Strategy
Center for Strategic Research
https://rahbord.csr.ir E-ISSN: 2588-6525
Vol. 32, No. 3, Issue. 108, Autumn 2023 **Received:** 2023/11/28 **Accepted:** 2023/12/21
Research paper

Redesigning and Updating Cyber Defense Strategies Based on the NATO Security Model

Mostafa Esmaili
Assistant Professor in International Relations, Supreme National Defense University, Tehran, Iran(Corresponding Author).
Email: esmaili133@gmail.com 0000-0002-3215-5256
Amir Abbas Rokni
Ph.D. Student in National Security, Supreme National Defense University, Tehran, Iran.
Email: Amir.roknni@gmail.com 0000-0002-0700-4624

Abstract
In recent years, the recognition of cyberspace as an emerging military domain has prompted significant changes in the approaches of countries and organizations to the concept of cyberdefense. NATO, as an international military organization, has also been impacted by this process and has undertaken the task of updating and redesigning its cyber defense strategy for nearly a decade. The purpose of this article is to investigate the impact of identifying cyberspace as a new military domain on NATO's cyber defense strategy and to analyze these effects descriptively. The findings of this research indicate that recognizing cyberspace as a new military domain has significantly influenced NATO's cyber defense strategy in recent years. NATO has developed new policies and frameworks to address cyber threats and has substantially increased its investments in strengthening cyber defense capabilities. Moreover, ensuring the security of cyberspace, as a fundamental aspect of creating an effective cyber defense strategy, has played a prominent role in realizing the principle of NATO's collective defense in the cyber domain. Given the importance and necessity of updating cyber defense strategies based on current requirements and complexities in this field, the results of this research can be a valuable resource for policymakers, military commanders, and researchers active in the field of cyber defense in the Islamic Republic of Iran to make innovative decisions and develop effective strategies in this area.

Keywords: Cyber Space, NATO, cyber defense, cyber security.

doi 10.22034/RAHBORD.2024.427447.1624

سال سی و دوم، شماره سوم (پیاپی ۱۰۸)، پاییز ۱۴۰۲، صص. ۳۵۷- ۳۸۲
تاریخ دریافت: ۱۴۰۲/۰۹/۰۷ ـ تاریخ پذیرش: ۱۴۰۲/۰۹/۳۰

مقاله پژوهشی

بازطراحی و به‌روزرسانی راهبردهای دفاع سایبری بر اساس الگوی امنیتی ناتو

مصطفی اسماعیلی
استادیار گروه روابط بین‌الملل، دانشگاه عالی دفاع ملی، تهران، ایران (نویسنده مسئول).
Email: esmaili133@gmail.com 0000-0002-3215-5256
امیرعباس رکنی
دانشجوی دکتری امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران.
Email: Amir.roknni@gmail.com 0000-0002-0700-4624

چکیده

در سال‌های اخیر، به رسیمت‌شناختن فضای سایبری به‌عنوان یک عرصه نظامی نوپدید، منجر به تغییرات چشمگیری در رویکرد کشورها و سازمان‌ها به مفهوم دفاع سایبری شده است. ناتو به‌عنوان یک سازمان نظامی بین‌المللی نیز تحت تأثیر این روند قرارگرفته است و نزدیک به یک دهه است که فرایند به‌روزرسانی و بازطراحی راهبرد دفاع سایبری خود را آغاز نموده است. هدف از مقاله حاضر، بررسی تأثیر شناسایی فضای سایبری به‌عنوان یک عرصه نظامی نوپدید بر راهبرد دفاع سایبری ناتو و است که به روش توصیفی - تحلیلی صورت گرفته است. یافته‌های این پژوهش نشان می‌دهد که به رسیمت‌شناختن فضای سایبری به‌عنوان یک عرصه نظامی نوپدید تأثیرات قابلِ‌توجهی بر راهبرد دفاع سایبری ناتو در طول سال‌های اخیر داشته است. ناتو، سیاست‌ها و چهارچوب‌های جدیدی را برای مقابله با تهدیدات سایبری ایجاد کرده و سرمایه‌گذاری‌های خود را در تقویت قابلیت‌های دفاع سایبری به‌شدت افزایش داده است. علاوه بر این، امنیتی‌سازی فضای سایبری به‌عنوان یکی از ضرورت‌های ایجاد یک راهبرد دفاع سایبری مؤثر، نقش برجسته‌ای در تحقق اصل دفاع جمعی ناتو در بستر سایبر داشته است. با توجه به اهمیت و ضرورت به‌روزرسانی استراتژی‌های دفاعی در فضای سایبری، براساس مقتضیات کنونی و پیچیدگی‌های حاکم بر این عرصه، نتایج پژوهش حاضر می‌تواند برای سیاست‌گذاران، فرماندهان نظامی و محققان فعال در حوزه دفاع سایبری جمهوری اسلامی ایران، منبعی ارزشمند برای اتخاذ تصمیمات نوآورانه و تدوین راهبردهای مؤثر در این حوزه باشد.

کلیدواژه‌ها: فضای سایبری، ناتو، دفاع سایبری، امنیت سایبری.

شاپای الکترونیک: ۶۵۲۵-۲۵۸۸/ پژوهشکده تحقیقات راهبردی/ فصلنامه علمی راهبرد

10.22034/RAHBORD.2024.427447.1624

مقدمه و بیان مسئله

پیشرفت سریع اینترنت و فناوری‌های مبتنی بر آن و وابستگی روزافزون تمام ساحات زندگی بشری به این فضا، تهدید علیه امنیت سایبری را به یک نگرانی جدی برای دولت‌ها و سازمان‌های بین‌المللی در سرتاسر جهان تبدیل کرده است. دراین راستا، ناتو به‌عنوان یک ائتلاف نظامی که مسئولیت حفاظت از کشورهای عضو خود را دارد، گام‌های مهمی در جهت ارتقای قابلیت‌های دفاع سایبری خود برداشته است. یکی از تحولات مهم در این زمینه، به رسمیت‌شناختن فضای سایبری به‌عنوان یک عرصه نظامی نوپدید در اجلاس سران ناتو در سال ۲۰۱۴ در کشور ولز است. این اقدام، تغییرات قابلِ‌توجهی در رویکرد امنیتی و راهبرد دفاع سایبری این سازمان داشته است.

به رسمیت‌شناختن فضای سایبری به‌عنوان یک عرصه نظامی نوپدید، راه‌های جدیدی را برای ناتو جهت تقویت استراتژی دفاع سایبری خود بازکرده است و پرسش اساسی این پژوهش نیز از همین نقطه آغاز می‌شود که اساساً این اقدام چگونه بر روند بازطراحی و به‌روزرسانی راهبردهای دفاع سایبری ناتو تأثیر گذاشته است؟ پاسخ به این سؤال بسیار مهم، زیرا بینش‌هایی در مورد اثربخشی پاسخ ناتو به تهدیدات سایبری و توانایی این سازمان برای محافظت از کشورهای عضو خود در دوران جنگ‌های نوپدید ارائه می‌دهد.

بررسی ادبیات پژوهشی و پیشینه این موضوع نشان می‌دهد که اقدام ناتو، یک نقطه عطف مهم در تاریخ تدوین راهبردهای دفاع سایبری در جهان است. ناتو اکنون در راستای این اقدام، با به‌روزرسانی سیاست‌های دفاع سایبری، ایجاد ساختارها و قابلیت‌های جدید و متوازن در تمامی اعضای خود و انجام رزمایش‌های سایبری متعدد سالیانه سعی در تحقق اصل دفاع جمعی در فضای سایبری دارد. البته این سازمان، نیازمند آن است که با توجه به ماهیت متغیر فضای سایبر، راهبرد دفاعی خود را به شکل پیوسته تغییرداده و با تهدیدات درحالِ‌تحول، تطبیق دهد.

علاوه بر این، اثربخشی استراتژی دفاع سایبری ناتو نیز به سطح همکاری و به اشتراک‌گذاری اطلاعات میان کشورهای عضو بستگی دارد که می‌تواند با ملاحظات سیاسی و دیپلماتیک مختلفی همراه باشد.

با توجه به مطالب ذکرشده، درک تأثیر شناسایی فضای سایبری به‌عنوان یک عرصه نظامی بر بازطراحی و به‌روزرسانی راهبرد دفاع سایبری ناتو بسیار مهم است.

پژوهش حاضر با تحلیل و مرور اقدامات انجام‌شده در سال‌های اخیر پیرامون این حوزه، به بررسی و واکاوی آثار این ابتکار نظامی سیاسی جدید می‌پردازد.

۱. مبانی نظری پژوهش

حوزه دفاع سایبری یک حوزه پیچیده و به‌سرعت درحالِ‌تحول است. به‌منظور درک و اتخاذ استراتژی‌های کارآمد در حکمرانی بر فضای سایبری، داشتن درک روشن و دقیق از مفاهیم و اصطلاحات مختلف مرتبط با این حوزه بسیار مهم است. مبانی نظری پژوهش، تعریف جامعی از اصطلاحات کلیدی در حوزه دفاع سایبری ارائه می‌کند پژوهش حاضر به‌دنبال کشف چرایی شناسایی فضای سایبری به‌عنوان یک عرصه نظامی توسط ناتو و اقداماتی است که این سازمان برای به‌روزرسانی و طراحی مجدد الگوی دفاع سایبری خود انجام داده است. برای درک صحیح و کامل اهمیت اقدامات ناتو، داشتن شناختی روشن از اصطلاحات و مفاهیم کلیدی حوزه دفاع سایبری مهم است. این بخش با بررسی عمیق این مفاهیم و با بررسی ادبیات آکادمیک موجود در این زمینه، مبانی نظری تحقیق را ارائه خواهد داد.

