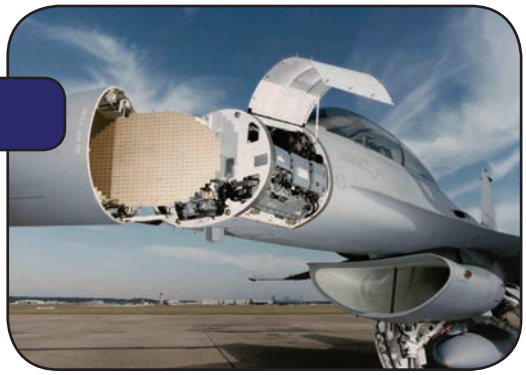
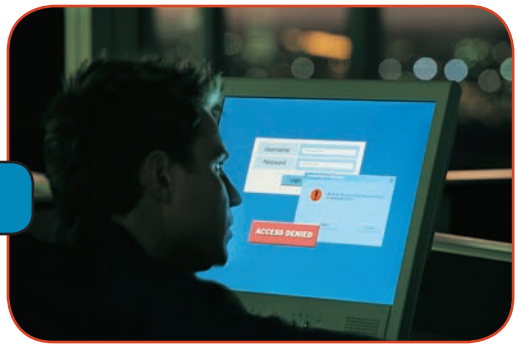
صاحب امتیاز:
مرکز تحقیقات سیاست علمی کشور
وزارت علوم، تحقیقات و فناوری
مدیر مسئول: حمید امیدوار
سردبیر: محمد حسن زاده
دستیار سردبیر: طاهره بزرگ‌بیگدلی
ویراستار: آزیتا منوچهری قشقایی
مدیراجرایی: فاطمه خسروانی
روابط عمومی: حسن چشمی
اعضای تحریریه:
حسن چشمی، فاطمه خسروانی
آزیتا منوچهری قشقایی
فریبا نیک‌سیر
همکاران این شماره:
مرضیه شفیعی، میثم امینی، مریم شفیعی
ناظرچاپ: سیاوش مشهدی سلمان
صفحه آرایی و طرح جلد: نسرین حاجی‌علی
حروفچین: مریم فلاح سفیدکوه
نشانی دفتر نشریه: تهران، میدان ونک، خیابان ملاصدرا، خیابان شیراز جنوبی، خیابان سهیل، شماره ۹، کدپستی:۱۴۳۵۸۹۴۴۶۱ – تلفن: ۸۸۰۳۶۱۴۴ داخلی ۱۰۳۴
پایگاه اینترنتی نشریه:
www.nrisp.ac.ir/daneshgar
پست الکترونیک نشریه:
daneshgar@nrisp.ac.ir

دوره جدید نشریه دانشگر با حمایت مالی معاونت پژوهشی وزارت علوم، تحقیقات و فناوری منتشر می‌شود. مسئولان محترم گروه‌های دانشجویی، مدارس و پژوهش‌سراها می‌توانند برای تهیه نشریه دانشگر با شرایط ویژه با دفتر تماس گیرند.



عملکرد جنگ الکتر

کاربردهای جنگ الکترونیک ۲۱



امنیت اطلاعا

دکتر علی‌اکبر جلالی، بنیانگذار روستای الکترونیکی ۵۱

چه کسی می‌تواند این قاتل ب

به نام خداوند علیم و حکیم

نبرد الکترونیک، پدیده‌ای که انسان را به یاد جنگی از نوع جدید می‌اندازد. با افزایش کاربرد فناوری اطلاعات و ارتباطات در عرصه‌های مختلف زندگی همه پدیده‌های فیزیکی با پسوندی الکترونیکی همراه شده است. مفاهیمی مانند پول الکترونیکی، آموزش الکترونیکی، بانکداری الکترونیکی، نامه الکترونیکی و نظایر آن تقریباً به صورت روزمره در تعامل‌های جاری افراد به کار می‌رود. اما مفهومی که این شماره از دانشگر به آن پرداخته است، مفهومی با ابعاد مختلف است. نبرد الکترونیک؛ از یک سو، موضوعی کاملاً فیزیکی که نمود مجازی و الکترونیکی پیدا کرده است، از سوی دیگر، اضافه کردن، صفت الکترونیکی به جنگ که موضوعی همه جانبه است، به خودی خود موضوعی چالش برانگیز است.

نبرد به معنای زورآزمایی برای نشان دادن قدرت خود به طرف مقابل است که شکل خصمانه آن جنگ نامیده می‌شود. در جنگ‌ها معمولاً از تمامی ادوات و امکانات لازم برای برتری‌جویی بر طرف مقابل استفاده می‌شود. البته ممکن است این امکانات برای دفاع از خود و کیان مملکت باشد که در آن حالت دفاع مشروع نامیده می‌شود. استفاده از ابزارهای پیشرفته در جنگ‌ها پدیده تازه‌ای نیست. اما آنچه که امروزه شگفت‌انگیز است، وارد شدن به جنگ تمام عیار در عرصه امواج و فضای عملیاتی الکترونیک است.

در نبرد الکترونیکی تمامی ابزارهای الکترونیکی و الکترومغناطیسی به کار برده می‌شود. ابزارهایی مانند هک کردن، سیستم‌های اطلاعاتی، دستیابی به اطلاعات حساس و محرمانه طرف مقابل، ایجاد فضای ترس و وحشت در بین جامعه از طریق محمل‌های الکترونیکی، آلوده کردن زیرسیستم‌های راهبری سامانه‌های حساس از جمله جنگ‌افزارهای نبرد الکترونیک هستند. بخشی از ابزارها نیز به از کارانداختن سیستم‌های تهاجمی و دفاعی طرف مقابل برمی‌گردد که از نمونه‌های آن به ایجاد اختلال در فرستنده‌ها و گیرنده‌های الکترونیک، رهگیری پیام‌ها و گمراه کردن سیستم ناوبری ادوات جنگی می‌توان اشاره کرد.

آگاهی از مقوله‌های مرتبط با نبرد الکترونیک می‌تواند به ارتقای آگاهی شهروندان از کارکرد و تأثیر فناوری‌های نوین کمک کند و از سوی دیگر، زمینه را برای همگانی شدن دغدغه‌های مرتبط با این امر در سطوح مختلف جامعه را فراهم می‌آورد. تمرکز این شماره از دانشگر بر این موضوع تلاشی است در این راستا. امیدواریم که مطالب ارائه شده بتواند به عنوان گامی هرچند کوچک در همگانی شدن مفاهیم نوین علم و فناوری مورد قبول جامعه دانشمند مخاطبان دانشگر واقع شود.

با آرزوی موفقیت

سردبیر

نبرد موج‌ها یا جنگ الکترونیکی

همراه با رشد فناوری‌های اطلاعاتی و ارتباطاتی چهره جنگ‌های نظامی و غیره نیز در دنیا تغییر کرده و انواع جدیدی از جنگ پا به عرصه وجود گذاشته است. جنگ الکترونیک، جنگ اینترنتی، جنگ رایانه‌ای، جنگ اطلاعاتی، جنگ رسانه‌ای، اصطلاحاتی هستند که این روزها در سطح بین‌الملل مطرح هستند.

گسترش روزافزون سیستم‌های الکترونیکی در حوزه‌های نظامی، غیرنظامی و تجاری موجب شده است تا بسیاری از فعالیت‌های عملیاتی، وابستگی کامل به مدارهای الکترونیکی داشته باشند. درحال حاضر بسیاری از بانک‌ها، مؤسسه‌های تجاری، سیستم‌های مخابراتی و در حوزه نظامی، سیستم‌های موشکی، شبکه‌های مخابراتی، مراکز کسب اطلاعات و سیستم‌های فرماندهی و کنترل، وابستگی بسیار زیادی به سیستم‌های الکترونیکی دارند.

باتوجه به این مطالب، می‌توانیم جنگال (کوتاه شده‌ی جنگ الکترونیک) را اینگونه تعریف کنیم:

" جنگ الکترونیک هنر و علمی است برای محافظت از استفاده‌ی دوستانه از طیف الکترومغناطیسی در عین ممانعت از استفاده‌ی خصمانه از آن."

براین اساس می‌توان شرایطی را فرض کرد که درآن سیستم‌های اطلاع‌رسانی مخابراتی، سیستم‌های رایانه‌ای و سیستم‌های الکترونیکی برخی از تجهیزات نظامی دریک جنگ الکترونیکی کارایی خود را ازدست بدهند.

اهداف عمده‌ی جنگ الکترونیک

الف- رهگیری امواج الکترومغناطیسی دشمن که به صورت عمدی یا سهوی پخش گردد؛

ب- ایجاد اختلال درطیف الکترومغناطیسی دشمن، به طوری که توانایی آن را خنثی کند؛

ج- حفاظت از طیف الکترومغناطیسی خودی در برابر جنگ الکترونیک دشمن، به نحوی که برتری توان نیروی خودی در این زمینه حفظ شود.

در این جنگ، سیستم‌های زیر به کار گرفته می‌شوند:

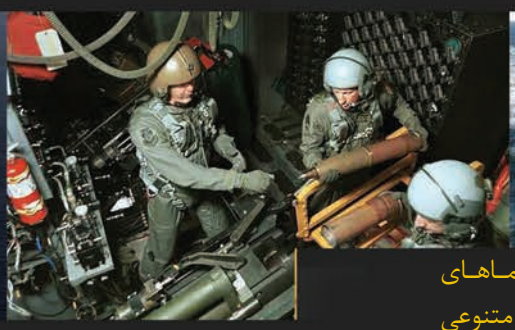
۱. سیستم‌های نظامی هشدار دهنده و شناسایی

مأموریت سیستم‌های هشداردهنده جلوگیری از غافلگیری تاکتیکی است اما سیستم‌های شناسایی مأموریت پیام‌رسانی درباره انجام یا احتمال انجام تهاجم و میزان نزدیکی، محل استقرار، حجم و نوع فعالیت و سلاح دشمن را به عهده دارند.

تاریخچه سیستم‌های نظامی هشداردهنده و شناسایی

مأموریت هشداردهنده‌ها علاوه بر عملیات شناسایی ، تحلیل و اتخاذ تصمیم مناسب، پس از دریافت اطلاعات لازم از انواع تجهیزات الکترونیک است. شیوه‌های هشدار از گذشته تاکنون دستخوش تحول فراوان گشته است. در جنگ‌های قدیم از نیروهای انسانی همچون دیده‌بان و از حیوانات برای شناسایی نزدیک نیروهای دشمن استفاده می‌شده است . در آستانه ورود به سال ۱۹۱۴ میلادی استفاده از دوربین و تلسکوپ و وسایل ارتباطی بی‌سیم و با سیم همچون ابزارهای جنگی به صورت امری عادی درآمد. در جنگ جهانی اول نورافکن‌های شناسایی و مُنوّرها، به منظور مشاهده هواپیماها و نیروهای مهاجم در شب و تجهیزات شنیداری مجهز به آژیرهای ویژه برای تعیین موقعیت هواپیماها به کار گرفته شد. در جنگ جهانی دوم اختراع‌هایی با تکنیک‌های پیشرفته‌تر مانند رادار و وسایل ارتباطی بی‌سیم، به ویژه در زمینه امواج با فرکانس بسیار بالا وارد میدان شد.

در این اوضاع و احوال بود که نیاز به سیستم‌های هشدار بهنگام نیز افزایش یافت. از این رو، همه توان تلاش‌های علمی و فناوری در راستای تأمین نیازهای نظامی به کار گرفته شد و در زمینه

ساماندهی، شناسایی و هشدار، به ویژه در ارتباط با هواپیماهای جت و ملخدار، بالگرد، زیردریایی‌ها، ماهواره‌ها و...، تجهیزات متنوعی ساخته شد. این سیستم‌ها ابزارهای گوناگونی، مثل تلویزیون، لیزر، شناسایی مغناطیسی و شنیداری، دستگاه‌های شناسایی مجهز به اشعه مادون قرمز دستگاه‌های شناسایی پرتوهای اتمی و تجهیزات شناسایی شیمیایی را به کار می‌گیرد.

۲. تجهیزات فرماندهی و کنترل

این تجهیزات بر فناوری رایانه مبتنی است که در خدمت نیروهای مسلح قرار می‌گیرد و در مأموریت‌ها جایگزین افراد

تجهیزات شناسایی ابداع شده

الف. در زمینه تجهیزات دیداری، تجهیزات بهتری برای دید در شب و جنگ شبانه ساخته شد. در تجهیزات شناسایی مجهز به اشعه مادون قرمز نیز تحولات چندی پدید آمد که از توانایی شناسایی نقاط داغ مثل موتور ماشین، هواپیما، موشک و آتش اردوگاه‌ها برخوردار بود. به طوری که می‌توانست اختلاف درجه حرارت اجسام گوناگون را تمیز دهد.

ب. تجهیزات شناسایی شنیداری برای شناسایی دشمن در زیر آب و بر فراز زمین ساخته شد.

ج. تجهیزات شناسایی امواج که در زمینه ره‌گیری امواج صوتی عبورکننده از لایه‌های خاک و شناسایی نفوذ افراد با تجهیزات دشمن کاربرد دارد.

د. تجهیزات شناسایی مغناطیسی که برای شناسایی اجسام بزرگ فلزی که تحرکاتشان بر هر نقطه‌ای از میدان مغناطیسی زمین تأثیرگذار است. مثل: زیردریایی‌ها، کاروان‌های نظامی فرازمینی، این تجهیزات هم به وسیله هواپیما قابل حمل هستند و هم قابلیت نصب درون زمین را دارند.

ه. تجهیزات شناسایی تشعشعات اتمی: که عبارت است از تجهیزات سنجش پرتوهای حاصل از انفجارهای اتمی. این تجهیزات در هواپیما، موشک‌ها و ماهواره‌ها کاربرد دارند.

و. تجهیزات شناسایی شیمیایی که قابلیت شناسایی بوها و ترشحات حاصل از جسم انسان را داراست که به میزان اندکی در فضا پخش می‌شود.

این تجهیزات به طور مخفیانه در میدان نبرد کار گذاشته می‌شود و در حوزه فعالیتش رفت وآمد نیروهای دشمن را شناسایی می‌کند.

می‌گردد؛ برخی از آنها اطلاعات را از سیستم‌های شناسایی دریافت و به منظور محاسبه و تعیین دقیق اماکن فعالیت دشمن و شناخت نوع و جهت این فعالیت آنها را تنظیم و تحلیل می‌کنند. در همین حال کامپیوترهای دیگری به انتشار و دریافت امواج راداری اقدام می‌کنند و به منظور تعیین سرچشمه فعالیت، با در نظر گرفتن توپوگرافی زمین، تجهیزات آنها را هدف دقیق آتش توپخانه قرار می‌دهد؛ به این ترتیب که با استفاده از داده‌های دستگاه‌های شناسایی، مختصات هدف را تعیین می‌کند، آنگاه فرمان لازم را به دستگاه‌های اتوماتیکی صادر می‌کند که کارشان تعیین سَمت و اجرای آتشباری است. خلاصه اینکه عملیات تبدیل اطلاعات و داده‌های سیستم‌های هشدار به فرامین روشن و قابل استفاده، مقدمه ورود به میدان جنگ الکترونیک است و مغزهای الکترونیک بخش لاینفک آنها محسوب می‌گردد.

۳. سیستم‌های ناوبری

هماهنگ با سیستم‌های پیشین، تجهیزات ناوبری نیز ناگزیر باید ارتقا می‌یافت و دقت هدف‌گیری سلاح‌های گوناگون تضمین می‌گردید. بسیاری از تجهیزات در جهت اهداف ناوبری و به کارگیری آنها در ناوهای فضایی و دریایی و انواع سلاح‌ها ارتقا یافت و در این فرایند سیستم‌های زیر اختراع شد:

الف. سیستم‌های ناوبری و هدایت الکترونیک چشمی با استفاده از فناوری تلویزیون: مثل بمب‌های هواپیماهای آمریکایی «وال آی » Walleye و« هابوس» Habos که هر دوی آنها به وسیله سیستم تلویزیونی هدایت می‌شود. نحوه عمل به این صورت است که خلبان هدفی را که روی صفحه تلویزیون نصب شده در نوک بمب درست مقابل هدف قرار می‌دهد، آنگاه به طور خودکار به سوی هدف شلیک می‌کند.

ب. سیستم ناوبری و هدایت الکترونیک مجهز به لیزر مانند بمب‌های هواپیمایی هوشمندآمریکایی هدایت شونده به وسیله اشعه لیزر؛ در این روش از دو هواپیما استفاده می‌شود. هواپیمای اول پرتو لیزر را به سوی هدف موردنظر هدایت می‌کند و هواپیمای دوم بمبی را شلیک می‌کند که در پی نور منعکس شده از اشعه لیزر حرکت می‌کند.

ج. تجهیزات ناوبری و هدایت الکترونیک مجهز به اشعه مادون قرمز که به وسیله نفر حمل می‌گردد و به طرف اشعه مادون قرمز منبعث از موتورهای هواپیما هدف‌گیری می‌شود.

د. تجهیزات هدایت راداری: این سیستم به یک مغز الکترونیک مجهز است که می‌تواند پس از دریافت اطلاعات مربوط به هدفی معین، هواپیما را با دقت بسیار بالا به سوی آن هدف هدایت کند. این در حالتی است که فعالیت خلبان به حوزه اطلاعات دریافتی از رادار مذکور محدود بوده باشد.

۴. ارتباطات الکترونیک

ارتباطات الکترونیک تشکیل می‌شود از دستگاه‌های ارتباطی باسیم و بی‌سیم به شکل ویژه که در ایجاد ارتباط میان تجهیزات ذکر شده و سلاح‌های متعلق به آنها و فرماندهی تاکتیکی و استراتژیکی از اهمیت ویژه‌ای برخوردار است. با آنکه این نوع از ارتباطات در گذشته شناخته شده بود، طبیعت جنگ الکترونیک پیشرفت دستگاه‌های الکترونیک را به منظور وصول به هدف‌های زیر قطعی ساخت:

کسب اطلاعات از منابع مربوط به پایگاه‌های فرماندهی و کنترل به منظور اتخاذ تصمیم و عکس‌العمل مناسب. این امر موجب پیدایش شبکه‌های ارتباطی بسیار پیچیده‌ای گردید که از پایگاه‌های تقویت و انتقال ارتباطات و شبکه‌های ماهواره‌ای نظامی برای زیر پوشش قرار دادن همه کره زمین برخوردار بود.

فناوری جنگ الکترونیک

ابزارهای الکترونیک در جنگ‌های جدید به صورت اصلی‌ترین

ابـزارهـای تـسـلط بر نیروها و سلاح‌ها در میان دو طرف متخاصم درآمده است، به طوری کـه بـدون وجـود ابـزارهـای الکـتـرونیک لازم، رسیدن به پیروزی برای آنها میسر نیست. از آنـجـا کـه بـرخـی از این تجهیزات ویژگی شناسایی شدن دارند به این معنا که به محض استفاده از آنها، جایگاه و کدهایشان شناسایی می‌گردد، جنگال وسـایـل ضـد آنـهـا را بـه کار می‌گیرد تا کارایی آنها را کاهش دهد. مانند شناخت ویژگی‌هـای شـنـاسـایـی شـونـدگـی رادار هـمـچـون فـرکـانـس امـواج نـاقـل، نمایش ضربان در ثانیه، میانگین تکرار ضربان در ثانیه، میانگین چرخش آنتن یـا مـیـانـگـیـن پـیـمـایـش آنـتـن در یـک دقـیـقـه، مـکـان رادار، شـکـل و حجم آنتن و ساماندهی رادار. هدف از این کار تعیین پایگاه‌های تجهیزات الکترونیک و تـحـلـیـل ویژگی‌های آنها برای دریافت اطلاعات لازم از نیروهای دشمن است تا بتوان از این راه وسایل لازم را برای مقابله با او تدارک دید. از ویـژگـی‌هـای بـرجـسـته این تجهیزات ضدالکترونیک، سری بودن فعالیت آنهاست. زیـرا ایـنـهـا مـثـل ـ تـجهیزات ارسال بی‌سیمی و راداری ـ دستگاه‌هایی هستند که در هنگام دریافت پیام قابل شناسایی نیستند.

مقابله با تجهیزات ضد الکترونیک

به مقتضای پیشرفت دائم فناوری نظامی، موضوع تنها به مجادله اراده‌ها میان اقدام‌ها و ابـزار الکـتـرونـیـک بـا اقـدام‌ها و تـجـهـیـزات ضـدالکـترونیک محدود نمی‌گردد، بلکه عـامـل تـازه‌ای بـه ایـن درگـیـری وارد گـشـتـه کـه هـدف آن افـزایش اقدام‌ها و تجهیزات الکترونیک به منظور مقابله با اقدام‌ها و تجهیزات ضدالکترونیک است. به عبارت دیگر ارتش‌ها توانسته‌اند اقدام‌ها و تجهیزات ضدالکترونیک را اخـتـراع کـنند که برخی جنبه سلبی و برخی دیگر جنبه ایجابی دارند.

عوامل سلبی به دو نوع استتار و فریب الکترونیک تقسیم می‌گردد.

الف. استتار الکترونیک

که به نوبه خود به دو گونه اقدام تقسیم می‌گردد:

۱. اخـتـفـای بـی‌سـیـمـی؛ اقدام‌هایی که به منظور اختفای فعالیت ارتباطات بی‌سـیـمـی انـجـام مـی‌گـیـرد، مثل به‌کارگیری تلگراف رادیویی با تجهیزات کدنویسی پـیـچیده در ارسال و دریافت و به کارگیری آنتن‌های رادیویی برای هدایت ارتباط در جهت دلخواه؛ ارسال به منظور گرفتن فرصت شناسایی جایگاه؛ سایت‌های ارسال از دشمن و مانور به وسیله فرکانس‌ها و شبکه‌های بی‌سیمی.

۲. اختفای راداری؛ شامل اقدام‌های امنیتی که برای استتار پرتوهای رادار انجام می‌گـردد. مـانند محدود ساختن زمان فعالیت رادارها که موجب کاهش فرصت دریافت پرتو آنها می‌گردد و روشـن کـردن سایت‌های رادار با کمترین نیروی خرج ممکن به طوری که بتواند هـدف‌هـای شـنـاسـایـی مـورد نـظـر را بـه انـجـام بـرسـانـد و در عـیـن حـال تـعـیـیـن دقـیـق مواضع آنها از سوی جاسوسی الکترونیک دشمن ممکن نباشد و دشمن در شناخت فرکانس‌های ثابت سایت‌ها و راه‌های کنترل دوباره این فرکانس‌ها گمراه شود.

