانی تکرار واژه‌ها، مولفه‌های اصلی مورد بازشناسی اولیه قرار گرفتند و این مولفه‌ها از طریق تکنیک دلفی با اجماع نظر خبرگان اصلاح گردیدند.

یافته‌ها: بر این اساس با استناد به مقالات علمی- پژوهشی در این حوزه و اسناد موسسات جهانی و با به کارگیری فن خوشه‌بندی در تحلیل محتوا و روش دلفی، چهار مرحله از چرخه مدیریت رویداد تاب‌آوری با افزودن بعد " کشف" به سایر ابعاد متداول تاب‌آوری سایبری مورد تایید قرار گرفت همچنین چهار حوزه دکترین جنگ شبکه محور شامل فیزیکی، اطلاعاتی، شناختی و اجتماعی مورد بررسی قرار گرفت و نهایتا با استفاده از تعاریف فوق و ایجاد یک ماتریس عمومی از معیارها و ارزیابی پیامدهای آنها در طول مراحل و حوزه‌های مختلف، ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی پس از تایید خبرگان حوزه سایبر ارائه گردید.

نتیجه‌گیری: از نتایج این پژوهش می‌توان برای شناسایی و تبیین ابعاد و مولفه‌ها، تولید ادبیات، ایجاد وفاق در مراکز تصمیم‌سازی و تصمیم‌گیری، تقویت و ارتقاء تفکر راهبردی، روش های هوشمند مقابله‌ای با تهدیدات روزافزون در حوزه تاب‌آوری لجستیک و زنجیره دفاعی استفاده نمود.

استناد: باغبانی، هادی و سعادتمند، امیر مسعود. (۱۴۰۲). تبیین ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی. فصلنامه *مدیریت دفاع هوایی*، ۲(۵)، ۱۵۹-۱۷۰.

مقدمه

امروزه استفاده شتابان و روز افزون فناوری اطلاعات و ارتباطات در عرصه‌های اقتصادی، سیاسی، اجتماعی، نظامی و فرهنگی جوامع بر کسی پوشیده نیست و متولیان سیاست‌گذاری و تصمیم‌سازان از یک سو و صاحبان صنایع و مشاغل از سوی دیگر، ضمن تاکید بر بهره‌برداری از مزایای این فناوری، افزایش بهره‌وری و ارتقاء قابلیت‌های سازمان‌ها و سامانه‌های اطلاعاتی را در گرو استفاده هرچه بیشتر از این فناوری‌ها می‌دانند.

سازمان‌های دفاعی با بهره‌گیری حداکثری از قابلیت‌ها و ظرفیت‌های فناوری اطلاعات و ارتباطات در چرخه عمر زیرساخت‌های دفاعی و آفندی خود، به ویژه در سامانه‌های فرماندهی و کنترل، زنجیره تامین، ناوبری، موشک‌ها و ...، شاخص‌هایی نظیر دقت، سرعت، اطمینان و سایر قابلیت‌های نظامی خود را به طرز فوق‌العاده‌ای افزایش داده‌اند، به گونه‌ای که در راهبرد مدرن‌سازی دیجیتال وزارت دفاع ایالات متحده در سال ۲۰۱۹، استفاده از این فناوری به منظور سرعت بخشیدن به سازگاری و ادغام قابلیت‌های هوش مصنوعی، تحول سازمانی و انتقال به محیط ابری و مدرن‌سازی زیرساخت‌ها و سامانه‌های فرماندهی، کنترل، ارتباطات و رایانه‌های تسلیحات جنگی به وضوح مشاهده می‌شود(دستور العمل،۲۰۱۶).

همزمان با به کارگیری و تعبیه فناوری اطلاعات و ارتباطات در زنجیره تامین و لجستیک نیروهای مسلح، آنها به عنوان اهدافی جذاب برای حملات سایبری مورد توجه قرار گرفته است؛ به گونه‌ای که امروزه فضای سایبر توسط برخی از کشورها از جمله ایالات متحده و کشورهای عضو پیمان آتلانتیک شمالی(ناتو) به عنوان پنجمین قلمرو نظامی همراه با قلمروهای سنتی زمین، دریا، هوا و فضا به رسمیت شناخته شده است(ایگو لینکوف،۲۰۱۳).

تجارب چهار دهه اخیر نشان می‌دهد که جمهوری اسلامی ایران به واسطه موقعیت ممتاز ژئوپلیتیکی و نیز مختصات سیاسی و ایدئولوژیکی انقلاب اسلامی و نظام سیاسی آن، با طیف وسیعی از تهدیدهای سخت و نرم مواجه بوده و در این راستا تهدیدات سایبری با ویژگی‌هایی نظیر گمنامی، سرعت، محدود نبودن به مرزهای جغرافیایی و ... به عنوان یکی از مهمترین تهدیدات حال حاضر زیرساخت‌های حیاتی، امنیتی و دفاعی کشور و از جمله زنجیره تامین و لجستیک نیروهای مسلح محسوب می‌شوند. در حال حاضر بخشی از نیازمندی‌های دفاعی و تجهیزاتی نیروهای مسلح در قالب پروژه‌های تحقیقاتی و تولیدی توسط وزارت دفاع و پشتیبای نیروهای مسلح، سازمان‌های تحقیقات و جهادخودکفایی، دانشگاه‌ها و شرکت‌های دانش بنیان با استفاده از قابلیت‌های فناوری اطلاعات و ارتباطات تامین می‌گردد. رویکرد و اولویت اصلی در طراحی این محصولات، برآورده نمودن نیازمندی‌

