دریافت مقاله: ۱۴۰۰/۰۸/۰۷
پذیرش مقاله: ۱۴۰۰/۱۲/۲۳
مقاله پژوهشی

فصلنامهٔ مدیریت نظامی
سال بیست و دوم، شمارهٔ۱، بهار ۱۴۰۱
ص‌ص ۱۲۵-۱۵۸

ارائه الگوی مفهومی تسلیحات سایبری

هانی رحیم‌اف [۱*] و محمدرضا موحدی‌صفت [۲]

چکیده

با وابستگی انسان به فناوری اطلاعات، شکل نوینی از جنگ با عنوان جنگ سایبری ظهور پیداکرده است. در عصر اطلاعات و ارتباطات، تسلیحات سایبری از ارکان اصلی جنگ سایبری محسوب شده و جزء موضوعات راهبردی دولت‌ها شمرده می‌شود. توانایی تولید، توسعه و بکارگیری این تسلیحات باعث ارتقاء قدرت دفاعی کشور در فضای سایبر شده و افزایش قدرت ملی را در پی خواهد داشت. امکان بکارگیری تسلیحات سایبری علیه زیرساخت حیاتی، حساس و مهم سبب شده است که متولیان حوزه دفاعی تلاش نمایند تا با استفاده از آخرین دستاوردهای فناوری، به این عرصه نوین ورود نموده و بیش‌ازپیش بازدارندگی سایبری را محقق سازند. بر این اساس، مقاله حاضر با رویکرد آمیخته (کمی و کیفی) و روش تحقیق تحلیل محتوا و عقلایی، با مطالعه و پژوهش پیشینه تحقیق، به بررسی تسلیحات سایبری در سطح راهبردی پرداخته و با استفاده از نظرات ۷۹ نفر از فرماندهان، مدیران و کارشناسان سطوح راهبردی، عملیاتی و تاکتیکی دفاع سایبری کشور، الگوی مفهومی تسلیحات سایبری را به‌صورت اکتشافی ارائه نموده است. در این تحقیق، طی مصاحبه عمیق با خبرگان، سه مفهوم کارایی، هوشمندی و گمنامی تسلیحات سایبری به‌مثابه ابعاد راهبردی الگو، شناسایی گردیده و پس از استخراج مؤلفه‌های هر بعد، شاخص‌های هر مؤلفه تعیین‌شده است. سپس با تجزیه‌وتحلیل آماری نتایج پرسشنامه، الگوی مفهومی تسلیحات سایبری در سه بعد، نه مؤلفه و چهل‌وچهار شاخص ارائه‌شده است.

واژه‌های کلیدی: سلاح سایبری، تسلیحات نوین، عملیات سایبری، الگوی مفهومی

---

۱. دانشجوی دکترای رشته مدیریت راهبردی فضای سایبر گرایش امنیت سایبری، دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران؛ (* نویسنده مسئول h.rahimov98@sndu.ac.ir)

۲. استادیار دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران؛ movahedi@sndu.ac.ir

مقدمه

امروزه، عرصه تسلیحات سایبری به رقابتی بین دولت‌ها تبدیل‌شده است. آن‌ها تلاش می‌کنند با تولید و توسعه این تسلیحات، قدرت سایبری و به‌تبع آن قدرت ملی خود را افزایش دهند. مقام معظم رهبری در حکم اعضای شورای عالی فضای مجازی، قدرت سایبری را حائز اهمیت دانسته و خاطرنشان کرده‌اند که: "یکی از وظایف و مأموریت‌های این شورا، ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی است." (مقام معظم رهبری, ۱۳۹۴) بر اساس (Mezzour et al., 2018, p. 9) قدرت‌های سیاسی و نظامی حاضر دنیا، تلاش نموده‌اند تا در عرصه تولید و توسعه تسلیحات سایبری از سایر کشورها پیشی بگیرند و در این راستا به موفقیت نیز دست‌یافته‌اند.

افزایش قدرت سایبری جمهوری اسلامی ایران، ایجاد بازدارندگی سایبری و انجام دفاع مشروع؛ یکی از مسائلی است که بخشی از آن با پژوهش و دستیابی به تسلیحات سایبری بروز و کارآمد میسر است. در این راستا، محققین اقدام به ارائه الگوی مفهومی تسلیحات سایبری و تعیین ابعاد، مؤلفه‌ها و شاخص‌های قابل‌اندازه‌گیری این تسلیحات نموده‌اند تا با بکارگیری چارچوب حاصل‌شده از پژوهش، بتوان گامی در جهت اعتلای قدرت سایبری جمهوری اسلامی ایران برداشت.

در عصر حاضر، ماهیت بسیاری از جنگ‌ها از حوزه فیزیکی بـه سایبری تغییریافته و حملات سایبری از طریق این فضا بـه زیرساخت‌های مهم کشورها صورت می‌پذیرد. وقایع و حوادث سایبری سال‌های اخیر کشور نیز مؤید این واقعیت است که کثرت عملیات سایبری علیه کشور به‌ویژه در زیرساخت‌های حیاتی، جمهوری اسلامی ایران را به یکی از قربانیان اصلی فضای سایبر تبدیل نموده است. عملیات سایبری از ابعاد گوناگونی تشکیل‌شده است که یکی از آن‌ها تسلیحات سایبری است.(Leuprecht et al., 2019, p. 5) بدلیل درآمدزا بودن تولید تسلیحات سایبری، علاوه بر دولت‌ها، بخش خصوصی نیز اقدام به تولید و توسعه تسلیحات سایبری نموده است. بر اساس آخرین گزارش موسسه تحقیقاتی Zion در زمینه بازار تسلیحات سایبری، بازار جهانی این تسلیحات در سال ۲۰۲۰ بالغ بر ۴۸۰,۵ میلیارد دلار بوده و پیش‌بینی می‌شود این رقم تا سال ۲۰۲۸ به ۷۰۱,۸ میلیارد دلار برسد. بر این اساس، بازار جهانی تسلیحات سایبری رشدی حدود ۴,۹ درصدی را بین سال‌های ۲۰۲۱ تا ۲۰۲۸ تجربه خواهد نمود. در این مطالعه، مناطق جغرافیایی آسیا و اقیانوسیه ، خاورمیانه و آفریقا ، آمریکای شمالی ، اروپا و آمریکای

لاتین به تفکیک موردبررسی قرارگرفته است. بر اساس نتایج حاصل‌شده از این تحقیق، منطقه آمریکای شمالی، بازار جهانی تسلیحات سایبری را هدایت می‌کند و پیش‌بینی می‌شود در سال‌های آینده نیز این موقعیت را حفظ نماید. علت این امر وجود تعداد زیادی از فعالان بازار تسلیحات سایبری مستقر در آمریکای شمالی است؛ بعلاوه در این منطقه استفاده گسترده‌ای از تسلیحات سایبری در بخش‌های هوافضا، دفاع و سرویس‌های اطلاعاتی صورت می‌پذیرد (Zion Market Research, 2021) .

با توجه به رابطه‌ای که بین دولت آمریکا و جمهوری اسلامی ایران حاکم است؛ این آمارها نشانگر وجود تهدید جهت تولید و بکارگیری تسلیحات سایبری علیه کشور است. با ارائه الگوی مفهومی تسلیحات سایبری، پرداختن به ادبیات و پیشینه این حوزه و مشخص نمودن ابعاد و مؤلفه‌های راهبردی تسلیحات سایبری، نگرشی جامع و همه‌جانبه برای متولیان دفاع سایبری جمهوری اسلامی ایران ایجادشده و با توجه به تأثیر راهبردی عملیات سایبری بر امنیت ملی، از مشکل غافلگیری راهبردی در خصوص این بعد عملیات سایبری —یعنی تسلیحات سایبری- جلوگیری می‌گردد.

درآمد هنگفت مالی تسلیحات سایبری باعث شده است تا شرکت‌های امنیتی متعددی شکل‌گرفته و به‌صورت مستمر اقدام به کشف این تسلیحات نمایند. بر اساس گزارش[۱]ENISA که از ژانویه ۲۰۱۹ تا آوریل ۲۰۲۰ سراسر دنیا را موردبررسی قرار داده است؛ روزانه ۲۳۰ هزار بدافزار جدید کشف‌شده که ۶۷ درصد آن‌ها از طریق ارتباطات رمزنگاری‌شده تحت وب[۲] انتقال‌یافته‌اند. در ۷۱ درصد سازمان‌ها، بدافزار از طریق یکی از کارکنان خود آن‌ها منتشر و به سایرین سرایت کرده و ۸۴ درصد حملات سایبری بر اساس مهندسی اجتماعی شکل‌گرفته است. بیشترین دارایی موردتوجه نفوذگران نیز به ترتیب شامل اطلاعات صنعتی و داده‌های محرمانه تجاری، اطلاعات محرمانه دولتی و نظامی، اطلاعات سرورهای زیرساخت، اطلاعات احراز هویت و اطلاعات مالی مانند کارت اعتباری و حساب بانکی بوده است. (Enisa, 2020, pp. 9–15) با استفاده از شاخص‌های الگوی مفهومی تسلیحات سایبری، حوزه دفاع سایبری جمهوری اسلامی ایران خواهد توانست جنبه‌های مختلف تسلیحات سایبری را بررسی نموده و

۱. European Union Agency For Cybersecurity

۲. HTTPS

علاوه بر مرتفع نمودن مشکل نگرش همه‌جانبه متولیان حوزه دفاعی جمهوری اسلامی ایران به موضوع تحقیق، از آن در جهت شناسایی بهتر این تسلیحات نیز استفاده نماید.

بر اساس موارد بیان‌شده، این پژوهش به دنبال پاسخ به سؤال اصلی "الگوی مفهومی تسلیحات سایبری چیست؟"جهت دستیابی به هدف "الگوی مفهومی تسلیحات سایبری" می‌باشد و در این مسیر از نظرات و تجربیات خبرگان حوزه تحقیق بهره‌مند شده است.

مبانی نظری

فرهنگ لغت آکسفورد کلمه سلاح را به‌عنوان "وسیله‌ای که برای ایجاد خطر فیزیکی یا آسیب جسمی طراحی یا استفاده‌شده است" تعریف می‌کند (Oxford University Press, 2021) توماس رید و پیتر مک برنی در (Rid & McBurney, 2012, p. 2) تسلیحات سایبری را چنین تعریف می‌کنند که: "سلاح سایبری یک کد رایانه‌ای است که باهدف تهدید یا ایجاد صدمه فیزیکی، عملکردی یا روحی به سازه‌ها، سیستم‌ها یا موجودات زنده مورداستفاده قرار می‌گیرد. " کتاب راهنمای تالین، تسلیحات سایبری را یکی از ابزارهای سایبری جنگ که قادر به آسیب رساندن به افراد یا مرگ آن‌ها یا آسیب رساندن به اشیا یا تخریب آن‌ها می‌باشد؛ بیان می‌دارد.(Schmitt, 2013, pp. 141–142) کتاب موسسه East-West بنام مبانی اصطلاحات حیاتی دوجانبه روسیه و آمریکا در امنیت سایبری، تسلیحات سایبری را چنین تعریف می‌کند که: " نرم‌افزار ، میان‌افزار یا سخت‌افزاری که برای آسیب رساندن به قلمرو سایبر طراحی یا اعمال می‌شود." (Godwin III et al., 2014, p. 56) مقاله (Maathuis et al., 2016, p. 4) سلاح سایبری را چنین تعریف می‌کند که:" سلاح سایبری، یک برنامه کامپیوتری برای ایجاد تغییر یا آسیب رساندن (به یک جز ICT) به سیستم جهت دستیابی به اهداف (نظامی) در برابر دشمنان داخل و/یا خارج از فضای سایبری است." مقاله (Bellovin et al., 2017, p. 267) نیز سلاح سایبری را چنین تعریف نموده است:" سلاح سایبری، یک مصنوع یا ابزار نرم‌افزاری مبتنی بر فناوری اطلاعات است که می‌تواند اثرات مخرب ، آسیب‌زا یا کاهش دسترسی را بر روی سیستم یا شبکه‌ای که علیه آن هدایت می‌شود ایجاد کند. " ازآنجاکه هدف اصلی تسلیحات جاسوسی، جمع‌آوری داده و اطلاعات بوده و با تخریب، تغییر یا ایجاد آسیب فیزیکی فاصله دارد، در تعاریف بیان‌شده قرار نمی‌گیرند؛ لذا محقق در ذیل اقدام به تعریف عملیاتی سلاح سایبری نموده است. بر این اساس، سلاح سایبری ابزاری نرم‌افزاری است که جهت

دستیابی به اهداف مهاجم اقدام به جاسوسی، تخریب، تغییر یا ایجاد اختلال در اطلاعات یا سامانه‌های هدف می‌نماید."

