بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۳۶
آبان ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

امنیتی‌سازی فضای مجازی؛ دستور کار ناتو

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات اخلاقی فضای مجازی)

تهیه‌کننده: امیرعباس رکنی(دانشجوی ارشد جزا و جرم‌شناسی دانشگاه علوم قضایی)

ناظر علمی: محمدمهدی نصر هرندی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست ۵
چکیده ۹
مقدمه ۱۳

بخش اول (پیشینه نظری امنیتی سازی فضای سایبر) ۲۱

بخش دوم (فرایند امنیتی سازی) ۲۷
۲-۱- سطوح تحلیل ۳۰
۲-۲- امنیت سایبری؛ ویژگی‌ها و ملزومات ۳۴
۲-۳- دستور کار دفاع جمعی ۳۷

بخش سوم (امنیتی سازی تهدیدات سایبری توسط ناتو) ۴۱
۳-۱- اهداف و چالش‌ها ۴۴
۳-۲- پیش‌زمینه طراحی سیاست دفاع سایبری ناتو ۴۶

بخش چهارم (وضعیت فعلی دستورکار امنیت جمعی ناتو در فضای مجازی) ۴۹
۴-۱- اجلاس سال ۲۰۱۴ سران ناتو در ولز ۵۱
۴-۲- اجلاس سال ۲۰۱۶ سران ناتو در ورشو ۵۳
۴-۳- اجلاس سال ۲۰۱۸ سران ناتو در بروکسل ۵۹
۴-۴- اجلاس سال ۲۰۲۱ سران ناتو باز هم در بروکسل ۶۳

جمع بندی ۷۳
منابع ۷۹

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

اعضای پیمان آتلانتیک شمالی به‌تازگی در ژوئن ۲۰۲۱ در راستای بازطراحی و به‌روزرسانی راهبردهای دفاع سایبری در شهر بروکسل تشکیل جلسه داده‌اند. ناتو با شناسایی تهدیدات سایبری، به‌عنوان یک تهدید وجودی علیه امنیت جمعی اعضای اتحاد، دستور کار امنیتی جدید خود را معطوف به سازگاری اعضا با این فضای متحول قرار داده است. از همین رو، ناتو با به‌رسمیت‌شناسی فضای مجازی به‌عنوان یک بستر عملیاتی جدید در کنار آسمان، دریا و زمین، کشورهای این پیمان نظامی را موظف کرده است تا خود را برای انجام وظایف اصلی - که عبارت است از: دفاع جمعی، مدیریت بحران و همکاری امنیتی- آماده کرده و دفاع از زیرساخت‌های اینترنتی و مواجهه با تهدیدهای روزافزون فضای سایبر و حملات سایبری را در دستور کار خود قرار دهند. این اقدامات، همگی در راستای پروژه‌ی امنیتی‌سازی فضای سایبری انجام‌گرفته است. گزارش حاضر، با بررسی نشست‌های امنیت سایبری که با توجه به اهمیت آن‌ها در سطح سران دولت‌های عضو ناتو برگزار می‌شود، خواهد پرداخت و با تحلیل مفاد اسناد و راهبردهای این اجلاس‌ها، زوایای استراتژی

امنیتی جدید ناتو در بعد سایبری و پیش‌زمینه نظری آن را معرفی می‌کند.

واژگان کلیدی: ناتو، امنیتی‌سازی، بروکسل، مکتب کپنهاگ، امنیت سایبری، استراتژی سایبری

مقدمه

مقدمه

پایان جنگ سرد و فروپاشی اتحاد جماهیر شوروی نویدبخش گسترش صلح و آزادی بود و درنتیجه آن احتمال جنگ‌های هسته‌ای و حتی جنگ‌های بزرگ متعارف رنگ می‌باخت. حتی برخی از صاحب‌نظران، این تحولات را چنان نویدبخش می‌پنداشتند که می‌گفتند دیگر به مباحث مربوط به نیروی نظامی یا امنیت ملی نیازی نیست. شاید این وضعیت ازنظر تاریخی شبیه به وضعیتی بود که ملت‌ها بعد از پایان جنگ جهانی اول داشتند و همگان مشتاق صلح بودند[1]؛ اما طولی نکشید که تهدیدات امنیتی جدید خود را نمایان کرد و بحران هراس دوباره به‌سوی ملت‌ها بازگشت. تهدیدات تروریستی، گسترش سلاح‌های کشتارجمعی، تهدیدات زیست‌محیطی، شیوع بیماری‌های فراگیر جهانی و ظهور فناوری‌های نوین، گسترش قابلیت‌های مخرب و استفاده نظامی از آن‌ها مهم‌ترین بحران‌های امنیتی جدید پیش روی بشر در فراسوی جنگ سرد بود.

تهدیدات امنیتی نوظهور دارای وجوه مشترکی هستند؛ تهدیداتی همانند تهدیدات سایبری به‌مراتب فراگیرتر و محتمل‌تر از تهدیدات سنتی هستند. این تهدیدات امنیتی نوظهور از حیث گستره و شدت،

۱. شولتز، ریچارد و همکاران، رویکردهای جدید در مطالعات امنیتی، پژوهشکده مطالعات راهبردی، جلد اول، چاپ سوم، تهران،۱۳۹۴.

گوناگون هستند و ازاین‌رو برآورد آن‌ها دشوارتر است. بسیاری از عوارض آن‌ها به‌صورت غیرمستقیم نمود پیدا می‌کند و در درازمدت از حجم خسارات وارده قابل ارزیابی هستند. پیامدهای آن‌ها اغلب منجر به صدمه دیدن اقتصاد، کاهش میزان جذب سرمایه‌گذاری خارجی و اخلال در زیرساخت‌های حیاتی می‌شوند که دامنه وسیعی دارند. تعیین‌کننده‌ترین وجه مشترک تهدیدات امنیتی معاصر، این واقعیت است که این تهدیدات در بسیاری از موارد، نه‌تنها دولت‌ها بلکه جوامع و افراد را نیز هدف قرار می‌دهند. تهدیدات جدید به شکل فراملی خودنمایی می‌کنند. تهدیدهای امنیتی فراملی، ابزارها و فن‌آوری‌های جدید ارتباطی را به کار می‌گیرند که برای جهانی‌شدن تجارت و سرمایه مفید و ضروری هستند. آن‌ها نشان می‌دهند که پیشرفت فنّاوری نه‌تنها می‌تواند منجر به پیدایش فرصت‌های جدید شود، بلکه ممکن است خطرات جدید نیز به وجود بیاورد. این تهدیدات دیگر با چارچوب‌های تحلیلی مطالعات امنیتی حاکم بر دوران جنگ سرد منطبق نیستند. دولت‌ها و سازمان‌های بین‌المللی به ناگزیر پذیرفته‌اند که ترتیبات امنیتی گذشته، از قبیل استفاده سنتی از نیروهای نظامی و تمرکز صرف بر مرزهای داخلی برای تأمین امنیت ملی کافی نیست[1]. ویژگی‌های تهدیدات جدید نشان‌دهنده این است که بدون تغییر رویکرد جامعه مطالعاتی و عملیاتی به مفهوم امنیت از یک‌سو و نگاه حاکمیت به امنیت از سوی دیگر نمی‌توان درک درستی از تهدیدات امنیتی و درنتیجه مواجهه مؤثر با آن‌ها داشت.

تغییر ماهیت تهدیدات امنیتی و پیدایش تهدیدات امنیتی نوظهور،

۱. یزدان فام، محمود، دولت های شکننده و امنیت انسانی، پژوهشکده مطالعات راهبردی، چاپ دوم،۱۳۹۲، ص ۱۲۲-۱۲۴.

ضرورت تجدیدنظر در استراتژی‌های امنیتی را بیش از هر زمان دیگر ایجاب می‌نمود. از همین رو، مکتب‌های امنیتی جدید درصدد رفع خلأهای نظری موجود برآمده و نظریات امنیتی و راهبردهای جدیدی تدوین نمودند. در مورد کشورهای اروپایی که بعد از جنگ جهانی دوم به سمت هم‌بافتی و امنیت جمعی حرکت نمودند، مکتب امنیتی کپنهاگ بیش‌ترین اثرگذاری را بر سیاست‌های کلان امنیتی کشورهای عضو این قاره گذاشت. برابر آموزه‌های این مکتب، مفهوم امنیت دیگر دارای بعد نظامی نبوده و متشکل از پنج بعد سیاسی، اقتصادی، اجتماعی، زیست‌محیطی و نظامی است. هر یک از این ابعاد در ارتباط مستقیم با همدیگر قرار داشته و نیازمند تأمین امنیت اختصاصی و اشتراکی هستند. از سوی دیگر، نظریه‌پردازان این مکتب بر این باور هستند که تهدیدات امنیتی در طول زمان به شکل یکسان مطرح نبوده و ممکن است یک تهدید امنیتی، در یک بازه زمانی دیگر در قامت یک تهدید مطرح نبوده و تهدیدات امنیتی جدید جای آن را بگیرد. آنچه در این خصوص حائز اهمیت است، فرایندی موسوم به فرایند امنیتی‌سازی است. در این فرایند، نخبگان امنیتی با مطرح کردن یک تهدید به‌عنوان تهدید وجودی، به جامعه اعلام می‌کنند که فائق آمدن بر تهدید وجودی نوظهور علیه ملت و دولت از طرق عادی میسر نبوده و نیازمند به‌کارگیری راه حال‌های فوق‌العاده و اضطراری است. درنتیجه ادبیات امنیتی، بازیگر امنیتی و طی نمودن صحیح فرایند امنیتی‌سازی در مکتب کپنهاگ از اهمیت بسزایی برخوردار است.

سازمان پیمان آتلانتیک شمالی به‌عنوان بازوی نظامی کشورهای اروپایی

در یک سطح تحلیل منطقه‌ای، تحت تأثیر آموزه‌های این مکتب نزدیک به پانزده سال است که در حال امنیتی‌سازی فضای سایبر است. در گفتمان امنیتی جدید ناتو، تهدیدات سایبری به‌عنوان یک تهدید وجودی به رسمیت شناخته‌شده‌اند که امنیت ملی و جمعی اعضای ناتو را به خطر می‌اندازند. در همین راستا، ناتو فضای مجازی را به‌عنوان یک بستر عملیاتی جدید در کنار آسمان، زمین و دریا به رسمیت شناخته و برای تأمین امنیت اعضای اتحاد در آن اقدام به عملیات آفندی و پدافندی می‌کند. افزایش تهدیدات سایبری و تکامل فزاینده آن‌ها موجب گردیده است تا ناتو سطح امنیتی‌سازی فضای سایبر را در طول این چند سال اخیر به‌شدت افزایش داده و حملات سایبری را به ماده ۵ اساس‌نامه این سازمان تسری دهد. بر اساس ماده ۵ اساس‌نامه ناتو که به قلب این سازمان معروف است، حمله نظامی به هر یک از اعضا به‌منزله حمله به‌تمامی اعضای ناتو تلقی می‌شود و ناتو با فراخوان نیروهای نظامی کشورهای عضو، به دولت متجاوز پاسخ نظامی خواهد داد. در کنار این اقدامات جدی، این سازمان دست به انجام رزمایش‌های مشترک سایبری، تأسیس مراکز آموزشی تخصصی و تربیت نیروهای زبده جنگ سایبری زده است.

