تعیین ابعاد عملیات سایبری در نیروهای نظامی، دسته‌بندی تهدیدات و حوزه‌های کاربری آنها

فرهاد فرنیا[1]، مهرداد نجفی نوکاشتی[2]، تورج قهرمانی[3]

۱- دانشجوی دکترا، ۲- دانشجوی دکترا و عضو هیات علمی داشگاه افسری و تربیت پاسداری امام حسین(ع)، ۳- دانشجوی دکترا

چکیده:

با ورود سایبر به عملیات نظامی و تشکیل عرصه پنجم صحنه نبرد، تعاریف و حوزه‌های رزم منحصر به‌فردی را ایجاد کرده است. یکی از تعاریف مهم ایجاد شده، سایبرالکترمغناطیس نظامی است که در کنار عملیات سایبر و عملیات جنگ‌الکترونیک مورد استفاده قرار می‌گیرد. در این تحقیق، پس از بررسی علمی و دقیق ابعاد سایبر در حوزه نظامی و بیان قابلیّت‌ها و **تفاوت** بُعدهای یادشده، متناسب با مراجع و گزارش‌های منتشرشده، نمونه‌ای از کاربردهای آنها در عملیات نظامی مورد توجه قرار گرفته است. این تحقیق از نظر هدف، کاربردی-توسعه‌ای و از نظر شیوه‌ی گردآوری داده‌ها، توصیفی- موردی است. به‌منظور گردآوری داده‌ها، از منابع کتابخانه‌ای، اَسناد و گزارشات علمی داخلی و خارجی استفاده شده و رویکرد مورد استفاده برای تجزیه و تحلیل داده‌ها نیز از نوع کیفی است. نتایج حاصل از این تحقیق نشان می‌دهد، عملیات سایبرالکترومغناطیس به عنوان یک بُعد، جُدای از عملیات سایبر و عملیات جنگ الکترومغناطیس در نظرگرفته می شود؛ برای مقابله با تهدیدات منشعب شده از این بُعد، باید تفاوت‌ها و اشتراک‌های فی‌مابین بُعد سایبرالکترومغناطیس را با دو بُعد دیگر شناخت و مرز شفافی را برای این سه بُعد و اشتراکات آنها ترسیم کرد.

کلید واژه‌ها: سایبرالکترومغناطیس، عملیات سایبری، عملیات جنگ‌الکترومغناطیس.

Determining the dimensions of cyber operations in military forces, categorizing threats and their areas of use

[1]Farhad farnia*, [2]Mehrdad Najafi Nokashti ,[3]Toraj Ghahramani,

1- Ph.D Student in Cyber Defense, 2- Ph.D Student in Cyber Defense, 3- M.S in management

Abstract

With the introduction of cyber into military operations and the formation of the fifth battlefield, it has created unique definitions and areas of combat. One of the important definitions created is military cyber-electromagnetism, which is used alongside cyber operations and electronic warfare operations. In this research, after the scientific and detailed examination of cyber dimensions in the military field and the expression of the capabilities and differences of the mentioned dimensions in accordance with the published references and reports, an example of their applications in military operations has been considered. This research is applied-developmental in terms of purpose and descriptive-case in terms of data collection method. In order to collect data, internal and external library sources, documents and scientific reports were used, and the approach used for data analysis was qualitative and in-depth interviews with 12 specialists and university professors in the field of cyberelectromagnetism. The results of this research show that cyber-electromagnetic operations are considered as a separate dimension from cyber operations and electromagnetic warfare operations and have common limits with the two mentioned dimensions; The differences and commonalities between the cyberelectromagnetic dimension and the other two dimensions have been explained and the border between the cyberelectromagnetic dimension and other dimensions has been clearly defined.

Keywords: Cyber-electromagnetic, cyber operation, electromagnetic warfare operation

۱- مقدّمه

با پیشرفت فناوری و ورود تعاریف فضای سایبری به حوزه‌ی نظامی، علاوه بر در نظر گرفتن حوزه‌ی سایبری به عنوان عرصه‌ی پنجم صحنه‌ی نبرد، عامل توانمندسازی سایر عرصه‌های زمینی، هوایی، دریایی و فضایی نیز شناخته شد [۱]. در

* نویسنده مسئول: نویسنده اوّل

سال‌های اخیر تلاش‌های زیادی برای ایجاد یک تعریف مشخّص و مأموریت خاص نظامی به‌ویژه در ترکیب با سایر حوزه‌های عملیاتی صورت گرفت و به تبع آن به دنبال توسعه این مفهوم، واژه‌ها و تعاریف جدیدی ایجاد گردید. یکی از پُرکاربردترین و در عین حال پُرچالش‌ترین واژه‌های ایجادشده، واژه سایبرالکترومغناطیس است که اولین‌بار توسط وزارت دفاع آمریکا در سال ۲۰۱۴م تحت عنوان اقدامات سایبرالکترومغناطیس (CEMA[۳]) مورد بررسی و تعریف قرار گرفت[۲]. پیرو تعریف CEMA، ساختار سازمانی و یگان‌های عملیات سایبری تحت عنوان فرماندهی سایبری (CYBERCOM) در وزارت دفاع و نیروهای رزمی آمریکا تشکیل و دستورالعمل‌های مربوطه تنظیم و به‌کار گرفته شد.

ادّعای وجود تهدیداتی همانند پروژه سوتر[۴] و یا هک سیستم‌های پدافند هوایی در سوریه و هم‌چنین، اقداماتی مانند در اختیارگیری تجهیزات نظامی در حوزه رادار، هواپیما، ریزپرنده و ... بر اهمیّت شناخت دقیق بُعد سایبرالکترومغناطیس نظامی می‌افزاید. زیرا، می‌توان با تعیین حدود و مشخّصات این نوع ویژه از عملیات، صحّت ادّعاهای مطرح شده را آزمود و در صورت تأیید، اقدامات تقابلی مربوطه را در عملیات مدنظر قرار داد.

بر اساس اسناد منتشر شده، CEMA حدّ مشترک بین عملیات فضای سایبر، عملیات جنگ‌الکترونیک و مدیریت طیف الکترومغناطیس تعیین گردیده است[۳]؛ لذا، با توجه به نوع، محیط و مشخّصات خاص هر عملیات می‌توان بُعد سایبرالکترومغناطیس را تعریف کرد. سؤالی که در اینجا مطرح می‌شود این است که آیا اساساً، اشتراکی بین بُعدهای عملیات فضای سایبر، جنگ الکترونیک و مدیریت طیف الکترومغناطیس به معنای بیان شده در اسناد منتشره وجود دارد؟ در صورت وجود، ارتباط آنها چگونه است؟ و در غیر این‌صورت، بُعد سایبرالکترومغناطیس نظامی چیست و چه ابعادی را شامل می‌شود؟ برای پاسخ‌گویی به سؤالات مطرح‌شده، ابتدا تعاریف موجود در بُعد عملیات سایبری و عملیات جنگ الکترونیک را مورد مطالعه و بررسی قرار می‌دهیم؛ سپس، با توجه به تعاریف و مصادیق، بُعد سایبرالکترومغناطیس را تعریف و در نهایت، شباهت‌ها، تفاوت‌ها و محدوده‌های اشتراکی بین این بُعدها را تعریف و تشریح خواهیم کرد.