تسلیحات سنتی و تسلیحات سایبری

اگر بین هزینه جنگ با تسلیحات سنتی و جنگ با تسلیحات سایبری مقایسه‌ای انجام شود؛ چنین می‌توان گفت که هزینه‌های تسلیحاتی و سکوهای مورداستفاده در حملات سنتی عبارتند از: مهمات ۰,۵ تا ۱۰ میلیون دلار، هواپیماها ۱۰۰ تا ۲۰۰ میلیون دلار، واحدهای زمینی ۰,۵ تا ۳ میلیون دلار و واحدهای دریایی ۰,۵ تا ۶ میلیارد دلار؛ اما ارزیابی هزینه‌های سلاح‌های سایبری دشوار است. به استثنای سلاح‌های اتمی، هزینه تحقیق و توسعه سلاح‌های سایبری بیشتر از سلاح‌های سنتی است ولی بسیاری از تسلیحات ساده سایبری تنها چند دلار هزینه‌دارند. با این وجود آسیب‌پذیری‌های روز صفرم بسیار گران‌قیمت می‌باشند. به‌طور مثال یک آسیب‌پذیری روز صفرم آیفون ممکن است بیش از ۲ میلیون دلار ارزش داشته باشد (Bates, 2020, p. 29).

از نظر طول عمر نیز می‌توان تسلیحات سایبری و سنتی را با یکدیگر مقایسه نمود. طول عمر سلاح‌های سنتی به شرایط نگهداری‌شان در آب و هواهای گوناگون، مصون ماندن از حملات دشمن یا از رده خارج نشدن به واسطه تغییر فناوری و ورود مدل‌های جدید بستگی دارد اما معمولاً دهه‌ها عمر می‌کنند. به‌عنوان‌مثال یک هواپیمای جنگنده عمر ۳۰-۴۰ ساله دارد و در ادامه نیز می‌توان از آن در رژه‌های نظامی و نمایش قدرت استفاده نمود. (M. Hypponen, 2019) تسلیحات سایبری مانند سلاح‌های سنتی طول عمر مشخصی دارند و پس‌ازآن کار نخواهند کرد؛ یا درنهایت استفاده محدودی خواهند داشت. به‌عنوان‌مثال، یک اکسپلویت روز صفرم برای سیستم‌عامل ویندوز سرانجام کشف و وصله خواهد شد یا در نسخه‌های جدیدتر کارایی خود را از دست خواهد داد. هزینه سرمایه‌گذاری در تسلیحات سایبری می‌تواند میلیون‌ها دلار باشد اما ناگهان از کار افتاده و از رده خارج می‌شود. مطالعه‌ای در مورد مدت حیات تسلیحات سایبری نشان داده است که میانگین چرخه حیات اکسپلویت-های روز صفرم و آسیب‌پذیری‌های اساسی ۶,۹ سال است. ۲۵٪ آسیب‌پذیری‌ها در کمتر از ۱,۵ سال کشف و وصله شده و ۲۵٪ نیز پس از ۹,۵ سال کماکان فعال هستند (L. Ablon and A. Bogart, 2017).

چرخه حیات تسلیحات سایبری

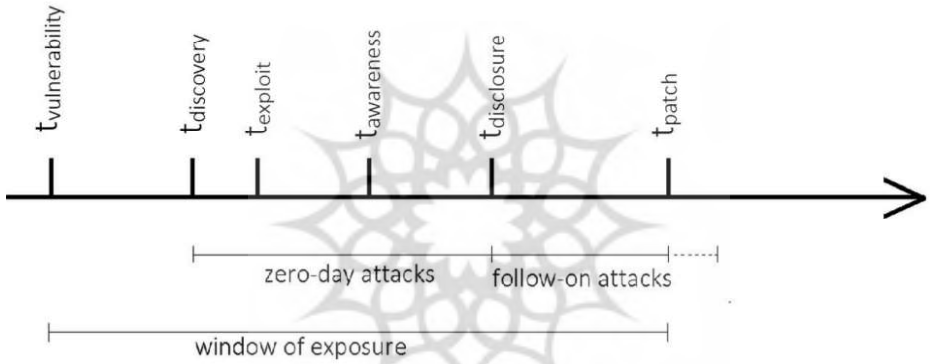
بر اساس مقاله (Maathuis et al., 2016, p. 3) چرخه حیات تسلیحات سایبری بر اساس فرآیند انجام عملیات سایبری تعریف می‌شود و پس از اتمام عملیات، حیات سلاح سایبری نیز پایان می‌پذیرد. نکته مهم این چرخه حیات این است که سلاح سایبری به‌صورت خاص منظوره و بر اساس آسیب‌پذیری موجود در هدف مشخصی تولید می‌شود. این مراحل عبارتند از:"

۱- تعریف پروژه: در این مرحله مفهوم سلاح سایبری از دو منظر استراتژیک و مدیریتی تعریف می‌شود؛ و بر اساس آن معماری یک سلاح سایبری تدوین‌شده و عملکرد اصلی آن تعیین می‌شود.
۲- شناسایی: در این مرحله تحقیق در مورد هدف عملیات سایبری به‌منظور یافتن آسیب‌پذیری‌های موجود در آن انجام می‌شود.
۳- طراحی: در این مرحله طراحی سلاح سایبری شامل ویژگی‌های دقیق، مشخصات، وظایف و مهلت تعیین‌شده برای هر ماژول آن تعیین می‌شود.
۴- توسعه: در این مرحله مهندسان کد سلاح سایبری را با استفاده از زبان‌های متنوع برنامه‌نویسی یا اسکریپت‌نویسی پیاده‌سازی کرده و فرآیند آزمایش آن را مشخص می‌کنند.
۵- آزمون: در این مرحله مهندسان با استفاده از موارد آزمایش که در مرحله قبل تعریف‌شده‌اند، محیط آزمایش شبیه‌سازی‌شده با محیط واقعی را ایجاد و سلاح را آزمایش می‌کنند.
۶- اعتبارسنجی: در این مرحله نتایج حاصل از فاز ۵ با اهداف و ویژگی‌های تعریف‌شده در فازهای ۱ و ۳ مقایسه می‌شوند. اگر نتیجه این مقایسه منفی باشد، لازم است با بازگشت به فازهای ۳، ۴ و ۵ بازنویسی و اصلاح صورت پذیرد.
۷- نفوذ و کنترل: در این مرحله به سیستم هدف نفوذی به‌دوراز ایجاد اثر صورت پذیرفته برای زمان مناسب حمله تصمیم‌گیری می‌شود.
۸- حمله: این مرحله مهم‌ترین قسمت چرخه حیات سلاح سایبری است که بر اساس آن سلاح از راه دور یا به‌صورت خودکار فعال‌سازی می‌شود.

۹- استمرار حمله: در این مرحله عملکرد سلاح سایبری کنترل شده و از اثرات مطلوب آن، اطمینان حاصل می‌شود. اگر مواردی که مطابق برنامه نیست روی دهد، تدابیری برای حل مشکل و ادامه حمله یا رفتن مستقیم به فاز ۱۰ اتخاذ خواهد شد.

۱۰-خروج سلاح از عملیات: در این مرحله چرخه حیات سلاح سایبری پایان‌یافته و سلاح از سیستم هدف خارج می‌شود. " (Maathuis et al., 2016, p. 3)

شکل ۱ چرخه حیات تسلیحات سایبری را به نقل از مقاله (Smeets, 2018, pp. 9–۱۲) نشان می‌دهد.



شکل ۱: چرخه حیات تسلیحات سایبری

بر اساس مقاله مذکور:" $t_{vulnerability}$ زمانی است که آسیب‌پذیری کشف می‌شود. $t_{discovery}$ زمانی است که از روش بهره‌برداری از آسیب‌پذیری کشف می‌گردد. $t_{exploit}$ زمانی است که کد بهره‌برداری یا اکسپلویت آسیب‌پذیری منتشر می‌شود. $t_{awareness}$ زمانی است که تولیدکننده محصول از وجود آسیب‌پذیری مطلع می‌شود. وی ممکن است از طریق کشف آسیب‌پذیری در آزمایش خود از وجود آسیب‌پذیری مطلع شود یا با گزارش شخص ثالثی از آن اطلاع یابد. تولیدکننده محصول بسته به ارزیابی ریسک آسیب‌پذیری، اولویت ایجاد وصله متناسب با آن را تعیین می‌کند. $t_{disclosure}$ زمانی است که اطلاعات آسیب‌پذیری توسط نویسنده معتبری در رسانه‌ای عمومی منتشر شود؛ و درنهایت، t_{patch} زمانی است که وصله امنیتی برطرف‌کننده آسیب‌پذیری منتشر می‌شود. از این مرحله به بعد، تجهیزاتی که بر روی آن‌ها وصله نصب‌شده

است؛ در معرض خطر از جانب آن آسیب‌پذیری نیستند. حمله‌ای که بین $t_{exploit}$ و $t_{disclosure}$ اتفاق می‌افتد، حمله با استفاده از آسیب‌پذیری روز صفرم است. نامیده می‌شود. اگر یک سلاح سایبری -که از آسیب‌پذیری خاصی استفاده می‌کند- علیه هدفی استفاده شود، اثر خود را در برابر سایر اهداف از دست خواهد داد؛ بنابراین عملیات سایبری علیه یک شخص ممکن است حمله‌ای علیه همگان نباشد؛ اما دفاع سایبری برای همگان را به ارمغان خواهد آورد.

در سه بازه زمانی است که اهداف موردحمله سایبری قرار می‌گیرند: ۱- قبل از اینکه اکسپلویت آسیب‌پذیری منتشر شود. در این زمان است که مهاجمان با دقت هدف خود را انتخاب کرده و سود سلاح سایبری توسعه‌یافته‌شان را به حداکثر می‌رسانند. ۲- هنگامی است که اکسپلویت آسیب‌پذیری برای عموم منتشر می‌شود. در این زمان شرایط آزاد و رقابتی برای تمامی مهاجمان ایجادشده و از تنوع اهداف، کاسته می‌شود. ۳- زمانی است که در نصب وصله امنیتی منتشرشده، تعلل شده است. در این حالت برای مهاجمان وضعیت "گرفتن آنچه می‌توان گرفت" ظاهر می‌شود.

با توجه به آنچه بیان شد، از رده خارج شدن تسلیحات سنتی به‌صورت خطی و به‌صورت تدریجی مدل‌سازی می‌شود؛ اما این مدل برای تسلیحات سایبری خطی نبوده و با وجودیکه توانایی بهره‌برداری از آن‌ها برای مدت محدودی ثابت است؛ اما به سرعت کاهش می‌یابد."

