امنیت طیف الکترومغناطیس

نگاهی جامع به آخرین پیشرفت‌ها و رویکردها به فضای سایبر
با محوریت امنیت ملی و جنگ‌های نوین و هیبریدی

آزمایشگاه امنیت کی‌پاد

نویسنده میلاد کهساری الهادی

فهرست

دفاع / بهره‌برداری از طیف الکترومغناطیس در برابر / برای جنگ سایبری [i]:

تا دهه ۹۰، دو دامنه ارتباطی مجزا از هم وجود داشت: اولین دامنه را با عنوان مخابرات[۱] و دومین دامنه را با عنوان کامپیوترها می‌شناسیم که دامنه اول برای ارسال و دریافت صدا[۲] و دامنه دوم برای ارسال و دریافت داده‌های خام / ویدیو[۳] مورد استفاده قرار می‌گرفت.

هر چه فناوری پیشرفت می‌کند، ما مشاهده می‌کنیم که محصولات مخابراتی بیشتر بر روی پلتفرم‌های کامپیوتری توسعه داده می‌شوند، و همچنین اکثریت سرویس‌ها از سخت‌افزار محور بودن به نرم‌افزار محور بودن در حال مهاجرت هستند.

به عبارت دیگر با توجه به سطوح تغییرات وسیع در فناوری‌های مخابراتی / الکترونیکی، تصور می‌شود به زودی دیگر خبری از دستگاه‌های الکترونیکی برای مخابرات و ارتباطات نباشد و بلکه یک کامپیوتر بتواند تمامی سرویس‌های مخابراتی را ارائه کند. ولی از آنجایی که کامپیوترها متکی به سخت‌افزار و همچنین نرم‌افزار هستند، سطح بسیار گسترده‌ای از تهدیدات [ii] را شامل می‌شوند، همین مسئله در ادامه موجب خواهد شد، طیف وسیعی از مسائل با محوریت امنیت[۴] و حفظ محرمانگی[۵]، یکپارچگی ارتباطات[۶] رخ بدهد.

رشد تجهیزات کامپیوتری اکنون موجب شده است چندین برنامه کاربردی بتوانند درون یک دستگاه نصب و پیکربندی شوند و همچنین در نهایت خدمات‌دهی کنند و به همین دلیل دیگر نمی‌توان بین فناوری اطلاعات و مخابرات مرز مجزایی در نظر گرفت چون به یکدیگر اکنون متکی هستند. به عنوان مثال، فناوری موبایل، به خصوص گوشی‌های هوشمند و تبلت‌ها اکنون چندین فناوری را بر روی دستگاه ارائه می‌دهند و کاربران علاوه بر استفاده از آن‌ها برای کارهای روزمره می‌توانند از آن‌ها برای انتقال اطلاعات به صورت بی‌سیم استفاده کنند.

---

[1] Telecom
[2] Voice
[3] Data/Videos
[4] Safety
[5] Confidentiality
[6] Communication Integrity

زیرساخت شبکه‌های خطوط ثابت[1] (شبکه‌های خانگی) که دارای کانال داده و صدای[2] مجزا هستند، با زیرساخت گوشی‌های همراه[3] بسیار متفاوت است، چون بر روی زیرساخت موبایل تمامی فعل و انفعالات ارتباطی بر روی یک کانال صورت می‌گیرد و مانند زیرساخت شبکه‌های خانگی به دو کانال مجزا برای ارسال داده و صدا نیاز نیست، زیرا با معرفی پروتکل VoIP دیگر می‌توان بر روی شبکه‌های داده[4]، صدا هم ارسال کرد.

گوشی‌های همراه اکنون یک دستگاه مخابراتی وایرلس (و همچنین دروازه‌ای به اینترنت[5]) مبتنی بر تعریف هستند، به همین دلیل اکنون می‌توانیم آن‌ها را آسیب‌پذیر به حملات سایبری با محوریت بهره‌برداری از طیف الکترومغناطیس[6] بدانیم.

شایان ذکر است، اکنون ماهواره‌ها همچنین توسط تجهیزات کامپیوتری کنترل و مدیریت می‌شوند که ممکن است در ادامه به شبکه ابری نظامی یا یک شبکه ایرگپ در محیط مبارزه تاکتیکی[7] متصل شده باشند. رهگیری[8]، جمینگ[9]، منع سرویس[10] سیگنال‌های ماهواره‌ای اکنون نسبت به سامانه‌های ارتباطی بی‌سیم زمینی ساده‌تر است. به همین دلیل، حملات سایبری بر علیه ماهواره‌ها گزارش شده است که در آن سیگنال تله متری[11] خراب شده بود.

از آنجایی که اکنون کامپیوترها نقش بسیار مهمی در کنترل و حتی طراحی خود ماهواره‌ها دارند، محدوده آسیب‌پذیری آن‌ها از منظر نرم‌افزار و همچنین پروتکل‌های ارتباطی به همین دلیل گسترش پیدا خواهد کرد. به عنوان مثال، اگر در ماهواره برای ارتباط با ایستگاه زمینی و بالعکس از پروتکلی مانند CubeSat استفاده شود [iii]، و در ادامه اگر در طراحی آن آسیب‌پذیری کشف شود، به راحتی می‌توان از آن بهره‌برداری کرد تا به ماهواره فرمان مخرب داد. زیرا همانطور که ایستگاه زمینی می‌تواند با آن تعامل کند، دیگر عناصر هم خواهند

---

[1] Fixed Line Networks Infrastructure
[2] Voice and Data Channels
[3] Mobile Phone Infrastructure
[4] Data Networks
[5] Gateway to Internet
[6] Electromagnetic Spectrum
[7] Tactical Battle Area
[8] Interception
[9] Jamming
[10] Denial of Service
[11] Telemetry Signal

توانست با تشخیص مسیر حرکت ماهواره و پیدا کردن محل آن در مدار زمین، با آن ارتباط بگیرند یا بر روی فرکانس آن عملیات جمینگ انجام بدهند تا ارتباط آن با مرکز کنترل ایستگاه زمینی از بین برود.

به هر صورت، فناوری شبکه با سرعت بسیار بالایی دارد به سمت پروتکل IP برای تمامی سرویس‌های خود حرکت می‌کند، از همین روی ارتباطات بی‌سیم وسعت بیشتری پیدا خواهند کرد. در نتیجه انتظار خواهیم داشت جنگ سایبری که به صورت سنتی متوجه لایه ۳ به بالا در شبکه بود (مخصوصاً لایه برنامه‌های کاربردی[۱])، به لایه فیزیکی در قالب لینک‌های فرکانس رادیویی[۲] برسد. همچنین این شرایط با ورود اشیاء اینترنتی[۳] به صنایع حیاتی پیچیده‌تر خواهد شد چون ابزارهای جنگ الکترونیک[۴] سنتی می‌توانند با جستجوی فراگیر فرکانس رادیوی برای جمینگ ارتباطات گسترده این تجهیزات را از کار بیندازند.

همچنین، شبکه‌های نظامی[۵] نسبت به فناوری و تغییرات آن مستثنا نیستند. فناوری‌هایی مانند تلفن همراه، ماهواره‌ها، رادیوهای زیرساخت بی‌سیم[۶]، رادیوی نرم‌افزاری[۷]، به حملات سایبری از طریق کانال‌های بی‌سیم اکنون آسیب‌پذیر هستند.

در این گزارش به احتمالات مرتبط با انجام حملات سایبری از طریق بهره‌برداری طیف الکترومغناطیس با توجه به شبکه‌های نظامی در محیط رزم تاکتیکی (TBA) خواهیم پرداخت. همچنین در این مورد هم بحث خواهیم کرد که در شرایط فعلی چگونه باید عمل کرد و زیرساختی برای مقابله و بهره برداری از حملات سایبری با محوریت مسائل نظامی و امنیت ملی ایجاد کرد. شایان ذکر است، این مقاله دارای دو بخش است. در بخش دوم به استفاده از طیف الکترومغناطیس برای انجام جنگ سایبری خواهیم پرداخت.

مقدمه‌ای بر امنیت طیف الکترومغناطیس

فناوری‌های مخابراتی و اطلاعاتی می‌توانند زیربنای انجام عملیات‌های نظامی را به صورت کامل تغییر بدهند. به عنوان مثال، جنگ اول خلیج فارس[۸] تصویری از انقلابی بالقوه ارائه کرد که در آن فناوری به همراه دکترین

---

[1] Application Layer
[2] Radio Frequency Links
[3] Internet of Things
[4] EW Tools
[5] Military Networks
[6] Wireless Backhaul Network
[7] Software Defined Radio
[8] Gulf War

و آموزش‌های مناسب به کار گرفته شد، و نتایج بی‌سابقه‌ای به عمل آورد. به عنوان مثال، به دست آوردن و بهره‌برداری از حاکمیت اطلاعاتی[1] یک هدف کلیدی برای عملیات طوفان صحرا[2] بود.