ب. فریب الکترونیک

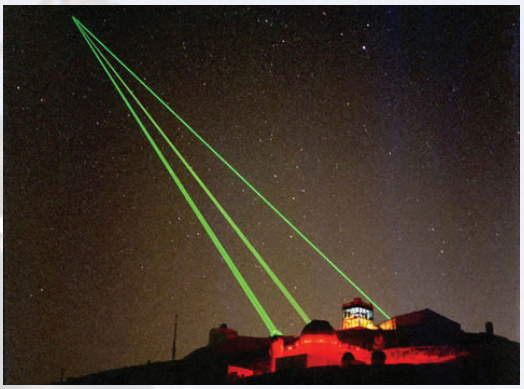
اقـدام‌هـایـی است که هدف آن به کارگیری منظم پرتوها و امواج وسـایـل الکـتـرونـیـک دوسـت بـرای گـمـراه سـاخـتـن دشـمـن نـسـبـت بـه شـکـل واقـعـی تـجـمـع نـیـروهـا و اهـداف بـه ویـژه در اثـنـای عملیات جنگی است. از مشهورترین شیوه‌های فریب الکترونیک به موارد زیر می‌توان اشاره کرد: بـه کارگیری تجهیزات الکترونیک در حین آماده‌باش عملیات جـنـگـی بـه مـنـظـور اسـتـتـار نیروها - در هنگام عملیات - و ایجاد این توهم در دشمن که در مـواضـع و نـیـروهـای خـودی هیچ‌گونه تغییری صورت نگرفته است؛ تنظیم تجهیزات الکـتـرونـیـک در راسـتـای دادن اطـلاعـات غـلط به نیروهای اطلاعاتی دشمن درباره اوضاع نـیـروهـا، مـراکـز فـرمـانـدهـی، پـایـگـاه‌هـای راداری خـودی و وانـمـود کـردن تـجـمـع وسـایـل الکـتـرونـیـک نـیـروهـای عـمـل کـنـنـده در مـنـاطـق عـمـلـیـاتـی ثـانـوی؛ ایـجـاد اخـتـلال در شـبـکـه‌هـای مـخابراتی دشمن با القای فرامین و

آموزش‌های گمراه کننده - این شیوه در هنگامی به کار گرفته می شود که دشمن وقت کافی برای تعیین درستی و نادرستی آنها را نداشته باشد.

عوامل ایجابی: اقدام‌ها و ابزارهایی هستند که به هدف ایجاد آشفتگی در تجهیزات الکترونیک دشمن و یا نابودی آنها به کار گرفته می‌شوند؛ و شامل موارد زیر است:

۱. پارازیت و فریب الکترونیک: هدف از این اقدام‌ها، استتار هدف‌های حقیقی از راه ایجاد اختلال در تجهیزات ارسال پیام دشمن و صفحه نمایش تجهیزات راداری آن به صورتی ویژه است. از جمله این اقدام‌ها موارد زیر است :

الف. پخش امواج با قدرت بالا به صورت پیوسته بر روی امواج مورد استفاده دشمن به طوری که اطلاع از کار آنها از طریق تجهیزاتی که هواپیماها به طور معمول حمل می‌کنند، امکان‌پذیر نیست. چه بسا که موج ارسال دشمن شناخته شده نیست و در این حالت انجام عملیات پارازیت در حوزه همه امواج صورت می‌گیرد. به منظور پرهیز از عملیات اختلال، رادارها



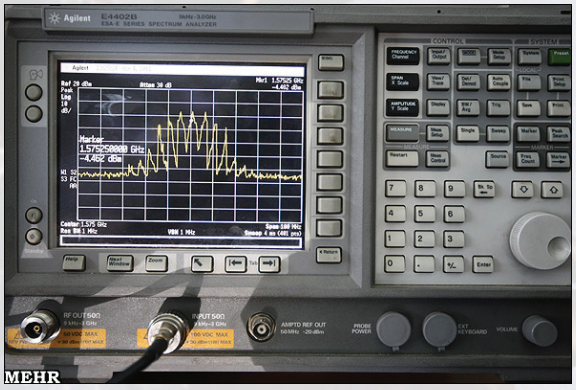
اقدام به تغییر امواج خود می‌کنند. این موضوع بر اهمیت ویژه سرعت انتقال امواج مثل اقدام‌های ضداختلال می‌افزاید؛ و این نیز به نوبه خودش منجر به ساخت تجهیزاتی گردیده که می‌تواند امواجش را با هر ضربانی تغییر دهد.

ب. اختلال از طریق محو، به این ترتیب که تجهیزات اختلال همه امواج را از راه ایجاد اختلال کوتاه‌مدت بر روی هر یک از امواج محو و این کار را به طور متناوب تکرار می‌کنند.

ج. اختلال از طریق تکرار: در این روش دستگاه‌های خودی رمزهای دشمن را دریافت و فرکانس‌های مشابهی را پخش می‌کنند که به دشمن اطلاعات غلط می‌دهد، یا چنان مداخله می‌کنند که در پاسخگویی به فرکانس‌ها تأخیر ساده‌ای صورت گیرد و موجب فریب دشمن شود. برای مقابله با این نوع اختلال از رمزهایی استفاده می‌شود که تغییر فرکانس‌های آنها از برنامه مشخصی پیروی می‌کند به طوری که تقلید از آنها ناممکن است.

د. افشاندن شمار فراوانی نوار فلزی در فضا به منظور ایجاد نوعی ((غبار الکترونیک)) که مشاهده هواپیما از میان آنها دشوار می‌گردد. چنین کاری از طریق پایه‌های ویژه‌ای انجام‌پذیر است که به وسیله هواپیما حمل می‌گردد. معایب این شیوه در این خلاصه می‌شود که این نوارها به سرعت در دنبال هواپیما آشکار می‌گردد و علاوه بر آن امکان تشخیص آنها از هواپیما نیز به دلیل اختلاف سرعت آنها وجود دارد.

ه. کاستن از کارایی رادارها از طریق مواد دارای خاصیت انعکاسی ضعیف یا استفاده از نقشه‌هایی که به میزان بسیار شامل انواع ویژه‌ای از روغن‌هایی است که توان جذب امواج الکترومغناطیسی را دارا هستند.



و. به کارگیری وسایل گمراه کننده گرمازا در مقابله با تجهیزاتی که دارای اشعه مادون قرمز هستند؛ مانند پرتاب بالون یا فوران‌های گرمایی به منظور گمراه‌سازی موشک‌های ضدهواپیمایی هدایت شونده به وسیله پرتو مادون قرمز.

۲. نابودسازی وسایل الکترونیک: هدف از این کار آن است که تجهیزات الکترونیک دشمن پس از تعیین جایگاه آنها، با به کارگیری وسایل شناسایی الکترونیک و دیگر

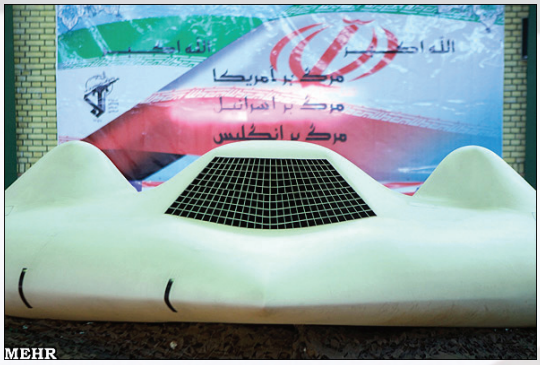
روش‌های معمول نظامی مورد حمله قرار گیرد. از سوی دیگر سلاح‌های تاکتیکی پیشرفته‌ای اختراع شده که خود هدایت کننده به سوی هدف‌های راداری هستند، مانند موشک «شرایک» که پرتوهای منبعث از آنتن رادار را دریافت می‌کند و آن را برای هدایت خودش به کار می‌گیرد و هدف را نابود می‌سازد.

امروزه مشهور است که هواپیماها و ماهواره‌های جاسوسی متعلق به دستگاه‌های اطلاعاتی دولت‌های بزرگ، نه تنها در زمان جنگ، بلکه در زمان صلح نیز فعال هستند و اطلاعات مورد نظرشان را درباره تأسیسات نظامی، صنعتی، اقتصادی، محصولات زراعی، جاری شدن سیلاب‌ها، مناطق و خشکسالی و دیگر اطلاعاتی که آنان را به ارزیابی وضعیت اقتصادی و نظامی کشورهای مورد نظرشان کمک می‌کند، گرد می‌آورند، و می‌کوشند تا بر پایه این اطلاعات به حساسیت‌های سیاسی آن کشور پی ببرند.

دستگاه‌های جاسوسی، متناسب با توان و امکاناتشان، انواع ابزارهای الکترونیکی را برای دریافت اطلاعات سرّی مورد نظرشان به کار می‌گیرند. از مهم‌ترین وسایل الکترونیک، وسایل قابل حمل زمینی مانند تجهیزات شناسایی بی‌سیمی و راداری زمینی و تجهیزات تصویربرداری با اشعه مادون قرمز قابل حمل به وسیله هواپیماها یا ماهواره‌های نظامی هستند.

توان ایران در جنگ الکترونیکی

توان جنگال ایران قبل از فرونشاندن پهپاد آمریکایی بارها در رزمایش‌های مختلف نظامی به معرض نمایش گذاشته شده بود. ایران نه‌تنها توانایی در اختیار گرفتن پهپاد را دارد بلکه از زمان جنگ ایران و عراق، با به پرواز درآوردن پهپاد به نام «تلاش»، زمینه‌ای را برای توسعه پهپادهای خود آغاز کرد. بعد از این جنگ، ایران روی بسیاری از انواع پهپادهای نظامی و چندکاره، کار کرد و اکنون ایران از توانایی ساخت پرنده بدون‌سرنشین یا UAV برخوردار است. در این میان می‌توان به انواع پهپادهای نوع ابابیل، خانواده مهاجر ۱، ۲، ۳ و ۴، خانواده فراز، خانواده صاعقه ۱ و ۲، پهپادهای ثاقب، کی دو، شاهین و سپهر و... اشاره کرد.



در رزمایش پدافند هوایی ثامن‌الحجج (ع) این توان ایران بارها آزمایش شد. در این رزمایش، جدیدترین سامانه‌های کشف غیرفعال و تجهیزات جنگ الکترونیک بومی ساخته شده در طیف‌های مختلف فرکانسی با موفقیت مورد آزمون قرار گرفت و نیروهای خودی نوعی اخلال در سامانه‌های هدایت اهداف پرنده دشمن فرضی ایجاد کردند. همچنین دیده‌بان‌ها، سامانه‌های پیشرفته ارتباطی و الکترونیکی خود را ارزیابی کردند و کارشناسان نظامی هم امنیت تبادل اطلاعات را مورد سنجش و ارزیابی قرار دادند.

دستگیری عبدالمالک ریگی نیز آغاز یکی از پیروزی‌های ایران در جنگی الکترونیک بود، به این معنا که صدا و سیستم‌های ارتباطی هواپیمایی که ریگی در آن بود، ردیابی و سپس با فشار نیروهای ایران هواپیما ناچار به فرود شده و عبدالمالک ریگی دستگیر شد.

رزمایش دریایی ولایت ۹۰ نیز که به مدت ۱۲ روز برگزار شد، گام دیگری در راستای تقویت توان عملیاتی ایران از جمله در زمینه جنگ الکترونیکی بود و در آن تجهیزات نوین تولید شده به دست متخصصان این نیرو و صنایع دفاعی کشور در زمینه جنگ الکترونیک در کنار سایر دستاوردهای نظامی ایران مورد آزمایش و بررسی قرار گرفت.

منابع:

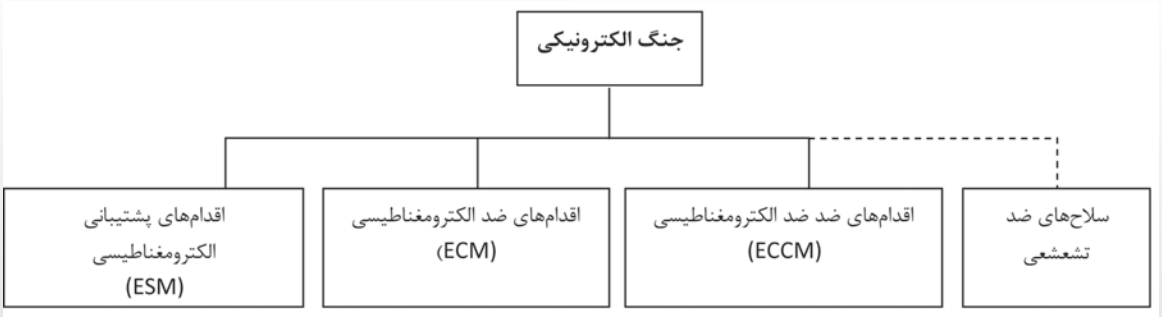
۱- آدامی، دیوید. (۱۳۸۵). جنگ الکترونیک. (برگردان، محمدمهدی نایبی و علی حرمتی). تهران: انتشارات علمی.

۲- بینش، عبدالحسین. (۱۳۸۷). جنگ الکترونیک. ماهنامه حصون. شماره ۱۵. تهران: پژوهشکده تحقیقات اسلامی.

۳- جنگال، مبنای نبرد درعصر جدید [homepage] ۱ اسفند ۱۳۹۰ [online] <www.Jamejamonline.ir> ۲ اسفند ۱۳۹۰.

عملکرد جنگ الکترونیک

جنگ الکترونیک هنر و علمی است برای محافظت از استفاده‌ی دوستانه از طیف الکترومغناطیسی در عین ممانعت از استفاده‌ی خصمانه از آن. طیف الکترومغناطیسی شامل بسامدهای DC طیف مرئی (و فراتر از آن) است و بنابراین جنگ الکترونیک (EW) طیف کامل بسامد رادیویی، طیف فروسرخ، نوری و فرابنفش را در بر می‌گیرد.



جنگ الکترونیکی به صورت کلاسیک به اقدام‌های پشتیبانی الکترونیکی، اقدام‌های ضد الکترونیکی و اقدام‌های ضد ضد الکترونیکی تقسیم شده است. سلاح‌های ضد تشعشعی جزئی از جنگ الکترونیکی به حساب نمی‌آمد.

مطابق شکل فوق جنگ الکترونیکی به صورت کلاسیک چنین طبقه‌بندی می‌شود:

- اقدام‌های پشتیبانی الکترومغناطیسی که بخش گیرنده‌ی جنگ الکترونیکی است.
- اقدام‌های ضد الکترومغناطیسی شامل اخلال، خاشاک و فلیر (شعله‌زن) است که به منظور مختل کردن سیستم‌های راداری، مخابرات نظامی و سلاح‌های جستجوگر گرما به کار می‌روند.

• اقدام‌های ضد ضد الکترومغناطیسی که شامل تمهیداتی است که در طراحی و عملیات سیستم‌های راداری و مخابرات نظامی در نظر گرفته می‌شود تا با اثرات مقابله کند.

سلاح‌های ضد تشعشع و انرژی هدایت شده بخشی از جنگ الکترونیک محسوب نمی‌شدند با اینکه ارتباط تنگاتنگی با جنگ الکترونیک دارند. آنها در قسمت سلاح‌ها قرار می‌گرفتند.

در سال‌های اخیر، زیر بخش‌های جنگ الکترونیک مطابق شکل زیر در بسیاری از کشورها مجدداً تعریف شده‌اند. در حال حاضر تعریف‌های پذیرفته شده در ناتو عبارتند از:

• پشتیبانی جنگ الکترونیک (ES) که همان ESM پیشین است.

•حمله‌ی الکترونیکی (EA) که ECM پیشین (اخلال، خاشاک، شعله‌زن) را در بر می‌گیرد، با این تفاوت که سلاح‌های ضد تشعشع و هدایت شده‌ی انرژی نیز به آن اضافه شده‌اند.

• حفاظت الکترونیکی (EP) که همان ECCM پیشین است.

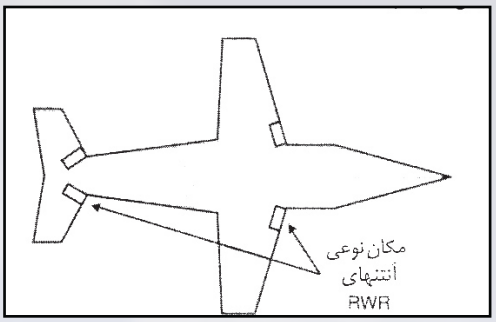
پشتیبانی جنگ الکترونیکی با مباحث جاسوسی سیگنالی شامل جاسوسی مخابراتی و جاسوسی الکترونیکی کاملاً تفاوت دارد، اگرچه تمام آنها به دریافت پیام‌های دشمن مربوط می‌شود. این تفاوت‌ها که با افزایش پیچیدگیِ سیگنال‌ها روز به روز نامشخص‌تر می‌شوند مربوط به مقتضیاتی است که با توجه به آنها پیام‌های ارسالی دشمن دریافت می‌شوند.

طبق تعاریف جاری ناتو، جنگ الکترونیکی به پشتیبانی الکترونیکی، حمله‌ی الکترونیکی و حفاظت الکترونیکی تقسیم می‌شود. حمله‌ی الکترونیکی در حال حاضر شامل سلاح‌های ضد تشعشع و سلاح‌های انرژی هدایت شده است.

آنتن‌ها

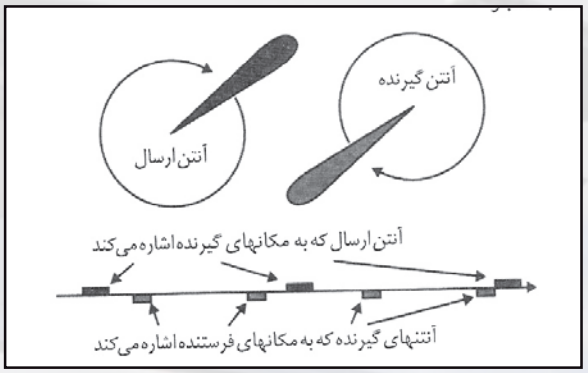
آنتن‌ها به انحای مختلف بر روی سیستم‌های جنگ الکترونیکی اثر می‌گذارند. بنابراین به اختصار نقش و قابلیت‌هایی از آنها آورده می‌شود. آنتن به هر وسیله‌ای اطلاق می‌شود که سیگنال‌های الکترونیکی (داخل کابل‌ها) را به امواج الکترومغناطیسی در فضای آزاد و یا برعکس تبدیل کند. انواع بسیار متنوعی از آنتن‌ها از نظر طراحی و اندازه، بسته به بسامد سیگنال‌هایی که با آنها کار می‌کنند و پارامترهای کاری آنها، وجود دارند. درعمل، هر آنتن می‌تواند سیگنال را هم ارسال و هم دریافت کند. در هر صورت آنتن‌های طراحی شده برای ارسال‌های پرقدرت باید بتوانند مقادیر زیادی توان را ضبط و ربط کند.

آنتن‌ها در سیستم‌های گیرنده بهره و جهت‌مندی را تأمین می‌کنند. در بسیاری از سیستم‌های جهت‌یاب، پارامترهای آنتن‌ها منابع اطلاعاتی هستند که از روی آنها جهت ورود سیگنال به دست می‌آید. در سیستم‌های اخلال‌گر، آنتن‌ها بهره و جهت‌مندی را در اختیار قرار می‌دهند. در گسیل‌گرهای تهدید کننده، به خصوص رادارها، الگوی بهره و مشخصات روبش آنتن فرستنده یکی از مهمترین راه‌ها را جهت شناسایی سیگنال تهدید کننده در اختیار قرار می‌دهد. روبش و قطبش آنتن‌های گسیل‌گر تهدید کننده امکان استفاده از بعضی اقدام‌های متقابل را به کاربر می‌دهد.



گیرنده‌ها

گیرنده‌ها در تمامی سیستم‌های جنگی الکترونیکی قسمت مهمی به شمار می‌آیند. انواع مختلفی از گیرنده‌ها وجود دارند و نقش آنها را مشخصه‌هایشان تعیین می‌کنند. گیرنده‌ی ایده‌آل جنگ الکترونیکی می‌تواند همه‌ی انواع سیگنال‌ها را در تمام بسامدها با حساسیت بسیار خوب در ۱۰۰ درصد اوقات دریافت کند و قادر خواهد بود چند سیگنال همزمان شامل سیگنال‌های خیلی ضعیف را در حضور سیگنال‌های قوی آشکار و وامدوله کند. همچنین گیرنده‌ی ایده‌آل ابعاد کوچک، وزن کم، قیمت ارزان و مصرف توان پایینی دارد.



عموماً از گیرنده‌های تصویری کریستالی و اندازه‌گیری لحظه‌ای بسامد (IFM) در سیستم‌های ارزان و میان قیمتی استفاده می‌شوند که درمحیط‌های از نظر پالسی چگال به کار می‌روند. هر دو گیرنده می‌توانند محدوده‌ی بزرگی از بسامد را به صورت ۱۰۰ درصد پوشش دهند اما قابلیت ضبط و ربط چند سیگنال همزمان را از هر نوعی ندارند. بنابراین یک سیگنال CW با قدرت بالا در هر کجایی از محدوده‌ی بسامدی آنها به شدت قابلیت آنها را در دریافت پالس‌ها کاهش می‌دهد. همچنین آنها حساسیت کمی دارند، از این رو آنها در برابر سیگنال‌های بسیار قوی بهترین عملکرد را دارند. در سیستم‌های جدید از آنها به همراه گیرنده‌هایی با پهنای باند کم استفاده می‌کنند تا بتوان موقعیت‌های مشکل را ضبط و ربط کرد.

از آنجا که سیستم‌های تنظیم شده‌ی ثابت و گیرنده‌های سوپر هترودین از نوع باند باریک هستند، آنها عمدتاً همراه با گیرنده‌های دیگر استفاده می‌شوند تا سیگنال‌های همزمان جداسازی شوند و حساسیت سیستم بهبود یابد. گیرنده‌های تنظیم شده‌ی بسامدهای رادیویی (TRF) نیز سیگنال‌های همزمان باریکی از طیف بسامدی را در هر لحظه پوشش می‌دهند، بنابراین احتمال دریافت سیگنال‌های پیش‌بینی نشده را پایین می‌آورند.