۲- مبانی نظری

۲-۱- تعاریف

۲-۱-۱- مفهوم سایبر و عملیات سایبری

مفهوم عملیات سایبر، اولین‌بار توسط نویسنده آمریکایی ویلیام فورد[۵] در رُمان علمی- تخیّلی نئورومانسر[۶] در سال ۱۹۸۴م آورده شده است[۴]. تاکنون تعاریف متعددی توسط مراکز علمی، پژوهشی و نظامی در بُعد فضای سایبر صورت گرفته است. امّا، با توجه به رویکرد نظامی مدنظر این پژوهش، تعاریف مورد استفاده توسط اسناد دفاعی آمریکا و ناتو را مورد توجه قرار می‌دهیم. مهم‌ترین اسناد وزارت دفاع آمریکا که به تعریف فضای سایبر و عملیات فضای سایبر پرداخته‌اند عبارتند از: JP 1-02، JP 3-0، FM 3-38 و FM 3-12.

تعریف وزارت دفاع آمریکا از فضای سایبر: «فضای سایبر یک بُعد جهانی محیط اطلاعاتی است که متشکل از شبکه مستقل زیرساخت فناوری اطلاعات و اطلاعات موجود در این شبکه بوده و شامل اینترنت، شبکه‌های ارتباطی، سیستم‌های رایانه‌ای و کنترل‌گرها و پردازنده‌های تعبیه‌شده در آنها است»[۵] . این تعریف به تجهیزات الکترونیکی پردازش اطلاعات و نرم‌افزار رایانه‌ای نصب شده روی این تجهیزات اشاره می‌کند.

تعریف ناتو از محیط اطلاعاتی: «فضای فیزیکی و مجازی است که در آن اطلاعات دریافت، پردازش و انتقال می‌یابند. این محیط شامل اطلاعات و سیستم‌های اطلاعاتی است». در این تعریف ، «فضای فیزیکی» به معنی تجهیزات الکترونیکی (رایانه‌ها) بوده و «فضای مجازی» به معنی محیط نرم‌افزاری است. همکاری هر دو محیط می‌تواند منجر به دریافت، پردازش و انتقال اطلاعات گردد[۶].

---

[۳] Cyber Electromagnetic Activity

[۴] SUTER

[۵] William ford

[۶] Neuromancer

تعریف عملیات فضای سایبر: به‌کارگیری قابلیت‌های فضای سایبر درجایی که هدف اولیه‌ی آن دست‌یابی به اهداف دریا از طریق فضای سایبری باشد[۳].

آنچه در تعاریف فوق مشترک است، محیط اطلاعاتی است که از محدوده الکترونیکی (جایی که اطلاعات به صورت فیزیکی توسط رایانه پردازش می شوند) و فضای مجازی (جایی‌که اطلاعات توسط نرم‌افزار پردازش می شوند) تشکیل شده است. در واقع، باید به این مهم توجه کرد که تمام عملیات‌ها تنها در محیط اطلاعاتی انجام می‌گیرند. بنابراین، عملیات در فضای سایبر، به سه بخش عمده‌ی زیر تقسیم می‌شود:

۱- دزدی اطلاعات (نشت اطلاعات) توسط نرم‌افزار ویژه

۲- ایجاد خطای عمدی روی تجهیزات توسط نرم‌افزار ویژه

۳- ایجاد داده خطا توسط سیستم فریب (مانند فیشینگ و ...) توسط نرم‌افزار ویژه

در این تقسیم‌بندی عملیات سایبری بر اساس روش (تکنیک) مشترک استفاده از نرم‌افزار ویژه، رایانه پردازش اطلاعات را انجام می‌دهد که می‌توان تمام روش‌های یادشده را تحت عنوان «فعالیت سایبری» در نظر گرفت[۷]. این نوع عملیات تنها منوط به کاربرد نظامی نبوده و در حوزه‌های غیرنظامی توسط انواع افراد، گروه‌ها، شرکت‌ها و حتی دولت‌ها اقداماتی در راستای ارتقای امنیّت و یا آسیب‌رسانی بر امنیّت سایبری با انواع انگیزه‌ها و اهداف غیرنظامی نیز انجام می شود و مقالات متعددی در این حوزه منتشر گردیده است[۸]. برای انجام عملیات فضای سایبری در بُعد نظامی از سلاح سایبری استفاده می‌شود که برابر تعریف فرهنگ لغت نظامی وزارت دفاع ایالات متحده آمریکا، سلاح سایبری «سلاحی است که به طور ویژه، به گونه‌ای طراحی می‌شود که پرسنل یا مواد (تأسیسات، تجهیزات و ...) را از کار بیندازد و در عین حال، تلفات، صدمات دائمی به پرسنل و آسیب‌های نامطلوب را به اموال و محیط‌زیست به حداقل برساند»[۹]. انواع ویروس‌ها، کرم‌ها، بدافزارها، باج افزارها و ... را می‌توان به عنوان سلاح سایبری[۷] در نظر گرفت.

برای مقابله با عملیات فضای سایبری دشمن، از تجهیزات و نرم‌افزارهایی همانند آنتی‌ویروس، فایروال‌ها[۸] سیستم‌های شناسایی نفوذ (IDS) و رمزگذاری داده استفاده می شود. این تجهیزات حیاتی که اقدامات مقابله‌ای را انجام می‌دهند، از این پس آن را «پدافند سایبری[۹]» می‌نامیم، شامل معیارهایی به شرح زیر است[۱۰]:

۱- معیار فنّی، که بر پایه زیرساخت و دوره پاسخ به حوادث طراحی می‌شود.

۲- امنیّت بازگشت سرمایه (ROI)، که به محاسبه هزینه- فایده برای به‌کارگیری سیاست یا فناوری جدید می‌پردازد.

۳- حالت خطر، که به تحلیل رخداد یک رویداد سایبری نسبت به سرمایه‌گذاری و عملیات انجام شده می‌پردازد.

با توجه به مطالب بیان شده به منظور دسته‌بندی اجزای عملیات فضای سایبری متناسب با نوع اقدام (تهاجم، پدافند، بهره‌برداری) می‌توان حوزه های اختلال و فریب را در بخش تهاجم سایبری[۱۰] تحت عنوان رزم سایبری در نظر گرفت. بخش‌های عمده سایبری در جدول (۱) آورده شده است. لازم به یادآوری است واژه‌ی دفاع سایبری در زبان فارسی دارای دو معنی آفند سایبری و پدافند سایبری استو در سند سازمان پدافند غیرعامل کشور، پدافند سایبری را به صورت «بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیر سایبری کشور،به‌منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به موقع،مقابله‌ی مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری، توسط متخاصمین سایبری، اَعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید»، آورده شده است.

---

[۷] Cyber weapon

[۸] Firewall

[۹] Cyber defense

[۱۰] Cyber attack

جدول(۱): بخش‌های عمده عملیات فضای سایبری.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	اطلاعات سایبری	دزدی اطلاعات (نشت اطلاعات) توسط نرم‌افزار ویژه	بهره‌برداری
۲	رزم سایبری	ایجاد خطای عمدی روی تجهیزات توسط نرم‌افزار ویژه	اختلال در عملکرد
۳	رزم سایبری	ایجاد داده خطا توسط سیستم فریب توسط نرم‌افزار ویژه	فریب
۴	پدافند سایبری	مقابله با عملیات سایبری دشمن	پدافند

۳- مفهوم جنگ الکترونیک و جنگ‌الکترومغناطیس

در اسناد وزارت دفاع آمریکا، تا سال ۲۰۲۱م از واژه جنگ‌الکترونیک[۱] استفاده شده، ولی از سال ۲۰۲۱م این واژه به جنگ‌الکترومغناطیس[۲] تغییر نموده است؛ تمام تعاریف و زیربخش های دو تعریف مذکور یکسان بوده و فقط کلمه الکترومغناطیس جایگزین الکترونیک گردیده است. به عنوان مثال، حمله‌ی الکترونیک با همان تعریف قبلی به حمله‌ی الکترومغناطیس تغییر کرده است.

