تکامل راهبرد ناتو در قبال جنگ سایبری؛ دلایل، ابعاد و مؤلفه‌ها

تاریخ دریافت: ۱۳۹٤/۲/۱٤ تاریخ پذیرش: ۱۳۹٤/٤/۱۸

قاسم ترابی*

چکیده:

هدف اصلی این مقاله تبیین دلایل روی‌آوردن سران ناتو به فضای سایبر و معرفی اصول و محورهای راهبرد سایبری ناتو در قبال جنگ سایبری می‌باشد. سؤال اصلی این است که چه عواملی باعث تدوین و تکامل راهبردی سایبری ناتو در قبال جنگ سایبری شدند؟ در پاسخ، فرضیه مقاله این گونه مطرح می‌شود که ماهیت پیچیده و متفاوت فضای سایبر، آسیب‌پذیری‌های جدی کشورهای عضو و نگرانی از تهدیدات سایبری سایر کشورها، مهم‌ترین دلایل تدوین و تکامل راهبردی سایبری ناتو محسوب می‌شوند. تحت تأثیر این دلایل، ناتو در پروسه‌ای چندساله، در نهایت جنگ سایبری را پدیده‌ای هم‌سطح جنگ نظامی ارزیابی نمود و طبق بند ۵ اساسنامه، برای خود حق دفاع همه‌جانبه و جمعی به شکل نظامی و سایبری را در نظر گرفت. بر این اساس، ناتو اولین پیمان نظامی جهان شد که دفاع نظامی و سایبری را جزو وظایف اولیه خود معرفی کرد.

کلیدواژه‌ها: جنگ سایبری، راهبرد سایبری، پیمان آتلانتیک شمالی، تهاجم سایبری.

---

* استادیار دانشگاه آزاد اسلامی واحد همدان.

مقدمه

امروزه با توجه به تحولات صورت‌گرفته در سطح جهان و به خصوص انقلاب اطلاعات و ارتباطات، تهدیدات فضای سایبر و به خصوص «جنگ سایبری»[1] از جمله مهم‌ترین مصادیق «جنگ‌های جدید»[2] محسوب می‌شوند. گستردگی و همچنین جدی‌بودن این نوع جنگ در سطحی است که تقریباً تمامی کشورها حوزه سایبر را به عنوان حوزه‌ای امنیتی و حتی گاه نظامی در نظر می‌گیرند و ساختارها و مراکزی را برای مقابله با تهدیدات و خطرات این حوزه ایجاد کرده‌اند. در این زمینه می‌توان به کشورهایی همچون آمریکا، رژیم صهیونیستی و کشورهای اروپای غربی اشاره نمود که از سه دهه پیش، عملاً نگاهی امنیتی به فضای سایبر داشته و اولین واحدها و مراکز فعال در زمینه جنگ سایبری را ایجاد نموده‌اند. در مرحله بعد نیز کشورهایی همچون چین، روسیه و ایران، اهمیت حوزه سایبر را درک کردند و سرمایه‌گذاری‌های نسبتاً گسترده‌ای در این حوزه نمودند. همین وضعیت، کم‌وبیش در مورد سایر کشورها نیز وجود داشته، به شکلی که می‌توان گفت اصولاً کشورها جنگ سایبری و به شکل کلی، تهدیدات سایبری را تهدیدی جدی و در سطح تهدیدات نظامی در نظر گرفته‌اند.

البته، موضوع جنگ سایبری در سطح کشورها باقی نمانده و نگرانی از این نوع جنگ وارد مباحث اتحادها و پیمان‌های نظامی کلاسیک همچون «سازمان پیمان آتلانتیک شمالی»[3] به عنوان بزرگترین و قدرتمندترین پیمان نظامی و دفاعی جهان شده است. در واقع، این موضوع خود نشانه‌ای دیگر از اهمیت جنگ‌های سایبری و نگرانی گسترده کشورها، به ویژه کشورهای پیشرفته از این محیط پیچیده و مبهم امنیتی محسوب می‌شود. در این راستا، کشورهای عضو ناتو طی چند سال گذشته و به خصوص از سال ۲۰۰۷، به دنبال تدوین راهبرد سایبری جامع و محکمی بوده‌اند تا تهدیدات فضای سایبر را تحت کنترل درآورند و در عین حال، خود تبدیل به قدرت سایبری برتر در سطح جهان گردند. با توجه به اهمیت این موضوع، سؤال اصلی مقاله به این شکل مطرح می‌شوند: چه عواملی باعث تدوین و تکامل راهبردی سایبری ناتو در قبال جنگ سایبری شده‌اند؟

---

1. Cyber War
2. New War
3. North Atlantic Treaty Organization

در پاسخ به این سؤال، فرضیه مقاله این‌گونه مطرح می‌شود: «ماهیت پیچیده و متفاوت فضای سایبر، آسیب‌پذیری‌های جدی کشورهای عضو و نگرانی از تهدیدات سایبری سایر کشورها به خصوص روسیه و چین، مهم‌ترین دلایل تدوین و تکامل راهبردی سایبری محسوب می‌شوند». در کنار این سؤال اصلی، برای فهم کامل‌تر و جامع‌تر موضوع مورد بحث، سؤالات فرعی زیر مطرح می‌شوند:

«جنگ سایبری از منظر مفهومی و محتوایی، چه تفاوت‌هایی با جنگ‌های گذشته دارد؟»

«ناتو به عنوان پیمان نظامی– دفاعی، چه رویکردی به جنگ سایبری دارد و این رویکرد چه تأثیری بر راهبرد سایبری آن داشته است؟

«مهم‌ترین محورها و اصول راهبرد سایبری ناتو در مقابله با جنگ‌های سایبری، کدام‌اند؟»

لازم به اشاره است که در راهبرد سایبری ناتو، تمرکز اصلی بر جنگ سایبری قرار دارد و سایر تهدیدات فضای سایبر همچون سایبرتروریسم و جاسوسی سایبری، ذیل جنگ سایبری مورد ارزیابی قرار گرفته‌اند. البته، این بدان معنا نیست که از منظر سران ناتو این تهدیدات اهمیت چندانی ندارند، بلکه نگرانی بیشتر کشورهای اروپایی ناشی از جنگ سایبری به خصوص از سوی کشوری چون روسیه است. افزون بر این، اصولاً تأکید بر افزایش توان تدافعی در حوزه جنگ سایبری، به شکل هم‌زمان افزایش قابلیت در حوزه مقابله با سایر تهدیدات فضای سایبر چون سایبرتروریسم و جاسوسی سایبری را به دنبال دارد. به عبارت دیگر، هرچند در سطح نظری و مفهومی جنگ سایبری از سایر تهدیدات جدا می‌شود، اما در سطح عملی چنین جدایی‌ای وجود ندارد. در واقع، به همین دلیل است که در مورد تقریباً تمامی کشورها، راهبردها، تاکتیک‌ها و مراکز مشابهی در قبال تهدیدات سایبری در معنای عام وجود دارد که به شکل هم‌زمان وظیفه دفاع در برابر تمامی تهدیدات سایبری را بر عهده دارند. بر این اساس، باید گفت هرچند در راهبرد سایبری ناتو محور بحث بر آمادگی در برابر تهدیدات فضای سایبر با محوریت جنگ سایبری قرار دارد، اما سایر تهدیدات در قالب جنگ سایبری مورد توجه بوده‌اند.

درباره اهمیت و ضرورت پاسخ به این سؤالات و همچنین اهمیت کلی موضوع، باید به این نکته اشاره نمود که موارد متعدد جنگ سایبری، طی چند سال گذشته و به خصوص

حملات سایبری متنوع علیه کشورمان، خود گواهی روشن از اهمیت و ضرورت شناخت در این حوزه می‌باشد. در واقع، می‌توان گفت ایران از جمله کشورهایی است که طی چند سال گذشته با انواع و اقسام تهدیدات سایبری و به خصوص حملات سایبری مشخص علیه برنامه هسته‌ای مواجه بوده است. در این زمینه می‌توان به حملات سایبری با بدافزارها و ویروس‌هایی همچون «استاکس نت»[1]، «شعله آتش» یا «فلیم»[2] و دیگر موارد اشاره نمود. بر این اساس، برای ایران که یکی از اهداف حملات سایبری، به خصوص از ناحیه ایالات متحده آمریکا و رژیم صهیونیستی محسوب می‌شود، شناخت ابعاد مختلف موضوع، به خصوص شناخت دلایل تدوین و اصول و مؤلفه‌های راهبرد سایبری ناتو اهمیت و ضرورتی جدی دارد. تردیدی در این زمینه وجود ندارد که در بلندمدت، قدرت و توان سایبری ناتو می‌تواند تهدیدی جدی برای کشورهای خارج از حوزه فرهنگ و تمدن غرب، به ویژه ایران، چین و روسیه باشد. با عنایت به این موضوع، شناخت اصول و محورهای راهبرد ناتو در عرصه جنگ سایبری از اهمیت و ضرورتی جدی برخوردار می‌باشد.

