بخش دوم

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

بهره‌برداری از طیف الکترومغناطیس برای جنگ سایبری

به دلیل گسترش ارتباطات بی‌سیم در سطح شبکه‌های کامپیوتری خانگی، تجاری، و همچنین ارتباطات نظامی، بهره‌برداری از طیف الکترومغناطیس در این محیط با هدف جنگ سایبری اکنون بسیار ساده شده است. هدف اصلی از این بهره‌برداری در جنگ الکتروسایبر، نفوذ به یک شبکه کامپیوتری و نصب بدافزار بر روی تجهیزات ارتباطی و عملیاتی در یک محیط ارتباطی است.

حتی از این رویکرد می‌توان برای دریافت سیگنال‌های رادیویی خام استفاده کرد تا سپس با تحلیل آفلاین آن سیگنال‌ها بتوان اطلاعات رد و بدل شده را استخراج کرد یا در موقعیت‌های دیگری با دستکاری آن سیگنال‌ها و ارسال سیگنال‌های دستکاری شده عملیات فریب را بر علیه دشمن در محیط رزمی انجام داد.

به عنوان مثال، نمونه حملات شبکه ایرگپ که توسط دانشمندان دانشگاه بن‌گورین اسرائیل ارائه شده است، بعد از آلوده‌سازی یک ماشین به بدافزار با استفاده از آسیب‌پذیری‌های روز–صفر، مهاجم می‌تواند در ادامه اطلاعات جمع‌آوری شده توسط بدافزار را به محیط خارج از شبکه توسط کانال‌هایی از قبیل صوت و نور و گرما و ... ارسال و همچنین دریافت کند[i]. در جدول ۱، به نمونه حملات با محوریت بهره‌برداری از طیف الکترومغناطیس اشاره شده است:

جدول ۱: حملات الکتروسایبری به همراه تشریح نوع حمله

نوع حمله	تشریح نوع حمله
حملات مبتنی بر روز–صفر[1]	اساس حملات سایبری مهم جهان از قبیل حمله هدفمند بدافزار استاکس‌نت (Stuxnet) به زیرساخت غنی‌سازی اورانیوم ایران، بدافزار انرژی سیاه (Blackenergy) به زیرساخت انرژی و نظامی اوکراین، و بدافزارهای هدفمند دیگر بر روی استفاده از آسیب‌پذیری‌های روز–صفرم بود[ii] زیرا تنها راهی که یک مهاجم

[1] Zero-day Attacks

می‌تواند یک ماشین را مورد نفوذ قرار بدهد استفاده از آسیب‌پذیری‌هایی است که هنوز بر روی سامانه‌های قربانی شناسایی و در نتیجه وصله نشده‌اند. این دست آسیب‌پذیری‌ها را با عنوان آسیب‌پذیری‌های روزصفرم و کدهای بهره‌برداری آن‌ها با عنوان اکسپلویت‌های روزصفرم شناخته می‌شوند. به عنوان مثال، اگر بر روی ماشین قربانی سرویس آپاچی (Apache) وجود داشته باشد، مهاجم می‌تواند به سادگی با بهره‌برداری از یک آسیب پذیری روزصفرم بر روی این سرویس، ماشین قربانی را مورد نفوذ قرار بدهد [iii]. مهاجم، وقتی ماشین قربانی را با موفقیت مورد نفوذ قرار داد، می‌تواند در فاز پس از بهره‌برداری[1] عملیات‌های مختلفی از قبیل نصب بدافزار و دستکاری تنظیمات، سرقت اطلاعات و ... را انجام بدهد[iv].

بدافزارهای تزریق شده از هوا[2]

علاوه بر تمامی رویکردهای مستند شده به منظور تزریق بدافزار به سامانه‌های هدف از قبیل استفاده از آسیب‌پذیری‌های روز صفرم و همچنین آسیب‌پذیری‌های روز اول به منظور خرابکاری، احتمال تزریق بدافزار از هوا به واسطه ارتباطات بیسیم هم وجود دارد. به عنوان مثال، دانشگاه نظامی West Point آمریکا یک تفنگ کامپیوتری و آنتن[3] ایجاد کرده است که می‌تواند با ارائه اطلاعات به درون یک کانال ارتباطی باز یک پهپاد آن را از کار بیندازد. چنین ابزارهایی همچنین توسط روسیه در جنگ اوکراین برای مقابله با حملات پهپادی مورد استفاده قرار گرفت. در این نوع حملات، از لینک‌های رادیویی بی‌سیم برای تزریق بدافزار استفاده شده بود[v].

[1] Post-Exploitation Phase
[2] Air Injected Malware
[3] Computer and Antenna Riffle

جاسوسی/نشت داده‌های خام[1]	احتمالا عمومی‌ترین رویکرد به منظور دسترسی گرفتن از سامانه‌های مورد هدف کامپیوتری بهره‌برداری از ارتباطات بی‌سیم تحت استاندارد WiMAX، رادیوهای IP بی‌سیم[2]، Wi-Fi، Bluetooth، ارتباطات بیسیم شبکه سلولی[3] (موبایل به دکل مخابراتی[4]) و... باشد. از آنجایی که تمامی این پروتکل‌ها به خوبی تعریف شده‌اند و اطلاعات آن‌ها به صورت عمومی وجود دارد، طراحی حملات سایبری برای آن ها ساده‌تر است اگرچه کانال‌های رمزنگاری شده یک چالش جدی برای انجام حمله بر علیه آن‌ها ایجاد می‌کنند. به عنوان مثال، پلتفرم جاسوسی هوایی بی‌سیم (WASP)[5]، یک پهپاد جاسوسی برای آمریکا است که ۶ فوت طول و عرض بال‌های آن است. این پهپاد توانایی کرک پسوردهای شبکه تحت پروتکل Wi-Fi را دارد. این پهپاد همچنین توانایی عملکرد در قالب یک آنتن برای شبکه GSM را دارد که این امکان را به آن می‌دهد تا تماس‌ها و پیام‌های ارسال شده تحت شبکه GSM را شنود کند [vi].
پالس الکترومغناطیس انرژی بالا[6]	یک پالس الکترومغناطیسی انرژی بالا، که گاهی اوقات یک اختلال الکترومغناطیسی[7] گذرا هم خوانده می‌شود، یک انفجار انرژی الکترومغناطیسی است. نقطه خلق چنین پالسی می‌تواند رخدادهای طبیعی یا ساخت انسان باشد و می‌تواند در قالب یک فیلد مغناطیسی، الکتریکی یا تابشی رخ دهد یا در قالب جریان الکتریکی انجام شود مبتنی بر نوع منبعی که دارد. ایجاد اختلال به وسیله EMP می تواند به تجهیزات الکترونیکی آسیب برساند یا تخریب کند یا حتی در سطح

[1] Data Spying/Leakage
[2] Wireless IP Radio
[3] Air interface of the cellular connection
[4] Cell phone to the tower
[5] Wireless Aerial Surveillance Platform
[6] High Energy Electro Magnetic Pulse (EMP)
[7] Transient electromagnetic disturbance

انرژی‌های بالاتر می‌تواند اشیاء فیزیکی از قبیل ساختمان‌ها و ماشین‌ها را از بین ببرد. اگرچه این نوع ابزارها نمی‌توانند به صورت کامل تحت سلاح‌های سایبری قرار بگیرند اما به هر صورت از آن می‌توان برای از بین بردن تجهیزات الکترونیکی و کامپیوتری بهره برد. از همین روی، اکنون بسیاری از کشورها مانند روسیه، چین، آمریکا [vii] و اسرائیل به سمت ساخت چنین تسلیحاتی رفتند [viii]. به عنوان مثال، کره شمالی در آخرین دست آوردها خود توانسته است با موفقیت یک سلاح پالس الکترومغناطیسی ایجاد کند که زیرساخت الکترونیکی یک کشوری مانند آمریکا را از بین ببرد[ix]. یک تهدید دیگر با همین محوریت، برنامه Alabuga روسیه برای ایجاد تسلیحات پالس الکترومغناطیسی است[x]. با توجه به گزارش رسانه‌ها به نظر می رسد روسیه تحت این برنامه قصد تولید تسلیحات از نوع EMP دارد که بتواند یک محیط محدود را تحت تاثیر قرار دهد زیرا این تسلیحات می‌توانند برای از بین بردن زیرساخت تولید برق دشمن مورد استفاده قرار بگیرند یا در رویکرد دیگر تمامی تجهیزات الکترونیکی و کامپیوتری را از بین ببرند. این مسئله می‌تواند در کم‌ترین زمان ممکن آشوب برای دشمن ایجاد کند، چون تمامی توانایی او از بین خواهد رفت.