های عملیاتی و ارتقاء قابلیت‌ها و توانمندی‌های سامانه‌های تولیدی، به ویـژه در مقایسـه بـا نمونه‌های خارجی است و این موضوع در صورتی است که راهبـرد تـاب‌آوری سـایبری ایـن سامانه‌ها، در چرخه عمر محصولات دفاعی شـامل ایـده‌پـردازی، توسـعه، تولیـد، بهـره‌وری، پشتیبانی و رهایی، به منظور مواجهه فعال با تهدیدات و حمـلات سـایبری و کـاهش سـطح آسیب‌پذیری‌ها و غافلگیری راهبردی به عنـوان بخـش اساسـی و سـاختاری زنجیـره تـامین محصولات دفاعی ملحوظ نمی‌گردد و این موضوع در مواردی که نیازمند خریداری تعدادی از اجزاء و زیر سامانه‌ها از منابع و شرکت‌های خـارجی وجـود دارد و آزمایشـگاه مرجعـی بـرای ارزیابی امنیت و تاب‌آوری سایبری آنها نیست، تشدید شده و عملاً مدیریت ریسـک زنجیـره تامین را با مخاطرات جدی مواجه ساخته است(آلکساندر،۲۰۱۸).

بدون شک به کارگیری استانداردها و کنترل‌های امنیتی تاب‌آوری سـایبری بـه عنـوان خط مبنا و حداقل الزامات مورد نیاز برای اعتماد و اطمینان به سامانه‌ها و تجهیزات نظامی بـا ماهیت سایبری محسوب می‌شوند. این موضـوع در صـورتی اسـت کـه در حـال حاضـر اولاً استانداردهای نظامی بومی در این حوزه تدوین نگردیده و ثانیاً رعایت و اجرای اسـتانداردهای معادل خارجی به دلیل عدم انطباق با زیست‌بوم این فناوری‌ها و تهدیـدات مـرتبط در کشـور عملاً با مشکلات جدی مواجه بوده و کارایی لازم را ندارند(ایگو لینکوف،۲۰۱۳).

از سوی دیگر، یکی از مهمترین ارکان مقابله با مخاطرات و تهدیدات سایبری و به تبـع آن تاب‌آوری سایبری در هر سازمانی، آگاهی‌رسانی و تبیین مضرات و آسیب‌های ناشی از آن می‌باشد. به عبارت دیگر به دلیل پیچیدگی و آشوبناک بودن محیط‌های سایبری و بعضا غیـر ملموس بودن تهدیدات این حوزه، کارکنان نیروهای مسلح درک مشخصی از تهدیـدات ایـن حوزه نداشته و این موضوع تبعات ناشی از این تهدیدات را دوچندان مـی‌کنـد. همچنـین بـه دلیل فقدان آموزش جامع و مدون در خصوص چگونگی طراحی، سـاخت و ارزیـابی سـخت‌–افزارها و نرم‌افزارهای امن همانند آمـوزش‌هـای طـولی و عرضـی مرسـوم در سـازمان‌هـای نیروهای مسلح، نیروی انسانی ماهر و آموزش دیده با چالش‌های جدی مواجه بوده و ضرورت دارد تدابیر لازم در این خصوص اتخاذ گردد(آلکساندر،۲۰۱۸).

بر این اساس و با توجه به اهمیت موضوع ضروری است به منظور بـرآوردی صـحیح از شرایط و آمادگی سامانه‌ها و تجهیزات جهت مقابله با تهدیدات و حملات سایبری به رویکـرد جامعی در رابطه با تاب‌آوری سایبری در ابعاد، مولفه‌هـا مربوطـه بـه منظـور ارتقـاء وضـعیت موجود، تقویت توانمندی‌ها، رفع معایب و جبران نواقص و نهایتا ترسیم افـق‌هـای آتـی نیـاز است تا از برخورد انفعالی و مقطعی با حوادث و بحران‌هـای سـایبری و اتخـاذ تصـمیم‌هـای عجولانه و علاج موقت آنها، پرهیز و ضمن ریشه‌یابی موضوعات، نسبت به برطـرف نمـودن

دلایل اصلی مشکلات اقدام شود . بر این اساس مسئله اصلی این تحقیق تبیین ابعاد و مولفه‌های اصلی تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی می‌باشد.

پیشینهٔ پژوهش

در اینکه کلمه تاب‌آوری مربوط به کدام حوزه علمی است بحث وجود دارد. برخی آن را مربوط به حوزه بوم‌شناسی و برخی دیگر آن را متعلق به فیزیک می‌دانند. مفهوم چند بعدی تاب‌آوری که دارای کاربردهای رو به رشد است، ابتدا در مطالعات منطقه‌ای مفهوم سازی شد و هدف از آن توضیح تفاوت بین مناطق مختلف اقتصادی بود. ولی با توجه به اینکه این مفهوم در بسیاری از رشته‌های دانشگاهی کاربرد دارد، از همین رو تعاریف متعدد و گاه کاملاً متفاوت از آن ارائه شده است به نحوی که آنها را می‌توان به هر کسی یا هر مکانی و یا هر پدیده‌ای اعم از اقتصادی، سیاسی، دفاعی و غیره نسبت داد.

تاب‌آوری معادل واژه انگلیسی RESILIENCE و در لغتنامه وبستر به معنای توانایی بازیابی، بهبودی سریع، تغییر، شناوری، کشسانی و همچنین خاصیت فنری و ارتجاعی آمده است. براساس تحلیل محتوای انجام شده از حدود ۱۲۰ تعریف از تاب‌آوری در رشته‌های مختلف، تفسیر مشترکی از رفتار سامانه‌های تاب‌آور ارائه شده است که این رفتار را می‌توان با کلماتی همانند انطباق، بازیابی عملکرد، جذب، حفظ، مقابله، بازگشت، پاسخ و مقاومت بیان کرد.