دستور کار استراتژی‌های امنیت سایبری ناتو در نشست های منظم سالانه‌ای که در سطح سران ارشد کشورهای عضو برگزار می‌شود، اتخاذ می‌گردد. گزارش حاضر، با بررسی پیشینه نظری امنیتی‌سازی فضای سایبر و توضیح آموزه‌های مکتب امنیتی کپنهاگ، به شکل مروری به بررسی مهم‌ترین و کلیدی‌ترین اجلاس‌های ناتو در خصوص امنیت سایبری پرداخته و تصمیمات و راهبردهای مصوب

آن‌ها را مورد تحلیل قرار می‌دهد. اهمیت بررسی این استراتژی‌ها ازآن‌جهت است که در شرایط کنونی جهان و افزایش سرسام‌آور حملات مخرب سایبری، ظهور گروه‌های تروریسم سایبری که به شکل نیابتی و بازیگران غیردولتی دست به خرابکاری‌های سایبری می‌زنند و مطرح‌شدن تهدیدات سایبری به‌عنوان یک تهدید وجودی، امنیتی‌سازی فضای مجازی یکی از ضرورت‌های حکمرانی بر این فضای متکثر است که نیازمند انجام اقدامات مطالعاتی و کارشناسی گسترده و ازجمله مطالعه تجربیات کشورها و سازمان‌های مهم بین‌المللی است.

بخش اول

بخش اول

پیشینه نظری 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 امنیتی قاره اروپا بودند. بری بوزان[2]، استاد روابط بین‌الملل دانشگاه اقتصاد لندن[3] به‌عنوان شاخص‌ترین نظریه‌پرداز این نظم جدید، مکتب امنیتی نوینی را پایه‌گذاری کرد

1. Copenhagen Peace Research
2. Barry Buzan
3. London School of Economics

که به مکتب امنیتی کپنهاگ مشهور شد[1].

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 تک ساحتی را نفی کرد و اعلام نمود که امنیت مفهومی چندبعدی است. او برای امنیت ملی قائل به پنج بعد نظامی، سیاسی، اقتصادی، اجتماعی و زیست‌محیطی است. بوزان در شاخص‌ترین اثر خود بانام مردم، دولت‌ها و هراس[2] به شرح و توضیح ابعاد پنج‌گانه امنیت ملی پرداخته و برداشت‌های سنتی از امنیت را بسیار مضیق می‌داند.[3] نتیجه مهمی که از این تقسیم‌بندی به دست آمد، توجه و اولویت دادن 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 دریکی دیگر از آثار مهم خود بانام «چارچوبی تازه برای تحلیل امنیت[4]» از مفهومی بانام امنیتی‌سازی[5] سخن به میان آورد. این مفهوم مهم، نقش بسزایی در وسعت بخشیدن به فهم حکمرانان از امنیت و همچنین ارائه چارچوبی 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 همکارانش امنیت موضوعی در خصوص بقا است و زمانی کانون توجه قرار می‌گیرد که یک موضوع به‌عنوان تهدید وجودی[6] برای یک مرجع امنیتی مطرح می‌شود. این

1. The Copenhagen School of security studies
2. People, States & Fear
۳. بوزان، بری، مردم، دولت‌ها و هراس، پژوهشگاه مطالعات راهبردی، چاپ ششم، تهران، ۱۳۹۹، ص ۱۲۳.
4. Security: A New Framework for Analysis
5. securitization
6. Existential threat

مرجع امنیتی به‌طور سنتی و نه ضرورتاً دولت است که متشکل از سرزمین، حکومت و جامعه است. مکتب کپنهاگ با در نظر 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 امنیتی ساز و مرجع‌های امنیت 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 امنیتی ساز نظم‌های امنیتی هستند[1].

۱. کالینز، الن، مطالعات امنیت معاصر، پژوهشکده مطالعات راهبردی، چاپ اول، تهران، ۱۳۹۹، ص ۱۹۰.

بخش دوم

بخش دوم

فرایند امنیتی‌سازی

امنیت، سیاست را به ورای قواعد جاافتاده بازی می‌برد و مسئله را به‌صورت نوع ویژه‌ای از سیاست یا به شکل چیزی فراتر از سیاست درمی‌آورد. پس امنیتی کردن را می‌توان نوع حادتری از سیاسی کردن دانست. 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 قرار نمی‌گیرد. 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 سنگین کردن مسائل است درمی‌گذرد باید تهدیدی وجودی باشد، زیرا می‌تواند کل فرایند سبک و سنگین کردن 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 امنیتی ساز مدعی می‌شود که حق دارد با مسئله موردبحث با توسل به وسایل فوق‌العاده برخورد کند و قواعد بازی سیاسی را بشکند. پی امنیت رویه‌ای خود مرجع و معطوف به خود است، زیرا طی خود این رویه است که مسئله‌ای را به یک مسئله امنیتی مبدل می‌کند[1].

۲-۱- سطوح تحلیل

بحث بر سر سطوح تحلیل، جایگاهی محوری در نظریات امنیتی دارد. منظور از سطوح تحلیل، مسائل تحلیل است که روی طیفی از مقیاس‌های فضایی-مکانی، از کوچک به بزرگ تعریف‌شده‌اند. سطوح تحلیل کانون‌هایی هستند که در آن‌ها هم نتایج و هم مثابه تبیین را می‌توان یافت. در بررسی‌های امنیتی و مطالعات روابط بین‌الملل، سطوح تحلیل پنج‌گانه‌ای که بیش از همه رایج هستند عبارت‌اند از:

نظام‌های بین‌المللی به معنی بزرگ‌ترین همتافت‌های متشکل از واحدهای متعامل یا به هم وابسته که هیچ‌گونه سطح منظومه‌ای بالاتر از آن وجود ندارد. در حال حاضر این سطح کل کره زمین را در برمی‌گیرد.

خرده نظام‌های بین‌المللی به معنی گروه‌هایی از واحد در نظام

۱. بوزان، بری و همکاران، چارچوبی تازه برای تحلیل امنیت، پژوهشکده مطالعات راهبردی، چاپ سوم، تهران، ۱۳۹۹، ص ۵۲-۵۳.

بین‌المللی که به‌واسطه سرشت یا شدت تعاملاتشان با یکدیگر می‌توان آن را از نظام کل تشخیص داد. این خرده نظام‌های می‌توانند یا دارای قلمروی‌ای منسجم باشند و یا فاقد چنین قلمرو منسجمی باشند. در صورت فقدان قلمرو منسجم، این خرده نظام‌ها دیگر منطقه‌ای نبوده و صرفاً خرده نظام هستند.

واحدها به معنی بازیگرانی تشکیل یافته از خرده گروه‌ها، سازمان‌ها و جوامع مختلف و افراد متعددی که از چنان انسجامی برخوردارند که می‌توان آن‌ها را از واحدهای دیگر تمییز داد (مانند کشورها، دولت‌ها و شرکت‌های فرامرزی).

واحدهای فرعی به معنی گروه‌های سازمان‌یافته از افراد در دل واحدهای ک قادر به تأثیرگذاری بر رفتار واحد باشند (مانند دیوان‌سالارها و کارچاق‌کن‌ها).[1]

افراد که نازل‌ترین سطح تحلیل هستند.

یکی از مهم‌ترین دستاوردهای مکتب امنیتی کپنهاگ، معرفی مناطق به‌عنوان مهم‌ترین واصلی‌ترین سطح تحلیل و پرداختن به آن است. به باور بوزان، پس از پایان جنگ سرد روابط بین‌الملل سرشتی منطقه‌ای پیداکرده است. تضعیف رهبری در سطح جهانی و تضعیف پایبندی قدرت‌های بزرگ به تعهدات جهانی با فروپاشی شوروی، این فرض را تقویت می‌کند که مناطق در مقایسه با گذشته دست‌باز تری برای سامان دادن به امور خود دارند. ازلحاظ سطوح تحلیل، مناطق نوع ویژه‌ای از خرده نظام‌ها هستند. دسته‌بندی جغرافیایی یکی از ویژگی‌های مهم خرده نظام‌های بین‌المللی است. اهمیت مناطق در مکتب کپنهاگ موجب گردید تا بوزان به همراه اُلی ویرو[2]،

۱. برای مطالعه بیشتر در این خصوص به فصل اول کتاب «**چارچوبی تازه برای تحلیل امنیت**» رجوع کنید.

2. Ole Waever

«نظریه مجموع امنیتی منطقه‌ای[1]» را طراحی کند. بوزان در کتاب «مناطق و قدرت‌ها: ساختار امنیت بین‌الملل[2]» به شرح این نظریه می‌پردازد. ایده اصلی این نظریه این است که چون انتقال تهدیدها در فواصل کوتاه‌تر به‌مراتب راحت‌تر از انتقال آن در فواصل طولانی است، ازاین‌رو، وابستگی متقابل امنیتی به‌صورت طبیعی به الگوی دسته‌بندی‌های منطقه‌ای این مجموعه‌ها تبدیل می‌شود. ازنظر تاریخی اغلب دولت‌ها در وهله اول نگران قابلیت‌ها و نیات همسایگان خود بوده‌اند. میزان وابستگی متقابل امنیتی و فرایندهای امنیتی شدن در میان بازیگران داخلی چنین مجموعه‌هایی به‌مراتب بیشتر از همین میزان بین بازیگران داخلی و مجموعه‌های خارج از آن‌ها است. ممکن است قدرت‌های جهانی در مقیاس وسیع در این مجموعه‌ها نفوذ کنند، اما پویش‌های منطقه‌ای به میزان درخور توجهی مستقل از الگوهای مدنظر قدرت‌های جهانی هستند. ترسیم چهره مناسبی از امنیت جهانی مستلزم فهم هر یک از سطوح به شکل مستقل و نیز تعامل آن‌ها است[3].