اولین اهداف عراقی که توسط آمریکایی‌ها مورد هدف قرار گرفتند شامل پدافند هوایی، مراکز رهبری[3] از جمله مراکز فرماندهی[4]، کنترل[5]، مخابرات[6] و استخبارات[7] و خطوط انتقال برق[8] بودند که دارای الویت بالایی در جریان اطلاعات[9] عراقی‌ها داشتند. همچنین جنگ عراق و افغانستان فرماندهان را با تهدیدات طیف الکترومغناطیسی و سایبری جدیدی مواجه کرد. به عنوان مثال، نیروهای شورشی عموما در فضای سایبری با استفاده از اینترنت پیام‌های خودشان را تبلیغ می‌کردند، در حالیکه در زمانی مشابه به صورت فیزیکی سربازان را با به کارگیری تسلیحات الکترومغناطیسی از قبیل بمب‌های کنارجاده‌ای قابل فرماندهی رادیویی تهدید می‌کردند. اکنون به هر صورت، جنگ سایبری به عنوان پنجمین بعُد جنگ بعد از زمین، دریا، هوا و فضا شناخته می‌شود چون از آن می‌توان برای مسائل تهاجمی استفاده کرد.

یکی از محوریت‌های اصلی منازعات فیزیکی (جنگ تمام عیار)، انهدام زیرساخت‌های انرژی، اقتصادی و ارتباطی است تا هدف دیگر امکان حیات و دفاع از خود را نداشته باشد. در جنگ‌های سنتی از تسلیحات فیزیکی برای انهدام این نوع زیرساخت‌ها استفاده می‌کردند، اما از آنجایی که امروز بسیاری از تجهیزات در زیرساخت تولید انرژی و همچنین ارتباطی متکی به کامپیوترها هستند، مهاجمین می‌توانند با توسعه جنگ‌افزارهای سایبری مانند بدافزارها[iv] و همچنین استفاده از آسیب‌پذیری‌های روز-صفر[v] به این نوع زیرساخت‌ها آسیب جدی برسانند تا قابل سرویس‌دهی و عملیات نباشند یا حتی در مواردی آن‌ها را به کل نابود کنند. حمله بدافزار استاکس‌نت به زیرساخت غنی‌سازی اورانیوم ایران که موجب از بین رفتن تعداد زیادی سانتریفیوژ شد[vi] و یا حمله بدافزار BlackEnergy به زیرساخت تولید برق اوکراین که موجب شد[vii] اوکراین به مدت طولانی دچار مشکل در تامین برق و انرژی خود شود، مثالهایی از این نوع حملات هستند.

[1] Information Dominance
[2] Desert Storm
[3] Leadership
[4] Command
[5] Control
[6] Communication
[7] Intelligence
[8] Electrical Grid
[9] Information Flow

خط تمییز بین فناوری اطلاعات و مخابرات

در گذشته ما رادیو، دوربین، ماشین حساب، تلویزیون، تلفن ثابت، فکس و کامپیوتر برای انجام کارهایی مانند انتشار صوت، عکاسی، محاسبات ریاضی، انتشار ویدیو، ارتباطات صوتی، ارسال و دریافت مستندات، و ... به صورت مجزا داشتیم. اکنون به دلیل پیشرفت و رشد فناوری، ما شاهد مهاجرت تمامی این سرویس‌ها از سخت‌افزار محور بودن به نرم‌افزار محور بودن هستیم. به عبارتی اکنون یک دستگاه کامپیوتری مانند تبلت، گوشی همراه، یا لپ‌تاپ مدرن می‌توانند تمامی سرویس‌های ذکر شده را به صورت یکجا در قالب راه‌حل‌های نرم‌افزاری ارائه بدهند. همین مسئله اکنون موجب شده است که دیگر ما نتوانیم بین مخابرات و کامپیوتر خط تمایز واضحی در نظر بگیریم. اکنون ما گوشی‌های هوشمندی داریم که توانایی ارائه دیتا، صوت، و ویدئو بر روی یک کانال فرکانسی مشترک به همراه انجام کارهای دیگر مانند فیلم‌برداری، محاسبات، وب گردی، ارسال پیام و ... هستند.

اکنون گوشی‌های موبایل، مانند یک دستگاه مخابراتی وایرلس عمل می‌کنند و همچنین دروازه‌ای برای دسترسی به اینترنت هستند، از همین روی می‌توانیم آن‌ها را مستعد به بهره‌برداری از آسیب‌پذیری‌های موجود در طیف الکترومغناطیس بدانیم. بسیاری از تجهیزات مخابراتی مانند مسیریاب‌ها[۱]، سوییچ‌ها[۲]، و... در قالب سرویس نرم‌افزاری بر روی یک پلتفرم محاسباتی[۳] در حال ارائه هستند. حتی سرویس‌های قدیمی TDM، مانند صدا اکنون در شبکه‌های کامپیوتری با استفاده از پروتکل صدا بر روی پروتکل اینترنت[۴] (VoIP) ارائه می‌شوند. حتی سامانه‌های مخابراتی مانند ماهواره‌ها از طریق کامپیوترها کنترل می‌شوند که همانطور پیش از این ذکر شد به حملات سایبری آسیب‌پذیر هستند.

شبکه‌های نظامی[۵]

در شبکه‌های نظامی همچنین ما شاهد یک موج از تغییرات در فناوری‌ها هستیم [viii]. اکنون شبکه رادیویی نبرد (CNR)[۶] در حال مهاجرت به راه‌حل رادیو نرم‌افزاری (SDR)[ix] هستند که این راه‌حل مبتنی بر یک

[1] Routers
[2] Switches
[3] Computing Platform
[4] Voice over IP
[5] Military Network
[6] Combat Net Radio - CNR

پلتفرم کامپیوتری کار می‌کند. به همین دلیل، هنگام استفاده از راه‌حل رادیو نرم‌افزاری، این احتمال وجود دارد که با بهره‌برداری از آسیب‌پذیری‌های موجود در طیف الکترومغناطیسی بر علیه ارتباطات مبتنی بر رادیو نرم‌افزاری حملات سایبری انجام داد. گوشی‌های ماهواره‌ای[۱]، گوشی‌های سلولی[۲]، رادیوهای خطوط ترانک[۳] اکنون توسط سربازان در میدان نبرد[۴] مورد استفاده قرار می‌گیرند.

همچنین شایان ذکر است، اکنون کنترل و فرماندهی تاکتیکی[۵]، لجیستیک[۶]، شبکه‌های پاکسازی ترافیک[۷]، در حال انتقال به پروتکل IP مبتنی بر شبکه‌های موردی موبایل (MANET)[۸] به همراه لینک‌های رادیویی انتقال کوتاه بی‌سیم مبتنی بر پروتکل IP[۹] در زیرساخت هستند.

با فراگیر شدن تجهیزات اینترنتی (IoT) در میدان نبرد، بهره‌برداری از طیف الکترومغناطیس همچنین افزایش پیدا خواهد کرد. این مسئله موجب خواهد شد، دید سنتی که که اذعان می‌کرد حملات سایبری مرتبط با سطح راهبردی است، تغییر کند و اکنون حملات سایبری همچنین در سطح تاکتیکی و عملیاتی انجام شوند.

هم‌گرایی[۱۰]

همانطور که پیش از این بحث شد، گسترش فناوری‌های ارتباطی بی‌سیم عملیات‌های سایبری را به طیف الکترومغناطیس کشیده است که در گذشته به صورت سنتی فقط در آن جنگ الکترونیکی[۱۱] صورت می‌گرفت که اکنون خود پلتفرم‌های انجام جنگ الکترونیک از پلتفرم‌های الکترونیکی گسسته به پلتفرم‌های محاسباتی در حال مهاجرت هستند.

از همین روی، اکنون می‌توانیم حملات سایبری و جنگ الکترونیک را با یکدیگر درهم تنیده فرض کنیم، چون پتانسیل هم‌گرایی با یکدیگر را دارند. توانایی استفاده از جنگ سایبری و جنگ الکترونیکی می‌تواند

---

[1] Satellite Phones
[2] Cellular Phones
[3] Trunked Radio
[4] Battle Field
[5] Tactical Command and Control
[6] Logistics
[7] Traffic Clearance Networks
[8] Mobile Ad Hoc Networks
[9] Short Haul IP Radio Wireless Links
[10] Convergence
[11] Electronic Warfare

توانایی فرماندهان در دستیابی به نتایج دفاعی[1] و تهاجمی[2] از میدان نبرد بهبود ببخشد. به هر صورت، اکنون به نظر می‌رسد فعالیت‌های سایبری/ الکترومغناطیسی[3] باید به عنوان فعالیت‌های ذاتاً مشترک[4] درک شوند.

جنگ الکترونیکی و سایبری در جنگ‌های اخیر

جنگ اول خلیج فارس اهمیت اصلی جنگ الکترونیکی را در انجام جنگ هوایی مدرن نشان داد. در نتیجه حمله ابتدایی آمریکا به نیروی هوایی عراق، این نیرو به شکلی زمین گیر شد که تا پایان جنگ امکان بازیابی پیدا نکرد.