تعریف واژه جنگ الکترومغناطیس: «اقدام نظامی شامل استفاده از الکترومغناطیس و انرژی هدایت‌شده برای کنترل طیف الکترومغناطیس یا حمله به دشمن است»[۳] .

عملیات جنگ الکترومغناطیس را می‌توان به بخش‌های زیر تقسیم کرد[۷] :

۱- ایجاد خطای عمدی روی تجهیزات دشمن از طریق تشعشع مستقیم و پُرقدرت موج الکترومغناطیس.

۲- ایجاد داده‌ی خطا توسط تولید میدان الکترومغناطیس پُرتوان بُردبلند که سیستم ناوبری و تشخیص الکترونیکی را فریب می‌دهد.

۳- آسیب فیزیکی و قابل توجه روی تجهیزات الکترونیکی و الکترومغناطیسی توسط گسیل انرژی مستقیم (مانند HEMP).

علاوه بر بخش‌های یادشده، می‌توان شنود سیگنالی (اَعم از ارتباطی و راداری) را نیز به صورت در لحظه (سامانه‌های ESM[۱۳]) و راهبردی (سامانه های ELINT[۱۴] و COMINT[۱۵]) به عنوان بهره‌بردای اطلاعات سیگنال الکترونیکی در نظر گرفت. هم‌چنین، استفاده از تکنیک‌های ECCM[۱۶] را به عنوان روش مقابله‌ای با اقدامات تهاجمی جنگ الکترومغناطیس در نظر گرفت[۱۱]. بخش‌های عمده‌ی عملیات جنگ‌الکترومغناطیس در جدول (۲) نشان داده شده است. لازم به ذکر است که سلاح جنگ الکترومغناطیس، شامل سامانه‌های اخلالگر و فریب سیگنالی است.

در سال ۲۰۰۷م، آژانس امنیّت ملّی آمریکا سند یک فناوری که با نام کد شده TEMPEST شناسایی می شود و در سال ۱۹۶۰م منتشر گردیده را از طبقه‌بندی خارج نمود[۱۰]. در سند مذکور به نشت اطلاعات از طریق تشعشع ناخواسته

---

[۱] Electronic warfare
[۲] Electromagnetic warfare
[۱۳] Electronic Support measurements
[۱۴] Electronics Intelligence
[۱۵] Communication Intelligence
[۱۶] Electronics Counter Counter- Measurements

الکترومغناطیس ا شاره می‌کند که امکان بازیابی اطلاعات مذکور تو سط یک آنتن در فا صله‌ای قابل توجه از محل انت شار وجود دارد. این پدیده در سند با نام کد TEMPEST شناخته می‌شود.

جدول(۲): بخش‌های عمده عملیات جنگ الکترومغناطیس.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	پشتیبانی جنگ الکترومغناطیس	شنود اطلاعات سیگنالی (راداری و ارتباطی)	بهره‌برداری
۲	حمله الکترومغناطیس	ایجاد خطای عمدی روی تجهیزات توسط تشعشع الکترومغناطیس	اختلال در عملکرد
۳	حمله الکترومغناطیس	ایجاد داده خطا توسط سیگنال الکترومغناطیس	فریب
۴	مصون سازی الکترومغناطیس[۱۷]	استفاده از تکنیک‌های ضد جنگ الکترومغناطیس	پدافند

TEMPEST چیست؟

یک اسم رمز آژانس امنیّت ملی آمریکا (NSA[۱۸]) و ناتو است[۱۲]، که مرتبط با جاسوسی از سیستم‌های اطلاعاتی از طریق نشت سیگنال‌ها، شامل سیگنال‌های رادیویی ناخواسته یا سیگنال‌های الکتریکی، صوتی و ارتعاشات می‌شود. در واقع این اسم رمز هم به روش‌های جاسوسی و هم راهکارهای محافظت از تجهیزات در مقابل این روش‌ها را پوشش می‌دهد[۱۳]. تعاریف متفاوتی برای این اسم رمز آورده شده است که هیچ یک تاکنون به طور رسمی توسط آژانس امنیّت ملّی آمریکا تأیید نشده است. از مهم‌ترین این تعاریف می‌توان به موارد زیر اشاره کرد:[۱۹]

- مواد الکترونیکی ارتباطات از راه دور محافظت شده از انتقالات جعلی[۲۰]
- تابش‌گذاری محافظت شده از انتقالات جعلی[۲۱]
- استاندارد انتشار پالس الکترمغناطیس گذرا[۲۲]
- استاندارد امنیّت انتشار ارتباطات راه دور[۲۳]

روش‌های حفاظت در برابر آن نیز به عنوان امنیّت انتشار (EMSEC[۲۴]) شناخته می‌شوند که زیرمجموعه‌ای از امنیّت ارتباطات (COMSEC[۲۵]) می‌با شند. تعریف دیگر از آن عبارت ا ست از: تجهیزات پردازش اطلاعات الکترونیکی و الکترومکانیکی می‌توانند انتشارات ناخواسته اطلاعاتی را ایجاد کنند که معمولاً به عنوان TEMPEST شناخته می‌شود. در صورت رهگیری و تجزیه و تحلیل این انتشارات، ممکن است اطلاعات منتقل‌شده، دریافت، پردازش یا پردازش‌شده توسط تجهیزات را فاش کنند.

با وجود آنکه TEMPEST بی شتر برای ن شت امواج الکترومغناطیس ا ست، امواج صوتی و لرزش‌های مکانیکی را نیز در بر می‌گیرد. برای مثال، ممکن است به منظور به دست آوردن کلمه‌ی عبور یک کاربر از سنسور حرکت داخل گوشی هوشمند او ا ستفاده کنند[۱۴]. سیگنال‌های حامل اطلاعات غیرعمدی که در صورت قطع و تجزیه و تحلیل (حمله کانال جانبی)، ممکن

---

[۱۷] مصون‌سازی الکترومغناطیس که ترجمه واژه Electromagnetics protection می‌باشد، در بعضی از منابع فارسی تحت عنوان حفاظت الکترومغناطیس یا دفاع الکترومغناطیس آورده شده است که به لحاظ لغوی مصون‌سازی ترجمه صحیح‌تری می‌باشد (توضیح مولّف).

[۱۸] National Security Agency

[۱۹] https://www.learnsecurityonline.com

[۲۰] Telecommunications Electronics Material Protected from Emanating Spurious Transmissions

[۲۱] Transient Emanation Protected from Emanating Spurious Transmissions

[۲۲] Transient Electromagnetic Pulse Emanation Standard

[۲۳] Telecommunications Emission Security Standards

[۲۴] Emission Security

[۲۵] Communication Security

ا ست انتقال، دریافت و به‌کارگیری اطلاعات به‌د ست آمده و یا پردازش تو سط هر سامانه پرداز شگر اطلاعات را فاش نماید، به خطر افتادن از طریق انتشار تعریف می‌شود[۱۳].