حافظه فرکانس رادیویی دیجیتال[1]

حافظه فرکانس رادیویی دیجیتال (DRFM)، یک متد الکترونیکی برای دریافت دیجیتالی و انتقال مجدد سیگنال‌های رادیویی است. این متد عموماً در جمینگ رادارها مورد استفاده قرار می‌گیرد، اگرچه از این متد می‌توان برای جمینگ ارتباطات تحت شبکه‌های سلولی را هم مورد هدف قرار داد.

[1] Digital Radio Frequency Memory

در صنایع دفاعی از DRFM برای ایجاد اهداف تقلبی روی رادار استفاده می‌شود. در این تکنیک عمل نمونه‌برداری[1] از سیگنالی‌های رادیویی با سرعت بالا صورت می‌گیرد تا در نتیجه بتوان با دقت بالایی آن را دیجیتالی و تحلیل/پردازش کرد.

به عبارت دیگر، اکنون سامانه‌های تجاری DRFM، سیگنال‌های آنالوگ را دریافت می‌کنند، آن‌ها را به سیگنالی‌های دیجیتالی تبدیل می‌کنند، سیگنال‌های دیجیتالی شده را پردازش، تحلیل و دستکاری می‌کنند، سپس سیگنال‌های دیجیتالی دستکاری شده را به آنالوگ تبدیل کرده و ارسال مجدد خواهند کرد [xi].

از آنجایی که سیگنال کپی و دستکاری شده توسط تجهیزات DRFM، دارای انطباق با سیگنال دریافتی از منبع اصلی است، رادار قادر نخواهد بود بین آن و دیگر سیگنال‌ها که به عنوان هدف دریافت و پردازش می‌کند، تفاوتی قائل شود. به هر صورت، می‌توانیم از این رویکرد برداشت کنیم که یک سامانه DRFM بر علیه یک گیرنده RF عمل حمله مرد میانی را انجام می‌دهد و مهاجم توانایی دستکاری ترافیک شبکه در یک کانال ارتباطی در سطح بیت ها با تزریق خود در کانال ارتباطی بین فرستنده و گیرنده را خواهد داشت [xi i].

ارتش و نیروی دریایی آمریکا در حال استفاده از سامانه‌های مبتنی بر فناوری DRFM برای تقویت توانایی‌های جمینگ و همچنین فریبکاری خود هستند. شایان ذکر است، فناوری Senior Suter توسعه داده شده توسط واحد Big Safari آمریکا بر پایه DRFM است.

[1] Sampling

نشت داده‌های خام از طریق شبکه‌های ایرگپ[1]

اولین مولفه‌ای که در ساختارهای نظامی باید مورد بررسی قرار بگیرد، نوع معماری شبکه‌بندی سامانه‌های کنترلی است. برخلاف معماری ارتباطی سامانه‌های اداری و سازمانی، شبکه‌بندی سامانه‌های کنترلی در محیط‌های نظامی به صورت ایزوله یا ایرگپ هستند، به این معنا که تجهیزات درون شبکه نظامی، ارتباط مستقیم به اینترنت جهانی ندارند. به این نوع شبکه‌ها، ایرگپ یا ایزوله گویند.

یکی از دلایل مهم پیکربندی شبکه به صورت ایرگپ اهمیت ساختارهای نظامی است زیرا به هر دلیلی اگر شخصی بتواند از راه دور به این تجهیزات و کلا شبکه زیرساخت حیاتی / نظامی دسترسی بگیرد و یا با بهره‌برداری از آسیب‌پذیری‌های روزصفرم به آن‌ها رخنه کند، و بر روی تجهیزات تغییراتی اعمال یا اختلالی ایجاد کند، فاجعه صورت خواهد گرفت.

به صورت خلاصه، از آنجایی که در این نوع معماری شبکه‌بندی، تجهیزات، سامانه‌های نظارتی و سامانه‌های ایستگاه–کاری به اینترنت جهانی دسترسی ندارند، تصور می‌شود نسبت به تهدیدات خارجی مانند اکسپلویت‌های راه‌دور ایمن هستند، چون از بیرون شبکه صنعتی کسی امکان برقراری ارتباط با آن‌ها را ندارد. حال اگر معماری شبکه‌بندی ساختار نظامی به درستی ایزوله / ایرگپ پیکربندی شود، حتی در صورت آلودگی سامانه‌ها به بدافزار از طریق هدف قرار دادن زنجیره تامین تجهیزات یا تهدیدات داخلی (یک نفوذی)، به دلیل اینکه ساختار ارتباطی سیستم‌ها به صورت ایرگپ و محلی است، ارتباط بین بدافزار در تجهیزات آلوده با سرور کنترل و فرماندهی خود ممکن نیست.

[1] Data Exfiltration Through the Airgap

از همین روی، بدافزار نه امکان سرقت اطلاعات از روی سیستم‌ها را دارد و نه اینکه می‌تواند فرمانی را از سرورهای کنترل و فرماندهی خود دریافت کند. اگرچه اکنون تحقیقاتی در دانشگاه بن‌گورین و تل‌آویو رژیم صهیونیستی صورت گرفته است که نشان می‌دهد معماری شبکه‌بندی ایرگپ یا ایزوله را می‌توان به واسطه کانال‌های جانبی دیگری مانند گرما، الکترومغناطیس، صوت، و ... دور زد تا در نتیجه بتوان اطلاعات را بین دو سیستم مجزا از یکدیگر انتقال داد یا به عبارت دیگر، بین دو ماشین بدون هیچ ارتباطی، تبادل اطلاعات انجام داد [xiii].

شایان ذکر است، معماری ایرگپ فقط می‌تواند ارتباط مرکز کنترل و فرماندهی با بدافزار در زیرساخت را غیرممکن یا سخت کند، اما طراحی بدافزاری مانند استاکس‌نت نشان داد، طراحان حرفه‌ای بدافزار با جمع‌آوری اطلاعات (جاسوسی) به صورت پسیو نسبت به محیط عملیاتی زیرساخت مورد نظر خود می‌توانند بدافزاری طراحی کنند که حتی بدون ارتباط با مرکز کنترل و فرماندهی عملیات خود را با موفقیت انجام بدهد[xiv].

با اینکه ساختار و معماری شبکه‌بندی سیستم‌های نظامی به صورت ایرگپ و ایزوله طراحی شده‌اند، اما این به معنای امنیت ۱۰۰ درصد نیست، چون راه‌های بسیار دیگری وجود دارد که بتوان یک بدافزار را در یک سیستم ایزوله وارد کرد[xv]، و با آن از طریق کانال‌های ارتباطی دیگر مانند صوت، الکترومغناطیس، نور و ... ارتباط موثر برقرار کرد [xvi]. از همین روی، این فرض که معماری شبکه‌بندی ایرگپ می‌توان از نفوذ به شبکه صنعتی جلوگیری کرد، ایده کاملا صحیحی نیست زیرا اکنون موارد نقض آن نمایش داده شده است [xvii].

نشت داده‌های خام به واسطه انتشار الکترومغناطیس[1]

تاریخچه نشت اطلاعات از طریق انتشار امواج الکترومغناطیسی (EMR) ناخواسته و همچنین مبحث محافظت بر علیه این نوع شیوه نشت اطلاعات به زمان معرفی پروژه محافظت مواد الکترونیکی مخابراتی بر علیه ارسال امواج مزاحم (TEMPEST)[2] بر می‌گردد که توسط آژانس امنیت ملی آمریکا ساخته شد [xviii]. در این پروژه اثبات شد که انتشار امواج الکترومغناطیسی (EMR) از صفحه نمایش کامپیوترها، کابل‌های داده، کابل‌های الکتریکی، صفحه کلید، و ... می‌توانند نظارت و همچنین ذخیره شوند. تجهیزات نظارتی TEMPEST شامل انواع مختلفی از گیرنده‌های حساس می‌شوند که می‌توانند طیف وسیعی از فرکانس‌ها را نظارت کنند و همچنین با استفاده از ترکیبی از سخت‌افزارها و نرم‌افزارها سیگنال‌های دریافتی را پردازش کرده و داده‌های خام را از آن استخراج کنند[xix].