۱-۱. امنیتی‌سازی فضای سایبر

با فروپاشی اتحاد جماهیر شوروی و سرنگونی حکومت‌های کمونیستی بلوک شرق، استراتژی‌های امنیتی قاره اروپا دستخوش تغییراتی بنیادین شد. بسیاری از اندیشمندان و صاحب‌نظران حوزه امنیت بر این باور هستند که فروریختن دیوار حائل میان شرق و غرب اروپا، نقطه عطفی مهم در تحولات امنیتی نه‌تنها اروپا بلکه در سرتاسر جهان است. تا پیش‌ازاین، مفهوم امنیت ملی در بسیاری از کشورهای جهان در راستای اتکای صرف به قدرت نظامی و توسعه تجهیزات بازدارنده جنگی تعریف می‌شد. این دیدگاه رئالیستی درباره امنیت ملی، آن را به مفهوم تک‌بعدی تبدیل کرده بود که در نظامی‌گری خلاصه می‌شد. از ابتدای دهه هشتاد میلادی، رفته‌رفته ناکارآمدی و ضعف نظریات رئالیستی درباره امنیت ملی آشکار گردید. در طول همین دهه، تعدادی از نظریه‌پردازان حوزه روابط بین‌الملل و امنیت ملی در «مؤسسه تحقیقات صلح کپنهاگ»[1] مشغول به طراحی و ساخت استراتژی جدید

1. Copenhagen Peace Research Institute

امنیتی قاره اروپا بودند. «بری بوزان»[1]، استاد روابط بین‌الملل دانشگاه اقتصاد لندن[2] به‌عنوان شاخص‌ترین نظریه‌پرداز این نظم جدید، مکتب امنیتی نوینی را پایه‌گذاری کرد که به «مکتب امنیتی کپنهاگ»[3] مشهور شد.

آموزه‌های مکتب کپنهاگ، سیاست امنیتی بسیاری از کشورهای جهان را تحت تأثیر خود قرارداد، اما اثرگذاری آن بیش از همه بر کشورهای اروپایی مشهود است. بری بوزان، به‌عنوان مغز متفکر این مکتب در اولین قدم، امنیت تک‌ساحتی را نفی کرد و اعلام نمود که امنیت مفهومی چندبُعدی است.

او برای امنیت ملی قائل به پنج بُعد نظامی، سیاسی، اقتصادی، اجتماعی و زیست‌محیطی است. بوزان در شاخص‌ترین اثر خود با نام «مردم، دولت‌ها و هراس»[4] به شرح و توضیح ابعاد پنج‌گانه امنیت ملی پرداخته و برداشت‌های سنتی از امنیت را بسیار مضیق می‌داند (بوزان، ۱۳۹۹، ص. ۱۲۳). نتیجه مهمی که از این تقسیم‌بندی به دست آمد، توجه و اولویت‌دادن به دیگر ابعاد امنیت و درک اثرگذاری مستقیم این ابعاد بر همدیگر بود. مکتب کپنهاگ، در ادامه تکمیل فرایند نظریه‌پردازی خود، مفاهیم جدیدی نیز به حوزه مطالعات امنیتی وارد کرد. بوزان و همکارانش در یکی دیگر از آثار مهم خود بانام «چهارچوبی تازه برای تحلیل امنیت»[5] از مفهومی با نام «امنیتی‌سازی»[6] سخن به میان آورد. این مفهوم مهم، نقش بسزایی در وسعت‌بخشیدن به فهم حکمرانان از امنیت و همچنین ارائه چهارچوبی برای تحلیل چگونگی امنیتی‌سازی یک موضوع داشته است. بوزان در کتاب مذکور کار خود را با تعریف امنیت بین‌المللی در بافت نظامی سنتی آغاز می‌کند. از دید او و همکارانش، امنیت موضوعی درخصوص بقا است و زمانی کانون توجه قرار می‌گیرد که یک موضوع به‌عنوان «تهدید وجودی»[7] برای یک مرجع امنیتی مطرح می‌شود. این مرجع امنیتی به‌طور سنتی و نه ضرورتاً، دولت است که متشکل از سرزمین، حکومت و جامعه است. مکتب کپنهاگ با در نظرگرفتن این موضوع، امنیت را به پنج دسته پیش‌گفته تقسیم می‌کند؛ درنتیجه منطق امنیت - بقا حفظ می‌شود و چهار بعد دیگر نیز به امنیت نظامی افزوده می‌شود. کنشگران امنیتی‌ساز و مرجع‌های امنیت

1. Barry Buzan
2. London School of Economics
3. The Copenhagen School of security studies
4. People, States & Fear
5. Security: A New Framework for Analysis
6. Securitization
7. Existential threat

تعیین‌کننده این پنج بعد امنیتی هستند. کنشگر امنیتی با اعلام اینکه یک مرجع امنیتی به لحاظ وجودی مورد تهدید قرارگرفته است، آن چیز را امنیتی می‌کند. رهبران سیاسی، حکومت‌ها، نظریه‌پردازان، لابی‌گرها و گروه‌های فشار از مهم‌ترین کنشگران امنیتی‌ساز نظم‌های امنیتی هستند (کالینز، ۱۳۹۹، ص. ۱۹۰).

بر همین اساس، مکتب کپنهاگ طیفی را ترسیم می‌کند که هر مسئله عمومی را می‌توان روی آن جای داد. نقطه آغاز این طیف، امور غیرسیاسی است که دولت با آن سروکار ندارد و از هیچ راه دیگری هم موضوع بحث و تصمیم‌گیری همگانی قرارنمی‌گیرد. در میانه این طیف، امور سیاسی قرار می‌گیرد که بخشی از سیاست‌گذاری همگانی است و مستلزم تصمیم‌گیری و تحصیل منابع از سوی دولت یا به شکلی نادرتر نیازمند گونه‌های دیگری از اداره جمعی است. درنهایت، در انتهای این طیف، امور امنیتی قرار دارد که همچون تهدیدی وجودی جلوه می‌کند و نیازمند اتخاذ تمهیدات اضطراری است و انجام اقداماتی در بیرون از مرزهای عادی رویه سیاسی را موجه می‌سازد. در اصل جایگاه یک مسئله بر روی این طیف ثابت و قطعی نیست و بسته به اوضاع‌واحوال، هر مسئله می‌تواند روی هر بخشی از طیف جای بگیرد. اگر بتوان گفت که مسئله‌ای از منطق معمول سیاسی که سبک و سنگین‌کردن مسائل است درمی‌گذرد باید تهدیدی وجودی باشد، زیرا می‌تواند کل فرایند سبک و سنگین‌کردن را بر هم بزند: «اگر به این مسئله نپردازیم پرداختن به هر امر دیگری بی‌مورد خواهد بود، زیرا دیگر وجود نخواهیم داشت یا آزاد نخواهیم بود که چنان‌که می‌خواهیم با آن برخورد کنیم». بدین ترتیب کنشگر امنیتی‌ساز مدعی می‌شود که حق دارد با مسئله مورد بحث با توسل به وسایل فوق‌العاده برخورد کند و قواعد بازی سیاسی را بشکند. امنیت، رویه‌ای مرجع و معطوف به خود است؛ زیرا طی خود این رویه است که مسئله‌ای را به یک مسئله امنیتی مبدل می‌کند (بوزان، ۱۳۹۹). مکتب کپنهاگ در بیشتر مواقع رهیافتی اروپا محور تلقی می‌شود؛ رهیافتی که بازتاب‌دهنده موضوع‌ها و نگرانی‌های امنیتی اروپا است (کالینز، ۱۳۹۹، ص. ۲۰۱). آموزه‌های این مکتب، با برجسته‌سازی سطح تحلیل امنیت منطقه‌ای تأثیر قابلِ‌توجهی بر استراتژی امنیتی اروپای پس از جنگ سرد گذاشت. در پارادایم امنیتی جدید اروپا، با گره‌خوردن امنیت تمامی کشورهای این قاره به همدیگر، مفهوم امنیت ملی جای خود را به امنیت جمعی داده است (جمشیدی و همکاران، ۱۳۹۹، ص. ۱۱۱).

بر همین مبنا، هرچند پیشینه بسیاری از پیمان‌ها و توافق‌نامه‌های یکپارچه‌ساز اروپایی به سال‌های آغازین دهه پنجاه میلادی و پس از جنگ دوم جهانی بازمی‌گردد، بااین‌وجود، قطب‌بندی میان شرق و غرب و آغاز جنگ سرد مانع تحقق اهداف این پیمان‌ها گردید. از سوی دیگر، ملاحظه‌ای تاریخی نشان می‌دهد که هدف اولیه بسیاری از توافقات اتفاق‌آفرین در اروپا مبنای اقتصادی داشته است. بارزترین گواه این ادعا، توافق‌نامه رم در ۲۵ مارس ۱۹۵۷ بین کشورهای فرانسه، آلمان غربی، ایتالیا، بلژیک، هلند و لوکزامبورگ است که در شهر «رم» به امضا رسید و منجر به تشکیل جامعه اقتصادی اروپا شد (Deschamps, 2016).

با فروریختن دیوار برلین در سال ۱۹۸۹ میلادی، شاهد آن هستیم که اروپا به شکل عملی به سمت یک امنیت منطقه‌ای تغییر جهت می‌دهد. «پیمان ماستریخت»[1] در تاریخ ۷ فوریه ۱۹۹۲، اصلی‌ترین گام اروپا در این خصوص به‌حساب می‌آید. این پیمان که در کشور هلند به امضا رسید، منجر به تشکیل «اتحادیه اروپا»[2] شد. در کنار دستاوردهای مهمی چون توافق بر سر ایجاد پول مشترک (یورو)، دستگاه قضایی مشترک (یورو جاست)[3] و پلیس مشترک (یورو پُل)[4]، توافق بر سر سیاست امنیتی مشترک، به‌عنوان یکی از ستون‌های اصلی پیمان ماستریخت شناخته می‌شود (هریسی‌نژاد، ۱۳۷۴، ص. ۱۴۷). از این مقطع زمانی به بعد، اروپا با جمع‌سپاری کار ویژه امنیت که همان حفاظت اعضای اتحادیه از تهدیدات وجودی است، تحت تأثیر آموزه‌های امنیتی مکتب کپنهاگ، دستور کار جدیدی برای بازوی نظامی خود یعنی سازمان ناتو تعریف کرده است. نکته مهم دیگری که در اینجا لازم به ذکر است، تحولات عمیق بعد نظامی امنیت در نظم امنیتی جدید است. در این شرایط، بعدی نظامی امنیت با فاصله‌گرفتن از معنای سنتی خود افق‌های جدیدی پیش‌رِوی دارد و بسیاری از امور محوله‌ای که تا پیش‌ازاین امنیتی‌سازی شده و در حوزه فعالیت آن قرار می‌گرفت، از طیف امنیتی خارج‌شده و موضوعات جدیدی جای آن‌ها را گرفته است.