در مقایسه با تعاریف گفته شده، به نظر می‌رسد این تعریف از جامعیت بهتری برخوردار باشد: توانایی جذب اثرات یک رویداد مخرب، به حداقل رساندن اثرات نامطلوب، پاسخ مؤثر پس از رویداد، حفظ و یا بازیابی عملکرد و سازگاری به صورتی که با یادگیری برای مقابله با اثرات نامطلوب آینده آماده می شود.

این تعریف تقریباً به چهار دسته زمانی تقسیم می شوند: ۱- مرحله تأثیرپذیری (جذب، مقابله، مقاومت، حفظ)؛ ۲- مرحله پاسخ (پاسخ)؛ ۳- مرحله بهبودی (بازیابی، بازگشت)؛ ۴- آماده شدن برای تغییر حال و آینده (انطباق عملکرد). جردن و جاورنیک (۲۰۱۸) با تاکید بر سرعت بهبودی، تاب‌آوری را توانایی مقابله با فاجعه و اثرات آن به نحوی که به سرعت، بهبودی حاصل شود، می‌دانند.

موسسه ملی استاندارد و فناوری ایالات متحده تاب‌آوری سایبری را توانایی پیش‌بینی، مقاومت در برابر، بازیابی از و سازگاری با شرایط نامطلوب، استرس‌ها، حملات یا مصالحه در سامانه‌هایی که شامل منابع سایبری هستند، معرفی می‌کند. تاب آوری سایبری ممکن به یک سامانه، مؤلفه یا عنصر یک سامانه، یک زیرساخت حیاتی یا منطقه، سیستمی از سیستم

ها یا حتی به یک ملت اطلاق شود.

لجستیک و زنجیره تامین؛ لجستیک ریشه‌ای یونانی دارد و در امور نظامی برای جابجایی جنگ‌افزار، مهمات و جیره غذایی در مواقع حرکت از مکان اصلی به سمت خط مقدم استفاده می‌شود. در زبان یونانی، رومی و امپراطوری رم شرقی، نظامیانی وجود داشتند با نام LOGISTIKAS که وظیفه مسائل مالی و تقسیم مایحتاج بر عهده آنان بوده‌است. در فرهنگ فارسی معین، این لغت به معنی آماد، آمادگاری، بخشی از علوم نظامی که به حمل و نقل افراد و تجهیزات ارتش اختصاص دارد و در واژه‌نامه آکسفورد، قسمتی از علوم نظامی که وظیفه تهیه و تحویل آماد و جابجایی مواد و افراد و تجهیزات را دارد اشاره شده است(آلکساندر،۲۰۱۸).

بانک جهانی لجستیک را مجموعه‌ای از فعالیت‌ها از قبیل حمل و نقل، انبارداری، یکپارچه‌سازی بارهای تجاری، ترخیص کالا از گمرک، سامانه‌های توزیع درون کشوری و نظام‌های پرداخت توسط نهادهای دولتی و بخش خصوصی تعریف می‌کند و نهایتا انجمن مدیریت لجستیک، لجستیک را قسمتی از فرآیندهای زنجیره عرضه تعریف می‌کندکه جریان مؤثر و کارایی انبار و اطلاعات وابسته به کالاها و خدمات مربوط به آنها را از ابتدا تا نقطه مصرف به منظور برآورده کردن نیاز مشتری برنامه‌ریزی، اجراء و کنترل می‌نماید. لجستیک به آن بخش از فرآیند زنجیره تأمین اطلاق می‌شود که ذخیره‌سازی و جریان مؤثر و کارای کالاها، خدمات و اطلاعات وابسته به آنها را از نقطه شروع تا نقطه مصرف، جهت پاسخگویی به نیاز مشتریان، برنامه‌ریزی، اجرا و کنترل می‌نماید(ایگو لینکوف،۲۰۱۳).

از طرفی زنجیره تأمین به کلیه فعالیت‌های مرتبط با جریان تولید کالا از مرحله تأمین مواد اولیه تا مرحله تحویل کالای نهایی به مصرف کننده می‌باشد و مدیریت زنجیره تامین دارای سه فرآیند عمده شامل مدیریت اطلاعات، مدیریت لجستیک و مدیریت روابط می‌باشد.

تاب‌آوری زنجیره تامین عبارت است از قابلیت تطبیق‌پذیری یک زنجیره تامین برای آمادگی نسبت به اختلالات و پاسخگویی به آنها، بهبود و بازگشت به هنگام و مقرون به صرفه، و بنابراین پیشروی به سمت وضعیت عملکرد پس از اختلال که در حالت ایده‌آل، وضعیتی بهتر از وضعیت پیش از بروز اختلال است(صدیق پور،۱۳۹۶). چنانچه تاب‌آوری در مقابل اختلال ناشی از تهدیدات و حملات سایبری به سامانه لجستیک و زنجیره تامین دفاعی باشد، به آن تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی می‌گویند.

پیشینه تحقیق

لینکوف و همکاران در سال ۲۰۱۳، در مقاله‌ای با عنوان معیارهای تاب‌آوری سامانه‌های سایبر (ایگو لینکوف،۲۰۱۳) ادعا می‌کنند که ترکیبی از حوزه‌های دکترین جنگ شبکه محور

و تعریف ارائه شده از تاب‌آوری توسط آکادمی ملی علوم ایالات متحده می‌تواند برای توسعه معیارهای تاب‌آوری سایبری مورد استفاده قرار گیرد. در این مقاله چهارمرحله از چرخه مدیریت رویداد که برای تاب‌آوری لازم است شامل برنامه‌ریزی/ آماده‌سازی، جذب، بازیابی و سازگاری مورد استفاده قرار گرفته است.