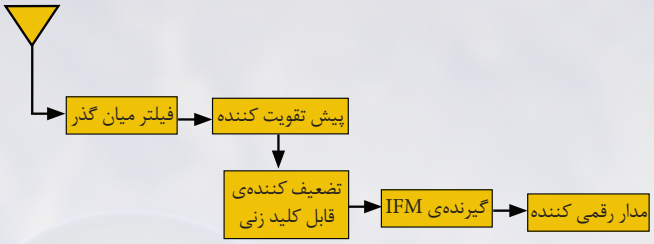
گیرنده‌های با سلول براگ و تراکمی قابلیت پوشش لحظه‌ای یک باند وسیع بسامدی به همراه ضبط و ربط چند سیگنال همزمان را دارند اما آنها نمی‌توانند سیگنال‌ها را وامدوله کنند. گیرنده‌های کانال‌بندی شده و رقمی دستاوردهای آینده هستند. آنها اغلب پارامترهای گیرنده‌ی مورد نیاز سیستم‌های جنگی الکترونیکی را فراهم می‌کنند اما اندازه، وزن و مشخصات توانی آنها منعکس کننده‌ی مرحله‌ای از هنر فناوری در زمینه‌ی ادوات و کوچک کردن زیر سیستم‌ها است. در فناوری کنونی هر دو نوع گیرنده آنقدر بزرگ، سنگین و با توان مصرفی بالا و گران هستند که عمدتاً در سیستم‌های پیچیده سخت‌ترین قسمت وظایف را انجام می‌دهند.

۱- گیرنده‌های تصویری کریستالی

گیرنده‌های تصویری کریستالی ساده‌ترین نوع گیرنده‌ی رایج امروزی هستند. این گیرنده شامل یک آشکارسازی کریستالی به همراه یک تقویت کننده‌ی تصویری است. این گیرنده هر سیگنال ورودی به آشکارسازی را از DC (مگر آنکه آشکارساز با تقویت کننده ترویج AC شده باشد) تا بسامدهای بالای ریز موج وامدوله‌ی دامنه می‌کند. مدوله‌سازی دامنه‌ی تمام این سیگنال‌ها در تقویت کننده‌ی تصویری و خروجی گیرنده با هم ترکیب می‌شوند.

۲- گیرنده‌های IFM

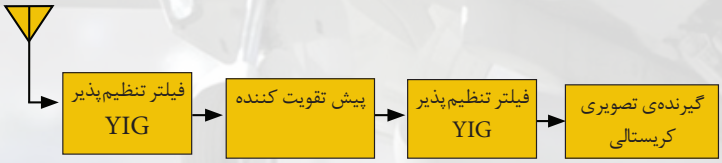
گیرنده‌های اندازه‌گیری بسامدی لحظه‌ای، درست همان کاری را که از نام آن بر می‌آید، انجام می‌دهند. مدار پایه‌ی گیرنده‌ی IFM یک جفت سیگنال را که تابعی از بسامد رادیویی سیگنال دریافتی هستند، تولید می‌کند. این سیگنال به صورت رقمی تبدیل می‌شود تا خواندن مستقیم بسامد سیگنال امکان‌پذیر باشد. مطابق شکل صفحه بعد پهنای باند سیگنال ورودی محدود است. خط تأخیر در مدار IFM محدوده‌ی خروجی را به گونه‌ای تنظیم می‌کند تا بتوان محدوده‌ی بسامدی سیگنال ورودی را با دقت ماکزیمم و به وضوح پوشش داد. از آنجا که مدار IFM به سطح سیگنال حساس است، ورودی گیرنده‌ی IFM در ابتدا از یک محدود کننده‌ی سخت عبور می‌کند تا یک سیگنال با سطح ثابت تولید شود.



۳- گیرنده‌های تنظیم شده‌ی بسامد رادیویی

در سال‌های اولیه‌ی ظهور رادیو، بسیاری از گیرنده‌ها از طرح‌های تنظیم شده‌ی بسامد رادیویی استفاده می‌کردند. آنها دارای طبقه‌های مختلف فیلترهای تنظیم شده و بهره در بسامد واقعی سیگنال دریافتی بودند. سادگی روش سوپر هترودین باعث جایگزینی عمده‌ی طراحی گیرنده‌های بسامد رادیویی با روش سوپر هترودین شده است. با وجود این، مطابق شکل زیر روش دیگری در طراحی گیرنده‌های جنگی الکترونیکی به کار می‌رود که گاهی اوقات بسامد رادیویی نامیده می‌شود.

گیرنده‌ی بسامد رادیویی در اصل یک گیرنده‌ی تصویری کریستالی است که گستره‌ی بسامد ورودی آن به وسیله‌ی یک فیلتر میان گذر YIG تنظیم شده، محدود شده است. این امر به گیرنده‌ی تصویری کریستالی اجازه می‌دهد تا چند سیگنال همزمان را کنترل و همچنین حساسیت آن را به خاطر پهنای باند RF باریک بهتر کند. در کاربردهای سیستمی، گیرنده‌ی RF ممکن است به دنبال یک پیش تقویت کننده دیگر و یک تضعیف کننده‌ی قابل کلید زنی قرار گیرد تا گستره‌ی پویای آن بهبود یابد.



۴- گیرنده‌های سوپر هترودین

گیرنده‌ی سوپر هترودین بسیار قابل انعطاف است. از آنجا که این نوع گیرنده از یک آشکارساز یا تمیزدهنده‌ی خطی استفاده می‌کند، بهترین حساسیت موجود را به صورت تابعی از پهنای باند قبل آشکارسازی و بهره‌ی پردازش بعد آشکارسازی ارائه می‌دهد. یک گیرنده‌ی پایه‌ی سوپر هترودین به وسیله‌ی یک نوسانگر تنظیم شده‌ی محلی (LO) قسمتی از محدوده‌ی بسامدی خود را به طور خطی به یک بسامد ثابت میانی (IF) تغییر می‌دهد. بسامد میانی ثابت از نظر ایجاد بهره‌ی لازم و قابلیت انتخاب فیلتر بسیار مؤثرتر است.

۵- گیرنده‌های ثابت تنظیم شده

در کلیه‌ی حالت‌هایی که در آنها یک سیگنال (یا چند سیگنال که همیشه در یک بسامد خاص هستند) باید مشاهده شود، بهتر است گیرنده‌ی ثابت تنظیم شده استفاده شود. این نوع گیرنده عموماً متشکل از یک گیرنده‌ی واقعی TRF و یا یک گیرنده‌ی سوپر هترودین به همراه یک نوسانگر محلی پیش تنظیم شده‌ی LO است. در هر دو حالت، گیرنده احتمال ۱۰۰ درصد دریافت سیگنال در یک بسامد خاص را فراهم می‌کند.

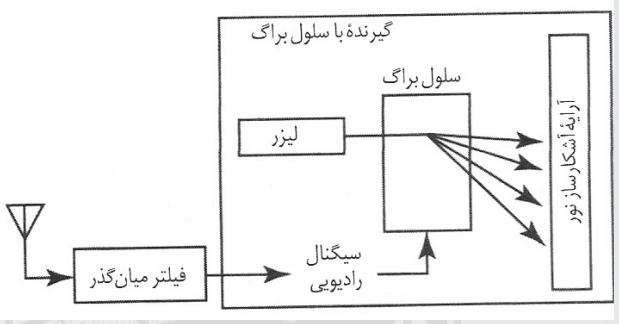
۶- گیرنده‌های کانال‌بندی شده

مجموعه‌ای از گیرنده‌های با بسامد ثابت که در آنها باند گذر کانال‌ها نزدیک به هم قرار داده می‌شوند، گیرنده‌ی کانال بندی شده نامیده می‌شود. این نوع گیرنده از نوع گیرنده‌های ایده‌آل است و خروجی وامدوله شده‌ای را برای سیگنال‌های هر کانال تولید می‌کند. این گیرنده می‌تواند جهت داشتن حساسیت و قابلیت انتخاب عالی، پهنای باند باریکی داشته باشد. این گیرنده قادر است احتمال ۱۰۰ درصد دریافت را گستره‌ی بسامدی خود ارائه دهد و البته قادر است دریافت مشخصات سیگنال همزمان را تا هنگامی که در بسامدهای مختلفی هستند، انجام دهد.

۷- گیرنده‌ی با سلول براگ

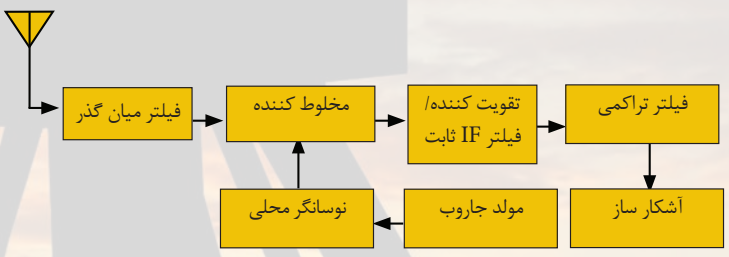
گیرنده‌ی با سلول براگ یک تحلیل‌گر طیف لحظه‌ای است که توانایی کنترل چند سیگنال همزمان را دارد. سیگنال‌های رادیویی که تا سطح توان بالایی تقویت شده‌اند به یک کریستال «سلول براگ» اعمال می‌شوند که با تولید خطوط تراکم داخلی که متناسب با طول موج هر سیگنال RF موجود در ورودی گیرنده قرار گرفته‌اند واکنش نشان می‌دهد. این امر سبب می‌شود یک باریکه‌ی لیزری با زاویه‌ای متناسب با بسامد RF موجود منحرف شود. این مجموعه باریکه‌های لیزری منحرف شده بر روی یک آرایه‌ی آشکارساز نور متمرکز می‌شود. این آرایه زوایای انحراف تمام اجزای باریکه‌ی منحرف شده‌ی لیزری را آشکار و سیگنال‌های خروجی را تولید می‌کند که به وسیله‌ی آن

می‌توان تمام بسامدهدی سیگنال‌های موجود در ورودی را به صورت رقمی مشخص کرد.



۸- گیرنده‌های تراکمی

شکل زیر نمودار بلوکی یک گیرنده‌ی تراکمی را که گیرنده‌ی ریزروبشگر نیز نامیده می‌شود، نشان می‌دهد. این گیرنده اساساً یک گیرنده‌ی سوپر هترودین است که به سرعت تنظیم می‌شود. معمولاً گیرنده‌ی سوپر هترودین با آهنگی که به پهنای باند آن اجازه‌ی ماندن در یک بسامد برای دوره‌ای مساوی یا بزرگتر از پهنای باندش را می‌دهد قابل تنظیم است. آهنگ تنظیم گیرنده‌ی تراکمی بسیار سریع‌تر از آهنگ پیشگفته است اما خروجی آن از یک فیلتر تراکمی عبور می‌کند که تأخیری متناسب با بسامد دارد. شیب تأخیر بر حسب بسامد آهنگ جاروب گیرنده را کاملاً جبران می‌کند. بنابراین، همان طور که گیرنده پهنای باند خود را در طول یک سیگنال جاروب می‌کند، خروجی گیرنده به طور همزمان متراکم می‌شود تا یک اسپایک سیگنال قوی در خروجی ایجاد کند. خروجی حاصل شده نمایشی طیفی از کل پهنای باندی است که گیرنده روی آن تنظیم شده است.



گیرنده‌ی تراکمی بسیار سریع‌تر از یک گیرنده‌ی معمولی با پهنای باند محدود جاروب می‌کند و از یک فیلتر تراکمی تطبیق یافته برای انتگرال‌گیری سیگنال‌های دریافتی برای اندازه‌گیری بسامد تمام سیگنال‌هایی استفاده می‌کند که در گستره‌ی بسامدی گیرنده قرار دارند.

۹- گیرنده‌های رقمی

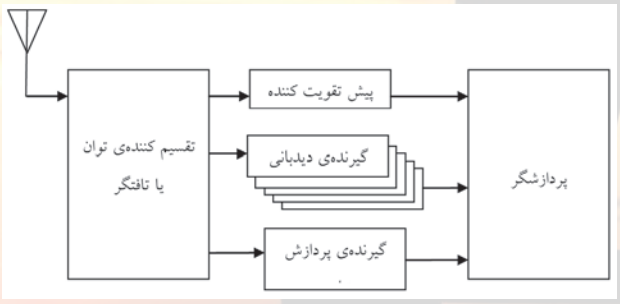
به نظر می‌رسد گیرنده‌های رقمی امید بزرگ آینده هستند. اساساً این گیرنده، سیگنال را برای پردازش توسط رایانه، رقمی می‌کند. از آنجایی که نرم افزار قادر به شبیه‌سازی هر نوع فیلتر وامدوله ساز است، سیگنال رقمی شده می‌تواند به صورت بهینه، فیلتر، وامدوله، پردازش پس از آشکارسازی و غیره شود.

البته مشکلات در پیاده‌سازی پدیدار می‌شوند. مبدل قیاسی به رقمی حیاتی‌ترین عنصر مدار است. دو نمونه در هر سیکل بزرگ‌ترین بسامد موجود در سیگنال رقمی شونده برای ارائه اطلاعات کافی به رایانه لازم است. فناوری تقریباً هر روز در حال پیشرفت است اما هنوز محدودیت‌هایی برای بیشترین بسامدی که قابل رقمی شدن است و بیشترین دقتی که می‌توان به دست آورد، وجود دارد.

۱۰- سیستم‌های گیرنده

تقریباً تمام انواع سیستم‌های شناسایی و جنگی الکترونیکی بیش از یک نوع گیرنده لازم دارند تا بتوانند وظایف خود را به درستی انجام دهند. ساختار یک سیستم نوعی گیرنده در شکل زیر نشان داده شده است. ورودی‌ها از یک یا چند آنتن تقسیم توان می‌شوند (اگر تمام گیرنده‌ها روی تمام باند بسامدی کار کنند) و یا مالتی پلکس (تافتگری) می‌شوند (اگر گیرنده‌ها روی قسمت‌های مجزایی از گستره‌ی بسامدی سیستم تنظیم شده باشند). در سیستم‌های پیچیده، توزیع سیگنال ترکیبی از هر دو روش است. در سیستم‌های جنگی الکترونیکی و شناسایی که دارای گیرنده‌های باند باریک هستند، کاملاً معمول است که یک گیرنده (و یا مجموعی از گیرنده‌ها) در پی جستجوی سیگنال‌های جدید باشد و سپس سیگنال‌های جدید را به گیرنده‌های مربوط ارجاع دهد. این گیرنده‌های اختصاصی در بسامدها و پهنای باند و تنظیمات وامدوله‌سازی خود تا آنجا که برای تحلیل کامل سیگنال لازم است باقی می‌مانند مگر آنکه به سیگنال‌های با اولویت بالاتری اختصاص یابند.

روش معمول دیگر استفاده از یک گیرنده‌ی با قابلیت پردازش مخصوص است تا اطلاعات بیشتری را درباره‌ی سیگنال تحت پردازش توسط یکی از چند گیرنده‌ی دیدبانی ارائه دهد.



پردازش جنگ الکترونیکی

جنگ الکترونیکی بنا به ماهیت خود پذیرای سیگنال‌های تهدید کننده‌ی موجود در محیط پیرامون خود است. بنابراین، از زمان شروع جنگ الکترونیک پیشرفته در اوایل دهه‌ی ۱۹۴۰ میلادی، انجام نوعی از پردازش برای مشخص‌سازی اینکه کی و چه‌طور باید به طور صحیح اقدام‌های ضد را انجام داد لازم می‌نمود. در ابتدا وابستگی زیادی به متصدیان ماهر وجود داشت که این متصدیان وظیفه‌ی مشخص ساختن نوع سیگنال تهدید کننده را داشتند تابتوان اقدام‌های ضد را به طور صحیح پیاده کرد. از آنجا که انسان قابلیت تشخیص مستقیم سیگنال‌های با بسامد رادیویی را ندارد، پس از اینکه سیگنال‌ها توسط گیرنده‌ها دریافت شدند به نحوی پردازش و تبدیل می‌شوند که توسط متصدیان قابل تشخیص باشند.

همچنان که محیط سیگنال‌ها پیچیده‌تر شد، سلاح‌های کنترل شده با رادار مرگ‌بارتر شدند، و فرصت‌ها کوتاه‌تر شدند، مسئله‌ی کشف و شناسایی خودکار تهدیدها لازم به نظر می‌رسید. شناسایی تهدیدها همچنان یکی از وظایف عمده‌ی پردازش جنگ الکترونیکی در تمام سیستم‌های جنگی الکترونیکی به حساب می‌آید.

تشخیص مکان گسیل‌گر وظیفه‌ی پایه‌ای دیگری در عملیات جنگی الکترونیکی است. از آنجا که سیستم‌های جدید جنگ الکترونیک، به خصوص در کاربردهای هوابرد، با سیگنال‌های زیادی سروکار دارند، جدا کردن سیگنال‌های خاص از توده‌ای از انرژی RF وظیفه‌ی سنگین و حساس پردازش است. سیستم‌های پیشرفته‌ی جنگ الکترونیک اغلب بسیار یکپارچه و شامل چند حسگر و چند اقدام‌های ضد هستند. تمام این اجزای سیستمی باید کنترل و با هم هماهنگ شوند.

شناسایی تهدیدهای RF

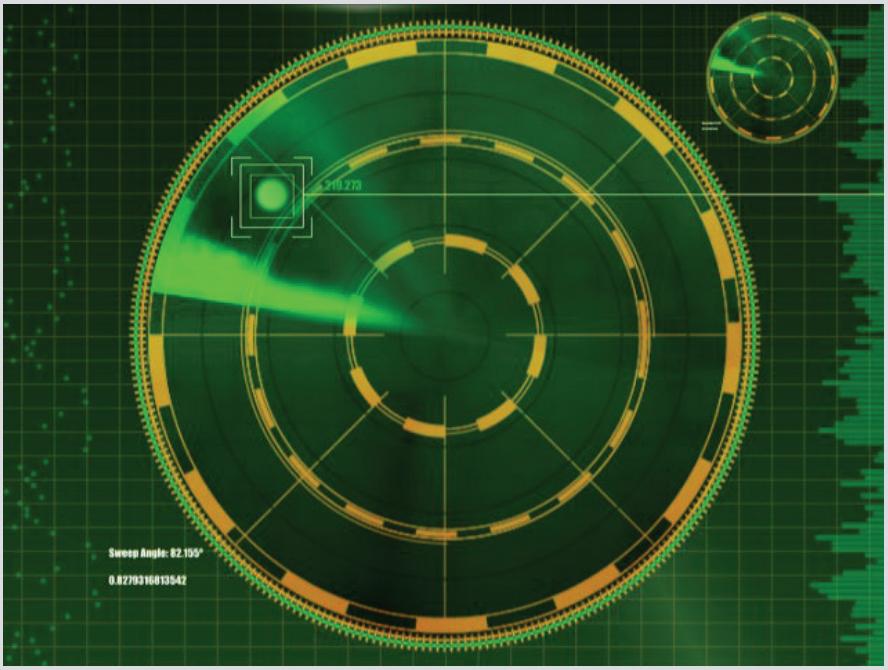
شناسایی تهدیدها را از روی پارامترهای سیگنال‌های RF شروع می‌کنیم. عموماً پارامترهای سیگنال تهدید کننده پارامترهای در پی آمده را در بر می‌گیرند.

- توان تشعشعی مؤثر؛
- الگوی آنتن؛
- انواع روبش آنتن؛
- آهنگ روبش آنتن؛
- بسامد سیگنال ارسالی؛
- انواع مدوله‌سازی؛
- پارامترهای مدوله‌سازی.

هنگامی که این سیگنال‌ها به گیرنده می‌رسند، به طریقی متفاوت مشخص می‌شوند. پارامترهای سیگنال دریافتی چنین هستند:

- قدرت سیگنال دریافتی؛
- بسامد سیگنال دریافتی؛
- روبش آنتن مشاهده شده؛
- نوع مدوله‌سازی؛
- پارامترهای مدوله‌سازی.

بعضی از پارامترها نسبتاً ساده اندازه‌گیری می‌شوند اما اندازه‌گیری بعضی دیگر مشکل‌تر است و نیازمند استفاده از وسایل مخصوص هستند. از آنجا که شناسایی تهدید کننده در جنگ الکترونیک معمولاً رویه‌ای بلادرنگ است، ترتیبی را که مطابق آن پارامترها تحلیل می‌شوند باید با دقت در نظر گرفت.



آشکارسازی سیگنال‌های تهدید

یکی از مشکلات مهمی که طراحان سیستم‌های جنگی الکترونیکی با آن روبه‌رو هستند آشکارسازی وجود سیگنال‌های تهدید است. به طور ایده‌آل بخش گیرنده در سیستم جنگی الکترونیکی می‌تواند همه‌ی جهت‌ها را در یک زمان در تمام بسامددهی برای تمام مدوله‌سازی‌ها و با حساسیت بسیار بالا ببیند. با وجود این که امکان ساخت چنین سیستمی وجود دارد، ابعاد، پیچیدگی و قیمت آن ساخت آن را در بیشتر کاربردها غیر عملی می‌سازد. بنابراین زیرسیستم‌های عملی گیرنده‌های جنگی الکترونیکی مصالحه‌ای را مابین تمام عوامل پیشگفته جهت رسیدن به بهترین احتمال شنود در ابعاد و وزن و توان و قیمت مورد نظر برقرار می‌کنند.

سیگنال‌های با احتمال شنود کم LPI

سیگنال‌های راداری و مخابراتی جزء سیگنال‌های با احتمال شنود کم (LPI) به شمار می‌آیند. رادارهای LPI دارای ترکیبی از پهنای باریکه‌ی آنتن کوچک، توان تشعشعی مؤثر کم و مدوله‌سازی هستند که سیگنال راداری را از نظر بسامد پخش می‌کند. سیگنال‌های مخابراتی LPI معمولاً بستگی به مدوله‌سازی پخش کننده‌ای دارند که آشکارسازی و اخلال آنها را مشکل می‌سازد. این بحث بر روی سیگنال‌های مخابراتی LPI متمرکز شده است و به خصوص مباحث مدوله‌سازی پخش بسامدی را مطرح می‌کند که آنها را در مقابل گیرنده‌ها و اخلال‌گرهای دشمن برتر می‌سازد. سیگنال‌های LPI برای سیستم‌های گیرنده‌ای که سعی در آشکارسازی آنها دارند مشکل‌زا هستند و سیگنال‌های LPI تعریف بسیار گسترده‌ای دارند و هر نوع ویژگی‌ای که سیگنال را برای آشکارسازی سخت‌تر و یا مکانیابی گسیل‌گر را مشکل‌تر می‌کند در برمی‌گیرد. ساده‌ترین ویژگی LPI کنترل تشعشع است، کاهش توان ارسالی تا سطح مینیممی که به سیگنال تهدید (راداری و مخابراتی) امکان ایجاد نسبت سیگنال به نویز کافی برای گیرنده‌ی مربوط را بدهد. توان ارسالی پایین‌تر فاصله‌ای را که هر گیرنده‌ی مشخص دشمن می‌تواند سیگنال‌های ارسالی را آشکار کند، کاهش می‌دهد.