عملیات بیرون از جعبه[5] یا عملیات بوستان شاید احتمالا اولین نمایش از به کارگیری جنگ الکترونیک و جنگ سایبری بوده باشد. در این عملیات ارتش رژیم صهیونیستی، منطقه‌ای از دیرالزور سوریه را بمباران کرد که ادعا شده بود مرکز ساخت بمب هسته‌ای توسط سوریه بوده است و همچنین در نتیجه این حمله ۱۰ دانشمند هسته‌ای کره شمالی کشته شده‌اند.

شایان ذکر است، این حمله با تکیه بر توان جنگ الکترونیک و سایبری اسرائیلی‌ها صورت گرفته بود که در آن موفق شده بودند سامانه‌های پدافندی سوریه از قبیل Tor-M1 و S-200 و بسیاری دیگر از سامانه‌های پدافندی روسی را با موفقیت از کار بیندارند. در این حمله نیروی هوایی اسرائیل، یک آسمان تقلبی برای سامانه‌های دفاعی سوریه ترسیم کرده بودند تا رادارهای این سامانه‌ها متوجه تجاوز جنگنده‌های اسرائیلی به خاک سوریه نشوند.

همچنین در فیلم مستند Orchard Operation، ادعا شده است که روس‌ها کدهایی با محوریت غیرفعال‌سازی رادار سامانه‌های پدافندی ارائه شده به سوریه را به اسرائیلی‌ها فروخته بودند. از همین روی، اسرائیلی‌ها توانسته بودند با موفقیت ساختار راداری این سامانه‌ها را دور بزنند و از آن بگریزند . اگر این ادعا درست باشد، سامانه‌های پدافندی روسی امکان غیرفعال‌سازی از راه دور را باید داشته باشند که با دلایل امنیتی در این تجهیزات نهفته شدند.

---

[1] Defensive
[2] Offensive
[3] Cyber/Electro-Magnetic
[4] Inherently Joint Activities
[5] Operation Outside the Box/Orchard
[6] Bypass
[7] Evade

در نتیجه عدم عملکرد صحیح رادارها، جنگنده‌های اسرائیلی توانسته بودند با موفقیت هدف خود را در دیرالزور نابود کنند. فناوری استفاده شده توسط اسرائیلی‌ها گفته می‌شود توسط برنامه US Senior Sutter آمریکا پشتیبانی شده بود، اما به صورت گسترده حدس زده می‌شود که در این حمله اسرائیلی‌ها با استفاده از فناوری حافظه فرکانس رادیویی دیجیتال (DRFM)[1] استفاده کرده بودند تا اطلاعات غلط به رادار سامانه دفاعی روسیه بدهند.

در مثالی دیگر، منازه بین روسیه و اوکراین در سال ۲۰۱۴ تاثیر هم‌گرایی عملیات ابزارهای جنگ اطلاعاتی را به شکل دیگری نمایش داد. در این منازه، روس‌ها با استفاده از ابزارهای تهاجمی نرم‌افزاری (بدافزار Blackenergy) توانستند با انجام حملات سایبری بر علیه زیرساخت برق اوکراین، زیرساخت تولید برق این کشور را منهدم کنند.

اشتراکات بین جنگ سایبری و جنگ الکترونیک

انقلاب در فناوری اطلاعات و ارتباطات فقط از نظر نظامی اهمیت ندارد، بلکه ابزار راهبردی و سیاسی برای سیاست‌های امنیتی منطقه‌ای و جهانی آینده است اما به هر صورت برای اینکه تغییرات واقعی رخ بدهد، تنها به تغییرات لبه فناوری پاسخ نیاز نیست، بلکه در سطح فرهنگ، سازمان‌ها، راهبردها، تاکتیک‌ها، آموزش‌ها، تجهیزات و لجیستیک نظامی هم باید تغییرات و انتقال صورت گیرد تا تغییرات واقعی با محوریت به روزرسانی با شرایط جدید حاصل شود.

به عبارتی اکنون دیگر نمی‌توان انتظار داشت با تهیه چندین فناوری یا ابزار بتوان در سطوح مختلف نظامی، چه برای تهاجم و چه برای دفاع امکان بهره‌وری از تمامی پتانسیل این بعد به وجود آید. بلکه اکنون باید زیرساخت نظامی به شکل کامل با محوریت تطابق با آخرین تغییرات فناوری اطلاعات و ارتباطات به‌روزرسانی شود و تغییرات در تمام جنبه‌های آن صورت گیرد. اکنون بسیار از فعل‌های نظامی و امنیتی در بستر سایبر از قبیل جمع‌آوری اطلاعات[2]، تخریب تجهیزات فیزیکی[3]، انتشار اطلاعات غلط[4]، ایجاد تداخل در سرویس‌های

[1] Digital Radio Frequency Memory
[2] Information Gathering
[3] Physical Sabotage
[4] False Information Propagation

ارتباطی[1] و ... صورت می‌گیرد که تطابق با چنین شرایطی نیازمند بازبینی مجدد تمامی پروسه‌های عملیاتی و راهبردی و تاکتیکی و فرماندهی است.

جنگ اطلاعاتی[2] می‌تواند فرض شود که از تشکیل نیروی انسانی[3]، پروسه[4]، و فناوری تشکیل می‌شود. همچنین برای جنگ الکترونیک و جنگ روانی[5] هم این سه مولفه وجود دارند. همانطور که در تصویر ۱ نمایش داده شده است، این سه مولفه بین جنگ الکترونیک و جنگ سایبر شباهت‌های زیادی وجود دارد.

شکل ۱: مثلث نیروی انسانی، فناوری، پروسه.

- **نیروی انسانی:** مجموعه افرادی که عملیات‌های جنگ الکترونیک را طراحی و اجرایی می‌کنند، متخصصان فناوری اطلاعات و ارتباطات هستند. بدون دانش پایه فناوری اطلاعات و ارتباطات، انجام عملیات در این دامنه‌ها غیرممکن است. مخصوصا با گسترش مباحث مرتبط با جنگ سایبری و الکترونیکی، اکنون تربیت متخصص در این حوزه، و همچنین به‌روزرسانی دانش آن‌ها به آخرین

[1] Communication Denial of Service
[2] Information Warfare
[3] People
[4] Process
[5] Psychological Warfare

مکانیزم‌های دفاعی / تهاجمی و همچنین آخرین تغییرات حوزه فناوری یکی از چالش‌های بسیار مهم است که نیاز به نقش‌راه و همچنین برنامه کامل با این محوریت است.

از آنجایی که بسیاری از شاخه‌های جنگ سایبری مانند مهندسی معکوس، کشف آسیب‌پذیری[x]، توسعه اکسپلویت[xi]، توسعه بدافزار[xii]، تحلیل بدافزار[۱]، رمزنگاری[۲]، رمزگشایی[۳] و ... با یکدیگر در هم تنیده هستند و متاسفانه مبتنی بر پلتفرم از قبیل وب، دسکتاپ، موبایل، تجهیزات کنترلی و نهفته دامنه تخصص‌ها، رویکردها، متدها، تکنیک‌ها بسیار متغییر هستند، اگر نیروهای متخصص جنگ سایبری به شکل بالینی این علوم را فرا نگیرند، و همچنین در قالب کارگروه‌هایی تخصصی امکان همکاری با هم را نداشته باشند، غیرممکن است که بتوانند در طراحی و عملیات با محوریت جنگ سایبری با توجه به پیچیدگی‌هایی که اکنون وجود دارد، موثر عمل کنند.

- **پروسه:** همانطور که تا به الان باید درک کرده باشید، یک ارتباط یک به یک بین عملیات‌های حوزه جنگ سایبری و جنگ الکترونیکی وجود دارند. به عبارت دیگر، بسیاری از عملیات‌هایی که در گذشته فقط با انجام جنگ الکترونیک روی طیف الکترومغناطیس صورت می‌گرفت، اکنون انجام همان کارها در جنگ سایبری هم ممکن است و حتی در برخی شرایط بسیار ساده‌تر هم شده است. در جدول زیر این مسئله به صورت یک به یک آورده شده است تا مشخص شود که بین جنگ الکترونیک و جنگ سایبر یک همگرایی واضحی وجود دارد. در برخی شرایط، از هر دو می‌توان برای رسیدن به حداکثر بهره‌وری استفاده نمود.