سناریوهای بهره‌برداری از طیف الکترومغناطیسی در محیط نبرد

همانطور که پیش از این بحث شد، شبکه‌های کامپیوتری و متعاقباً شبکه‌های نظامی به شکل کامل در حال انتقال به پروتکل TCP/IP و همچنین الگوی ارتباطی بی‌سیم هستند. از همین روی، شانس بسیار زیادی وجود دارد که در محیط نبرد از تکنیک‌های شناخته شده بهره‌برداری از طیف الکترومغناطیسی برای انجام جنگ الکتروسایبری استفاده کرد. در قسمت زیر، برخی از این سناریوها توضیح داده شده است:

تکنیک هوابرد

یکی از کاربردی‌ترین سناریوهای جنگ الکتروسایبری استفاده از یک سامانه هوابرد برای انتقال بدافزار به درون فضای سایبری دشمن از طریق لینک‌های ارتباطی رادیویی است. در این نوع حمله، یک سامانه هوابرد

[1] Data Leakage Through Unintended EM Radiations
[2] Telecommunication Electronics Material Protected from Emanating Spurious Transmissions

مانند پهپاد می‌تواند این حمله را بر علیه ارتباطات و تجهیزات دشمن انجام بدهد، و در نهایت پس از نفوذ به آن سامانه‌ها، بر روی آن‌ها یک بدافزار نصب کند.

جعل IP

رویکرد بعدی ورود به یک شبکه رادیو نرم‌افزاری با استفاده از یک IP جعلی است تا در نتیجه با کنترل سیگنال‌ها در نحوه عملکرد سیستم مداخله کرد و کارهایی از قبیل نمایش اطلاعات غلط GPS یا ارسال پیام‌های اشتباه به دشمن بهره برد.

حملات DRFM

در رویکرد بعدی، می‌توان با استفاده از تکنیک‌هایی مانند DRFM، سیگنال‌های دستکاری شده به آنتن رادارهای دشمن ارسال کرد تا قادر به شناسایی پهپادها و جنگنده‌های ما نباشند، یا حتی در برخی موارد می‌توان با استفاده از این حمله هواپیماهای دشمن را به عنوان هواپیما مهاجم به سامانه پدافندی خودشان معرفی کرد، تا سامانه پدافندی جنگنده یا پهپاد خودشان را منهدم کند.

ایجاد BTS جعلی

در این رویکرد، مهاجم یک دکل BTS جعلی ایجاد خواهد کرد تا در نتیجه آن تلفن‌های همراه دشمنان مجبور به برقراری ارتباط با آن دکل BTS تقلبی شوند. هنگامی که آن ها به BTS تقلبی متصل شوند، مهاجم خواهد توانست گفتگوهای تلفنی آن‌ها را نظارت و شنود کند، پیام‌های ارسالی آن‌ها را بخواند، ایمیل‌ها و تمامی داده‌های انتقال داده شده توسط کاربر را دریافت کند.

تفنگ ضدپهپاد

در این رویکرد، مهاجم می‌تواند با استفاده از تفنگ‌های ضدپهپاد کانال ارتباطی یک پهپاد که هدف انجام عملیات‌های جاسوسی یا الکتروسایبری را دارد با سامانه کنترل و فرماندهی خود از بین ببرد، تا در نتیجه پهپاد یا سقوط کند یا نتواند عملیات خود را با موفقیت انجام بدهد.

جمینگ

در این رویکرد، مهاجم می‌تواند با انجام حملات جمینگ بر روی کانال‌های ارتباطی رادیویی در سطح ستون فقرات (WiMax یا IP Radio یا ...) یا در نقطه دسترسی (Bluetooth، WiFI یا ...) ارتباطات در سطح یک شبکه کامپیوتری را مختل کند. این موجب خواهد شد کامپیوترها نتوانند با یکدیگر ارتباط برقرار کنند.

بهره‌برداری از پروتکل‌های سیگنالینگ

یکی از مهم‌ترین رویکردهای نفوذگری، هک پروتکل‌های سیگنالینگ شبکه موبایل مانند SS7 و Diameter و ... است. به عنوان مثال، با بهره‌برداری از آسیب‌پذیری پروتکل SS7، می‌توان ارتباطات تحت نرم‌افزار تلگرام را شنود کرد. هک تلگرام به این روش، از طریق سو استفاده از یک آسیب‌پذیری امنیتی قدیمی در پروتکل‌های مخابراتی SS7 انجام می‌شود.

تکنیک و رویکردهای دیگر

رویکردها و تکنیک‌های دیگر مانند استفاده از آسیب‌پذیری‌های روز–صفرها، انجام حملات زنجیره تامین تجهیزات، پروژه TEMPEST، پروژه Suter، بدافزارها و ... هم وجود دارند که می‌توانند در محیط‌ها و سناریوهای ترکیبی مورد استفاده قرار بگیرند. به هر صورت، مسئله‌ای که اکنون واضح است، کاربرد و سطح تاثیرگذاری این حملات برای جمع‌آوری اطلاعات، جاسوسی و همچنین تخریب زیرساخت ارتباطی و تهاجمی دشمن در محیط نبرد است.

شایان ذکر است، اکنون یک هواپیمای نظامی توسط شرکت بوئینگ توسعه یافته است که یک هواپیما با محوریت مسائل اطلاعاتی، نظارتی و شناسایی (ISR) است که اوایل سال ۲۰۱۲ توسط اداره هوانوردی فدرال به بوئینگ سفارش داده شد. اساس و ساختار این هواپیما که با عنوان ایمارس[1] شناخته می‌شود، مبتنی بر هواپیمای تجاری بیچ‌کرفت کینگ‌ایر ۳۵۰ است[xx].

سری هواپیمای کینگ‌ایر ۳۵۰ یک پلتفرم ارزان قیمت است که می‌تواند برای ارتش ایالات متحده قابلیت‌های زیادی همچون جمع‌آوری و آنالیز هوشمند اطلاعات بلادرنگ محیط جنگی را فراهم کند. سیستم‌های نصب

[1] EMARSS

شده در این هواپیما می‌توانند اهداف سطحی را حتی در شرایط نور کم شناسایی و ردگیری کنند. در واقع عملیات نظارت و شناسایی با دقت بسیار بالا و در هر شرایط آب و هوایی انجام شود [xxi].

هواپیماهای اطلاعاتی، نظارتی و شناسایی را می‌توان بر اساس معیارهای مختلفی همچون نوع حسگرهای جمع‌آوری اطلاعات، شکل ظاهری، اندازه، پیکربندی، استمرار پروازی، سقف سرویس‌ها، نوع عملیات‌ها و میزان همکاری و به اشتراک‌گذاری داده‌ها دسته‌بندی کرد. با توجه به این دسته‌بندی‌ها، کاربردهای مختلفی نیز برای آن‌ها در نظر گرفته می‌شود که از مهم‌ترین آن‌ها می‌توان به بخش نظامی و گشت‌های مرزی، عملیات‌های جستجو و نجات، نقشه‌برداری و تحلیل تغییرات جغرافیایی، بررسی پیامدهای حوادث طبیعی و همچنین بخش کشاورزی اشاره کرد.

معمولا بسیاری از عملیات‌های هوایی اطلاعاتی، نظارتی و شناسایی از طریق سیستم‌های خودکار مانند ماهواره‌ها یا هواپیماهای بدون سرنشین مثل گلوبال‌هاوک[1] انجام می‌شود. با این حال تعداد محدودی از هواپیماهای سرنشین‌دار اطلاعاتی، نظارتی و شناسایی نیز وجود دارد. بیشتر این نوع هواپیماها برای کاربردهای ویژه یا شناسایی اهداف خاص طراحی شده‌اند. در واقع تعداد کمی از این هواپیماها قابلیت تغییر نوع عملیات را داشته و مجهز به حسگرهایی برای انجام ماموریت‌های مختلف هستند. هواپیمای ایمارس یکی از اینگونه پلتفرم‌ها است که ایالات متحده تاکنون از آن برای انجام عملیات در آفریقا، آمریکای لاتین، عراق و افغانستان استفاده کرده است [xxi i].

ارتش ایالات متحده ۲۴ فروند از این هواپیما را سفارش داده است که در حال حاضر بیش از نیمی از آن عملیاتی شده است. هواپیماهای سفارش داده شده شامل مدل اصلی و نسخه‌های G، M، S و V است که هرکدام از آن‌ها متناسب با سیستم‌ها و حسگرهای نصب شده، توانایی انجام عملیات‌های مربوط به خود را دارا هستند [xxi i i].