اداره امنیت شبکه و اطلاعات اتحادیه اروپا در سال ۲۰۱۱، در سندی با عنوان شاخص‌ها و چارچوب تاب‌آوری شبکه و خدمات (دستورالعمل،۲۰۱۱)، نسبت به معرفی شاخص‌های ارزیابی تاب‌آوری سامانه‌های فناوری اطلاعات پرداخته است. در این سند، شاخص‌ها در قالب یک مدل دو بعدی سازماندهی شده است. بعد اول این مدل مبتنی بر این واقعیت است که می‌توان تاب‌آوری سایبری را نسبت به زمان وقوع حادثه طبقه‌بندی نمود. بر این اساس مولفه‌های این بعد شامل آماده‌سازی (قبل از حادثه)، خدمت‌رسانی(حین وقوع حادثه) و بازیابی عملکرد شبکه(پس از وقوع حادثه) می‌باشد. بعد دیگر این مدل دامنه‌هایی است که از مفهوم تاب‌آوری اقتباس شده است و مولفه‌های آن شامل قابلیت اطمینان، امنیت و کارایی است. این مدل در واقع ماتریسی است که ستون‌های آن مولفه‌های مبتنی بر زمان وقوع حادثه و سطرهای آن مولفه‌های مبتنی بر مفهوم تاب‌آوری است و نهایتا اینکه مولفه‌های این ماتریس شامل شاخص‌هایی قابل اندازه‌گیری از وضعیت تاب‌آوری شبکه و سرویس‌دهی به تعداد ۲۴ مورد می‌باشد.

وزارت امنیت داخلی ایالات متحده در سال ۲۰۱۶، در قالب سندی با عنوان بررسی تاب‌آوری سایبری(دستورالعمل،۲۰۱۶)، به توضیح و بررسی شاخص‌های کنترلی تاب‌آوری سایبری در زیرساخت‌های حیاتی سایبری پرداخته است. این شاخص‌ها و زیر مجموعه آنها که در این سند به تفسیر مورد بررسی قرار گرفته، شامل: مدیریت دارایی‌ها، مدیریت کنترل، پیکربندی و مدیریت کنترل، مدیریت آسیب‌پذیری، مدیریت حوادث، مدیریت تداوم خدمات، مدیریت ریسک، مدیریت وابستگی‌های خارج از سازمان، آموزش و آگاهی رسانی و آگاهی وضعیتی می باشد.

دی بورا و همکاران طی سه مرحله در سال‌های ۲۰۱۱ و ۲۰۱۵ و ۲۰۱۸ در قالب اسنادی با عنوان مهندسی تاب‌آوری سایبری(ماریوس،۲۰۱۶)، نسبت به تعریف و بروزرسانی چارچوب تاب‌آوری سایبری شرکت MITRE پرداخته و اطلاعاتی در خصوص مهندسی سیستم و معماری آن جهت اعمال تکنیک‌های تاب‌آوری سایبری ارائه نموده‌اند. بویژه در سند اخیر به شناسایی هم‌افزایی، تضاد و وابستگی‌های تکنیک‌های تاب‌آوری سایبری پرداخته شده است. در این سند تاب‌آوری سایبری با فرض وجود یک مهاجم مخفی، پایدار و پیشرفته که ممکن است اجزای یک سیستم را به خطر انداخته و جای پایی در سیستم‌های

سازمان ایجاد کند، مورد بررسی قرار گرفته و آرمان‌ها (پیش‌بینی، تحمل، بازیابی و تکامل)، اهداف(درک، آماده‌سازی، اجتناب/جلوگیری، ادامه دادن، محدودسازی، بازسازی، تبدیل و معماری مجدد) و تکنیک‌های تاب‌آوری سایبری(پاسخ تطبیقی، نظارت تحلیلی، دفاع هماهنگ، فریب، تنوع، موقعیت‌یابی پویا، نماینده پویا، عدم ماندگاری، محدودیت امتیاز، تنظیم مجدد، افزونگی، تقسیم‌بندی/کنارگذاری، تمامیت اساسی و غیر قابل پیش‌بینی بودن) مورد بررسی قرار گرفته است.

الکساندر الکسیف و همکاران در سال ۲۰۱۸ در قالب کارگاهی با عنوان تاب‌آوری سایبری در محیط‌های نظامی(الکساندر،۲۰۱۷)، علم تاب‌آوری سایبری را یک فعالیت سیستماتیک برای بدست آوردن و سازماندهی دانش به منظور تفسیر قابل آزمون و پیش‌بینی توانایی یک سیستم سایبری برای بازیابی خودکار و قابل اطمینان از حوادث یا وضعیت‌هایی که باعث می‌شود سیستم خارج از اهداف و ماموریت تعریف شده به لحاظ امنیتی و عملیاتی یا محدودیت‌های موقت فعالیت کند، تعریف می‌کند. در این گزارش علاوه بر معیار تحمل خطا، معیارهای اضافی شامل جامع بودن، قابل فهم بودن، امکان پذیر بودن، منحصر بفرد بودن، سادگی، دقت، بموقع بودن و تکرارپذیری به عنوان شاخص‌های ارزیابی تاب‌آوری سایبری یک سیستم معرفی شده است. همچنین بر اهمیت عنصر زمان در میدان نبرد شامل، مدت زمان صرف شده برای تشخیص تخریب، مدت زمان بازیابی و مدت زمان کارکرد سیستم خارج از اهداف و ماموریت تعریف شده، تاکید شده است.