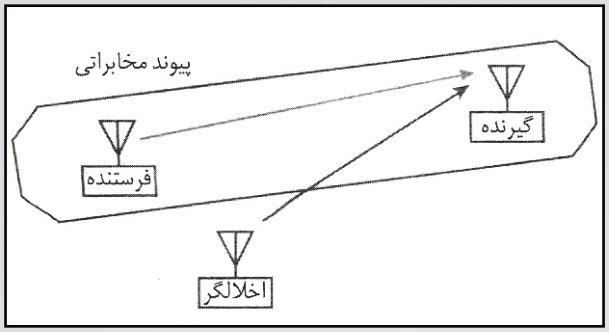
راهکارهای جستجوی LPI

روش‌های پایه‌ی جستجوی LPI همیشه شامل بهینه‌سازی پهنای باند شنود و یک یا چند مورد از موارد در پی آمده است:

- آشکارسازی انرژی با روش‌های یکپارچه‌سازی گوناگون؛
- جاروب سریع با انباشتگی و تحلیل شنود چندگانه؛
- اندازه‌گیری بسامدی باند پهن با ارائه‌ی آن به یک گیرنده‌ی سریع تنظیم شونده؛
- رقمی کردن و پردازش به کمک انواع گوناگون تبدیل‌های ریاضی.

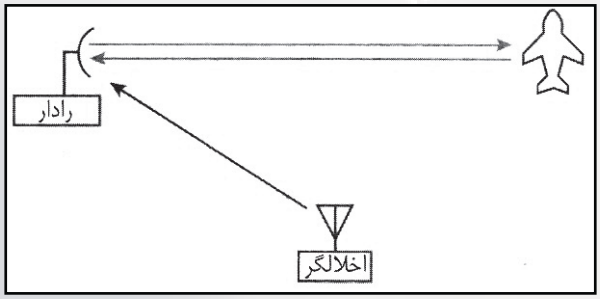
اخلال

هدف تمام اخلال‌ها، مختل کردن استفاده‌ی مؤثر دشمن از طیف الکترومغناطیس است. استفاده از طیف شامل ارسال اطلاعات از نقطه‌ای به نقطه‌ی دیگر است. این اطلاعات می‌تواند به شکل مخابرات صوتی یا غیر صوتی، سیگنال‌های فرمان برای کنترل تجهیزات دوردست، داده‌های برگشتی از تجهیزات دوردست یا مکان و حرکت تجهیزات خودی یا دشمن باشد.



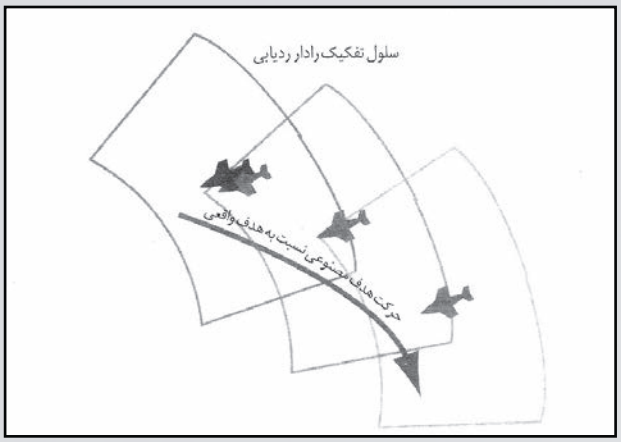
سال‌ها بود که اخلال را برای بیان اقدام‌های ضد الکترومغناطیسی به کار می‌بردند. اما در حال حاضر در بیشتر کتاب‌ها اخلال به صورت حمله‌ی الکترونیکی (EA) مطرح می‌شود. EA همچنین شامل استفاده از سطوح بالای توان تشعشعی و یا انرژی هدایت شده برای خسارت زدن فیزیکی به تجهیزات دشمن است. اخلال را بعضی مواقع «کشتن نرم» می‌نامند زیرا اخلال به طور موقتی یک وسیله‌ی دشمن را غیر مؤثر می‌کند اما آن را نابود نمی‌کند.

روش پایه‌ای اخلال، قرار دادن یک سیگنال تداخل کننده به همراه سیگنال مطلوب در گیرنده‌ی دشمن است. اخلال هنگامی مؤثر است که سیگنال تداخل کننده در گیرنده به اندازه‌ی کافی قوی باشد تا از دریافت اطلاعات مورد نیاز از سیگنال مطلوب توسط دشمن جلوگیری کند، زیرا یا محتویات اطلاعات سیگنال مطلوب به وسیله‌ی قدرت سیگنال اخلال به هم ریخته است و یا سیگنال مخلوط (مطلوب + اخلال) دارای مشخصاتی است که اجازه‌ی استخراج یا استفاده‌ی صحیح از اطلاعات مطلوب را به پردازش‌گر نمی‌دهد.



هدف‌های مصنوعی

با افزایش پیچیدگی سلاح‌های هدایت شده و به خصوص با افزایش استفاده از حالت‌های «آشیانه‌یابی اخلال» اهمیت هدف‌های مصنوعی راداری بیشتر شده است. بنابراین در ادامه انواع مختلف هدف‌های مصنوعی و مأموریت‌های هدف مصنوعی را بررسی می‌کنیم.

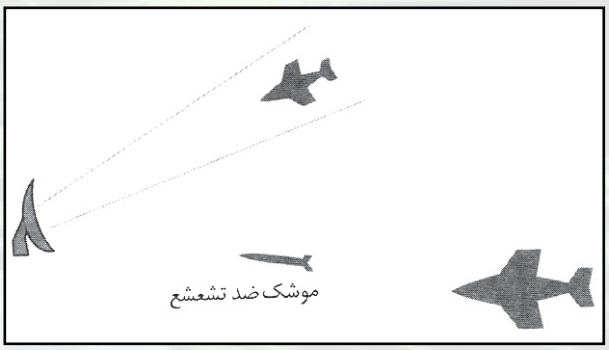


انواع هدف‌های مصنوعی

هدف‌های مصنوعی را می‌توان بر اساس روشی که مورد استفاده قرار می‌گیرند، روش مقابله با تهدیدها، یا انواع سکوهایی که آنها محافظت‌شان می‌کنند، دسته‌بندی کرد؛ در هر دسته واژه‌های خاصی به کار می‌روند. برای گردآوری واژگان معمول به کار رفته در مطالب بعدی، نوع هدف مصنوعی را بر اساس روشی که به کار گرفته می‌شود، مأموریت هدف مصنوعی را بر اساس روشی که از هدف حفاظت می‌کند، و سکوی آن را بر اساس خودروی نظامی‌ای که محافظت می‌شود، تعریف می‌کنیم. انواع مختلف هدف‌های مصنوعی را به سه نوع مصرفی، کششی و «مانور مستقل» تقسیم می‌کنیم. هدف‌های مصنوعی مصرفی از موشک‌های هواپیمای جنگی و یا پرتاب کننده‌های راکت از کشتی‌ها خارج می‌شوند. این هدف‌های مصنوعی به نوعی برای مدت کوتاهی فعال هستند.

هدف مصنوعی کششی با کابل به هواپیما متصل می‌شود و می‌تواند به وسیله‌ی هواپیما کنترل و یا به داخل کشیده شود. هدف‌های مصنوعی کششی با مأموریت‌های طولانی مدت مرتبط هستند. قایق‌های کششی، برای کشتی‌ها از بازتابنده‌های گوشه‌ای بزرگی استفاده می‌کنند و می‌توان آنها را هدف‌های مصنوعی کششی نامید اما به نوعی آنها را جداگانه در نظر می‌گیرند.

هدف‌های مصنوعی مانور مستقل بر روی سکوهای پیشرونده به نوعی هوابرد استفاده می‌شوند. برای مثال می‌توان از بارهای هدف مصنوعی UAV، هدف‌های مصنوعی با پنکه‌ی لوله مانند که در محافظت از کشتی استفاده می‌شوند و از هدف‌های مصنوعی نام بردکه بر رو و یا زیر هلی‌کوپتر نصب می‌شوند. هنگامی که هدف‌های مصنوعی مانور مستقل برای محافظت یک سکو استفاده می‌شوند، دارای قابلیت انعطاف کامل در حرکت نسبی هستند. (در مقایسه با هدف‌های مصنوعی کششی که باید به دنبال هدف باشند و یا هدف‌های مصنوعی مصرفی که می‌افتند و دور می‌شوند و یا به سمت جلو شلیک می‌شوند). کاربرد عمده‌ی هدف‌های مصنوعی مانور مستقل، حفاظت از کشتی است و وظیفه‌ی دیگر آن پرتاب از جلوی هواپیما برای آشکار کردن قدرت دفاعی دشمن به منظور اجتناب یا حمله است.



مأموریت‌های هدف مصنوعی

هدف‌های مصنوعی سه مأموریت عمده دارند. یکی اشباع دفاع دشمن، دیگری مجبور کردن دشمن برای عوض کردن هدف حمله از هدف واقعی به هدف مصنوعی و آخرین مأموریت اینکه سبب شوند دشمن نیروهای حمله‌ی خود را برای هجوم به هدف مصنوعی آشکار کند. سابقه‌ی این سه مأموریت هدف مصنوعی به تاریخچه‌ی تعارض‌های میان انسان‌ها بر می‌گردد که قدمت آن بسیار پیش‌تر از تولد جنگ الکترونیکی است. تفاوت آنها این است که به جای اینکه به طور مستقیم حس‌های جنگجویان دشمن را فریب دهند، هدف‌های مصنوعی جدید جنگ الکترونیکی، حسگرهای الکترونیکی را که اهداف را آشکارسازی و مکانیابی می‌کنند و سلاح‌ها را به سمت آنها هدایت می‌کنند، فریب می‌دهند.

شبیه‌سازی

عموماً از شبیه‌سازی جنگ الکترونیکی به منظور کاهش هزینه استفاده می‌شود. اما دلایل احتمالاً مهمتر دیگری نیز برای شبیه‌سازی وجود دارند. شبیه‌سازی ارزیابی واقعی کارایی متصدیان، تجهیزات و روش‌ها را تحت شرایطی که هنوز وجود ندارد، ممکن می‌سازد. شبیه‌سازی همچنین امکان آموزش واقعی افراد در شرایطی که در دنیای واقعی ممکن است آنها را بکشید فراهم می‌سازد.

در شبیه‌سازی، شرایطی مجازی خلق می‌شود که درست مشابه حالتی که در شرایط واقعی در حال اجراست، پیشامدی به وجود می‌آید. شبیه‌سازی جنگ الکترونیکی اغلب شامل ایجاد سیگنال‌هایی شبیه سیگنال‌های تولید شده به وسیله‌ی تجهیزات الکترونیکی دشمن است. این سیگنال‌های مجازی به منظور آموزش متصدیان، ارزیابی کارایی سیستم‌ها و زیرسیستم‌های جنگی الکترونیکی و پیش‌بینی کارایی تجهیزات الکترونیکی دشمن یا سلاح‌هایی که کنترل می‌کنند به کار می‌روند.

از طریق شبیه‌سازی، متصدیان و تجهیزات جنگی الکترونیکی می‌توانند موظف به انجام اعمالی شوند انگار که یک یا بیش از یک سیگنال تهدید موجود است و کاری را انجام دهند که طی برخورد نظامی انجام می‌دادند. معمولاً شبیه‌سازی شامل به روز کردن فعال تهدید شبیه‌سازی شده به صورت تابعی از پاسخ متصدی و تجهیزات به سیگنال تهدید است.

منابع:

۱- نباتی، عزت الله. (۱۳۹۰) جنگ الکترونیک. تهران: مرکز آموزشی پژوهشی شهید سپهبد صیاد شیرازی.

۲- واحدی، مرتضی و قیاسی کرمانی، علی اکبر. (۱۳۹۰). کلیات جنگ الکترونیک. تهران: دانشکده علوم و فنون فارابی، معاونت پژوهش.

۳- یاوری، احیا و [دیگران]. (۱۳۸۵). نقش فناوری اطلاعات در جنگ های آینده. تهران: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، طرح فراسازمانی فرماندهی و کنترل: دانشگاه صنعتی مالک اشتر.

کاربردهای جنگ الکترونیک

جنگ الکترونیک را می‌توان در سه شاخه مورد بررسی قرارداد:

۱- بهره‌برداری از سیگنال‌های الکترومغناطیس انتشاریافته توسط دشمن به‌منظور کسب آگاهی در مورد توانایی‌ها و مقاصد آن؛

۲- به کارگیری اقدام‌های لازم علیه دشمن برای جلوگیری یا کاهش دادن استفاده‌ی مؤثر از طیف الکترو مغناطیس؛

۳- استفاده‌ی مفید و مطمئن نیروهای خودی از پهنای باند.

بحث جنگ الکترونیک در دو زمینه رادار و مخابرات وجود دارد ولی تفاوت‌هایی در این دو زمینه مشاهده می‌شود:

۱- در مخابرات پیام وجود دارد و می‌توان با روش‌های رمزنگاری آن را از دید دشمن مخفی کرد ولی در رادار پیام نداریم.

۲- در مخابرات پیام با تضعیف در یک مسیر به گیرنده می‌رسد ولی در رادار تضعیف در دو مسیر (رفت و برگشت) اتفاق می‌افتد.

۳- در رادار گیرنده معمولاً همان فرستنده است یا در نزدیکی آن قرار دارد و می‌توان آن را نابود کرد ولی در مخابرات مکان گیرنده معلوم نیست.

با توجه به موارد بالا روشن است که ایجاد نقصان در سیگنال‌های راداری بسیار ساده‌تر است و برای حفظ عملکرد مؤثر رادار به راهکارهای پیچیده‌تری نیاز داریم.

تقسیم‌بندی جنگ الکترونیک را به طریق دیگری نیز می‌توان بیان‌کرد که متناظر دسته‌بندی قبلی است:

۱- پشتیبانی الکترونیک (ESM)

۲- حمله الکترونیک (ECM)

۳- حفاظت الکترونیکی(EP یا ECCM)

♦ پشتیبانی الکترونیک (ESM)♦

جستجوی طیف یا باند فرکانسی مورد استفاده دشمن و نیز رهگیری و یافتن مکان‌های تشعشع امواج الکترومغناطیس برای تشخیص، شناسایی و ردیابی فوری تهدیدهای دشمن و همچنین اعلام سریع وجود خطر و انتخاب سلاح و روش مناسب برای مقابله با تهدیدهای احتمالی را پشتیبانی الکترونیک (ESM) گویند.

گیرنده‌ی مناسب، از احتیاجات اولیه تجهیزات ESM است که برای شناسایی و تشخیص تشعشع‌های خودی از امواج انتشار یافته توسط دشمن به کار می‌رود. طراحی یک گیرنده مناسب مشکلات خاص خود را دارد زیرا با یک آنتن یا سیستم گیرنده نمی‌توان کل طیف

الکترومغناطیس را پوشش داد. راه حل مورد استفاده، طراحی چند مدار حساس به فرکانس‌های متفاوت در یک زنجیره به همراه تقویت‌کننده‌های متناظر با هریک به همراه یک صفحه نمایش بوده است.

خصوصیات مورد نیاز یک گیرنده ESM

یک گیرنده‌ی ESM هم درموارد اصلی و هم در تجهیزات کمکی مربوط به آن با گیرنده‌ی معمولی تفاوت دارد. احتیاجات ضروری این گیرنده عبارتند از:

۱- جستجوی پهنای باند وسیع: فرکانس مورد استفاده رادار دشمن پیشاپیش مشخص‌نیست یعنی باید طیف الکترومغناطیس را از فرکانس ۳۰ KHz تا ۵۰GHz بررسی‌کرد. این محدوده خیلی وسیع است و برای پوشش دادن آن باید از چند گیرنده استفاده کرد که هریک محدوده‌ی خاصی را پوشش می‌دهند.

۲- برد دینامیک گسترده: گیرنده باید قابلیت دریافت سیگنال‌های بسیار ضعیف و خیلی قوی را داشته باشد.

۳- بازگشت‌دادن سیگنال ناخواسته: سیگنال‌های خیلی زیادی با فرکانس‌های نزدیک به فرکانس کاری گیرنده وجود دارند. گیرنده باید به‌خوبی فرکانس مطلوب را از فرکانس‌های مجاور جدا کند.

۴- قابلیت تعیین زاویه‌ی ورود سیگنال دریافتی

۵- قابلیت تحلیل سیگنال: می‌توان مشخصات سیگنال دریافتی مانند مدولاسیون و پهنای پالس آن را تعیین‌کرد. این اطلاعات به شناسایی سیگنال و در نتیجه نوع تهدید کمک می‌کند.

۶- صفحه‌ی نمایش

۷- سیستم ذخیره‌ی اطلاعات: برای بررسی بیشتر توسط یک سیستم کامل‌تر(درصورت نیاز) سیگنال‌های دریافتی در سیستم ذخیره اطلاعات ثبت و نگهداری شود.

۸- پردازش سیگنال: جمع‌آوری سیگنال یک پردازش سه مرحله‌ای شامل اعلام خطر، طبقه‌بندی و تحلیل است. اعلام خطر، دریافت یا حضور سیگنال را به کاربر اعلام می‌کند. در مرحله‌ی بعد سیگنال‌های دریافتی برحسب اهمیت طبقه‌بندی می‌شوند. خصوصیات فرستنده با تحلیل سیگنال دریافتی به‌دست می‌آید.

♦ حمله‌ی الکترونیکی یا EA یا ECM

قسمت دوم جنگ الکترونیک، حمله‌ی الکترونیکی یا ECM است که عبارت است از: استفاده از انرژی الکتریکی جهت‌دار برای حمله به پرسنل، امکانات و تجهیزات دشمن به‌قصد آسیب‌رساندن، خنثی‌کردن و یا نابودکردن توان نظامی آنها.

چند نمونه از تجهیزات الکترونیکی که علیه آنها از تکنیک‌های ECM استفاده می‌شود، عبارتند از: آشکارسازهای بلندبرد غیرفعال، رادارهای گشت هوایی، رادارهای دوربرد، موشک‌های هدایت‌شونده به‌وسیله راداریا مادون قرمز، IFF ، توپخانه‌های ضدهواپیما و...

در واقع هدف از به‌کاربردن تکنیک‌های ECM کاهش اطلاعات مفید داخل سیگنال‌هایی است که توسط حسگرهای تجهیزات دفاعی دشمن دریافت می‌شود. ایجاد مشکلات دفاعی بیشتر معادل کارایی بهتر تاکتیک‌های ECM است.

نکته‌ی مهمی که همیشه باید درنظر داشت این است که هدف از ECM جلوگیری کامل از عملکرد حسگرهای دشمن (مثلاً فقدان

ردیابی اهداف توسط یک رادار ردگیر) نیست. بلکه ایجاد یک تأخیر حتی کوتاه در ردیابی اهداف، برای لحظه‌ای گیج‌کردن دشمن و یا مجبورکردن تصمیم‌گیرنده به درنگ چند ثانیه‌ای در اتخاذ تصمیم درست، برای ضربه‌زدن به دفاع دشمن کافی است.

برای ایجاد اخلال در عملکرد رادارهای دشمن، به‌طورکلی دو راه وجود دارد:

۱- تولید پارازیت یا جمینگ ۲- فریب. هرکدام از این دو را می‌توان به روش‌های مختلف مانند انتشار سیگنال فعال برای تداخل با سیگنال‌های راداری (که دربیشتر موارد این روش مورد استفاده قرار می‌گیرد)، تغییر دادن خواص الکتریکی محیط واسط بین رادار و هدف مانند به کاربردن چَف، تغییردادن خواص بازتابشی اهداف که با به کاربردن مواد جاذب امواج راداری یا به کاربردن افزایش‌دهنده‌های بازتاب امواج برای ایجاد هدف دروغی انجام می‌شود، پیاده کرد.

♦ فرستنده‌های ECM ♦

توانایی فرستنده‌ی ECM به موارد مختلفی از جمله توان خروجی، تلفات خطوط انتقال، بهره‌ی آنتن در جهت گیرنده‌ی هدف و پهنای باند فرستنده بستگی دارد. به‌علاوه میزان توان فرستنده‌ی ECM که به گیرنده‌ی هدف می‌رسد، به پهنای باند گیرنده، بهره‌ی آن و سطح مقطع مؤثر گیرندگی آنتن وابسته است. بنابراین عملکرد مؤثر فرستنده ECM منوط به گسیل توان کافی در محدوده‌ی فرکانسی گیرنده‌ی هدف به‌منظور پوشاندن سیگنال مطلوب گیرنده و یا فریب دادن آن است.

برای برآورده کردن این احتیاجات، بیشتر فرستنده‌های ECM با توانایی‌های گوناگون و چند بعدی طراحی می‌شوند. هنگامی که این وسیله بر علیه یک موشک، یک رادار یا گروهی از این وسایل که در محدوده فرکانسی نزدیک به هم کار می‌کنند استفاده شود، فرستنده توان خروجی خود را در یک باند محدود فرکانسی متمرکز می‌کند. ولی اگر تجهیزات دشمن در فرکانس‌های متفاوتی کارکنند، فرستنده ECM باید توان خروجی را در محدوده مورد نیاز گسترش دهد. بنابراین می‌توان گفت میزان کارایی فرستنده ECM به چگالی توان خروجی آن در محدوده فرکانسی گیرنده هدف بستگی دارد.

تعریف Burn through : فواصلی که در آن توان اکوی برگشتی از هدف قوی‌تر یا برابر با توان فرستنده ECM باشد را Burn through می‌گویند.

♦ پارازیت نویزی ♦

یک راه برای جلوگیری از عملکرد صحیح گیرنده رادار(یا هرگیرنده دیگر) اشباع آن با نویز است. نویز یک سیگنال تصادفی پیوسته است که تشابهی با سیگنال رادار ندارد. هدف از نویز در این روش پنهان‌سازی پالس‌های رادار برگشتی از هدف است. بنابراین باید توان متوسط جمر با توان پیک اکوی برگشتی برابر یا از آن بیشتر باشد. به بیان دیگر نسبت نویز به سیگنال در ورودی گیرنده باید به حدی زیاد شود که گیرنده نتواند سیگنال را از نویز تشخیص دهد.