جدول ۱: مقایسه جنگ الکترونیک و جنگ سایبری در عملیات‌های نظامی

نوع عملیات رزمی - تاکتیکی	شیوه انجام در جنگ الکترونیک	شیوه انجام در جنگ سایبری
یکی از عملیات‌های مهم در مباحث نظامی و امنیتی، جمع‌آوری اطلاعات از دشمن است. هر چه میزان اطلاعات ما بیشتر از دشمن باشد، توان تحلیل ما بالاتر خواهد	**پشتیبانی الکترونیکی**[۵] – در مبحث پشتیبانی الکترونیکی، ارتباطات دشمن در طیف الکترومغناطیس شنود می‌شود تا توانایی و همچنین فرامین الکترونیکی جنگ[۶] مشخص شوند. به شکل ویژه، ابزارهای جمع‌آوری اطلاعات الکترونیکی (ابزار شنود) در این قسمت	**اکسپلویت شبکه کامپیوتر**[۷] – مهاجم با اکسپلویت یک آسیب‌پذیری روز-صفر می‌تواند به یک کامپیوتر رخنه کند و سپس یک بدافزار از خانواده جاسوس‌افزارها در آن کامپیوتر نصب کند تا آن بدافزار از دشمن اطلاعات جمع‌آوری کرده و برای مهاجم ارسال کند. جاسوس‌افزارها[xiii]،

[1] Malware Analysis
[2] Encryption
[3] Decryption
[5] Electronic Support
[6] Electronic Order of Battle
[7] Computer Network Exploitation

رفت و در نتیجه بهتر می‌توانیم تصمیم‌گیری کنیم. از همین روی، جمع‌آوری اطلاعات و در نمونه پیشرفته‌تر جمع‌آوری اینتلیجنس[۱] اهمیت زیادی دارد که در جنگ الکترونیک و جنگ سایبر امکان انجام آن اکنون وجود دارد.	مورد استفاده قرار می‌گیرند. در جنگ الکترونیکی، جمع‌آوری اطلاعات کاملا راه‌حل‌های سخت‌افزاری دارند تا این امکان به وجود بیاد که ارتباطی بر روی یک فرکانس را شنود کرد.	روتکیت‌ها[xiv] و بوتکیت‌ها[xv] اصلی‌ترین ابزارها برای انجام وظایف گوناگون از قبیل جمع‌آوری اطلاعات و ماندگاری بر روی ماشین هدف به منظور جاسوسی بلندمدت هستند. برخلاف جمع‌آوری اطلاعات در جنگ الکترونیکی، جمع‌آوری اطلاعات در جنگ سایبری، کاملا رویکرد نرم‌افزار محور دارد.
ایجاد تداخل در توانایی عملیاتی دشمن برای مباحث تهاجمی اهمیت بسیار زیادی دارد. به عنوان مثال، اگر مهاجم بتواند فقط در ارتباطات میدان نبرد با مرکز فرماندهی دشمن تداخل ایجاد کند، در نتیجه خواهد توانست ضربه سنگینی به آن‌ها وارد کند. یا اگر مهاجم بتواند در نحوه عملکرد سامانه‌های شناسایی مانند رادارها تداخل ایجاد کند که این سامانه‌ها نتوانند وظایف خود را با محوریت شناسایی اشیاء پرنده به خوبی انجام بدهند، در نتیجه موجب خواهد شد مهاجم بتواند بدون اینکه شناسایی شود، دشمن خود را مورد آماج قرار بدهد بدون اینکه آن امکان دفاع از خود را داشته باشد.	**حمله الکترونیکی[۵] –** به منظور ایجاد تداخل در ارتباطات الکترونیکی، می‌توان از مبحث جمینگ یا فریب بهره برد. ابزارهای جنگ الکترونیکی که عمل جمینگ را انجام می‌دهند، کاربردهای فراوانی دارند. از این ابزارها می‌توان برای ایجاد تداخل بر روی فرکانس طیف الکترومغناطیس استفاده کرد تا در ارتباطات دشمن تداخل شکل گیرد. مثلا می‌توان با جمینگ در باند فرکانسی یک ماهواره نظامی، ارتباطات بین آن و شبکه نبرد را مختل کرد یا به صورت کامل از بین برد. در برخی شرایط همچنین می‌توان با انجام حملات جمینگ پهپادهای شناسایی یا تهاجمی را از کار انداخت، چون این پهپادها زمانی که ارتباط خود را با مرکز کنترل خود از دست بدهند، یا سقوط خواهند کرد، یا به یک مختصات مشخصی باز خواهند گشت که در دو حالت عملکرد یا انجام وظیفه آن‌ها مختل می‌شود.	**حمله شبکه کامپیوتری[۶] –** به منظور ایجاد تداخل در توانایی دشمن در فضای سایبر می‌توان از آسیب‌پذیری‌های نرم‌افزاری برای ایجاد وضعیت منع سرویس‌دهی در یک نرم‌افزار – سرویس (مانند نرم‌افزارهای نظارتی – راداری) استفاده کرد. منع سرویس‌دهی موجب خواهد شد که آن نرم‌افزار یا آن سرویس که عمل مشخصی را انجام می‌دهد، دیگر نتواند کار کند. البته تجهیزات کامپیوتری طیف متنوعی از آسیب‌پذیری‌ها را دارند که می‌توان از هر کدام برای پیاده‌سازی یک بردار حمله مشخصی بهره برد. برای مثال، با استفاده از آسیب‌پذیری در پروتکل‌ها می‌توان در ارتباطات تحت شبکه تداخل ایجاد کرد یا با استفاده از بدافزارهای پیشرفته تجهیزات فیزیکی–نظامی مانند کنترلرهای موشک‌ها و ... را تخریب کرد. این موارد، نمونه رویکردهایی هستند که در جنگ سایبری می‌توان برای ایجاد تداخل در توانایی‌های دشمن مورد استفاده قرار داد.

[۱] در زبان فارسی، برای کلمه Intelligence، معنی صحیحی در نظر گرفته نشده است. بلکه به واژه Information و Intelligence تنها معنی اطلاعات را نسبت داده‌اند که این دو واژه از منظر ترمینولوژی با یکدیگر تفاوت معنا دارند و نمی‌توان به هر دو معنی اطلاعات را داد. از همین روی، در این متن، از واژه معادل خود اینتلیجنس استفاده شده است که به اطلاعات طبقه‌بندی و پردازش شده اشاره دارد.