ویژگی تسلیحات سایبری

در مقاله (Lin & Zegart, 2017, p. 2)، ۴ ویژگی برای تسلیحات سایبری شمرده‌شده است: " الف) دشواری تشخیص تسلیحاتی که برای جمع‌آوری اطلاعات و انجام حمله و ایجاد آسیب استفاده می‌شوند. ب) استفاده از فریب در نصب یا بکارگیری تسلیحات؛ بدین معنی که در عملیات سایبری به هدف حمله گفته نمی‌شود که با کلیک روی این لینک، رایانه‌اش مورد نفوذ قرار خواهد گرفت. پ) نیازمندی به اطلاعات شناسایی از هدف عملیات سایبری در قبل و حین انجام عملیات جهت تأثیرگذار بودن سلاح سایبری؛ بدین معنی که در بسیاری از موارد، کوچک‌ترین تغییر پیکربندی هدف، می‌تواند اثر سلاح سایبری را در به‌طور کامل از بین ببرد. ت) نیازمندی تسلیحات به آماده سازی قبلی و ایجاد رخنه در هدف عملیات سایبری به‌منظور برقراری ارتباطات آتی نفوذگر با تسلیحات سایبری"

در مقاله (Leuprecht et al., 2019, pp. 4–5) ویژگی‌های کلیدی تسلیحات سایبری چنین بیان‌شده است:" الف) تسلیحات سایبری معمولاً یک‌بار مصرف هستند؛ زیرا در صورت یک‌بار استفاده، امکان افشاء آن‌ها وجود داشته و باعث می‌شود که در ابتدای استفاده بعدی، کشف گردند. ب) تسلیحات سایبری را می‌توان قبل از استفاده، در زیرساخت هدف تزریق کرد تا درزمانی مشخص فعال گردد. پ) با توجه به اینکه امکان کنترل تسلیحات سایبری حتی در زمان اجرا وجود دارد، مقدار و گستردگی صدمه‌ای که وارد می‌سازد نیز قابل‌کنترل است. حتی می‌توان به نحوی آن را بکار گرفت که تنها به هدفی خاص، حمله‌ور شود. ت) کشف هویت و انتساب عاملیت بکارگیری تسلیحات سایبری دشوار بوده و برای مدافع تشخیص مبدأی حمله پیچیده است. ارائه شواهد متقن جهت متقاعد ساختن سازمان‌های دیگری مانند سازمان پیمان آتلانتیک شمالی (ناتو) یا سازمان ملل نیز دشوارتر می‌باشد. ث) با توجه به سرعت زیاد تغییرات در حوزه سایبر، ماندگاری تسلیحات سایبری طولانی مدت است؛ زیرا معمولاً آسیب‌پذیری‌های مورداستفاده در تسلیحات سایبری تنها در بخشی از سیستم‌ها رفع می‌شود و این آسیب‌پذیری‌ها در تعداد زیادی از سیستم‌های دیگر باقی می‌ماند. ج) سلاح‌های سایبری در جهان فیزیکی عمل نمی‌کنند بلکه در فضای مجازی فعال بوده و دارای ساختاری هستند که عمدتاً با جهان بی‌ارتباط است. تا همین اواخر ، برخی از بخش‌های فضای مجازی مانند شبکه‌های نظامی و هواپیماهای جنگنده از اینترنت جداشده بودند، اما نشان داده‌شده است که این جدایی با توسعه تکنیک‌های پل زدن و نیاز به‌روزرسانی نرم‌افزاری تجهیزات شبکه‌های ایزوله، کامل و همیشگی نیست. چ) با توجه به مرزهای جغرافیایی، نتایج بکارگیری سلاح‌های سایبری با سلاح‌های معمول یکسان نیست. زیرساخت‌های شبکه اینترنت عمدتاً توسط مشاغل خصوصی چندملیتی اداره می‌شود و دلیلی ندارد که ترافیک، مسیر مستقیم را بپیماید بلکه عموماً از چندین کشور واسط عبور خواهد کرد و دراین‌بین ممکن است مورد سوءاستفاده واقع شود."

دسته‌بندی تسلیحات سایبری

بر اساس مقاله (Buchanan, 2020, p. 2) تسلیحات سایبری را می‌توان بر اساس اثر، به ۳ دسته تقسیم‌بندی نمود: "

۱. تسلیحات جاسوسی سایبری: جاسوسی سایبری شامل جمع‌آوری اطلاعات و شناسایی میدان جنگ با استفاده از ابزارهای سایبری است.

۲. تسلیحات سیاسی سایبری: این نوع از تسلیحات سایبری برای اثرگذاری بر انسان‌ها، کنترل فضای سیاسی یا دیکته نمودن روایتی است و می‌تواند از قدرت نرم تبلیغات تا قدرت سخت اعمال فشار از طریق تهدید نشت اطلاعات هک شده باشد.

۳. تسلیحات سایبری با آسیب فیزیکی: این نوع تسلیحات سایبری برای بی‌ثبات‌سازی و ایجاد اختلال به‌منظور قدرت‌نمایی انجام می‌شود یا باعث آسیب دائمی فیزیکی به تجهیزات یا انسان‌ها می‌گردد"

بر اساس مقاله (Bellovin et al., 2017, pp. 2–3) نیز تسلیحات سایبری به ۲ دسته تقسیم‌بندی می‌شوند: " تسلیحاتی که تفاوتی در اهداف گوناگون قائل نیستند و به اصطلاح "ذاتاً بدون تبعیض"[۱] هستند. این نوع از تسلیحات سایبری و بر اساس راهنمای جنگ وزارت دفاع ایالات‌متحده، استفاده از آن‌ها به‌عنوان ابزار جنگی ممنوع است. دسته دوم تسلیحاتی است که با دقت هدف‌گذاری شده‌اند و خسارت قابل‌توجهی را فراتر از هدف اصلی خود وارد نمی‌کنند. این نوع از تسلیحات باید دو شرط زیر را رعایت کنند: ۱- سلاح سایبری باید بتواند علیه اهدافی که صراحتاً تعیین‌شده است، هدایت شود. ۲- سلاح سایبری باید اثرات منفی خود را روی سایر اهدافی که مهاجم مستقیماً آن‌ها را به‌عنوان هدف تعیین نکرده است، به حداقل برساند. حملات سایبری به استونی ، جورجیا ، ایران ،و شرکت سونی از این دست بوده‌اند. این حملات، آغاز استفاده از فضای سایبر در درگیری‌های بین دولت‌ها است."

مقاله (Bellovin et al., 2017, p. 2) تسلیحات سایبری را دارای ۲ مؤلفه می‌داند: " مؤلفه نفوذ و مؤلفه کارایی. مؤلفه نفوذ مکانیسمی است که از طریق آن سلاح به سیستم هدف دسترسی پیدا می‌کند. مؤلفه کارایی سازوکاری است که درواقع آنچه را که قرار است سلاح انجام دهد – مانند بین بردن داده‌ها ، قطع ارتباطات ، خارج نمودن اطلاعات ، سرعت بخشیدن به سانتریفیوژهای کنترل شده توسط رایانه و غیره- انجام می‌دهد. نفوذ عموماً با استفاده از

---

۱. inherently indiscriminate

آسیب‌پذیری‌های شناخته‌شده که وصله امنیتی آن‌ها نیز منتشرشده است. اکثر قریب به اتفاق حملات از این طریق انجام می‌شود اما با این وجود برخی حملات مانند حمله پیچیده استاکس‌نت به تأسیسات هسته‌ای ایران در نطنز ، از آسیب‌پذیری‌های روز صفرم استفاده کردند."

تسلیحات سایبری به ۳ مشخصه متکی هستند: ۱. آسیب‌پذیری: ضعف یا نقص طراحی در سخت‌افزار یا نرم‌افزاری که می‌تواند توسط مهاجم دستکاری‌شده و امکان دسترسی به سیستم موردحمله فراهم شود. در اکثر قریب به اتفاق عملیات سایبری از آسیب‌پذیری‌های شناخته‌شده استفاده می‌شود. حتی در موارد متعددی وصله‌های امنیتی نیز برای آسیب‌پذیری منتشرشده است؛ اما در برخی عملیات سایبری، از آسیب‌پذیری‌های روز صفر استفاده می‌شود. ۲. اکسپلویت[۱] کدی که برای ایجاد تأثیری خاص از طریق استفاده از آسیب‌پذیری نوشته‌شده است. ۳. روش انتشار: روشی است که در آن اکسپلویت منتشر می‌گردد تا به هدف نهایی برسد (Lin & Zegart, 2019, pp. 384–385).

هوشمندی تسلیحات سایبری

در سال‌های اخیر با پیشرفت هوش مصنوعی و فضای سایبر، چشم‌انداز تسلیحات خودمختار و خودآموز موردتوجه قرارگرفته و نگرانی‌هایی را نیز برای امنیت ملی کشورها ایجاد کرده است. قدرت‌های نظامی جهان به‌طور فزاینده‌ای درگیر تحقیق و توسعه بکارگیری هوش مصنوعی در کاربردهای نظامی بوده و از هوش مصنوعی در جهت تقویت و اثربخشی بیشتر اهداف تهاجمی استفاده می‌نمایند.(Shoaib, 2020, p. 1) درواقع، عوامل تهدید به‌طور مداوم در حال تغییر و بهبود راهبرد حملات خود با تأکید ویژه بر استفاده از تکنیک‌های مبتنی بر هوش مصنوعی در روند حمله هستند ، این حملات که به حمله سایبری مبتنی بر هوش مصنوعی شناخته می‌شوند؛ می‌توانند همراه با تکنیک‌های سنتی حمله برای آسیب رساندن و ایجاد خسارت بیشتر استفاده گردند.(Kaloudi & Li, 2020, p. 2) مقاله (Bellovin et al., 2017, pp. 4–5)

---

۱. Exploit

حملات سایبری را به ۱- حملات جلوگیری از دسترسی[۱]شامل حملات جلوگیری از دسترسی و جلوگیری از دسترسی توزیع‌شده؛ ۲- حملات آسیب رساندن به فایل[۲]شامل تغییر یا تخریب فایل و ۳- حملات وارد ساختن آسیب فیزیکی[۳]که جدی‌ترین نوع حمله به‌حساب آمده و باعث آسیب فیزیکی به رایانه‌ها یا تجهیزات متصل به آن‌ها می‌شود؛ تقسیم‌بندی می‌کند.

"تسلیحات سایبری خودمختار، توسط الگوریتم‌های از پیش تعیین‌شده‌ای کنترل شده و هدف عملیاتی خود را طبق سناریوهای تعیین‌شده از قبل، انجام می‌دهند. تسلیحات خودمختار سایبری، برای شناسایی و دستیابی به اهدافی که در محیط‌های پیچیده، پویا و به‌دوراز هرگونه ارتباط با عامل راهبر انسانی قرار دارند؛ از قابلیت تطبیق‌پذیری و یادگیری خودکار استفاده نموده و بدین روش، مستقلاً قادر به تصمیم‌گیری در پاسخ به متغیرهای خارجی و تعامل با محیط خارجی هستند. این تسلیحات بر اساس برنامه‌ریزی داخلی، اطلاعات، فرایندها، شرایط و محدودیت‌های محیطی این تصمیمات را اتخاذ می‌نمایند. استاکس‌نت[۴]مثال خوبی از چنین تسلیحاتی است. این سلاح سایبری به‌طور پنهانی و احتمالاً از طریق یک حافظه USB بر روی شبکه ایزوله مرکز هسته‌ای نطنز ایران بارگیری می‌شد و با جستجو در یک شبکه پیچیده و به‌هم‌پیوسته، مدل‌های خاصی از کنترل‌کننده‌های منطقی قابل‌برنامه‌ریزی[۵]تولیدشده توسط شرکت زیمنس[۶]را شناسایی می‌کرد. این PLC ها به رایانه‌های این مرکز اجازه کنترل سانتریفیوژهای غنی‌سازی اورانیوم را می‌دادند. استاکس‌نت برای مخفی ماندن خود، مقادیر حسگرها را در دوره‌ای که PLC ها به‌طور عادی کار می‌کردند، ثبت می‌کرد؛ سپس برنامه‌نویسی PLC ها را تغییر داده و هم‌زمان مقادیر عادی جمع‌آوری‌شده را به اپراتورها نمایش می‌داد. با این کار بدون متوجه شدن اپراتورها باعث چرخش سریع و طولانی مدت سانتریفیوژها می‌شد که منجر به از بین رفتن فیزیکی تعداد زیادی سانتریفیوژ گردید. ویژگی جالب استاکس‌نت این

---

۱. Denial of service attacks
۲. File damage
۳. Physical damage
۴. Stuxnet
۵ programmable logic controller (PLC)
۶. Siemens

بود که پس از استقرار، نمی‌توانست با اپراتورهای خود ارتباط برقرار کند و همه تصمیمات را به‌صورت خودمختار اتخاذ می‌کرد" (Buchan & Tsagourias, 2020, pp. 3–4).