مکتب کپنهاگ در بیشتر مواقع رهیافتی اروپا محور تلقی می‌شود؛ رهیافتی که بازتاب‌دهنده موضوع‌ها و نگرانی‌های امنیتی اروپا است[4]. آموزه‌های این مکتب، با برجسته‌سازی سطح تحلیل امنیت منطقه‌ای تأثیر قابل‌توجهی بر استراتژی امنیتی اروپای پس از جنگ سرد گذاشت. در پارادایم امنیتی جدید اروپا، با گره خوردن امنیت تمامی کشورهای این قاره به همدیگر، مفهوم امنیت ملی جای خود را به امنیت جمعی داده است. بر همین مبنا، هرچند پیشینه بسیاری از پیمان‌های و توافق‌نامه‌های یکپارچه ساز اروپایی به سال‌های

1. Regional security complex theory
2. Regions and Powers: The Structure of International Security
3. بوزان، بری، ویرو، اُلی، مناطق و قدرت‌ها: ساختار امنیت بین‌الملل، پژوهشکده مطالعات راهبردی، چاپ سوم، تهران،۱۳۹۸، ص ۱۶.
4. کالینز، الن، مطالعات امنیت معاصر، ص ۲۰۱.

آغازین دهه پنجاه میلادی و پس از جنگ دوم جهانی بازمی‌گردد، باوجوداین، 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 اتفاق آفرین 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[1].

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[2] 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[3] شد. در کنار دستاوردهای مهمی چون توافق بر سر ایجاد پول مشترک (یورو) دستگاه قضایی مشترک (یورو جاست)[4] و پلیس مشترک (یورو پُل[5])، توافق بر سر سیاست امنیتی مشترک، به‌عنوان یکی از ستون‌های اصلی پیمان ماستریخت شناخته می‌شود[6]. از این مقطع زمانی به بعد اروپا با جمع سپاری کار ویژه امنیت که همان حفاظت اعضای اتحادیه از تهدیدات وجودی است، تحت تأثیر آموزه‌های امنیتی مکتب کپنهاگ، دستور کارهای جدیدی برای بازوی نظامی خود یعنی سازمان ناتو تعریف کرده است. نکته‌ی مهم دیگری که در اینجا

1. Drafting of the Rome Treaties. (2021). Retrieved 14 July 2021, from https://www.cvce.eu/obj/drafting_of_the_rome_treaties-en-8efe2279-ee12-4a75-aeeb-0bd547f4128f.html
2. Maastricht Treaty
3. European Community
4. Eurojust
5. Euro Pool

۶. هریسی نژاد، کمال‌الدین، نظری به پیمان ماستریخت و اتحاد اروپا، فصلنامه جغرافیا و برنامه‌ریزی، پاییز ۱۳۷۴ - شماره ۱، ص ۱۴۷ و ذاکریان امیری، مهدی، فرآیند اتحاد اروپا، فصلنامه دین و ارتباطات، تابستان ۱۳۷۸، شماره ۱۰، ص ۹۹.

لازم به ذکر است، تحولات عمیق بعد نظامی امنیت در نظم امنیتی جدید است. در این شرایط، بعدی نظامی امنیت بافاصله گرفتن از معنای سنتی خود افق‌های جدیدی پیش روی 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.

۲-۲- 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[1]. امنیت سایبری اولین شرط برای فراهم ساختن بستر رشد و پیشرفت فنّاوری در جهان 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[2] 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

1. What is Cyber Security? (2021). Retrieved 22 July 2021, from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
2. Internet lifestyle

فضای مجازی در زندگی اجتماعی، تهدیدات سایبری همان‌گونه که پیش‌تر مورداشاره قرار گرفت 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 متعقب آن منطقه‌ای منظور نظر است. پس در چنین مقیاسی از سیاست‌گذاری امنیت سایبری را باید به‌مثابه یک استراتژی و هم‌زمان یک چارچوب عملیاتی[1] در نظر گرفت، موضوعی که جایگاه خود را به‌عنوان عنصری اساسی در تمام ابعاد سیاسی، اجتماعی، اقتصادی، نظامی و زیست‌محیطی امنیت تثبیت کرده است[2].

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. در حال حاضر 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 چارچوبی 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.

1. operational framework
2. Efthymiopoulos, M.P. A cyber-security framework for development, defense and innovation at NATO. J Innov Entrep 8, 12 (2019).

ازآنجاکه امنیت ملی و استراتژی‌های دفاعی امروزه به‌شدت به پروتکل‌های امنیت سایبری و پیاده‌سازی آن متکی هستند، در نظر گرفتن سطح چندبعدی تهدیدها و چالش‌های فضای سایبر و تجزیه‌وتحلیل آن‌ها به حصول امنیت و فراهم ساختن سازوکارهای پیشرفت فناوری‌های دفاعی کمک شایان توجهی می‌کند. برای مناطقی همچون اروپا که هم تافت های 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 چارچوب 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 پیش روی 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.

۲-۳- دستور کار دفاع جمعی

اصل دفاع جمعی، شاکله بنیان‌گذاری سازمان ناتو است. این‌یک 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 هم تافت امنیتی ساخته است. پیشینه ایجاد اصل دفاع جمعی به سال ۱۹۴۹ بازمی‌گردد که در آن هسته اولیه تشکیل ناتو به دنبال 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 بر می‌گیرد:

در قلمرو هر یک 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 ین مناطق یا هر منطقه دیگری در اروپا که نیروهای تصرف کننده هر یک از دولت‌ها در تاریخ لازم‌الاجرا شدن این پیمان مستقر هستند یا در دریای مدیترانه و یا منطقه آتلانتیک شمالی در شمال مدار رأس‌السرطان.

ماده ۹ اساس‌نامه نیز اشعار می‌دارد که دولت‌های عضو موظف هستند شورایی تأسیس کنند که همه‌ی آن‌ها در آن نمایندگانی داشته تا مسائل مربوط به اجرای مفاد پیمان موردتوجه 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 پاترویت 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.[1]

از سال ۲۰۱۴ و به دنبال بالا گرفتن منازعات میان اکران و روسیه، افزایش چالش‌های امنیتی در خاورمیانه و ظهور داعش در چندین قاره،

1. Collective defense - Article 5. (2021). Retrieved 31 July 2021, from https://www.nato.int/cps/en/natohq/topics_110496.htm

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 ۵۰۰۰ 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[2].

در طول یک دهه اخیر، ناتو اقدامات متعددی در خصوص تسری امنیت سایبری به ماده ۵ اساس‌نامه انجام داده است تا با به‌رسمیت‌شناسی آن به‌عنوان یک بستر عملیاتی جدید، بتواند از امنیت زیرساخت‌های اینترنتی، شبکه‌ها و سامانه‌های خود محافظت کند و در این فضا به عملیات بپردازد. در بخش‌های بعدی توضیحاتی بیشتری در این خصوص ارائه خواهد شد.

1. NATO›s ‹Eye In The Sky›
2. NATO›s ‹Eye in the Sky›. (2021). Retrieved 31 July 2021, from https://www.napma.nato.int/awacs/a0.html

بخش سوم

بخش سوم

امنیتی‌سازی تهدیدات سایبری توسط ناتو

لزوم به‌رسمیت‌شناسی تهدیدات سایبری به‌عنوان یک تهدید وجودی علیه امنیت جمعی اعضای ناتو برای اولین بار 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 قرارگرفته 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]. 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.

1. Collective defense - Article 5. (2021). Retrieved 15 July 2021, from https://www.nato.int/cps/en/natohq/topics_110496.htm

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 قابل‌توجهی افزایش‌یافته و این فرایند در آینده نیز به‌مراتب بیشتر خواهد شد[1]. چالش‌های مداوم و درعین‌حال 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 مواجه با چالش‌های پیش روی خود به شکل مناسبی اقدام می‌کند؟

۳-۱- اهداف و چالش‌ها

اصلی‌ترین هدف ناتو از تسری استراتژی دفاع جمعی به فضای مجازی بار ها در نشست های سران اتحاد مطرح‌شده 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 کند[2].

1. NATO Review - NATO's role in cyberspace. (2019). Retrieved 18 July 2021, from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
2. Lewis, D. (2019). What Is NATO Really Doing in Cyberspace? - War on the Rocks. Retrieved 18 July 2021, from https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/

در این رهگذر، بزرگ‌ترین واصلی‌ترین چالش پیش روی 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 درزمینهٔ 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. به‌عنوان‌مثال، 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 مور ناتو با تهدیدات سایبری هست[1]. فرماندهی سایبری ایلات متحده آمریکا[2] بر این باور است که دشمنان آمریکا به شکل مداوم برای کسب منافع استراتژیک در فضای سایبر علیه ایلات متحده 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.

هرچند که ناتو رسالت خویش را در ماده ۵ پیمان‌نامه تعریف کرده است، اما سابقه قابل‌توجهی در اقدامات مادون نظامی دارد.

1. Achieve and Maintain Cyberspace Superiority, Available at: https://www.cybercom.mil/
2. The United States Cyber Command

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. در خصوص فضای سایبر نیز ناتو باید معین 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 بی اندازد. چالش‌های پیش روی ناتو، تعدد ذی‌نفعان، تهدیدات بی‌شمار فضای مجازی و تغییر پرشتاب این عرصه آسیب‌پذیری‌های کشورهای عضو ناتو را بیش‌ازپیش افزایش می‌دهد و فرصتی برای سیاست‌گذاری‌های زمان‌بر باقی نمی‌گذارد.

۳-۲- پیش‌زمینه طراحی سیاست دفاع سایبری ناتو

کارشناسان سایبری ناتو، مجموعه حملات سایبری روسیه به کشور استونی در سال ۲۰۰۷ را نقطه عطفی تاریخی در خصوص شکل‌گیری استراتژی دفاع سایبری در اروپا می‌دانند. در صبح ۲۷ آوریل سال ۲۰۰۷، خدمات دیجیتال کشور استونی از دسترس خارج شدند. این اولین بار در تاریخ بود که یک حمله همه‌جانبه متوجه کلیت یک دولت می‌شد. مراکز اداری، بانک‌ها، پایگاه‌های پلیس، بخش بهداشت و درمان، شبکه اینترنت و رسانه‌های آنلاین همگی تحت تاثیر این حمله سایبری قرار گرفت. حملات روسیه اگرچه ماهیت پیچیده و مخربی نداشت، اما در مقیاس بسیار وسیعی انجام‌شده بود و اهمیت آن از این جهات بیشتر بود که کشور استونی یکی از بزرگ‌ترین

پیشگامان دولت الکترونیک در سطح جهان است و بخش اعظمی از سیستم اداره کشور وابسته به اینترنت است[1]. استونی درمجموع ۲۲ روز درگیر این حملات سایبری بود و کل سیستم دیجیتال این کشور مختل شده بود. آژانس اطلاعات استونی[2] به‌سرعت اعلام کرد که این حملات از مبدأ روسیه و از طریق فراخوان‌های گسترده‌ای که کاربران روسی برای مشارکت در حملات سایبری با دستورالعمل‌های ساده منتشر کرده‌اند، انجام می‌شود؛ اما نشانه‌های از انگیزه‌های سیاسی و اختلافات قومیتی میان حوزه بالکان و روسیه نظریه دولتی بودن و سازمان‌یافته بودن این حملات را تقویت می‌کرد[3].