از منظر ساختاری، مقاله حاضر مشتمل بر چهار بخش کلی است. محور بخش اول مقاله، ارائه چارچوبی مفهومی از تهدیدات فضای سایبر با محوریت جنگ سایبری می‌باشد. هدف از طرح این موضوعات، کمک به فهم مطالب ارائه‌شده در بخش‌های دیگر، به خصوص در مورد دلایل روی‌آوردن ناتو به فضای سایبر و همچنین، اصول و محورهای راهبرد سایبری ناتو است. در راستای تحقق این هدف، تفاوت‌های محتوایی جنگ سایبری با جنگ‌های گذشته مورد بحث قرار می‌گیرد. اتخاذ رویکرد مقایسه‌ای در این بخش بدین علت است که مقایسه جنگ‌های سایبری با جنگ‌های نظامی، کمک فراوانی به درک فضای جدید امنیتی و فهم عمیق‌تر راهبرد سایبری ناتو می‌کند. همچنین، در این بخش در مورد جایگاه جنگ سایبری به عنوان حوزه‌ای جدید در عرصه امنیت بحث خواهد شد. در بخش دوم، با عنایت به بحث‌های محتوایی و مفهومی بخش اول، به شکل موردی مهم‌ترین دلایل تدوین و تکامل راهبرد سایبری ناتو مورد بحث قرار می‌گیرند. در بخش سوم، تکامل محورهای راهبرد سایبری ناتو

1. Stuxnet
2. Flame

تحت تأثیر دلایل یادشده مطرح می‌شوند. در نهایت، در بخش چهارم نیز آخرین تحولات در رویکرد ناتو در زمینه جنگ سایبری سایبر ارائه می‌شود تا مباحث بخش سوم با توجه به آخرین تحولات صورت گرفته کامل‌تر شوند.

الف. چارچوب مفهومی

در فهم ابعاد و شاخص‌های جنگ سایبری، اولین نکته‌ای که به ذهن می‌رسد، گنگی و ابهام ذاتی این مفهوم و نداشتن مرزی روشن بین آن با سایر تهدیدات و حتی تهدیدات سایبری از جمله «جاسوسی سایبری»[1] و «سایبرتروریسم»[2] می‌باشد. در این راستا، به نظر می‌رسد بخشی از ابهامات موجود در ارتباط با مفهوم جنگ، حملات یا تروریسم سایبری ناشی از جدیدبودن، متفاوت‌بودن و پیچیده‌بودن مفهوم، عینیت و مصادیق فضای سایبر و عدم آمادگی کشورها و به خصوص نیروی‌های دفاعی و امنیتی آنها برای درک متفاوت این حوزه در مقایسه با سایر حوزه‌های امنیتی باشد. منظور از جدیدبودن مفهوم جنگ سایبری این است که تا کنون مفهوم جنگ عموماً به فضای نظامی و استفاده خشونت‌بار از تسلیحات اشاره داشته است. حتی در منشور ملل متحد که البته پیش از ظهور و بروز تهدیدات جدید مدون گشته، تجاوز و جنگ بر اساس استفاده خشونت‌بار از تسلیحات توسط نیروی هوایی، دریایی و زمینی کشورها تعریف شده است (منشور ملل متحد، فصل هفتم، ۱۳۹۱). بنابراین، در متون کلاسیک امنیتی، جنگ به منزله استفاده از نیروی نظامی با هدف کشتار، تخریب، تجاوز و در نهایت، شکست کشور یا کشورهای دشمن مفهوم‌پردازی می‌شود. در مقابل، در فضای سایبر، هر گونه تخریب، خراب‌کاری، هک‌کردن، پاک‌کردن و مواردی از این قبیل، جنگ سایبری نام‌گذاری می‌شود که در آن از هیچ گونه سلاح به غیر از اینترنت، برنامه، نرم‌افزار و ویروس استفاده نمی‌شود. بنابراین، بخشی از نوبودن جنگ سایبری ناشی از متفاوت‌بودن در حوزه ابزار، روش، ماهیت کار و همچنین، سلاح متفاوت به کار برده‌شده می‌باشد (ترابی، شهریور ۱۳۹۲).

---

1. Cyber Spy
2. Cyber Terrorism

البته، در راستای این تحول ماهوی، برخی به دنبال تعریفی جدید از تسلیحات هستند. لازم به ذکرست که بر اساس تعریف سنتی، سلاح ابزاری است که نیروهای نظامی برای ایجاد تخریب از آن استفاده می‌کنند. بر این اساس، تسلیحات به «تسلیحات متعارف»[1] و «تسلیحات غیر متعارف»[2] شامل بمب هسته‌ای، شیمیایی و میکروبی تقسیم می‌شوند. برخی بر این باورند که این تعریف باید تغییر کند و سلاح شامل هر گونه ابزاری گردد که توانایی تخریب، مشکل و حتی دردسر برای طرف مقابل را دارد. ضمن اینکه دیگر مهم نیست این سلاح توسط یک ارتش یا یک نظامی تنومند و آموزش‌دیده استفاده شود و یا یک جوان لاغراندام دانشگاهی که کمترین آگاهی از فنون نظامی را ندارد. به عبارت دیگر، سلاح دیگر اختصاص به نیروی‌های نظامی و شرایط جنگی ندارد و انحصار استفاده از آن به دلیل ماهیت متفاوت سلاح‌های جدید در حال خارج‌شدن از دست نیروی‌های نظامی است. معنای دیگر این گفته این است که اصولاً معنای نیروی نظامی و شیوه آموزش و عملکرد آنها و همچنین، معنای صلح و جنگ در حال تغییر است (Lieutenant, Beidleman, 2009: 1-2).

البته، طرح موضوع فضای سایبر به عنوان سلاح، مخالفینی نیز دارد. به باور مخالفان، گسترش مفهوم جنگ به حوزه سایبر مشکلات نظری، مفهومی و عملی گسترده‌ای در این زمینه ایجاد می‌کند. در مقابل، موافقان طرح این موضوع اشاره می‌کنند که امروزه کشورها توانایی لازم برای استفاده از فضای سایبر به عنوان ابزار کاملاً کارآمد با هدف تخریب، خرابکاری و منهدم‌کردن تأسیسات حیاتی دشمن را دارند. این کارشناسان که تعداد آنها به خصوص در آمریکا در حال افزایش است، از مفاهیمی همچون «پرل هاربر سایبری»[3] استفاده می‌کنند که اشاره به توان و ظرفیت سلاح‌های خطرناک و ویرانگر فضای سایبری دارد. ضمن اینکه امروزه با قاطعیت در مورد امکان حملات سایبری ویرانگری صحبت می‌شود که می‌توانند تأسیسات نظامی، دفاعی، هسته‌ای و حتی مدنی یک کشور مثل سیستم‌های هوایی، مالی و بانکی، تأسیسات برق، گاز، نفت و سدها را نابود سازد. با توجه به این شرایط، امروزه تردیدی در زمینه امنیتی‌بودن فضای سایبر و پذیرش جنگ سایبری به عنوان یکی از مصادیق جنگ‌های جدید وجود ندارد (Lewis, 2006: 1).

---

1. Conventional Weapons
2. Unconventional Weapons
3. Cyber Pearl Harbor

موضوع بعدی، متفاوت‌بودن ماهیت و محتوای جنگ سایبری در مقایسه با جنگ نظامی است که درک این موضع می‌تواند ابعاد دیگری از جنگ سایبری روشن‌تر کند. از جمله اینکه در جنگ نظامی، مصادیق و مفاهیمی همچون دشمن، دوست، اتحاد و ائتلاف، جبهه، آغاز و پایان جنگ و مسائلی از این قبیل، کاملاً روشن هستند. در جنگ‌های نظامی، با توجه به اینکه جنگ را یک یا چند کشور علیه یک یا چند کشور دیگر آغاز می‌کنند، شروع و پایان جنگ، طرف‌های مهاجم و مدافع، کشورهای متحد، دشمن و حتی بی‌طرف و جبهه (در معنای محلی که طرفین با هم درگیر می‌شوند) کاملاً روشن هستند. برای مثال، در جنگ عراق علیه ایران، به عنوان نمونه‌ای از جنگ کلاسیک و نظامی، تاریخ شروع و پایان جنگ کاملاً مشخص، دوستان و متحدان ایران و همچنین عراق روشن و جبهه و محل درگیری طرفین واضح بودند. در این جنگ، عراق به عنوان کشور متجاوز شناخته شد و ایران نیز اجازه داشت بر اساس تعریف روشن دفاع مشروع، از خود دفاع کند.