[5] Electronic Attack

[6] Computer Network Attack

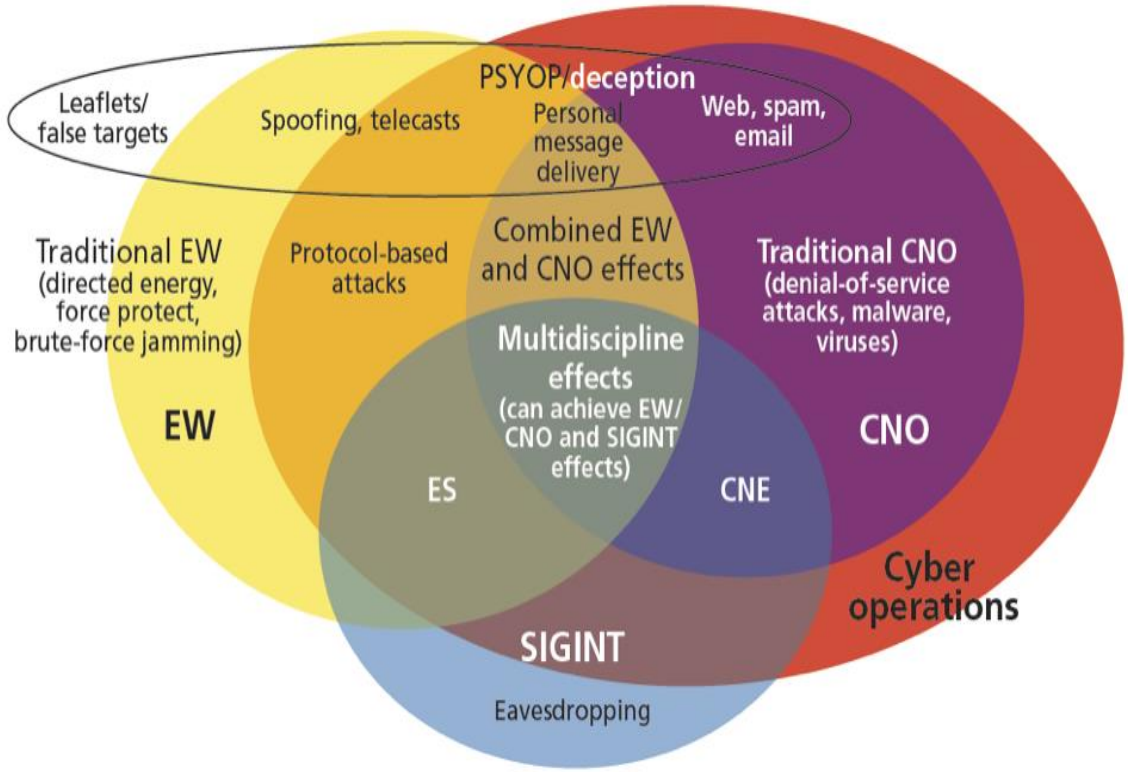
دفاع از توانایی‌های در مقابل تداخلات و تهاجمات وظیفه مهم دیگر از منظر نظامی و امنیتی است. علاوه بر توانایی تهاجم، در یک ساختار نظامی – امنیتی باید توانایی محافظت یا دفاع از خود در مقابل دشمن در تمامی بُعدهای شناخته شده هم وجود داشته باشد.	**محافظت الکترونیکی[1] –** در مبحث محافظت الکترونیکی، تلاش خواهد شد تا از ایجاد تداخل و همچنین انجام حملات جنگ الکترونیکی مانند جمینگ در ارتباط بین تجهیزات با یکدیگر، ارتباط بین واحدها با مرکز فرماندهی، ارتباط بین سامانه ناوبری ماهواره ای با تجهیزات زمینی و ... دفاع شود تا یکپارچگی ارتباطات تحت هیچ شرایطی از بین نرود. برای دفاع از خود در مقابل حملات جنگ الکترونیکی، رویکردهای بسیاری وجود دارد که می‌توان با استفاده از آن‌ها سامانه‌ها را در مقابل حملاتی مانند جمینگ، جی‌پی‌اس اسپوفینگ و ... محافظت کرد.	**دفاع شبکه کامپیوتری[2] –** استفاده از راه‌حل‌های نرم‌افزاری و سخت‌افزاری دفاعی مانند فایروال‌های هوشمند، ضدویروس‌ها، سامانه‌های تشخیص و پیشگیری از نفوذ، سندباکس‌ها و ... می‌توانند سامانه‌های کامپیوتری را در مقابل بسیاری از تهدیدات محافظت کنند اما اگر مهاجم از اکسپلویت‌های روز–صفر استفاده کنند، تقریبا شانس دفاع در مقابل آن حملات صفر است چون هیچ راهی وجود ندارد که جلوی آن اکسپلویت‌ها گرفته شود. ولی به هر صورت، با استفاده از راه‌حل‌های مبتنی بر هوش مصنوعی و یادگیری ماشین اکنون می‌توان تا سطح خیلی خوبی، تهدیدات بالقوه و بالفعل را شناسایی کرد.
ایجاد شرایطی که موجب شود سامانه‌ها و همچنین افراد اشتباه تصمیم‌گیری کنند، یکی دیگر از انواع عملیات‌های مهم نظامی و امنیتی است.	ایجاد یک طعمه که نشان دهنده اهداف واقعی هستند و دشمن را فریب می‌دهند. به عنوان مثال، در جنگ الکترونیک می‌توان با ارائه سیگنال‌های تقلبی GPS، مختصات ارائه شده توسط ماهواره‌های جهانی ناوبری را جعل کرد. در نتیجه جعل این مختصات، سامانه های که عمل مسیریابی را با کمک این نوع سیگنال ها انجام خواهند داد، دچار مشکل و فریب خواهند شد.	در مبحث جنگ سایبر، انتشار اطلاعات غلط یا انجام کارهایی که موجب تصمیم‌گیری اشتباه شود می‌تواند به شکل‌های گوناگون صورت گیرد. یکی از مهم‌ترین رویکردها استفاده از پتانسیل شبکه‌های اجتماعی برای ایجاد موجی از اخبار غلط و انتشار اطلاعات نادرست با محوریت جنگ روانی است. یا با انجام حملات مبتنی بر شبکه از قبیل جی‌پی‌اس اسپوفینگ [xvi] می‌توان اطلاعات غلط ناوبری ارائه کرد تا یک شی پرنده در مسیریابی خود دچار مشکل شود مانند حمله بر علیه پهپاد RQ170 که با جعل مختصات پهپاد به جای اینکه به پایگاه خود باز گردد، در نقطه دیگری فرود آمد. همچنین می‌توان بدافزارهایی طراحی کرد که این بدافزارها بتوانند در شبکه دشمن عملیات خرابکارانه با همین نوع محوریت انجام بدهند.

- **فناوری:** عملیات‌های فضای سایبر و جنگ الکترونیک اکنون مکمل یکدیگر هستند و همچنین هم‌افزایی بالقوه‌ای با یکدیگر دارند. به عبارتی، اکنون دیگر نمی‌توانیم بین جنگ الکترونیک و جنگ سایبر تفاوت و

[1] Electronic Protection
[2] Computer Network Defense

تمایز قائل شویم، یا شرایط استفاده از آن‌ها را مجزا از یکدیگر بدانیم. در شرایط فعلی، مخصوصا با ورود و گسترش اشیاء اینترنتی (IoT) که دارای ماهیت نرم‌افزاری و سخت‌افزاری هستند، و همچنین با استفاده از یک لینک وایرلس رادیویی با یکدیگر شبکه می‌شوند، جنگ الکترونیک و جنگ سایبر در کنار هم دیگر می‌توانند برای هدف قرار دادن این نوع تجهیزات مورد استفاده قرار بگیرند.

به هر صورت، با گسترش شبکه‌های وایرلس، محاسبات دیجیتال، و مخابرات به همراه یکپارچه‌سازی کامپیوترها با تجهیزات مخابرات فرکانس رادیویی موجب شده است که مرز بین عملیات‌های شبکه سایبری[1] و جنگ الکترونیک به شکل قابل توجه‌ای کم رنگ شود. اکنون این واقعیت وجود دارد که هر چقدر بیشتر عملیات‌های سایبری با عملیات‌های جنگ الکترونیکی یکپارچه شوند، جمع‌آوری اطلاعات سری، دستکاری و انتشار اطلاعات ساده‌تر خواهد شد.



شکل ۲: نمایش کاربردی محیط‌های همگرا

[1] Cyber Network Operations -CNO

اکنون، وابستگی کامپیوترها به طیف الکترومغناطیس به عنوان یک بستر جهت انتقال اطلاعات بین کامپیوترها موجب شده است این احتمال به وجود آید که از طیف الکترومغناطیس بتوان برای نفوذ الکترونیکی به کامپیوترها بهره‌برداری کرد. از همین روی، حساب بر روی جنبه های جنگ الکترونیک در هنگام اکسپلویت شبکه کامپیوتری (CNE)، حمله شبکه کامپیوتری (CNA)، و دفاع از شبکه کامپیوتری (CND) حیاتی است. محافظت الکترونیکی (EP) مانند دفاع از شبکه کامپیوتری (CND) اهمیت دارد چون شبکه کامپیوتری دوست باید در مقابل حملات الکترونیکی و حملات شبکه کامپیوتری مورد محافظت قرار بگیرد.

شایان ذکر است، پلتفرم‌های تسلیحات جنگ الکترونیک دیگر سامانه‌های الکترونیکی گسسته نیستند. این پلتفرم‌ها اکنون بر روی پلتفرم‌های کامپیوتری توسعه داده می‌شوند، یک رادیو نرم‌افزاری یا جمرهای مبتنی بر میکروکنترلر و سامانه‌های DF هستند. علاوه بر همه این‌ها، خطی که جنگ الکترونیک (که سامانه‌های مخابراتی دشمن را از طریق طیف الکترومغناطیس هدف قرار می داد) با جنگ سایبری (که شبکه‌های کامپیوتری دشمن را هدف قرار میداد) اکنون در حال کم رنگ شدن است.

رویکرد کشورهای مختلف با محوریت تحولات بعُد پنجم

به هر صورت، بدون شک جنگ‌های آینده تکیه بر فناوری خواهند داشت. از همین روی، کشورهای گوناگون تلاش می‌کنند تا با ارائه راهنماهای جامعه پیش‌بینی کنند که با چه چیزی رو به رو هستند و چطور باید در این محیط‌های جدید راهبردهای دفاعی و تهاجمی خود را پیاده‌سازی و عملیاتی کنند.

در جدول زیر، به تفکیک کشورهای قدرتمند جهان، این مسئله مورد بررسی قرار گرفته است که چطور کشورها اقدام به تطابق ساختار نظامی خود با تغییرات وسیع سطح فناوری و الکترونیکی کرده‌اند و اینکه این فضا را چطور برای خود ترسیم می‌کنند.

جدول ۲: آخرین تغییرات و اصلاحات کشورها با محوریت فضای سایبر

کشور	توضیحات
آمریکا	ارتش و نیروی دریایی آمریکا پیشرو در مسئله جنگ الکترونیک و جنگ سایبر و همچنین هم‌افزایی این دو با یکدیگر بوده‌اند و پیش از هر کشور دیگری فضای سایبر و طیف الکترومغناطیس را به عنوان یک نیازمندی برای اصلاح در نظر گرفتند. همچنین این مسئله برای آن‌ها روشن بوده است که با تدوین

نقشه‌راه و برآوردهایی به صورت سازماندهی شده به سمت یک دکترین جدید برای این بعُد حرکت کنند که بتوانند از پتانسیل آن نهایت استفاده را ببرند.

ارتش آمریکا در این راستا با تدوین سند "توانایی‌های رقابتی الکترومغناطیسی و سایبری ارتش[۱]" و نیروی دریایی با تدوین سند "نقشه راه سلطه اطلاعاتی دریایی آمریکا ۲۰۱۳-۲۰۲۸[۲]" به مسائل مطرح با محوریت تغییرات فضای سایبر و الکترونیکی پرداخته است. این اسناد آینده‌ای را ترسیم می‌کنند که محیط اطلاعاتی متکی به هم افزایی طیف الکترومغناطیس و سایبری است.