اختفاء تسلیحات سایبری

روش‌های مختلفی در تسلیحات سایبری جهت اختفاء استفاده می‌شود، این روش‌ها به نقل از مقاله (بارانی & سبزه کار, ۱۳۹۶, ۷–۸) عبارتند از:

- مبهم کردن کد:[۱] در این روش توسعه‌دهندگان تسلیحات سایبری تلاش می‌کنند تا با تغییر کد منبع سلاح و مثلاً درج فرامین اشتباه و پرش‌های غیر لازم، تجهیزات امنیتی را که بر اساس امضاء یا الگوهای استخراج‌شده پیشین تسلیحات سایبری کار می‌کنند را فریب دهند.
- رمزنگاری کد:[۲] تسلیحات سایبری معمولاً جهت فرار از شناسایی اقدام به رمزنگاری کد خود می‌کنند. با این روش تجهیزات امنیتی و دفاعی قادر به دسترسی به کد منبع سلاح حداقل در کوتاه‌مدت و تا زمانی که سلاح خود را از حالت رمزنگاری‌شده خارج نماید؛ نخواهند شد.
- نیمه چند ریختی:[۳] برخی از تسلیحات سایبری قادر هستند جهت مخفی ماندن طولانی مدت خود، الگوریتم رمزنگاری‌شان را در بازه‌های زمانی مشخص تغییر دهند و بدین روش تجهیزات امنیتی را از شناسایی ناکام گذارند.
- چند ریختی:[۴] تسلیحات سایبری که از این روش جهت مخفی سازی خود استفاده می‌کنند؛ در اوقات مشخص مثلاً زمان‌هایی که احتمال شناسایی خود را می‌دهند، کد منبعشان را بدون ایجاد تفاوت در وظیفه سلاح، تغییر می‌دهند.

---

۱. Obfuscation
۲. Code encryption
۳. Oligomorphic strategy
۴. Polymorphic strategy

- فرا ریختی[۱] تسلیحات سایبری که از روش فرا ریختی جهت اختفاء بهره می‌برند؛ جزء پیچیده‌ترین سلاح‌ها هستند. آن‌ها به نحوی تغییر می‌یابند که نمونه‌های جدید، شباهتی با نمونه اصلی ندارد. این تسلیحات موتور کدگذاری نداشته و در هر انتقال به‌طور خودکار الگوریتم نوشتاری یا دستوراتشان تغییر می‌کند.

بر اساس آنچه تاکنون بیان شد، تسلیحات سایبری را به ۳ بعد امنیت، هوشمندی و کارایی می‌توان دسته‌بندی نمود.

روش

این تحقیق با روش توصیفی- تحلیلی و موردی- زمینه‌ای به‌صورت آمیخته صورت می‌پذیرد. دلیل توصیفی- تحلیلی بودن، این است که برای گردآوری اطلاعاتی که مدون نشده به کار می‌رود و با این روش، توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد. علت موردی- زمینه‌ای بودن نیز این است که مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیطی واقعی صورت می‌گیرد.

نوع پژوهش درزمینه شناخت الگوی مفهومی تسلیحات سایبری، توسعه‌ای خواهد بود؛ زیرا دانش موجود در خصوص موضوع پژوهش را گسترش می‌دهد. از سوی دیگر، کاربرد الگوی ارائه‌شده در حوزه دفاعی جمهوری اسلامی ایران است؛ بنابراین مقاله حاضر از این منظر کاربردی محسوب گردیده و در مجموع توسعه‌ای- کاربردی خواهد بود. برای جمع‌آوری اطلاعات از روش تحلیل محتوا در کتابخانه علمی- تخصصی و سایت‌های معتبر اینترنتی بهره برده شد. همچنین با روش عقلایی به‌صورت میدانی مصاحبه با خبرگان عملیات سایبری و تنظیم پرسشنامه صورت پذیرفت. برای تحلیل داده‌های بخش کمی (داده‌های حاصل از پرسشنامه) نیز از روش‌های آمار توصیفی و استنباطی ازجمله معادلات ساختاری، تحلیل واریانس، ضریب همبستگی استفاده‌شده است.

به‌منظور اخذ نظر خبرگان جهت ارائه مدل مفهومی پژوهش، مصاحبه عمیق با روش اشباع نظری با جامعه آماری ۸ نفر به‌صورت تمام شمار صورت گرفت؛ بنابراین حجم نمونه با حجم جامعه برابر است. مشخصات خبرگانی که مصاحبه عمیق با آن‌ها صورت پذیرفته، در جدول ۱

---

۱. Metamorphic strategy

آمده است. سپس به‌منظور ارزیابی مدل مفهومی احصاء شده، پرسشنامه‌ای بر اساس طیف لیکرت تنظیم گردید. با توجه به جامعه آماری ۷۱ نفره -بر اساس جدول مورگان- پرسشنامه به‌صورت تمام شمار به ۷۱ نفر از خبرگان ارسال شد؛ بنابراین در این مرحله نیز حجم نمونه با حجم جامعه برابر است. مشخصات خبرگانی که پرسشنامه به آن‌ها ارسال گردید؛ در جدول ۲ آمده است. تعداد ۴ پرسشنامه بدلیل نقصی که داشت کنار گذاشته شد و داده‌ها با تعداد ۶۷ پرسشنامه گردآوری و تحلیل گردید. پرسشنامه به لحاظ روایی ظاهری و محتوا به تائید جمعی از اساتید رسانده شد و به لحاظ پایایی با استفاده از نرم‌افزار SPSS آلفای کرونباخ پرسشنامه ۰,۸۰۶ محاسبه شد که پایایی قابل قبولی است.

جدول ۱: مشخصات خبرگان در مصاحبه عمیق

ردیف	سن خدمتی	تحصیلات	تعداد سال فرماندهی/مدیریت در مشاغل مرتبط	تعداد نفرات	درصد فراوانی
۱	بیش از ۳۰ سال	۴ نفر دکترا و ۱ نفر کارشناسی ارشد	بیش از ۱۰ سال	۵	۶۲,۵٪
۲	بین ۲۵ تا ۳۰ سال	۲ نفر دکترا و ۱ نفر کارشناسی ارشد	بیش از ۱۰ سال	۳	۳۷,۵٪

جدول ۲: مشخصات خبرگانی که پرسشنامه به آن‌ها ارسال شد

ردیف	سن خدمتی	تحصیلات	تعداد سال فرماندهی/مدیریت در مشاغل مرتبط	تعداد نفرات	درصد فراوانی
۱	بین ۲۰ تا ۲۵ سال	۴ نفر دکترا و ۸ نفر کارشناسی ارشد	بیش از ۵ سال	۱۲	۱۶,۹٪
۲	بین ۱۵ تا ۲۰ سال	۵ نفر دکترا و ۱۷ نفر کارشناسی ارشد	بیش از ۵ سال	۲۲	۳۱٪
۳	بین ۱۰ تا ۱۵ سال	۱ نفر دکترا و ۳۶ نفر کارشناسی ارشد	بیش از ۵ سال	۳۷	۵۲,۱٪

جهت بررسی الگو این تحقیق نیز از روش آماری حداقل مربعات جزئی[۱]استفاده‌شده است. این روش، در قالب کلی مدل معادلات ساختاری[۲]مطرح می‌باشد. الگوسازی معادلات ساختاری از دو بخش الگوی اندازه‌گیری و الگوی ساختاری تشکیل‌شده است. الگوی اندازه‌گیری شامل سؤالات (شاخص‌های) هر بعد به همراه آن بعد است و روابط میان سؤالات و ابعاد در این بخش مورد تجزیه‌وتحلیل قرار می‌گیرد. بخش الگوی ساختاری نیز شامل تمامی سازه‌های مطرح در الگوی اصلی تحقیق است و میزان همبستگی سازه‌ها و روابط علی میان آن‌ها در این قسمت موردسنجش قرار می‌گیرد. شاخص‌ها که معمولاً به سؤال‌های پرسشنامه اطلاق می‌شود، متغیرهای آشکار تحقیق به شمار می‌روند که توسط پاسخگویان به‌طور مستقیم و بی‌واسطه موردسنجش قرار می‌گیرند؛ اما لایه‌های بعدی که مؤلفه‌ها و ابعاد پرسشنامه هستند متغیرهای مکنون[۳]می‌باشند که قابلیت سنجش مستقیم نداشته و با استفاده از روابط بین آن‌ها و نشانگرها یا متغیرهای آشکارشان موردسنجش قرار می‌گیرند. (علی نژاد, ۱۳۹۹, ص. ۱۵) اگر مقدار بار عاملی بین سؤالات پرسشنامه و متغیرهای مکنون بیشتر از ۰/۴ باشد نتیجه می‌گیریم که سؤالی که برای آن سازه به‌کاربرده‌ایم به خوبی متغیر مکنون موردنظر را سنجیده است. مقدار آماره t درواقع ملاک اصلی تأیید یا رد فرضیات است. اگر این مقدار آماره به ترتیب از ۱/۶۴، ۱/۹۶ و ۲/۵۸ بیشتر باشد نتیجه می‌گیریم که آن فرضیه در سطوح ۹۰، ۹۵ و ۹۹ درصد تأیید می‌شود. همچنین باید گفت که اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته مثبت باشد نتیجه می‌گیریم که با افزایش متغیر مستقل شاهد افزایش در متغیر وابسته خواهیم بود؛ و بالعکس اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته منفی باشد نتیجه می‌گیریم که با افزایش متغیر مستقل شاهد کاهش در متغیر وابسته خواهیم بود. در این پژوهش برای انجام محاسبات بیان‌شده از نرم‌افزار Smart PLS استفاده‌شده است.

یافته‌های پژوهش

بر اساس مبانی نظری تحقیق و با بکارگیری روش تحلیل محتوا، ابعاد هوشمندی، گمنامی و کارایی از الگوی مفهومی تحقیق، استخراج گردیدند. با توجه به عدم دستیابی پژوهشگران به مؤلفه‌ها و شاخص‌های الگوی مفهومی از ادبیات تحقیق، به‌صورت اکتشافی با خبرگان حوزه

---

۱. Partial Least Squares

۲. Structural Equation Modeling

۳. Latent Variables

پـژوهش مصـاحبه عمیـق انجـام شـد. بـا بکـارگیری روش عقلایـی در مصـاحبه عمیـق، ابعـاد به‌دست‌آمده از مبانی نظری، تائید شده و مؤلفه‌های و شاخص‌های اولیه الگوی مفهومی حاصـل گردیدند. الگوی اولیه، در قالب پرسشنامه‌ای که روایی و پایایی آن تأییدشده بـود؛ بـه خبرگـان شرح داده‌شده در جدول ۲ ارسال گردید. با جمع‌آوری و تحلیل آمـاری خروجـی پرسشـنامه‌ها، یافته‌های ذیل به‌دست‌آمده است.

جهت بررسی همبستگی داده‌ها ابتدا باید مشـخص شـود کـه داده‌هـا پـارامتری هسـتند یـا ناپارامتری. برای این منظور از آزمون کلموگوروف –اسمیرنوف اسـتفاده می‌شـود. بـرای بررسـی نرمال بودن داده‌ها فرضیه‌ای به شکل زیر مطرح و سپس مورد آزمون قرار گرفت.

H۰: توزیع داده‌های متغیرها نرمال است.

H۱: توزیع داده‌های متغیرها نرمال نیست.

بر اساس اطلاعات به‌دست‌آمده از نتیجه آزمون مـذکور، میـزان sig متنـاظر بـا هـر یـک از داده‌ها برابر با ۰,۰۰۰ گردید. همان‌طور که مشخص است مقـدار مـذکور از ۰,۰۵ کمتـر اسـت؛ بنابراین داده‌های پرسشنامه از توزیع نرمال برخوردار نیستند و از آمار ناپارامتریک برای تحلیـل استنباطی آن‌ها استفاده می‌کنیم. تمامی آزمون‌های آماری بر اسـاس سـطح معنـاداری قضـاوت می‌شود (چه آزمون‌های پارامتریک و چـه ناپارامتریـک). اگـر سـطح معنـاداری کمتـر از مقـدار خطای ۰,۰۵ به‌دست آمد فرضیه H۱ تائید و اگر بیشتر به‌دست آمد، فرضیه H۰ تائید می‌گردد.

با توجه به ناپارامتری بودن داده‌ها، برای محاسبه ضریب همبستگی از آزمون اسپیرمن بهـره می‌بریم.

الف) بررسی ارتباط بین مؤلفه‌ها و ابعاد: ارتباط بین مؤلفه‌ها و ابعاد با استفاده از ضـریب همبستگی اسپیرمن محاسبه‌شده است. فرض H0 بیانگر عدم وجود همبستگی معنی‌دار اسـت و فرض H1 وجود همبستگی معنی‌دار می‌باشد. نتایج این آزمون به شرح جدول ۱ ارائه‌شده است.