با این وجود، هیچ کدام از این موارد در حوزه جنگ سایبری مشخص نیستند. به عنوان نمونه، در مورد آغاز و پایان جنگ سایبری نمی‌توان زمانی را مشخص نمود؛ اتفاقاً جنگ سایبری زمانی می‌تواند تأثیرگذار باشد که زمان آن مشخص نباشد. کشور هدف در این نوع جنگ‌ها زمانی از حمله آگاهی می‌یابد که تقریباً هدف دشمن محقق شده و در واقع، از تخریب‌ها و دود به پا شده از حمله آگاهی می‌یابد (Libicki, 2009: 170-182). ابهام دیگر در این زمینه در مورد کشور یا نیروهای مهاجم می‌باشد. واقعیت این است که به دلیل مجازی‌بودن فضا و ابهام در نوع و ماهیت حمله، هیچ کس نمی‌تواند به آسانی کشور یا نیروی مهاجم را شناسایی کند. ماهیت حملات سایبری به گونه‌ای است که در آن کمترین نشانه‌ای از عامل حمله وجود دارد. ضمن اینکه مکان حمله سایبری نیز چندان مشخص نیست و ویروس یا بدافزار ارسال‌شده نیز کمترین نشانه‌ای از عامل حمله را دارد. همچنین، به دلیل تعدد بازیگران در حوزه و فضای سایبر که شامل کشورها، سازمان‌ها و نهادهای دولتی و غیر دولتی، تروریست‌ها، هکرها و حتی افراد می‌شود، شناخت عامل حمله سخت‌تر و پیچیده‌تر می‌باشد. لازم به ذکرست که در حملات سایبری که تا کنون صورت گرفته، کشور یا عامل حمله نه بر اساس حملات سایبری و شواهد روشن، بلکه بر اساس اوضاع و احوال سیاسی و نیات و اهداف کشورها شناسایی شده‌اند. به

عنوان نمونه، حملات سایبری صورت‌گرفته علیه ایران، به این دلیل به آمریکا و رژیم صهیونیستی نسبت داده می‌شوند که فضای سیاسی و امنیتی دیدگاه‌ها را به این سو شکل می‌دهند. البته، بعدها شواهدی مطرح شدند که این دیدگاه را تأیید کردند، از جمله اینکه برخی از رسانه‌های آمریکایی اطلاعات و مستنداتی را منتشر نمودند که دخالت دولت آمریکا و رژیم صهیونیستی در حملات سایبری علیه ایران را تأئید می‌کردند. بر این اساس، ابهام در شناسایی عامل حمله خود بر پیچیدگی و ابهام جنگ سایبری می‌افزاید و آن را تبدیل به حوزه‌ای جذاب برای کشورهایی می‌کند که توانایی بالایی در این حوزه برای آسیب‌رساندن به دیگران دارند (Sanger, 2015: 1).

موضوع بعدی، مرگ مفهوم جبهه در جنگ سایبری می‌باشد. در ادبیات نظامی، جبهه محل درگیری، نزاع و برخورد مستقیم طرفین است، اما آیا در حملات و جنگ سایبری می‌توان از مفهوم جبهه صحبت نمود؟ واقعیت این است که در جنگ سایبری، جبهه دقیقاً در امتداد و گستردگی فضای سایبر وجود دارد و تمامی مراکز نظامی، سیاسی، اقتصادی و حتی منازل و حوزه‌های به شدت خصوصی را در بر می‌گیرد. در این زمینه می‌توان به ویروس فلیم اشاره نمود. فلیم این توانایی را دارد که تمامی اقدامات یک کاربر در هر کجا و هر لحظه‌ای را ثبت و ضبط کند و از محیط اطراف فیلم‌برداری و صدابرداری کند. به تعبیر دیگر، فلیم و سایر بدافزارهایی که احتمالاً هم‌اکنون در حال فعالیت هستند و هنوز اطلاعاتی از آنها در دسترس نیست، تمامی نقاط، زمان‌ها و مکان‌ها را تبدیل به حوزه و جبهه حملات سایبری کرده‌اند. بر این اساس، به نظر می‌رسد مفهوم جبهه در جنگ سایبری متلاشی و در نتیجه گسترده و همه‌گیر می‌شود و به همین شکل، مفهوم تهاجم و به خصوص تدافع نیز گستردگی و پراکندگی خاصی پیدا می‌کند (ترابی، مرداد ۱۳۹۲).

همچنین می‌توان به مفهوم «دفاع مشروع»[1] اشاره نمود که بیان‌گر تفاوت دیگر جنگ سایبری با جنگ‌های کلاسیک و همچنین، ابهام گسترده و مفهومی جنگ سایبری است. در جنگ‌های کلاسیک، طبق حقوق بین‌الملل کشور مورد تهاجم حق دفاع از خود در مقابل مهاجم را دارد. این دفاع باید بر اساس سه اصل «ضرورت»[2]، «تناسب»[3] و دفاع تا مرزهای

1. Self-defense
2. Necessity
3. Proportionality

بین‌المللی باشد (Van den hole, 2003: 70-77)، در غیر این صورت، دفاع معنای خود را از دست می‌دهد و تبدیل به تهاجم و تجاوز می‌شود. در مقابل، در جنگ سایبری، مفهوم دفاع چندان روشن نیست. دفاع در مقابل چه چیزی و چه کسی باید صورت گیرد؟ جنگی که عامل و مهاجم آن روشن نیست، دفاع در آن چه معنای دارد؟ همچنین، دفاع سایبری گاهی خود به معنای حمله سایبری به کشور مهاجم به حساب می‌آید که این امر بر ابهام مفهومی آن می‌افزاید. ضمن اینکه چگونه می‌توان از ضرورت و تناسب صحبت نمود؟ بر این اساس، دفاع مشروع در جنگ سایبری معنا، مفهوم و محتوای خود را از دست می‌دهد. همه این موارد نشان می‌دهند جنگ سایبری به رغم آنکه به عنوان یکی از مصادیق جنگ‌های جدید شناخته می‌شود، تا چه میزان دارای تفاوت ماهوی و محتوایی با جنگ در معنای کلاسیک به خصوص جنگ‌های نظامی است. به هر حال، با عنایت به این ابعاد و مؤلفه‌ها و همچنین، تفاوت‌های ماهوی جنگ سایبری با جنگ نظامی و به خصوص، ابهام ذاتی این حوزه، جنگ سایبری را می‌توان با تسامح اینگونه تعریف نمود:

«جنگ سایبری جنگی است که دولت‌ها به عنوان بازیگر اصلی آن را رهبری می‌کنند تا تأسیسات، امکانات، توانایی‌ها و نقاط قوت دشمن را تخریب کنند. هدف از این جنگ تسلیم دشمن در برابر خواسته‌های کشور مهاجم است. لازم به اشاره است که در این جنگ، دولت‌ها می‌توانند از ارتش سایبری خود، بازیگران غیر دولتی و یا حتی هکرها و افراد استفاده کنند. با این وجود بازیگر اصلی و راهبر دولت‌ها هستند» (Lee, 2013: 99-113). به تعبیر دیگر، در صورتی که هجوم سایبری توسط سایر بازیگران از جمله هکرها، افراد، شرکت‌ها، سایبرتروریست‌ها و گروه‌های سازمان‌یافته و جنایت‌کار بین‌المللی صورت گیرد، نمی‌توان آن را جنگ سایبری ارزیابی نمود. مؤسسه «رند»[1] جنگ سایبری را به شرح زیر تعریف می‌کند:
«جنگ سایبری جنگی با محوریت دولت‌ها و سازمان‌های بین‌المللی علیه سایر دولت‌ها با هدف ایجاد تخریب در شبکه اطلاعات و کامپیوتر است. این حملات با ویروس‌ها، تروجان‌ها و سایر بدافزارها صورت می‌گیرد» (Cyber Warfare, 2015: 1).

1. Rand Corporation

برخی دیگر از کارشناسان، در برداشتی نسبتاً مشابه، جنگ سایبری را حوزه‌ای جدید و مستقل از جنگ و دفاع در نظر گرفته‌اند که به شکل هم‌زمان، برخی از ابعاد و مؤلفه‌های «جنگ سخت»[1] و «جنگ نرم»[2] را دارد، اما در عین حال دارای ماهیت و محتوایی متفاوت از هر دوی آنها می‌باشد. به باور آنها، جنگ سایبری حوزه‌ای جدید از جنگ محسوب می‌شود که طی آن بازیگران دولتی تلاش می‌کنند از فضای سایبر به عنوان سلاح مستقل استفاده کنند. در این جنگ، طرف‌های درگیر طیف گسترده‌ای از بازیگران شامل دولت‌ها و شرکت‌های دولتی و خصوصی، هکرها و افراد، البته تحت فرمان دولت‌ها هستند که تلاش می‌کنند از سلاحی جدید به عنوان فضای سایبر استفاده کنند تا به دشمن آسیب برسانند و یا اینکه عزم آن را برای انجام یا عدم انجام کاری تحت فشار قرار دهند (Krepinevich, 2012: 1-7). نیازی به توضیح ندارد که هیچ کدام از تعاریف مورد اجماع کارشناسان و کشورها قرار نگرفته و هنوز در عرصه بین‌المللی تعریف روشنی از جنگ سایبری وجود ندارد. با این وجود، عناصر اصلی تعریف کم‌وبیش روشن هستند. از جمله اینکه، بازیگر اصلی در این جنگ دولت‌ها و تا اندازه‌ای سازمان‌های بین‌المللی به خصوص سازمان‌های نظامی و دفاعی همچون ناتو هستند. دوم اینکه در جنگ سایبری، هدف اصلی ایجاد تخریب به کمک فضای سایبر در کشور یا کشورهای دشمن با هدف متقاعدکردن آنها به انجام یا عدم انجام کاری است (Morgus, 2014: 1-2).