1. Maastricht Treaty
2. European Community
3. Eurojust
4. Euro Pool

۱-۲. امنیت سایبری؛ ویژگی‌ها و ملزومات

امنیت سایبری عبارت است از مجموعه اقدامات پیشگیرانه استراتژیک در فضای سایبر. اهمیت عنصر پیشگیری در امنیت سایبری ازآن‌جهت است که یک استراتژی امنیتی از رایانه‌ها، سرورها، دستگاه‌های الکترونیک شبکه‌ها و داده‌ها پیش از وقوع یک حمله مخرب دفاع کرده و در صورت وقوع حمله در بدترین سناریوی مفروض آسیب‌های ناشی از آن را به حداقل ممکن کاهش می‌دهد (Shea, 2023).

امنیت سایبری اولین شرط برای فراهم‌ساختن بستر رشد و پیشرفت فناوری در جهانِ حال حاضر است. امروزه، تمام عناصر زندگی انسان به نحوی با فضای مجازی در ارتباط است و محافظت مداوم از این بستر از ضروریات «سبک زندگی اینترنتی»[1] است.

ازنظر استراتژیک، کارشناسان بر این باور هستند که تداوم تاب‌آوری زیرساخت‌های فضای سایبر از اهمیت اساسی برخوردار است. بنا بر آموزه‌های مکتب کپنهاگ، امنیت موضوعی در خصوص بقا است و زمانی کانون توجه قرار می‌گیرد که یک موضوع به‌عنوان تهدید وجودی برای یک مرجع امنیتی مطرح شود. با افزایش دامنه نفوذ فضای مجازی در زندگی اجتماعی، تهدیدات سایبری همان‌گونه که پیش‌تر مورد اشاره قرارگرفت به‌عنوان یک تهدید وجودی علیه این مرجع نوظهور امنیتی خود را نمایان کرده و روزبه‌روز به‌شدت آن‌ها افزوده می‌شود. درنتیجه مضاف بر تأمین امنیت، تداوم امنیت و تاب‌آوری مرجع امنیت نیز باید موردتوجه قرار بگیرد. مشخصاً در این حوزه از سیاست‌گذاری، سطح تحلیل امنیت فراتر از فرد و یک شرکت خاص قرار می‌گیرد (هرچند که تأمین امنیت آن‌ها نیز مهم است) و سطوح ملی و منطقه‌ای مد نظر است. پس در چنین مقیاسی از سیاست‌گذاری امنیت سایبری را باید به‌مثابه یک استراتژی و هم‌زمان یک «چهارچوب عملیاتی»[2] در نظر گرفت، موضوعی که جایگاه خود را به‌عنوان عنصری اساسی در تمام ابعاد سیاسی، اجتماعی، اقتصادی، نظامی و زیست‌محیطی امنیت تثبیت کرده است (Efthymiopoulos, 2019, p. 23).

تاب‌آوری به‌عنوان یکی از ویژگی‌های اصلی امنیت سایبری در تمام سطوح امنیت باید ایجاد گردد. بر همین اساس، نظام‌های امنیتی در سطوح مختلف (ملی و منطقه‌ای) سعی در ایجاد و تقویت تاب‌آوری امنیت سایبری می‌کنند.

1. Internet lifestyle
2. Operational framework

درحال‌حاضر، در منطقه اروپا نیاز به یک ظرفیت استراتژیک و عملیاتی برای ایجاد این تاب‌آوری به‌شدت احساس می‌شود. ناتو به‌عنوان بازوی نظامی اتحادیه اروپا مأمور انجام این وظیفه است. ویژگی‌های ذاتی ناتو به‌عنوان یک اتحاد دفاعی، آن را به چهارچوبی برای تداوم امنیت در بعد سایبری تبدیل کرده است. این امر به تقویت ارتباط متقابل و تقویت تلاش‌های امنیتی برای مقابله با تهدیدهای امنیتی متقارن و نامتقارن کمک خواهد کرد.

ازآنجاکه امنیت ملی و استراتژی‌های دفاعی امروزه به‌شدت به پروتکل‌های امنیت سایبری و پیاده‌سازی آن متکی هستند، در نظرگرفتن سطح چندبعدی تهدیدها و چالش‌های فضای سایبر و تجزیه‌وتحلیل آن‌ها به حصول امنیت و فراهم‌ساختن سازوکارهای پیشرفت فناوری‌های دفاعی کمک شایان توجهی می‌کند. برای مناطقی همچون اروپا که همتافت‌های امنیتی در آن به‌شدت متکی به همدیگر هستند، تجزیه‌وتحلیل تهدیدها و چالش‌ها در حد ملی کافی نیست؛ آنچه منجر به ایجاد امنیت سایبری در این منطقه می‌شود یک رویکرد مشترک پیوسته برای استراتژی امنیت سایبری در قالب دفاع جمعی است. این استراتژی یک چهارچوب سیاسی و نظامی کارآمد برای کشورهای عضو اتحاد فراهم می‌کند؛ اما پیش‌نیازهای دستیابی به این سطح ایدئال از امنیت، ازجمله امنیتی‌سازی تهدیدات سایبری، ایجاد یک ساختار قانونی برای اقدام و عمل و همچنین انطباق دستورالعمل‌های امنیت سایبری با موازین قانونی یکپارچه اتحادیه اروپا، خود اصلی‌ترین چالش پیش‌روی ناتو در این سال‌های اخیر بوده است. سران کشورهای عضو ناتو در طول دو دهه اخیر به همین منظور اجلاس‌های مهمی تشکیل داده‌اند و ضمن صرف بودجه‌های اختصاصی قابل‌توجه، پروژه‌های تحقیقاتی متعددی برای ایجاد یک سند دفاعی در حوزه سایبری انجام داده‌اند. در ادامه به بررسی مسیری که سازمان پیمان آتلانتیک جنوبی از نخستین تجربه حمله سایبری به یکی از اعضای خود تا امروز طی کرده است، پرداخته خواهد شد.

۱-۳. دستور کار دفاع جمعی

اصل دفاع جمعی، شاکله بنیان‌گذاری سازمان ناتو است. این یک اصل منحصربه‌فرد است که اعضای این پیمان نظامی را به همدیگر متصل کرده، آن‌ها را به امنیت همدیگر متعهد کرده، روحیه همبستگی در اتحاد ایجاد کرده و از کشورهای عضو،

یک هم‌تافت امنیتی ساخته است. پیشینه ایجاد اصل دفاع جمعی به سال ۱۹۴۹ بازمی‌گردد که در آن هسته اولیه تشکیل ناتو به‌دنبال راهی برای مواجهه با سلطه افکنی اتحاد جماهیر شوروی بر سرتاسر جهان بود. ماده ۵ تصریح می‌کند که چنانچه یکی از اعضای سازمان ناتو قربانی حمله نظامی یک دولت متخاصم قرار بگیرد، تمامی اعضای دیگر این اقدام مسلحانه را حمله علیه خود تلقی کرده و اقدامات مقتضی (اعم از نظامی و پشتیبانی) جهت کمک به عضو قربانی انجام می‌دهند. ماده ۶ اساس‌نامه به‌عنوان مکمل ماده ۵ بیان می‌دارد که یک حمله مسلحانه به یکی از دولت‌ها این موارد را در برمی‌گیرد:

- در قلمرو هر یک از دولت‌ها در اروپا یا آمریکای شمالی، در قلمرو جزایر تحت حاکمیت فرانسه، در قلمرو یا در جزایری که تحت صلاحیت قانونی هر یک از دولت‌ها در منطقه آتلانتیک شمالی در مدار رأس‌السرطان قرار می‌گیرند.
- علیه نیروها، کشتی‌ها و یا هواپیماهای هر یک از دولت‌ها، زمانی که در این مناطق یا هر منطقه دیگری در اروپا که نیروهای تصرف‌کننده هر یک از دولت‌ها در تاریخ لازم‌الاجراشدن این پیمان مستقر هستند یا در دریای مدیترانه و یا منطقه آتلانتیک شمالی در شمال مدار رأس‌السرطان.

ماده ۹ اساس‌نامه نیز اشاره می‌دارد که دولت‌های عضو موظف هستند شورایی تأسیس کنند که همه آن‌ها در آن نمایندگانی داشته تا مسائل مربوط به اجرای مفاد پیمان مورد توجه و رسیدگی قرار بگیرد. این شورا باید به نحوی سازمان‌دهی شود تا بتواند در هرزمانی بلافاصله تشکیل جلسه دهد. این شورا ارکان دیگر موردنیاز را تأسیس خواهد نمود؛ خصوصاً شورا به‌فوریت یک کمیته دفاعی تشکیل خواهد داد که اقدامات مقتضی جهت اجرای مواد ۳ و ۵ را توصیه می‌نماید.

کمک‌هایی که متحدان به قربانی حملات نظامی انجام می‌دهند لزوماً نظامی نیست و به منابع مادی هر کشور عضو بستگی دارد؛ بنابراین، تعیین نحوه مشارکت هر عضو در فرایند دفاع جمعی به خود آن کشور واگذار می‌شود. هر کشور عضو در مشورت با دیگر اعضا باید این نکته مهم را در نظر داشته باشد که هدف غایی سازمان، حفاظت و صیانت از امنیت منطقه آتلانتیک شمالی است.