وزارت امنیت داخلی ایالات متحده (دستورالعمل،۲۰۱۸) در سال ۲۰۱۸ با همکاری تیم تاب‌آوری و واکنش سایبری، پژوهشی را در راستای تاب‌آوری زیرساخت‌های حیاتی از جمله حوزه‌های حمل و نقل، انرژی، نرم‌افزارهای رایانه‌ای و ... انجام داده و در گزارش آن تاب–آوری سایبری را دارای چهار ویژگی اصلی، سازگاری، آماده‌سازی، تحمل و بازیابی معرفی می‌کند. در این گزارش تاب‌آوری در فضای سایبر به معنی توانایی سازگاری با شرایط متغیر و آماده‌سازی، تحمل در برابر و بازیابی سریع از اختلال تعریف شده است.

سازمان پیمان آتلانتیک شمالی ناتو در سال ۲۰۱۸ در قالب سندی با عنوان رهیافت تقویت تاب‌آوری سایبری (آلکساندر،۲۰۱۸) که توسط لابراتوار تحقیقات ارتش ایالات متحده منتشر گردیده، تاب‌آوری را به معنی توانایی بازیابی از یا سهولت تعدیل مشکلات و تغییرات بیان نموده و عنوان می‌کند که تاب‌آوری شامل چهار توانایی: برنامه‌ریزی/آماده سازی، جذب، بازیابی و سازگاری با تهدیدات شناخته شده و ناشناخته است. در این سند نیز تاب‌آوری را به توانایی سیستم در بازیابی یا بازآفرینی عملکرد خود به سطح کافی پس از تخریب غیر منتظره عملکرد آن در اثر یک رویداد بیان می‌کند.

ایگور لینکوف و الکساندر کوت [12] در سال ۲۰۱۹، تاب‌آوری سایبری را به توانایی سیستم در بازیابی عملکرد خود پس از حمله سایبری تعریف می‌کنند. بعبارت دیگر هرگاه دو

سیستم A وB با عملکرد و سطوح حمله یکسان تحت تاثیر یک حمله سایبری قرار گیرند، تاب‌آوری سایبری سیستم A بیشتر است اگر پس از سپری شدن یک دوره زمانی مشخص T، سیستم A بتواند به سطح عملکردی بالاتری از سیستم B خود را بازیابی نماید. آنها همچنین معتقدند که مفهوم تاب‌آوری اغلب با مفاهیمی نظیر ریسک، امنیت و استحکام آمیخته شده است. آنها با استناد به فرهنگ لغات آکسفورد، تاب‌آوری را " ظرفیت بازیابی سریع از مشکلات " بیان می‌کنند و بر فاکتور سرعت در تعریف تاب‌آوری تاکید دارند.

شاخص تاب‌آوری جهانی (دستورالعمل،۲۰۱۹) در سال ۲۰۱۹ به رتبه بندی تاب‌آوری ۱۳۰ کشور بر اساس اطلاعات بدست آمده از بانک جهانی، مجمع جهانی اقتصاد، اتحادیه بین‌المللی مخابرات و ... پرداخته و در آن تاب‌آوری دارای سه بعد و دوازده مولفه می‌باشد که عبارتند از: بعد اقتصادی (شامل مولفه‌های بهره وری اقتصادی، ریسک سیاسی، وابستگی اقتصادی به نفت و نرخ شهرنشینی)، بعد کیفیت ریسک(شامل مولفه‌های ریسک قرار گرفتن در معرض بلایای طبیعی، کیفیت مدیریت ریسک بلایا، کیفیت مدیریت ریسک آتش سوزی و ریسک سایبری) و بعد زنجیره تأمین (شامل مولفه‌های کنترل فساد، زیرساخت، کیفیت عرضه کنندگان داخلی و ثبات زنجیره تأمین).

موسسه ملی استاندارد و فناوری ایالات متحده در سال ۲۰۱۹، استانداردی را با عنوان توسعه سامانه‌های تاب‌آور سایبری (دستورالعمل،۲۰۱۹) منتشر نموده که در این استاندارد کلیه آرمان‌ها، اهداف و تکنیک‌های تاب‌آوری سایبری بر مبنای اصول مدیریت ریسک و راهبردهای مرتبط با آن پایه‌گذاری شده و با تعریف آرمان‌ها(پیش‌بینی، تحمل، بازیابی و سازگاری) و اهداف(جلوگیری، آمادگی، ادامه دادن، محدودسازی، بازسازی، درک، تبدیل و معماری مجدد) و نهایتا تکنیک‌هایی که این اهداف و آرمان‌ها را محقق خواهند ساخت، به تفسیر و بررسی سامانه‌های تاب‌آور پرداخته است.

روش‌شناسی پژوهش

این پژوهش با توجه به اینکه شاخص‌هایی را به منظور بررسی تاب‌آوری سایبری لجستیک و زنجیره تامین نیروهای مسلح ارائه می‌نماید که می‌تواند در ارتقاء آن موثر باشد و نیز به عنوان ابزار و راهنمایی برای خط مشی‌گذاری در حوزه تاب‌آوری سایبری عمل نماید، کاربردی است و با توجه به ارائه چارچوب و توسعه دانش در این زمینه، توسعه‌ای محسوب می‌شود. بنابراین، این پژوهش با توجه به موضوع و هدف تحقیق، از نوع کاربردی- توسعه‌ای است و روش تحقیق به کار گرفته شده در این پژوهش، روش آمیخته است.

همچنین این پژوهش در سه گام به مرحله اجراء درآمده است. در ابتدا با توجه به تعدد اسناد و مدارک مرتبط در بخش مطالعات کتابخانه‌ای با استفاده از روش تحلیل محتوای کیفی، ابعاد و مولفه‌های تاب‌آوری سایبری احصاء گردید. پس از آن با استفاده از تکنیک دلفی ابعاد بدست آمده در مرحله اول، با اجماع نظر خبرگان اصلاح و تکمیل گردیدند و در

ادامه به منظور نهایی نمودن مدل ارائه شده، پرسشنامه‌ای محقق ساخته، تهیه و با اخذ نظرات کارشناسان حوزه امنیت و تاب‌آوری سایبری، صحت آن مورد تایید قرار گرفت. هر یک از گام‌های سه گانه روش‌های تحقیق در این پژوهش بشرح ذیل می‌باشد.