بعد از سه هفته از آغاز این جنگ سایبری، وقت آن فرارسیده بود تا ناتو از میزان آسیب‌پذیری اعضای خود در حوزه سایبری درس بگیرد. از سرقت اطلاعات حساس دولتی تا اخلال در خدمات عمومی یک کشور مانند صنعت برق، راه‌آهن، صنایع دفاعی و ارتباطات؛ یک دولت متخاصم می‌تواند از راه دور و با کمترین هزینه به یک برتری نظامی قابل‌توجه دست‌یافته و بیشترین خسارات را برای دولت قربانی به بار آورد. درواقع، این اولین بار در تاریخ تشکیل ناتو بود که بر اساس ماده ۵ اساس‌نامه یک عضو درخواست کمک در حوزه دفاع سایبری می‌کرد و ناتو هیچ‌گونه آمادگی و برنامه‌ای برای انجام وظایف خود نداشت. غافل‌گیری ناتو سبب شد تا سران کشورهای عضو برای کمک به استونی تشکیل جلسه بدهند. دیگر جای هیچ تردیدی باقی نمانده بود ناتو نیازمند طراحی یک استراتژی در حوزه داغ سایبری است و برای سناریوهای مشابه در آینده می‌بایست آماده شود[4].

1. Herzog, Stephen, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,Journal of Strategic Security, Vol. 4, No. 2, Strategic Security in the Cyber Age (Summer 2011), pp. 49-60.
2. Estonian intelligence agency
3. 2007 cyber-attacks on Estonia, Retrieved 18 July 2021, from https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf
4. How Russia Strengthened NATO's Cyber Defense. (2020). Retrieved 18 July 2021, from https://warsawinstitute.org/russia-strengthened-natos-cyber-defence/

اگرچه این حملات آسیب‌های قابل‌توجهی به بار نیاورد، اما به ناتو هشدار داد تا تهدیدات سایبری را به‌عنوان یک تهدید وجودی علیه دفاع جمعی اعضای اتحاد در نظر بگیرد. درنتیجه، مرکز عالی همکاری‌های دفاع سایبری ناتو به پیشنهاد کشور استونی باهدف پیشگیری از اتفاقات مشابه و همچنین طراحی یک پروتکل ویژه دفاع سایبری برای مواجهه با مدرن‌ترین شیوه‌های جنگی در تالین[1] پایتخت استونی تأسیس شد. این مرکز دریکی از اولین اقدامات خود یک کتابچه راهنما تهیه کرد که به تطبیق ماده ۵ اساس‌نامه ناتو با جنگ‌های سایبری پرداخت. این اولین تلاشی بود که با رویکردی جامع به‌ضرورت های دفاع سایبری در ناتو پرداخت و تا حدودی چالش‌های حقوقی پیرامون آن را روشن ساخت. این کتابچه بعد از انتشار بازتاب گسترده‌ای در مجامع نظامی و رسانه‌های اروپایی پیدا کرد و پیش‌زمینه انجام اقدامات استراتژیک درزمینهٔ دفاع سایبری در ناتو شد.

1. Tallin

بخش چهارم

بخش چهارم

وضعیت فعلی دستور کار امنیت جمعی ناتو در فضای مجازی

با طرح اهداف و چالش‌های پیش روی ناتو در فضای مجازی و مرور مهم‌ترین واقعه زمینه‌ساز طراحی سیاست دفاع سایبری ناتو در این بخش به‌منظور آشنایی با وضعیت فعلی دستور کار امنیت جمعی ناتو در فضای مجازی، مهم‌ترین اقدامات که تاکنون ناتو برای تحقق دفاع جمعی در بستر اینترنت انجام داده است را مرور می‌کنیم. به این منظور، لازم است تا اصلی‌ترین نشست های سالانه اعضای ناتو که در سطح سران ارشد کشورهای عضو تشکیل‌شده است و امنیت سایبری جزو دستور کار آن‌ها بود است موردبررسی قرار گیرد.

۴-۱- اجلاس سال ۲۰۱۴ سران ناتو در ولز

یکی از اصلی‌ترین وظایف مرکز عالی همکاری‌های دفاع سایبری ناتو، تعیین تکلیف در خصوص چلاش های حقوقی استراتژی دفاع سایبری در میان کشورهای عضو اتحاد بود. بر همین اساس، این چالش‌های حقوقی در دستور کار اجلاس سال ۲۰۱۴ ولز[1] قرار گرفت. رهیافت‌ها و دست‌آوردهای مهم این اجلاس، آن را به یکی از مهم‌ترین مقاطع دفاع سایبری ناتو تبدیل کرده است. این اجلاس

1. Wales

در سپتامبر سال ۲۰۱۴ در سطح سران ارشد کشورهای عضو ناتو در شهر نیوپورت[1] برگزار شد. استراتژی دفاع سایبری ناتو یکی از مهم‌ترین رئوس این اجلاس بود. در طول نشست، گفتگو بر سر چالش‌های حقوقی دفاع سایبری منتج به این شد که ناتو قوانین بین‌المللی در خصوص جنگ را در فضای مجازی نیز به رسمیت شناخته و اعمال کند. با انطباق قوانین بین‌المللی و عرف‌های جنگی بر فضای مجازی، اولین مصوبه این اجلاس تسری حملات سایبری به ماده ۵ اساس‌نامه ناتو بود[2]. بااین‌حال، بر اساس پاراگراف ۷۲ اعلامیه نشست ولز، تشخیص این امر که یک حمله سایبری مشمول ماده ۵ می‌گردد بر عهده سران شورای آتلانتیک خواهد بود. نتیجه مهمی که در آن مقطع زمانی از این شرط به دست می‌آمد، تجویز موردی و به‌عبارت‌دیگر استثناء تلقی کردن تسری بود و همچنان اصل بر عدم شمول حملات سیبری بر دفاع جمعی باقی ماند؛ اما چنان‌چه شورای آتلانتیک تشخیص بدهد که حمله سایبری به یکی از اعضا، مشمول ماده می‌گردد، این حمله به‌مثابه حمله به‌تمامی اعضای ناتو بوده و راه برای اقدام علیه تجاوز سایبری باز می‌شود. در این خصوص ناتو می‌تواند برای بازگشت وضع به حالت سابق و برقراری امنیت سایبری حتی از گزینه‌های نظامی نیز استفاده کند. مشخصاً تلقی کردن حملات سایبری به‌عنوان یک حمله نظامی یکی از اقدامات پیش‌رونده ناتو در استراتژی امنیت سایبری پیمان آتلانتیک شمالی تلقی می‌شود و این جزء دستاوردهای مهم اجلاس ولز است. نکته مهمی که در این خصوص لازم به ذکر است عبارت از این است که وزارت دفاع ناتو برای پیشنهاد این مؤلفه، تحت تأثیر

1. Newport
2. Wales Summit Declaration, Paragraph 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm

جنگ‌های سایبری در طول دوران ناآرامی‌های سوریه، گرجستان و اکراین قرار داشته است. جیم پاتریک شی[1] دستیار وقت دبیر کل ناتو و معاون چالش‌های امنیتی نوپدید[2] این سازمان در این خصوص بیان می‌کند اتفاقات اخیر در جنگ سوریه و حتی اکراین به ما ثبات کرد که حملات سایبری به بخش جدایی‌ناپذیر جنگ‌های حال حاضر تبدیل‌شده است و وسعت خرابکاری در آن‌ها واقعاً معتنابه است[3].

آموزش نیروهای ویژه سایبری یکی دیگر موضوعات مهمی بود که در اجلاس ولز به‌عنوان یکی از حیاتی‌ترین بخش دفاع سایبری به آن پرداخته شد. در طول اجلاس، کشور استونی پیشنهاد داده بود تا وظیفه آموزش نیروهای متخصص در حوزه دفاع سایبری را بر عهده بگیرد که این پیشنهاد توسط فرماندهی عالی ناتو مورد تائید قرار گرفت. به همین منظور، کشور استونی موظف گردید در ارتباط با مدرسه ارتباطات و اطلاعات ناتو[4] واحد آموزش سایبری ناتو را میزبانی کند[5]؛ اما مبحث مهم آموزش، صرفاً در اجلاس ولز به شکلی مقدماتی موردبررسی قرار گرفت و تعیین جزئیات و نقشه راه آن به آینده موکول شد.

۴-۲- اجلاس سال ۲۰۱۶ سران ناتو در ورشو

در جولای سال ۲۰۱۶ کشور لهستان میزبان اجلاس سران ناتو بود. این اجلاس بنا بر شرایط جدید حاکم بر منطقه اروپا به‌شدت موردتوجه قرار گرفت. در کنار انجام چندین عملیات تروریستی توسط

1. Jamie Patrick Shea
2. Emerging Security Challenges
3. Steve Ranger, NATO updates cyber defense policy as digital attacks become a standard part of conflict, https://www.zdnet.com/
4. NATO Communications and Information School
5. CCDCOE. (2021). Retrieved 19 July 2021, from https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/#footnote_6_2663

گروه داعش در قلب اروپا، اصلی‌ترین دلیل اهمیت یافتن این اجلاس مربوط به تغییر نگاه ناتو به فدراسیون روسیه بود. آن‌طور که از ماه قبل از ملاقات سران ارشد ناتو پیش‌بینی می‌شد، رفتارهای توسعه‌طلبانه روسیه باعث گردید که ناتو دیگر به‌عنوان یک شریک به این کشور نگاه نکرده و دست به اتخاذ راهبردهای محتاطانه‌تری در رابطه با روسیه بزند. رهبران ناتو به این باور رسیده‌اند که روسیه در اکثر درگیری‌های منطقه‌ای و فرا منطقه‌ای به نحوی دخالت دارد و ناتو نیازمند آن است تا مشخص کند تدابیر گذشته کافی است یا خیر. از همین رو، در کنار بازنگری در سیاست‌های موشکی و هسته‌ای، ناتو بازنگری در استراتژی دفاع سایبری را نیز در دستور کار اجلاس ورشو قرارداد.