به هر حال و فارغ از این ابهامات مفهومی، امروزه بیشتر کشورها جنگ سایبری را به عنوان حوزه‌ای مستقل از امنیت و در نتیجه، حوزه‌ای جدید در عرصه جنگ و دفاع به رسمیت شناخته و بسیاری از آنها واحد، قرارگاه، نیرو یا مرکزی را برای دفاع و هجوم سایبری طراحی نموده‌اند. به عنوان نمونه، دولت آمریکا جز اولین کشورهایی است که «فرماندهی جنگ سایبری»[3] به فرماندهی ژنرال «کیت الکساندر»[4] را فعال کرد. وظیفه اصلی این قرارگاه، هماهنگ‌سازی بخش‌های مختلف دفاع سایبری نهادها و نیروهای نظامی و اطلاعاتی آمریکا و در نتیجه، بالابردن توان دفاعی در برابر حملات سایبری و در هنگام ضرورت، انجام حملات

1. Hard War
2. Soft War
3. United State Cyber Command
4. Keith B. Alexander

سایبری هماهنگ می‌باشد. از دیگر وظایف این قرارگاه، کمک به دولت آمریکا برای طراحی استراتژی دفاعی و هجومی در زمینه جنگ سایبری است (ترابی، مرداد ۱۳۹۲). دولت ایران نیز برنامه‌ها و انجام اقدامات گسترده‌ای در زمینه دفاع سایبری را در اولویت قرار داده که هدف اصلی آنها مقابله با تهاجم سایبری کشورهایی همچون آمریکا و رژیم صهیونیستی است. از دیگر کشورهای فعال در زمینه جنگ سایبری می‌توان به انگلستان، فرانسه، آلمان، رژیم صهیونیستی، چین، کره شمالی و روسیه اشاره کرد که هر کدام راهبردها، تاکتیک‌ها و مراکز خاص سایبری خود را دارند (Siboni and Kronenfeld Iran's Cyber, 2012).

ب. زمینه‌ها و دلایل تدوین راهبرد سایبری ناتو

ناتو از سال ۲۰۰۷ در حوزه سایبر فعال شد و به شکلی موضوع تهدیدات سایبری را در دستور جلسات رسمی خود وارد کرد. آنچه بر اساس دلایل و شواهد موجود می‌توان گفت این است که مهم‌ترین دلایل ورود مباحث سایبری در دستور جلسه ناتو، نگرانی شدید اعضا از تهدیدات سایبری و به خصوص ماهیت متفاوت آن و در عین حال، مصادیقی چون حملات سایبری روسیه و چین می‌باشد. این نگرانی‌ها زمانی به اوج خود رسید که مشخص شد به رغم پیش‌گامی کشورهای غربی عضو ناتو و به خصوص آمریکا در حوزه سایبری، همین کشورها جزو آسیب‌پذیرترین کشورهای سایبری جهان هستند. در ادامه، مهم‌ترین دلایل تدوین و تکامل راهبرد سایبری ناتو مورد بحث قرار می‌گیرد.

۱. آسیب‌پذیری کشورهای عضو ناتو

واقعیت این است که کشورهای عضو ناتو به رغم پیشرفته‌بودن در حوزه سایبری، جزو کشورهای آسیب‌پذیر در این حوزه محسوب می‌شوند. دلایل چندی در این زمینه قابل شناسایی هستند. اولین مورد به ماهیت متفاوت جنگ سایبری در مقایسه با جنگ‌های نظامی و کلاسیک برمی‌گردد که در بخش پیشین به شکل کامل توضیح داده شد. خلاصه اینکه، به دلیل ماهیت متفاوت فضای سایبر، امکان بازدارندگی و انجام اقدامات پدافندی در این حوزه، حتی برای

پیشرفته‌ترین کشورهای جهان میسر نیست. بر این اساس، در شرایطی که کشورهای ناتو به واسطه قدرت نظامی متعارف و غیر متعارف گسترده خود، عملاً احساس امنیت نظامی دارند، اما چنین احساسی در حوزه سایبر برای آنها وجود ندارد. موضوع دوم به گستردگی استفاده از اینترنت و فضای سایبر در کشورهای غربی عضو ناتو برمی‌گردد. به هر حال، کشورهای عضو ناتو جزو پیشگامان استفاده از اینترنت و امکانات فضای سایبر در ابعاد مختلف سیاسی، اقتصادی، نظامی و فرهنگی و سطوح فردی و اجتماعی هستند. همین موضع باعث شده تمامی مراکز و مؤسسات حیاتی آنها تبدیل به اهداف بالقوه تهدیدات سایبری گردند.

در این زمینه می‌توان به آمریکا به عنوان قدرتمندترین عضو ناتو و پیشرفته‌ترین کشور جهان در حوزه سایبری اشاره نمود که خود جزو آسیب‌پذیرترین کشورهای جهان در حوزه سایبر به حساب می‌آید. لازم به اشاره است که در گزارش سال ۲۰۱۳ «مرکز اطلاعات ملی آمریکا»[1] تحت عنوان «گزارش سالانه ارزیابی تهدیدات جهانی علیه آمریکا» بر تهدیدات سایبری تأکید جدی شده است. در این گزارش، برای اولین بار تهدیدات سایبری به عنوان مهم‌ترین تهدید علیه منافع آمریکا ارزیابی شده‌اند. این در شرایطی است که در سال‌های قبل، تروریسم به عنوان مهم‌ترین تهدید علیه منافع و امنیت آمریکا ارزیابی می‌شد. همچنین می‌توان به «راهبرد سایبری وزارت دفاع»[2] در سال ۲۰۱۵ اشاره نمود که در آن تأکید بر آسیب‌پذیری سایبری، یکی از مهم‌ترین محورهای گزارش است. در این گزارش که توسط «اشتون کارتر»[3] وزیر دفاع آمریکا ارائه شده، مهم‌ترین تهدید علیه آمریکا تهدیدات سایبری و مهم‌ترین مشکل موضوع آسیب‌پذیری گسترده عنوان شده است (the DoD Cyber Strategy, 2015: 1-33).

در نهایت، باید به این نکته اشاره نمود که تأکید و اذعان دولت آمریکا به سطح بالای آسیب‌پذیری سایبری، خود گویای میزان و عمق آسیب‌پذیری سایر کشورهای عضو ناتو می‌باشد که در این حوزه از آمریکا عقب‌تر هستند. بر این اساس، می‌توان گفت عملاً بسیاری از کشورهای جهان آمادگی، ظرفیت و حتی گاهاً آگاهی لازم را در ارتباط با تهدیدات سایبری و آسیب‌پذیری‌های خود ندارند. این موضوع را می‌توان در جنگ‌های سایبری چند سال گذشته

---

1. National Intelligence
2. the DoD Cyber Strategy
3. Ashton Carter

کاملاً مشاهده نمود که طی آنها، مهاجمان به آسانی توانستند به اهداف خود دست یابند. این در شرایطی بود که کشورهای مورد تهاجم عملاً بعد از تهاجم و تنها بر اساس آسیب‌های واردشده متوجه شدند که مورد تهاجم سایبری قرار گرفته‌اند. در نتیجه این شرایط، کشورهای عضو ناتو به رهبری آمریکا، تلاش جدی در قالب ناتو برای مقابله با تهدیدات سایبری را یکی از راه‌کارهای تقویت خود در برابر تهدیدات ارزیابی می‌کنند. این موضوعی است که در تک‌تک اسناد رسمی ناتو و همچنین گزارش‌های امنیتی و اطلاعاتی آمریکا بدان تأکید شده است. به عنوان نمونه در راهبرد سایبری وزارت دفاع آمریکا، به وضوح بیان شده که وزارت دفاع دولت آمریکا باید به دنبال ایجاد ائتلاف بین‌المللی در قالب ناتو برای ایجاد «بازدارندگی سایبری»[1] باشد. هدف از این کار، ایجاد جبهه‌ای قدرتمند و مسلط در حوزه سایبری است تا هیچ بازیگری به خود اجازه هجوم سایبری به کشورهای غربی و متحدان آنها را ندهد و یا در غیر این صورت، با پیامدهای ویرانگری مواجه شود (the DoD Cyber Strategy, 2015: 15).

۲. تهدیدات سایبری روسیه و چین

تهدیدات و حملات سایبری روسیه علیه کشورهای اروپایی، یکی دیگر از دلایل تمرکز ناتو بر حوزه سایبر محسوب می‌شود. این موضوعی است که می‌توان به شکل کاملاً مشخصی تأثیرگذاری آن را در روند تکامل راهبرد سایبری ناتو مشاهده نمود. به عنوان نمونه، مقامات ناتو برای اولین بار در سال ۲۰۰۷ بر ضرورت تمرکز بر جنگ‌های سایبری تأکید کردند. سال ۲۰۰۷ سالی است که در آن مراکز مدنی و صنعتی استونی مورد تهاجم حملات سایبری هکرهای روسی قرار گرفتند (Herzog, 2011: 49-60). به دنبال این حملات، مقامات و سران ناتو خواهان ورود بحث جنگ‌های سایبری به دستور جلسه سران ناتو شدند. آنها با تأکید بر نگرانی‌های جدی در زمینه جنگ سایبری، خواهان آن شدند که کارگروه‌هایی برای درک عمیق‌تر و بهتر این فضا آماده شود تا با ارائه پیشنهاداتی، زمینه‌های لازم برای ورود ناتو به عرصه امنیت سایبری فراهم شود. بر این مبنا، اصولاً حمله روسیه به استونی را می‌توان آغازی بر فعالیت‌های ناتو در حوزه سایبر در نظر گرفت.