۱- تحلیل محتوای کیفی: در این پژوهش به تحلیل محتوای کیفی مقالات علمی و پژوهشی و اسناد منتشر شده توسط سازمان‌های معتبر بین‌المللی پرداخته شد و با تکنیک خوشه بندی، کلید واژه‌های موثر در تاب‌آوری سایبری استخراج شدند و بر اساس فراوانی کلیدواژه‌ها، ابعاد و مولفه‌های اصلی تاب‌آوری سایبری مورد بازشناسی قرار گرفتند.

۲- تکنیک دلفی: در این مرحله با استفاده از روش دلفی، ابعاد بازشناسی شده در گام اول برای طراحی مدل مفهومی تاب‌آوری سایبری با اجماع نظر خبرگان اصلاح گردیدند. جمعیت نمونه تکنیک دلفی در این پژوهش، پانزده نفر از جامعه آماری اساتید و اعضای گروه مطالعاتی، متخصصین حوزه امنیت فضای سایبر، پژوهشگران، مدیران و متصدیان اجرایی در حوزه فناوری اطلاعات و فضای سایبری کشور هستند که با استفاده از روش نمونه گیری قضاوتی انتخاب گردیدند.

۳- پرسشنامه باز: در گام سوم، پرسشنامه‌ای شامل سوالات باز به منظور ارزیابی چارچوب ارائه شده تهیه گردید و با توجه به جامعه آماری دوم که به صورت تمام شمار ۲۳ نفر از متخصصین امنیت فضای سایبر بودند، صحت مدل مورد تأیید قرار گرفت.

یافته‌های پژوهش

در این مرحله، با تجزیه وتحلیل مفاهیم تاب‌آوری و تاب‌آوری سایبری و همچنین بررسی اسناد، ادبیات تحقیق، مطالعات تطبیقی و مقالات علمی و پژوهشی، ابعاد و مولفه‌های تاب-آوری سایبری لجستیک و زنجیره تامین دفاعی را شناسایی و ارائه خواهیم نمود.

ابعاد تاب‌آوری سایبری؛ با تحلیل محتوای مفهوم تاب‌آوری و نیز تاب‌آوری سایبری و همچنین بررسی اسناد، ادبیات تحقیق و مقالات علمی و پژوهشی با استخراج کلید واژه‌های مهم این تعاریف مبتنی بر تکنیک خوشه‌بندی و دریافت اجماع نظر خبرگان درباره این کلیدواژه‌ها از طریق تکنیک دلفی و با استناد به ماهیت دفاعی این تحقیق، ترکیبی از ابعاد دکترین جنگ شبکه محور و تعریف ارائه شده از تاب‌آوری می‌تواند برای توسعه ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره دفاعی مورد استفاده قرار گیرد.

بر این اساس چهار مرحله از چرخه مدیریت رویداد تاب‌آوری با افزودن بعد " کشف" به سایر ابعاد متداول تاب‌آوری سایبری مطابق با مندرجات جدول شماره ۱ مورد تایید قرار گرفت که این بعد اخیر، ازچارچوب امنیت سایبری موسسه ملی استاندارد و فناوری، اقتباس و دلیل آن رفع نقاط ضعف درک شده از چارچوب‌های مطالعه شده بر اساس نتایج جلسات خبرگان در پنل دلفی با توجه به ماهیت دفاعی این تحقیق بوده است. چرا که زمان عنصر کلیدی در میدان نبرد است و لذا یک اقدام اساسی برای تاب‌آوری آن خواهد بود و مدت

زمان صرف شده برای تشخیص یک رویداد یا حمله، می‌تواند بر سرعت بازیابی و عملکرد سامانه در خارج از اهداف تعیین شده، تاثیرگذار باشد.

همچنین چهار حوزه دکترین جنگ شبکه محور شامل فیزیکی(منابع فیزیکی، قابلیت‌ها و طراحی آن منابع)، اطلاعاتی (توسعه اطلاعات و اطلاعات حوزه فیزیکی)، شناختی(استفاده از اطلاعات و حوزه‌های فیزیکی برای تصمیم‌گیری) و اجتماعی (ساختار و سازمان و ارتباطات برای تصمیم‌گیری‌های شناختی)، مورد بررسی قرار گرفت و نهایتا با استفاده از تعاریف فوق و ایجاد یک ماتریس عمومی از معیارها و ارزیابی پیامدهای آنها در طول مراحل و حوزه‌های مختلف، ابعاد تاب‌آوری سایبری لجستیک و زنجیره تامین استخراج گردید.

جدول شماره ۱. ابعاد تاب‌آوری سایبری

ابعاد	تعریف
برنامه‌ریزی/ آماده‌سازی	در اختیار داشتن توان لازم برای دسترسی به خدمات و دارایی‌ها در طول یک رویداد مخرب.
کشف	شناسایی فوری حمله یا نقص و شروع اجرای مراحل مهار.
جذب	حفظ مهمترین عملکرد، دارایی‌ها و خدمات، حین دفع یا جداسازی رویداد.
بازیابی	بازگرداندن عملکردهای دارایی‌ها و در دسترس بودن خدمات مطابق با وضعیت قبل از وقوع رویداد.
سازگاری	دستیابی به تاب‌آوری بیشتر با استفاده از اطلاعات رویدادها، تغییر پروتکل‌ها، پیکربندی مجدد سامانه‌ها، آموزش کارکنان.