برخلاف نظریاتی که تا پیش این در خصوص تهدیدات امنیتی جنگ‌های سایبری در ناتو مطرح‌شده بود، در اجلاس ورشو کارشناسان اعلام کردند که جنگ‌های سایبری اگرچه به‌تنهایی دامنه آسیب‌زایی گسترده‌ای می‌توانند داشته باشند، اما چالش اصلی در مواجهه با حملات سایبری استفاده از آن در کنار دیگر شیوه‌های متعارف و غیرمتعارف جنگی است؛ به‌عبارت‌دیگر، اکنون حملات سایبری در جنگ‌های ترکیبی (هیبریدی) تبدیل به یک رکن اصلی شده است و پیامدهای آن را به‌شدت افزایش داده است[1]. آنچه در اجلاس ورشو به‌عنوان یک تهدید وجودی ناشی از فضای مجازی مطرح گردید، تبدیل آن به یک سلاح مخرب بود[2]. این مسئله خصوصاً در قالب انتشار سازمان‌یافته اخبار جعلی به‌منظور اثرگذاری

1. The 2016 NATO Summit: What will be on the agenda in Warsaw? | SIPRI. (2016). Retrieved 20 July 2021, from https://www.sipri.org/commentary/topical-background-er/2016/2016-nato-summit-what-will-be-agenda-warsaw

۲. Weaponization- در اصل به عملی گفته می‌شود که در آن یک‌چیز که ماهیت غیرنظامی دارد تبدیل به یک اسلحه شده و مورداستفاده نظامی قرار بگیرد.
WEAPONIZATION (noun) definition and synonyms | Macmillan Dictionary. (2021). Retrieved 20 July 2021, from https://www.macmillandictionary.com/dictionary/british/weaponization

بر افکار عمومی، رویدادهای مهم سیاسی، روحیه سربازان و ایجاد آشوب در پشت جبهه نبرد به‌شدت خود را نشان می‌دهد و روسیه به این وسیله امنیت جمعی کشورهای عضو اتحاد را موردتعدی قرار می‌دهد.

اخبار جعلی به‌عنوان یکی از اصلی‌ترین تهدیدات وجودی علیه امنیت کشورهای عضو ناتو در نظر گرفته می‌شود. انتشار سازمان‌یافته اخبار جعلی توسط رقبا و دشمنان اعضای ناتو می‌تواند منجر به وقوع فجایع ویرانگری به گستردگی یک جنگ تمام‌عیار منطقه‌ای شود. دبیر کل ناتو، ینس استولنبرگ[1] معتقد است ظهور شبکه‌های اجتماعی و افزایش اثرگذاری آن‌ها مبارزه با اخبار جعلی را بسیار پیچیده‌تر از قبل کرده است. نگران‌کننده‌ترین جنبه‌ی این فرایند که معروف به جهان پس از حقیقت است، بی‌اهمیتی کاربران شبکه‌های اجتماعی به امر حقیقت است. از همین رو، ناتو در نشست ورشو اقدامات مقدماتی در خصوص مبارزه هدفمند با اخبار جعلی و کنترل گردش اطلاعات را مورد تأکید قرارداد و تکامل و ارتقای این اقدامات را منوط به انجام پروژه‌های مطالعاتی گسترده و آغاز برنامه‌های آزمایشی کرد.

یکی از مهم‌ترین موضوعاتی که در اجلاس ولز مورد تأکید سران ناتو قرار گرفت، موضوع شناسایی فضای مجازی به‌عنوان یکی از بسترهای عملیاتی سازمان پیمان آتلانتیک شمالی بود. باوجوداین، با توجه به مناقشه برانگیز بودن این تصمیم و پیامدهای حقوقی و نظامی مترتب بر این امر، اعضای سازمان در سال ۲۰۱۴ به نتیجه قطعی نرسیدند. این موضوع مهم در اجلاس ورشو به شکل کامل تعیین تکلیف شد.

1. Jens Stoltenberg

ناتو در راستای به‌رسمیت‌شناسی فضای مجازی به‌عنوان بستر جدید اجرای عملیات، از سال ۲۰۱۶ تاکنون مبادرت به اقدامات مهمی نموده است. یکی از قابل‌توجه‌ترین اقدامات ناتو، تأسیس مرکز عملیات فضای مجازی[1] هست. مقر فرماندهی این مرکز در شهر مونس[2] کشور بلژیک واقع‌شده است. این مرکز به‌عنوان بازوی کلیدی ناتو در فضای مجازی فعالیت می‌کند و مسئول کنترل و هشدار زودهنگام[3] تهدیدات مخرب سایبری، برنامه‌ریزی متمرکز برای جبهه‌های مختلف عملیات در فضای مجازی، سازمان‌دهی مأموریت‌های اعضای پیمان و ایجاد هماهنگی میان آن‌ها است. بازدارندگی سایبری، هسته اصلی تشکیل‌دهنده مرکز عملیات فضای مجازی ناتو است و به‌نوعی ارتش سایبری متحدان پیمان آتلانتیک شمالی تلقی می‌شود. از دیگر رئوس اصلی وظایف این مرکز مقابله با حملات سایبری دولتی و سایبر تروریسم سازمان‌یافته است. این مرکز در ارتباط مستقیم با مرکز عالی همکاری‌های دفاع سایبری ناتو[4] است که وظیفه تأمین پشتوانه علمی و پژوهشی دفاع سایبری ناتو را بر عهده دارد. پیش‌نیازها و محتواهای آموزشی، چشم‌اندازهای عملیاتی و نیروهای تربیت‌شده خبره از طریق این مرکز در اختیار مرکز عملیات فضای مجازی ناتو قرار می‌گیرد[5].

همان‌طور که پیش‌تر مورداشاره قرار گرفت، سیاست‌های امنیتی جداگانه اعضای اتحاد در خصوص تهدیدات سایبری یکی از چالش‌های جدی ناتو در مواجهه مور با این فضا هست. مرکز عملیات فضای مجازی موظف است تا سال ۲۰۲۳ با ادغام توانایی‌های دفاع سایبری هر یک از اعضا و یکپارچه‌سازی آن‌ها بر اساس سند محرمانه‌ای که

1. the Cyberspace Operations Centre
2. Mons
3. early warning and control
4. The NATO Cooperative Cyber Defense Centre of Excellence
5. About us. (2021). Retrieved 17 July 2021, from https://ccdcoe.org/about-us/

وزارت دفاع اتحادیه اروپا تدوین کرده و به نقشه راه فضای مجازی[1] معروف است، به این چالش غلبه کند[2]. باوجوداین، ازآنجایی‌که این مرکز بر اساس ماده ۵ پیمان ناتو به فعالیت می‌پردازد، شرح وظایف کنونی آن مبتنی بر اصل دفاع جمعی و پدافند است.

در اجلاس ورشو نیز اعضای ناتو همچنان در خصوص اقدامات آفندی و انجام عملیات سایبری نظامی به شکل تهاجمی، پیش‌دستانه و یا پاسخ ثانویه به توافق قطعی نرسیدند. در صورت دست‌یابی به توافق در این خصوص، مرکز عملیان مونس می‌تواند در جایگاه مرکز عالی فرماندهی نظامی اقدام به جنگ‌های سایبری کند. کشور استونی یکی از اصلی‌ترین پشتیبان‌های رویکرد تهاجمی در حوزه سایبری است[3].

نکته مهمی که به باور کارشناسان در اجلاس ورشو مورد غفلت قرارگرفته عبارت از این است که استراتژی دفاع جمعی و به‌رسمیت‌شناسی فضای مجازی به‌عنوان یک بستر عملیاتی چه وضعیت جدیدی در تعامل ناتو با کشورهای هم‌سود که خارج از پیمان هستند به وجود می‌آورد؛ این نکته ازاین‌رو حائز اهمیت است که کشوری همچون گرجستان هنوز به عضویت ناتو درنیامده است و کشورهای عضوی همچون ایسلند نیز اساساً فاقد ارتش و نیروی نظامی هستند[4]. این نکته به چالش اساسی استراتژی امنیت سایبری داخلی متفاوت کشورهای عضو ناتو و فقدان وحدت رویه در این خصوص، به‌شدت می‌افزاید.

1. Cyberspace Roadmap
2. Bussoletti, F. (2018). NATO, the new Cyber Operations Centre (CYOC) should be fully operative in 2023. Retrieved 17 July 2021, from https://www.difesaesicurezza.com/en/defence-and-security/nato-the-new-cyber-operations-centre-cyoc-should-be-fully-operative-in-2023/
3. Offense as the New Defense: New Life for NATO's Cyber Policy. (2018). Retrieved 18 July 2021, from https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy#_ftnref6
4. NATO Warsaw summit 2016, what about cyber security? (2016). Retrieved 25 July 2021, from https://securityaffairs.co/wordpress/49255/cyber-warfare-2/nato-warsaw-summit-2016.html

در پایان این نشست، سران ناتو در بیانیه‌ای اعلام کردند که متعهد می‌شوند ارتش‌های کشورشان در راستای تحقق اصل دفاع جمعی، همان‌گونه که به محافظت از آسمان، دریا و خشکی می‌پردازند، به فضای سایبری نیز به همین دید نگریسته و امنیت آن را تأمین کنند. آن‌ها همچنین تعهد خود را در قبال دفاع از تمامی اعضای اتحاد اعلام کرده و پذیرفتند که ناتو به‌اندازه ضعیف‌ترین عضو خود در فضای مجازی قوی است و این به معنی آن است که تمامی اعضا موظف هستند تا به بهبود شرایط فعلی کمک کنند. در بخش دیگری از این بیانیه با تأکید بر کاربرد قوانین بین‌الملل در فضای سایبر، به همکاری ناتو با دیگر مجامع بین‌المللی در خصوص ایجاد فضای مجازی ایمن تأکید گردید و کشورهای عضو متعهد به اعتمادسازی و رفتار مسئولانه در فضای مجازی شدند. در بخش پایانی این بیانیه، سران کشورهای عضو به‌عنوان عالی‌ترین نمایندگان کشورهای خود در ناتو متعهد شدند تا در سطح ملی، به‌منظور تقویت توانایی‌های دفاع سایبری کشور خود بودجه‌های کلان مالی تخصیص دهند؛ با تمامی ذی‌نفعان ناتو همکاری و تعامل کنند؛ درک خود از تهدیدات سایبری را با اشتراک‌گذاری اطلاعات با دیگر اعضا بهبود بخشند؛ به شکل همه‌جانبه از زیرساخت‌های سایبری اروپا دفاع کنند؛ به‌صورت مستمر عملکرد ملی خود را ارزیابی کرده و گزارش آن را به ناتو تحویل دهند؛ و درزمینهٔ آموزش نیروهای متخصص فضای مجازی و شرکت در رزمایش‌ها و دوره‌های آموزشی و میزبانی از این دوره‌ها به شکل مؤثر مشارکت کنند[1].