(۱) ارتباط بین ابعاد الگوی مفهومی تسلیحات سایبری

جدول ۳: نتایج همبستگی بین ابعاد الگوی مفهومی تسلیحات سایبری

بعد	آماره	کارایی	هوشمندی	گمنامی
تسلیحات سایبری	ضریب همبستگی	۰,۸۱۶	۰,۶۰۲	۰,۶۸۶
	سطح معناداری	.۰۰۰	.۰۰۰	.۰۰۰

سطوح معناداری قیدشده در جدول ۱ نشان می‌دهد که در تمامی موارد، ابعاد با همدیگر دارای ارتباط مثبت و معنادار هستند. همچنین همبستگی بین ابعاد ذکرشده با الگوی مفهومی تسلیحات سایبری در تمامی موارد معنادار است که نشان‌دهنده وجود همبستگی قوی بین این ابعاد و کل پرسشنامه است.

(۲) ارتباط بین مؤلفه‌های بعد کارایی و بعد مذکور

جدول ۴: نتایج همبستگی بین مؤلفه‌های بُعد کارایی

مؤلفه / بعد		جاسوسی	تغییر اطلاعات	تخریب	اختلال
کارایی	ضریب همبستگی	۰٫۵۰۹	۰٫۷۳۵	۰٫۷۶۳	۰٫۵۸۹
	سطح معناداری	۰.۰۰۰	۰.۰۰۰	۰.۰۰۰	۰.۰۰۰

سطوح معناداری در جدول ۲ نشان می‌دهد که همبستگی بین مؤلفه‌های بعد کارایی با بُعد مربوطه در سطح کمتر یا مساوی ۰٫۰۰۱ معنادار است که نشان‌دهنده وجود همبستگی معنادار و غیر تصادفی بین مؤلفه‌های مذکور و بُعد کارایی است.

(۳) ارتباط بین مؤلفه‌های بعد هوشمندی و بعد مذکور

جدول ۵: نتایج همبستگی بین مؤلفه‌های بُعد هوشمندی

بعد / مؤلفه		تحلیل و یادگیری	تصمیم‌گیری
هوشمندی	ضریب همبستگی	۰٫۹۱۴	۰٫۸۶۲
	سطح معناداری	۰.۰۰۰	۰.۰۰۰

سطوح معناداری در جدول ۳ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد هوشمندی با بعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد هوشمندی است.

(۴) ارتباط بین مؤلفه‌های بعد گمنامی و بعد مذکور

جدول ۶: نتایج همبستگی بین مؤلفه‌های بُعد گمنامی

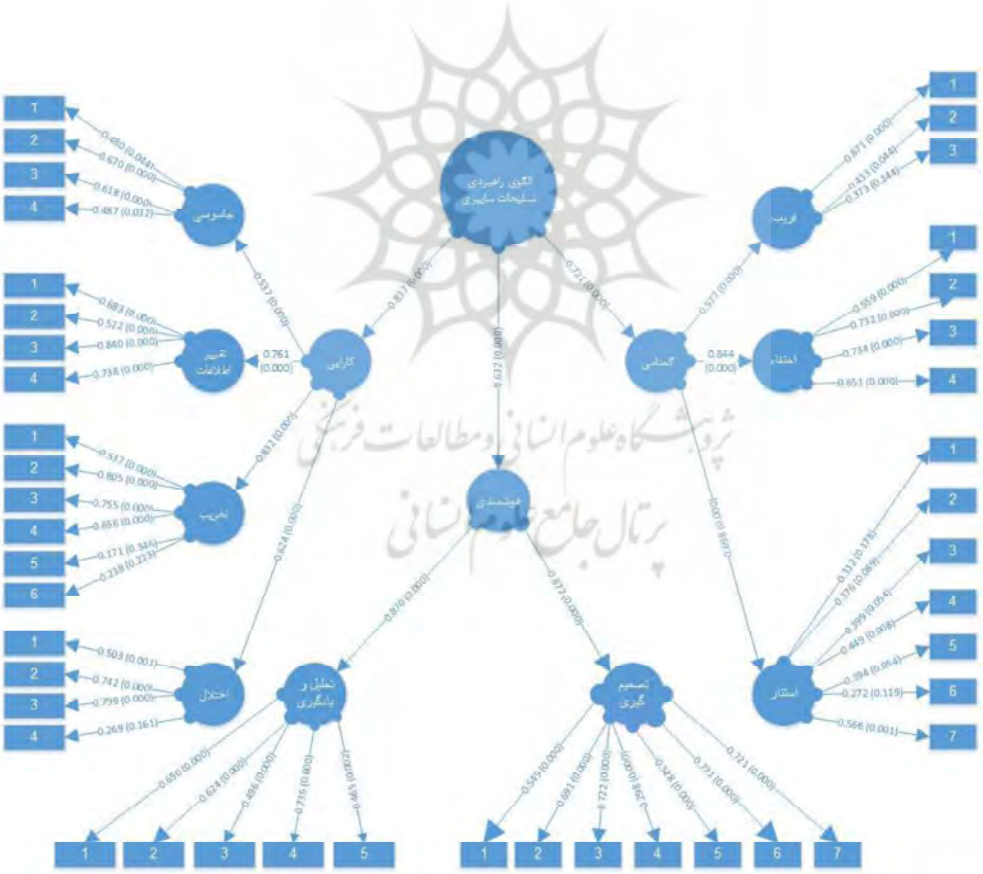
بعد / مؤلفه	استتار	اختفاء	فریب

گمنامی	ضریب همبستگی	۰,۶۸۳	۰,۸۱۹	۰,۴۱۹
	سطح معناداری	۰.۰۰	۰.۰۰۰	۰.۰۰۰

سطوح معناداری قیدشده در جدول ۴ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد گمنامی با بعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد گمنامی است.

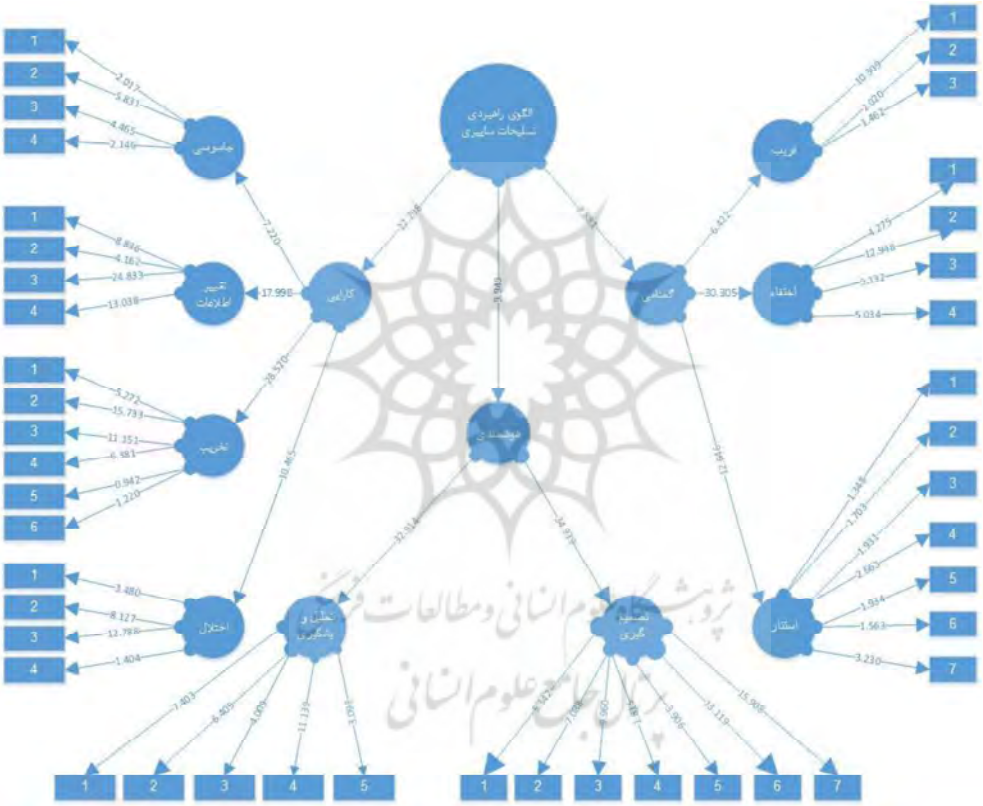
ب) بررسی الگوی تحقیق:

(۱) الگوی ساختاری تحقیق: در شکل‌های ۲ و ۳ الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو، مقادیر t الگوی ساختاری و مقدار P ترسیم‌شده است.



شکل ۲: الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو و مقدار P

در الگوی ساختاری شکل ۲ ابعاد، مؤلفه‌ها و شاخص‌های مورد تأیید نشـان داده‌شـده‌اند. در این الگو شاخص‌ها همان متغیرهای آشکار هستند کـه بـه مؤلفـه‌های مربـوط بـه خـود متصـل شده‌اند. همچنین مقدار بار عاملی، ضرایب مسیر و مقدار P مربوط به ابعاد، مؤلفه‌ها و شاخص‌ها نیز در الگو مشخص‌شده است. در شـکل ۳ نیـز الگـوی سـاختاری تحقیـق بـه همـراه ضـریب معناداری (آماره t) به تصویر درآمده است. با توجه به اینکه مقدارt برای تمام ابعاد و مؤلفه‌های پژوهش بیشتر از ۱/۹۶ هست بنابراین رابطه بین ابعاد و مؤلفه‌ها تائید می‌شود.



شکل ۳: الگوی ساختاری تحقیق به همراه مقادیر t الگوی ساختاری

(۲) نتایج الگوی ساختاری:

جدول ۷: نتایج حاصل از یافته‌های الگوی ساختاری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
کارایی ← الگوی مفهومی تسلیحات سایبری	۰,۸۳۷	۰,۰۳۸	۲۲,۲۹۸	۰.۰۰۰	تأیید رابطه
هوشمندی ← الگوی مفهومی تسلیحات سایبری	۰,۶۳۲	۰,۰۶۴	۹,۹۴۹	۰.۰۰۰	تأیید رابطه
گمنامی ← الگوی مفهومی تسلیحات سایبری	۰,۷۲۱	۰,۰۸۱	۸,۸۸۱	۰.۰۰۰	تأیید رابطه

جدول ۵ نشان می‌دهد که همه ضرایب الگوی ساختاری با سطح اطمینان ۹۹ درصد یا بیشتر از آن به معناداری آماری رسیده‌اند. معناداری ضرایب آماری نشان می‌دهد که الگوی مفهومی تسلیحات سایبری از ابعاد کارایی، هوشمندی و گمنامی تشکیل‌شده است. بعد کارایی اجرا با ضریب مسیر ۰,۸۳۷ بیشترین تبیین را نسبت به الگوی مفهومی تسلیحات سایبری دارد؛ به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در بعد کارایی، موجب ایجاد تغییری به‌اندازه ۰,۸۳۷ انحراف معیار در الگوی ارائه‌شده خواهد شد. این نتایج نشان می‌دهد که ساختار الگوی مفهومی تسلیحات سایبری از استحکام بالایی برخوردار است.

(۳) نتایج الگوهای اندازه‌گیری

جدول ۸: نتایج حاصل از یافته‌های الگوی اندازه‌گیری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
جاسوسی ← کارایی	۰,۵۳۷	۰,۰۷۴	۷,۲۲۰	۰.۰۰۰	تأیید رابطه
تغییر اطلاعات ← کارایی	۰,۷۶۱	۰,۰۴۲	۱۷,۹۹۸	۰.۰۰۰	تأیید رابطه
تخریب ← کارایی	۰,۸۳۲	۰,۰۲۹	۲۸,۵۲۰	۰,۰۰۰	تأیید رابطه
اختلال ← کارایی	۰,۶۲۴	۰,۰۶۰	۱۰,	۰.۰۰۰	تأیید

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
			۴۶۵		رابطه
تحلیل و یادگیری → هوشمندی	۰,۸۷۷	۰,۰۲۵	۳۴,۹۳۹	۰.۰۰۰	تأیید رابطه
تصمیم‌گیری → هوشمندی	۰,۸۷۰	۰,۰۲۶	۳۲,۹۱۴	۰.۰۰۰	تأیید رابطه
استتار → گمنامی	۰,۶۹۸	۰,۰۵۵	۱۲,۶۴۶	۰.۰۰۰	تأیید رابطه
اختفاء → گمنامی	۰,۸۴۴	۰,۰۲۸	۳۰,۳۰۵	۰,۰۰۴	تأیید رابطه
فریب → گمنامی	۰,۵۷۷	۰,۰۹۰	۶,۴۲۲	۰.۰۰۰	تأیید رابطه

نتایج جدول ۶ نشان می‌دهد که:

مؤلفه‌های جاسوسی، تغییر اطلاعات، تخریب، اختلال دارای تأثیر مثبت و معنادار بر بعد کارایی هستند. دراین‌بین مؤلفه تخریب بیشترین تبیین را نسبت به بعد کارایی دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۸۳۲ انحراف معیار در بعد کارایی خواهد شد.