۴- پیشینه

شـــنود اطلاعات از ســـیگنال به جنگ جهانی دوّم باز می‌گردد. در طول جنگ جهانی دوّم، شـــرکت تلفن بل[۶] یک دســـتگاه میک سر[۷] با نام B2-131 را در اختیار ارتش آمریکا قرار داد تا سیگنال‌های تله چاپگر را با ا ستفاده از XOR نمودن با مواد کلیدی از نوارهای یکبار مصـرف (سـیسـتم SIGTOT) و یا پیش از آن توسـط یک ژنراتور کلیدی مُبتنی بر روتور، رمزگذاری می‌کرد که SIGCUM نامیده می شد. در این زمان، بل اعلام نمود که با استفاده از میخ‌های الکترومغناطیسی در فواصل مشخصی از میکسر می‌توانند متن ساده را بازیابی نمایند. در سال ۱۹۵۶م، آزمایشگاه نیروی دریایی آمریکا، میکسر بهتری را توسعه داد که در ولتاژ و جریان کمتری کار می‌کرد. بنابراین، امکان ا ستخراج داده از تشعشات آن کمتر بود. این طراحی در سیستم‌های جدید رمزنگاری NSA مورد ا ستفاده قرار گرفت. در سال ۱۹۵۸م، NSA ا ستانداردهای تشعشع NAG-1 را برای تجهیزات و تأ سیسات بر ا ساس محدود یت ۵۰ فوت (معادل ۱۵ متر) برای کنترل تعیین کرد و در این اســـتاندارد، ســـطوح طبقه‌بندی جنبه های مختلف TEMPEST را م شخّص نمود. با گذ شت زمان و اهمیّت مو ضوع، ا ستانداردهای TEMPEST در دهه ۱۹۷۰م و بعد از آن با انجام آزمایش‌های جدیدتر و دســـتورالعمل‌های دقیق‌تر که خطرات را در مکان‌ها و موقعیت‌های خاص در نظر می‌گرفت، به تکامل خود ادامه دادند[۱۵].

روش‌های مختلفی برای ارزیابی و تنظیم تشـعشـعات ناخواسـته امواج الکترومغناطیس[۸] (CE) وجود دارد که یکی از اولین روش‌ها، بر مفهوم قرمز/ سیاه مُبتنی ا ست. این مفهوم تفکیک سیگنال‌هایی که محرمانگی اطلاعات را حفظ می‌کند (سیگنال قرمز) و سیگنال‌هایی که حاوی اطلاعات غیرطبقه‌بندی شده و غیر رمز ه ستند (سیگنال‌های سیاه) را تو صیف می‌کند. این تفکیک غالباً تو سط طبقه‌بندی فایروال‌ها یا درگاه‌های بدون جهت، تشخیص داده می شود. در جدول (۳) سطوح ایزولا سیون الکتریکی مطابق با دستورالعمل نصب RED/BLACK فاقد طبقه‌بندی نشان داده شده است. برنامه مراقبتی ECHELON که به طور رســـمی در ســـال ۱۹۷۱م ایجاد و توســـط آمریکا، اســـترالیا، کانادا، نیوزلند و انگلســـتان به‌کار گرفته شـــد، معروف به پنج‌چشـــم[۹] اســـت که هدف آن کنترل اتحاد جماهیر شـــوروی بود.اما بعدها دامنه‌ی جســـتجوی آن گســـترش یافت و به برنامه مراقبت جهانی که وظیفه آن علاوه بر مانیتور اهداف نظامی، مانیتور ارتباطات تجاری و خصوصی هم بود، تغییر یافت[۱۶].

جدول (۳): سطح ایزولاسیون الکتریکی برای جلوگیری از تشعشعات نخواسته در اسناد استاندارد سازی آمریکا[۱۵].

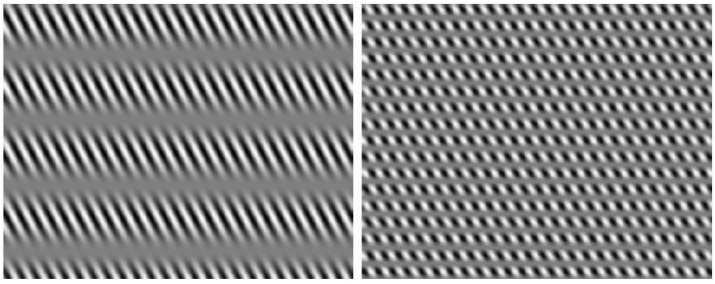
نوع سیگنال قرمز	سطح ایزولایون	محدوده فرکانسی
صوتی آنالوگ	۱۰۰dB	۱۰۰ تا ۵۰۰۰ هرتز
سیگنال‌های آنالوگ شامل ویدئوی آنالوگ	۸۰dB	کمترین نرخ سیگنال‌دهی به بیشینه‌ی نرخ سیگنال‌دهی
سیگنال‌های دیجیتال	۶۰dB	کمترین نرخ سیگنال دهی به ۱۰ برابر بیشترین نرخ سیگنال‌دهی

برنامه TEMPEST بخ شی از برنامه‌های بالاد ستی را شکل می‌دهد که همانند برنامه ECHELON مراقبت و جا سو سی سیگنالی را پوشش می‌دهند[۱۷]. به دنبال آن، سایر کشورها نیز برنامه‌هایی مشابه آن را در سرویس‌های اطلاعاتی خود ایجاد کرده‌اند که می‌توان به SORM[۱۰] روســـی[۱۸]، برنامه مراقبتی فرانســـه "L infrastructure demutualisation (IM)" که به Ferenchelon معروف است[۱۹]، برنامه Projekt 6 آلمان و برنامه Onyx سوئیس اشاره کرد.

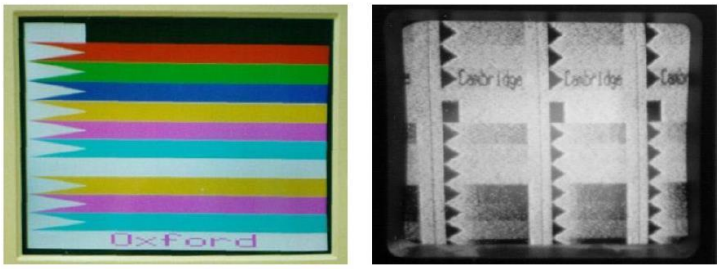
---

[۶] Bell Telephone
[۷] Mixer
[۸] Compromising Emanation (CE)
[۹] Five eyes
[۱۰] System for Operation Investigative Activities
[۱۱] Russian SORM

آخرین سند غیرمحرمانه منتشرشده درباره TEMPEST مربوط به سال ۲۰۰۲م است که استاندارد ارزیابی NSA TEMPEST 01-02 NONSTOP نام دارد[۲۰]. در این سند، بخش‌های کوچکی از تکنیک‌های مراقبتی NONSTOP آورده شده است. مطابق با مفاد این سند، مشخص می‌شود که تکنیک‌های NONSTOP بسیار شبیه به تکنیک‌های TEMPEST است[۲۱]. حملات شاره شده در این سند از نوع غیرفعال[۳۲] هستند که با بهره‌برداری[۳۳] از نشت غیرعمدی امواج الکترومغناطیس، موجب کشف اطلاعات آن شده، به‌دست می‌آید. گروه اقدام **آادی** اطلاعات (FOIA[۳۴]) که اقدام به افشای اطلاعات مرتبط با اسناد TEMPEST کرده است، نشان می‌دهد که NSA هم‌چنین، بر روی روش‌های ایجاد تشعشعات الکترومغناطیس عمدی روی سیستم‌های امنیتی با استفاده از بدافزار سرمایه‌گذاری نموده است. اسم رمز TEAPOT که برای این نوع از اقدامات استفاده می‌شود اشاره دارد به «سرمایه‌گذاری، مطالعه، و کنترل تشعشعات الکترومغناطیس عمدی»[۲۱ و ۲۲]. این بدافزار می‌تواند داده‌های ویدئویی را در درجات کوچک غیرقابل تشخیص برای کاربرد، به گونه‌ای دست‌کاری نماید که به ایجاد نشت الکترومغناطیس قوی‌تر در سیستم به واسطه‌ی جا دادن یک فرکانس خاص در تولید سیگنال ویدئویی مدوله‌شده روی فرکانس رادیویی حامل گردد، بیانجامد. این امر به تبدیل شدن سیستم به یک فرستنده‌ی سرتاسری رادیویی می‌انجامد که می‌تواند یک کانال رادیویی را پوشش دهد. یک مثال از این در شکل (۱) نشان داده شده است. این حمله به‌ویژه برای سیستم‌های امن شده با شکاف هوایی[۳۵] بسیار خطرناک است. یک روش مناسب‌تر تغییر ارزش بایت[۳۶] در ارزش پیکسل[۳۷] است که منجر به انحراف کوچک در رنگ می شود، امّا در میدان دور[۳۸] شتی الکترومغناطیس قوی‌تری ایجاد خواهد کرد[۲۳ و ۲۴]. مثال این نوع حمله در شکل (۲) نشان داده شده است.