1. Cyber Defense Pledge. (2021). Retrieved 27 July 2021, from https://www.nato.int/cps/en/natohq/official_texts_133177.htm

۴-۳- اجلاس سال ۲۰۱۸ سران ناتو در بروکسل

سران کشورهای عضو ناتو در نشست بروکسل می‌بایست در خصوص موضوعات مهمی تصمیم‌گیری می‌کردند. دفاع از پیمان ناتو در قبال تهدیدات خارجی، تقویت اتحاد و بازدارندگی، مبارزه با تروریسم و تعدیل بار مسئولیت بین اعضا از رئوس مهم این اجلاس بود. در این اجلاس مقرر گردید تا به‌منظور اطمینان از آمادگی نیروهای ناتو در مواجهه با تهدیدات سایبری و دسترسی اعضا به سریع‌ترین شکل از پشتیبانی، کشورهای عضو ناتو رزمایش‌های متعددی در آینده انجام دهند. مدرنیزه کردن ساختار فرماندهی نظامی با ایجاد ستاد فرماندهی مشترک در ایالات‌متحده آمریکا، واحد پشتیبانی و توانمندسازی در آلمان و راه‌اندازی گروه‌های پشتیبانی ضد نبردهای هیبریدی[1] ازجمله ابتکارات مهم این اجلاس محسوب می‌گردد.

این اجلاس به شکل ویژه‌ای بر دفاع سایبری و افزایش امنیت سایبری متمرکز بود. یکی از تصمیمات مهمی که در این اجلاس گرفته شد، الزام کشورهای عضو به فعالیت در فضای مجازی بر اساس ماده ۳ اساس‌نامه ناتو است. بر اساس این ماده، دولت‌های عضو موظف هستند به‌منظور دستیابی هرچه بیشتر به اهداف این پیمان، به‌صورت انفرادی یا جمعی، به‌وسیله خودیاری و کمک‌های متقابل به‌صورت مداوم و مؤثر، ظرفیت‌های فردی یا جمعی خود را حفظ کرده و توسعه دهند تا در مقابل حملات مسلحانه مقاومت نمایند[2]. ماده ۳ اساس‌نامه ناتو را در حقیقت می‌بایست پیش‌شرط تحقق هدف دفاع جمعی (ماده ۵) دانست. بر این مبنا، تعهد فردی هر یک از متحدان برای افزایش تاب‌آوری و تقویت توانایی‌های

1. counter-hybrid support
2. Resilience and Article 3. (2021). Retrieved 26 July 2021, from https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=The%20principle%20of%20resilience%20is,develop%20their%20individual%20and%20collective
360-degree approach to security

بازدارنده خود از آسیب‌پذیری پیکره ناتو می‌کاهد. در دستور کار ناتو، تاب‌آوری بیش از هر چیز یک مسئولیت ملی است و هر عضو اتحاد برای مقابله و پاسخ‌دهی به‌تمامی تهدیدات وجودی و بحران‌های پیش‌بینی‌شده توسط ناتو باید به‌اندازه کافی قوی و سازگار باشد.

حال با الزام کشورهای عضو به تسری ماده ۳ به سیاست‌های امنیت سایبری، ناتو در تلاش است تا دفاع جمعی در فضای سایبر به شکل موثق‌تری تحقق یابد. کشورهای عضو موظف هستند که با تشکیل واحدهای سایبری در ارتش‌های خود و آموزش نیروهای زبده در این زمینه، برای مقابله با هر تهدیدی در فضای سایبر، بر اساس دستورات ناتو آماده باشند.

اجلاس بروکسل در بخش دیگر از تصمیمات خود دستور کار امنیتی جدیدی برای کشورهای عضو تدوین نمود. این راهبرد جدید برای تأمین امنیت سایبری «رویکرد ۳۶۰ درجه‌ای امنیت » نام دارد. بر این اساس، کشورهای عضو می‌بایست تمرکز خود را بر کمپین‌های اخبار جعلی، تلاش‌های دشمنان برای دخالت در فرایند انتخابات و فعالیت‌های مخرب سایبری به‌عنوان سه چالش هیبریدی قرار دهند. در رویکرد ۳۶۰ درجه‌ای امنیت، ناتو عزم خود را برای کنترل فضای سایبری و تهدیدات پیش‌رونده آن جزم کرده است و بازیگران غیردولتی که تحت حمایت دولت‌ها قرار دارند، به‌عنوان تهدیدات نوظهور علیه امنیت سایبری مورد شناسایی قرار می‌گیرند.

یکی از نکات جالب‌توجه در اجلاس بروکسل، تصمیم‌گیری در خصوص سوءاستفاده گروه‌های تروریستی از فضای مجازی بود. ناتو تصمیم گرفته است تا به‌منظور تأمین امنیت فضای مجازی،

شناسایی مجرمان و بهبود قابلیت‌های اعضا برای مبارزه با تروریسم سایبری داد های بیومتریک[1] کاربران را جمع‌آوری و پردازش کند. ناشناسی کاربران در فضای مجازی یک تهدید جدی علیه امنیت ناتو تلقی می‌شود. همان‌طور که پیش‌تر مطرح گردید، بازیگران غیردولتی امروزه با استفاده از فرصت ناشناسی در قالب گروه‌های مجرمانه سازمان‌یافته، تروریسم، هکر و کلاه‌بردار امنیت کشورهای عضو ناتو را به خطر می‌اندازند. این بازیگران وقتی با نیروهای ناتو مواجه می‌شوند، سعی می‌کنند به بهترین شکل ناشناسی خود را حفظ کرده و آسیب زندگی خود را از این طریق به حداکثر برسانند. در اجلاس بروکسل، سران ناتو با دریافت نظر کارشناسان متعدد به این نتیجه رسیدند که برای تأمین امنیت اتحاد لازم است تا با استفاده از روش‌های موجود این افراد شناسایی شوند و کاهش توانایی ناشناس ماندن آن‌ها در اولویت امنیت سایبری ناتو قرار بگیرد. به همین منظور، استفاده از داده‌های بیومتریک و تجزیه‌وتحلیل آن‌ها یکی بهترین استراتژی‌های ناتو در نظر گرفته می‌شود.

داده‌های بیومتریک عبارت است از روش شناسایی منحصربه‌فرد انسان‌ها بر مبنای یک یا چند ویژگی یا مشخصه طبیعی، بیومتریک به‌ویژه به‌عنوان یک شیوه مدیریت دسترسی به هویت و کنترل دسترسی و عمدتاً در گروه‌های تحت نظارت مورداستفاده قرار می‌گیرد. معرف‌های بیومتریک یا زیست‌سنجی شناسایی به دو گروه اصلی تقسیم می‌شوند:

فیزیولوژیکی: در ارتباط با شکل بدن مانند اثرانگشت، شناسایی چهره، تصویربرداری از شبکیه چشم،DNA، دست‌نگاری، صدا نگاری و...

1. biometric data

رفتاری: مرتبط با رفتارهای گوناگون فرد مانند آهنگ و روش تایپ کردن، شیوه راه رفتن و ...

برخی از محققین برای گروه اخیر اصطلاح مؤلفه‌های رفتار سنجی را در مقابل مؤلفه‌های زیست‌سنجی در گروه اول ابداع نموده‌اند.[1]

افزایش کیفیت بهره‌برداری از داده‌های بیومتریک در ارتباط مستقیم با پایگاه داده‌ای که اطلاعات در آن ذخیره می‌شود و نحوه عملکرد آن قرار دارد. از همین رو، ناتو اقدام به تأسیس مرکزی تخصصی برای ذخیره و پردازش داده‌های بیومتریک کرده است. این مرکز دارای یک سیستم بانام سیستم شناسایی خودکار داده‌های بیومتریک ناتو[2] امکان ذخیره‌سازی و آرشیو کردن حجم عظیمی از داده‌ها و جستجو و تطبیق خودکار آن‌ها با همدیگر را دارد. همچنین این سیستم در یک فضای کنترل‌شده، امکان اشتراک‌گذاری داده‌های بیومتریک میان تمام اعضای ناتو را فراهم کرده است.[3] از سوی دیگر کشورهای عضو موظف هستند که آرشیو اطلاعات بیومتریک خود را که پیش‌تر به شکل داخلی جمع‌آوری و پردازش کرده‌اند را به این سامانه منتقل کنند.

اطلاعات پیرامون سامانه نابیس بسیار محدود است، اما برابر آنچه تاکنون کارشناسان ناتو مطرح کرده‌اند، این سامانه ابزار برتری نظامی ناتو در فضای مجازی و محیط‌های عملیاتی جنگی است. از مهم‌ترین مزیت‌هایی که این سامانه در اختیار ناتو قرار می‌دهد می‌توان به‌دقت بالای علمی، خودکارسازی در سریع‌ترین زمان، بهره‌برداری فنی و در اختیار داشتن اطلاعات جامع از تروریست‌ها و هکرها و پیش‌بینی پذیر کردن رفتارهای آن‌ها از طریق تحلیل الگو رفتاری موجود درداده های قبلی اشاره کرد[4].

۱. محسنی، فرید، حریم خصوصی اطلاعات، انتشارات دانشگاه امام صادق (ع)، چاپ دوم، تهران، ۱۳۹۴، ص ۳۳۱.
2. NATO Automated Biometrics Identification System (NABIS)
3. Bogdan, R, Cristian, COMAN, NATO Automated Biometric Identification System (NABIS), MTA Review, Vol. XXVII, No. 2, Dec. 2017.
4. Wing Commander Mark Lunan, NEW doctrinal concept BIOMETRICS, The Three Swords Magazine, 33/2018.