بدون توجه به نسخه‌های ایمارس، تمام آن‌ها مجهز به سیستم‌های ارتباطی و اویونیک پیشرفته هستند. در طراحی هواپیما سعی شده است از مدرن‌ترین ابزارآلات استفاده شود و به دلیل اهمیت اطلاع خدمه از محیط عملیاتی، برای هر یک از اپراتورهای هواپیما (خلبان و کمک او) یک جفت صفحه نمایش بزرگ در نظر گرفته

[1] Global Hawk

شده است. در ترکیب با این سیستم‌ها ابزارهای عملیاتی دیگری روی هواپیماها نصب است که از مهم‌ترین آن‌ها می‌توان به موارد زیر اشاره کرد[xxiv]:

- دوربین فیلم‌برداری MX-15 (ساخت شرکت L3) با قابلیت ضبط فیلم در روز و شب
- رادار و لیدار (رادار لیزری)
- سیستم هوش جغرافیایی (GeoINT)
- رادار روزنه مصنوعی (SAR)
- تصویربرداری مادون قرمز
- سیستم هویت هوایی دقیق
- سیستم هوشمند شناسایی عوارض زمینی
- سیستم تصویری نظارت بر محیط‌های وسیع
- لینک مخابرات ماهواره‌ای (ستکام)
- حسگرهای جمع‌آوری سیگنال (SIGINT)
- حسگرهای جمع‌آوری اطلاعات مخابراتی (COMINT)
- لینک‌های مخابراتی دید مستقیم (LoS) و دید غیر مستقیم (BLoS)
- فرستنده ADS-B
- سیستم ضدجاسوسی الکترونیک (ECMs)

در واقع معماری باز هسته اصلی اویونیک هواپیما، امکان تلفیق طیف وسیعی از حسگرها و نرم‌افزار را با توجه به نیازمندی‌های عملیات فراهم می‌کند. چالش اصلی در رابطه با این سیستم‌ها نحوه تلفیق داده‌های آن‌ها در ایستگاه‌های زمینی هوشمند ارتش است.

ارتش ایالات متحده در واحدهایی به نام سیستم زمینی مشترک توزیع شده (DCGS-A) می‌تواند اطلاعات ورودی از بیش از ۵۰۰ سیستم مختلف را جمع‌آوری، ترکیب، سازماندهی، نمایش و توزیع کند. این سیستم پس از تجزیه و تحلیل بلادرنگ داده‌های مختلف ورودی، آن‌ها را از طریق یک لینک اختصاصی برای نمایش به خدمه روی سیستم‌های اویونیک هواپیما ارائه می‌کند[xxv].

ایمارس برای شناسایی تهدید موشک‌های هدایت شونده با مادون قرمز به دو سیستمAAR-57 و AAR-47 (از محصولات شرکت BAE) مجهز شده است. سیستم هشدار موشک AAR-57 از حسگرهای الکترو-نوری استفاده می‌کند که می‌تواند با سرعت به تهدیدات موشکی (در مرحله وضعیت موشک) پاسخ دهد. این محصول می‌تواند روی پلتفرم‌های بال متحرک یا بال ثابت نصب و راه‌اندازی شود. سیستم AAR-47 نیز یک سامانه قدرتمند برای هشدار نزدیک شدن انواع موشک‌های هدایت‌شونده توسط مادون قرمز و لیزر است.

با توجه به رویکرد نرم‌افزاری در این محصول، تمام سخت‌افزارهای عرشه پرواز در نسخه‌های مختلف ایمارس برخلاف نوع حسگرهای هواپیما کاملا با هم مشابه هستند. ولی به هر صورت، با توجه به گسترش روش‌های هک و نفوذ به سیستم و همچنین پیامدهای خطرناک اینگونه اتفاقات در جنگ‌های آینده، ارتش ایالات متحده آمریکا توجه خاصی به سطح بالای امنیت در لایه‌های مختلف سیستم‌ها و شبکه‌های ایمارس داشته است.

لینک‌های انتقال داده در ایمارس توانایی ارسال و دریافت داده‌ها را حتی در فواصلی بسیار دور دارا هستند. تبادل سریع و امن اطلاعات در این لینک‌ها خیال ارتش را از ارتباط مداوم ایستگاه DCGS با هواپیما راحت می‌کند. ایمارس همچنین می‌تواند از مخابرات ماهواره‌ای مبتنی بر اینمارست برای برقراری ارتباط در نواحی خارج از پوشش DCGS استفاده کند. در واقع برای سیستم‌های اویونیک ایمارس تلفیقی از محصولات نظامی و تجاری است.

با این حال، هنوز مسئله امنیت طیف الکترومغناطیس اهمیت فراوانی دارد. چون اگر در این محصول، یک مولفه فقط دارای ضعف امنیتی باشد، می‌تواند عملکرد آن را تحت شعاع قرار بدهد. چون در ساخت آن از محصولات متنوع نرم‌افزاری و سخت‌افزاری استفاده شده است.

به هر صورت، از آنجایی که امروز بسیار از فناوری‌ها به سمت رویکردهای نرم‌افزار در حال حرکت هستند، باید به مسئله امنیت آن‌ها توجه ویژه داشت. به عنوان مثال، واشنگتن پست در گزارشی افشاگرانه، درباره‌ی جاسوسی آژانس اطلاعاتی ایالات متحده، CIA، از کشورهای دیگر با سوءاستفاده از دستگاه‌های رمزنگاری خبر داده است [xxvi].

از نیم قرن پیش تاکنون، حکومت‌ها در سرتاسر جهان برای حفظ امنیت و محرمانه ماندن پیام‌های ردوبدل شده میان جاسوس‌ها، دیپلمات‌ها، مقام‌های سیاسی و سربازهای خود به یک شرکت واحد اعتماد کرده‌اند. شرکت مذکور، موسوم به Crypto AG اولین قرارداد خود را در جریان جنگ جهانی دوم و با ارتش ایالات متحده‌ی آمریکا امضا کرد. آن‌ها که از قرارداد اول سود بالایی کسب کرده بودند، به‌سرعت به فرمان‌روای بازار

دستگاه‌های رمزنگاری تبدیل شدند. با گذشت دهه‌ها، فناوری دستگاه‌های رمزنگاری این شرکت از ماشین‌های مکانیکی به مدارهای الکترونیکی و امروزه به تراشه‌های سیلیکونی و نرم‌افزار، تکامل پیدا کرد.

شرکت سوئیسی کریپتو با فروش تجهیزات و فناوری‌های رمزنگاری به بیش از ۱۲۰ کشور جهان تا قرن ۲۱، میلیون‌ها دلار درآمد کسب کرد. از مشتریان مهم این شرکت می‌توان به کشورهایی در خاورمیانه، نیروهای نظامی حاضر در آمریکای لاتین، پاکستان و هند و حتی واتیکان اشاره کرد. هیچ‌یک از مشتریان نمی‌دانستند که شرکت کریپتو، درواقع تحت مالکیت محرمانه آژانس اطلاعاتی آمریکا موسوم به CIA قرار دارد که طی یک قرارداد طبقه‌بندی‌شده با سازمان‌های اطلاعاتی آلمان غربی، تصاحب شد. آژانس‌های اطلاعاتی، دستگاه‌های شرکت را دست‌کاری می‌کردند تا با سوءاستفاده از آن‌ها، پیام‌های رمزنگاری‌شده‌ی کشورهای دیگر را به آسانی رمزگشایی کنند.

جزئیات برنامه سوءاستفاده از شرکت کریپتو با عمری به‌اندازه چند دهه که شامل اسرار طبقه‌بندی شده‌ی جنگ سرد هم می‌شود، در تاریخچه‌ای جامع و محرمانه از عملیات سیا نگه‌داری شده است. واشنگتن پست در پروژه گزارش تحقیقاتی مشترک با هم‌تای آلمانی خود، ZDF، به اسناد دست پیدا کرده و گزارش حاضر را منتشر کرد. اسناد به‌دست آمده، حتی نام مقام‌های آمریکایی مرتبط با پرونده و مدیران اجرایی حاضر در شرکت کریپتو را فاش می‌کند. اطلاعاتی از ریشه‌های شرکت سوئیسی و همکاری با آژانس‌های اطلاعاتی و حتی درگیری‌های داخلی در اسناد سیا وجود دارد که کریپتو را از مسیر اصلی حرکت خارج کرد.

اسناد محرمانه و گزارش حاضر نشان می‌دهد که بی‌احتیاطی در همکاری با یک شرکت رمزنگاری چگونه باعث شد آمریکا از کشورهای بسیار متعدد و حتی متحدان خود، سوءاستفاده کند. آن‌ها از کشورها هزینه دریافت می‌کردند و هم‌زمان، اطلاعات‌شان را می‌دزدیدند. پروژه‌ی مذکور ابتدا به‌نام Thesaurus و سپس Rubicon و Minerva در سیا شناخته می‌شد و درمیان بزرگ‌ترین پروژه‌های این سازمان اطلاعاتی قرار دارد.