شکل (۱): مثالی از مانیتور CRT (لوله اشعه کاتودی) با انتشار ۳۰۰ مگاهرتز (تصویر سمت چپ) و ۱۲۰۰ مگاهرتز (تصویر سمت راست)، تنظیم‌شده برای فرکانس حامل مدوله‌شده دامنه ۲ مگاهرتز[۲۳].



شکل (۲): تصویر نمایش داده شده روی مانیتور CRT (سمت چپ). تصویر ویدئویی بازیابی‌شده (سمت راست) نشان می‌دهد که پیام مخفی‌شده قابل مشاهده وی تصویر ویدئو اصلی نیست[۲۳].

---

[۳۲] Passive
[۳۳] exploit
[۳۴] Freedom-Of-Information-Act
[۳۵] Air-gapped secured system
[۳۶] Byte
[۳۷] Pixel
[۳۸] Far-field

۵- تحقیقات منتشرشده

با ظهور این تهدید خاص، توجه محقّقین به‌ویژه در ۳۵ سال اخیر به این بُعد جلب شده است. در سال ۱۹۸۵م، دبلیو وان اِک[۳۹] تحقیقاتش را درباره نشت ناخواسته الکترومغناطیس صفحات CRT منتشر کرد که در آن موفق به بازسازی تصویر نمایش داده شده در CRT با استفاده از یک آنتن، گیرنده مدولاسیون دامنه (AM) و تولیدکننده سیگنال شده بود[۲۵]. در واقع اثبات کرد که نه تنها امکان استراق سمع VDUها[۴۰] وجود دارد، بلکه می‌توان این کار را با تجهیزات فاقد سکوی تجاری (COTS[۴۱]) نیز انجام داد. تحقیقات مشابه توسط پی. اسمولدرس[۴۲] روی کابل‌های RS-232 و ام.جی. کوهن[۴۳] روی صفحات نمایش تخت[۴۴] انجام شد[۲۴]. کوهن اثبات کرد که سیگنال‌های ویدئو دیجیتال روی کابل LVDS[۴۵] یا لینک FPD[۴۶] هم قابل استراق سمع هستند.

سایر محققین برر سی‌های خود را درباره خطرات استراق سمع در این بُعد تو سعه دادند[۲۴، ۲۶، ۲۷ و ۲۹]. این تحقیقات ثابت می‌کند که VDUها در حالت کلی و کابل‌های سیگنال‌دهی دیتا مانند VGA[۴۷]، DVI[۴۸]، HDMI[۴۹] و LVDS دارای نشت الکترومغناطیس ناخواسته هستند. تاناکا و همکاران[۵۰] پژوهش کوهن را روی نمایشگرهای کریستال مایع (LCD[۵۱]) تو سعه دادند. در این تحقیق، تشعشعات LCD در میدان دور و نزدیک و هم‌چنین، اثر کوپلینگ LCD[۵۲] روی کابل‌های برق مورد بررسی قرار گرفت. تاناکا توانست تصویر را در فاصله ۶ متری بازیابی کند. هایاشی و همکاران[۵۳] در سال ۲۰۱۷م [۳۰] و لی و همکاران[۵۴] در سال ۲۰۱۸م [۳۱]، به دنبال روشی برای بازیابی اطلاعات ویدئویی نشت یافته از فاصله ۱۰ متری همراه با روش شنا سایی هم‌زمانی بودند. باید توجه کرد که به‌دلیل نوع خاص این تهدید، هنوز مستندات حاصل از تحقیقات علمی به اندازه کافی حاصل نشده و یا به دلایل امنیتی در دسترس عموم قرار نگرفته است.

۵-۱- TEMPEST نرم[۵۵]

همان‌گونه که پیش‌تر بیان گردید، حملات TEMPEST، بر استفاده از تشعشعات الکترومغناطیس ناخواسته در انواع سناریوهای موجود دلالت دارد؛ امّا نوع دیگری از حملات وجود دارد که در آن حمله‌کننده از نشت سیگنال الکترومغناطیس برای ایجاد یک کانال ارتباطی پوششی غیرمستقیم برای عدم پالایش و فیلترینگ داده استفاده می‌کند. این مدل از حملات را TEMPEST نرم می‌نامند. در این حالت مهاجم از نشت سیگنال الکترومغناطیس به‌منظور ایجاد یک کانال مخفی یک‌طرفه برای استخراج و بهره‌برداری داده استفاده می‌کند؛ این بهره‌برداری ممکن است فعال کردن یک نرم‌افزار مخرب به صورت عمدی با اهداف مختلف از جمله مدوله کردن[۵۶] یک تشعشع الکترومغناطیس جعلی استفاده کند[۲۳] . چنین کانال‌های مخفی فیزیکی

---

[۳۹] W. van Eck
[۴۰] Video Display Unit
[۴۱] Commercial off-the-shelf
[۴۲] P. Smulders
[۴۳] M. G. Kuhn
[۴۴] Flat panel display
[۴۵] Low-Voltage differential signaling
[۴۶] Front panel display
[۴۷] Video graphics array
[۴۸] Digital Visual Interface
[۴۹] High- Definition Multimedia Interface
[۵۰] Tanaka et al.
[۵۱] liquid crystal displays
[۵۲] Copling effect
[۵۳] Hayashi et al
[۵۴] Lee et al
[۵۵] Soft TEMPEST
[۵۶] Modulation

معمولاً به عنوان کانال‌های مخفی شـــکاف‌هوایی[۵۷]نامیده می‌شـــود و مطالعات متعددی در حوزه طراحی و تجزیه و تحلیل حملات TEMPET نرم شـامل سـیگنال‌های ویدیویی[۳۲]، ارتباطات CPURAM [۳۳]، دسـترسـی به هارد دیسـک[۵۸][۳۴] و ارتباطات USB [۳۵] انجام شـده اسـت. یک مثال معروف از چنین حملاتی، اثبات مفهوم "TEMPESTforElisa" اسـت که در آن یک جریان ویدئویی در هنگام نمایش نسخه مدوله‌شده از آهنگ Für Elise اثر بتهوون را منتشر می‌کند[۳۲].