---

1. Cyber Deterrence

به دنبال این موضوع، در سال ۲۰۰۸ تأسیسات و مراکز حیاتی گرجستان هدف حملات سایبری روسیه قرار گرفتند. این امر باعث شد مقامات ناتو فراتر از موضع قبلی از ضرورت تدوین «سیاست دفاع سایبری ناتو»[1] صحبت کنند (Cyber security, 2008). همچنین، مقامات و سران ناتو خواهان آن شدند که امنیت سایبری به وظایف پیمان اضافه شود تا ناتو عملاً بتواند از مراکز حیاتی خود و اعضا در مقابل حملات سایبری دفاع نماید. تحت تأثیر این نگرانی‌ها و چندین سال کار تحقیقاتی و گروهی، در سال ۲۰۱۱ سند راهبردی ناتو در زمینه دفاع سایبری با عنوان «سیاست ناتو در زمینه دفاع سایبری»[2] آماده شد و به تصویب اعضا رسید (NATO Policy on Cyber Defence, 2011). بر اساس مفاد این سند، دفاع سایبری به وظایف ناتو اضافه شد و این سازمان اجازه یافت در حوزه سایبری از خود و اعضا در مقابل سایرین دفاع کند. در واقع در این سند، تفسیر موسعی از بند ۵ اساس‌نامه پیمان صورت گرفت و ناتو تبدیل به مرکزی برای همکاری گسترده اعضا در حوزه جنگ سایبری شد. به همین شکل و با توجه به اهمیت موضوع، در اجلاس‌های بعدی نیز از جمله در «اجلاس سران ناتو در ولز»[3] تأکیدهای گسترده‌ای بر جنگ سایبری صورت گرفت و اعضا اصول و محورهای دیگری از راهبرد سایبری خود را مورد موافقت قرار دادند (Wales Summit Declaration, 2014). لازم به اشاره است که اجلاس ولز تحت تأثیر دخالت‌های روسیه در اوکراین برگزار شد که طی آن نگرانی از حملات روسیه به خصوص در حوزه سایبری، یکی از محورهای جلسه بود. با توجه به این شرایط، تردیدی در این زمینه نیست که نگرانی روبه افزایش اعضای ناتو از تهدیدات سایبری رو به افزایش روسیه، یکی از دلایل اصلی تمرکز بر حوزه سایبری و تدوین و تکامل راهبرد سایبری ناتو بوده است.

در کنار روسیه، تهدیدات سایبری چین علیه کشورهای غربی و به خصوص آمریکا، یکی دیگر از دلایل تدوین راهبرد سایبری ناتو محسوب می‌شود. بر اساس گزارش‌های موجود، تهدیدات سایبری چین علیه کشورهای عضو ناتو ابعاد بسیار پیچیده‌تری به نسبت تهدیدات روسیه دارد. از جمله اینکه دولت آمریکا چین را بزرگترین کشور فعال جهان در حوزه اقدامات خرابکارانه سایبری و به خصوص «جاسوسی صنعتی سایبری»[4] معرفی می‌کند. بر اساس برآوردهای صورت‌گرفته، جاسوسی سایبری صنعتی چین سالیانه میلیاردها دلار برای کشورهای غربی هزینه به دنبال دارد.

---

1. NATO Cyber Defense Policy
2. NATO Policy on Cyber Defence
3. NATO Summit Wales 2014
4. Industrial Cyber Spy

ضمن اینکه این امر پیامدهای جدی برای شرکت‌های غربی در عرصه رقابت با شرکت‌های چینی به دنبال خواهد داشت (Lee, 2013). همچنین، آمریکا و کشورهای اروپایی نگرانی جدی از هکرهای مورد حمایت دولت چین دارند. این هکرها تقریباً به تمام مراکز حیاتی اقتصادی، نظامی، صنعتی و مدنی کشورهای غربی حمله می‌کنند و اطلاعات بسیار حیاتی آنها را به سرقت می‌برند. به عنوان نمونه، در یکی از حملات اخیر هکرهای چینی، اطلاعات ۲۲ میلیون نفر از کارمندان، نظامیان و پیمانکاران دولت فدرال را هک کردند (Kevin, 2015 :1). در نتیجه، همین شرایط در راهبرد سایبری سال ۲۰۱۵ آمریکا تهدیدات سایبری چین در کنار تهدید سایبری روسیه و برخی از دیگر کشورها از جمله کره شمالی و ایران، مهم‌ترین تهدیدات سایبری علیه منافع آمریکا و سایر کشورهای غربی عنوان شده است (the DoD Cyber Strategy, 2015: 15).

ج. تکامل راهبرد سایبری ناتو در مقابله با جنگ سایبری

راهبرد سایبری ناتو از سال ۲۰۰۷ مدام با توجه به شرایط و دیدگاهای کشورهای عضو تغییر کرده است. مهم‌ترین تغییر در این زمینه، پذیرش حمله سایبری در سطح حمله نظامی می‌باشد. در نتیجه این تغییر، ناتو فضای سایبر را به عنوان فضایی امنیتی و حتی نظامی در نظر گرفت و آن را مشمول «بند اساسنامه ۵»[1] خود کرد. البته، در مراحل اول این امر با مخالفت‌هایی از سوی برخی اعضا مواجه شد. با این حال در نهایت، در اجلاس سران ناتو در سال ۲۰۱۱، کشورهای عضو حملات سایبری را در حکم حمله نظامی ارزیابی کردند و در نتیجه، مجوز دفاع سایبری و نظامی، شامل استفاده از نیروی هوایی، دریایی و زمینی را برای خود محفوظ

---

۱. در بند ۵ پیمان ناتو آمده است: «دولت‌ها توافق دارند که حمله مسلحانه علیه یک یا چندی از آن‌ها در اروپا و آمریکای شمالی، به معنای حمله‌ای علیه تمامی آن‌ها تلقی خواهد شد. در نتیجه آنها موافقت می‌نمایند در صورتی که اینچنین 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، هر آنچه ضروری می‌نماید، به صورت انفرادی یا به اتفاق دیگر دولت‌ها، مساعدت نمایند تا امنیت را در منطقه آتلانتیک شمالی بازگردانده و برقرار نمایند. این امر می‌تواند شامل استفاده از نیروهای مسلح نیز باشد. هر گونه حمله مسلحانه و اقدامات اتخاذشده در نتیجه آن فوراً به شورای امنیت گزارش خواهد شد. این اقدامات زمانی که شورای امنیت اقدامات لازم را جهت بازگرداندن و برقراری صلح و امنیت بین المللی اتخاذ نماید، متوقف می‌شود.

داشتند. در واقع، این همان چیزی است که مقامات ناتو از آن تحت عنوان «اصل دفاع مشترک سایبری»[1] یاد می‌کنند که در برگیرنده هر گونه اقدام لازم دفاعی در برابر تهاجمات سایبری می‌باشد. لازم به ذکرست که در سطح ملی، اولین بار این مقامات آمریکایی بودند که حملات سایبری را در حکم حمله نظامی برآورد کردند و عملاً حق دفاع مشروع برای خود، آن هم در سطح نظامی را در نظر گرفتند. بعدها نیز برخی دیگر از کشورها به همین حق استناد کردند و حتی روسیه اعلان نمود که حق توسل به هر گونه ابزار نظامی در برابر حملات سایبری را دارد (ترابی، دی ۱۳۹۲). با این حال، ناتو اولین پیمان نظامی در سطح جهان به حساب می‌آید که از چنین رویکرد و نگاهی به جنگ سایبری دفاع می‌کند. مقامات ناتو همچنین در سلسله اسناد مختلف خود، به ویژه در سند سیاست ناتو در زمینه دفاع سایبری و همچنین، «اعلامیه سران در شیکاگو»[2]، مجموعه اصولی را برای مقابله با جنگ سایبری در نظر گرفتند که مطالعه آنها هم شناخت از راهبرد سایبری ناتو را عمیق‌تر می‌کند و هم نشان می‌دهد اصل ابهام و پیچیدگی حرف اول را در فضای سایبر می‌زند (Chicago Summit Declaration, 2012). تأکید اصلی این اصول بر تشریک مساعی، همکاری گسترده و عمیق و در عین حال همه‌جانبه اعضا با یکدیگر قرار دارد که در ادامه، مهم‌ترین موارد آنها مورد بررسی قرار می‌گیرد.

۱. اولویت دفاع سایبری

یکی از مهم‌ترین محورهای سند دفاع سایبری ناتو، تأکید سران این سازمان بر «اولویت دفاع سایبری»[3] به عنوان یکی از اهداف و مأموریت‌های اصلی ناتو و همچنین کشورهای عضو می‌باشد. بر این اساس، در سند نهایی ذکر شده که دفاع سایبری در مقابله با هجوم خارجی باید در اولویت تک‌تک کشورهای عضو قرار گیرد و تمامی اعضا باید سرمایه‌گذاری‌های لازم در این عرصه را جزو اولویت‌های ملی خود قرار دهند. از جمله اینکه، تمامی کشورهای عضو باید راهبرد مشخصی در عرصه سایبری مدون سازند و بر اساس آن، مراکز و مؤسسات ملی

1. Collective Cyber Defense
2. 2012 Chicago Summit Declaration
3. Priority for Cyber Defense

خود را برای دفاع سایبری فعال کنند. البته، ناتو در تمامی این مراحل و در تدوین راهبرد کشورهای عضو و همچنین، ایجاد مراکز فعال در زمینه دفاع سایبری، به تمامی کشورهای عضو مشورت‌های لازم را می‌دهد. هدف اصلی مقامات و سران ناتو در این بخش آن است که مطمئن شوند تمامی اعضا موضوع جنگ سایبری را جدی گرفته‌اند و تنها برای دفاع به توان ناتو اکتفا نمی‌کنند (Principle Cyber Defense Activities, 2008: 1).