تابه‌حال به درخواست دولت ترکیه، ناتو چندین اقدام مبتنی بر اصل دفاع جمعی انجام داده است. در سال ۱۹۹۱ در طول جنگ خلیج‌فارس، سامانه موشک‌های

پاتریوت در این کشور استقرار یافت. در سال ۲۰۰۳ و در طول بحران‌های جنگ عراق، ناتو یک بسته دفاعی آماده کرد و چندین عملیات بازدارنده انجام داد. همچنین، در سال ۲۰۱۲ و در طول بحران سوریه، چندین سامانه موشکی دیگر در واکنش به بحران‌های خاورمیانه توسط ناتو در ترکیه مستقر شد(NATO, 2021).

از سال ۲۰۱۴ و به‌دنبال تشدید منازعات میان اکران و روسیه، افزایش چالش‌های امنیتی در خاورمیانه و ظهور داعش در چندین قاره، ناتو بزرگ‌ترین تحرکات مبتنی بر اصل دفاع جمعی را از زمان جنگ سرد تاکنون انجام داده است. نیروهای واکنش سریع این سازمان را به ۳ برابر افزایش داده است، یک واحد نظامی چندملیتی متشکل از ۵،۰۰۰ سرباز در استونی، لتونی، لیتوانی و لهستان مستقر کرده است. همچنین حضور نظامی خود را در جنوب شرقی اتحاد به‌شدت افزایش داده است و چندین تیپ نظامی پیشرفته در رومانی مستقر کرده است. گشت‌های هوایی و پروژه «چشم‌های آسمان ناتو»[1] که شاملِ برنامه هشدار و کنترل اولیه هوابرد ناتو است را به‌عنوان یکی از موفق‌ترین اقداماتی مشارکتی چندملیتی برای حفظ امنیت آسمان اجرا کرده است(napma, 2021) . در طول یک دهه اخیر، ناتو اقدامات متعددی در خصوص تسری امنیت سایبری به ماده ۵ اساس‌نامه انجام داده است تا با به رسمیت‌شناسی آن به‌عنوان یک بستر عملیاتی جدید، بتواند از امنیت زیرساخت‌های اینترنتی، شبکه‌ها و سامانه‌های خود محافظت کند و در این فضا به عملیات بپردازد.

۲. فرایند تکامل مفهوم دفاع سایبری در ناتو

گسترش سریع قلمرو سایبری و کاربردهای مبتنی بر آن در تمامی ابعاد زندگی بشر، منشأ عصر نوینی از جنگ‌های مدرن گردیده است. تشدید شیوع و پیچیدگی حملات سایبری، لزوم اتخاذ استراتژی‌های دفاعی کارآمدتر را برای دولت‌ها و سازمان‌های نظامی اجتناب‌ناپذیر ساخته است. ناتو، به‌عنوان یک ائتلاف نظامی مقتدر، در پیشگامی تلاش‌ها برای صیانت و حمایت از کشورهای عضو خود در برابر تهدیدات سایبری قرار دارد. شناسایی قلمرو سایبری به‌عنوان یک قلمرو نظامی نوین توسط این سازمان، گامی مهم در جهت به‌روزرسانی و بازطراحی نقشه راه دفاع سایبری بود.

1. NATO's 'Eye In The Sky'

این امر منجر به اجرای اقدامات و ابتکارات متعددی گردید که هدف آن‌ها ارتقای توانایی ناتو در پاسخگویی به تهدیدات سایبری است.

در سال ۲۰۱۴، سازمان پیمان آتلانتیک شمالی (ناتو) در اجلاس ولز، با هدف بررسی و به‌روزرسانی استراتژی دفاع سایبری سازمان، تشکیل شد. اجلاس ولز در سال ۲۰۱۴، نقطه عطفی در تلاش‌های ناتو برای ادغام ملاحظات سایبری در استراتژی دفاعی خود بود. این اجلاس با پذیرش تعمیم قوانین جنگی موجود به قلمرو سایبری و شناسایی قابلیت اعمال ماده ۵ معاهده ناتو در مورد حملات سایبری ویرانگر، گام‌های مهمی در جهت تقویت امنیت سایبری این ائتلاف برداشت. اگرچه آستانه دقیق برای فعال‌شدن اقدامات دفاع جمعی ناتو هنوز مشخص نیست، اما این اجلاس نقطه شروع یک نقشه راه جدید برای توسعه و تقویت توانمندی‌های سایبری این ائتلاف بود. همچنین، این اجلاس بر ضرورت توسعه و حمایت از نیروهای سایبری متخصص، به‌عنوان یک شکاف مهم در توانمندی‌های ناتو، تأکید کرد.

اجلاس ولز در سال ۲۰۱۴، زمینه‌های لازم را برای پیشرفت‌های قابلِ‌توجه درزمینه مسائل سایبری فراهم کرد. اجلاس ورشو در سال ۲۰۱۶، با تداوم این پیشرفت‌ها، به بلوغ بسیار بیشتری در این زمینه دست‌یافت. قلمرو سایبری، همانند هوا، زمین یا دریا، به‌عنوان یک حوزه عملیاتی رسمی شناخته شد. این امر منجر به تأسیس مرکز عملیات سایبری ناتو در «شهر مون» بلژیک شد که فعالیت‌های سایبری اتحاد را درزمینه‌های هشدار اولیه، برنامه‌ریزی، تمرینات و تأمین سازگاری هماهنگ می‌کند. ظهور جنگ هیبریدی باعث شد سایبر به‌طور فزاینده‌ای با ابزارهای نظامی متعارف برای دشمنانی مانند روسیه مرتبط شود. اطلاعات نیز از طریق کمپین‌های جعلی خبری و مداخله در انتخابات به سلاح تبدیل شد. در نتیجه، رویکرد امنیتی ۳۶۰ درجه‌ای طراحی شد تا به اعضای ناتو در تقویت آسیب‌پذیری‌های اجتماعی فراتر از قدرت سخت سنتی کمک کند. اما اجلاس ورشو همچنین نشان داد که بین متحدان ناتو درزمینه اولویت‌ها، سیاست‌ها، ساختارها، توانمندی‌ها و فرهنگ‌های سایبری ناهمگونی‌هایی وجود دارد که می‌تواند دفاع جمعی را تضعیف کند. درحالی‌که تلاش‌هایی برای ایجاد درک مشترک از تهدیدات سایبری و هماهنگی بیشتر پاسخ‌ها در حال انجام بود، چالش‌هایی همچنان وجود داشت. در ورشو، اختلافاتی در مورد مسائلی مانند مسئولیت‌های سایبری تهاجمی و

مدل‌های تعامل با شرکای فاقد منابع یا آگاهی سایبری وجود داشت. این امر مانع از توانایی ناتو در ارائه یک پاسخ هماهنگ و مؤثر در برابر تهدیدات سایبری شد.

اجلاس بروکسل در سال ۲۰۱۸، با تداوم تلاش‌های ناتو برای تقویت امنیت سایبری، با الزام اعضای ناتو به تقویت پایداری ملی در برابر تهدیدات سایبری، گامی مهم در این مسیر برداشت. ماده ۳ پیمان آتلانتیک شمالی، که پیش از این عمدتاً بر تهدیدات نظامی متعارف متمرکز بود، اکنون بر آمادگی همه‌جانبه ملی در برابر بحران‌های احتمالی، ازجمله حملات سایبری، تأکید می‌کند. این امر منجر به ابتکاراتی در برخی محافل برای ایجاد اقدامات سایبری در داخل نیروهای مسلح و مشارکت با صنعت شد. همچنین، اجلاس بروکسل به‌دنبال ساده‌سازی سلسله‌مراتب فرماندهی ناتو درزمینه امنیت سایبری از طریق مراکز تعالی منتخب بود. علاوه بر این، پیشرفت‌هایی درزمینه تیم‌های جدید ضد جنگ هیبریدی حاصل شد تا به آماده‌سازی در برابر حملات پیچیده و مبهمی که سایبر را به تصویر می‌کشند، کمک کند. اگرچه ناتو در اجلاس بروکسل، حق دفاع فردی یا جمعی را تحت قوانین بین‌المللی تایید کرد، اما بیانیه این اجلاس از اشاره به پاسخ تهاجمی در برابر حملات سایبری خصمانه خودداری کرد. این امر نشان‌دهنده تردید برخی اعضای ناتو در مورد پاسخ به حملات سایبری بدون شناسایی قطعی مهاجم و نگرانی از تشدید تنش‌ها بود. در عوض، اجلاس بروکسل بر پایداری، همکاری و گفت‌وگو تأکید کرد. بااین‌حال، تایید انتساب به‌عنوان حق ملی حاکمیتی مستقل برای متحدان، نشان‌دهنده تغییر در برخی از دیدگاه‌های اعضای ناتو در مورد نیاز به گزینه‌های بازدارندگی فراتر از پایداری تنها برای تحمیل هزینه‌ها بر مهاجمان بود.

اجلاس سال ۲۰۲۱ ناتو در بروکسل، در شرایطی که تنش‌های ژئوپلیتیک با روسیه در حال افزایش بود، برگزار شد. حملات سایبری پیچیده‌ای که روسیه انجام داده بود، اعضای ناتو را بر آن داشت تا اقدامات متقابلی برای مقابله با این تهدید در نظر بگیرند. یکی از موضوعات مهم این اجلاس، بحث بر سر خطوط قرمز سایبری بود. بایدن در این اجلاس به پوتین هشدار داد که حملات سایبری به زیرساخت‌های حیاتی کشورهای عضو ناتو، با پاسخی قاطع از سوی ایالات‌متحده مواجه خواهد شد. پوتین نیز در این اجلاس، اتهامات آمریکا را رد کرد و ادعا کرد که این کشور نیز حملات سایبری انجام می‌دهد. بااین‌حال، در پایان این اجلاس، توافقی برای آغاز گفت‌وگوهای کارشناسی بین کارشناسان دو کشور برای کاوش در هنجارهای سازنده در حوزه سایبری حاصل شد. در حاشیه اجلاس، دیدگاه‌های اعضای ناتو در مورد

جنگ سایبری همچنان در حال تکامل بود. احتمال اینکه پس از حمله به خط لوله کلونیال، دفاع جمعی اعمال شود، نشان‌دهنده کاهش آستانه واکنش ناتو در برابر حملات سایبری بود. بازدارندگی گسترده‌تر نیز از اتکا بر تحریم‌ها و کیفرخواست‌ها به سمت استقرار مخفیانه تسلیحات سایبری به‌عنوان مکانیسم بازدارندگی تدریجی تغییر یافت. این رویکرد موسوم به «دفاع پیش‌گیرانه» می‌توانست به‌طور موقت تهدیدات را بدون تخریب بلندمدت خنثی کند. بااین‌حال، اثربخشی تحمیل هزینه‌ها بر عوامل نیابتی، در غیاب مقابله قاطع‌تر با حامیان دولتی، نیز مورد بررسی قرارگرفت.