مولفه‌های تاب‌آوری سایبری؛ به منظور استخراج مولفه‌های تاب‌آوری سایبری، مضامین مرتبط با تاب‌آوری سایبری، با مطالعه ادبیات پژوهش و تحلیل کیفی اسناد موجود صورت پذیرفت و سپس با تکنیک خوشه‌بندی و بر اساس فراوانی تکرار واژه‌ها، مولفه‌های اصلی مورد بازشناسی اولیه قرار گرفتند و این مولفه‌ها از طریق تکنیک دلفی با اجماع نظر خبرگان اصلاح گردیدند که نتایج در جدول شماره ۲ ارائه گردیده است

جدول شماره ۲: ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی

ابعاد	فیزیکی	اطلاعاتی	شناختی	اجتماعی
برنامه‌ریزی/ آماده‌سازی	۱- بکارگیری تجهیزات کنترلی/ حساسه‌ها در دارایی‌های حیاتی ۲- ارزیابی ساختار شبکه و ارتباط اجزاء سامانه با محیط ۳-افزونگی زیرساخت‌های فیزیکی حیاتی ۴- افزونگی داده‌ها بصورت فیزیکی و منطقی در مکانی خارج از شبکه.	۱- طبقه‌بندی دارایی‌ها و خدمات بر اساس حساسیت یا تاب‌آوری ۲- مستندسازی گواهینامه‌ها، مدارک ارائه‌دهندگان سخت‌افزار و یا نرم‌افزارهای حیاتی ۳- تهیه برنامه‌هایی برای ذخیره‌سازی و محدودسازی دسترسی به اطلاعات طبقه‌بندی شده یا حساس ۴- تعیین میزان وابستگی‌ها به سامانه‌های داخلی و خارجی.	۱- پیش‌بینی و برنامه‌ریزی برای شرایط و رویدادهای سامانه ۲- درک اولویت اهداف سازمانی ۳- استفاده از بازی جنگ سایبری مبتنی بر سناریو.	۱- شناسایی و هماهنگی با اشخاص خارجی که ممکن است تحت تأثیر حملات سایبری داخلی قرار بگیرند یا تحت تأثیر قرار دهند (ایجاد نقطه تماس) ۲- تربیت و آموزش کارکنان در مورد تاب‌آوری و برنامه تاب‌آوری سازمان ۳- واگذاری مسئولیت دارایی‌ها و خدمات به کارکنان خاص ۴- آماده‌سازی و ایجاد ارتباطات تاب‌آور ۵- اشاعه فرهنگ سایبری آگاهانه.
کشف	۱- نظارت بر محیط فیزیکی جهت شناسایی وقایع احتمالی امنیت سایبری ۲-نظارت بر فعالیت کارکنان برای شناسایی وقایع احتمالی امنیت سایبری.	۱- شناسایی کد مخرب و غیر مجاز ۲- نظارت بر فعالیت ارائه دهنده خدمات خارجی برای شناسایی وقایع احتمالی امنیت سایبری.	۱- تحلیل رویدادهای شناسایی شده را برای درک اهداف حمله و روشها ۲- بررسی ارتباط و همبستگی داده‌های رویداد از منابع و سنسورهای مختلف ۳- تعیین تأثیر حوادث و آستانه هشدار.	۱- تعیین نقش‌ها و مسئولیت‌های کشف برای اطمینان از پاسخگویی مناسب ۲- ابلاغ اطلاعات تشخیص رویدادها به طرفهای ذیربط ۳- بهبودبخشی مداوم فرآیندهای تشخیص.

جذب	۱- ایجاد مصالحه بین دارایی‌ها و خدمات ۲- افزونگی دارایی‌ها برای تداوم خدمت‌رسانی و انجام ماموریت ۳- اختصاص منابع سایبری برای دفاع در برابر حملات سایبری.	۱- دیده‌بانی اطلاعات سنسورهای خدمت‌رسانی و دارایی‌های مهم ۲- انتقال مؤثر و کارآمد داده‌های مرتبط به ذینفعان/ تصمیم گیرندگان مسئول.	۱- استفاده از پروتکل‌های تصمیم- گیری یا ابزارهای کمکی برای تعیین زمان قطعی رویداد ۲- توانایی ارزیابی عملکرد برای تعیین اینکه آیا ماموریت ادامه دارد یا خیر ۳- تمرکز تلاش‌ها بر روی دارایی‌ها و خدمات حیاتی شناسایی شده.	۱- آشنایی و ارتباط‌گیری با کارشناسان مشخص شده و کارکنان مسئول تاب‌آوری.
بازیابی	۱- بررسی و ترمیم تجهیزات کنترلی و حساسه‌های معیوب ۲- ارزیابی خسارت خدمات/ دارایی‌ها ۳- ارزیابی فاصله تا بهبود عملکرد ۴- جداسازی و دورریزی دارایی‌های ترمیم‌ناپذیر بصورت ایمن.	۱- ثبت رویدادها و اطلاعات سنسورها را در طول رویداد ۲- بررسی و مقایسه سامانه‌ها قبل و بعد از رویداد.	۱- مرور نکات مهم نقص فیزیکی و اطلاعاتی به منظور تصمیم‌گیری آگاهانه ۲- ایجاد پروتکل‌های تصمیم‌گیری یا کمکی برای انتخاب گزینه‌های بازیابی.	۱- پیروی از یک برنامه ارتباط‌گیری تاب‌آوری ۲- ایجاد تعهد برای سازمان جهت تاب‌آور نمودن سامانه‌ها.
سازگاری	۱- بررسی پیکربندی دارایی‌ها و خدمات در پاسخ به رویداد اخیر ۲- خارج نمودن دارایی‌های منسوخ و معرفی دارایی‌های جدید.	۱- مستندسازی پیامدها و علت رویداد سایبری ۲- ثبت زمان بین بروز مشکل و کشف/ کشف و بازیابی ۳- پیش بینی بهبود وضعیت سامانه‌ها در آینده ۴- مستندسازی نقطه ورود حمله.	۱- مرور مدیریت پاسخ‌دهی و فرآیندهای تصمیم گیری ۲- تعیین انگیزه‌های بروز رویداد (حمله).	۱- ارزیابی پاسخ‌دهی کارکنان به رویداد به منظور تعیین آمادگی و اثربخشی ارتباطات ۲- حساس نمودن کارکنان به مناطق کلیدی که قبلاً نادیده گرفته شده ۳- اطلاع‌رسانی و اشتراک‌گذاری به سازمان در مورد آخرین تهدیدات و روش‌های محافظت.