محافظت از سیستم‌های نظامی در مقابل حملات کانال جانبی

مبحث بعدی که باید به آن اهمیت داد، مسئله محافظت و ایجاد امنیت در تجهیزات الکترونیکی و اویونیک نظامی در مقابل تهدیدهایی مانند نفوذ، مهندسی معکوس و رمزگشایی است که از عوامل مهم در موفقیت یک عملیات نظامی به حساب می‌آیند. درحالی که در سال‌های اخیر جنگ سایبری و فناوری‌های مورد استفاده

در آن بسیار پیچیده شده است، اما همچنان روش‌هایی ساده و کم هزینه برای نفوذ در سیستم‌های الکترونیکی وجود دارد.

حملات کانال جانبی

حملات کانال جانبی[1]، یکی از این روش‌ها است که می‌تواند با هزینه کم برای خرید تجهیزات عادی آزمایشگاه‌های الکترونیک اجرا شود. این حملات در واقع توسط اطلاعات نشتی از ساختار فیزیکی یک سیستم رمزنگار انجام می‌شود. این اطلاعات از قبیل توان مصرفی، تشعشعات الکترومغناطیسی، اطلاعات زمانی یا حتی صوت هستند. این نوع حملات به دلیل سادگی اجرا و موثر بودن از اهمیت زیادی در حوزه رمزنگاری برخوردارند [xxvi i].

از جمله مهم‌ترین حملات کانال جانبی می‌توان به تحلیل ساده توان (SPA)[2] و تحلیل تفاضلی توان (DPA)[3] اشاره کرد. این روش‌های غیرتهاجمی از تحلیل توان مصرفی یک دستگاه که در حال اجرای عملیات‌های معمول خود شامل الگوریتم‌ها و کلیدهای رمزنگاری است، استفاده می‌کنند. راهکارهای ساده روش موثری برای مقابله با چنین تهدیدهایی نیستند و دستگاه نیازمند یک رویکرد لایه‌ای مقاوم است که داخل خود سیستم ادغام شده باشد.

تاریخچه حملات کانال جانبی – شنود سفارت مصر

اولین گزارش رسمی در رابطه با حملات کانال جانبی به سال ۱۹۶۵ میلادی بر می‌گردد. یکی از دانشمندان وقت ستاد ارتباطات دولت بریتانیا سال‌ها بعد گزارش داد که سازمان اطلاعات داخلی انگلستان (MI5) در تلاش برای کشف کدهای یک دستگاه رمزنگار به کار گرفته شده در سفارت مصر بوده است.

این دستگاه از نوع سایفر مکانیکی بوده و به دلیل محدودیت در توان محاسباتی برای کشف رمز، انجام آن با مانع مواجه شد. این شخص که دانشمندی در GCHQ بوده است، در ادامه پیشنهاد کرد یک میکروفن در کنار این دستگاه مکانیکی قرار دهند تا از طریق صدای کلیک تولید شده از سوی دستگاه بخشی از رمز آن کشف شود.

---

[1] Side-Channel Attacks
[2] Simple Power Analysis
[3] Differential Power Analysis

با گوش دادن به صدای کلیک‌های دستگاه، MI5 با موفقیت موقعیت اصلی ۲ یا ۳ روتور این ماشین مکانیکی را کشف کرد. از طریق این اطلاعات توان محاسباتی مورد نیاز برای شکستن رمز دستگاه به شدت کاهش یافت و MI5 توانست برای سال‌ها ارتباطات این سفارت را جاسوسی کند.

با وجود این حمله، سهم عمده پیشرفت در این حوزه مربوط به آقای کوچر است که در سال ۱۹۹۶ موفق به معرفی یک تکنیک موثر با نام «حمله زمانی در برابر پیاده‌سازی‌ها» شد. در این گزارش آقای کوچر گفته است که با اندازه‌گیری زمان عملیات کدگذاری خصوصی، می‌توان به اطلاعات بسیار ارزشمندی برای کشف رمز آن دست یافت. در سال‌های بعد نیز تحقیقات دانشمندان منجر به دستیابی به روش‌های مختلف دیگری در راستای حمله کانال جانبی شد [xxviii].

اهمیت حملات کانال جانبی

حفظ اطلاعات و سعی در کسب اطلاعات دشمن از مهمترین کارهایی است که در یک جنگ بایستی صورت بگیرد. برتری اطلاعاتی گاه برتری نظامی را به چالش می‌کشد و کاملا بی اثر می‌کند.

برای مثال در جنگ ۱۹۶۷ خاورمیانه بین کشورهای عربی و رژیم اشغال‌گر قدس میزان قوای نظامی اعراب به مراتب بیش از رژیم اشغال‌گر قدس بود و با توجه به اینکه اعراب حمایت شوروی را پشت سر خود داشتند چندان ترسی از حامیان بین‌المللی رژیم رژیم اشغال‌گر قدس نداشتند. اما برتری اطلاعاتی رژیم اشغال‌گر قدس و حمله ناگهانی او و نابودی نیروی هوایی اعراب سبب شکست اعراب در جنگ شد.

روش‌های معرفی شده در حملات کانال جانبی نشان داده است که کدگذاری اطلاعات به تنهایی برای امنیت در فضای سایبری کافی نبوده و سیستم‌های الکترونیکی در بخش‌های نظامی باید در مقابل تهدیدهای این چنینی مقاومت کافی را داشته باشند.

از آنجا که بسیاری از سیستم‌های الکترونیکی مانند تجهیزات هواپیما یا جنگ‌افزارهای زمینی و دریایی ممکن است در طول جنگ در اختیار دشمن قرار گیرند، مهندسان یکپارچه‌ساز سیستم باید تمهیدات حفاظتی لازم در مقابل دسترسی غیر مجاز دشمن (از طریق راهکارهایی مانند حملات کانال جانبی) به این سیستم‌ها را در نظر گیرند. دستگاه‌های مخابراتی و تجهیزات الکترونیکی قابل حمل از مستعدترین گزینه‌های حملات کانال جانبی به شمار می‌روند و دشمن می‌تواند از طریق آن‌ها علاوه بر جاسوسی، به جعل دستورات نظامی نیز بپردازد.

بنابراین تجهیزاتی که از رمزنگاری برای محافظت از انتقال اطلاعات حساس و امنیتی استفاده می‌کنند باید در برابر انواع مختلف حملات کانال جانبی از جمله تحلیل تفاضلی توان و تحلیل ساده توان مقاوم باشند. شاید جای تعجب نباشد که تراشه‌های سیلیکونی با کاربرد عمومی همچون FPGAها و ASICها به دلیل سهولت در دسترسی، بیشتر از همه مورد توجه مهاجمان حملات کانال جانبی هستند.

حملات تحلیل توان

امروزه تقریبا تمام مدارات مجتمع دیجیتالی با استفاده از فناوری CMOS ساخته می‌شوند. در صورتی که خروجی یک گیت CMOS تغییر وضعیت دهد، اثر آن را می‌توان در توان مصرفی تراشه مشاهده کرد. این توان مصرفی به راحتی از جریان ورودی به پایه Vdd قابل اندازه‌گیری خواهد بود.

از آنجایی که تغییر در حالات و فعالیت سوئیچینگ تراشه وابسته به داده اصلی است، می‌توان کلید مورد استفاده در الگوریتم رمزنگاری را از طریق خصوصیات آماری توان مصرفی دستگاه رمزنگار و با اعمال تعداد زیادی داده ورودی به دست آورد.

تحلیل ساده توان

در تکنیک تحلیل ساده توان[xxi x] اطلاعات جمع‌آوری شده از توان مصرفی دستگاه هدف در حین رمزنگاری مستقیما تفسیر می‌شود. به عبارت دیگر مهاجم سعی دارد با تعداد محدودی داده‌های اثر توان، تا حدودی به کلید یا اطلاعاتی پیرامون الگوریتم رمزنگاری سیستم دست یابد.

هرچند این روش در اجرا ساده است، اما نیازمند داشتن اطلاعاتی از جزئیات پیاده‌سازی دستگاه مورد حمله است. روش SPA زمانی مفید است که تنها یک یا تعداد محدودی از نمونه‌های تغییرات توان مصرفی دستگاه برای مجموعه ثابتی از داده‌های ورودی در دسترس است.

کشف کلید الگوریتم رمزنگاری RSA با استفاده از تحلیل توان. پیک سمت چپ نشان دهنده تغییرات توان CPU در حین اجرای گامی از الگوریتم بدون انجام عملیات ضرب و پیک سمت راست نشان‌دهنده توان مصرفی با انجام عملیات ضرب است که مقایسه این دو مقادیر صفر و یک کلید را مشخص می‌کند.