۲. کمک به اعضا

یکی دیگر از اصول سند دفاع سایبری ناتو، «کمک به کشورهای عضو»[1] در زمینه مقابله با حملات سایبری کشورها و عوامل دشمن است. بر این اساس، ناتو وظیفه خود می‌داند در تعامل با کشورهای عضو، عملاً زمینه لازم برای همکاری و تعامل برای مقابله با حملات سایبری را آماده سازد و در هنگام تهاجم، با تمامی امکانات و ظرفیت به کمک کشور مورد حمله بشتابد. البته، این بدان معنا نیست که کشورها به شکل کامل وظیفه دفاع سایبری از مراکز و تأسیسات حیاتی خود را به ناتو واگذار می‌کنند. در واقع، وظیفه اصلی ناتو در زمینه دفاع سایبری بیشتر ماهیتی حمایتی و هماهنگ‌کننده دارد. به عبارت دیگر، کشورهای عضو می‌بایست زیر نظر ناتو امکانات، مراکز و نیروی انسانی فعال خود در حوزه جنگ سایبری را آماده کنند. بنابراین، هدف اصلی ناتو بالابردن توان کشورهای عضو در مقابله با دفاع سایبری از طریق ارتقاء توان ملی آنها و همکاری همه‌جانبه می‌باشد. با توجه به این شرایط، مقامات و سران ناتو انتظار دارند کشورهای عضو و همچنین مراکز فعال ناتو در زمینه دفاع سایبری، طی چند سال بتوانند کارایی خود را به شدت ارتقا دهند و ناتو دارای کامل‌ترین و کارآمدترین سیستم دفاع سایبری در سطح جهان گردد. این سیستم باید توانایی لازم در مقابله با هر گونه تهاجم سایبری از سوی هر کشور و هر عاملی در سطح جهان را داشته باشد (Principle Cyber Defense Activities: 2008: 2).

---

1. Assisting Individual Allies

۳. هم‌گرایی سیستم‌های دفاع سایبری

«هم‌گرایی دفاعی»[1] یکی دیگر از اصول مورد توجه ناتو در عرصه جنگ سایبری می‌باشد. به تعبیر دیگر، سران و مقامات ناتو کلید موفقیت خود در عرصه جنگ سایبری را در هم‌گرایی سیستم دفاع سایبری خود و فراتر از آن در راهبرد، سیاست و اقدامات مشترک و متحد سایبری ارزیابی می‌کنند. در این راستا در اجلاس لیسبون در سال ۲۰۱۲، دفاع سایبری در «پروسه برنامه‌ریزی دفاعی ناتو»[2] ترکیب شد. پروسه برنامه‌ریزی دفاعی ناتو، مهم‌ترین ابزار برای ایجاد هم‌گرایی اعضا و ناتو در زمینه دفاع سایبری محسوب می‌شود. در این اجلاس همچنین «نوآوری دفاع هوشمند ناتو»[3] به تصویب رسید. این نوآوری با هدف ارتقاء همکاری و هماهنگی مابین کشورهای عضو در مواجهه و مقابله با تهدیدات و حملات سایبری ایجاد گردید. در نهایت، باید به «گروه مشورتی صنعتی ناتو»[4] اشاره نمود که با هدف همکاری ناتو با صنعت در زمینه دفاع سایبری فعال می‌باشد. همه این موارد نشان می‌دهد هدف نهایی ناتو این است که کشورهای عضو آن در تمامی عرصه‌ها و ابعاد جنگ سایبری، همکاری و کار جمعی را در اولویت قرار دهند تا عملاً خلاقیت‌ها و موفقیت‌های ملی به شکل جمعی مورد استفاده همه قرار گیرد (Principle Cyber Defense Activities: 2008: 3).

٤. همکاری در زمینه تحقیق و آموزش

ناتو همچنین در زمینه تحقیق و آموزش در حوزه جنگ سایبری فعال است و «افزایش توانایی‌ها در زمینه آموزش و تمرین سایبری»[5] را یکی از مهم‌ترین اصول راهبردی سایبری خود می‌داند. مقامات و سران ناتو به خوبی بر این امر واقفند که مهم‌ترین موضوع در عرصه جنگ سایبری، برتری تکنولوژیکی و پیش‌گامی در زمینه علم و آگاهی است. به تعبیر دیگر، جنگ سایبری از جمله جنگ‌هایی است که پیروزی و شکست در آن به شدت تحت تأثیر برتری تکنولوژیکی قرار دارد. در این راستا، سران ناتو مراکز و مؤسسات مختلفی در زمینه

---

1. Integrated Cyber Defense
2. NATO Defense Planning Process (NDPP)
3. NATO Smart Defense Initiative
4. NATO Industrial Advisory Group (NIAG)
5. Enhances its Capabilities for Cyber Education, Training and Exercises

تحقیق و توسعه سایبری ایجاد نموده‌اند که مهم‌ترین آنها، «مرکز دفاع مشترک سایبری»[1] است که در شهر «تالین»[2] پایتخت استونی قرار دارد. در این مرکز، بهترین کارشناسان و پرسنل فعال در زمینه دفاع سایبری مشغول به تحقیق و توسعه و همچنین آموزش هستند. ناتو به کشورهای عضو توصیه نموده همکاری‌های علمی و فنی خود در زمینه جنگ سایبری را در این مرکز متمرکز نمایند. هدف نهایی از این همکاری علمی و فنی، ایجاد کامل‌ترین مرکز دفاع سایبری در سطح جهان توسط ناتو و همچنین ارتقاء توان تک‌تک کشورهای عضو می‌باشد. مقامات و سران ناتو ارزش و اعتبار خاصی برای این مرکز قائلند و آن را مرکزی برای همکاری بین بهترین کارشناسان و نخبگان کشورهای عضو در ارتباط با جنگ سایبری معرفی می‌کنند (Principle Cyber Defense Activities: 2008:4).

۵. همکاری با سایر کشورها و سازمان‌های بین‌المللی

یکی دیگر از محورهایی که در سند دفاع سایبری بر روی آن تأکید شده، موضوع «همکاری با شرکا»[3] یعنی سایر کشورها و سازمان‌های بین‌المللی متحد با غرب می‌باشد. یکی از این سازمان‌های مهم، اتحادیه اروپاست. سران و مقامات ناتو بر این باورند که گستردگی تهدیدات در فضای سایبر و همچین فرامرزی و فرامنطقه‌ای بودن آنها، باعث شده ضرورت همکاری میان کشورهای متحد غربی افزایش یابد. بر این اساس، باید همکاری‌های عمیق و جدی بین ناتو و سایر سازمان‌های غربی، به ویژه اتحادیه اروپا در تمامی زمینه‌ها و ابعاد صورت گیرد. این همکاری‌ها باید در حوزه پژوهش و آموزش مشترک سایبری، همکاری در زمینه پیش‌بینی، پیش‌گیری، دفاع و تهاجم سایبری و سایر ابعاد قابل همکاری باشد. به عبارت دیگر، ناتو خواهان همکاری با اتحادیه اروپا و دیگر سازمان‌های غربی در زمینه تدوین راهبرد، سیاست و اقدامات مشترک سایبری است. افزون بر این، در سند سایبری تأکید شده که کشورهای عضو ناتو باید از طریق مراکز و نهادهای ناتو، همکاری‌هایی در حوزه دفاع سایبری با سایر کشورهای غیر عضو داشته باشند. بر این اساس، ناتو باید تبدیل

---

1. The Cooperative Cyber Defense Centre of Excellence
2. Tallinn
3. Cooperating with Partners

به مرکزی برای همکاری‌های گسترده در ارتباط با جنگ سایبری بین کشورهای عضو و سایر کشورها گردد (Principle Cyber Defense Activities: 2008: 5).

٦. همکاری گسترده با بخش خصوصی و صنعت

در سند نهایی ناتو «همکاری با صنعت»[1] کشورهای عضو، یکی از مهم‌ترین محورهای تأثیرگذار در عرصه جنگ سایبری ارزیابی شده است. در این سند بارها تأکید شده که کلید موفقیت ناتو در دفاع از مراکز و تأسیسات حیاتی خود و اعضا، در همکاری نزدیک و همه‌جانبه با صنعت می‌باشد. در واقع، یکی از محورهای اصلی بحث اعضا در اجلاس لیسبون این موضوع بود که چگونه ناتو می‌تواند از صنعت برای کمک به کشورهای عضو در مقابله با جنگ سایبری کمک گیرد. ناتو خواهان آن است که مراکز مشترکی با صنعت کشورهای عضو داشته باشد تا بتواند با همکاری در حوزه‌های مختلف توانایی خود و کشورهای عضو را در دفاع سایبری و حوزه‌هایی چون تبادل اطلاعات، مدیریت بحران، برنامه‌ریزی و اجرا ارتقا دهد. همان گونه که اشاره شد، در این زمینه ناتو «گروه مشورتی صنعتی ناتو» را ایجاد نموده که وظیفه ایجاد ارتباط و همکاری بین ناتو و بخش صنعت کشورهای مختلف عضو را بر عهده دارد (Principle Cyber Defense Activities: 2008:6).