بحث و نتیجه‌گیری

ابعاد و مولفه‌های تاب‌آوری سایبری لجستیک و زنجیره تامین دفاعی پس از مطالعه و بررسی شاخص‌های جهانی، مقالات علمی و پژوهشی و اسناد موسسات بین‌المللی و نیز از طریق مراجعه به آرای خبرگان در حوزه‌های راهبردی و امنیتی فضای سایبر، به طور منطقی و مفهومی استنباط گردید و با تجزیه و تحلیل مفاهیم و مضامین به دست آمده و ارتباط و تاثیر و تاثر آنها با یکدیگر و با در نظر گرفتن مقتضیات و زیست بوم فضای سایبر در حوزه دفاعی کشور به صورت مدلی متشکل از ابعاد ومولفه‌ها با استفاده از روش پژوهش آمیخته استخراج گردید. مهم‌ترین محورهایی که می‌توان از نتایج این پژوهش برشمرد عبارتند از:

- شناسایی و تبیین ابعاد و مولفه‌های تاب‌آوری لجستیک و زنجیره تامین دفاعی
- تولید ادبیات در حوزه تاب‌آوری لجستیک و زنجیره دفاعی
- ایجاد و فراهم نمودن وفاق در فرآیند تصمیم سازی و تصمیم گیری مابین دستگاه های مسئول در این حوزه.
- تقویت و ارتقاء تفکر راهبردی در حوزه تاب‌آوری لجستیک و زنجیره تامین دفاعی
- فراهم آوردن زمینه لازم برای مواجهه هوشمندانه و مقتدرانه با تهدیدات روزافزون فضای سایبر
- بی‌نیاز نمودن دستگاه‌های مسئول تاب‌آوری لجستیک و زنجیره تامین دفاعی از مراجعه به الگوهای غیر بومی.

با توجه به تبیین ابعاد و مولفه‌های تاب‌آوری لجستیک و زنجیره تامین دفاعی در این تحقیق، شایسته است:

- با مقایسه وضعیت موجود تاب‌آوری لجستیک و زنجیره تامین دفاعی در کشور با مدل ارائه شده، پیشنهاد می‌گردد با ایجاد مراکز اشتراک و تحلیل اطلاعات نسبت به افزایش تاب‌آوری لجستیک و زنجیره تامین دفاعی اقدام لازم صورت پذیرد.
- با توجه به وضعیت نظام جمهوری اسلامی ایران ونیروهای مسلح در تقابل دائمی با استکبار جهانی و نظام سلطه، تسریع در ارتقاء تاب‌آوری لجستیک و زنجیره تامین دفاعی نیروهای مسلح که منجر به ارتقاء امنیت ملی می‌شود، پیشنهاد می‌گردد.
- دستگاه‌ها و نهادهایی که در حوزه تاب‌آوری لجستیک و زنجیره تامین دفاعی دارای مسئولیت هستند از نتایج این تحقیق استفاده نمایند.
- با ایجاد مراکز علمی و فناوری با مشارکت ذی نفعان مختلف و انجام تحقیقات در حوزه تاب‌آوری لجستیک و زنجیره تامین دفاعی، نسبت به ارتقاء تاب‌آوری سایبری جمهوری اسلامی ایران اقدام لازم صورت پذیرد.
- در تحقیقات آتی مرتبط با موضوع این پژوهش، پرداختن به شاخص‌های ارزیابی تاب‌آوری سایبری حوزه دفاعی می‌تواند افق وسیع‌تری در ادامه این پژوهش بگشاید.

منابع

صدیق پور، ۱۳۹۶، عبدالرضا، طراحی و تبیین مدل زنجیره تامین تاب آور در صنعت داروسازی ایران، *فصلنامه علمی – پژوهشی مطالعات مدیریت صنعتی*، ۱۶(۵۱)، ۵۵-۱۰۶

Department of Defence, DOD Digital Modernization Strategy,2019.

Igor Linkov(2013), Resilience metrics for cyber systems.

European Network and Information Security Agency (ENISA), Measurement Frameworks and Metrics for Resilient Networks and Services - Technical report, 2011.

Department of Homeland Security(DHS), Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide,2016.

Marios P. Efthymiopoulos, NATO Smart Defense and Cyber Resilience, 2016.

World Economic Forum, A Framework for Assessing Cyber Resilience, 2016.

Deborah Bodeau, Cyber Resiliency Engineering Aid the Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, 2015.

Alexander Alexeev(2017). Constructing a Science of Cyber-Resilience for Military Systems,.

U.S. Department of Homeland Security(DHS), Cyber Resilience and Response, 2018.

Alexander Kott, Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153, 2018.

Alexander Kott, Igor Linkov(2019), Cyber Resilience of Systems and Networks, 2019.

FM Global, Resilience Index Annual Report, NIST SP800- 160, 2019