اجلاس سال ۲۰۲۱ سران ناتو در شهر بروکسل برگزار شد. پاندمی کرونا، این اجلاس را همانند بسیاری از اجلاس‌های مهم چندین ماه اخیر تحت تأثیر قرارداد. بااین‌وجود، این اجلاس علاوه بر چالش‌های کرونایی تحت تأثیر چندین موضوع مهم دیگر قرار داشت که آن را از اجلاس‌های پیش از خود متمایز کرد. نخستین موضوع، مربوط به ریاست جمهور جدید آمریکا «جو بایدن» است. جو بایدن به‌عنوان رئیس‌جمهور جدید ایالات‌متحده آمریکا و یک عضو کلیدی ناتو در سوئیس به ملاقات ولادیمیر پوتین رفت. این دیدار و حاشیه‌های پیرامون آن، اجلاس سران ناتو در شهر بروکسل را تحت تأثیر خود قرارداد. روسیه همواره به‌عنوان یک تهدید جدی علیه امنیت اعضای ناتو در نظر گرفته می‌شود. از همین رو، بخش مهمی از ملاقات رهبران این دو ابرقدرت جهانی به فضای سایبر اختصاص پیدا کرد. در چند ماه منتهی به ملاقات بایدن و پوتین، موجی از حملات سایبری علیه زیرساخت‌های کشاورزی و انرژی ایالات‌متحده آمریکا صورت گرفت و این حملات سایبری تنش میان مسکو و واشنگتن را به‌شدت افزایش داد. پیش‌ازاین نیز، بایدن در خصوص مسائل مربوط به حقوق بشر، پوتین را قاتل خطاب کرده بود و این نیز بر تیرگی روابط این دو رقیب سنتی افزوده بود. اولین ملاقات بایدن و پوتین، فرصت مناسبی برای تعیین تکلیف حملات سایبری بود. بایدن در طول این ملاقات نسبت به حملات سایبری روسیه و ماجراجویی‌های هکرهای روسی به پوتین هشدار داد. نکته مهم در این خصوص آن است که ایالات‌متحده آمریکا در قبال جنگ‌های سایبری که حقیقت پذیرفته‌شده جهان حال حاضر است، قائل به اعمال برخی استثنائات است. آمریکا معتقد است که در جنگ‌های سایبری به برخی از زیرساخت‌های حیاتی (همچون سامانه‌های تأمین انرژی و آب) طرف‌های مقابل نباید حمله کرد و این موضوع نقطه آغاز بحث بایدن و پوتین درخصوص امنیت سایبری دو طرف بود. بایدن فهرستی از

شانزده بخش صنعتی را به‌عنوان اهداف غیرمجاز در جنگ‌های سایبری به پوتین پیشنهاد داد و این دو توافق نمودند که کارشناسانی را برای بررسی جزئیات این توافق تعیین کنند. بایدن به پوتین هشدار داد که چنانچه از این توافق تعدی شود، ارتش سایبری ایالات‌متحده آمریکا پاسخ مشابهی به تجاوز به زیرساخت‌های حیاتی خود خواهد داد(Walsh, 2021) . بااین‌وجود، پوتین همواره انجام حملات سایبری از سوی روسیه را انکار کرده و معتقد است که این حملات از سوی هم‌پیمان‌های آمریکا، همچون کانادا و انگلستان انجام می‌گیرد و آمریکا خود نیز یکی از اصلی‌ترین جنایت‌کاران سایبری در جهان است(Brewster, 2021) .

تمامی این عوامل دست‌به‌دست هم دادند تا نشست مهمی که انتظار می‌رفت بیش از پنج ساعت زمان ببرد، در کمتر از سه ساعت پایان یافت. پس‌ازاین ملاقات بایدن به خبرنگاران اعلام کرد که موضوعات مهمی مورد گفت‌وگو قرارگرفت و اکنون زمان آن است تا منتظر بنشینیم و نتایج کوتاه‌مدت آن را مورد ارزیابی قرار دهیم. چنانچه روسیه به تعهدات خود عمل کند، در آینده به توافقات بیشتری می‌توان دست‌یافت(Peter Wilkinson, 2021) .

با توجه به این مقدمه، می‌توان گفت که روابط ایالات‌متحده آمریکا به‌عنوان یکی از کلیدی‌ترین اعضای ناتو با دولت روسیه در شکننده‌ترین حالات خود پس از دوران جنگ سرد قرارگرفته است. الحاق کریمه به خاک روسیه، افزایش حملات سایبری توسط این کشور، انتشار سازمان‌یافته اخبار جعلی و جنگ‌های اطلاعاتی سبب‌شده تا دیگر اعضای ناتو نیز همین سطح از شکنندگی روابط را با روسیه پیدا کنند.

اجلاس سال ۲۰۲۱ سران ناتو در بروکسل تحت تأثیر تمامی این حوادث، در ۱۴ ماه ژوئن آغاز به کارکرد. جو بایدن به‌عنوان یکی از مهمانان برجسته این اجلاس که برای اولین‌بار در کسوت رئیس‌جمهور ایالت متحده در اجلاس سران ناتو شرکت می‌کرد، سخنرانی مهمی ایراد کرد که بخشی از آن متوجه استراتژی جدید ناتو درخصوص مواجهه با تهدیدات فضای مجازی است. مهم‌ترین مسئله مربوط به فضای مجازی که در اجلاس بروکسل مورد بررسی قرارگرفت، تهدیدات جمهوری خلق چین علیه اتحاد ناتو بود. چین برای اولین‌بار در طول سال‌های فعالیت ناتو، در کنار روسیه و حتی فراتر از آن به‌عنوان یک تهدید علیه ناتو به رسمیت شناخته شد. در بخشی از دستور کار اجلاس بروکسل با عنوان «مفهوم جدید استراتژیک»[1] سران

1. A New Strategic Concept

اتحاد مطرح کردند که با تجدیدنظر در سیاست‌های استراتژیک خود، چهارچوب جدیدی طراحی کنند که در آن با مدنظر قراردادن فضای در حال تکامل تهدیدات، اقدامات تهاجمی دشمنان را بی‌اثر کنند. دولت چین در این چهارچوب استراتژی جدید، تهدیدی علیه امنیت جمعی، شکوفایی و ارزش‌های دموکراتیک ناتو است. علاوه بر این، تهدیدات سایبری و تغییرات اقلیمی به‌عنوان دیگر تهدیدات وجودی علیه امنیت جمعی ناتو شناخته شدند و به شکل اضطراری، در سند استراتژیک جدید ناتو باید تعیین تکلیف شوند.

تقابل چین با ایالات‌متحده آمریکا و اروپا در فضای حقیقی و سایبر منجر به پیدایش سطح جدیدی از دغدغه‌های امنیتی در ناتو شده است. ناتو در اجلاس بروکسل چین را به جاسوسی گسترده در فضای مجازی متهم کرد و خواهان تمرکز همه‌جانبه ائتلاف علیه پکن شد.

«آنتونی بلیکنن»[1] وزارت خارجه آمریکا در این خصوص اعلام کرد که فعالیت‌های مخرب چین در فضای مجازی، تهدیدی جدی علیه امنیت ملی و اقتصادی ایالات‌متحده و هم‌پیمان‌هایش است. جو بایدن در خصوص چین معتقد است که این کشور برخلاف روسیه، شخصاً دست به حملات سایبری نمی‌زند و خرابکاری‌های سایبری منتسب به پکن توسط نیروهای نیابتی تحت حمایت حزب کمونیست صورت می‌گیرد. برجسته‌سازی دولت چین به‌عنوان یک تهدید وجودی علیه امنیت سایبری ناتو بسیار فراتر از حد انتظار حزب کمونیست چین بود. نه‌تنها در بیانیه اجلاس بروکسل به شکل اختصاصی به این موضوع اشاره شد، در اجلاس گروه هفت که در همین ماه جاری برگزار شد نیز، رهبران هفت قدرت بزرگ اقتصاد جهان صراحتاً به چین هشدار دادند. بااین‌وجود، باید توجه داشت که برخلاف ایالات‌متحده آمریکا، دیگر اعضای ناتو بااحتیاط بیشتری در این خصوص صحبت کرده و بیشتر ادعاهای آمریکا را تصدیق می‌کنند (Chiacu & Holland, 2021).