د. اجلاس سران ناتو در ولز

اجلاس سران ناتو در شهر نیوپورت ولز در سال ۲۰۱٤، یکی از مهم‌ترین اجلاس‌های پیمان آتلانتیک شمالی طی چند دهه گذشته و به خصوص در دوران پساجنگ سرد محسوب می‌شود. علت اصلی اهمیت این اجلاس، به اوضاع و احوال بی‌ثبات و نگران‌کننده جهان، به ویژه در منطقه اروپای شرقی و خاورمیانه برمی‌گردد. در این راستا، سه موضوع در اجلاس سران ناتو در ولز محور جلسات را به خود اختصاص دادند که عبارت بودند از نگرانی از وضعیت اروپای شرقی، مسئله خروج ناتو از افغانستان و نگرانی‌های سایبری. در واقع، مسئله

1. Cooperating with Industry

تهدیدات و امنیت سایبری در اجلاس ولز بخش مهمی از مذاکرات را به خود اختصاص داد. با وجود این، رسانه‌ها و کارشناسان کمتر این موضوع را مورد توجه قرار دادند. این در شرایطی بود که در متن رسمی منتشرشده، ۲۰ بار به واژه سایبر اشاره شده و ٤ بند اصلی از متن به این حوزه از نگرانی‌های کشورهای عضو اشاره دارد (Wales Summit Declaration, 2014). نکته نگران‌کننده این است که سران ناتو باز در همین متن به شکل رسمی حملات سایبری را مشمول بند ۵ اساسنامه ناتو تعبیر نمودند و عملاً مجوز دفاع مشروع را برای خود قائل شدند. با توجه به این شرایط، موضوع سایبر را باید یکی از مهم‌ترین موضوعات محوری اجلاس ناتو در ولز دانست که در ادامه این موضوع در ابعاد مختلف مورد بحث و بررسی قرار می‌گیرد.

۱. تکامل رویکرد ناتو به جنگ سایبری در اجلاس ولز

همان گونه که گفته شد، یکی از مهم‌ترین موضوعات مطرح در اجلاس ولز، نگرانی‌های متعدد و متنوع اعضای ناتو در حوزه سایبر بود. در واقع، موضوع سایبر تنها موضوعی در این اجلاس بود که هم به شکل مستقل و هم در کنار و در ارتباط با سایر نگرانی‌ها مورد بحث قرار گرفت. منظور از ارتباط سایبر با سایر موضوعات، پیوستگی حوزه سایبر با سایر نگرانی‌های اصلی سران ناتو، از جمله موضوع دخالت‌های روسیه در شرق اروپا و استفاده داعش یا «دولت اسلامی»[1] از فضای سایبر می‌باشد. در مورد موضوع اول، نگرانی این است که روسیه مطابق رویه گذشته خود از حوزه سایبر به عنوان ابزاری برای تحت فشار قراردادن کشورهای هدف، که در اینجا اوکراین و سایر کشورهای اروپای شرقی هستند، استفاده کند. لازم به اشاره است دولت روسیه طی دو دهه گذشته، از فضای سایبر به عنوان ابزاری برای تحت فشار قراردادن کشورهایی که سیاست مستقلی در اروپای شرقی، منطقه قفقاز و آسیای مرکزی داشته‌اند، استفاده نموده است (ترابی، مهر ۱۳۹۳). بنابراین، علاوه بر ملاحظات راهبردی، کشورهای عضو ناتو نگران حملات سایبری روسیه به کشورهای اروپای شرقی هستند. این نگرانی به خصوص زمانی تشدید می‌شود که اتحادیه اروپا و آمریکا در حال افزایش تحریم‌ها علیه روسیه هستند و مقامات کرملین ابزار چندانی برای مقابله با این تحریم‌ها ندارند. به همین

1. Islamic State

دلیل، این نگرانی وجود دارد که مقامات روس دستور حملات سایبری گسترده به اوکراین و سایر کشورهای اروپای شرقی را صادر کنند. به هر حال، در این اجلاس، سران ناتو هشدارهایی به روسیه در زمینه به راه انداختن جنگ سایبری علیه کشورهای اروپای شرقی دادند. از جمله اینکه به شکل غیر رسمی اعلان نمودند که حمله سایبری روسیه به اروپای شرقی با پاسخ‌های جدی ناتو مواجه خواهد شد (Wales Summit Declaration, 2014: 1).

موضوع دیگر در این زمینه، توسل داعش یا دولت اسلامی به امکانات فضای سایبر، آن هم به شکل بسیار گسترده و حرفه‌ای با اهداف مختلف می‌باشد. لازم به اشاره است که دولت اسلامی توانایی بسیار بالایی در زمینه استفاده از فضای سایبر دارد و از این ابزار با اهدافی همچون تبلیغ ایده‌های خود، آن هم به شکل بسیار جذاب و تحریک‌کننده استفاده می‌کند. همچنین، دولت اسلامی به شکل گسترده از اینترنت برای اهدافی همچون ایجاد جنگ روانی، ترس و وحشت بهره‌برداری می‌کند. به واقع، استفاده از اینترنت برای جنگ روانی و ایجاد ترس قبل از حمله اصلی، یکی از مهم‌ترین تاکتیک‌های موفق دولت اسلامی در عراق و سوریه بوده است. دولت اسلامی با نشان‌دادن خشونت گسترده خود علیه مخالفان، ترس و نگرانی گسترده را در دل سایرین ایجاد می‌کند. علاوه بر این، دولت اسلامی از فضای سایبر برای کسب درآمد و جذب کمک‌های مالی استفاده می‌کند. بر این اساس می‌توان گفت، فضای سایبر اهمیت محوری در تمامی فعالیت‌های دولت اسلامی، من جمله در حوزه‌هایی چون راهبرد جنگی، یارگیری، تبلیغ و کسب درآمد دارد. در این راستا، سران ناتو در اجلاس ولز یکی از محورهای مقابله موفق با دولت اسلامی را در حوزه سایبر ارزیابی نمودند. در این اجلاس، قرار بر این شد که دولت‌های عضو در همکاری با بخش خصوصی، زمینه حذف حضور دولت اسلامی از فضای سایبری را مهیا سازند. از جمله اینکه قرار شد دسترسی این گروه به سایت‌هایی مثل فیس‌بوک و سایر شبکه‌های اجتماعی قطع شود تا این گروه نتواند از آن برای کسب اهداف خود استفاده کند (Wales Summit Declaration, 2014: 1-3). علاوه بر این، دو موضوع کلی که به شکلی با فضای سایبر ارتباط جدی داشتند، سران ناتو در اجلاس ولز نگرانی کلی خود از تهدیدات در فضای سایبر را اعلان نمودند. بر این اساس، در بند ۷۲ و ۷۳ سند نهایی اجلاس ولز به شکل اختصاصی به موضوع سایبر پرداخته شده است. در این دو بند، به شکل خلاصه گفته می‌شود:

«وضعیت کنونی و نگاه به آینده نشانگر آن است که تهدیدات سایبری در حال تبدیل‌شدن به یکی از مهم‌ترین نگرانی‌های امنیتی هستند. ضمن اینکه این تهدیدات مدام در حال پیچیده و جدی‌شدن هستند. بر این اساس، همان گونه که «سیاست دفاع سایبری»[1] را مدون کردیم، باید جدیت بیشتری برای اجرای آن داشته باشیم. همچنین، ناتو به عنوان هماهنگ‌کننده اقدامات و سیاست‌های کشور عضو، باید مسئولیت اصلی دفاع سایبری در مقابل تهدیدات را بر عهده داشته باشد. امروزه، حملات سایبری می‌تواند پیامدهای گسترده‌ای در سطح جنگ‌های متعارف داشته باشد. بنابراین، ضروری است اقدامات ما در مقابل چنین خطراتی در چارچوب ناتو هماهنگ باشد. ما تأکید داریم که باید اقدامات ما در حوزه سایبر مطابق با حقوق بین‌الملل و حقوق بشردوستانه و منشور ملل متحد باشد» (Wales Summit Declaration, 2014: 5).

در ادامه همین بند و به شکل صریح بیان می‌شود که حملات سایبری به کشورهای عضو ناتو در حکم حمله نظامی و مشمول بند ۵ اساسنامه محسوب می‌شود که این امر عملاً مجوز دفاع مشروع سایبری و نظامی را به سازمان می‌دهد. این جمله کلیدی‌ترین جمله سند نهایی ناتو در حوزه سایبری محسوب می‌شود. بر این اساس، سران ناتو مجدداً در اقدامی که چندان مطابق با حقوق بین‌الملل موجود نیست، حمله سایبری به یکی از کشورهای عضو را معادل حمله نظامی و در نتیجه مشمول بند ۵ اساسنامه معرفی می‌کنند (Melze, 2011: 1-6). همان‌گونه که گفته شد، در اجلاس گذشته نیز این موضوع مورد بحث قرار گرفت. با وجود این، برای اولین بار بود که در متن نهایی اجلاس ناتو، بدون هیچ ابهامی از دفاع متعارف و دفاع سایبری مشروع در برابر حملات سایبری بحث می‌شود. به هر حال، این موضوع چندان با رویه و حقوق بین‌الملل موجود هم‌خوانی ندارد و طرح آن می‌تواند مباحث گسترده‌ای را در حوزه‌های مختلف سیاسی، حقوقی، نظامی و دفاعی ایجاد کند.

علاوه بر این موضوع مهم، در ادامه سند در مورد لزوم آمادگی، هماهنگی و یکپارچگی بین ناتو و اعضا و همچنین بین اعضا با یکدیگر در زمینه دفاع سایبری صحبت شده است؛ از جمله اینکه کشورهای عضو متعهد شده‌اند بیش از گذشته دفاع سایبری را جدی بگیرند و برنامه‌های بیشتری را برای ارتقاء آمادگی در برابر هر گونه حمله سایبری در اولویت قرار دهند. همچنین، بر این نکته

1. Cyber Defense Policy

تأکید شده که ناتو باید مرکز هماهنگی تمامی اقدامات کشورهای عضو در زمینه تهدیدات سایبری باشد. در واقع، اصل هماهنگی با محوریت ناتو، یکی از مهم‌ترین اصول مورد نظر سران در مقابله با تهدیدات سایبری محسوب می‌شود. همچنین، سران ناتو یکبار دیگر بر اهمیت گسترش همکاری با سایر نهادها و سازمان‌های بین المللی از جمله اتحادیه اروپا و همچنین بخش‌های خصوصی و صنعتی فعال در حوزه سایبری تأکید نمودند. از نظر آنها، کلید نهایی مقابله با تهدیدات سایبری گسترش همکاری با تمامی بازیگرانی است که می‌توانند در این امر خطیر و پیچیده یاری‌دهنده دفاع سایبری پیشرو باشند (Wales Summit Declaration, 2014: 4).