در همین راستا، آمریکا واحد جنگ الکترونیک خود را منحل کرد و آن را درون یک ساختار جدید با عنوان مرکز فرماندهی سایبری در پنتاگون[۳] گنجاند. تحت برنامه جنگ الکترونیک و سایبری پکپارچه[۴]، پژوهش‌های الکترونیکی و مخابراتی، مرکز مهندسی و توسعه در حال کار برای شناسایی راه هایی به منظور ترکیب توانایی های جنگ الکترونیکی با تاکتیک های جنگ سایبری هستند.

شایان ذکر است، در سال ۲۰۱۷ آمریکا یک راهنمایی انتشار داد که با عنوان FM 3-12 شناخته می‌شود. این راهنمای فیلد دارای عنوان عملیات‌های جنگ الکترونیکی و سایبری است. در این راهنما آورده شده است که در تمامی سطوح جنگ و نبرد نیاز است که عملیات‌های الکترومغناطیسی/سایبری[۵] صورت گیرند [xvi i].

همچنین در این سند آمده است: در آینده هنگامی که قابلیت‌های دشمن‌های ما رشد پیدا کنند، توانایی ما در تسلطیابی بر روی فضای سایبر و طیف الکترومغناطیس پیچیده‌تر و برای پیروزی در عملیات‌ها حیاتی‌تر خواهد شد. گنجاندن فعالیت‌های الکترومغناطیس و فضای سایبری در تمامی فازهای یک عملیات اکنون کلید به دست آوردن و نگهداری قدرت و برتری است و همچنین از دستیابی دشمن‌های خود به همچین قابلیتی باید جلوگیری کرد.

[1] Army Cyber-Electromagnetic Contest Capabilities Based Assessment
[2] U.S. Navy Information Dominance Roadmap 2013-2028
[3] Cyber Command at Pentagon
[4] Integrated Cyber and Electronic Warfare
[5] Cyber Electro Magnetic Activities

در راهنمای تدوین شده توسط نیروی دریایی آمریکا مفهومی در نظر گرفته شده است که با عنوان مانور جنگی الکترومغناطیسی[1] شناخته می‌شود. این مفهوم به یک‌پارچه‌سازی عملیات‌های الکتروسایبر، جمینگ، اسپوفینگ، دستکاری صحیح سیگنال‌ها به منظور کور کردن اهداف و همچنین بهم ریختن یکپارچگی دشمن اشاره دارد.

نیروی هوایی آمریکا در فوریه ۲۰۱۴ همچنین مطالعه‌ای انجام داد که در آن ذکر شده بود [xviii]: چیزی که نیروی هوایی آمریکا تاکنون به خوبی انجام نداده است، تراز کردن تلاش‌های خود با محوریت عملیات‌های سایبری به همراه جنگ الکترونیکی و عملیات‌های طیف الکترومغناطیسی است تا به شکل کاملی از فضای سایبر و طیف الکترومغناطیس بتوان با محوریت اهداف خود بهره‌برداری کند. شایان ذکر است، برخلاف نیروی هوایی، ارتش و نیروی دریایی آمریکا، پیش از این نیازمندی به طیف الکترومغناطیس–فضای سایبر را با رسمیت شناخته بودن تا عملیات‌ها و راهبردها و تاکتیک‌های خود را با الکترومغناطیس و فضای سایبر تراز کنند.

به هر صورت، اکنون آژانس امنیت ملی (NSA) آمریکا نقش کلیدی در نظارت جهانی دارد. این آژانس علاوه بر توسعه نرم‌افزارهای کاربردی با محوریت مسائل امنیتی، کشف و شناسایی آسیب‌پذیری‌های نرم‌افزاری از قبیل نرم‌افزاری Ghidra[xix]، در مبحث توسعه بدافزارهای مانند استاکس‌نت، پروژه Valut7 و ... فعالیت گسترده‌ای دارد[xx]. به هر صورت، Vault7 آخرین افشاسازی مشهور ویکی‌لیکس محسوب می‌شود. این افشاسازی حاوی اسنادی بود که تسلیحات سایبری CIA را تشریح می‌کرد. با اینکه هیچ‌گاه کدمنبعی منتشر نشد، این افشاسازی افراد را از قابلیت‌ها فنی CIA نظیر هک آیفون‌ها، تمامی سیستم‌های عامل پرمصرف، پرکاربردترین مرورگرها و حتی تلویزیون‌های هوشمند آگاه ساخت.

شایان ذکر است، بین اوت ۲۰۱۶ تا آوریل ۲۰۱۷، گروهی از هکرها که خود را شدو بروکرز[2] می‌نامیدند، برخی از ابزارهای هک توسعه داده‌شده Equation

[1] Electromagnetic Manoeuvre Warfare
[2] The Shadow Brokers

	Group یا NSA را منتشر کردند. این ابزارها که همگی کیفیت و عملکردی فوق‌العاده داشتند، تأثیری سریع گذاشتند. تنها یک ماه پس از آخرین افشاگری این گروه، یکی از این ابزارها، یعنی نوعی آسیب‌پذیری برای پروتکل SMB مایکروسافت که با نام EternalBlue شناخته می‌شود، به موتور اصلی باج‌افزار Wannacry تبدیل شد. ناگفته نماند هویت افراد این گروه تا امروز ناشناخته مانده است.
چین	چینی‌ها یک راهبرد جنگ اطلاعاتی رسمی[1] با عنوان شبکه جنگ الکترونیک یک‌پارچه[2] را ترسیم کرده اند که در آن ماموریت‌های تهاجمی حملات شبکه کامپیوتری و جنگ الکترونیک، زیرنظر واحد اقدامات متقابل الکترونیکی[3]، ستاد کل ارتش جمهوری خلق چین در نظر گرفته شده است. تئوریسین‌های جمهوری خلق چین اصطلاح شبکه جنگ الکترونیک یکپارچه را ابداع کرده‌اند که نشان‌دهنده یکپارچگی استفاده از جنگ الکترونیک (EW)، عملیات شبکه کامپیوتری (CNO)، ضربات محدود نظامی[4] است. در این رویکرد، با استفاده یک پارچه از جنگ الکترونیک و حملات سایبری و همچنین حملات نظامی تلاش خواهد شد مراکز کنترل و فرماندهی کلیدی، گره‌های ارتباطی و کامپیوترهای در زیرساخت شبکه نظامی دشمن تخریب شود. جمهوری خلق چین جنگ سایبری را به عنوان اولین گزینه به منظور جلوگیری از انجام عملیات‌های نظامی مرسوم[5]، و نه یک نیروی تقویتی[6] برای انجام حملات نظامی [xxi] می‌داند. شایان ذکر است، چین یک نیروی جدید با عنوان نیروی پشتیبانی راهبردی[7] در سال ۲۰۱۵ ایجاد کرده است که هسته راهبردی جنگ اطلاعاتی چین را شکل می‌دهد و احتمالا مباحث مربوط به شناسایی[8]،

[1] Formal
[2] Integrated Network Electronic Warfare
[3] Electronic Countermeasures
[4] Limited Kinetic Strikes
[5] Conventional Military Operations
[6] Multiplier Force
[7] Strategic Support Force
[8] Reconnaissance

	هشدار سریع[1]، سایبری، ارتباطات[2]، فرمان، کنترل، جهت‌یابی[3]، اقیانوس دیجیتالی، سرزمین دیجیتالی، و ... را با یکدیگر یکپارچه‌سازی می‌کند و پشتیبانی قوی برای عملیات‌های مشترک برای تمامی شاخه‌های نظامی ارائه خواهد کرد. علاوه بر این، در حالیکه در برخی کشورها بخش فضایی به عنوان یک شاخه مجزای نظامی شناخته می‌شود، اما جمهوری خلق چین آن را به عنوان بخشی از نیروی پشتیبانی راهبردی (SSF) در نظر گرفته است [xxiii xxii]. به صورت کلی، نیروی پشتیبانی راهبردی (SSF) چین را می‌توان مهم‌ترین شاخه نظامی این کشور دانست که وظایف آن با محوریت جنگ الکترونیک، جنگ سایبری و جنگ فضایی شکل گرفته است. به هر صورت، بخش اعظمی از اصلاحات در ارتش چین، به تأسیس نیروی پشتیبانی راهبردی این کشور، در سال ۲۰۱۵، مربوط می‌شود. این نهاد، به‌عنوان یک سازمان نوپدید بعد از اصلاحات وسیع ساختار ارتش چین، وظیفه درهم‌آمیختن توان فضایی، سایبری و جنگ الکترونیک را با قدرت نظامی متعارف این دولت برعهده دارد[xxiv]. به عنوان مثال، بعد از شکل‌گیری این نهاد در ارتش چین، نیروی پشتیبانی راهبردی توانست با موفقیت ایالات متحده را هدف حملات سایبری قرار بدهد و چندین ترابایت از اطلاعات محرمانه مربوط به هواپیما V-22 Osprey، جنگنده F35 Lightning و F22 Raptor[xxv] را سرقت کند تا در ادامه بتواند از آن اطلاعات در طراحی جنگنده خود به عنوان J20 و همچنین هواپیما و بالگردهای خود بهره ببرد. [xxvi] این یکی از کاربردهای استفاده از فضای سایبر با محوریت جمع‌آوری اطلاعات محرمانه و حیاتی است.
روسیه	با توجه به توضیحات ژنرال استفان فاگرتی، فرمانده مرکز عالی سایبر آمریکا [xxvii]: فعالیت‌های روسیه در اوکراین، یک مورد مطالعاتی جدی با محوریت انجام فعالیت‌های الکترومغناطیسی–سایبری در میدان نبرد است.