به‌روزرسانی سیاست‌های دفاع سایبری، یکی دیگر از مباحث اصلی اجلاس بروکسل بود. رهبران ناتو تأکید کردند که در سیاست دفاعی جدید، هماهنگی میان اعضای ناتو می‌بایست به‌شدت افزایش پیدا کند و این اطمینان حاصل شود که سازمان در برابر تهدیدات مکرر حملات سایبری توسط بازیگران غیردولتی و دولت‌های متخاصم، قدرت تاب‌آوری دارد. این سیاست‌های به‌روزرسانی شده

1. Antony Blinken

همچنین حاوی یک رهنمای استراتژیک برای تمامی اعضا است تا به‌وسیله آن تهدیدات سایبری در بخش‌های سیاسی، نظامی و فنی را خنثی کرده و امکان مواجه با طیف وسیعی از حملات سایبری را پیدا کنند. نسل جدید ارتباطات از دیگر دغدغه‌های رهبران ناتو در اجلاس بروکسل بود. سران اتحاد تایید کردند که با توجه به نقش پررنگ بخش خصوصی در ارائه خدمات اینترنتی در اروپا و آمریکا، برای راه‌اندازی نسل جدید اینترنت در سرتاسر مناطق تحت حفاظت ناتو، باید از ارائه‌دهندگان مطمئن و مورد تایید ناتو جهت تأمین اینترنت شهروند استفاده کرد. راه‌اندازی یک شتاب دهند نوآوری در حوزه «صنایع دفاعی»[1] به‌منظور حصول اطمینان از تأمین نیازهای دفاعی و حفظ قدرت فنی ناتو در حوزه سایبری از دیگر تصمیمات مهم سران پیمان آتلانتیک شمالی بود(Biden, 2021) .

این پروژه با الگوبرداری از «شتاب‌دهنده نوآوری امنیت ملی»[2] ایالات‌متحده (NSIN) آمریکا قرار است راه‌اندازی شود. پروژه شتاب‌دهنده نوآوری در حوزه دفاعی (DIA)، تحت نظر وزارت دفاع آمریکا به پشتیبانی از استارتاپ‌های حوزه فناوری می‌پردازد. این پروژه با استخدام متخصصین از جوامع دانشگاهی و استارتاپی، علاوه بر تأمین کامل هزینه‌های مالی راه‌اندازی پروژه‌ها، به آموزش افراد پرداخته و مخترعین وزارت دفاع آمریکا این دوره‌های آموزشی را اداره می‌کنند. تجاری‌سازی پروژه‌های نوآورانه در حوزه صنایع دفاعی یکی از اصلی‌ترین اولویت‌های این مرکز است. این مرکز با کاهش بروکراسی‌های رایج حوزه استارتاپی، آزمایشگاه‌ها و فرصت‌های مالی وزارت دفاع آمریکا را در اختیار مبتکران قرار می‌دهد. امنیت سایبری و امینت شبکه یکی از اصلی‌ترین اولویت‌های حمایتی وزارت دفاع آمریکا محسوب می‌شود(Ingstad, 2023) . بر همین اساس، سران ناتو در اجلاس بروکسل تصمیم گرفتند به‌منظور افزایش سرعت فرایند نوآوری، تجاری‌سازی و ایجاد جو رقابتی در حوزه امنیت سایبری چنین مرکزی را احداث کنند.

در بخش پایانی اجلاس بروکسل ۲۰۲۱، رهبران ناتو مجدداً در خصوص تسری حملات سایبری به ماده ۵ اساس‌نامه ناتو تبادل‌نظر کردند. به نظر می‌رسد این موضوع چالش‌برانگیزترین موضوع استراتژی دفاع سایبری ناتو است، چراکه بعد از گذشت یک دهه از آغاز اقدامات عملی و جدی، ناتو در خصوص امنیت سایبری

1. Defense Innovation Accelerator
2. National Security Innovation Network

همچنان به نتیجه مشخصی نرسیده است. همان‌طور که پیش‌تر مورداشاره قرارگرفت، نوع مواجهه و واکنش اعضای اروپایی ناتو به حملات سایبری دولت‌های متخاصم با ایالات‌متحده آمریکا متفاوت است. آمریکا با صراحت و شدت بیشتری به حملات سایبری چین و یا روسیه واکنش نشان می‌دهد، درحالی‌که شواهد امر گویای آن است که با تسری حملات سایبری به اصل دفاع جمعی و درواقع یک پاسخ جنگی تمام‌عیار به حملات سایبری، ناتو نگران عواقب جبران‌ناپذیر آن در جهان واقعی است.

اجلاس بروکسل ۲۰۲۱ با در نظرداشتن تمامی این ملاحظات، به راه‌حلی متناسب با شرایط حال حاضر جهان برای پاسخ‌دهی به حملات سایبری دست‌یافت. بنا بر آنچه در مشروح این تصمیم‌گیری اخیر مطرح شده است، با توجه به آنکه اکثر حملات سایبری به اعضای ناتو حملاتی از جنس مادون نظامی بوده و ماهیتاً غیرجنگی هستند، رهبران ناتو این حق را برای ملل عضو سازمان به رسمیت می‌شناسند که در پاسخ به جنایات سایبری مهاجمان، پیگیری‌های تلافی‌جویانه اقتصادی و سیاسی انجام دهند؛ زیرا این نوع از پاسخ‌دهی درحالِ‌حاضر بهترین نتیجه را برای سازمان به همراه خواهد داشت. در بیانیه پایانی اجلاس بروکسل همچنین به این نکته تأکید شد که ناتو با پایبندی به ماده ۵ اساس‌نامه سازمان، در هر زمان که تشخیص دهد یک حمله سایبری از آستانه غیرنظامی بودن عبور کرده و ماهیت جنگی به خود گرفته است، به‌صورت «موردی» در خصوص آن تصمیم‌گیری کرده و چنانچه آن را به‌منزله یک «حمله مسلحانه» تشخیص دهد[1]، تمامی اعضای اتحاد را برای پاسخ نظامی تمام‌عیار فراخوان می‌کند(Watson, 2021) .

در خصوص پاسخ به حملات درجه پایین سایبری، ناتو طیف وسیعی از اقدامات را در این اجلاس پیش‌بینی کرده است. در پاسخ‌دهی دیپلماتیک، ممکن است دامنه واکنش تا قطع روابط با دولت متخاصم و اخراج سفیر پیش برود و در پاسخ‌های اقتصادی این واکنش‌ها از قطع کامل روابط تجاری تا تحریم‌های اقتصادی سنگین از سوی تمامی کشورهای عضو سازمان ممکن است پیش برود. نکته مهمی که در طول رایزنی‌های کارشناسان و رهبران ناتو در اجلاس بروکسل مورد تأکید قرار گرفت، توجه به «اصل تناسب»[2] بود. از همین‌رو، چنانچه یک حمله سایبری ۱۰ میلیون دلار خسارت وارد کند، پاسخ متقابل آن باید هزینه‌ای ۱۰ میلیون دلاری به دولت

1. “be considered as amounting to an armed attack”
2. The principle of proportionality

مهاجم تحمیل کند. در این مورد، تفاوتی میان حملاتی که مستقیما از سوی یک دولت انجام می‌گیرد با حملاتی که از سوی نیروهای نیابتی آن انجام می‌گیرد وجود ندارد؛ زیرا ناتو حق انتساب‌دهی حملات سایبری را در اجلاس‌های قبلی برای اعضای خود به رسمیت شناخته است. این راه‌حل جدید دارای سه فایده مهم برای سازمان پیمان آتلانتیک شمالی است: از یک‌سو مبانی اصل دفاع جمعی و ماده ۵ اساس‌نامه را حفظ کرده و به روح آن لطمه‌ای نمی‌زند، از سوی دیگر حملات دولت متخاصم را بی‌پاسخ نگذاشته و اصل مسئولیت‌پذیری در حقوق بین‌الملل را محقق می‌کند و نهایتاً مانع از شکل‌گیری نبردهای حقیقی و تحمیل هزینه‌های هنگفت بر سازمان می‌شود.

۳. بازطراحی و به‌روزرسانی راهبردهای دفاع سایبری ناتو

لزوم به رسمیت‌شناسی تهدیدات سایبری به‌عنوان یک تهدید وجودی علیه امنیت جمعی اعضای ناتو برای اولین‌بار توسط سران ناتو در اجلاس سال ۲۰۰۲ در شهر پراگ مطرح شد. از آن زمان تاکنون، تهدیدات سایبری به شکلی پیوسته در دستور کار اجلاس‌ها و هم‌اندیشی‌های رهبران ناتو قرار گرفته است. در سال ۲۰۰۸، ناتو اولین سند دفاع سایبری خود را تنظیم کرد.

در سال ۲۰۱۴، اعضای ناتو دفاع سایبری را به بخش اصلی دستور کار دفاع جمعی اضافه کرده و اعلام نمودند که با حملات سایبری مطابق با ماده ۵ پیمان ناتو برخورد می‌کنند. قلب پیمان ناتو ماده ۵ آن است که در آن اعضا توافق کرده‌اند حمله نظامی علیه یک یا چند کشور عضو در اروپا یا آمریکای شمالی را به‌عنوان حمله به‌تمامی کشورهای عضو تلقی می‌کنند و به مقابله آن برمی‌خیزند[1]. درواقع، در این شرایط جدید ناتو به‌دنبال یک دگردیسی از عرصه دفاع جمعی به امنیت جمعی است (عسگرخانی و محمدی، ۱۳۹۵، ص. ۲۱۶).

---

۱. دولت‌ها توافق دارند که حمله‌ای مسلحانه علیه یک یا چندی از آن‌ها در اروپا و آمریکای شمالی، به معنای حمله‌ای علیه تمامی آن‌ها تلقی خواهد شد و در نتیجه آن‌ها موافقت می‌نمایند در صورتی که چنین حمله‌ای اتفاق افتد، هر یک از آن‌ها، در راستای عمل به حق دفاع انفرادی یا دسته جمعی از خود بر اساس ماده ۵۱ منشور سازمان ملل، دولت یا دولت‌های مورد حمله قرار گرفته را از طریق اقدامات آنی، هرآنچه که ضروری می‌نماید، به صورت انفرادی یا به اتفاق دیگر دولت‌ها، مساعدت نمایند تا امنیت را در منطقه آتلانتیک شمالی بازگردانده و برقرار نمایند که می‌تواند شامل استفاده از نیروهای مسلح نیز باشد.