۲-۵- TEMPEST نرم مرتبه‌دوّم[۵۹]

حالت دیگری از حملات TEPEST است. TEMPEST نرم مرتبه‌دوّم امکان بهره‌برداری آبشاری از اثرات متقابل تشعشات الکترومغناطیس زیاد و کم در دسـتگاه هدف به‌منظور ایجاد یک کانال مخفی دور برد تعریف می‌شـود. در واقع حمله TEMPEST نرم مرتبه‌دوّم به حمله TEMPEST نرم دو مرحله‌ای اشـاره دارد که فرآیند مخرب در آن داده‌های درگیر در انتشارات الکترومغناطیس که می‌تواند مستقیماً توسط مهاجم دریافت شود را کنترل نمی‌کند. در عوض، انتشارات کنترل شده یک مؤلفه داخلی را به خطر می‌اندازد که به نوبه‌ی خود داده‌ها را به سـمت گیرنده مهاجم منتشـر می‌کند[۳۶]. در این نوع حملات فرآیند اصلی به‌صورت زیر است:

- یک عملیات عمدی (خرابکارانه) انجام می‌شود.
- این عملیات به طور خاص تقابل داخلی تشعشعات الکترومغناطیس را ایجاد می‌کند.
- اثر این اثرات متقابل بین اجزای دارای انتشار کم و انتشار بالای الکترومغناطیس است.
- موجب یک حمله n مرحله‌ای TEMPEST نرم می‌شود

در جدول (۴)، مقایسه سه نوع حمله TEMPEST آورده شده است.

جدول۴: مقایسه حملات TEPEST، TEMPEST نرم وTEMPEST نرم مرتبه‌دوّم[۳۶].

	TEMPEST	TEMPEST نرم	TEMPEST مرتبه‌دوّم
عملیات	قانونی	ایجاد شده برای اهداف مخرب	ایجاد شده برای اهداف مخرب
تشعشع الکترومغناطیس	غیرعمدی	عمدی	عمدی
اثر متقابل نرم‌افزار موج الکترومغناطیس	مستقیم	مستقیم	غیرمستقیم
اثر حمله	بازیابی اطلاعات	ایجاد کانال مخفی	ایجاد کانال مخفی

۶ – روش‌شناسی

در این تحقیق به مفهوم‌سازی و توصیف ابعاد عملیات سایبری نظامی مشتمل بر عملیات سایبر، جنگ الکترومغناطیس و عملیات سایبرالکترومغناطیس و کاربردهای آنها به همراه اشتراکات و افتراق‌های آنها پرداخته شده است. بنابراین، این تحقیق از نوع کاربردی- توسعه‌ای است. این تحقیق از نظر ماهیّت و روش گردآوری داده‌ها از نوع توصیفی موردی است. در تحقیقات توصیفی موردی، محقّق به دنبال مطالعه‌ی عمیق در چیستی و چگونگی یک موضوع و توصیف ویژگی‌ها و تجزیه و تحلیل یک پدیده است. به منظور گردآوری داده‌ها، از منابع کتابخانه‌ای، سایت‌های معتبر علمی، اسناد و گزارش‌های داخلی و خارجی استفاده شده است. این تحقیق از نظر رویکرد مورد استفاده برای تجزیه و تحلیل داده‌ها از نوع کیفی است. روایی و پایایی تحقیق

---

[۵۷] Air-gap covert channel
[۵۸] Hard disk
[۵۹] Second order soft TEMPEST

بر مبنای معیارهای کرسول محقق شده است[۳۷]. در این روش، معیارهای روایی و پایایی شامل تماس طولانی با فضای پژوهش، مشاهده مستمر، بررسی از زوایای مختلف، گردآوری از منابع اطلاعاتی متنوع و تبادل نظر با همتایان است.

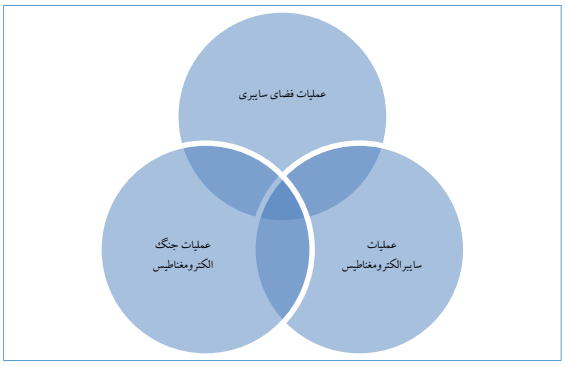
۷- تجزیه و تحلیل داده‌ها

۷-۱- تعریف سایبر الکترومغناطیس نظامی

TEMPEST شامل حمله TEMPEST، TEMPEST نرم و TEMPEST نرم مرتبه‌دوّم را به عنوان زیرگروه جدید از تهدیدات که در آن ابزار داده بوده و محیط اثر طیف الکترومغناطیس می‌باشد، در نظر گرفت. بخش‌های عمده عملیات سایبر الکترومغناطیس در جدول ۵ نشان داده شده است. این مجموعه دارای تفاوت‌هایی با عملیات سایبری و عملیات جنگ الکترومغناطیس است و در عین حال دارای اشتراکات جزیی در بعضی حوزه‌ها است؛ این اشتراکات را به عنوان سایبر الکترومغناطیس نظامی تعریف می‌کنیم. جنگ‌الکترومغناطیس و سایبرالکترومغناطیس هردو به طیف‌الکترومغناطیس وابسته هستند. در جدول ۶ مقایسه بین EMP[۶۰] به عنوان یکی از زیربخش‌های جنگ الکترومغناطیس با حملات TEMPEST به عنوان یکی از زیر بخش‌های سایبرالکترومغناطیس نظامی آورده شده است. بدیهی است ابزاری که برای اثرگذاری بر داده‌ها و از طریق امواج الکترومغناطیس به‌کار گرفته می‌شود را می‌توان به عنوان سلاح سایبرالکترومغناطیس در نظر گرفت.

۷-۲- حدود اشتراک سه بُعد عملیات

ساختار نهایی عملیات‌های فضای سایبری، سایبرالکترومغناطیس و جنگ الکترومغناطیس برابر شکل (۳) هست، **می‌باشد**. در ادامه، به بررسی تفاوت این سه بُعد به صورت دو به دو خواهیم پرداخت.



شکل(۳): ابعاد عملیات فضای سایبر، جنگ الکترومغناطیس عملیات سایبرالکترومغناطیس

جدول (۵): بخش‌های عمده عملیات سایبر الکترومغناطیس.

ردیف	عنوان بخش	اقدام عملیاتی	نوع عملیات
۱	TEMPESR	استراق سمع داده‌های محرمانه	بهره‌برداری
۲	TEMPEST نرم و EMI[۶۱]	ایجاد کانال مخفی یک‌طرفه جهت اختلال در عملکرد	اختلال در عملکرد
۳	TEMPEST نرم مرتبه دوم	ایجاد کانال مخفی برد بلند به‌منظور انجام کنترل در عملکرد	فریب
۴	EMC[۶۲]	استفاده از فیلترها و محدودسازهای تشعشع ناخواسته الکترومغناطیس	پدافند

[۶۰] High Electromagnetic Puls
[۶۱] Electromagnetic Interference
[۶۲] Electromagnetic Compatibility

جدول (۶): مقایسه HEMP و TEMPEST [۶].