[1] Early Warnings
[2] Communication
[3] Navigation

فقط سایبر نیست، فقط جنگ الکترونیک نیست، بلکه روسیه به شکل قابل توجه‌ای از جنگ الکترونیک و جنگ سایبر به صورت یکپارچه برای تهاجم به اوکراین بهره‌برده بوده است.

به عنوان مثال، هنگامیکه روس‌ها به اوکراین حمله کردند، آن‌ها توانستند با استفاده از حملات سایبری و همچنین جنگ الکترونیک به صورت کامل تمامی سامانه‌های نظامی اوکراین را از کار بیندازند. از همین روی سربازان اوکراینی مجبور بودند از تلفن همراه برای برقراری ارتباط با یکدیگر یا مرکز فرماندهی بهره ببرند. همین مسئله موجب شده بود، به سادگی روس‌ها با استفاده از سیگنالی‌های ارسالی تلفن همراه این سربازان، محل آن‌ها را شناسایی کنند و آن‌ها را با حملات موشکی از بین ببرند.

به هر صورت، حمله‌ی سایبری به شبکه‌ی برق اوکراین در دسامبر ۲۰۱۵ موجب خاموشی گسترده در بخش غربی اوکراین شد. این حمله اولین حمله‌ی موفق سایبری به شبکه‌ی کنترل برق محسوب می‌شود. در این حمله از بدافزاری به‌نام Black Energy استفاده شد و دسامبر ۲۰۱۶ نیز، حمله‌ای مشابه شکل گرفت. در حمله‌ی دوم از بدافزاری به‌مراتب پیچیده‌تر موسوم به Industroyer استفاده و برق یک‌پنجم پایتخت اوکراین با موفقیت قطع شد.

اگرچه استاکس‌نت و شمعون نخستین حملات سایبری علیه اهداف صنعتی بودند، دو حمله به شبکه‌ی برق اوکراین نخستین حملاتی از این دست بودند که توجه مردم را به خود معطوف و افراد را از خطر واقعی حملات سایبری به زیرساخت‌های اساسی کشور آگاه کردند. این دو حمله، تنها شروع سلسله‌ای طولانی از هک‌های هکرهای روسی علیه اوکراین پس از تهاجم این کشور علیه کریمه در سال ۲۰۱۴ بود. از سایر این هک‌ها می‌توان به باج‌افزارهای NotPetya و Bad Rabbit در سال ۲۰۱۷ اشاره کرد. از گروه پشت این حملات با نام سندورم (Sandworm) یاد می‌شود و احتمال می‌رود بخشی از ارتش سایبری روسیه باشد. کتاب Sandworm نوشته‌ی اندی گرین‌برگ، فعالیت‌های امنیتی این گروه را در جزئیاتی بیشتر شرح داده است.

	به هر صورت، استفاده روس‌ها به صورت یکپارچه از حملات سایبری، جنگ الکترونیک، پهپادها، و مواد منفجره قدیمی جنگ‌های آینده پیش روی ما را به تصویر می‌کشد. وزیر دفاع وقت روسیه، سرگی شویگو، همچنین سال ۲۰۱۶ در پارلمان این کشور ابراز کرد: روسیه قصد دارد یک شاخه جدید با محوریت تمرکز بر روی جنگ اطلاعاتی ایجاد کند [xxviii].
هند	کشور هند، با انتشار مستند "دکترین جنگ اطلاعاتی برای ارتش هند[۱]" توسط سرفرماندهی مرکز آموزش ارتش (ARTAC) و "دکترین مشترک برای جنگ الکترونیکی[۲]" توسط وزارت دفاع در مورد مباحث مطرح و همچنین دکترین جنگ اطلاعاتی و الکترونیکی بحث کرده‌اند. در این مستندات، برخلاف آمریکا، بین جنگ الکترونیک و جنگ سایبری هم‌گرایی در نظر گرفته نشده است و آن دو را مجزا از یکدیگر می‌دانند.
استرالیا	واحد جنگ الکترونیک و سایبر[۳] استرالیا، عهده‌دار پژوهش و توسعه مبتنی بر شناسایی، تحلیل، و مقابله با تهدیدات دفاعی استرالیا و همچنین امنیت ملی این کشور از طریق محیط الکترونیکی شده است. این بخش از ارتش استرالیا، وظیفه یکپارچه‌سازی توانایی‌های علمی و فناوری با محوریت فضای سایبر، جنگ الکترونیک، پردازش سیگنال، و ارتباطات به منظور پوشش فضای سایبر و طیف الکترومغناطیس را بر عهده دارد. واحد جنگ الکترونیک و سایبر (CEWD) ارتش استرالیا در مستند طرح راهبردی ۲۰۱۶ تا ۲۰۲۱ خود آورده است[xxix]: فضای سایبر از منظر پیچیدگی و پویایی به سرعت در حال رشد است. این مورد به دلیل خواست روز افزون قابل حمل بودن تجهیزات[۴]، انفجار در تعداد تجهیزات متصل به شبکه، رمزنگاری گسترده[۵]، افزایش حجم داده‌ها، و استفاده گسترده از سیستم‌های رادیو نرم‌افزاری است. این ترندهای فناوری چالش‌های پژوهشی قابل توجه‌ای

[1] Information Warfare Doctrine for the Indian Army 2010
[2] Joint Doctorine for Electronic Warfare 2010
[3] Cyber and EW Division
[4] Mobility
[5] ubiquitous encryption

	با محوریت نگهداری، توسعه توانایی‌های سایبری و الکترونیکی با محوریت دسترسی، تحلیل، بهره‌برداری و دفاع ایجاد کرده‌اند. به هر صورت، شبکه‌های مخابراتی بی‌سیم در سایبر مرکز تمامی این مشکلات هستند. شایان ذکر است، در مستند طرح راهبردی واحد جنگ الکترونیک و سایبر برای سال ۲۰۱۶ تا ۲۰۲۱ به صورت مستقیم تحت سرفصل سنجش و شکل‌دهی سایبر[1] اشاره شده است که ارتباطات شبکه بی‌سیم و کشف آسیب‌پذیری (به منظور توسعه کدهای روز–صفرم) اصلی‌ترین مباحث برای سرمایه‌گذاری عنوان شده است.
رژیم صهیونیستی (اسرائیل)	دیگر کشور از قبیل کشورهای آسیایی به جزء اسرائیل به دست آورد جدی در این زمینه نرسیده اند. البته در مورد توانایی‌ها، دکترین، راهبرد، نقشه‌راه، اسرائیل در زمینه جنگ الکترونیک و جنگ سایبری اطلاعات کافی در دسترس نیست با اینکه این کشور در زمینه فناوری‌های نوین جنگ الکترونیکی نسبت به دیگر کشورهای جهان پیشگام است. در سال ۲۰۱۵، این کشور اعلام کرد یک مرکز فرماندهی سایبری واحد[2] ایجاد خواهد کرد[xxx] تا تمامی فعالیت‌های سایبری و الکترونیکی این کشور تحت یک سازمان مجزا و واحد قرار گیرد، ولی در سال ۲۰۱۷ این طرح را بعد دو سال تحلیل و بررسی کنار گذاشتند[xxxi]. البته هنوز دلایل آن مشخص نیست که چرا اسرائیل ایجاد این مرکز فرماندهی سایبری را کنار گذاشت، و به ادامه فعالیت‌های سایبری واحد ۸۲۰۰ تحت نظارت سازمان جاسوسی نظامی (امان) اسرائیل رضایت دادند. واحد ۸۲۰۰ اسرائیل یکی از قدرتمندترین واحدهای سایبری جهان است [xxxi i] که امکان جاسوسی وسیع حتی از ارتباطات تحت Skype را هم دارد که یکی از ایمن‌ترین نرم‌افزارها برای ارتباطات صوتی و تصویری بر روی پلتفرم کامپیوتر است. به عنوان مثال، پیش از این، در تحلیل برنامه Skype به مشکلات این نرم‌افزار از منظر امنیتی اشاره شده است [xxxi i i] که مثلا این برنامه دارای حدود ۷۰۰ تابع Checksum است که هر کدام صحت یه