در راستای افزایش اقدامات امنیتی در مواجهه با حملات سایبری، سران ناتو در سال ۲۰۱۶ فضای مجازی را به‌عنوان یکی از بسترهای عملیات نظامی (در کنار زمین، آسمان و دریا) به رسمیت شناخته و دفاع سایبری از شبکه‌ها و زیرساخت‌های ملی اعضا را به‌عنوان یک اولویت امنیتی قلمداد کردند. اعضای ناتو گام‌های استراتژیک، عملیاتی و فنی متعددی را برای مقابله با تهدیدات وجودی سایبری برداشته‌اند. رهبران ناتو در اجلاس سال ۲۰۱۸ در شهر بروکسل هشدار دادند که تهدیدات سایبری علیه امنیت جمعی ناتو به شکل قابلِ‌توجهی افزایش‌یافته و این فرایند در آینده نیز به‌مراتب بیشتر خواهد شد (Brent, 2019). چالش‌های مداوم و درعینِ‌حال پیش‌رونده تهدیدات سایبری، مستلزم آن است که ناتو به‌طور مداوم انطباق سیاست‌های امنیتی و تناسب واکنش‌های خود با تهدیدات سایبری را مورد ارزیابی قرار دهد. کارشناسان ناتو، سه سؤال کلیدی را برای ارزیابی نقش ناتو در فضای مجازی مطرح می‌کنند: هدف اصلی ناتو در فضای مجازی چیست؟ ناتو برای دستیابی به هدف خود با چه چالش‌هایی مواجه است؟ آیا ناتو برای مواجهه با چالش‌های پیشِ‌روی خود به شکل مناسبی اقدام می‌کند؟

۴. تحلیل اهداف و چالش‌های ناتو

اصلی‌ترین هدف ناتو از تسری استراتژی دفاع جمعی به فضای مجازی بارها در نشست‌های سران اتحاد مطرح شده است. بر این اساس، ناتو معتقد است که باید همان‌طور که در زمین، آسمان و دریا اقدام به انجام عملیات آفندی و پدافندی می‌کند، در فضای مجازی نیز بتواند فعالیت کرده و برای خود و متحدانش سنگرهای تدافعی و بازدارندگی سایبری ایجاد نماید (LEWIS, 2019).

در این رهگذر، بزرگ‌ترین واصلی‌ترین چالش پیشِ‌روی ناتو این است که صرفاً نمی‌تواند با ابزار نظامی به هدف خود دست‌یابد، درحالی‌که نتیجه مطلوب او نظامی است. تمام عملیات و مأموریت‌های ناتو در فضای مجازی تا حد بسیاری به بخش خصوصی وابستگی دارد، خصوصاً درزمینه زیرساخت‌های ارتباطاتی، تدارکات، تجهیزات و بسترهای میزبان. پاسخگویی به تهدیدات سایبری نیز دارای پیچیدگی‌های مخصوص به خود است که تا حد بسیاری آن را از پاسخگویی به تهدیدات نظامی متمایز می‌سازد. همین پیچیدگی‌های مختلف در مواجهه با تهدیدات سایبری سبب گردیده است تا اعضای ناتو در کنار دستور کار اتحاد، برای

خود استراتژی‌های فردی نیز اتخاذ کنند که در بسیاری از موارد منجر به موازی کاری و ایجاد استانداردهای چندگانه شده است. به‌عنوان مثال، حضور ایالات‌متحده آمریکا به‌عنوان هم‌پیمان خارج از قلمرو اروپا در ناتو که خود دارای دستور کار دفاع سایبری جداگانه است، یکی از چالش‌های اصلی ایجاد وحدت رویه در برخورد مؤثر ناتو با تهدیدات سایبری است. «فرماندهی سایبری ایالات متحده آمریکا»[1] بر این باور است که دشمنان آمریکا به شکل مداوم برای کسب منافع استراتژیک در فضای سایبر علیه آمریکا فعالیت می‌کنند. در چنین شرایطی اگرچه ایالات‌متحده آمریکا خواهان تعامل مداوم با متحدان خویش است، اما درعین‌حال به آن‌ها به چشم رقیب‌های سیاسی نیز نگاه می‌کند (Nakasone, 2018).

هرچند که ناتو رسالت خویش را در ماده ۵ پیمان‌نامه تعریف کرده است، اما سابقه قابلِ‌توجهی در اقدامات مادون نظامی دارد. فلسفه وجودی تشکیل ناتو سه وظیفه اصلی دفاع جمعی، مدیریت بحران و همکاری امنیتی است. در همین راستا، امروزه ناتو مأموریت‌های آموزشی در عراق را دنبال می‌کند و هم‌زمان در عملیات برقراری امنیت در آب‌های دریای مدیترانه مشارکت فعال دارد. درخصوص فضای سایبر نیز ناتو باید تعیین کند که چگونه به شکل مشابهی مسیر فعالیت‌های خود را ترسیم می‌کند، زیرا یک حمله سایبری غیرنظامی به‌اندازه یک اقدام نظامی می‌تواند امنیت متحدان را به خطر بیندازد. چالش‌های پیش‌روی ناتو، تعدد ذی‌نفعان، تهدیدات بی‌شمار فضای مجازی و تغییر پرشتاب این عرصه، آسیب‌پذیری کشورهای عضو ناتو را بیش‌ازپیش افزایش می‌دهد و فرصتی برای سیاست‌گذاری‌های زمان‌بر باقی نمی‌گذارد.

۵. نتیجه‌گیری و پیشنهاد

در شرایط کنونی جهان، امنیتی‌سازی فضای سایبر یکی از ملزومات اصلی حکمرانی بر این فضا است. با توجه به ماهیت آنارشیک نظام بین‌الملل و فقدان نهادهای ناظر بین‌المللی بر فضای مجازی و اساساً نظارت‌گریزی این فضا، حملات سایبری توسط بازیگران دولتی، نیروهای نیابتی آن‌ها و گروه‌های مجرمانه سازمان‌یافته می‌توانند هزینه‌های جبران‌ناپذیری بر زیرساخت‌های فناورانه یک کشور تحمیل کند. نظام‌های امنیتی پیشرفته، با درک پیچیدگی‌ها و دگرگونی‌های فضای مجازی دستور کارهای

1. The United States Cyber Command

امنیتی مختلفی متناسب با فضای مجازی برای خود تدوین و طراحی کرده‌اند. سازمان پیمان آتلانتیک شمالی، به‌عنوان بازوی نظامی ۳۰ کشور اروپایی و آمریکای شمالی بر اساس یک سطح تحلیل منطقه‌ای، در یک فرایند پانزده‌ساله مسیر پُرفرازونشیبی در خصوص طراحی یک استراتژی امینی برای فضای سایبری پشتِ‌سر گذاشته است. بررسی تجربه ارزشمند این سازمان مهم نظامی بیانگر چند نکته مهم است: ناتو با توجه به اهمیت فضای سایبر، آن را به‌عنوان یک دامنه عملیاتی جدید مورد شناسایی قرار داده است. این امر بیانگر آن است که فضای مجازی در آینده‌ای نه‌چندان دور تبدیل به محل اصلی منازعات و درگیری‌های نظامی میان کشورهای مختلف خواهد شد و هرگونه غفلت و کوتاهی در قبال این فضا منجر به بروز خسارات مادی و امنیتی قابلِ‌توجه خواهد شد. تجربه ناتو بیانگر این است که این سازمان علی‌رغم برنامه‌ریزی‌های دقیق و حفظ آمادگی خود در دامنه‌های عملیاتی شناخته‌شده همچون آسمان، دریا و خشکی تا قبل از تجربه حمله سایبری به کشور استونی فاقد یک دستور کار مشخص در خصوص امنیت سایبری بود و بلافاصله بعد از حملات آوریل سال ۲۰۰۷ تصمیم به تدوین کار ویژه امنیتی برای فضای مجازی گرفت. این نکته ازاین‌جهت حائز اهمیت است که در طول این سال‌ها، حملات سایبری ازنظر شدت و گستردگی به‌مراتب خطرناک‌تر و پیشرفته‌تر شده‌اند و چنانچه کشورها مقوله امنیت سایبری را به کسب تجربه یک حمله سایبری تمام‌عیار موکول کنند، هزینه زیادی در این خصوص متحمل خواهند شد. درنهایت مسئله مهمی که از تحولات استراتژی امنیت سایبری ناتو می‌بایست موردِتوجه قرارداد، تسری حملات سایبری به ماده ۵ اساس‌نامه این سازمان است. هرچند در شرایط کنونی سازمان ناتو با توجه به شرایط منطقه‌ای خود و رقبایی همچون چین و روسیه بااحتیاط بیشتری در خصوص این موضوع صحبت می‌کند و بیشتر سعی بر غیرنظامی جلوه‌دادن حملات سایبری دارد، کارشناسان این سازمان بر این باور هستند که با توجه به تغییر پارادایم نظامی جهان و انتقال بسترهای عملیاتی به فضای مجازی، این سازمان بر اساس رسالت دفاع جمعی ناگزیر از آن است که خود را برای جنگ‌های تمام‌عیار سایبری در آینده نزدیک آماده کند.

با توجه به آنچه گذشت، این تحقیق طراحی مجدد و به‌روزرسانی راهبرد دفاع سایبری ناتو را با توجه به شناسایی فضای مجازی به‌عنوان یک عرصه نظامی جدید موردبررسی قرار داد و از طریق این بررسی نتایج ذیل حاصل گردید:

نخست، به رسمیت‌شناسی فضای سایبری به‌عنوان یک عرصه نظامی جدید در کنار آسمان، زمین و دریا توسط ناتو گامی مهم در به‌روزرسانی و طراحی مجدد راهبرد دفاع سایبری این سازمان است. این اقدام به ناتو کمک می‌کند تا تمرکز خود را از حوزه‌های فیزیکی سنتی به حوزه‌های سایبری جدید تغییر دهد. با انجام این کار، ناتو با چشم‌انداز دائماً درحالِ‌تغییر تهدیدات سایبری و جنگ‌های مدرن دیجیتال سازگار می‌شود و همین امر برای موفقیت مستمر و حفظ بقای این سازمان در عرصه جنگ‌های نوپدید حیاتی است. بر همین اساس، جمهوری اسلامی ایران نیز باید با توجه به اهمیت و ضرورت ایجاد یک راهبرد دفاع سایبری نوین و کارآمد، به شکل رسمی فضای سایبری را به‌عنوان یک عرصه نظامی جدید در کنار آسمان، زمین و دریا به رسمیت بشناسد و راهبرد دفاع سایبری کنونی خود را بر اساس این رویکرد بازنگری کند.