از آنجایی‌که جمر برخلاف رادار، سیگنال را به طور پیوسته در فضا منتشر می‌کند به توان متوسط بالایی نیاز دارد. این توان بالا منجر به حجم و وزن زیاد تجهیزاتی می‌شود که قرار است مثلاً توسط هواپیما یا کشتی حمل شود. با اینکه در مورد کشتی محدودیتی وجود ندارد، هواپیما یا وسایل نقلیه کوچک نمی‌توانند جمرهای خیلی سنگین همراه داشته باشند.

وقتی آنتن رادار در جهت جمر قرار گیرد، سیگنال را می‌بیند و جهت ورود آن را تشخیص می‌دهد ولی فاصله آن معلوم نمی‌شود. بنابراین، نقطه ضعف جمر کمک به تشخیص حضور هدف و جهت مختصات زاویه‌ای آن به رادار است.

تکنیک‌های اصلی ایجاد پارازیت یا نویز

سه روش متفاوت برای تولید نویز و ایجاد پارازیت وجود دارد: ۱- نویز نقطه‌ای،۲- نویز رگباری و ۳- نویز جاروب. در روش اول تمام انرژی خروجی نویز در یک طیف بسیار باریک متمرکز می‌شود که در حالت ایده‌آل برابر با طیف رادار است. در روش‌های دوم و سوم، انرژی خروجی جمر در طیفی گسترده می‌شود که بسیار پهن‌تر از طیف سیگنال رادار

است. در نویز رگباری از مدولاسیون دامنه در ارسال سیگنال استفاده می‌شود و پهنای باند آن برابر ۱۰ درصد فرکانس مرکزی است. در نویز جاروب سیگنال با مدولاسیون فرکانس ارسال شده و فرکانس در یک محدوده خیلی گسترده از بالا به پایین و پایین به بالا جاروب می‌شود. بنابراین روش اول تنها علیه یک رادار یا یک گروه رادار خاص به کار می‌رود ولی دو روش دیگر می‌تواند در عملکرد تعداد زیادی رادار اختلال ایجاد کند.

چون یکسان کردن فرکانس جمر با رادار عملاً غیر ممکن است، در عمل به جمر با پهنای باند بالا نیاز داریم. با توجه به اینکه توانی که توسط گیرنده یک رادار دریافت می‌شود، توان سیگنال با فرکانسی یکسان با فرکانس مورد استفاده آن رادار است، در مورد جمرهای طیف گسترده، مفهوم چگالی طیف توان تعریف می‌شود. چگالی توان برابر است با توان طیف خروجی جمرتقسیم بر پهنای باند آن، که معمولاً با واحد بیان می‌شود.

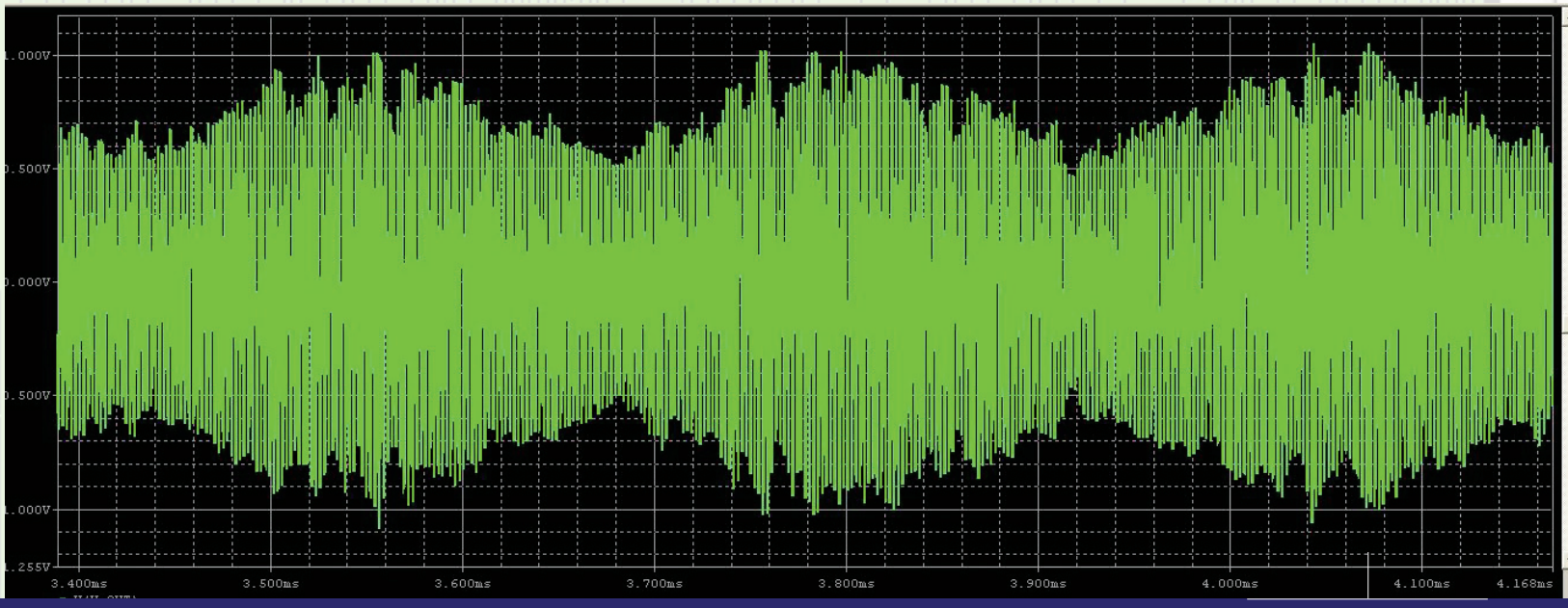
چون یک هواپیما در حمل جمرهای سنگین محدودیت دارد، می‌توان برای غلبه بر پارازیت آن در سامانه‌های پدافندی از فرکانس‌های متفاوت با فواصل زیاد استفاده کرد. در یک رادار هم می‌توان فرکانس‌های متفاوتی را برای غلبه برجمر نقطه‌ای مورد استفاده قرارداد که به این روش جهش فرکانسی می‌گویند.

♦ تاکتیک‌های استاندارد ایجاد پارازیت ♦

سه تاکتیک استاندارد مورد استفاده عبارتند از:

جمر خود محافظ: در این حالت، هدف از حمل جمر حفاظت از خود وسیله است. بنابراین جمر به همراه آن وسیله مثلاً هواپیما حمل می‌شود و یا داخل ناحیه‌ای که از آن دفاع می‌شود. هنگام حمل جمر باید یک مصالحه بین توان جمر و در نتیجه حجم و وزن آن و فضای در نظر گرفته شده برای دیگر وسایل مانند حسگرها، سوخت و سلاح برقرار باشد.

جمر خارج از محل: در این حالت جمر در ناحیه‌ای بسیار دور از محلی که از آن دفاع می‌شود و به بیان دیگر در مکانی دور از دسترسی سلاح‌های دشمن قرار می‌گیرد. کاربرد جمر خارج از محل در گیج کردن

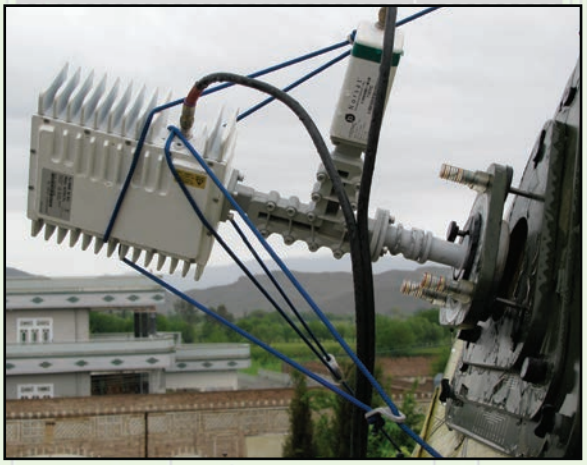


رادارهای جستجوگر دشمن است به طوری‌که موشک‌های خودی در شرایطی مطمئن و ایمن به سرزمین آنها نفوذ کند. نقطه ضعف این روش این است که زودتر با ناحیه Burn through مواجه می‌شویم زیرا سلاح به رادار دشمن نزدیک می‌شود در حالی‌که جمر در مکانی بسیار دور از رادار قرار دارد.

جمر پیش‌رو: جمر بین حسگرهای دشمن (رادارها) و واحد حمله کننده قرار می‌گیرد. با اینکه حفظ این موقعیت بین جمر، حمله کننده و رادار مشکل است این روش بهترین بازده را در استفاده از توان جمر به دست می‌دهد. البته خطر زیادی جمر را تهدید می‌کند زیرا به عنوان هدف اولیه در همه سیستم‌های دفاعی شناخته شده و همواره توسط موشک‌های ضد تشعشع و سلاح‌های آشیانه یاب جمر، مورد تهدید قرار می‌گیرد.

♦ فریب ♦

نوع دیگر ECM فعال، فریب است. در این روش سعی بر ایجاد سیگنالی شبیه سیگنال برگشتی دارند که رادار منتظر دریافت آن است به طوری که رادار در تشخیص فاصله هدف یا سمت حرکت آن دچار اشتباه شود. فریب تاکتیکی معمولاً به وسیله تکرارکننده‌ها و ترانسپوندرها انجام می‌شود و در بعضی مواقع جمرتکرارکننده نامیده می‌شود.



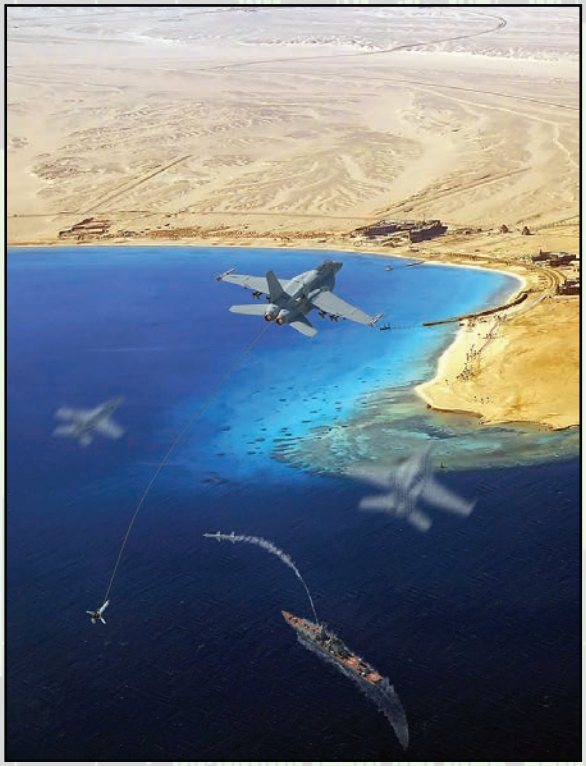
تکرارکننده: با اینکه عملکرد تکرارکننده‌ها از نظر تئوری خیلی ساده است، پیاده‌سازی عملی آنها به مدارهای خیلی پیچیده‌ای نیازمند است. در یک تکرارکننده، سیگنال رادار دریافت شده و با تأخیر، تقویت و مدولاسیون مورد نظر دوباره به سمت رادار فرستاده می‌شود.

ترانسپوندر: سیگنال ارسال شده در حد امکان شبیه سیگنال رادار ساخته می‌شود. در ترانسپوندرسیگنال رادار ذخیره شده و پس از دریافت پالس بعدی که به‌عنوان راه‌انداز آن عمل می‌کند، پالس شبیه سیگنال ذخیره شده به سمت رادار فرستاده می‌شود. پالس ارسالی باید درحد امکان شبیه پالس‌های رادار باشد.

♦ فریب در فاصله ♦

اگر تکرارکننده به محض دریافت پالس رادار آن را به سمت رادار ارسال کند نه تنها در عملکرد آن اخلال ایجاد نمی‌کند بلکه به تشخیص هدف کمک هم می‌کند. ولی اگر پالس دریافتی برای مدتی نگهداری شده و پس از یک بازه زمانی کوتاه به سمت رادار ارسال شود، رادار ابتدا اکوی ضعیف حاصل از هدف و به دنبال آن پالس یکسان ولی قوی‌تر از پالس قبلی را دریافت می‌کند. اگر تکرار کننده تعدادی پالس با تأخیرهای متفاوت به سمت رادار بفرستد می‌تواند هدف‌های دروغی متعدد و در فواصل گوناگون ایجاد کند.

در صورتی‌که قصد تکرار کننده، ایجاد یک هدف دروغی و نزدیکتر از هدف واقعی در نمایشگر رادار باشد، تأخیر را زیاد می‌کند به حدی که پالس بعدی قبل از رسیدن پالس رادار به تکرارکننده به سمت رادار فرستاده شود. این اطلاعات غلط در مورد فاصله هدف، خطاهای بزرگ در هدف‌گیری و هدایت موشک‌های پدافندی ایجاد می‌کند. ساده‌ترین روش برای غلبه بر این مشکل تغییر حالت عملکرد رادار به مددستی است.



♦ فریب در تشخیص زاویه ♦

می‌توان رادار و سیستم کنترل مرکزی آن را طوری گیج کرد که اطلاعات نادرست از زاویه سمت و زاویه ارتفاع هدف به دست دهند. برای این منظور باید سیستم فریب طوری عمل کند که رادار حضور هدف را زمانی اعلام کند که در جهت زاویه سمت و ارتفاع هدف نباشد. برای نیل به این مقصود دو روش کلی وجود دارد:

۱- فریب زاویه لوب فرعی: ابتدا باید لوب فرعی در نمودار تشعشعی آنتن رادار برای واحد ECM آشکار شود. پس از آن، پالس ایجاد هدف دروغی زمانی ارسال می‌شود که جمر در جهت لوب فرعی رادار باشد. از آنجا که در رادار سیگنال دریافتی همیشه در جهت لوب اصلی فرض می‌شود، بنابراین هدف دروغی با خطای زاویه‌ای برابر با اختلاف زاویه لوب‌های اصلی و فرعی آنتن در صفحه نمایش نشان داده خواهد شد. در برابر تمام رادارهایی که در آنها از تکنیک‌های خنثی کردن یا کنسل کردن لوب فرعی به طور مؤثر استفاده نمی‌شود می‌توان این روش را به کار برد. اگر به طور همزمان از تکنیک فریب در فاصله هم استفاده کرد می‌توان چند هدف دروغی در فواصل و زوایای مختلف در صفحه نمایش ایجاد کرد در حالی‌که انرژی بسیار کمتری در مقایسه با جمر نویزی لازم است.

۲- فریب مدار تشخیص زاویه خطا: در رادارهایی که در آنها ردیابی با ایجاد پرتو چپ شده و تشخیص زاویه خطا و چرخش آنتن به سمتی انجام می‌شود که منجر به صفر شدن زاویه خطا می‌گردد (مانند ردیاب مونو پالس، اسکن مخروطی و...)، می‌توان رادار را طوری فریب داد که آنتن آن در جهتی غیر از جهتی که باعث صفر شدن زاویه خطا می‌شود، حرکت کند. با این کار، واحد ECM خطای قابل توجه به همراه تأخیر در کاربرد سیستم دفاعی دشمن ایجاد می‌کند. فریب مدار تشخیص زاویه خطا، برای هر تکنیک معمولاً به تجهیزات خاصی نیاز دارد. در مورد تمام روش‌ها، واحد فریب‌دهنده باید از تکنیک مورد استفاده رادار در ردیابی مطلع باشد. در مورد روش اسکن مخروطی این اطلاعات با یک گیرنده

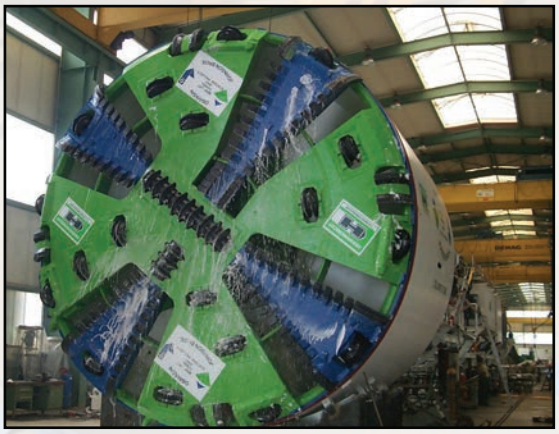
ESM به دست می‌آید. ولی مثلاً در روش مونوپالس، رادار هیچ اطلاعاتی به اپراتور ESM در مورد نحوه ردیابی به دست نمی‌دهد. به طورخلاصه، دو روش را می‌توان مقابل کلیه ردیاب‌های متفاوت به کاربرد:

چشمک زدن: نویز یا نمونه‌ای از پالس ارسال شده توسط رادار، تقویت شده و از نقاط مختلف که با فاصله زیاد از هم قراردارند در یک مد تصادفی به سمت رادار ارسال می شوند. این کار باعث افزایش حرکت یا سرگردانی واحد متحرک می‌شود که رادار آن را ردیابی می‌کند. یک رادار ردیاب باید مرکز هدف را رهگیری کند و این کار باعث افزایش خطای ردیابی خواهد شد.

لوچ شدن: دو نقطه بسیار دور روی فریب دهنده (مانند دماغه و دم هواپیما) انتخاب می‌گردد و به دو ترانسپوندر متصل می‌شوند. با دریافت پالس رادار در هرکدام از این دو نقطه، ترانسپوندر سمت مقابل راه‌اندازی می‌شود و پالسی شبیه پالس رادار با ۱۸۰° اختلاف فاز نسبت به آن به سمت رادار می‌فرستد. نتیجه این عمل، معکوس شدن علامت زاویه خطا در رادار ردیاب و در نتیجه جابه‌جایی آنتن در جهت نادرست است.

♦ افزایش‌دهنده اکوی برگشتی ♦

نوع دیگر تکرارکننده‌های فریب دهنده، افزایش دهنده اکوی بازگشتی است. این تکرارکننده‌ها اکوی برگشتی را چنان تقویت می‌کنند که یک هدف کوچک بزرگ شده و مانند یک سلاح خطرناک در رادار نمایش داده شود. این عمل را می‌توان به طور مکانیکی و با طراحی مناسب بازتاب‌دهنده‌ها نیز انجام داد.



♦ نوارهای منعکس‌کننده یا چف ♦

روش اصلی برای تغییر دادن خصوصیات فضای بین رادار و هدف استفاده از نوارهای منعکس‌کننده است. چف شامل دو قطبی‌های فلزی

(آلومینیوم) کوچک است و طوری طراحی شده‌اند که فرکانس رادار را تشدید می‌کنند.

دوقطبی‌های نیم‌موج منعکس‌کننده‌های راداری بسیار خوبی می‌سازند. ابعاد معمول برای استفاده از آنها در برابر یک رادار با فرکانس ۱۰ GHz برابراست با: طول ۰/۶ اینچ، عرض ۰/۰۱ اینچ و ضخامت ۰/۰۰۱ اینچ. تنها با وزنی معادل ۴۵ gr (۰/۱ پوند) می‌توان بازگشتی معادل یک بمب بزرگ ایجاد کرد. هزاران عدد از این دوقطبی‌ها را در یک بسته کوچک قرار می‌دهند. وقتی توسط هواپیما این دوقطبی‌ها در هوا منتشر شوند یک ابر منعکس‌کننده امواج راداری تولید می‌کنند که به آن راهروی چف می‌گویند.

هرکدام از بسته‌های چف که به طور مستقل رهاشده و پایین می‌آیند، می‌توانند یک هواپیمای دیگر را در رادار شبیه‌سازی کنند. یک دیواره چف که شامل هزاران هدف دروغی است می‌تواند توسط تعداد کمی هواپیما ایجاد شود. این دیواره، رادار را طوری گیج می‌کند که نتواند هدف واقعی را از میان ابر چف تشخیص دهد. دیواره چف با سرعت خیلی کمی سقوط می‌کند و معمولاً ساعت‌های زیادی طول می‌کشد تا به زمین برسد. البته باتوجه به وجود اصطکاک، سرعت قطعه‌های چف در جهت‌هایی غیر از جهت سقوط خیلی سریع به‌سمت صفر میل می‌کند و بنابراین در رادارهای پالس داپلر به عنوان کلاتر دیده می‌شود و تأثیری بر عملکرد آن ندارند.

حفاظت الکترونیکی(EP یا ECCM)

حفاظت الکترونیکی یا ECCM عبارت است از داشتن توانایی و مهارت در کاهش میزان تأثیر حمله‌های الکترونیکی دشمن به طوری که انجام ECCM مؤثرتوسط آن مقدور نباشد یا هزینه آن بسیار گران شود. به طور ساده‌تر می‌توان گفت ECCM یعنی حفظ تجهیزات خودی در برابر اثرات نامطلوب حمله الکترونیکی دشمن.

یک طراح ECCM باید برای مثلاً یک رادار به روش‌های مختلف ECCM که رادار با آن مواجه می‌شود مسلط و از جزئیات آن مطلع باشد و انتخاب‌های متنوعی برای کاربر در دفاع از رادار و مقابله با حمله‌های الکترونیکی فراهم نماید. همچنین اپراتور باید با تکنیک‌های مختلف ECCM آشنا باشد و طوری آموزش ببیند که نوع حمله‌های الکترونیک را تشخیص دهد و هم بتواند یک روش یا ترکیبی از چند روش ECCM

را برای مقابله با آن انتخاب نماید.

بنابراین مؤثرترین امکان برای مقابله با حمله‌های الکترونیکی، داشتن تجهیزات ECCM به روز به همراه نیروی آموزش دیده است. یک رادار که در طراحی آن، ECCM در نظر گرفته شده است را می‌توان از سه جنبه مورد بررسی قرار داد: مدیریت پارامترهای رادار، تکنیک‌های پردازش سیگنال و فلسفه طراحی.

منابع

- Goddard, N. E., ‘‘Instantaneous Frequency-Measuring Receivers,’’ IEEE Trans. on Microwave Theory and Techniques, April 1972, pp. 292–293.
- Boose, G. M., ‘‘Wide Open Frequency Indicating Receiver,’’ paper presented to a joint
- RADAR AND ELECTRONIC WARFARE SYSTEMS Edited by Martin Streetly Fourteenth Edition2002-2003
- P.J. Dombrowski, E. Gholz and A.L. Ross, “Military transformation and the defense industry afterNext: the defemse industrial implications of Network – centric Warfare”, 2003, Naval War College,Newport, Rhode Island, USA

ساخت دستگاه لودری که در زمان چرخش نیاز به فرمان ندارد

به منظور رفع مشکلات کنترل لودر در هنگام چرخش، پژوهشگران کشور دستگاه لودری را عرضه کردند که ضمن کاهش مصرف انرژی برای چرخش به جهات مختلف نیاز به فرمان ندارد.