مؤلفه‌های تحلیل و یادگیری و تصمیم‌گیری دارای تأثیر مثبت و معنادار بر بعد هوشمندی هستند. دراین‌بین مؤلفه تحلیل و یادگیری بیشترین تأثیر را نسبت به بعد هوشمندی دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۸۷۷ انحراف معیار در بعد هوشمندی خواهد شد.

مؤلفه‌های استتار، اختفاء و فریب دارای تأثیر مثبت و معنادار بر بعد گمنامی هستند. دراین‌بین مؤلفه اختفاء بیشترین تبیین را نسبت به بعد گمنامی دارد. به‌عبارت‌دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۸۴۴ انحراف معیار در بعد گمنامی خواهد شد.

بحث و بررسی نتایج

بر اساس تجزیه‌وتحلیل‌های بیان‌شده، الگوی مفهومی تسلیحات سایبری به سه بعد، نه مؤلفه و چهل‌وچهار شاخص که هر یک در ذیل به‌اختصار بیان می‌شود؛ تقسیم‌بندی می‌گردد.

جاسوسی

جاسوسی سایبری عموماً توسط دولت‌ها یا سازمان‌های تحت حمایت آنان انجام‌شده و سیستم‌های اطلاعاتی را جهت به‌دست آوردن اطلاعات آن‌ها، هدف قرار می‌دهند. بر اساس قوانین بین‌المللی، جاسوسی تجاوز محسوب نشده و معاهده جهانی برای آن وجود ندارد؛ بنابراین معمولاً دولت قربانی به دنبال پاسخ دیپلماتیک برای چنین اقداماتی است. به‌طور مثال، پس از اعلام جمع‌بندی عملیات سایبری SolarWinds که آمریکا را در دسامبر سال ۲۰۲۰ هدف قرار داده بود، دولت بایدن در ۱۵ آوریل ۲۰۲۱ تصمیم به اخراج ده دیپلمات روسی گرفت. اندکی بعد، لهستان نیز برای همبستگی با ایالات‌متحده، این اقدام را دنبال کرد و مسکو پس از دو روز پاسخ این اقدامات را داد. (Hore & Raychaudhuri, 2021, p. 3) شاخص‌های یک جاسوس افزار سایبری عبارتند از: توانایی تشخیص اطلاعات حائز اهمیت بدین معنی که یک سلاح جاسوسی سایبری باید بتواند داده‌های حائز اهمیت را از بین حجم انبوه داده‌ها استخراج نموده و ارسال نماید. ساده‌ترین روش این کار گزینش داده اساس پسوند فایل می‌باشد؛ کاهش حجم اطلاعات ارسالی تا حساسیت سامانه‌های امنیتی برانگیخته نشود؛ ارسال غیر برخط اطلاعات بدین معنی که سیستم‌های اطلاعاتی معمولاً به اینترنت متصل نبوده و در شبکه‌های ایزوله قرار می‌گیرند. به همین دلیل سلاح جاسوسی سایبری به‌طور مستقیم به اینترنت دسترسی نداشته و باید بتواند از طریق تجهیزات واسط مانند حافظه فلش، اطلاعات را منتقل نماید؛ بدین طریق که هر زمان آن تجهیز به سیستم دارای اینترنت متصل گردید، اطلاعات خود را برای مبدأ عملیات سایبری ارسال نماید؛ پنهان‌سازی اطلاعات[۱] به این معنی که اطلاعاتی که توسط جاسوس افزار سایبری جمع شده است بدلیل حساسیت تجهیزات امنیتی باید به‌صورت پنهان ارسال شود. برای این منظور باید از دانش پنهان‌سازی اطلاعات

۱. Information Hiding

استفاده نمود که به بخش‌های مختلفی ازجمله پنهان نگاری[۱]دسته‌بندی می‌شود. با بکارگیری این روش، برخلاف رمزنگاری که محتویات پیام را پنهان می‌نماید؛ هرگونه نشانه‌ای از وجود اطلاعات، مخفی می‌گردد.

تغییر اطلاعات

برخی از تسلیحات سایبری به دنبال تغییر اطلاعات حساس هستند تا بدین طریق بتوانند تغییرات راهبردی را در شبکه تصمیم‌گیری هدف ایجاد نمایند. نمونه بارز این‌گونه از تسلیحات سایبری، استاکس‌نت است که در سال ۲۰۱۰ تأسیسات هسته‌ای جمهوری اسلامی ایران در نطنز را هدف قرار داد. (Bakić et al., 2021, p. 2) شاخص‌های کلیدی تسلیحات سایبری با کارایی تغییر اطلاعات عبارتند از: شناسایی تجهیز و تشخیص اطلاعات تصمیم‌ساز بدین معنی که در شبکه هدف، تجهیزات متعددی قرار دارند. بسیار حائز اهمیت است که سلاح سایبری بتواند تجهیز هدف و پشتیبان‌های آن را که دارای اطلاعات مؤثر هستند شناسایی نموده و از بین اطلاعات موجود آن‌ها، اطلاعات تصمیم‌ساز را مشخص نماید. با تغییر این اطلاعات، شبکه تصمیم‌گیری هدف دچار اختلال خواهد شد؛ یادگیری اطلاعات سامانه در حالت کارکرد عادی؛ تولید کردن اطلاعات جعلی مشابه اطلاعات سامانه در حالت عادی؛ نمایش دادن اطلاعات حالت عادی به ناظران امنیتی پس از تغییر زیرا اطلاعات تصمیم‌ساز به‌صورت مستمر توسط تجهیزات امنیتی یا مستقیماً توسط انسان کنترل می‌شوند. برای اینکه ناظران متوجه تغییر ایجادشده نگردند، لازم است سلاح سایبری اطلاعات کارکرد عادی سامانه را استخراج نموده و بازه تغییرات آن را با استفاده از هوش مصنوعی یاد بگیرد. سپس سلاح سایبری اطلاعات برخط و جعلی مشابه حالت عادی که آموخته بود، تولید نموده و پس از ایجاد تغییر در اطلاعات تصمیم‌ساز، داده‌های جعلی تولیدشده را به ناظران نمایش دهد. بدین روش اطلاعاتی که به‌دست تصمیم‌گیران خواهد رسید؛ اطلاعات تغییریافته‌ای خواهد بود که به تائید ناظران رسیده است.

تخریب

برخی تسلیحات سایبری، سخت‌افزار یا اطلاعات حائز اهمیتی را که برای ادامه کار هدف لازم

---

۱. Steganography

است، تخریب می‌نمایند. هدف این‌گونه عملیات سایبری، از کار انداختن موقتی یا دائم شبکه هدف است. نمونه بارز تسلیحات سایبری تخریب اطلاعاتی، سلاح شمعون است که باارزش‌ترین شرکت دنیا یعنی شرکت نفتی آرامکوی عربستان سعودی را هدف قرار داد. این سلاح سایبری باعث شد صادرات نفت این کشور برای چندین روز دچار اختلال شده و خسارت سنگینی متحمل گردد. (ALMAIAH & ALMOMANI, 2020, p. 4) شاخص‌های تسلیحات سایبری با کارایی تخریب اطلاعات یا سخت‌افزار عبارتند از: شناسایی توپولوژی شبکه هدف زیرا با این شناخت است که مشخصات رایانه‌های حاوی اطلاعات یا سخت‌افزارهایی که ستون اصلی شبکه به‌حساب می‌آیند، به‌دست‌آمده و سلاح سایبری به آن‌ها نفوذ خواهد نمود؛ تشخیص دادن ترتیب رایانه‌ها در تخریب زیرا ممکن است دسترسی عملیات کننده سایبری بدلیل از بین رفتن اطلاعات یا سخت‌افزار سیستمی که وی از طریق آن به هدف دسترسی دارد، قطع گردد. در این صورت تنها بخشی از شبکه هدف تخریب‌شده و عملیات سایبری به‌طور کامل به هدف خود دست نخواهد یافت؛ تشخیص بیشترین مدت بی‌کاری هدف زیرا اپراتور سامانه اندکی پس از شروع عملیات، از وقوع آن مطلع شده و با افزایش دامنه تخریب مقابله می‌نماید؛ انتشار خودکار سلاح؛ داشتن زمان‌بندی جهت شروع تخریب بدین معنی که جهت اجتناب از ناتمام ماندن عملیات سایبری می‌توان پیش از شروع، سلاح سایبری را در همه تجهیزات تزریق نمود یا به‌طور هوشمند سلاح خود را در کل شبکه منتشر نماید؛ سپس با انجام زمان‌بندی هوشمند سلاح –بدون دسترسی عامل عملیات– به‌طور کامل به هدف عملیات سایبری دست یافت؛ شناسایی پشتیبان برخط تجهیزات و سامانه‌های اطلاعاتی زیرا بدلیل نقش مهمی که این سامانه‌ها در بازدهی شبکه دارند، عموماً دارای پشتیبان‌های متعدد برخط می‌باشند. توانایی تسلیحات سایبری در شناسایی نسخ پشتیبان برخط سامانه‌های اطلاعاتی از طریق حجم ارتباطی این سامانه‌ها و سخت‌افزارهایی که به‌طور موازی با یکدیگر فعالیت می‌نمایند؛ در دستیابی به هدف عملیات سایبری بسیار حائز اهمیت است.

اختلال

تسلیحات سایبری که در ایجاد اختلال سرویس بکار می‌روند، با سایر تسلیحات سایبری متفاوت می‌باشند. در این نوع عملیات سایبری، سلاح سایبری بر روی رایانه قربانی نصب و کنترل آن را

از طریق سرور فرماندهی و کنترل در اختیار مهاجم قرار می‌دهد. رایانه نفوذ شده بات[۱]نامیده می‌شود و کنترل، هماهنگ‌سازی و گسترش شبکه بات[۲]بر عهده سلاح سایبری است. (رحیم اف & موحدی صفت, ۱۳۹۹, ص. ۲ و ۱۳) ذیلاً شاخص‌های اصلی تسلیحات سایبری با کارایی ایجاد اختلال بیان‌شده است: کنترل قربانی جهت بهره‌برداری از پهنای باند وی، انتشار خودکار سلاح جهت گسترش هرچه بیشتر شبکه بات؛ ایجاد ارتباط امن با سرور فرماندهی و کنترل شامل احراز هویت تمامی گره‌های کانال ارتباطی قبل از برقراری ارتباط، رمزنگاری کانال‌های ارتباطی، مدیریت و تغییر کلید رمزنگاری به ازای هر بخش از ارتباطات در بازه‌های زمانی کوتاه و با طول کلید مناسب؛ ارسال گزارش به سرور فرماندهی و کنترل و اجرای بلادرنگ فرمان آن سرور زیرا بدلیل گستردگی شبکه بات که بعضاً به صدها هزار بات نیز می‌رسد، اجرای بلادرنگ فرامین وارده حائز اهمیت بوده و هماهنگی بات‌ها با یکدیگر را در پی خواهد داشت. همچنین این نوع از تسلیحات سایبری لازم است در ابتدای نفوذ به قربانی سپس در بازه‌های زمانی مشخص، گزارش فعال بودن خود را به سرور فرماندهی و کنترل ارسال نمایند.