	HEMP	TEMPEST
توان سیگنال	کیلو ولت، مگاهرتز	میکرو ولت، میکروووات
محدوه فرکانسی	تا ۱۰۰ مگاهرتز	تا ۱۰۰ گیگاهرتز
اقدامات حفاظتی	موانع ولتاژی	فیلترهای ضد تداخل الکترومغناطیسی
اثرات مخرب	تخریب فیزیکی زیرساخت‌ها	دسترسی غیرمجاز به اطلاعات طبقه‌بندی‌شده
تجهیزات و روش‌های تست	تجهیزات بسیار بزرگ ولتاژ با توان بسیار بالا	تجهیزات الکترونیکی با حساسیت بسیار بالا

۳-۷- اشتراک عملیات فضای سایبری و عملیات جنگ الکترومغناطیس

همان‌گونه که پیش‌تر بیان شد، این دو بُعد از لحاظ ابزار و محیط اثر کاملاً متفاوت هستند. امّا اثر هر یک از عملیات‌های یادشده را می‌توان در خروجی پردازنده‌ی سامانه‌ی هدف مدنظر قرار داد. در عملیات فضای سایبری، سیگنال ورودی به پردازنده، سیگنال سالم و بدون خطا است ولی به واسطه‌ی عملیات فضای سایبر، کد مخرب موجب خطا در نرم‌افزار پردازنده شده و سیگنال خروجی دارای خطا خواهد بود که می‌تواند منجر به اختلال در عملکرد و یا فریب گردد. امّا، در عملیات جنگ الکترومغناطیس، سیگنال ورودی به پردازنده، سیگنالی خطا یا فریب است که با عملکرد صحیح پردازنده نیز خروجی از صحت و دقّت لازم برخوردار نبوده و نتیجه همان اختلال در عملکرد و فریب خواهد بود. در واقع اثر مخرب در ایجاد سیگنال خروجی پردازش شده خطا را می‌توان به عنوان حوزه‌ی مشترک کاربری این دو عملیات درنظر گرفت. مثال دیگر از این نوع عملیات، در روش‌هایی از رمزگشایی است که در آنها با ارسال سیگنال نویز، لینک داده را کشف و نسبت به رمزگشایی اقدام می‌گردد.

۴-۷- اشتراک عملیات فضای سایبری و عملیات سایبرالکترومغناطیس

هک و نفوذ به Wi-Fi و یا در اختیارگیری[۶۳]ریزپرنده[۶۴]یا پهپاد و امثال این نوع عملیات‌ها، حدمشترک عملیات فضای سایبری و عملیات سایبرالکترومغناطیس خواهد بود. به عنوان مثال، در عملیات در اختیارگیری ریزپرنده، سیگنال تبادل داده بین ریزپرنده و ایستگاه کنترل زمینی توسط یک گیرنده کشف و سپس، پروتکل استخراج و رمزگشایی می‌شود. در مرحله‌ی بعد با تغییر پارامترها در پروتکل ارتباطی مذکور، و ارسال آن به ریزپرنده، ضمن تغییر در مشخصات کنترلی، امکان در اختیارگیری هدایت و کنترل کامل ریزپرنده وجود خواهد داشت[۳۸ و ۳۹]. در این عملیات، هم از عملیات فضای سایبر (کشف پروتکل، رمزگشایی و تغییر) و هم عملیات سایبرالکترومغناطیس (ارسال داده خطا برای ریزپرنده از طریق موج الکترومغناطیس و در اختیارگیری هدایت آن) استفاده می‌شود.

۸- اشتراک عملیات سایبرالکترومغناطیس و عملیات جنگ الکترومغناطیس

تغییر نرخ نمونه‌برداری از سیگنال در یک پردازنده‌ی مخابراتی با استفاده از سر ریز شدن بافر، می‌تواند به ایجاد خطا در خروجی انجامد؛ این نوع از عملیات با حالت یاد شده در اشتراک عملیات فضای سایبر و جنگ الکترومغناطیس متفاوت است زیرا در آن سیگنال ورودی به پردازنده سالم بوده و پردازنده نیز به صورت درست در حال انجام عملیات پردازش است. امّا به دلیل تغییر در نوع ارسال سیگنال به عنوان مثال ارسال سیگنال پُرتوان در بازه‌هایی از باند گیرنده می‌تواند موجب سرریز شدن بافر، تغییر در نرخ نمونه‌برداری سیگنال، ایجاد خطا در پردازش و در نتیجه تولید سیگنال خطا خواهد شد[۴۰]. این حالت را که می‌توان به عنوان اشتراک عملیات سایبرالکترومغناطیس با عملیات جنگ الکترومغناطیس در نظر گرفت. در جدول ۷، مثال سیگنال ورودی و پردازنده برای سه بُعد عملیاتی آورده شده است.

---

[۶۳] Hijacking

[۶۴] Drone

جدول (۷): مقایسه عملکرد پردازنده مخابراتی در سه بُعد عملیاتی.

بُعد عملیات	سیگنال ورودی	عملکرد پردازنده	سیگنال خروجی
عملیات فضای سایبری	صحیح	خطا	خطا
عملیات جنگ الکترومغناطیس	خطا	صحیح	خطا
عملیات سایبرالکترومغناطیس	صحیح	صحیح	خطا

۹- نتیجه‌گیری و پیشنهاد

عملیات‌های وابسته به سیگنال و نرم‌افزار که موجب ایجاد اختلال در عملکرد سامانه‌های وابسته به رایانه می‌شوند، به واسطه ویژگی‌های سایبر و جنگ الکترونیک، دارای حدود فاصل نبوده و به واسطه اشتراکات همواره مشکلاتی را در تعریف و به‌کارگیری ایجاد کرده‌اند. با تعریف عملیات سایبر و عملیات جنگ‌الکترومغناطیس، تفاوت در عامل تأثیرگذاری و محیط اثر این مهم را نشان می‌دهد که این دو بُعد هیچ اشتراکی با هم نداشته و نمی‌توان سایبرالکترومغناطیس را به عنوان اشتراک آنها تعریف کرد. از طرفی با بررسی اسناد منتشرشده، می‌توان دریافت حالتی وجود دارد که به واسطه نشت الکترومغناطیس در بین اجزای الکترونیکی مانند پردازنده، صفحه نمایش و ...، می‌توان اطلاعات تبادل شده را به طور غیرمجاز استراق سمع کرد. این حالت که با کدرمز TEMPEST شناخته می‌شود دارای حملات در اشکال TEMPEST نرم و TEMPEST نرم مرتبه‌دوّم نیز هست که با ایجاد کانال‌های مخفی می‌توانند در عمکلرد اختلال، و یا تغییر در داده ایجاد کند.بُعد مذکور که از طریق موج الکترومغناطیس به‌صورت مستقیم از داده بهره‌برداری کنند و یا بر داده اثر گذارند را می‌توان به عنوان بُعد سایبرالکترومغناطیس در نظر گرفت. در جدول ۸ سه بُعد عملیاتی از لحاظ ابزار و محیط اثر نشان داده شده‌اند.

جدول (۸): مقایسه عملیات سایبری، جنگ الکترومغناطیس و سایبرالکترومغناطیس از منظر ابزار و محیط.

بُعد عملیات	اثرگذاری بر	محیط
عملیات سایبری	داده	نرم افزار
عملیات جنگ الکترومغناطیس	موج الکترومغناطیس	طیف الکترومغناطیس
عملیات سایبرالکترومغناطیس	داده	طیف الکترومغناطیس

با تعریف چهار عمل ا صلی در عملیات شامل اختلال در عملکرد، ایجاد فریب، بهره‌برداری سایبرالکترومغناطیس، می‌توان تفکیک بین این بُعدهای رزمی را درنظر گرفت. و عملیات دفاعی بین بُعدهای عملیات سایبری، عملیات جنگ الکترومغناطیس و عملیات جدول ۹ این دسته بندی را نشان می‌دهد.

جدول (۹): مقایسه سه بُعد عملیات از نظر بخش های عمده عملیاتی.