نیما حضوری- مجری طرح در گفتگو با مهر، با بیان اینکه این لودر با عنوان "لودر چرخشی- سرشی" طراحی شده است، افزود: کنترل لودر در هنگام چرخش به جهات مختلف از جمله مشکلاتی است که رانندگان لودر با آن روبه‌رو هستند. از این رو در این پروژه تحقیقاتی اقدام به بررسی مشکلات در این زمینه شد.

در طراحی این لودر از چند طرح نوآورانه استفاده شده است که از آن جمله می‌توان به سیستم حرکتی ویژه شاسی هرمی و به کارگیری دیفرانسیل به جای گریبکس و هیدروموتور اشاره کرد.

این لودر برای چرخش به جهات مختلف نیاز به فرمان ندارد، جک‌های به کار رفته در این دستگاه امکان استفاده از این دستگاه در ارتفاع‌های بیشتر از ۳۰ متر را فراهم می‌کند.

در نمونه‌های خارجی این لودر از موتوری با قدرت ۶۰ اسب بخار بهره گرفته شده، ولی در این طرح از موتور کوچکی با قدرت ۱۳ اسب بخار استفاده شده است.

این لودر به شکلی طراحی شده است که به طور همزمان دو جک می‌تواند بر روی آن فعال باشد، از دیگر ویژگی‌های لودر چرخشی طراحی شده می‌توان به کاهش مصرف انرژی و کاهش آهن مصرفی در بدنه آن اشاره کرد. این امر باعث پایین آمدن هزینه تولید می‌شود.

به جای قرارگیری "باگت" در جلوی این لودر می‌توان از انواع ابزارها بسته به نوع کارکرد استفاده کرد.

مشاهده رنگ واقعی افراد با «عینک‌های اجتماعی»

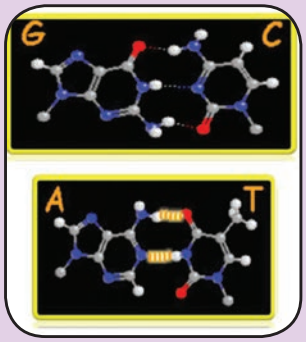
با یک جفت عینک مخصوص می‌توان دید انسان را بهبود بخشید و به او برای درک احساسات، خستگی و حتی وضعیت سلامتی از روی رنگ پوست کمک کرد.

به گزارش ایسنا، چشم انسان قادر است نشانه‌های احساسی، خستگی و سلامت را از روی رنگ پوست تشخیص دهد. رنگ پوست سرخ یا سبز می‌تواند وضعیت احساسی یا سلامتی فرد را تا حدودی مشخص کند. همین توانایی چشم برای تشخیص احساسات و سلامت از روی رنگ پوست، پژوهشگران را به این فکر انداخته است که به فکر طراحی «عینک اجتماعی» بیافتند.

آزمایشگاه ۲AI پیشگام ایده استفاده از قدرت چشم برای تشخیص تغییرات پوست ناشی از کم خونی یا تغییرات سطح اکسیژن در خون است. با محقق شدن ایده ساخت این عینک‌ها، جراحان می‌توانند وضعیت رگ‌های خونی بیماران را ببینند و مأموران امنیتی در فرودگاه‌ها از روی رنگ پوست صورت، افراد مشکوک را شناسایی کنند.

به گفته «مارک چنگیزی»، مدیر بخش شناخت انسان در آزمایشگاه ۲AI، پوست می‌تواند حقایق زیادی از وضعیت احساسی و سلامت انسان را بیان کند، چرا که پوست، در واقع قابلیت نمایش هر رنگی از ترکیب سبز، آبی، زرد و قرمز را دارد.

تشخیص سرطان خون در کمتر از ۲۰ دقیقه میسر شد



پژوهشگران دانشگاه صنعتی اصفهان موفق به طراحی و ساخت بیوسنسور DNA سرطان خون بر پایه نانوذرات اصلاح شده طلا شدند که می‌تواند در کمتر از ۲۰ دقیقه بر اساس توالی خاص ژن عامل سرطان خون این بیماری را شناسایی کند.

دکتر علی‌اصغرانصافی، استاد دانشکده شیمی دانشگاه صنعتی اصفهان و برگزیده گروه علوم پایه هفدهمین جشنواره تحقیقاتی علوم پزشکی رازی در گفت‌وگو با ایسنا، گفت: سرطان مزمن خون باعث افزایش گلبول‌های سفید خون در مغز استخوان می‌شود. سلول‌های سرطانی از مغز استخوان به خون راه می‌یابند و غدد لنفاوی و دیگر ارگان‌ها نظیر جگر و طحال را تحت تأثیر قرار می‌دهند. همچنین سرطان مزمن خون باعث اضمحلال مغز استخوان می‌شود و میزان ایمنی بدن را شدیداً کاهش می‌دهد.

تحقیقات متخصصان ژنتیک نشان می‌دهد که جهش ژنی یکی از عوامل مهم سرطان مزمن خون است، از آنجا که سنسورهای DNA دارای انتخابگری و حساسیت بالا در تشخیص کیفی و کمی گونه‌های هدف هستند، ارائه روش‌های انتخابی بر پایه تشخیص DNA در تحقیقات علوم زیستی و تشخیص بیماری‌های ژنتیکی از اهمیت بالایی برخوردار است.

در این بیوسنسور، تک رشته‌ای از DNA عامل بیماری سرطان مزمن خون را جدا کردیم و بر روی سطح نانوذرات طلا به عنوان بستر قرار دادیم که این تک رشته DNA به سرعت می‌تواند زوج خود را در نمونه خون بیماران تشخیص دهد.

از آنجا که DNA همیشه دو رشته‌یی است، هنگامی که بتوان DNA گونه مورد شناسایی را به صورت تک رشته‌یی از یکدیگر جدا کرد، در واقع یک سنسور حساس تشخیصی ساخته شده است چرا که انتخابگری و حساسیت بسیار بالایی در تک رشته‌ای جدا شده وجود دارد که فقط نسبت به رشته جدا شده خود حساسیت نشان می‌دهد و تنها با آن ممزوج می‌شود.

از آنجا که برخلاف دیگر روش‌های تشخیص بیماری در این روش هیچ‌گونه عملیات خاصی بر روی خون صورت نمی‌گیرد با بیوسنسور DNA می‌توان در مدت حدود ۲۰ دقیقه، وجود و یا نبود سرطان مزمن خون در بیماران را تشخیص داد.

کوچکترین ایستگاه رادیویی جهان توسط دانشمند ایرانی ساخته شد

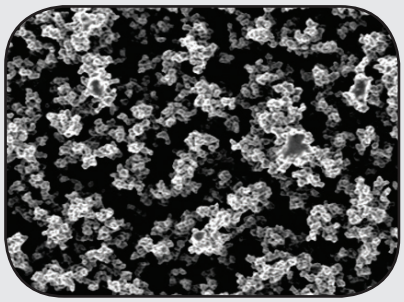
دانشمند ایرانی موسسه فناوری فدرال (ETH) سوییس و همکارانش موفق به ساخت کوچکترین ایستگاه رادیویی دنیا شدند؛ دو مولکول که از طریق تک فوتون‌ها با یکدیگر ارتباط برقرار می‌کنند!

دکتر وحید صندوقدار، سرپرست تیمی تحقیقاتی در مؤسسه ETH با همکاری پژوهشگرانی از مؤسسه ماکس پلانک آلمان در تحقیقات خود نشان دادند که حتی یک تک فوتون در حال حرکت می‌تواند با یک تک اتم یا مولکول در تعامل باشد. اصلی‌ترین چالش پیش روی پژوهشگران تأمین یک منبع مناسب از تک فوتون با فرکانس و پهنای باند مناسب است. زمانی که یک اتم یا مولکول، یک فوتون را جذب می‌کند، یک انتقال موسوم به حالت برانگیخته ایجاد می‌شود. پس از چند نانوثانیه (یک هزار میلیونیوم ثانیه) این حالت برانگیختگی تنزل می‌یابد و یک فوتون ساطع می‌کند.

تیم تحقیقاتی در آزمایش خود از دو نمونه حاوی مولکول فلوئورسنت جاسازی شده در بلورهای آلی استفاده کردند و آنها را تا ۲۷۲- درجه سانتی‌گراد سرد کردند. تک مولکول‌ها در هر دو نمونه با ترکیبی از انتخاب طیفی و فاصله‌ای شناسایی شدند.

برای تولید فوتون منفرد، یک تک مولکول در نمونه منبع برانگیخته شد. با کاهش حالت برانگیختگی مولکول، فوتون‌های ساطع شده جمع‌آوری و بر روی نمونه هدف در فاصله چند متری متمرکز شدند.

نوع تازه‌ای از شیشه‌های خودتمیزشونده تولید شد



پژوهشگران موفق به تولید یک روکش ابرآبگریز شفاف از جنس شیشه شدند.

تحقیقی که توسط دانشمندان بخش تحقیقات پلیمری مؤسسه «ماکس پلانک» در «ماینز» و دانشگاه فنی «دارمشتات» صورت گرفته است، در آینده نزدیک عینک‌ها نیازی به تمیز شدن نخواهند داشت و شیشه‌های کثیف خودرو بخشی از گذشته خواهند بود.

آنها از دوده شمع برای تولید یک روکش اَبَرآبگریز شفاف بهره برده‌اند که از شیشه ساخته شده است. آب و روغن از روی این روکش می‌لغزند و هیچ چیزی پشت سر خود باقی نمی‌گذارند. حتی زمانی که این روکش استفاده از روش ماسه‌پرانی (سندپلاست) آسیب می‌بیند، این ویژگی را حفظ می‌کند.

این ماده خاصیت خود را مدیون نانوساختار خود است. سطوح روکش‌دهی شده با استفاده از این ماده می‌توانند در هر کاربردی که کثیفی یا حتی لایه نازکی از آب مضر باشد و یا ایجاد مزاحمت کند، مورد استفاده قرار بگیرند. به عنوان مثال از کاربردهای دیگر این ماده می‌توان به استفاده از آن در شیشه‌های آسمانخراش‌ها یا ابزارهای پزشکی اشاره کرد.

این روکش از یک ماده بسیار ساده یعنی سیلیکا ساخته شده است که ماده اصلی تشکیل‌دهنده تمام شیشه‌ها است. پژوهشگران سطوح سیلیکایی را با یک ترکیب فلوئورید سیلیکونی روکش‌دهی کرده‌اند و ویژگی دفع آب و روغن را در این سطوح ایجاد کردند. بخش هوشمندانه این کار ساختار بسیار جالب این روکش است.

ساختار این لایه شبیه یک مارپیچ اسفنج مانند از حفرات کاملاً بی‌نظم است؛ دیواره‌های این مارپیچ از کُره‌های بسیار کوچک ساخته شده است.

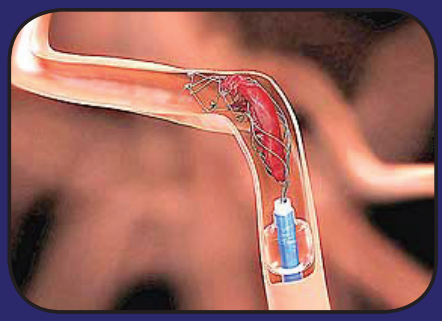
ابرها به زمین نزدیک‌تر می‌شوند

نتایج تحقیقات پژوهشگران دانشگاه اوکلند نشان می‌دهد، طی یک دهه اخیر ارتفاع ابرها کاهش یافته است و به سطح زمین نزدیک‌تر شده‌اند و علت اصلی این مسئله نیز گرمایش جهانی عنوان شده است.

در سال ۱۹۹۹ میلادی ماهواره «ترا» ناسا با سیستم اسپکترورادیومتر چند زاویه‌ای (MISR) به فضا پرتاب شد تا تغییرات جوی را مورد بررسی قرار دهد. این ماهواره مجهز به ۹ دوربین تصویربرداری است که می‌تواند از زوایای مختلف از ابرها تصویربرداری کند.

پروفسور «راجر دیویس» سرپرست تیم تحقیقاتی، تصاویر ماهواره «ترا» در ۱۰ سال اخیر را مورد تجزیه و تحلیل قرار داده است. با اندازه‌گیری ارتفاع و سرعت حرکت ابرها مشخص شد که ابرها در طول این مدت به سطح زمین نزدیک‌تر شده‌اند.

میزان دی اکسید کربن هر روز در حال افزایش است و این فرایند منجر به گرم شدن زمین و افزایش دمای سطح خواهد شد که باعث نزدیک‌تر شدن ابرها به زمین می‌شود و به دنباله آن، حجم ابرهایی که در ارتفاع‌های بالاتر قرار دارند، هر روز در حال کاهش یافتن است. نتایج این تحقیق در مجله تحقیقات ژئوفیزیک (Geophysical Research Letters) به چاپ رسیده است.



درمان لخته خونی در مغز

شیوه جدید درمان انسداد رگ‌های مغزی که توسط پژوهشگران دانشگاه کالیفرنیا لس آنجلس ارائه شده است، به صورت همزمان می‌تواند چرخه گردش خون را احیا کند و لخته‌های خونی را از بین ببرد.

آزمایش این ابزار در دوره‌های بالینی بسیار امیدوار کننده بوده است، پژوهشگران در آزمایشی با مقایسه این ابزار و ابزار دیگری که سازمان دارو و غذای آمریکا آن را به تأیید رسانده، دریافتند ابداع جدید با نام Covidien Solitaire در مقایسه با ابزاری که پیش از این به تأیید FDA رسیده بود در درمان مبتلایان به سکته مغزی از ۶۰ درصد کارایی بیشتر برخوردار است.

برای استفاده از این ابزار جدید چهار مرحله جراحی نیاز خواهد بود؛

۱- ایجاد حفره‌ای بر روی لخته خون با استفاده از یک میکروسوند؛

۲- راندن ابزار Solitaire به درون میکروسوند تا جایی که ابزار بتواند خود را به انتهای لخته خونی برساند؛

۳- عقب کشیدن سوند تا ابزار Solitaire منبسط می‌شود و لخته را به دام بیاندازد؛

۴- کشیدن دوباره ابزار به درون میکروسوند و استفاده از ابزار مکش برای خارج کردن لخته از رگ.

شیوه های پیشین از بین بردن لخته‌های خونی که به تأیید FDA رسیده بودند از کارایی زیادی برای خارج کردن لخته‌های خونی برخوردار نبودند و احتمال از دست دادن لخته با استفاده از این تکنیک‌ها زیاد بود.

میوه قرمز بخورید سالم بمانید

پژوهشگران می‌گویند خوردن میوه‌ها و سبزی‌های دارای رنگ قرمز برای سلامتی بسیار مفید است.

به نقل از یونایتدپرس، فیل لمپرت کارشناس تغذیه در آمریکا گفت: میوه و سبزی‌های دارای رنگ قرمز حاوی موادی هستند که خطر ابتلا به سرطان پروستات را کاهش می‌دهند، سبب کاهش فشار خون می‌شوند، روند رشد تومورها را کند می‌کنند و میزان لیپوپروتئین‌ها -کلسترول بد خون- را نیز کاهش می‌دهند.

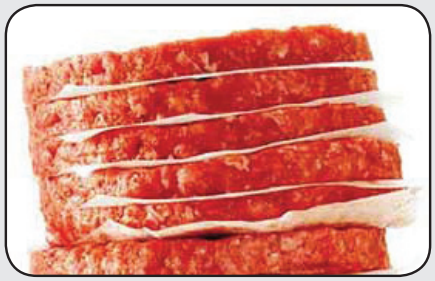
گوجه‌فرنگی و هندوانه دارای نوعی آنتی‌اکسیدان به نام لیکوپین هستند که برای سلامت چشم‌ها و درمان پروستات مفید است.

گوجه‌فرنگی پخته شده و رب گوجه، سس کچاپ و همچنین گوجه‌فرنگی‌های کنسرو شده دارای میزان زیادی لیکوپین هستند. آب زغال اخته که برای جلوگیری از عفونت ادرار مفید است همچنین میزان کلسترول خوب خون و مواد آنتی‌اکسیدان را در بدن افزایش می‌دهد. سیب قرمز نیز منبع غنی ویتامین سی، فیبر و آنتی‌اکسیدان‌هاست.

توت‌فرنگی حاوی مقادیر زیادی ویتامین منگنز است. منگنز به کاهش رادیکال‌های آزاد در بدن کمک می‌کند، سبب استحکام استخوان‌ها می‌شود، عملکرد غده تیروئید را بهبود می‌بخشد و میزان قند خون را تنظیم می‌کند.

گیلاس حاوی ملاتونین و آنتی‌اکسیدان است که به تنظیم الگوی خواب طبیعی بدن کمک و از زوال عقل جلوگیری می‌کند، میزان تورم، درد، خطر ابتلا به سرطان، بیماری‌های قلبی، دیابت، آلرژی‌ها را کاهش می‌دهد. فلفل دلمه‌ای قرمز نیز سرشار از ویتامین آ و ب ۶ است که به بهبود خلق و خو و خواب کمک می‌کند.

گوشت گیاهی تولید شد



یک پژوهشگر آمریکایی موفق به تولید گوشت با پایه گیاهی شده است که از لحاظ طعم شباهت زیادی با گوشت حیوانات دارد.

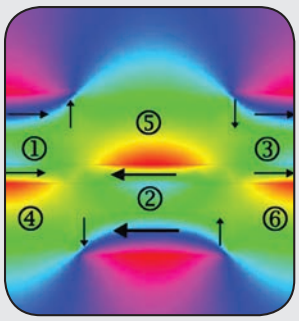
پیش‌بینی می‌شود مصرف گوشت تا سال ۲۰۵۰، به دو برابر میزان فعلی برسد و دستاورد جدید در تولید گوشت با پایه گیاهی می‌تواند پاسخگوی نیاز سیری‌ناپذیر مردم جهان به مصرف گوشت و گامی مهم برای پیشگیری از عوارض ناشی از مصرف این محصول باشد.

«پاتریک براون» متخصص زیست‌شناسی مولکولی دانشگاه استانفورد معتقد است: می‌توان با استفاده از مواد گیاهی فراوان و ارزان که در اطراف ما وجود دارند، یک ماده غذایی مقوی و سرشار از پروتئین تولید کرد که از لحاظ ظاهر و طعم مشابه گوشت حیوانات است.

«مارک پست» از پژوهشگران دانشگاه آیندهوون هلند تأکید می‌کند: این روش که مبتنی بر تکنیک سلول‌های بنیادی برای رشد اندام‌های جایگزین یا تولید بافت انسانی در آزمایشگاه است، بسیار پرهزینه است و برای تولید انبوه گوشت مناسب نیست.

روش ابداعی پژوهشگر آمریکایی در مقایسه با سایر ایده‌ها، مقرون به صرفه‌تر است و در صورت طعم مناسب می‌تواند جایگزین مناسبی برای گوشت حیوانات باشد. گوشت تولید شده با پایه گیاهی احتمالاً تا پایان سال جاری میلادی به بازار عرضه خواهد شد.

سوپرلنز با قابلیت استفاده در تمام طیف‌های نوری ساخته می‌شود



پژوهشگران آمریکایی موفق شدند با استفاده از پدیده پلاسمونیک، سوپرلنزی بسازند که از طیف مادون قرمز تا فرابنفش قابل استفاده باشد.

«دوردو گونی» از دانشگاه صنعتی «میشیگان» می‌گوید: با استفاده از یک سوپرلنز می‌توان وجود ویروس را در یک قطره خون مشاهده کرد. با این کار می‌توان میکروسکوپ‌هایی با قدرت تفکیک بالا ساخت.

لنزهای نوری دارای یک محدودیت ذاتی به نام «محدودیت پراش» هستند که موجب می‌شود تا ما قادر به دیدن اجسام کوچکتر از ۲۰۰ نانومتر نباشیم. هر چند با SEM می‌توان ذرات کوچکتر از این را هم دید، اما این دستگاه گران قیمت، سنگین و غیرقابل حمل است. برای ساخت سوپرلنز به ماده مصنوعی نیاز است، موادی سنتزی که در طبیعت وجود خارجی ندارند. پژوهشگران برای تحقق رویاهایی نظیر ساخت لباس نامرئی کننده و سوپرلنز، تلاش خود را برای ساخت سوپرلنز آغاز کرده‌اند. «دوردو گونی» موفق به ساخت سوپرلنزی شد که می‌توان با آن اجسامی در حد ۱۰۰ نانومتر را مشاهده کرد.

راز این کار در پدیده پلاسمونیک نهفته است. پلاسمون‌ها، نوسان‌های بارها در نزدیک سطح یک فیلم فلزی نازک هستند که با نانوساختارهای ویژه‌ای ترکیب شده‌اند. زمانی که این بارها توسط یک میدان مغناطیسی تحریک می‌شوند، پرتوهای نور را از یک جسم جمع‌آوری و به شکلی منعکس می‌کنند که مشابه آن در طبیعت وجود ندارد. با این کار می‌توان بر «محدودیت پراش» غلبه کرد و اجسامی به کوچکی یک هزارم قطر تار مو را مشاهده کرد.

برای ساخت تراشه‌های کامپیوتری از لیزر فرابنفش استفاده می‌شود که بسیار گران‌قیمت است، اما با سوپرلنز می‌توان از لیزر قرمز به جای فرابنفش استفاده کرد که بسیار ارزان و کار با آن ساده‌تر است.

راز زنده ماندن حشره میوه در دمای انجماد کشف شد

یک لارو حشره میوه که سال گذشته به حالت منجمد درآمده بود، اکنون بیدار شده و به رشد خود ادامه می‌دهد.

پژوهشگران چک در سال ۲۰۱۱، نیمی از آب بدن حشره Drosophila melanogaster را در دمای انجماد به شکل منجمد درآورده بودند. اکنون این حشره کاملاً از قدرت جفت‌گیری برخوردار است و لاروهای جدید آن نیز در سلامت کامل هستند.

تاکنون تصور بر این بوده که تحمل دمای انجماد در حیوانات یک فرایند پیچیده است و تنها برخی حشرات قادر به انجام آن هستند. این در حالی است که تجمع بلورهای یخ در بدن بسیاری از مهره‌داران بسیار مضر و یا کشنده است. پژوهشگران با هدف درک میزان پیچیدگی کمک به تحمل دمای انجماد در D. Melanogaster که یکی از مهم‌ترین مدل‌های جانوری در زیست‌شناسی مدرن است، این آزمایش را انجام دادند.