آخرین مسئله مهم دیگری که در اجلاس بروکسل موردبررسی قرار گرفت، امکان انتساب مسئولیت حملات سایبری به کشورهای متخاصم بود. با توجه به اینکه ماهیت حملات سایبری به‌گونه‌ای است که به‌سختی می‌توان مسئولیت آن را در فضای سایبر متوجه یک دولت متخاصم کرد و از سوی دیگر عموماً این حملات به شکل نیابتی و توسط بازیگران غیردولتی انجام می‌گیرد، یکی از دغدغه‌های اصلی ناتو تحمیل هزینه به کشور متخاصمی است که در پشت حملات سایبری به اعضای اتحاد قرار دارد. از همین رو، سران ناتو قدرت انتساب به شکل مستدل و مستند را به‌عنوان یک حق ملی برای اعضای خود به رسمیت شناختند. این حق، امروزه یکی از مناقشه برانگیز ترین موضوعات حقوق بین‌الملل است و همچنان به رسمیت شناختن آن در جوامع بین امیلی موردتردید است. نکته لازم به ذکر در این خصوص آن است که با توجه به ماده ۵ اساس‌نامه ناتو که اقدامات این سازمان را بر پایه دفاع جمعی و مشارکت اعضا تبیین می‌کند، این حق به یک کشور عضو ناتو این امکان را می‌دهد تا به‌صورت مستقل و یک‌جانبه هزینه‌هایی را به کشور متخاصم تحمیل کند، درحالی‌که دیگ اعضا در این فرایند دخالتی ندارند. با توجه به اینکه تسری حملات سایبری به اصل دفاع جمعی همچنان محل بحث و تردید است، این حق امکان جدیدی برای بی‌پاسخ نگذاشتن حملات سایبری علیه اعضای ناتو در نظر گرفته می‌شود.[1]

۴-۴- اجلاس سال ۲۰۲۱ سران ناتو باز هم در بروکسل

اجلاس سال ۲۰۲۱ سران ناتو در ۱۴ ژوئن مجدد در شهر بروکسل برگزار شد.

1. CCDCOE. (2021). Retrieved 27 July 2021, from https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018/#identifier_26_3346

پاندمی کرونا، این اجلاس را همانند بسیاری از اجلاس‌های مهم چندین ماه اخیر تحت تأثیر قرارداد. باوجوداین، 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 ریاست‌جمهور 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 و در پشت‌صحنه اغلب حملات سایبری به ناتو رد پایی از این کشور به چشم می‌خورد. 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، موجهی از حملات سایبری علیه زیرساخت‌های کشاورزی و انرژی ایالات‌متحده آمریکا صورت گرفت. این حملات سایبری که خسارت‌هایی را نیز به ایالت متحده آمریکا تحمیل نمود، 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

کـه ایالات‌متحـده آمریـکا در قبـال جنگ‌هـای سـایبری کـه حقیقـت پذیرفته‌شـده جهـان حـال حاضـر اسـت، قائـل بـه اعمـال برخـی اسـتثنائات اسـت.

آمریـکا معتقـد اسـت کـه در جنگ‌هـای سـایبری بـه برخـی از زیرسـاخت‌های حیاتـی (همچـون سـامانه‌های تأمیـن انـرژی و آب) طرف‌هـای مقابـل نبایـد حملـه کـرد و ایـن موضـوع نقطـه آغـاز بحـث بایـدن و پوتیـن در خصـوص امنیـت سـایبری دو طرف بـود. بایدن فهرسـتی از شـانزده بخـش صنعتـی را به‌عنـوان اهـداف غیرمجـاز در جنگ‌هـای سـایبری بـه پوتیـن پیشـنهاد داد و ایـن دو توافـق نمودنـد کـه کارشناسـانی را بـرای بررسـی جزئیـات ایـن توافـق تعییـن کننـد. بایـدن بـه پوتیـن هشـدار داد کـه چنان‌چـه از ایـن توافـق تعـدی شـود، ارتـش سـایبری ایالات‌متحـده آمریـکا پاسـخ مشـابهی بـه تجـاوز بـه زیرسـاخت‌های حیاتـی خـود خواهـد داد[1]. هفتـه قبـل از ایـن ملاقـات نیـز جـو بایـدن بـه خبرنـگاران گفتـه بـود کـه از نزدیـک در حـال بررسـی طرحـی بـرای پاسـخ بـه حمـلات سـایبری روسـیه علیـه زیرسـاخت‌های غذایـی ایالات‌متحـده اسـت. او در پاسـخ بـه پرسـش یکـی از خبرنـگاران گفـت کـه آمریـکا توانایی سـایبری قابل‌توجهـی دارد و پوتیـن نیـز خـود ایـن را می‌دانـد. واشـنگتن در حـال حاضـر علاقـه‌ای بـه اقـدام فـوری تلافی‌جویانـه نـدارد و همـه‌ی سـناریوهای در حـال بررسـی اسـت[2]. باوجودایـن، پوتیـن همـواره انجـام حمـلات سـایبری از سـویه روسـیه را انـکار کـرده و معتقـد اسـت کـه ایـن حمـلات از سـوی هم‌پیمان‌هـای آمریـکا، همچـون کانـادا و انگلسـتان انجـام می‌گیـرد و آمریـکا خـود نیـز یکـی از اصلی‌تریـن جنایـت‌کاران سـایبری در

1. Walsh, J. (2021). Biden Vows Retaliation on Any Future Russian Hacks on Critical Infrastructure. Retrieved 28 July 2021, from https://www.forbes.com/sites/joewalsh/2021/06/16/biden-vows-retaliation-on-any-future-russian-cyberattacks-on-critical-infrastructure/?sh=3f4aa2591fab
2. Biden says he is 'looking closely' at retaliation over Russian-linked cyber-attack. (2021). Retrieved 28 July 2021, from https://www.nbcnews.com/politics/white-house/biden-says-he-looking-closely-retaliation-over-russian-linked-cyber-n1269413

جهان است[1]. 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 موردگفتگو قرار گرفت 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[2].

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 سبب شده 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 میهمانان برجسته این اجلاس که برای اولین بار در کسوت رئیس‌جمهور ایالت متحده در اجلاس سران ناتو شرکت می‌کرد، سخنرانی مهمی ایراد کرد که بخشی از آم متوجه استراتژی جدید ناتو در خصوص مواجه با تهدیدات فضای مجازی است.

بایدن با ستایش اتحاد ناتو، تأکید کرد که ایالات‌متحده آمریکا عمیقاً به ماده ۵ اساس‌نامه این سازمان متعهد است و حمله به یک عضو، مساوی با حمله به‌تمامی اعضای ناتو است. با توجه به اینکه

1. Brewster, J. (2021). Putin Claims Most Cyber-attacks come From U.S. Not Russia. Retrieved 28 July 2021, from https://www.forbes.com/sites/jackbrewster/2021/06/16/putin-claims-after-biden-summit-most-cyberattacks-come-from-us-not-russia/?sh=3bba7b8230c4

2. Peter Wilkinson C. (2021). Here's what happened at the Biden-Putin Geneva summit. Retrieved 28 July 2021, from https://edition.cnn.com/world/live-news/biden-putin-meeting-geneva-updates-intl/index.html

ناتو مسئول حفاظت از امنیت بیش از یک میلیارد انسان در اروپا و آمریکای شمالی است، اکنون در هفتاد و سومین سالگرد تأسیس این اتحاد، یکی از مهم‌ترین وظایف این سازمان مواجه با تهدیدات امنیتی در فضای مجازی است.

مهم‌ترین مسئله مربوط به فضای مجازی که در اجلاس بروکسل موردبررسی قرار گرفت، تهدیدات جمهوری خلق چین علیه اتحاد ناتو بود. چین برای اولین بار 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 اتحاد مطرح کردند که با تجدیدنظر در سیاست‌های استراتژیک خود، چارچوب جدیدی طراحی کنند که در آن با مدنظر قرار دادن فضای در حال تکامل تهدیدات، اقدامات تهاجمی دشمنان بی‌اثر کنند. دولت چین در این چارچوب 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 بلیکن[2] وزارت خارجه آمریکا در این خصوص اعلام

1. A New Strategic Concept
2. Antony Blinken

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 نیز که در همین ماه جاری برگزار شد نیز، رهبران هفت قدرت بزرگ اقتصاد جهان صراحتاً به چین هشدار دادند. باوجوداین، باید توجه داشت که برخلاف ایالات‌متحده آمریکا، دیگر اعضای ناتو بااحتیاط بیشتری در این خصوص صحبت کرده و بیشتر ادعاهای آمریکا را تصدیق می‌کنند[1].

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 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

1. Holland, S. & Chiacu, D. (2021). U.S. and allies accuse China of global hacking spree. Retrieved 28 July 2021, from https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/

ارتباطات از دیگر دغدغه‌های رهبران ناتو در اجلاس بروکسل بود. سران اتحاد تائید 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 تائید 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.[2]

این پروژه با الگوبرداری از شبکه نوآوری امنیت ملی[3] ایالات‌متحده (NSIN) آمریکا قرار است راه‌اندازی شود. پروژه شتاب‌دهنده نوآوری در حوزه دفاعی (DIA)، تحت نظر وزارت دفاع آمریکا به پشتیبانی از استارتاپ های 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 امنیت شبکه یکی از اصلی‌ترین اولویت‌های حمایتی وزارت دفاع آمریکا محسوب می‌شود[4]. بر همین اساس، سران ناتو در اجلاس بروکسل تصمیم گرفتند به‌منظور افزایش سرعت فرایند نوآوری،

1. Defense Innovation Accelerator
2. FACT SHEET: NATO Summit: Revitalizing the Transatlantic Alliance | the White House. (2021). Retrieved 28 July 2021, from https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-nato-summit-revitalizing-the-transatlantic-alliance/
3. National Security Innovation Network
4. National Security Innovation Network: Defense Innovation Accelerator. (2021). Retrieved 28 July 2021, from https://www.nsin.us/defense-innovation-accelerator/

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 همچنان به نتیجه مشخصی نرسیده است. همان‌طور که پیش‌تر مورداشاره قرار گرفت، 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 جهانی واقعی است. رهبران ناتو در اجلاس‌های پیش‌ازاین نیز در خصوص امکان اجرای اصل دفاع جمعی در قبال حملات سایبری تصمیماتی گرفته بودند و آخرین راه‌حل عملی آن‌ها، تجویز واکنش ملی و مستقل از سوی دولت قربانی بود؛ اما این راه‌حل نیز عملاً سطح حداقلی از بازدارندگی را نیز محیا نمی‌کند و به‌عنوان‌مثال کشورهایی همچون ایسلند، سوئیس و یا لوکزامبورگ اساساً یا فاقد ارتش بوده و یا دارای نیروی نظامی بسیار محدودی هستند و امکان پاسخگویی نظامی به یک حمله سایبری را ندارند. از طرف دیگر، بسیاری از کارشناسان ناتو بر این باور هستند که حملات سایبری در

مقطع کنونی علی‌رغم خسارات سنگین و عواقب زیان باری که به همراه دارند، هنوز به آن مرحله از حدت نرسیده‌اند که هزینه‌های یک جنگ واقعی و پیامدهای آن را توجیه کنند؛ هرچند که در آینده نه‌چندان دور بدون شک به آن مرحله خواهند رسید و نبردهای متعاقب آن امری اجتناب‌ناپذیر خواهد شد. این نکته ازآن‌رو حائز اهمیت است که در نظم منطقه‌ای اروپا، یک جنگ واقعی تمامی اعضای اتحادیه را درگیر می‌کند و امنیت جمعی را به‌مراتب بیشتر از یک حمله سایبری تقلیل می‌دهد.