نتیجه‌گیری

علت اصلی تمرکز سران ناتو بر جنگ سایبری، تا حد زیادی به واسطه ماهیت پیچیده و متفاوت فضای سایبر به نسبت تهدیدات گذشته و همچنین، آگاهی عمیق از آسیب‌پذیری اعضا بوده است. این موضوع به خصوص زمانی آشکارتر شد که برخی از کشورهای اروپای شرقی مورد حملات سایبری روسیه قرار گرفتند و عملاً نتوانستند کار خاصی را انجام دهند. بر این اساس، حملات سایبری روسیه هم آسیب‌پذیری در حوزه سایبر را آشکارتر کرد و هم مهر تأییدی بر ماهیت متفاوت فضای سایبر زد. در نتیجه این شرایط و حملات، کشورهای عضو ناتو به رهبری آمریکا تصمیم گرفتند موضوع جنگ سایبری را در دستور جلسات خود قرار دهند. به هر حال، در نتیجه سال‌ها کار تحقیقاتی و تصمیمات سران، در نهایت محورهای راهبرد سایبری ناتو در قبال جنگ سایبری تدوین و تکامل یافت تا جایی که این پیمان دفاع سایبری را در حوزه وظایف ذاتی خود معرفی کرد.

تدوین و تکامل راهبرد سایبری ناتو، متضمن چند نکته بسیار مهم و تعیین‌کننده تحلیلی است که می‌تواند برای سایر کشورها نیز آموزنده باشد. اول اینکه، صرف تدوین راهبرد سایبری توسط این سازمان نظامی و دفاعی، خود گواهی روشن بر نگرانی‌های جدی از تهدیدات به شدت متفاوت و متنوع فضای سایبر و نقش تعیین‌کننده آن در سلسله‌مراتب قدرت و امنیت جهانی می‌باشد. بنابراین، ورود امنیت سایبری به دستور جلسه و همچنین، وظایف ناتو تردیدی در شکل‌گیری عرصه جدیدی در حوزه امنیتی باقی نگذاشته است. همان گونه که اشاره شد، علت اصلی این موضوع گستردگی و

همه‌گیربودن فضای سایبر و در نتیجه، گستردگی تهدید در تمام حوزه‌های اقتصادی، سیاسی، اجتماعی، فرهنگی و در سطوح مختلف فردی، جمعی، دولتی و جهانی می‌باشد. بنابراین، نکته اولی که می‌توان از راهبرد سایبری ناتو برداشت نمود، تأکید بر اهمیت، گستردگی و نگرانی عمیق از تهدیدات سایبری حتی برای کشورهای پیشرفته جهان است.

نکته **دوم** اینکه، هرچند جنگ سایبری حوزه‌ای جدید و متفاوت در عرصه امنیت است، اما خود می‌تواند مقدمه و همچنین، بهانه‌ای برای جنگ‌های نظامی باشد. همچنین، این امکان وجود دارد که در کنار جنگ‌های نظامی،کشورهای مختلف از جنگ سایبری به عنوان ابزاری برای شکست دشمن استفاده کنند. همان گونه که گفته شد، در راهبرد سایبری ناتو آمده است که این سازمان حملات سایبری به اعضا را در حکم حمله نظامی ارزیابی می‌کند و حق هر گونه پاسخ جمعی از جمله پاسخ سایبری و نظامی را دارد. البته، پیش از ناتو این آمریکا و روسیه بودند که چنین حقی را برای خود قائل شدند که این امر با انتقادات جدی از سوی کشورها و کارشناسان مواجه شد. به هر حال، این امر به خوبی نشان می‌دهد تا چه میزان فضای امنیتی تحت تأثیر فضای سایبر گنگ و پیچیده شده است.

نکته **سوم** اینکه، مطالعه اصول و محورهای راهبرد سایبری ناتو، نشان‌دهنده ماهیت متفاوت فضای سایبر در مقایسه با فضاهای سنتی امنیت می‌باشد. همان گونه که شرح آن رفت، ناتو برای آمادگی سایبری تأکید گسترده‌ای بر همکاری با بخش خصوصی، آموزش‌های جدید، دفاع متقابل جمعی و مواردی از این قبیل دارد که خود گویای تفاوت‌ها با راهبردهای سنتی این سازمان می‌باشد. در واقع، از این رویکرد می‌توان این گونه نتیجه گرفت که فضای سایبر نیازمند نگاهی جدید و متفاوت و در نتیجه راهبردها، تاکتیک‌ها، نیروها و آموزش‌های جدید می‌باشد. بنابراین، کشورهایی که می‌خواهند در این حوزه جدید و پیچیده امنیتی موفق باشند، باید رویکرد سنتی و نظامی به امنیت را حداقل در این حوزه تعدیل و اصلاح نمایند. در نهایت، باید اشاره نمود که در آینده، فضای سایبر نقش مهمی در امنیت و قدرت کشورها و در نتیجه جایگاه آنها در عرصه جهانی خواهد داشت. در این راستا، آنهایی که سرمایه‌گذاری لازم را در این حوزه می‌کنند، شانس بیشتری برای امنیت خواهند داشت. در مقابل، بازندگان جنگ‌های آینده آنهایی هستند که که این حوزه جدید را کمتر و دیرتر می‌شناسند و در نهایت، با نگاهی سنتی می‌خواهند به آن پاسخ دهند.

منابع

ترابی، قاسم (شهریور ۱۳۹۲) «جنگ سایبری؛ ابعاد و مؤلفه‌ها»، **برآورد؛ ماهنامه تخصصی مطالعات امنیت ملی**، شماره ٦.

ترابی، قاسم (مرداد ۱۳۹۲) «تبین مفهومی و محتوایی جنگ سایبری»، **برآورد؛ ماهنامه تخصصی مطالعات امنیت ملی**، شماره ۵.

ترابی، قاسم (دی ۱۳۹۲) «بررسی سند دفاع سایبری ناتو»، **برآورد؛ ماهنامه تخصصی مطالعات امنیت ملی**، شماره ۱۰.

ترابی، قاسم (مهر ۱۳۹۳) «بررسی موضوع سایبر در اجلاس سران ناتو در ولز»، **برآورد؛ ماهنامه تخصصی مطالعات امنیت ملی**، شماره ۱۹.

منشور ملل متحد (۱۳۹۳) **فصل هفتم**، قابل دسترس در:

http://dl.irpdf.com/ebooks/Part6/(2090).pdf

Chicago Summit Declaration (2012) at:
http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease

Cyber security (2008) at: http://www.nato.int/cps/en/natohq/topics_78170.htm

Cyber Warfare (2015) Cyber War Definition, at:
http://www.rand.org/topics/cyber-warfare.html

Don Lee (2013) "China Dismisses U.S. Accusations of Cyber-Spying", **Los Angeles Times**, May 7, 2013. http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-uscyber-spying-20130507.

Herzog, Stephen (2011) **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**, at:
http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

Krepinevich, Andrew (2012) **Cyber Ware: A "Nuclear Option?** at:
http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/

Lewis, James (2006) **Cyber security and Critical Infrastructure Protection**, at: http://cip.management.dal.ca/publications/Cybersecurity%20and%20Critical%20Infrastructure%20Protection.pdf

Libicki C. Martin (2009) **Cyber deterrence and Cyber war**, at:
http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lieutenant Colonel Scott W. Beidleman (2009) **Defining and Deterring Cyber War**, at: https://www.hsdl.org

McCaney, Kevin (2015) White House offers protections to 22 million affected by OPM hack, at: https://defensesystems.com/articles/2015/07/10/opm-hack-22-million-white-house-protections.aspx

Melzer, Nils (2011), **Cyberwarfare and International Law**, at:
http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

Morgus, Robert (2014), NATO Tries to Define Cyber War, at:
http://www.realclearworld.com/articles/2014/10/20/nato_tries_to_define_cyber_war_110755.html

NATO Policy on Cyber Defense (2011) at:
http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

Newton, Lee (2013) **Counterterrorism and Cyber security, Total Information Awareness**, Springer New York Heidelberg Dordrecht London

Principle Cyber Defense Activities (2008) at:
http://www.nato.int/cps/en/natohq/topics_78170.htm

Sanger E. David (2015), **Document Reveals Growth of Cyberwarfare between the U.S. and Iran**, at: http://www.nytimes.com

Siboni, Gabi and Kronenfeld, Sami (2012) **Iran's Cyber Warfare**, INSS Insight, at: www.inss.org.il/index. aspx?id=4538&articleid=5203

the DoD Cyber Strategy (2015) at; http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Van den hole, Leo (2003), **Anticipatory Self-Defence under International Law**, at: http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1160&context=auilr

Wales Summit Declaration (2014) at:
http://www.nato.int/cps/en/natohq/official_texts_112964.htm