یک گونه همسان حشره میوه قطبی موسوم به Chymomyza costata قادر است دمای منفی ۳۰ درجه نیتروژن مایع را تحمل کند. تحقیقات پیشین پژوهشگران نشان داده بود که این حشرات با انباشت اسید آمینه L پرولین در بدن خود قادر به تحمل این دما هستند. پژوهشگران چک با استفاده از نتایج پژوهش پیشین به تغذیه این لارو توسط L پرولین و گلیسرول پرداخته و سپس آن را منجمد کردند.

این حشره توانست این حالت نیمه انجماد را برای ۷۵ دقیقه تحمل کند و سپس دوباره به حیات خود ادامه دهد.

پژوهشگران دیگر در تلاش برای منجمد کردن حشرات میوه برای درک بهتر ژن‌های پایه‌گذار استعداد تحمل سرما در آنها هستند. این تحقیقات به درک بهتر احتمال اجرای این فرایند در انسان‌ها کمک کرده است و می‌توان مدت طولانی‌تری از اندام‌ها در یخ نگهداری کرد. همچنین زیست‌شناسان می‌توانند از این روش در تحقیقات خود بر روی این حشرات استفاده کنند.

پلاستیک زیستی با کمک نانوذرات تهیه می‌شود

گروهی از دانشمندان هلندی توانستند با استفاده از نانوذرات آهن به عنوان کاتالیزور واکنش‌های شیمیایی از بیومس پلاستیک زیستی تولید کنند.

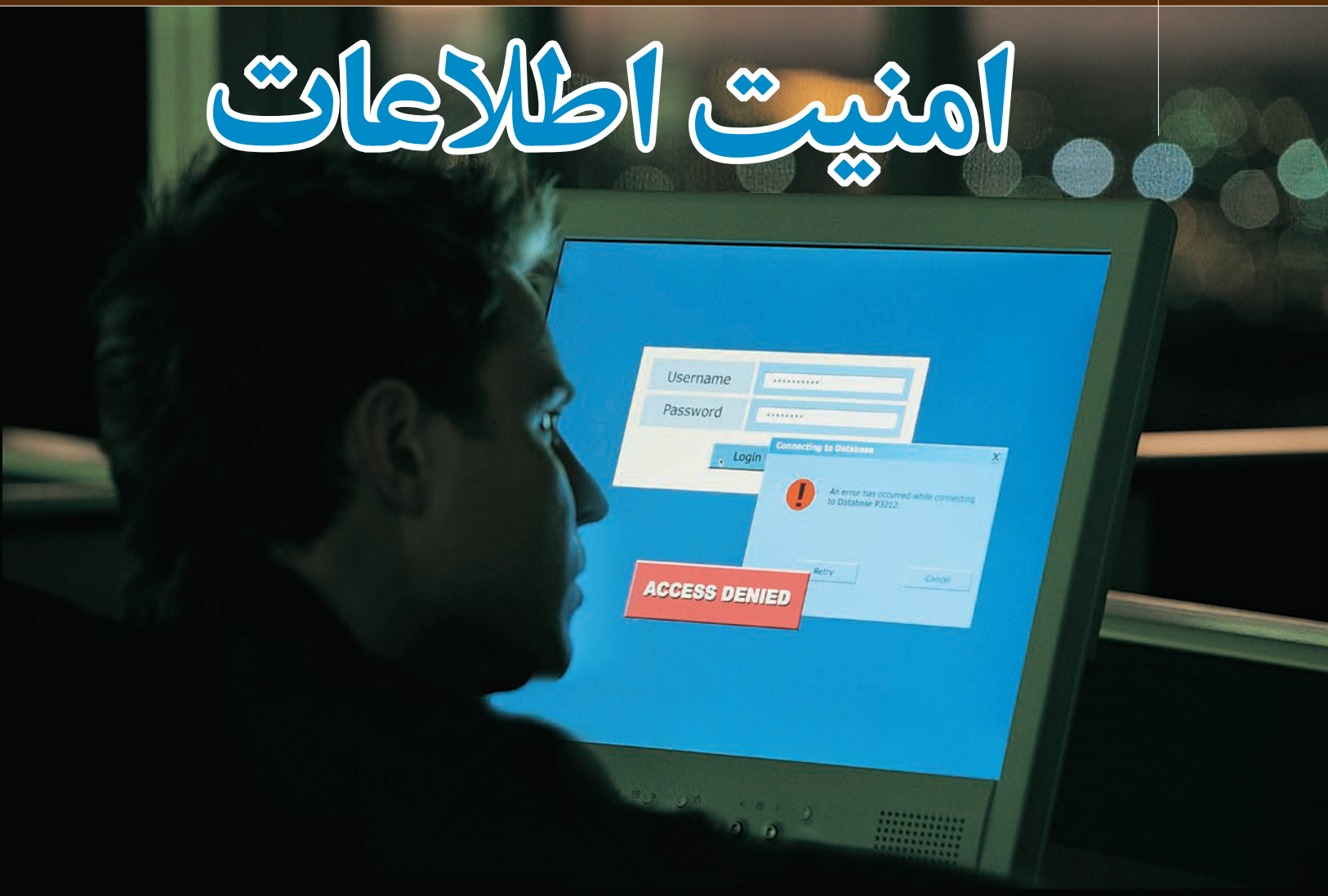
پژوهشگران دانشگاه اوتریخت در هلند نشان دادند که چگونه می‌توان بر پایه بیومس (زیست توده) ترکیبات پایه مواد پلاستیکی را به روشی مؤثر و پاک تولید کرد.

راه موفقیت این روش جدید در استفاده از کاتالیزوری از جنس نانو ذرات آهن روی ورقه‌ای از نانو الیاف کربن است که برای انجام واکنش‌های شیمیایی تبدیل مواد به کار می‌رود. تمام مواد پلاستیکی از ماده‌ای به نام "اولفین" ساخته می‌شوند. "اولفین" مولکولی آلی است که از اتم‌های کربن و هیدروژن ساخته می‌شود.

برای تهیه اولفین‌ها به روش سنتی از مشتقات نفتی چون "نفتا" استفاده می‌شود. این مشتقات از طریق واکنش‌های هوازدگی شیمیایی و ترموشیمیایی تبدیل می‌شوند. اما این روش‌های رایج چه از نظر زیست محیطی و چه از نظر هزینه‌ها مشکلاتی ایجاد می‌کنند. به همین دلیل شیمیدانان مدتها است به دنبال راهی برای تولید اولفین از طریق مواد اولیه و فرایندهای متفاوتی می‌گردند.

براساس گزارش ساینس، اکنون این دانشمندان توانستند با ساخت کاتالیزوری بر پایه نانوذرات آهن که روی ورقه‌ای از نانو الیاف کربن قرار گرفته است به روشی پاک از بیومس پلاستیک زیستی دست یابند.

امنیت اطلاعات

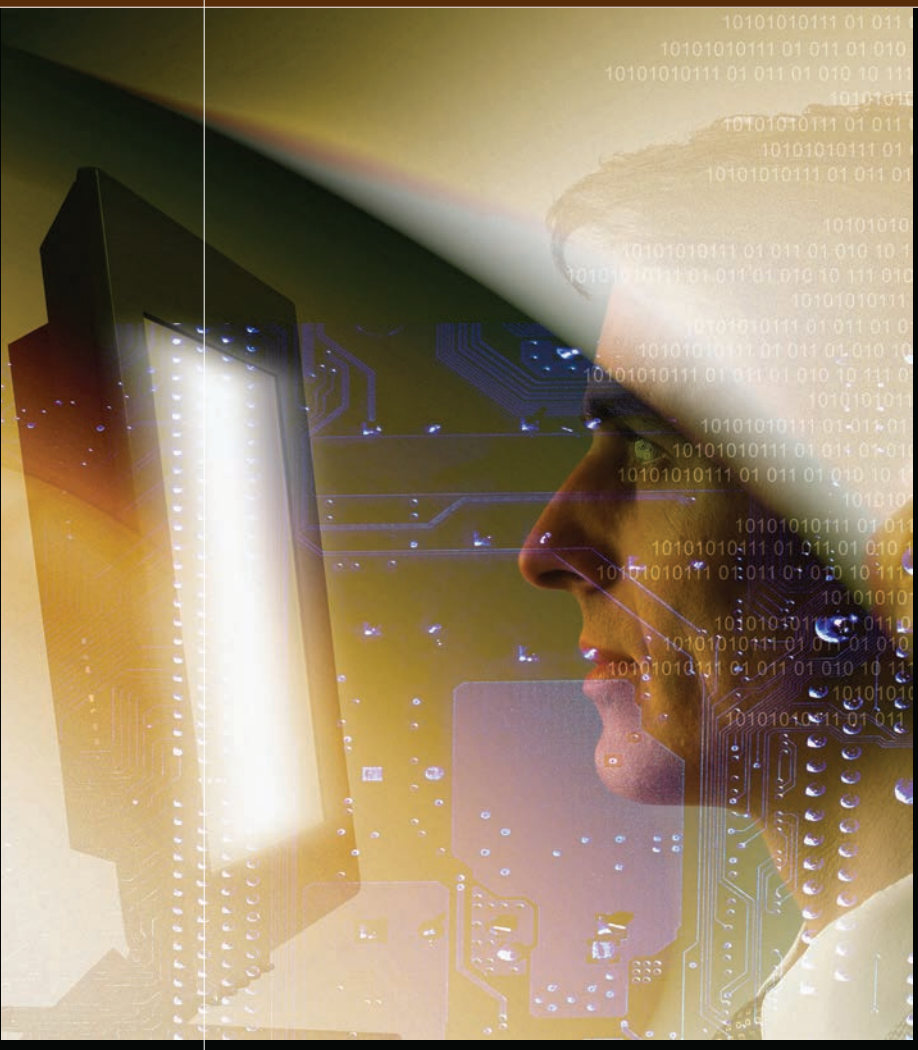


در سال‌های اخیر با پیشرفت فناوری اطلاعات و ارتباطات شاهد به کارگیری تجهیزات الکترونیک و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های روزمره همچون ارائه خدمات، مدیریت و نظارت و اطلاع‌رسانی هستیم. فضایی که چنین فعالیت‌هایی در آن صورت می‌پذیرد با عنوان فضای تبادل اطلاعات شناخته می‌شود. فضای مذکور همواره در معرض تهدیدهای الکترونیکی یا آسیب‌های فیزیکی از قبیل جرایم سازمان یافته به منظور ایجاد تغییر در محتوا یا جریان انتقال اطلاعات، تخریب بانک‌های اطلاعاتی، اختلال در ارائه خدمات اطلاع‌رسانی یا نظارتی و نقض حقوق مالکیت معنوی است.

از طرف دیگر با رشد و توسعه فزاینده‌ی فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای یاد شده، گسترده‌تر می‌شود. از این رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهم‌ترین اهداف توسعه فناوری اطلاعات و ارتباط محسوب می‌شود.

▫ عصر اطلاعات و دانش ▫

عصر کنونی عصر اطلاعات و دانش نامیده می‌شود. عمده‌ترین دلیل این نامگذاری به افزایش وسعت شبکه‌ها و دسترسی آسان به اطلاعات و همچنین اهمیت اطلاعات و دانش در مناسبت‌های اجتماعی است. البته همزمان با این وضعیت، خطرات امنیتی نیز می‌شوند. البته در سوی دیگر، طی پژوهشی پیرامون موضوع آگاهی از امنیت اطلاعاتی کاربران معلوم شد که در سال‌های بین ۲۰۰۴



تا ۲۰۰۶، میزان متوسط زیان و تعداد قانون شکنی‌های امنیتی به حد چشمگیری کاهش پیدا کرد. یکی از دلایل اصلی در ارتقای مشکلات امنیتی، سرمایه‌گذاری‌های مستمر شرکت‌های کوچک و متوسط در امنیت فناوری اطلاعات و برنامه‌های آگاهی از امنیت اطلاعات بوده است. کارمندان استفاده‌کننده از فناوری اطلاعات به تنهایی در متوقف‌سازی رخداد قانون‌شکنی‌های امنیتی نمی‌توانند مؤثر باشند بلکه آگاهی امنیتی کاربران نهایی باید ارتقاء داده شود و یک توازن منطقی بین راه‌حل‌های فنی و غیر فنی در سازمان وجود داشته باشد.

یکی از جنبه‌ها و راه‌های غیر فنی برای حفاظت و مدیریت امنیت اطلاعات ارتقای آگاهی کاربران از امنیت اطلاعات است در این صورت افراد، به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود آگاه خواهند بود. آگاهی از امنیت اطلاعات در افراد منجر به ایجاد تغییر رفتار و تقویت فعالیت‌های خوب امنیتی می‌شود و به آنها اجازه می‌دهد تا نسبت به امنیت فناوری اطلاعات نگران و پاسخگو باشند و به تدریج به فرهنگ در سازمان‌ها تبدیل خواهد شد.

بنابراین بایستی به موازات تمهیدات فنی اعمال شده برای امنیت اطلاعات، در قوانین و سیاست‌های جاری متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر گردد و فرهنگ و آموزش‌های صحیح به کارگیری اطلاعات و تأمین امنیت آنها در اولویتی بالاتر نیز در سطح جامعه ترویج شود. بدیهی است که فقدان توجه به مقوله امنیت اطلاعات و افزایش ندادن آگاهی‌های لازم برای امنیت اطلاعات متناسب با سطوح مختلف افراد مانع از گسترش فضای اطلاعاتی در میان آحاد جامعه و جلب اعتماد مدیران در به کاگیری روش‌های نوین نظارتی واطلاع‌رسانی خواهد شد. ایجاد چهارچوبی کلی در سطح کلان با لحاظ کردن ویژگی‌های خاص فضای تبادل اطلاعات و مقوله امنیت در این فضا یک ضرورت است.

با افزایش دانش و آگاهی‌های کارمندان یک سازمان از امنیت اطلاعات، رعایت اصول امنیتی در افراد به تدریج نهادینه می‌شود؛ و این امر به تغییر فرهنگ‌ها و ارزش‌های امنیتی کمک می‌کند و از این طریق صلاحیت امنیتی بهتری ایجاد می‌شود. اگرچه روشی واحد که با تمامی موقعیت‌ها منطبق باشد در سطح سازمانی و انسانی در عملکردهای مختلف برنامه‌های مربوط به ارزیابی و ارتقاء آگاهی امنیتی یکسانی وجود ندارد، داشتن یک رویه مشخص برای برقراری برنامه‌های ارزیابی و ارتقاء بر اساس سطوح آگاهی امنیتی بسیار ضروری است.

▫ تاریخچه‌ی امنیت اطلاعات ▫

مفهوم و اهمیت ایمنی و امنیت از همان آغاز زندگی بشر وجود داشت، بشر همیشه برای بقا و ادامه زندگی سعی کرده است که برای حفاظت از خود و دارایی‌هایش، آگاهی‌ها و دانش خود را نسبت به محیط و خطرات اطراف افزایش دهد. ایمنی و امنیت، مفهومی ذاتی است که با حفاظت از چیزهای ارزشمند ارتباط پیدا می‌کند؛ به طور خلاصه ایمنی به راه‌های ممکن که در آن سلامت یک سیستم

بایستی تأمین و دفع نقایصی که در راه حصول به اهداف وجود دارد، تعریف می‌شود.

جهان با گذشت زمان به قول دیوید هاروی به سوی نوعی فشردگی پیش می‌رود، زمان و مکان درهم آمیخته است، مرکزهای لرزان و بی‌ثبات داده است و هویت‌های کدر ناخالص جایگزین هویت‌های تاب و خالص گشته است. از این لحاظ، امنیت نیز مفهوم سنتی و کلاسیک خود را از دست داده است.

از منظر زبان‌شناسانه دال امنیت به مدلول خاص و ثابتی رجوع نمی‌دهد و در گفتمان‌های گوناگون مصداق‌های متفاوتی به خود می‌گیرد اما حفاظت از اطلاعات به عنوان مهم‌ترین سرمایه سازمان‌ها همیشه مورد توجه قرار داشت، قبل از ظهور عصر شبکه‌ها، اطلاعات به صورت پرونده‌های کاغذی بایگانی می‌شد هر چند این رویه هنوز رایج است. با پدید آمدن شبکه‌ها و دسترسی آسان به اینترنت قسمت اعظم اطلاعات از طریق این بستر که فضای تبادل اطلاعات نام دارد در حال انتقال و پردازش است. قسمت اعظم اطلاعات به صورت دیجیتالی ذخیره و بازیابی شده و در این فضا، سرعت و دقت انتقال اطلاعات خیلی بیشتر است. به موازات گسترش شبکه‌های محلی و سراسری تهدیدات و سرقت و تخریب اطلاعات نیز بیشتر می‌شود به طوری که شاید یکی از مهم‌ترین مسائل در عصر اطلاعات، حفاظت آنها باشد.

امنیت اطلاعات در عصر کامپیوتر

دامنه‌ی امنیت اطلاعات در عصر کامپیوتر به شدت تغییر کرده است. در آغاز این دوره، مسائل امنیتی مربوط به مسائل زیر می‌شد:

- امنیت فیزیکی مکانی و موقعیت کامپیوترها؛
- تأیید قابلیت اعتماد کارکنانی که با سیستم‌های کامپیوتری سروکار دارند.

بهترین مثال این دوره را می‌توان پروژه‌ی کلوسس دانست. پروژه مذکور در بلکی پارک لندن در نیمه دوم جنگ جهانی دوم به اجرا درآمد. بلکی پارک به منظور تسهیل رمزگشایی پیام‌های مبادله شده بین نیروهای متفقین ساخته شده بود. طی جنگ جهانی دوم، آلمان از مدل‌های ماشینی رمزگذاری/رمزگشایی الکترونیکی فراوانی با نام انیگما استفاده می‌کرد به منظور تسریع فرایند رمزگشایی پیام‌های منفصل، بلکی از ماشین حساب‌های الکترومغناطیسی با نام پمپ استفاده می‌کرد. در طول جنگ، آلمان‌ها هرگز در مورد فعالیت‌های بلکی پارک اطلاعاتی پیدا نکرد و پروژه، محرمانه ماند. اطلاعات در زمینه‌ی این پروژه در سال ۱۹۷۰، منتشر گردید.

در دهه ۱۹۷۰، تمرکز اصلی بر روی امنیت فیزیکی ساختمان‌ها و نیز ایجاد انگیزه مناسب در کاربران بوده است. مسائل این دوره به موارد زیر محدود می‌شد:

- محافظت در برابر فجایع مانند آتش، سیل، نوسان‌های نیرو و ...
- محافظت در برابر افشای اطلاعات. در این دوره سیستم‌های ارتباطی چندان برای انتقال داده بین تجهیزات مختلف به کار نمی‌رفت. بنابراین داده در قالب مستندات کاغذی ارائه شده و سپس وارد سیستم کامپیوتری می‌شد. از افشای اطلاعات نیز به طور عمده توسط جلوگیری از ذخیره غیر مجاز اطلاعات بر روی رسانه مغناطیسی یا مستندات کاغذی جلوگیری می‌شد. به منظور جلوگیری از این گونه تقلب‌ها، کارمندان به صورت کاملاً جدی تحت نظر مدیریت قرار داشتند.
- محافظت در برابر خطاهای ناشی از بد عمل کردن سخت افزار، در این دوره زمانی، فناوری بسیار ناپایدار از امروز بود، همان‌طور که نرم‌افزار در حال حاضر ناپایدار است. اجزای کامپیوتری ممکن بود هر روز از کار بیفتند و زمان بین خرابی‌ها در قیاس ساعت و بلکه روز بوده است.

اینترنت و امنیت اطلاعات

اینترنت در سال ۱۹۶۹، با شبکه‌ای به نام آرپانت که مربوط به وزات دفاع امریکا بود، راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌ای متصل به هم شرایطی ایجاد شود که حتی اگر بخش‌های عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد کل شبکه به کار خود ادامه دهد و اطلاعات شبکه حفظ شود. از همان ابتدا فکر ایجاد شبکه برای جلوگیری از اثرات مخرب حملات اطلاعاتی مطرح شد.

در سال ۱۹۷۱، تعدادی از رایانه‌های دانشگاه‌ها و مراکز دولتی به این شبکه‌ها متصل شدند و پژوهشگران از این طریق شروع به تبادل اطلاعات کردند. با بروز رخدادهای غیر منتظره در اطلاعات، توجه به مسائل امنیت اطلاعات بیشتر شد. در سال ۱۹۸۸، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه مواجه شد که بعداً کرم موریس نام گرفت. رابرت موریس که یک دانشجو در

نیویورک بود برنامه‌ای نوشت که می‌توانست به یک رایانه دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌ای دیگر نفوذ کند و سپس به صورت هندسی تکثیر گردد. آن زمان ۸۸۰۰۰ رایانه به این شبکه وصل بود این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه از کار بیفتد. به دنبال این حادثه، بنیاد مقابله با حوادث امنیت شکل گرفت که در هماهنگی فعالیت‌های مقابله با حمله‌های ضد امنیتی، آموزش و تجهیز شبکه‌ها و روش‌های پیشگیرانه نقش مؤثری داشت.

شرکت آی بی ام نخستین سازنده‌ای بود که اهمیت امنیت اطلاعات را تشخیص داد و گروهی را در اوایل دهه ۱۹۷۰، به عنوان مسئول مسائل امنیتی ایجاد کرد. در دهه‌های ۱۹۸۰ و ۱۹۹۰، دید وسیع‌تری نسبت به مسائل امنیت اطلاعات ایجاد شد. از جمله این پیشرفت‌ها عبارتند بودند از:

- توسعه سریع سیستم‌های ارتباطی؛
- معرفی کامپیوترهای شخصی و به خصوص محیط‌های محاسباتی توزیع شده در زیرساخت‌های ارتباطی.

در دهه‌ی اخیر با رشد روز افزون کامپیوترها، فناوری اطلاعات تقریباً در تمامی زمینه‌های زندگی ما وارد شد. تمدن ما وابسته به این فناوری است و عملکرد صحیح این فناوری برای پیشرفت مداوم ضروری است.

رهنمودهایی برای نشر اطلاعات در اینترنت

یکی از ویژگی‌های قابل توجه اینترنت، امکان نشر اطلاعات توسط علاقمندان متناسب با زمینه‌های مورد علاقه است. با توجه به اینکه اینترنت یک منبع عمومی است، در زمان نشر اطلاعات می‌بایست با رعایت موارد امنیتی از انتشار اطلاعاتی که دستیابی عمومی به آن توجیه منطقی ندارد، اجتناب شود.