اجلاس بروکسل ۲۰۲۱ با در نظر داشتن 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 مطرح‌شده 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 در حال حاضر 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

1. "be considered as amounting to an armed attack"

تمام‌عیار فراخوان می‌کند.[1] 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 همین رو، چنان‌چه یک حمله سایبری ۱۰ میلیون دلار خسارت وارد کند، پاسخ متقابل آن باید هزینه‌ای ۱۰ میلیون دلاری به دولت مهاجم تحمیل کند. در این مورد، تفاوتی میان حملاتی که مستقیم از سوی یک دولت انجام می‌گیرد با حملاتی که از سوی نیروهای نیابتی آن انجام می‌گیرد وجود ندارد؛ زیرا ناتو حق انتساب دهی 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.

1. A Defence of Defence. NATO's Response to Low-Grade Cyber-Attacks - ICDS. (2021). Retrieved 29 July 2021, from https://icds.ee/en/a-defence-of-defence-natos-response-to-low-grade-cyber-attacks/
2. The principle of proportionality

جمع بندی

جمع‌بندی

در شرایط کنونی جهان، امنیتی‌سازی فضای سایبر یکی از ملزومات اصلی حکمرانی بر این فضا است. با توجه با 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 کنند. نظام‌های امنیتی پیشرفته، با درک پیچیدگی‌ها و دگرگونی‌های فضای مجازی دستور کارهای 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 و در یک فرایند پانزده‌ساله، مسیر پرفرازونشیبی را در خصوص طراحی یک استراتژی امنیتی برای فضای سایبر پشت سر 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 قابل‌توجهی 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 کارویژه 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 گزافی در این خصوص متحمل خواهند شد. درنهایت مسئله مهمی که از تحولات استراتژی امنیت سایبری ناتو می‌بایست موردتوجه 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 با احتیاط بیشتری در خصوص این موضوع صحبت می‌کند و بیشتر سعی بر غیرنظامی جلوه دادن حملات سایبری دارد، اما 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 آینده‌ی نزدیک آماده کند، جنگ‌هایی که تبعات و نیز ادوات آن این بار از فضای سایبر نیز می‌تواند فراتر رود.

منابع

[1] Peter Wilkinson C. (2021). Here›s what happened at the Biden-Putin Geneva summit. Retrieved 28 July 2021, from https://edition.cnn.com/world/live-news/biden-putin-meeting-geneva-updates-intl/index.html

[2] 2007 cyber-attacks on Estonia, Retrieved 18 July 2021, from https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

[3] A Defence of Defence. NATO's Response to Low-Grade Cyber-Attacks - ICDS. (2021). Retrieved 29 July 2021, from https://icds.ee/en/a-defence-of-defence-natos-response-to-low-grade-cyber-attacks/

[4] About us. (2021). Retrieved 17 July 2021, from https://ccdcoe.org/about-us/

[5] Achieve and Maintain Cyberspace Superiority, Available at: https://www.cybercom.mil/

[6] Biden says he is ‹looking closely› at retaliation over Russian-linked cyber-attack. (2021). Retrieved 28 July 2021, from https://www.nbcnews.com/politics/white-house/biden-says-he-looking-closely-retaliation-over-russian-linked-cyber-n1269413

[7] Bogdan, R, Cristian, COMAN, NATO Automated Biometric Identification System (NABIS), MTA Review, Vol. XXVII, No. 2, Dec. 2017.

[8] Brewster, J. (2021). Putin Claims Most Cyber-attacks come From U.S. Not Russia. Retrieved 28 July 2021, from https://www.forbes.com/sites/jackbrewster/2021/06/16/putin-claims-after-biden-summit-most-cyberattacks-come-from-us-not-russia/?sh=3bba7b8230c4

[9] Bussoletti, F. (2018). NATO, the new Cyber Operations Centre (CYOC) should be fully operative in 2023. Retrieved 17 July 2021, from https://

www.difesaesicurezza.com/en/defence-and-security/nato-the-new-cyber-operations-centre-cyoc-should-be-fully-operative-in-2023/
[10] CCDCOE. (2021). Retrieved 19 July 2021, from https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/#footnote_6_2663
[11] CCDCOE. (2021). Retrieved 27 July 2021, from https://ccdcoe.org/incyder-articles/cyber-defence-at-the-28th-nato-summit-in-brussels-11-12-july-2018/#identifier_26_3346
[12] Collective defense - Article 5. (2021). Retrieved 31 July 2021, from https://www.nato.int/cps/en/natohq/topics_110496.htm
[13] Collective defense - Article 5. (2021). Retrieved 15 July 2021, from https://www.nato.int/cps/en/natohq/topics_110496.htm
[14] Cyber Defense Pledge. (2021). Retrieved 27 July 2021, from https://www.nato.int/cps/en/natohq/official_texts_133177.htm
[15] Drafting of the Rome Treaties. (2021). Retrieved 14 July 2021, from https://www.cvce.eu/obj/drafting_of_the_rome_treaties-en-8efe2279-ee12-4a75-aeeb-0bd547f4128f.html
[16] Efthymiopoulos, M.P. A cyber-security framework for development, defense and innovation at NATO. J Innov Entrep 8, 12 (2019).
[17] FACT SHEET: NATO Summit: Revitalizing the Transatlantic Alliance | the White House. (2021). Retrieved 28 July 2021, from https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-nato-summit-revitalizing-the-transatlantic-alliance/
[18] Herzog, Stephen, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses,

[19] Holland, S. & Chiacu, D. (2021). U.S. and allies accuse China of global hacking spree. Retrieved 28 July 2021, from https://www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19/

[20] How Russia Strengthened NATO's Cyber Defense. (2020). Retrieved 18 July 2021, from https://warsawinstitute.org/russia-strengthened-natos-cyber-defence/

[21] Journal of Strategic Security, Vol. 4, No. 2, Strategic Security in the Cyber Age (Summer 2011), pp. 49-60.

[22] July 2021, from https://www.macmillandictionary.com/dictionary/british/weaponization

[23] Lewis, D. (2019). What Is NATO Really Doing in Cyberspace? - War on the Rocks. Retrieved 18 July 2021, from https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/

[24] National Security Innovation Network: Defense Innovation Accelerator. (2021). Retrieved 28 July 2021, from https://www.nsin.us/defense-innovation-accelerator/

[25] NATO Review - NATO's role in cyberspace. (2019). Retrieved 18 July 2021, from https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[26] NATO Warsaw summit 2016, what about cyber security? (2016). Retrieved 25 July 2021, from https://securityaffairs.co/wordpress/49255/cyber-warfare-2/nato-warsaw-summit-2016.html

[27] NATO's 'Eye in the Sky'. (2021). Retrieved 31 July 2021, from https://www.napma.nato.int/awacs/a0.html

[28] Offense as the New Defense: New Life for NATO's Cyber Policy. (2018). Retrieved 18 July 2021, from https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy#_ftnref6

[29] Resilience and Article 3. (2021). Retrieved 26 July 2021, from https://www.nato.int/cps/en/natohq/topics_132722.htm#:~:text=The%20principle%20of%20resilience%20is,develop%20their%20individual%20and%20collective

[30] Steve Ranger, NATO updates cyber defense policy as digital attacks become a standard part of conflict, https://www.zdnet.com/

[31] The 2016 NATO Summit: What will be on the agenda in Warsaw? | SIPRI. (2016). Retrieved 20 July 2021, from https://www.sipri.org/commentary/topical-backgrounder/2016/2016-nato-summit-what-will-be-agenda-warsaw

[32] The NATO Cooperative Cyber Defense Centre of Excellence

[33] Wales Summit Declaration, Paragraph 72, http://www.nato.int/cps/en/natohq/official_texts_112964.htm

[34] Walsh, J. (2021). Biden Vows Retaliation on Any Future Russian Hacks on Critical Infrastructure. Retrieved 28 July 2021, from https://www.forbes.com/sites/joewalsh/2021/06/16/biden-vows-retaliation-on-any-future-russian-cyberattacks-on-critical-infrastructure/?sh=3f4aa2591fab

[35] WEAPONIZATION (noun) definition and synonyms | Macmillan Dictionary. (2021). Retrieved 20

[36] What is Cyber Security? (2021). Retrieved 22 July 2021, from https://www.kaspersky.com/resource-center/definitions/what-is-

cyber-security

[37] Wing Commander Mark Lunan, NEW doctrinal concept BIOMETRICS, The Three Swords Magazine, 33/2018.

[۳۸] بوزان، بری و همکاران، چارچوبی تازه برای تحلیل امنیت، پژوهشکده مطالعات راهبردی، چاپ سوم، تهران، ۱۳۹۹، ص ۵۳-۵۲.

[۳۹] بوزان، بری، مردم، دولت‌ها و هراس، پژوهشگاه مطالعات راهبردی، چاپ ششم، تهران، ۱۳۹۹، ص ۱۲۳.

[۴۰] بوزان، بری، ویرو، اُلی، مناطق و قدرت‌ها: ساختار امنیت بین‌الملل، پژوهشکده مطالعات راهبردی، چاپ سوم، تهران،۱۳۹۸، ص ۱۶.

[۴۱] شولتز، ریچارد و همکاران، رویکردهای جدید در مطالعات امنیتی، پژوهشکده مطالعات راهبردی، جلد اول، چاپ سوم، تهران،۱۳۹۴.

[۴۲] کالینز، الن، مطالعات امنیت معاصر، پژوهشکده مطالعات راهبردی، چاپ اول، تهران، ۱۳۹۹، ص ۱۹۰.

[۴۳] محسنی، فرید، حریم خصوصی اطلاعات، انتشارات دانشگاه امام صادق (ع)، چاپ دوم، تهران، ۱۳۹۴، ص ۳۳۱.

[۴۴] هریسی نژاد، کمال‌الدین، نظری به پیمان ماستریخت و اتحاد اروپا، فصلنامه جغرافیا و برنامه‌ریزی، پاییز ۱۳۷۴ - شماره ۱، ص ۱۴۷ و ذاکریان امیری، مهدی، فرآیند اتحاد اروپا، فصلنامه دین و ارتباطات، تابستان ۱۳۷۸، شماره ۱۰، ص ۹۹.

[۴۵] یزدان فام، محمود، دولت های شکننده و امنیت انسانی، پژوهشکده مطالعات راهبردی، چاپ دوم،۱۳۹۲، ص ۱۲۴-۱۲۲.

csri.majazi.ir