اگر چه این روش قادر به استخراج کلید رمزنگاری در محیط‌های پر نویز نیست، اما روشی کارآمد و موثر برای بدست آوردن داده‌های لازم به منظور کشف کلیدها است. تکنیک SPA به راحتی می‌تواند شاخه‌های شرطی

را در یک نرم‌افزار رمزنگار تشخیص دهد. برای پیش‌گیری از چنین حمله‌ای باید اطمینان حاصل کرد که اثری از مقادیر رمز و کلید در شاخه‌های شرطی نرم‌افزار وجود نداشته باشد.

حذف نقاط نفوذ مهم در الگوریتم‌ها و پیاده‌سازی سیستم اولین گام مقابله با SPA است. به طور خاص طراحان سیستم‌های رمزنگاری باید در الگوریتم‌های خود از مسیرهای اجرای ثابت استفاده کرده و تا حد ممکن از بکارگیری شاخه‌های مشروط جلوگیری کنند. علاوه بر استفاده از دستورالعمل‌ها و کدهای برنامه‌نویسی که بطور شناخته شده‌ای مصرف توان کمتری در سیستم ایجاد می‌کنند، می‌تواند حمله‌کنندگان را ناکام کند.

تحلیل تفاضلی توان

تحلیل تفاضلی توان همانند تحلیل ساده توان نوعی از حملات کانال جانبی است که در آن حمله‌کننده تغییرات مصرف توان الکتریکی یا انتشارات الکترومغناطیسی دستگاه هدف را تحت نظر می‌گیرد. تفاوت این روش با SPA در عدم نیاز به اطلاعات دقیق پیرامون دستگاه رمزنگار هدف و از طرف مقابل در اختیار داشتن تعداد زیاد نمونه از اندازه‌گیری‌های توان مصرفی دستگاه است. همچنین این روش برای استفاده در محیط‌هایی با نویز بالا نیز اثر بخش است[xxx].

روش DPA پیچیدگی بیشتری نسبت به SPA داشته و در آن معمولا از قابیت‌های تصحیح خطا و پردازش سیگنال استفاده می‌شود. حمله‌کننده با استفاده از این روش قادر خواهد بود به ازای ورودی‌های متفاوت و مشخص به دستگاه رمزنگار، کلید آن را کشف کند.

یک بلوک دیاگرام ساده از آنالیز تفاضلی توان

در حال حاضر استاندارد رمزنگاری پیشرفته (AES) برای کاربردهای صنعتی و نظامی وجود دارد. طراحان در بسیاری از سیستم‌های نظامی برای مخفی کردن اطلاعات تبادلی بین مبدا و مقصد از AES استفاده می‌کنند. اگر چه از طریق این استاندارد مهاجمان امکان شکستن کلید را با استفاده از روش‌های مرسوم ندارند، اما به شدت مستعد حملات تحلیل تفاضلی توان هستند. بنابراین طراحان باید اقدامات لازم برای مقابله با چنین تهدیدهایی را انجام دهند.

یکی از ساده‌ترین راهکارهای مواجهه با تحلیل تفاضلی توان کاهش نسبت سیگنال به نویز توان مصرفی دستگاه است. به عبارت دیگر کاهش تاثیر فرایندهای رمزگذاری در توان مصرفی دستگاه بهترین اقدام برای

جلوگیری از تهدیدهای تحلیل توان است. اضافه کردن مقداری نویز تصادفی به توان ورودی دستگاه می‌تواند کار مهاجمان را برای دستیابی به کلیدها بسیار دشوار کند.

علاوه بر این برخی از شرکت‌ها مانند Rambus ماژول‌هایی تحت عنوان «ضد اندازه گیری تحلیل تفاضلی توان» ارائه می‌دهند که با استفاده از آن‌ها در طراحی سخت‌افزاری دستگاه، می‌توان از حملات تحلیل توان جلوگیری کرد.

با توجه به اهمیت مخفی بودن اطلاعات مخابراتی در سیستم‌های نظامی، استفاده از روش‌های ضد حملات کانال جانبی از اهمیت زیادی برخوردار است. حتی اگر اطلاعات توان مصرفی دستگاه رمزنگار نیز در دسترس نباشد، دشمن می‌تواند با استفاده از تشعشعات الکترومغناطیسی دستگاه اقدام به حملات DPA کند. بنابراین شناخت کافی از روش‌های حملات کانال جانبی و بهره‌گیری از چند روش حافظتی به صورت همزمان بهترین ایده برای جلوگیری از چنین تهدیداتی است.

جنگ الکترونیک شناختی

امروزه تجهیزات فرکانس رادیویی قابل برنامه‌ریزی و دیجیتال که با نام رادیو نرم‌افزاری شناخته می‌شوند، روند رو به رشدی دارند. بر همین اساس رادارها می‌توانند به سرعت شکل موج را تغییر دهند و هویت و مشخصه منحصر به فردی روی پرواز ایجاد کنند.

در نتیجه در محیط‌های RF متراکم و رقابتی، کار فرستنده‌های دشمن برای موقعیت‌یابی، شناسایی، مسدود کردن و مغشوش کردن سخت‌تر می‌شود. از این‌رو امروزه تمرکز بر اعمال یادگیری ماشین بر طیف فرکانس رادیویی و جنگ الکترونیک (EW) یا همان جنگ الکترونیک شناختی (Cognitive EW) بیشتر شده است [xxxi].

آگاهی طیفی

هنگامیکه شما می‌توانید هزاران سیگنال در هر فرکانس در طیف RF ایجاد کنید، این مهم است بپرسید چه سیگنال‌های رادیویی دیگر مجموعه‌ای از فرکانس‌هایی را که به باند فرکانس رادیویی من نزدیک هستند اشغال می‌کنند؟ طیف و ویژگی هر یک از این سیگنال‌ها چیست؟ به عبارت دیگر طراح یک سیستم رادیویی باید از محیط عملیاتی دستگاه به لحاظ طیف‌های فرکانسی شناخت کامل داشته باشد.

یک گام مهم در راستای این مسیر، آگاهی طیفی است که یکی از اهداف برنامه سیستم‌های یادگیری ماشین RF در آژانس تحقیقات پیشرفته ایالات متحده است. دارپا این برنامه را بر پایه «نسل جدیدی از سیستم‌های RF که هدف محور هستند و می‌توانند از داده‌ها آموزش ببینند» طراحی کرده است. این یکی از چند برنامه‌ایست که به رابطه یادگیری ماشین و RF اشاره دارد.

برای دستیابی به مفهوم اطلاعات طیفی، دارپا قصد دارد الگوریتم‌ها و روش‌های پایه را که وظیفه اعمال یادگیری ماشین به طیف RF را دارند، توسعه دهد. در سطح بالاتر، دارپا می‌خواهد آگاهی از سیگنال RF را به عنوان وسیله‌ای برای گسترش ظرفیت منابع طیف فرکانسی از طریق بهبود اشتراک‌گذاری طیفی دنبال کند [xxxi].

رادیو شناختی

زمانیکه در رابطه با رادیو شناختی صحبت می‌کنیم در واقع در مورد توانایی درک محیط اطراف شامل تشخیص خودکار سیگنال‌های دوستانه از سیگنال‌های دشمن، تشخیص تهدیدات جمینگ و سپس عملیات انتقال به فرکانس‌های مختلف برای جلوگیری از حمله جمینگ صحبت می‌کنیم. اغلب چنین عملیاتی را با اصطلاح «رادیو انطباقی» نامگذاری می‌کنند.

در واقع رادیو شناختی یک فناوری مفید است که پیشرفت قابل توجهی در زمینه استفاده مؤثر از طیف فرکانسی به ارمغان می‌آورد. طراحی این فناوری به گونه‌ایست که با تغییر پارامترهای رادیویی، از طیف فرکانسی موجود استفاده بهینه را می‌برد.

یکی از مهمترین اهداف رادیو شناختی، قابلیت دسترسی به طیف است. با توجه به بررسی‌های انجام شده، بخش عمده‌ای از هر باند فرکانسی که به کاربران اختصاص داده می‌شود، بدون استفاده باقی می‌ماند.