تحلیل و یادگیری

در این مؤلفه، سلاح سایبری اقدام به تحلیل محیط پیرامونی خود نموده و جهت دستیابی به مقاصد عملیات سایبری، از محیط می‌آموزد. شاخص‌های اصلی این مؤلفه عبارتند از: رفتارشناسی تجهیزات امنیتی و فریب و یادگیری چگونگی انتشار و فعالیت زیرا سلاح سایبری بر اساس رفتار تجهیزات امنیتی و فریب شبکه هدف اقدام به شناسایی آن‌ها و یادگیری نموده و فعالیت خود را به نحوی تنظیم می‌نماید که مانع شناسایی تجهیزات امنیتی یا ورود به تجهیزات فریب گردد. همچنین سلاح سایبری از بین مقاصد و روش‌های مختلف انتشار خود، مقاصد سامانه‌های فریب آموخته‌شده از رفتارشناسی را حذف و روش انتشار مناسبی را با توجه به یادگیری از رفتار تجهیزات امنیتی برمی‌گزینند؛ محیط شناسی سامانه‌های تحلیل و فریب و یادگیری مقابله با آن‌ها بدین معنی که برای سلاح سایبری مهم است که توانایی تشخیص هوشمند محیط عملیاتی را از محیط شبیه‌سازی‌شده داشته باشد و بر اساس یادگیری از محیط

---

۱. Bot

۲. Botnet

تحلیل جعبه شن[۱] یا سامانه‌های فریب مانند تله سایبری،[۲] اقدام مقابله رفتاری و عملکردی با آن‌ها نموده و در واکنش‌های خود تغییر ایجاد نماید؛ یادگیری زمان و مدت فعالیت؛ آسیب‌شناسی شبکه و یادگیری جهت استفاده در شبکه‌های مشابه؛ یادگیری فعالیت‌ها و فرآیندهای مجاز هدف زیرا یکی از راه‌های گمنامی سلاح در شبکه هدف، انجام فعالیت با پرچم فرآیندهای مجاز می‌باشد. بدین منظور لازم است سلاح سایبری بالأخص تسلیحات سایبری خودمختار اقدام به یادگیری از فرآیندهای مجاز شبکه هدف نموده و فعالیت‌های خود را در آن قالب به انجام رساند.

تصمیم‌گیری

مؤلفه تصمیم‌گیری در تسلیحات سایبری هوشمند بالأخص تسلیحات خودمختار -که مستقل از مهاجم به فعالیت می‌پردازند- بسیار حائز اهمیت است. شاخص‌های این مؤلفه عبارتند از: زمان‌بندی بر اساس کارایی زیرا سلاح سایبری بر اساس کارایی خود نیاز به زمان‌بندی‌های متفاوتی دارد. مثلاً در تخریب، زمان‌بندی مناسب باعث بیشترین تأثیرگذاری می‌شود و در کارایی‌هایی که نیاز به پردازش دارد، انتخاب زمان بی‌کاری سیستم توجه کمتری را جلب می‌نماید. درواقع با این شاخص، سلاح بر اساس کارایی خود زمان و مدت مناسب فعالیتش را تنظیم می‌نماید؛ بازآرایی امنیتی متناسب با محیط یعنی سلاح سایبری بر اساس تجهیزاتی که در محیط پیرامونی خود شناسایی می‌کند؛ بدون تغییر وظیفه‌اش اقدام به تغییر کد، رفتار یا ارتباطات خود می‌نماید؛ انتخاب هدف مؤثر؛ بکارگیری اکسپلویت متناسب؛ مشابهت گزینی با فعالیت‌ها و فرآیندهای مجاز؛ امحاء خودکار در شرایط افشاء؛ امحاء خودکار در شرایط ویژه زیرا علت کشف بسیاری از تسلیحات سایبری، گسترش ناخواسته آن‌ها به خارج از شبکه هدف بوده است که باعث گردیده شرکت‌های امنیتی در سراسر دنیا به آن‌ها دسترسی یافته و وجودشان را اعلام نمایند. این شاخص تسلیحات سایبری بیان می‌دارد درزمانی که سلاح سایبری خارج از شبکه هدف قرار گرفت، یا بازه زمانی فعالیتش خارج از محدوده مدنظر مهاجم واقع شد؛ اقدام به امحاء خودکار خود نموده و مانع اکتشافش شود.

---

۱. Sandbox

۲. Honeypot

استتار

اولین مؤلفه از بعد گمنامی، استتار است. در تعریف استتار چنین آمده است که فن و هنری است که با استفاده از وسایل طبیعی یا مصنوعی امکان کشف و شناسایی نیروها، تجهیزات و تأسیسات را از دیده بانی، تجسس و عکس‌برداری دشمن تقلیل داده و یا مخفی داشته و حفاظت نماید. مفهوم کلی استتار هم‌رنگ و هم‌شکل کردن تأسیسات، تجهیزات و نیروها با زمینه محیط اطراف می‌باشد. (فریدون, ۱۳۹۴, ص ۷.) استتار تسلیحات سایبری با شاخص‌های زیر سنجیده می‌شود: میزان پیچیدگی مبهم سازی بدین معنی که انجام مبهم سازی برای به حداکثر رساندن پیچیدگی سلاح سایبری و درنتیجه شناسایی نشدن آن توسط تجهیزات امنیتی شبکه هدف صورت می‌پذیرد. این شاخص، میزان ابهام کد پس از انجام مبهم سازی را بررسی می‌نماید. هرچه تعداد گزاره‌های موجود در برنامه، بکارگیری انواع گوناگون روش‌ها در مبهم سازی قالب، داده (شامل مبهم سازی آرایه، کلاس، متغیر) و جریان کنترلی (شامل افزودن کد یا عملوندهای اضافه، موازی‌سازی کد، تکنیک‌های درون خطی و برون خطی، تکنیک‌های جایگذاری، تکنیک‌های کپی‌سازی، ایجاد تغییرات در حلقه و غیره)، عمق درخت ارث‌بری، سطوح تودرتو و غیره بیشتر باشد، درجه پیچیدگی مبهم سازی سلاح سایبری، بیشتر است؛ میزان بازگشت توسط ضد مبهم ساز؛ درواقع، این شاخص بیان می‌کند که شناسایی کد و رفع ابهام توسط برنامه‌های ضد مبهم سازی به چه میزان ممکن است. به عبارتی هرقدر ضد مبهم ساز نیاز به زمان و حافظه بیشتری برای خارج کردن سلاح سایبری از ابهام داشته باشد؛ سربار محاسبات و سربار زمانی بیشتر بوده و درجه بازگشت توسط ضد مبهم ساز کمتر است؛ تغییر دادن خودکار کد منبع بدون تغییر وظیفه یعنی سلاح در زمان‌هایی که احتمال شناسایی خود را توسط تجهیزات امنیتی شبکه هدف می‌دهد؛ در کد خود بدون ایجاد تفاوت در وظیفه تغییر ایجاد می‌نماید؛ تغییر ساختار سلاح سایبری در هر انتشار بدون تغییر وظیفه زیرا باعث می‌شود تا در هر انتشار، جهشی در کد سلاح ایجادشده و امضاءهای متفاوتی از یکدیگر داشته باشند. این کار به عدم شناسایی سلاح توسط ضدبدافزارها کمک شایانی می‌نماید؛ نداشتن امضاء ایستا توسط سلاح سایبری زیرا دلیل کشف بسیاری از تسلیحات سایبری، استفاده آن‌ها از کد تسلیحات افشاء شده است؛ زیرا توالی از بایت‌های تسلیحات افشاء شده، به‌عنوان اثر انگشت منحصربه‌فرد سلاح استخراج‌شده و در بانک ضدبدافزارها نگهداری می‌شود. تمامی فایل‌های موردبررسی این‌گونه نرم‌افزارها، با این بانک مطابقت داده‌شده و در صورت یافتن موارد

مشابه، اعلام خطر می‌نمایند؛ بنابراین سلاح سایبری نباید توسط ضد بدافزارهای گوناگون، قابل‌شناسایی باشد و به عبارتی لازم است تا ازFUD[۱] بودن تسلیحات سایبری اطمینان حاصل گردد؛ نداشتن ناهنجاری رفتاری سلاح سایبری بدین معنی که ممکن است یک سلاح سایبری امضاء ایستا نداشته باشد اما بدلیل انجام رفتار ناهنجار مشابه بدافزارها، توسط هوش مصنوعی ضدبدافزارها شناسایی گردد؛ بنابراین لازم است تسلیحات سایبری ناهنجاری رفتاری نداشته و فعالیت‌های خود را در قالب فرآیندها و فعالیت‌های عادی سیستم به نمایش گذارد؛ کم‌حجم بودن سلاح سایبری زیرا ضدبدافزارها به نرم‌افزارهای دارای حجم مگابایت بسیار حساس بوده و به سرعت آن‌ها را شناسایی می‌نمایند. داشتن حجمی در حدود چند کیلوبایت، به سلاح سایبری کمک می‌کند تا بتواند خود را از دید ضدبدافزارها استتار نماید.

اختفاء

اختفاء یا پنهان‌کاری به کلیه اقداماتی اطلاق می‌گردد که مانع از قرار گرفتن تأسیسات و تجهیزات در دید دشمن می‌گردد و یا تشخیص تأسیسات و تجهیزات و همچنین انجام فعالیت‌های خاص را برای او غیرممکن و یا مشکل می‌سازد. (فریدون, ۱۳۹۴, ص ۷۰) شاخص‌های زیر مواردی است که برای اختفاء تسلیحات سایبری باید رعایت گردد: رمزنگاری کد، اطلاعات و ارتباطات سلاح سایبری، تغییر دادن الگوریتم رمزنگاری در بازه‌های زمانی معین تا سلاح بتواند مدت بیشتری از دید تجهیزات امنیتی مخفی بماند؛ مخفی ساختن پروسه سلاح سایبری بدین معنی که هر نرم‌افزاری که روی سیستم نصب شود پروسه‌ای را ایجاد می‌کند که قابل‌مشاهده است. مخفی ساختن پروسه سلاح سایبری از دید تجهیزات امنیتی قابلیتی است که به اختفاء سلاح سایبری کمک می‌نماید؛ مخفی نمودن ردپا

فریب

فریب، به مجموعه اقداماتی گفته می‌شود که موجب گمراهی دشمن گردیده و او را در تشخیص هدف با شک و تردید مواجه می‌سازد. درواقع، گمراه نمودن دشمن از طریق تحلیل شکل، اندازه، رنگ، سایه و موقعیت اهداف به‌گونه‌ای که آن‌ها را به شکل دیگری نمایش دهد؛ فریب گفته می‌شود.(فریدون, ۱۳۹۴, ص ۷۰) ذیلاً شاخص‌های فریب در بعد گمنامی تسلیحات سایبری بیان می‌گردند: اجراشدن در قالب فایل‌های مجاز؛ درواقع، در این شاخص، سلاح

---

۱. Fully Undetectable

سایبری در قالب یک فایل متنی، عکس، فیلم یا غیره اجراشده و به‌طور مستقیم یا غیرمستقیم –با استفاده از رمزگشا[۱]و بارگزار[۲]– روی سیستم قربانی نصب می‌شود؛ بکارگیری گواهینامه‌های دیجیتال جعلی یا مسروقه، به‌طور نمونه، در سال ۲۰۱۱، گواهی‌های دیجیتال تقلبی صادرشده توسط DigiNotar مورداستفاده قرارگرفته و حساب‌های Gmail حدود ۳۰۰۰۰۰ کاربر ایرانی شنود گردید. (Leavitt, 2011, p. 2) در اواخر سال ۲۰۱۳ نیز Google متوجه شد حکومت فرانسه از گواهی‌های دیجیتال تقلبی دامنه‌های آن، برای انجام حملات مردمیانی استفاده می‌کند و در اواسط سال ۲۰۱۴، Google اعلام نمود که مرکز انفورماتیک ملی هند از گواهی‌های دیجیتال غیرمجاز برای برخی دامنه‌های Google استفاده کرده است.(مرکز آپا دانشگاه امیرکبیر, ۱۳۹۵)؛ فعالیت در قالب فرآیندهای مجاز

نتیجه‌گیری

تحلیل‌گران نظامی، فضای مجازی را به‌عنوان قلمرو جدیدی در جنگ به رسمیت شناخته و در حال حاضر اهمیت آن در حال فزونی از سایر قلمروهای چهارگانه زمین، دریا، هوا و فضاست. پیشرفت روزافزون فناوری اطلاعات و وابستگی دولت‌ها به سامانه‌های فناوری اطلاعات همچنین گستردگی ابزار و تجهیزات سخت‌افزاری و نرم‌افزاری، باعث شده است که جنگ سایبری با شدت تمام توسط کشورهای صاحب فناوری علیه سایرین جریان یابد. دراین‌بین، سلاح سایبری استاکس‌نت باهدف قراردادن زیرساخت حیاتی جمهوری اسلامی ایران، فصل نوینی از عملیات سایبری را در دنیا گشود و توجه دولت‌های گوناگون را متوجه قدرت تسلیحات سایبری ساخت؛ تا جایی که برخی کشورها اقدام به بازبینی سیاست‌های دفاعی خود نمودند. تسلیحات سایبری با توانایی هدایت از راه دور، تمرکز بر هدف‌های خاص منظوره، دشواری رهگیری عامل بکارگیری، حذف یا کاهش چشمگیر تلفات انسانی و حتی قابلیت خودمختاری در برخی از آن‌ها، در خط مقدم جنگ‌های نوین قرارگرفته و باعث شده است آستانه اعمال قدرت سخت دولت‌ها، کاهش یابد.