دوم، استراتژی دفاع سایبری ناتو از اجلاس سال ۲۰۱۴ در ولز دائماً در حال تکامل و به‌روزرسانی است. ناتو از طریق اجرای پیمان دفاع سایبری و رزمایش‌های گوناگون سایبری، پیشرفت‌های چشمگیری در ارتقای قابلیت‌های دفاع سایبری خود ایجاد کرده است. این تلاش‌ها نشان‌دهنده تعهد ناتو به حفاظت از کشورهای عضو این سازمان در برابر تهدیدات سایبری و تقویت قابلیت‌های دفاع جمعی است. در همین راستا، جمهوری اسلامی ایران نیز باید با توجه به اهمیت و ضرورت دفاع سایبری، راهبردهای دفاع سایبری خود را به‌طور مستمر به‌روزرسانی کند و با بهره‌گیری از تجربیات و دستاوردهای کشورهای پیشرو در این عرصه، قابلیت‌های دفاع سایبری خود را تقویت کند.

سوم، امنیتی‌سازی فضای سایبری و توسعه یک استراتژی جامع امنیت سایبری جنبه‌های کلیدی رویکرد ناتو به دفاع سایبری را برجسته می‌سازد. ناتو با اتخاذ رویکرد امنیتی‌سازی فضای سایبری، تهدیدات سایبری را به یک اولویت امنیت ملی در میان تمام اعضای خود تبدیل کرده است، در نتیجه این فرصت به وجود آمده است تا منابع و امکانات بیشتری جهت دفاع سایبری در سرتاسر سازمان بسیج شود. علاوه بر این، توسعه یک استراتژی جامعه امنیت سایبری به ناتو این امکان را می‌دهد که رویکردی جامع و فعالانه برای دفاع سایبری اتخاذ کند، نه اینکه صرفاً به حوادث سایبری در هنگام وقوع و پس از آسیب‌زایی واکنش نشان دهد. بر همین اساس، جمهوری اسلامی ایران نیز به‌عنوان یکی از کشورهای مهم در منطقه و جهان

که در سالیان اخیر قربانی حملات مستقیم یا غیرمستقیم و نیابتی سایبری بوده است، با توجه به ماهیت پیچیده و پویا فضای سایبری و ضرورت حفاظت از منافع ملی خود در این عرصه، باید با اتخاذ رویکرد امنیتی‌سازی فضای سایبری و توسعه یک راهبرد جامع امنیت سایبری، اقدامات پیشینی و دفاع سایبری فعال و رو به جلو را به‌منظور پیشگیری از وقوع تهدیدات سایبری و مقابله سریع و مؤثر با این تهدیدات انجام دهد.

در پایان باید خاطرنشان کرد که پژوهش حاضر در راستای ایجاد یک رویکرد تحول‌آفرین در پارادایم حاکم بر راهبرد کنونی دفاع سایبری در ایران، به تشریح مفاهیم و مسائل نوظهوری پیرامون دفاع سایبری نوین و فعالانه، با تأکید بر تجربیات، اقدامات و راهبردهای سازمان ناتو و اهمیت به رسمیت‌شناسی فضای سایبری به‌عنوان یک عرصه نظامی نوپدید برای سیاست‌گذاران، فرماندهان نظامی و محققان فعال در حوزه دفاع سایبری و امنیت ملی پرداخت و تلاش کرد تا اهمیت و ضرورت‌های چنین راهبردی را برجسته نماید.

فهرست منابع

- بوزان، باری (۱۳۹۹). ***چهارچوبی تازه برای تحلیل امنیت***. تهران: پژوهشکده مطالعات راهبردی.
- بوزان، باری (۱۳۹۹). ***مردم، دولت‌ها و هراس***. تهران: پژوهشگاه مطالعات راهبردی.
- جمشیدی و همکاران (۱۳۹۹). ***تأثیرپذیری ژئوپلیتیکی منافع ملی جمهوری اسلامی ایران از رقابت ناتو و سازمان همکاری شانگهای در آسیای مرکزی***. فصلنامه علمی راهبرد. ۹۶(۲۹).
- عسگرخانی، ابومحمد و محمدی، محمود (۱۳۹۵). ***تحول در مأموریت‌های ناتو و ضرورت تقویت رژیم نظارتی در حقوق بین‌الملل (راهبرد مسئولیت‌پذیری ناتو)***. فصلنامه علمی راهبرد، ۲۵(۸۱).
- کالینز، آلن (۱۳۹۹). ***مطالعات امنیت معاصر***. تهران: پژوهشکده مطالعات راهبردی.
- هریسی‌نژاد، کمال‌الدین (۱۳۷۴). ***نظری به پیمان ماستریخت و اتحاد اروپا***. فصلنامه جغرافیا و برنامه‌ریزی، شماره ۱.

References

- Asgharikhani, A. M., & Mohammadi, M. (2017). Evolutions in NATO Missions and the Need for Strengthening Supervisory System in International LAW (NATO Responsibility Strategy). A Quarterly Journal of Strategy, 25(81). (In Persian)
- Biden, J. (2021, February 19). Retrieved from whitehouse.gov: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-nato-summit-revitalizing-the-transatlantic-alliance/
- Brent, L. (2019, February). Retrieved from NATO REVIEW: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
- Brewster, J. (2021, jun). Retrieved from forbes: https://www.forbes.com/sites/jackbrewster/2021/06/16/putin-claims-after-biden-summit-most-cyberattacks-come-from-us-not-russia/?sh=5d5b96fc30c4
- Buzan, Barry. (2020). A New Framework for Security Analysis. Tehran: Strategic Studies Center. (In Persian)
- Buzan, Barry. (2020). People, States, and Fear. Tehran: Strategic Studies Center. (In Persian)
- Chiacu, S., & Holland, D. (2021, July). Retrieved from Reuters: https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/
- Collins, Alan. (2020). Contemporary Security Studies. Tehran: Strategic Studies Center. (In Persian)
- Deschamps, É. (2016). Retrieved from cvce.eu: http://www.cvce.eu/obj/drafting_of_the_rome_treaties-en-8efe2279-ee12-4a75-aeeb-0bd547f4128f.html
- Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship, 8(12), 23. doi:https://doi.org/10.1186/s13731-019-0105-z
- Herisinejad, Kameleddin. (1995). A Study of the Maastricht Treaty and the European Union. Journal of Geography and Planning, No. 1. (In Persian)
- Ingstad, C. (2023). NSIN Releases Year in Review - FY22. Retrieved from National Security Innovation Network: https://www.nsin.mil/year-in-review-fy22/
- Jamshidi, S. M., et al. (2020). Geopolitical Impact of National Interest of the Islamic Republic of Iran on Competition NATO and the Shanghai Cooperation Organization in Central Asia. A Quarterly Journal of Strategy, 29(96). (In Persian)
- LEWIS, D. (2019, FEBRUARY). Retrieved from Texas National Security Review: https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/
- Nakasone, P. (2018, April). Retrieved from cybercom: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf
- napma. (2021, jan). Retrieved from napma.nato.int: https://www.napma.nato.int/awacs/a0.html

- NATO. (2021, jan 31). Collective defense - Article 5. Retrieved from nato.int: https://www.nato.int/cps/en/natohq/topics_110496.htm.
- Peter Wilkinson, L. S.-M. (2021, jun). Retrieved from CNN: https://edition.cnn.com/world/live-news/biden-putin-meeting-geneva-updates-intl/index.html
- Shea, S. (2023, January 1). Retrieved from techtarget: https://www.techtarget.com/searchsecurity/definition/cybersecurity
- Biden, J. (2021, February 19). Retrieved from whitehouse.gov: https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-nato-summit-revitalizing-the-transatlantic-alliance/
- Brent, L. (2019, February). Retrieved from NATO REVIEW: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
- Brewster, J. (2021, jun). Retrieved from forbes: https://www.forbes.com/sites/jackbrewster/2021/06/16/putin-claims-after-biden-summit-most-cyberattacks-come-from-us-not-russia/?sh=5d5b96fc30c4
- Chiacu, S., & Holland, D. (2021, July). Retrieved from Reuters: https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/
- Deschamps, É. (2016). Retrieved from cvce.eu: http://www.cvce.eu/obj/drafting_of_the_rome_treaties-en-8efe2279-ee12-4a75-aeeb-0bd547f4128f.html
- Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship, 8(12), 23. doi:https://doi.org/10.1186/s13731-019-0105-z
- Ingstad, C. (2023). NSIN Releases Year in Review - FY22. Retrieved from National Security Innovation Network: https://www.nsin.mil/year-in-review-fy22/
- LEWIS, D. (2019, FEBRUARY). Retrieved from Texas National Security Review: https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/
- Nakasone, P. (2018, April). Retrieved from cybercom: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf
- napma. (2021, jan). Retrieved from napma.nato.int: https://www.napma.nato.int/awacs/a0.html

- NATO. (2021, jan 31). Collective defense - Article 5. Retrieved from nato.int: https://www.nato.int/cps/en/natohq/topics_110496.htm.
- Peter Wilkinson, L. S.-M. (2021, jun). Retrieved from CNN: https://edition.cnn.com/world/live-news/biden-putin-meeting-geneva-updates-intl/index.html
- Shea, S. (2023, January 1). Retrieved from techtarget: https://www.techtarget.com/searchsecurity/definition/cybersecurity

- Walsh, J. (2021, jun). Retrieved from forbes: https://www.forbes.com/sites/joewalsh/2021/06/16/biden-vows-retaliation-on-any-future-russian-cyberattacks-on-critical-infrastructure/?sh=3f4aa2591fab