رادیو شناختی این توانایی را دارد که از بخش‌های بدون استفاده طیف که به حفره‌های طیف معروف هستند، استفاده کند. بنابراین، رادیوشناختی یک فناوری مخابرات بی‌سیم هوشمند است که از محیط بیرونی خود آگاه است و با توجه به آن، پارامترهای عملیاتی خود از قبیل توان ارسالی، فرکانس حامل و روش مدولاسیون را تنظیم می‌کند تا بتواند هر زمان و در هر مکان که احتیاج شد، مخابره قابل اطمینانی داشته باشد. از آنجایی که این مساله نوعی استدلال و یادگیری است، می‌توان برای هوشمندسازی آن از الگوریتم‌های یادگیری ماشین استفاده کرد.

از آنجا که دشمن همیشه سعی دارد ارتباطات را از بین ببرد، رادیو شناختی باید یک قدم جلوتر از دشمن باشد و همیشه در طول زمان بهبود یابد. به دلیل اینکه سیستم‌های شناختی می‌توانند سریعتر از انسان‌ها واکنش نشان دهند، بنابراین برای جلوگیری از حملات مخرب و بازیابی لینک ارتباطات با حداقل زمان خرابی، یک قدم جلوتر از هر دشمن بالقوه است. در سیستم‌های جنگ الکترونیک شناختی نیز همین رویکرد وجود دارد، به‌طوریکه سیستم جنگ الکترونیک هوشمندتر و با سرعت بیشتر با تهدیدات و تداخل تطبیق می‌شود [xxxiii].

جنگ الکترونیک شناختی

جنگ الکترونیک یا جنگال اصطلاحی نظامی و بیانگر کاربرد الکترونیک و امواج الکترومغناطیس در نبردها است و شامل ارتباطات رادیویی، ایجاد اختلال در ارتباطات رادیویی دشمن و شنود گفتگوهای دشمن است. از این‌رو با ارائه فناوری رادیو شناختی، هوشمندسازی جنگ الکترونیک می‌تواند بسیار مفید باشد. به همین دلیل در سال‌های اخیر محققان با به کار بردن روش‌های هوش مصنوعی و یادگیری ماشین در تلاش برای ارائه فناوری‌های جنگ الکترونیک شناختی هستند.

جنگ الکترونیک شناختی، باید بتواند در عین نداشتن ذره‌ای شناخت از سامانه‌های دشمن، وارد محیط شود، سامانه‌ها را شناسایی کند و حتی اقدامات متقابل موردنیاز را به سرعت پیاده‌سازی کند. شناخت در این محیط شامل استفاده از آموزش ماشین برای ساخت سامانه‌های هوشمندتر است. این سامانه‌ها باید بتوانند سامانه‌های مقابل را تحریک کرده و با توجه به واکنش آن‌ها، ضمن تحمل کمترین آسیب به‌طور خودکار آموزش ببینند و به سرعت راهکار مقابله را کشف کنند [xxxiv].

مدیر پردازش حسگر و استخراج شرکت BAE Systems می‌گوید: «درگذشته هنگامی‌که نیروها وارد یک صحنه نبرد شده و با سیگنال‌های مختل‌کننده روبه‌رو می‌شدند، نوع سیگنال، فرکانس، طول‌موج و پهنای باند را جمع‌آوری می‌کردند و اطلاعات به آزمایشگاه منتقل می‌شد تا پس از بررسی اقدامات متقابل ارائه شود. بعد از چند ماه راه‌های مقابله در سامانه‌ها پیاده‌سازی می‌شد. پیشرفت نرم‌افزارها و تجهیزات رادیویی قابل‌برنامه‌ریزی مجدد، روش‌های قبلی را غیرممکن و بلااستفاده کرده و راه را برای گذر به نسل بعد با استفاده از یادگیری ماشین بازکرده است.»

نقش فناوری‌های جنگ الکترونیک شناختی

در حال حاضر محققان وزارت دفاع آمریکا در حال آزمایش فناوری‌های شناختی جنگ الکترونیک هستند. این فناوری‌ها در آینده می‌توانند سیستم‌های دشمن را به طور مستقل شناسایی کرده و بدون هیچ برنامه‌ریزی قبلی به مبارزه با آن‌ها بپردازند.

بر همین اساس آژانس تحقیقاتی دفاعی آمریکا (دارپا) در برخی پروژه‌های خود از هوش مصنوعی برای سیستم‌های جنگ الکترونیک استفاده کرده است. به عنوان نمونه پروژه اقدام متقابل راداری (ARC) و یادگیری رفتاری برای جنگ الکترونیک انطباقی (BLADE)، از سیستم‌های جنگ الکترونیک هوشمند استفاده کرده‌اند.

آقای پل تیلمن مدیر دفتر فناوری میکرو سیستم‌های دارپا، در این‌باره می‌گوید: «ما با استفاده از جنگ الکترونیک شناختی و شناسایی تهدیدات دشمن به سیستم‌ها نفوذ کرده تا در زمانی مناسب اقدام متقابل انجام دهیم.»[xxxv]

به عنوان مثال فناوری ARC می‌تواند سیستم‌های جنگ الکترونیک هوابرد را برای اقدامات مؤثر علیه رادارهای جدید و ناشناخته به صورت بلادرنگ آماده کند. در واقع این فناوری در برابر یک رادار جدید یا ناشناخته قادر به انجام فعالیت‌های زیر است.

- تفکیک سیگنال‌های رادار ناشناخته در برابر دیگر سیگنال‌ها
- کاهش تهدید از رادارهای ناشناخته
- ارسال سیگنال‌های متقابل و ارزیابی تاثیر آن‌ها روی رادار

همچنین به دلیل اینکه معماری این فناوری باز است، اجازه ورود، اصلاح و حذف ماژول‌های نرم‌افزاری توسط اپراتور داده می‌شود. علاوه بر این الگوریتم‌ها و نرم‌افزارهای پردازش سیگنال در فناوری ARC به گونه‌ای است که برای بکارگیری آن در نیروی هوایی و صنایع دفاعی نیاز به تغییرات سخت‌افزاری کلی نیست.

فناوری ARC به طور ویژه سیستم رادار را هدف قرار می‌دهد. در حالیکه پروژه BLADE با توسعه روش‌ها و الگوریتم‌های یادگیری ماشین، به‌سرعت تهدیدات رادیویی جدید را تشخیص داده و با ترکیب اقدامات متقابل جدید، خسارت جنگی را بر اساس مشاهدات هوایی به صورت دقیق ارزیابی می‌کند. هدف از طراحی این فناوری مقابله با تهدیدات ارتباطات بی‌سیم جدید و پویا در محیط‌های تاکتیکی است. علاوه بر این فناوری BLADE می‌تواند سیستم‌های ارتباطی بی‌سیم را با هدف متوقف کردن پخش اطلاعات زیر نظر بگیرد.

آقای تیلمن در رابطه با کاربرد هوش مصنوعی در سیستم‌های جنگ الکترونیک می‌گوید: «جامعه باید به این باور برسد که هوش مصنوعی می‌تواند به عنوان یک مساله مهم در جنگ الکترونیک دخیل باشد. با شروع تحقیقات دارپا در مورد فناوری‌های طیف‌های شناختی، بسیاری از افراد کاربرد هوش مصنوعی در جنگ الکترونیک را غیرضروری می‌دانستند. اما ما نشان دادیم که به کارگیری هوش مصنوعی بسیاری از مشکلات را رفع می‌کند زیرا ممکن است لازم باشد یک مقابله به دور از انتظار یا بدون برنامه‌ریزی قبلی انجام شود که در اینصورت باید بتوان از مشاهدات استفاده کرد. ما به جامعه نشان می‌دهیم که با رشد سریع نوآوری‌های فنی، هوش مصنوعی یک پاسخ حقیقی به چگونگی مبارزه با دشمنان در طیف فرکانس رادیویی است.» [xxxvi]
طبق گفته کارشناسان، ارتش ایالت متحده اغلب در استفاده از هوش مصنوعی در میدان جنگ احتیاط می‌کند. زیرا ممکن است تصمیم‌گیری در آن شرایط عواقب ناگواری داشته باشد. اما مدیران دارپا معتقدند که جنگ الکترونیک در فناوری‌های شناختی نقش مهمی دارد. از نظر آن‌ها میدان جنگ الکترونیک می‌تواند محیطی برای بهبود قابلیت‌های هوش مصنوعی باشد. اثرات مخرب ناشی از تصمیم‌گیری سیستم‌های جنگ الکترونیک هوشمند بسیار پایین است زیرا به سرعت اشتباهات خود را تصحیح می‌کنند.