بخش‌های عمده عملیات	عملیات سایبری	عملیات جنگ الکترومغناطیس	عملیات سایبرالکترومغناطیس
بهره برداری	اطلاعات سایبری	پشتیبانی جنگ الکترومغناطیس	TEMPESR
اختلال در عملکرد	رزم سایبری	حمله الکترومغناطیس(*)	TEMPEST نرم و EMI(*)
فریب	رزم سایبری	حمله الکترومغناطیس(*)	TEMPEST نرم مرتبه‌دوّم(*)
دفاع	پدافند سایبری	دفاع الکترومغناطیس	EMC

*: این موارد را می‌توان به عنوان حوزه سایبر در رزم لحاظ کرد

لازم به ذکر است که این عملیات سه‌گانه، علی‌رغم تفاوت‌های آشکار و حدود فاصل، دارای اشتراکاتی هستند که به صورت دوگانه با هم در ارتباط بوده و یک عملیات پیچیده را تشکیل می‌دهند. استفاده‌ی مؤثر، به‌موقع و همزمان از هر سه بُعد عملیات

درصورتی‌که با ملاحظات کامل به‌ویژه در تخصیص فرکانس صحنه نبرد همراه باشد می‌تواند برتری در صحنه نبرد را تضمین کند و توازن قوا در میدان نبرد را به شکل قابل توجهی تغییر دهد.

منابع:

[1] McGuffin, C., and Mitchell, P., "On domains: Cyber and the practice of warfare," International Journal, Vol. 3, No. 69, pp 394-412, 2014.
[2] FM 3-38 Cyber Electromagnetic Activities. United States Army, 2014.
[3] FM 3-12: Cyberspace Operations and Electromagnetic Warfe. United State Army, 2021.
[4] Gibson, W., Neuromancer. Ace, 1984.
[5] JP 1-02. US Department of Defense, 2010.
[6] AJP-3.10., "Allied joint Doctrine for Information Operation," NATO, 2009.
[7] Gurevich, V., "Cybernetic and Electromagnetic Impacts on Electronic Equipment: Do they have Anything in Common?," International Journal Of Research Studies in Electronics Engineering (IJRSEEE), Vol. 5, No. 3, pp 36-40, 2019.
[8] Moghaddasi, A., and Bagheri, M., "Automatic XSS Exploit Generation Using Grammatical Evolution," Journal of Electronical and Cyber Defense, Vol. 9, No. 2, pp 101-119, 2021.
[9] Mallick, M. G., Cyber Weapons: a weapon of war?. New Dehli: Vivekananda International Foindation, 2021.
[10] Winterfeld, S., and Andress, J., The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress, 2021.
[11] JP 3-13: Electronic Warfare. US Department of Defense, 2007.
[12] TEMPEST Equipment Selection Process. NATO, 1981.
[13] NACSIM 5000: TEMPEST Fundamentals. National Security Agency of United State, 2015.
[14] Goodman, C., An Introduction to TEMPEST. SANS Technology Institute, 2001.
[15] Boak, D. G., A History of U.S. Communications Security, National Security Agency of United States, 1973.
[16] Nabbali, T., and Perry , M., "Going for the throat: Carnivore in an ECHELON world," Computer Law & Security Review, Vol. 2, No. 20, pp 84-97, 2004.
[17] O'Neill, J., ECHELON: Somebody's Listening. Word Association, 2005.
[18] Maréchal, N., "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," Media and Communication, Vol. 1, No. 5, pp 29-41, 2017.
[19] Follorou, J., and Johannes, F., Révélations sur le Big Brother français. Le Monde, 2013.
[20] Committee in National Security Systems Adivisory Memorandum TEMPEST 01-02 Nonstop Evaluation Standard. National Security Agency of United States, 2002.
[21] NSA/CSS Regulation 90-6: Technical Security program. National Security Agency Of United States, 1999.
[22] Anderson, J. R., Security Engineering: A Guide to Building Dependable Distribute Systems. Wiley, 2008.
[23] Kuhn, G. M., and Anderson, J. R., "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," Internationl Workshop on Information Hiding. Berlin, 1998.
[24] Kuhn, G. M., Compromising emanations: Eavesdropping Risks of Computer Displays. Cambridge: University of Cambridge, 2003.
[25] Eck, v. W., "Electromagnetic radiation from video display units: An eavesdropping risk?," Computer & Security, Vol. 4, No. 4, pp269-286, 1985.
[26] Sekiguchi, H., and Seto, S., "Proposal of an Information Signal Measurment method in Display Image Contained in Electromagnetiv Noise Emanated from a Personal Computer," 2008 IEEE Instrumentation and Measurement Technology Conference, Victoria, BC, Canada, pp. 1859-1863, 2008.
[27] Kuhn, M. G., "Compromising Emanations of LCD TV sets," IEEE Transactions on Electromagnetic Compatibility, Vol. 3, No. 55, pp 564-570, 2013.
[28] Hayashi, Y.-i., Homma, N., Toriumi, Y., Takaya, K., and Aoki, T., "Remote Visualization of Screen Image Using a Pseudo-Antenna That Blends into Mobile Enviroment," IEEE

Transactions on Electromagnetic Compatibility, Vol. 59, No. 1, pp 24-33, 2017.
[29] Hidema, T., Takizawa, O., and Yamamura, A., "A Trial of the Intercaption of Display Image Using Emanation of Electromagnetic Wave," the institue of image Electronics Engineering of Japan, Vol. 25, No. 1/2, pp 213-223, 2005.
[30] Hayashi, Y., Homma, N., Miura, M., Aoki, T., and Sone, H., "A threat for Tablet PCs in Public Space: Remote Visualization of Screen Image Using EM Emanation," Computer and Communication Security, 2014.
[31] Lee, S. H., Choi, D. H., Sim, K., and Yook, J. G., "Information Recovery Using Electromagnetic Emanations From Display Devices Under Realistic Enviroment," IEEE Transactions on Electromagnetic Compatibility, Vol. 61, No. 4, pp 1098-1106, 2019.
[32] Thiele, E., Tempest for Eliza. the Guardian News, 2001.
[33] Guri, M., Kedma, G., Kachlon, A., and Elvoici, Y., "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequency," 9th International Conference on Malicious and Unwanted Software, 2014.
[34] Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., and Elovici, Y., "GSMem: Data Exfiltration from Air-Gapped Computers Over GSM Frequencies," 24th USENIX Security Symposium, Washington D.C., 2015.
[35] Guri, M., Monitz, M., and Elovici, Y., "USBee: Air-gap Covert-channel via Electromagnetic Emission from USB," 14th Annual Conference on Privacy, Security and Trust (PST), 2016.
[36] Cottais, E., Esteves, J. L., and Kasmi, C., "Second order soft-tempest in rf front-ends: Design and detection of polyglot modulations. Second order soft-tempest in rf front-ends," Desig International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018.
[37] Creswell, J. W., Qualitative inquiry and research design: Choosing among five approaches (4th ed.). thaousand Oaks, CA: Sage, 2014.
[38] Zheng, X. C., and Sun, H. M., "Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defende radio," Sensors and Mterials, Vol. 38, No. 8, pp. 2729-2743, 2020.
[39] Giray, S. M., "Anatomy of unmanned aerial vehicle hijacking with signal spoofing," 6th International Conference on Recent Advances in Space Technology (RAST), 2013.
[40] Kim, A., Wampler, B., Goppert, J. M., Hwang, I., and Aldeidge, H., "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," Infotech@Aerospace. California, 2012.