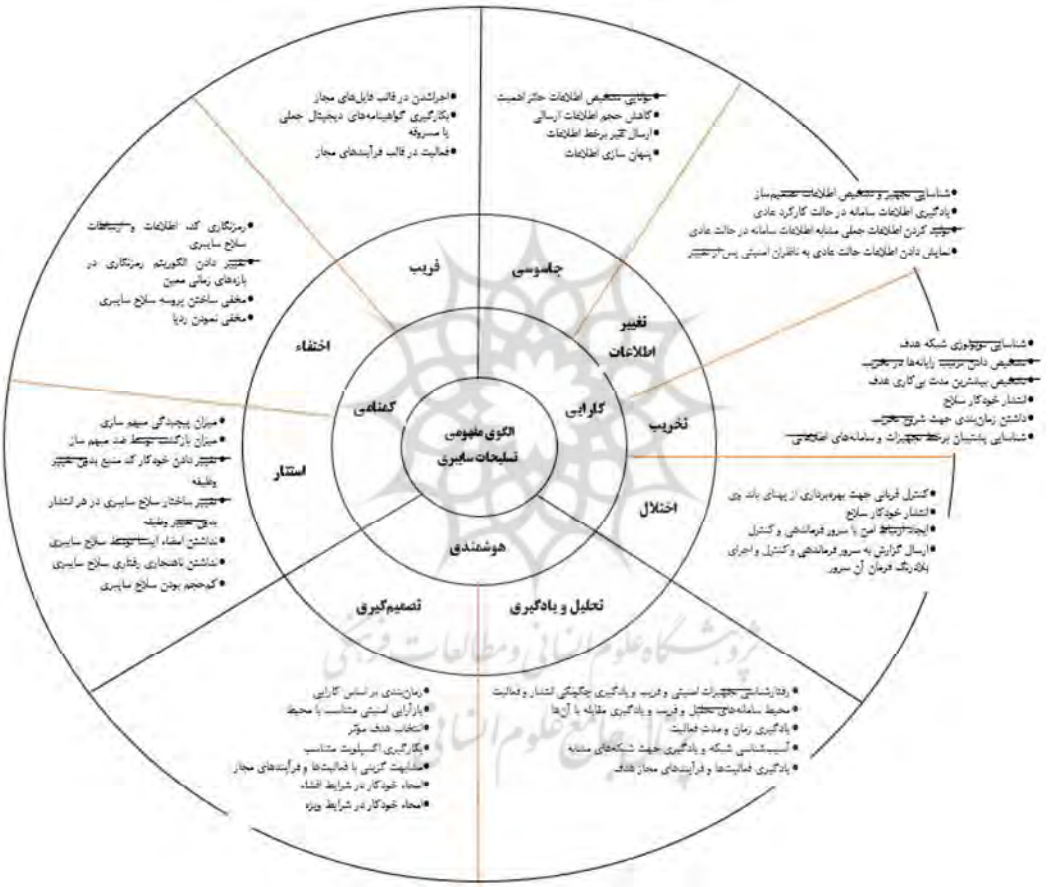
این مقاله با کمک ۸ خبره و ۷۱ کارشناس حوزه دفاع سایبری جمهوری اسلامی ایران، الگوی مفهومی تسلیحات سایبری را با ۳ بعد، ۹ مؤلفه و ۴۴ شاخص ارائه نمود. بر این اساس

---

۱. Decoder

۲. Downloader

تسلیحات سایبری دارای ابعاد کارایی، هوشمندی و گمنامی بوده و در بعد کارایی، دارای مؤلفه‌های جاسوسی، تغییر اطلاعات، تخریب و اختلال، در بعد هوشمندی، دارای مؤلفه‌های تحلیل و یادگیری و تصمیم‌گیری و در بعد گمنامی، دارای مؤلفه‌های استتار، اختفاء و فریب می‌باشند. بر اساس ابعاد، مؤلفه‌ها و شاخص‌های مورد تأیید خبرگان و کارشناسان، الگوی مفهومی تسلیحات سایبری به شرح شکل ۵ ارائه می‌گردد:



شکل ۴: الگوی مفهومی تسلیحات سایبری

پیشنهاد

با توجه به اینکه الگوی حاصل از این پژوهش در بالاترین سطح تسلیحات سایبری -یعنی سطح راهبردی- ارائه‌شده است؛ برای ادامه پژوهش می‌توان در سطوح عملیاتی و تاکتیکی نیز اقدام

به ارائه الگوی تسلیحات سایبری نمود.

همچنین جهت ادامه تحقیق حاضر می‌توان برای هر یک از ابعاد ارائه‌شده در الگو، اقدام به ارائه الگوی راهبردی، عملیاتی یا تاکتیکی نمود. به‌طور مثال می‌توان به الگوهای راهبردی، عملیاتی یا تاکتیکی هوشمندی تسلیحات سایبری و گمنامی تسلیحات سایبری اشاره کرد.

با توجه به خودمختاری برخی تسلیحات سایبری که آن‌ها را از نیروی انسانی عملیاتی بی‌نیاز کرده است، می‌توان به این تسلیحات پرداخت و ضمن بررسی ویژگی‌ها و هوش مصنوعی بکار رفته در این تسلیحات، الگوهایی در هر سطوح راهبردی و عملیاتی تهیه نمود.

با توجه به لزوم فرماندهی و کنترل در تولید، توسعه و بکارگیری تسلیحات سایبری، می‌توان به الگوی راهبردی فرماندهی و کنترل تسلیحات سایبری پرداخت و به چالش‌های این حوزه مانند امنیت تولید تسلیحات و امنیت عملیات سایبری پرداخت.

درنهایت، با توجه به ماهیت اکتشافی تحقیقات پیرامون مسائل تهاجمی سایبر و عدم انتشار اطلاعات بدلیل طبقه‌بندی محرمانه مباحث این حوزه، بندی پیشنهاد می‌شود به‌منظور ادامه این پژوهش، با همکاری متولیان حوزه دفاعی کشور، به طرح راهبردی مواجهه با تسلیحات سایبری پرداخته شود تا ضمن ایجاد بازدارندگی و انجام دفاع عامل سایبری ارتقاء قدرت سایبری جمهوری اسلامی ایران را در پی داشته باشد.

فهرست منابع

بارانی، ف. & سبزه کار، م. (۱۳۹۶). بررسی انواع روش های تشخیص بدافزارها و استراتژی های بدافزارها در مقابل آنها. چهارمین کنفرانس بین المللی یافته های نوین علوم و تکنولوژی . https://civilica.com/doc/۷۱۰۸۱۳

رحیم اف، ه. & موحدی صفت، م. ر. (۱۳۹۹). ارائه یک الگوی بومی برای امنیت فرماندهی و کنترل عملیات انکار سرویس توزیع شده. دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران . https://civilica.com/doc/۱۲۴۳۷۲۱

علی نژاد، میقانی، احمد، بوالحسنی، & رضایت. (۱۳۹۹). مقاله پژوهشی: طراحی الگوی آرایه‌های پدافند زمین به هوا در مقابله با تهدیدات علیه مراکز حیاتی و حساس در افق چشم‌انداز ۱۴۰۴ مطالعات دفاعی استراتژیک، ۱۸(۸۰), ۵۷–۸۲.

فریدون، ع. (۱۳۹۴). چگونگی بهره گیری از اصول (اختفا، فریب و استتار) در راستای دفاع در برابر سنجنده های دشمن. کنگره پیشگامان پیشرفت. http://fa.seminars.sid.ir/ViewPaper.aspx?ID=۵۶۴۹۵

مرکز آپا دانشگاه امیرکبیر. (۱۳۹۵). شفافیت گواهی، مدلی برای کشف گواهی‌های دیجیتال جعلی . Online. https://apa.aut.ac.ir/?p=۷۶۴

مقام معظم رهبری. (۱۳۹۴). حکم انتصاب دوره دوم اعضای شورای عالی فضای مجازی . https://farsi.khamenei.ir/message-content?id=

ALMAIAH, A. & ALMOMANI, O. (2020). An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response. *Journal of Theoretical and Applied Information Technology*, *98*(07).

Bakić, B. Milić, M. Antović, I. Savić, D. & Stojanović, T. (2021). 10 years since Stuxnet: What have we learned from this mysterious computer software worm? *2021 25th International Conference on Information Technology (IT)*, 1–4.

Bates, N. (2020). *Comparing Cyber Weapons to Traditional Weapons Through the Lens of Business Strategy Frameworks*.

Bellovin, S. M. Landau, S. & Lin, H. S. (2017). Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*, *3*(1), 59–68.

Buchan, R. & Tsagourias, N. (2020). Autonomous Cyber Weapons and Command Responsibility. *International Law Studies*, *96*(1), 21.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Enisa. (2020). *Main incidents in the EU and worldwide*.

Godwin III, J. B. Kulpim, A. Rauscher, K. F. & Yaschenko, V. (2014). Critical terminology foundations 2. *Russia-US Bilateral on Cybersecurity. Policy Report*, *2*, 2014.

Hore, S. & Raychaudhuri, K. (2021). Cyber Espionage-An Ethical Analysis. In M. K. Sharma, V. S. Dhaka, T. Perumal, N. Dey, & J. M. R. S. Tavares (Eds.), *Innovations in Computational Intelligence and Computer Vision* (pp. 34–40). Springer Singapore.

Kaloudi, N. & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1–34.

L. Ablon and A. Bogart. (2017). *Zero Days, Thousands of Nights The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. https://www.rand.org/pubs/research_reports/RR1751.html

Leavitt, N. (2011). Internet Security under Attack: The Undermining of Digital Certificates. *Computer*, *44*(12), 17–20. https://doi.org/10.1109/MC.2011.367

Leuprecht, C. Szeman, J. & Skillicorn, D. B. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, *40*(3), 382–407.

Lin, H. & Zegart, A. (2017). Introduction to the special issue on strategic dimensions of offensive cyber operations. *Journal of Cybersecurity*, *3*(1), 1–5.

Lin, H. & Zegart, A. (2019). *Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations*. Brookings Institution Press.

M. Hypponen. (2019). *Responding to a Cyber Attack with Missiles*. https://www.conferencecast.tv/talk-20213-responding-to-a-cyberattack-with-missiles

Maathuis, C. Pieters, W. & Van Den Berg, J. (2016). Cyber weapons: a profiling framework. *2016 International Conference on Cyber Conflict (CyCon US)*, 1–8.

Mezzour, G. Carley, K. M. & Carley, L. R. (2018). Remote assessment of countries' cyber weapon capabilities. *Social Network Analysis and Mining*, *8*(1), 1–15.

Oxford University Press. (2021). *Oxford Dictionary*. https://www.oxfordlearnersdictionaries.com/definition/english/oxford-university-press

Rid, T. & McBurney, P. (2012). Cyber-weapons. *The RUSI Journal*, *157*(1), 6–13.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Shoaib, M. (2020). AI-Enabled Cyber Weapons and Implications for Cybersecurity. *Journal of Strategic Affairs*.

Smeets, M. (2018). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, *41*(1–2), 6–32.

Zion Market Research. (2021). *The global Cyber Weapon market*. https://www.zionmarketresearch.com/news/cyber-weapon-market