به ادعای مقامات نظامی آمریکایی، در صورت تصمیم‌گیری نادرست از سوی سیستم هوشمند، از یک نیروی انسانی برای جبران اشتباه استفاده می‌شود؛ اما آقای تیلمن اینچنین استدلال می‌کند: «سیستم‌های شناختی جنگ الکترونیک می‌توانند کاملاً مستقل باشند. در یک مقطع، شما می‌توانید از یک انسان استفاده کنید. در ابتدا ارتش سیستم‌های راداری و ارتباطی دشمن را بررسی می‌کند تا بتواند حرکت متقابلی انجام دهد و سپس فناوری‌های جنگ الکترونیک را برای شناسایی و مسدود کردن سیستم‌های دشمن برنامه‌ریزی می‌کند. وقتی سیستم‌های راداری و ارتباطی توسط سخت‌افزار آنالوگ تعریف می‌شوند، این مسئله به‌مراتب حساس‌تر خواهد بود؛ اما بسیاری از نیروهای ارتش اکنون سیستم‌هایشان را با هسته دیجیتال توسعه می‌دهند و به این معناست که داشتن یک کتابچه راهنمای سخت‌افزاری واقعاً کار درستی به نظر نمی‌رسد زیرا آنچه در نهایت در میدان جنگ دیده می‌شود ممکن است واقعاً چیزی نباشد که برای آن برنامه‌ریزی صورت گرفته است. سیستم‌های جنگ الکترونیکی می‌توانند با شرایط غیرمنتظره خود را سازگار کنند.»

اجرای یادگیری ماشین

طبق گفته تیلمن، شرکت دارپا مطالعات اولیه را روی مسائلی که تا حدودی در ماهیت ساده‌تر هستند، انجام داده است. در ادامه یک شبکه عصبی پیچشی برای درک نوع مدولاسیون یک سیگنال (مانند AM، FM یا

تغییر فاز) ساخته شد. این مطالعات نشان داد که سیستم یادگیری ماشین عملکرد بهتری نسبت به رویکردهای سنتی در هر نرخ سیگنال به نویز دارد. از این‌رو سیستم‌های یادگیری ماشین می‌توانند ویژگی‌های اضافه و اطلاعات خارج از طیف RF را برای کمک به درک بهتر ما از محیط سیگنال بیفزایند.

طبق گفته تیلمن، همانطور که پروژه هوش مصنوعی گوگل (Google AI) با بازی GO اثبات شده است، پس هوش مصنوعی می‌تواند در فضاهای بسیار بزرگ تصمیم‌گیری کند. او امیدوار است که از یادگیری ماشین نه‌تنها برای پردازش اطلاعات طیفی استفاده شود، بلکه این فناوری به ما در پاسخ دادن به سوالاتی نظیر چه طیفی را باید بررسی و ضبط کرد؟ و همچنین تعیین زمان و مکان جستجوی آن کمک کند [xxxvi i]. از این‌رو یک سیستم شناختی قادر به یادگیری به صورت بلادرنگ است. چنین سیستمی می‌تواند آنچه را که می‌بیند (سیگنال‌هایی که دریافت می‌کند) یا آنچه را که می‌فرستند را بر اساس تجربه‌های کسب شده تغییر دهد. طبق گفته دارپا این قابلیت تصمیم‌گیری را می‌توان یک پیشرفت عمده نسبت به سیستم‌های RF سنتی که در آن فرکانس‌ها و جهت‌های فضایی صرف نظر از محیط عملیاتی اغلب دریک دنباله پیوسته اسکن می‌شوند، محسوب کرد. سیستم‌های سنتی درک کمی از آنچه که در طیف اتفاق می‌افتد دارند. همچنین سیگنال‌های تهدید ممکن است در یک ناحیه یا باند فرکانسی غیرمعمول باشند؛ اما از برنامه یادگیری ماشین انتظار می‌رود که سیگنال‌های غیر منتظره را نیز شناسایی کند.

سیستم‌های RF امروزی از استدلال‌های مبتنی بر قواعدی که مشابه نسل اول سیستم‌های هوش مصنوعی هستند، استفاده می‌کنند. جان تامپسون مدیر سیستم‌های عملیاتی شرکت نورثروپ‌گرومن می‌گوید: «برای مثال اکثریت سیستم‌های اقدامات حمایت الکترونیک (ESM) از جداول جستجو استفاده می‌کنند. به این صورت که داده‌ها جمع‌آوری شده وارد هواپیما می‌شوند و نرم‌افزار سیگنال ورودی را با پاسخ مناسب مرتبط می‌کند. اما افزایش دیجیتال‌سازی قابلیت‌های رادار، نیاز به سیستم‌های جنگ الکترونیک شناختی و انطباقی را مستلزم کرده است.»

آقای تامپسون اضافه کرد: «نیروهای نظامی دیگر نمی‌توانند برای مدت طولانی تنها به پایگاه داده‌های تهدید از پیش تعریف شده برای تشخیص، شناسایی، موقعیت‌یابی و واکنش به موقع متکی باشند، زیرا فناوری‌های امروزه قادرند شکل موج تهدیدها را از طریق نرم‌افزار و بدون نیاز به سخت‌افزار مجدد تغییر دهند. در چنین شرایطی سیستم‌های شناختی کلید موفقیت عملیات‌های آینده هستند.»

مراجع

[i] https://cyber.bgu.ac.il/air-gap/

[ii] https://securityintelligence.com/zero-day-malware-poses-a-growing-threat/

[iii] https://securityintelligence.com/apache-struts-2-a-zero-day-quick-draw/

[iv] https://www.offensive-security.com/metasploit-unleashed/msf-post-exploitation/

[v] https://www.militaryaerospace.com/communications/article/16709112/todays-battle-for-the-electromagnetic-spectrum

[vi] https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/

[vii] https://www.forbes.com/sites/arielcohen/2019/04/05/whitehouse-prepares-to-face-emp-threat/#57c6dafe7e21

[viii] https://freebeacon.com/national-security/china-russia-building-super-emp-bombs-for-blackout-warfare/

[ix] https://www.economist.com/business/2017/09/09/americas-utilities-prepare-for-a-nuclear-threat-to-the-grid

[x] https://www.sans.org/reading-room/whitepapers/privacy/introductiontempest-981

[xi] https://web.archive.org/web/20190626075229/http://magazine.milcyber.org/stories/physicallayerjammingthreats

[xii] https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

[xiii] https://cyber.bgu.ac.il/air-gap/

[xiv] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[xv] https://pgjonline.com/next-generation-cyber-attacks-target-oil-and-gas-scada

[xvi] GreenbergAndy, 02 Jul 2018,Mind The Gap: This Researcher Steals Data With Noise, Light, And Magnets

[xvii] https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotelyview-computer-cellphone-screen-using-radio-waves/

[xviii] https://www.sans.org/reading-room/whitepapers/privacy/introductiontempest-981

[xix] https://climateviewer.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/

[xx] https://asc.army.mil/web/portfolio-item/iews-emars-mep-ped/

[xxi] Enhanced Medium Altitude Reconnaissance and Surveillance System

[xxii] http://interactive.aviationtoday.com/avionicsmagazine/june-july-2018/emarss-the-hawker-beechcraft-turned-spy-plane/

[xxiii] https://asc.army.mil/web/portfolio-item/iews-emars-mep-ped/

[xxiv] http://interactive.aviationtoday.com/avionicsmagazine/june-july-2018/emarss-the-hawker-beechcraft-turned-spy-plane/

[xxv] https://asc.army.mil/web/portfolio-item/iews-dcgs-a/

[xxvi] https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[xxvii] https://www.csoonline.com/article/3388647/what-is-a-side-channel-attack-how-these-end-runs-around-encryption-put-everyone-at-risk.html

[xxviii] Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems

[xxix] https://link.springer.com/chapter/10.1007/978-0-387-38162-6_5

[xxx] https://link.springer.com/chapter/10.1007/978-0-387-38162-6_6

[xxxi] https://link.springer.com/chapter/10.1007/978-1-4020-5979-7_18

[xxxii] https://www.crows.org/news/416635/Cognitive-Electronic-Warfare-Radio-Frequency-Spectrum-Meets-Machine-Learning.htm

[xxxiii] https://ieeexplore.ieee.org/document/5783948/

[xxxiv] https://www.baesystems.com/en-us/definition/what-is-cognitive-electronic-warfare

[xxxv] https://www.afcea.org/content/smarter-ai-electronic-warfare

[xxxvi] https://www.popularmechanics.com/military/research/news/a22834/darpa-ai-defeat-enemy-radar/

[xxxvii] http://interactive.aviationtoday.com/avionicsmagazine/august-september-2018/cognitive-electronic-warfare-radio-frequency-spectrum-meets-machine-learning/