[1] Cyber Sensing and Shaping chapter
[2] Unified Cyber Command

	قسمتی از کد یا داده رو بررسی می‌کنند و همچنین نحوه عملکرد کلی آن به چه شکل است. در ادامه این تحقیق هم اشاراتی به موضوعاتی در خصوص مباحث امنیتی در سطح شبکه این برنامه‌ها شده است، مثلا نحوه عملکرد برنامه‌هایی مثل Signal و Wickr، و به صورت ضعیف هم البته Telegram به چه شکل است. اگرچه این تحلیل برای Skype نسخه ۵ است، ولی این مسئله را نشان می‌دهد که به دلیل ماهیت آسیب‌پذیر این نرم‌افزارها، واحدهای جاسوسی توانایی این را دارند که حتی ارتباطات مبتنی بر آن‌ها را در بستر سامانه‌های کامپیوتری شنود و نظارت کنند. به عنوان نمونه در یکی از اسناد WikiLeaks اشاره شده است[xxxiv] که بر روی یک ارائه‌دهنده سرویس اینترنت آلمانی این عمل شنود ترافیک Skype انجام شده است. این نشان می‌دهد بر خلاف تصور، با بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری، ارتباطات صوتی و تصویری بر روی پلتفرم‌های کامپیوتری هم قابل شنود و رهگیری است. همچنین مبتنی بر گزارش واشنگتن‌پست، اسرائیل نرم‌افزار جاسوسی به ریاض و دیگر کشورهای هم پیمان با خود فروخته است. بر اساس گزارش روزنامه واشنگتن‌پست به نقل از مقامات آمریکایی، اسرائیل، فروش فناوری جاسوسی شرکت نرم‌افزاری- اطلاعاتی NSO Group به عربستان سعودی را تأیید کرده بود. بنابر گزارش‌ها، عربستان سعودی از این نرم‌افزار برای هک ابزارهای ارتباطی مخالفان و دشمنان محمد بن‌سلمان، ولیعهد این پادشاهی استفاده می‌کند. گزارش واشنگتن‌پست در مورد فروش نرم‌افزار Pegasus به ریاض، چند روز پس از آن منتشر می‌شود که عمر عبدالعزیز، منتقد سرسخت شاهزادگان سعودی که در کشور کانادا در تبعید به سر می‌برد، شکایتی را در تل‌آویو علیه شرکت اسرائیلی NSO تنظیم کرد و مدعی شد که ارتباطات بین او و جمال خاشقجی، از سوی سعودی‌ها با استفاده از این نرم‌افزار، رصد می‌شد[xxxv]. خاشقجی، روزنامه‌نگار منتقد سعودی بود که حدود یک ماه و نیم پیش در کنسولگری

	عربستان در ترکیه به قتل رسید و شواهد حاکی از ارتکاب قتل به دست عوامل بن سلمان است. به عنوان مثال، برنامه جاسوسی Pegasus3 [xxxvi] که از تولیدات شرکت اسرائیلی NSO Group Technologies است، امکان رخنه به هر دستگاه تلفن همراه از طریق شماره تلفن آن را فراهم می‌کند. این نرم‌افزار می‌تواند از میکروفون و دوربین تلفن همراه برای ضبط گفت‌وگوها استفاده و اپلیکیشن‌های کدگذاری‌شده‌ای همچون Whatsapp را شنود کند [xxxvi i]. عربستان این برنامه را به قیمت ۵۵ میلیون دلار برای جاسوسی علیه شهروندانش خریداری کرده است. از جمله ویژگی های مهم این نرم‌افزار، رخنه بدون نیازی به لینک‌های فیشینگ است زیرا این نرم‌افزار برای نفوذ از آسیب‌پذیری‌های روز–صفرم موجود در تلفن همراه یا آسیب‌پذیری‌های اپلیکیشن‌های نصب‌شده در تلفن‌های همراه برای رخنه استفاده می‌کند. این برنامه از الگوریتم‌های پیچیده‌ای که NSO آن را با همکاری دولت اسرئیل نوشته استفاده می‌کند. عربستان با استفاده از این برنامه، تلفن همراه مخالفانی همچون خاشقجی، عمر بن عبدالعزیز، یحیی عسیری و... را شنود کرده است [xxxvi i i]. ادوارد اسنودن تاکید کرده که عربستان از طریق این برنامه به جاسوسی علیه خاشقجی پرداخته است.

در جدول بالا، آخرین تغییرات و تحولات کشورهای بزرگ و پیشرفته جهان را مورد بررسی قرار دادیم که چه گام‌هایی برای تطابق‌پذیری خود با تغییرات سطح فناوری انجام داده‌اند. همچنین به صورت ویژه مشاهده کردید که رژیم صهیونیستی و آمریکا به چه شکل از فضای سایبر برای نظارت و جاسوسی و حتی حمله به منظور تخریب زیرساخت‌های امنیتی، اقتصادی و انرژی دیگر کشورها بهره می‌برند.

به هر صورت، به نظر می رسد در طول تمامی فازهای یک عملیات به دست آوردن و نگهداری قدرت مانور در فضای سایبر و همچنین طیف الکترومغناطیس بسیار حیاتی است. علاوه بر اینکه باید قدرت مانور را به دست آورد، همچنین نباید اجازه داد دشمن بتواند از این فضا بر علیه خود ما بهره برداری کند. از همین روی، بسیاری از کشورها با ایجاد سازمان هایی تلاش می کنند تمامی دامنه و فعالیت های این حوزه را تحت ی چارچوب واحد مدیریت کنند.

مراجع

[i] Defending and Exploiting EM Spectrum Against-For Cyber Warfare By Brigadier Saurabh Tewari

[ii] https://www.veracode.com/directory/owasp-top-10

[iii] http://www.unisec.jp/cltp/online/7)CLTP4_Communication%20&%20GroundStation.pdf

[iv] https://blog.malwarebytes.com/101/business/2019/04/when-malware-becomes-a-threat-to-physical-security/

[v] https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

[vi] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

[vii] https://me-en.kaspersky.com/resource-center/threats/blackenergy

[viii] https://www.globalsecurity.org/military/library/policy/army/fm/11-32/Ch1.htm

[ix] http://mil-embedded.com/articles/software-defined-enhanced-military-communications/

[x] https://blog.trendmicro.com/the-importance-of-vulnerability-research-recent-findings/

[xi] https://blog.malwarebytes.com/101/2017/03/what-are-exploits-and-why-you-should-care/

[xii] https://www.avg.com/en/signal/what-is-malware

[xiii] https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

[xiv] https://www.veracode.com/security/rootkit

[xv] https://blog.malwarebytes.com/detections/bootkit/

[xvi] http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

[xvii] http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%20312%20FINAL%20WEB%201.PDF

[xviii] Warfare in the Electromagnetic Spectrum and Cyberspace: United States Air Force Cyber/Electromagnetic Warfare by

[xix] https://www.nsa.gov/resources/everyone/ghidra/

[xx] https://wikileaks.org/ciav7p1/

[xxi] Sharma Deepak, 2011, China's Cyber Warfare Capability and India's Concerns، Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/system/files/jds_5_2_dsharma.pdf) Accessed 22 Aug 2018

[xxii] Costello John, 2016, The Strategic Support Force: China's Information Warfare Service, China Brief, Volume: 16 Issue: 3, Jamestown Foundation (https://jamestown.org/program/the-strategic-support-force-chinas-informationwarfare- service/) Accessed 22 Aug 2018

[xxiii] https://thediplomat.com/2017/04/pla-strategic-support-force-theinformation-umbrella-for-chinas-military/, Accessed 25 Aug 2018

[xxiv] https://www.rand.org/pubs/research_reports/RR2058.html, Accessed 25 Aug 2018

[xxv] https://nationalinterest.org/blog/buzz/china-knows-all-about-f-35-and-f-22-thanks-data-it-stole-61912

[xxvi] https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231

[xxvii] Freedberg Sydney, 2015, Army Fights Culture Gap Between Cyber& Ops:Dolphin Speak, Breaking Defense, 10 November 2015,(http//:breakingdefense.com/2015/ 11/army-fights-culture-gap-between-cyber-opsdolphin-speak/) Accessed 20 Aug 2018

[xxviii] Independent, 22 Feb 2017(http://www.independent.co.uk/news/world/europe/russia-military-information-warfare-hacking-allegations-a7594456.html) Accessed 20 Aug 2018

[xxix] Australian Government, Department of Defence CEWD Strategic Plan 2016-2021: p 21 (https://www.dst.defence.gov.au/sites/default/files/divisions/documents/CEWD_Strategic_Plan_2016-2021.pdf) Accessed 23 Aug 2018

[xxx] https://www.timesofisrael.com/army-to-establish-unified-cyber-corps/

[xxxi] https://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/

[xxxii] https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5

[xxxiii] http://www.secdev.org/conf/skype_BHEU06.handout.pdf

[xxxiv] https://wikileaks.org/wiki/Skype_and_SSL_Interception_letters_-_Bavaria_-_Digitask

[xxxv] https://www.washingtonpost.com/opinions/2019/11/14/saudi-spies-hacked-my-phone-tried-stop-my-activism-i-wont-stop-fighting/

[xxxvi] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[xxxvii] https://research.checkpoint.com/2019/the-nso-whatsapp-vulnerability-this-is-how-it-happened/

[xxxviii] https://www.timesofisrael.com/israeli-hacking-firm-nso-group-offered-saudis-cellphone-spy-tools-report/