اینترنت، یک منبع بزرگ اطلاعاتی با قابلیت دستیابی همگانی است که از آن برای ارتباط، تحقیق و یافتن اطلاعات افراد در اقصی نقاط جهان استفاده می‌گردد. رسانه‌ای بس فراگیر که در عمر کوتاه خود توانسته است منشأ تحولات فراوانی در عرصه حیات بشر گردد. بسیاری از کاربران در زمان استفاده از اینترنت این تصور را دارند که به صورت ناشناس از منابع اطلاعاتی موجود استفاده می‌نمایند و در زمان برقراری ارتباط با سایر افراد به صورت گمنام باقی می‌مانند. ذکر این نکته ضروری و از جهاتی نیز حائز اهمیت است که شما در زمان استفاده از اینترنت ناشناس نخواهید بود و امکان یافتن اطلاعاتی در رابطه با شما برای دیگران وجود خواهد داشت همانگونه که شما نیز می‌توانید اطلاعاتی را در رابطه با سایر کاربران آنلاین اینترنت پیدا نمایید. فقدان توجه به موضوع فوق، کاربران اینترنت را در معرض تهدید یا آسیب جدی قرار خواهد داد. اکثر مردم عموماً درخصوص اشتراک اطلاعات شخصی با افراد غریبه‌ای که ممکن است در خیابان با آنها مواجه شوند، جانب احتیاط را رعایت می‌نمایند ولی همان افراد در زمان استفاده از اینترنت درخصوص ارسال اطلاعات شخصی خود با سایر کاربران اینترنت تردید نمی‌کنند و متأسفانه در مواردی نیز زیاده‌روی توأم با اغراق می‌شود. به خاطر داشته باشید پس از انتشار اطلاعات بر روی اینترنت، امکان دست‌یابی و استفاده از آن توسط افراد ناشناس بی‌شماری در اقصی نقاط جهان فراهم می‌گردد و شما هیچ تصوری درخصوص نحوه استفاده از اطلاعات منتشر شده نمی‌توانید داشته باشید.

- اینترنت را به عنوان یک رمان درنظر بگیرید نه یک دفتر خاطرات روزانه. آیا پس از نشر اطلاعات مورد علاقه خود و مشاهده‌ی آنان توسط سایر کاربران اینترنت برای شما مشکل

خاصی ایجاد نمی‌گردد؟ پس از انتشار اطلاعات مورد علاقه خود، افرادی که شما هرگز آنان را ندیده‌اید، می‌توانند صفحات و اطلاعات شخصی شما را پیدا کنند و به آنان دست‌یابی داشته باشند. حتی اگر شما دارای یک روزنامه و یا وبلاگ آنلاین هستید، به موازات انتشار مطالب، امکان استفاده عمومی از آنان فراهم می‌گردد. برخی سایت‌ها ممکن است از رمزهای عبور و سایر روش‌های امنیتی برای حفاظت از اطلاعات و محدودیت در دستیابی به آنان استفاده نمایند ولی روش‌های فوق توسط اکثر وب‌سایت به کار گرفته نمی‌شود. درصورتی که قصد انتشار اطلاعات خصوصی خاصی را دارید و یا تنها افراد محدودی می‌بایست به آنان دستیابی داشته باشند، شاید اینترنت بهترین گزینه در این رابطه نباشد.

- دقت لازم درخصوص نشر اطلاعات و ماهیت آن: در گذشته‌ای نه چندان دور، یافتن اطلاعات به جز شماره تلفن و آدرس سایر افراد کار مشکلی بود. ولی امروزه با توجه به ویژگی‌های منحصر به فرد اینترنت، یافتن اطلاعات متفاوت سایر افراد کار مشکلی نیست. هم اینک حجم بسیار گسترده‌ای از اطلاعات به صورت آنلاین است و امکان دست‌یابی عمومی به آن وجود دارد. با توجه به این که تعداد زیادی از علاقمندان، صفحات وب شخصی نیز ایجاد می‌نمایند، این موضوع روندی کاملاً تصاعدی و فزاینده دارد. در زمان انتشار اطلاعات همواره می‌بایست به این واقعیت مهم توجه شود که اطلاعات منتشر شده برای تمام کاربران در سراسر جهان قابل استفاده خواهد بود.

- توجه به این واقعیت که نمی‌توان وضعیت را به حالت قبل برگرداند: پس از انتشار اطلاعات، اطلاعات منتشر شده برای سایر کاربران و موتورهای جستجو در دسترس خواهد بود. قبل از انتشار اطلاعات می‌توان آن را ویرایش یا حذف کرد ولی پس از انتشار اطلاعات و استفاده از آن توسط سایر کاربران نمی‌توان آن را تغییر داد. حتی در صورتی که شما صفحات حاوی اطلاعات منتشر شده را حذف نمایید، همواره این احتمال وجود خواهد داشت که برخی از کاربران صفحات فوق را بر روی کامپیوتر خود ذخیره کرده باشند یا بخش‌هایی از آن در سایر منابع اطلاعاتی منتشر شده باشد. برخی از موتورهای جستجو، نسخه‌هایی از صفحات وب را به منظور بازیابی سریع‌تر، ذخیره موقت می‌نمایند. صفحات فوق ممکن است حتی پس از حذف نیز قابل دستیابی باشند. برخی مرورگرهای وب نیز ممکن است صفحاتی را که قبلاًمشاهده شده است، نگه‌داری نمایند.

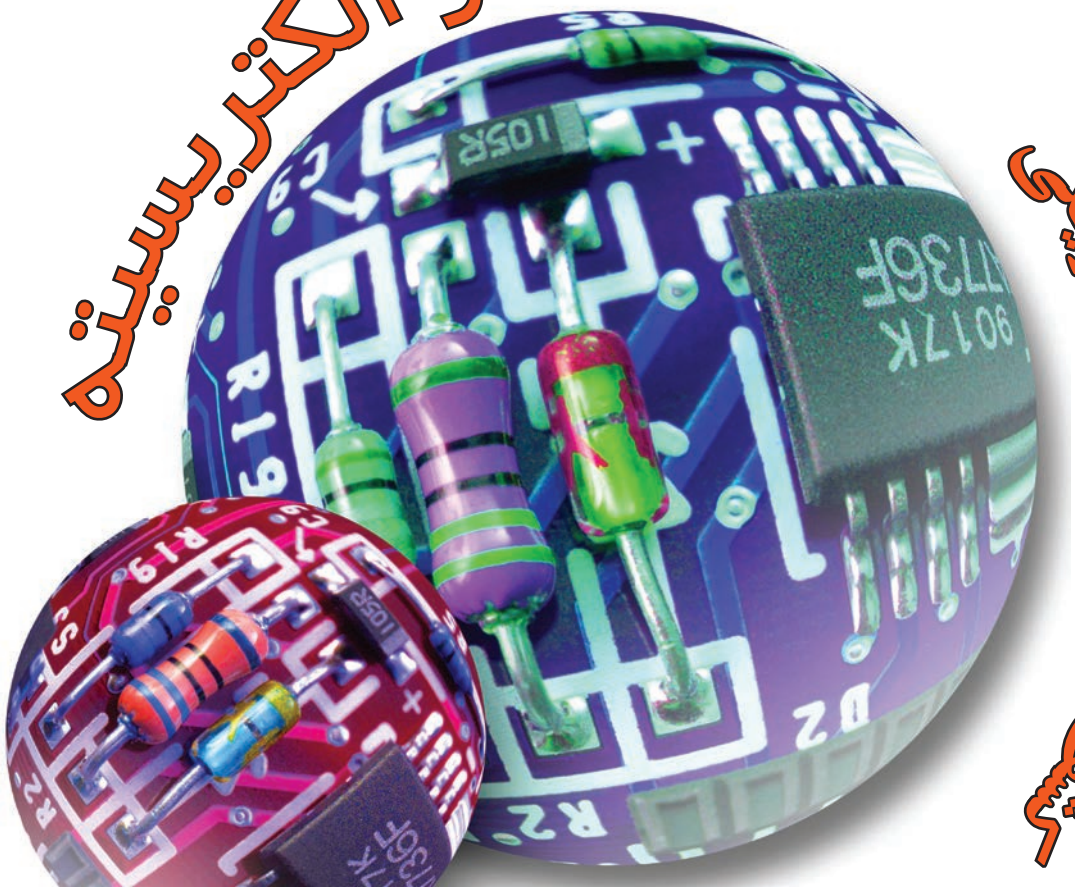
- در زمان انتشار اطلاعات بر روی منابع عمومی خصوصاً اینترنت می‌بایست قبل از هر اقدام ضرورت نشر اطلاعات و اینکه چه اطلاعاتی می‌بایست در دسترس همگان قرار داده شود به دقت بررسی گردد. سرقت هویت کاربران یکی از مسائل مهم در عرصه اینترنت است و با وجود اطلاعات بیشتر، مهاجمان قادر به جمع‌آوری اطلاعات بیشتر در رابطه با شما هستند و می‌توانند در مواردی خاص خود را به جای شما معرفی کنند و از موقعیت شما سوء استفاده نمایند.

برگرفته از کتاب

حسن‌زاده، محمد و جهانگیری، نرگس. (۱۳۹۰). امنیت اطلاعات (از آگاهی تا آموزش). تهران: نشر کتابدار.

عصر الکتریسیته

بخش‌هایی مهم فیزیک

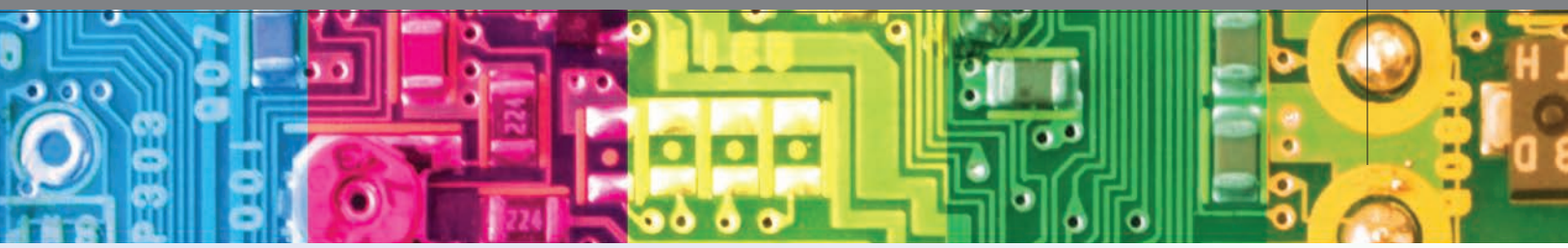


کشف الکتریسیته و به کارگیری نیروی برق یکی از مهم‌ترین تجربه‌های بشر در طول تاریخ است. از این رو طی دو قرن گذشته رشد علم و فناوری از سرعتی بی‌سابقه نسبت به قرن گذشته برخوردار بود و کاربرد الکتریسیته و شاخه‌های آن نظیر برق، قدرت، مخابرات، الکترونیک، کنترل و سایر شاخه‌های این دانش پیش‌رو در مجموعه‌ی علوم و فنون و نقش انکارناپذیر آن در پیشبرد فناوری، سبب شد که اهمیت و ضرورت فعالیت علمی و سرمایه‌گذاری تحقیقاتی در این علم بیش از پیش مورد توجه قرار گیرد.

الکترونیک دانش مطالعه‌ی عبور جریان الکتریکی از مواد مختلف- مانند نیمه‌رساناها، مقاومت‌ها، القاگرها و خازن‌ها- و آثار آن است. الکترونیک همچنین به عنوان شاخه‌ای از فیزیک نظری شناخته می‌شود. طراحی و ساخت مدارهای الکترونیکی برای حل مشکلات عملی، قسمتی از مباحث موجود در مهندسی الکترونیک را تشکیل می‌دهد. در برخی موارد مطالعه المان‌های جدید نیمه‌رسانا و فناوری‌های نزدیک به آن، شاخه‌ای از فیزیک در نظر گرفته می‌شود.

مهندسی الکترونیک

مهندسی الکترونیک یکی از شاخه‌های مهندسی است که از رفتار و اثر الکترون‌ها استفاده می کند و به توسعه‌ی قطعه‌ها، دستگاه‌ها، سیستم‌ها، یا تجهیزاتی می‌پردازد که انرژی الکتریکی یکی از فاکتورهای آنهاست؛ همانند لامپ‌های خلاء، ترانزیستورها، مدارهای مجتمع و مدارهای چاپی. این رشته به شاخه‌ی وسیعی از مهندسی اشاره دارد که زیرشاخه‌های بسیاری را دربرمی گیرد. شامل رشته‌هایی که با



توان، مهندسی ابزار دقیق، مخابرات، طراحی مدارهای نیمه هادی، و بسیاری دیگر در ارتباط هستند.

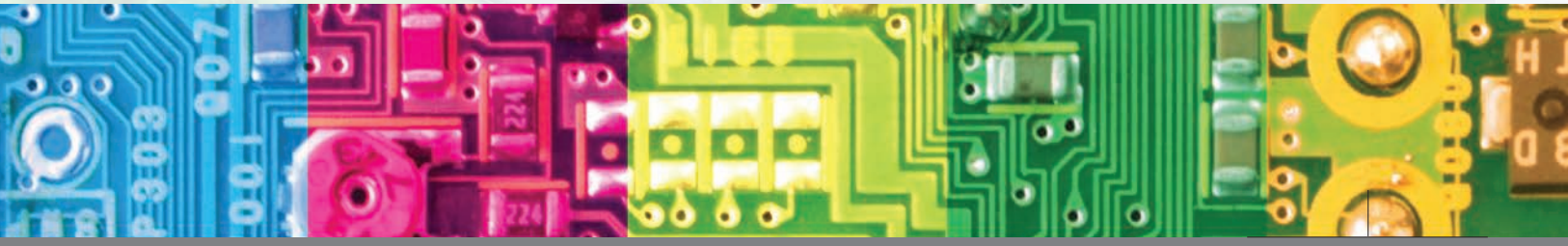
در رشته مهندسی الکترونیک؛ مهندسان، مدارهایی را تست و طراحی می‌کنند؛ که از خواص الکترومغناطیسی قطعه‌های الکتریکی همچون مقاومت، خازن، سلف، دیود و ترانزیستور برای رسیدن به عملکرد خاصی بهره می‌برند. مدار رادیو که به استفاده کننده امکان می‌دهد تا همه سیگنال‌ها به جز سیگنال‌های یک ایستگاه را فیلتر کند، تنها یک نمونه از این مدارهاست. در طراحی مدار مجتمع، مهندسان الکترونیک، ابتدا نقشه‌هایی را می‌سازند که قطعه‌های الکتریکی را مشخص می‌کند و ارتباطات بین آنها را وصف می‌کند. هنگامی که تکمیل شد، مهندسان کامپیوتر نقشه‌ها را به طرح‌هایی تبدیل می‌کنند که لایه‌های مختلف مواد هادی و نیمه هادی مورد نیاز برای ساخت مدار را رسم می‌کنند. تبدیل نقشه‌ها به پوسته‌ها می‌تواند توسط نرم‌افزار انجام پذیرد. اما اغلب به تنظیمات ریز انسان برای کاهش فضا و مصرف توان نیاز است. هنگامی که طرح کامل شد می‌تواند به یک کارخانه ساخت برای تولید فرستاده شود.

◄ واژه مهندسی الکترونیک

واژه مهندسی برق که در میان دانشگاه‌های قدیمی استفاده می‌شود هنوز هم مهندسی الکترونیک را تحت پوشش قرار می‌دهد و فارغ‌التحصیلان، مهندس برق لقب می‌گیرند. برخی از مردم بر این باورند که واژه‌ی مهندس برق باید برای آن دسته از کسانی به کار رود که در قدرت و جریان‌های بالا یا مهندسی فشار قوی تخصص دارند. در حالی که گروهی دیگر معتقدند که قدرت تنها یکی از زیرشاخه‌های مهندسی برق است (در واقع برای این شاخه از صنعت مهندسی قدرت استفاده می‌شود). در سال‌های اخیر رشد رشته‌هایی جدید و جداگانه همچون مهندسی اطلاعات و مهندسی سیستم‌های مخابراتی را شاهد بوده‌ایم که در اداره‌ی گروه‌های آموزشی تحت همین نام‌ها تحصیل می‌شوند. در آغاز دهه ۱۹۸۰، نیز واژه مهندسی کامپیوتر معمولاً برای اشاره به الکترونیک و مهندسی اطلاعات استفاده می‌شد. هرچند مهندسی کامپیوتر هم‌اکنون به عنوان یکی از زیرمجموعه‌های مهندسی الکترونیک در نظر گرفته می‌شود.

◄ پیشینه مهندسی الکترونیک در جهان

مهندسی الکترونیک به عنوان یک حرفه از پیشرفت‌های فنی در صنعت تلگراف در قرن ۱۹ و صنایع رادیو و تلویزیون در قرن ۲۰ حاصل شد. مردم به رادیو به خاطر جاذبه فنی؛ دریافت و سپس انتقال اطلاعات علاقمند شدند. بسیاری از مردمی که در دهه‌ی ۱۹۲۰، به رادیو و تلویزیون رفتند تنها آماتورهای دوره قبل از جنگ جهانی اول بودند. شاخه جدید مهندسی الکترونیک تا حد زیادی از پیشرفت تلفن، رادیو، تجهیزات تلویزیون و مقدار زیادی از توسعه سیستم‌های الکترونیکی در طول جنگ جهانی دوم از جمله رادار، سونار، سیستم‌های ارتباطی و مهمات پیشرفته و سیستم‌های جنگ‌افزاری حاصل شد. در مدت این سال‌ها این موضوع‌ها به عنوان مهندسی رادیو شناخته می‌شدند و تنها در اواخر دهه ۱۹۵۰، استفاده از واژه مهندسی الکترونیک آغاز شد. در همین هنگام آزمایشگاه‌های الکترونیک (برای نمونه آزمایشگاه بل در ایالات متحده آمریکا) ایجاد شدند و با استفاده از کمک



هزینه‌های شرکت‌های بزرگ صنایع رادیو، تلویزیون، و دستگاه‌های تلفن، شروع به تولید سلسله پیشرفت‌هایی در الکترونیک کردند. در سال ۱۹۴۸، ترانزیستور روی کار آمد و در سال ۱۹۶۰، مدارهای مجتمع انقلابی در صنعت الکترونیک برپا کردند. در انگلستان موضوع مهندسی الکترونیک به صورت مجزا از مهندسی برق به عنوان مدرک دانشگاهی در حدود سال ۱۹۶۰، اضافه شد. قبل از آن، دانشجویان مهندسی و موضوع‌های مرتبط همچون رادیو و تلویزیون، مجبور بودند تا در سازمان‌های آموزش برقی ثبت‌نام کنند که درس‌های مربوط به الکترونیک نداشت. مهندسی برق نزدیک‌ترین موضوعی بود که می‌توانست با مهندسی الکترونیک هم‌طراز قرار گیرد.

◄ الکترونیک جدید

در سال ۱۸۹۸، نیکولا تسلا اولین ارتباط رادیویی را به نمایش عموم در آورد. او جزئیات مبادی و اصول ارتباط رادیویی را نمایش و شرح داد. در سال ۱۹۰۴، جان آمیروز فلمینگ، اولین استاد مهندسی برق در کالج لندن، اولین لامپ خلاء (دیود) را اختراع کرد. یک سال بعد در سال ۱۹۰۶، رابرت فون لیبن و لی د فارست به طور مستقل لامپ‌های تقویت کننده‌ای را ساختند که لامپ سه قطبی نامیده می‌شد. آغاز الکترونیک معمولاً با اختراع لامپ خلاء توسط لی د فارست در ۱۹۰۷، در نظر گرفته می‌شود. در مدت ۱۰ سال، دستگاه او در فرستنده‌ها و گیرنده‌های رادیویی همچون سیستم‌هایی برای تماس‌های تلفنی راه دور استفاده می‌شد. در ۱۹۱۲، ادوین هاوارد آرمسترانگ تقویت کننده ریجنراتیو فیدبک و نوسان‌ساز را اختراع کرد. او همچنین گیرنده رادیو سوپرهترودین را اختراع کرد که می‌توان آن را پدر رادیوی پیشرفته امروزی نامید. لامپ‌های خلاء به مدت ۴۰ سال به عنوان دستگاه‌های تقویت کننده مطرح بودند. تا اینکه پژوهشگرانی که برای ویلیام شاکلی در آزمایشگاه بل در حال فعالیت بودند، ترانزیستور را در سال ۱۹۴۷، اختراع کردند. در همین سال‌ها رادیوهای ترانزیستوری، همچنین ساخت کامپیوترهای بزرگ و قدرتمند ممکن شد. ترانزیستورها کوچک‌تر بودند و برای کار به ولتاژ کمتری احتیاج داشتند. پیش از اختراع مدارهای مجتمع در سال ۱۹۵۹، مدارهای الکترونیکی از قطعه‌های جدا از هم ساخته می‌شد که می‌توانست با دست، دستکاری شود. مدارهای غیر یکپارچه به فضای بیشتری احتیاج و مصرف توان بالاتری داشتند، خطای بیشتر و همچنین سرعت پایین‌تری داشتند؛ گرچه هنوز در کاربردهای ساده استفاده می‌شوند. در مقابل مدارهای مجتمع تعداد زیادی، گاهی میلیون‌ها، قطعه ریز الکتریکی، و به طور عمده ترانزیستور، را در یک تراشه کوچک در حدود اندازه یک سکه بسته‌بندی می‌کنند.

در ۱۹۲۷، فیلو فرانسورد اولین تلویزیون را به نمایش عموم در آورد. در طول دهه ۱۹۳۰، چند کشور شروع به پخش برنامه کردند و تعداد تلویزیون‌ها بعد از جنگ دوم جهانی به میلیون‌ها گیرنده گسترش یافت و سرانجام جهانی شد. از آن زمان به بعد، الکترونیک کاملاً در دستگاه‌های تلویزیون حاضر شد. تلویزیون‌ها و نمایشگرهای تصویری جدید هم از فناوری لامپ‌های خلاء بزرگ تکامل یافتند، همانند پلاسما و ال‌سی‌دی.

در طول جنگ جهانی دوم تلاش‌های بسیاری در الکترونیک برای یافتن موقعیت اهداف و هواپیماهای دشمن صورت گرفت. اینها همچنین شامل هدایت الکترونیکی بمب‌افکن‌ها، پادکارهای الکترونیکی، سیستم‌های اولیه رادار و... می‌شوند.

◄ ادوات و مدارهای الکترونیکی

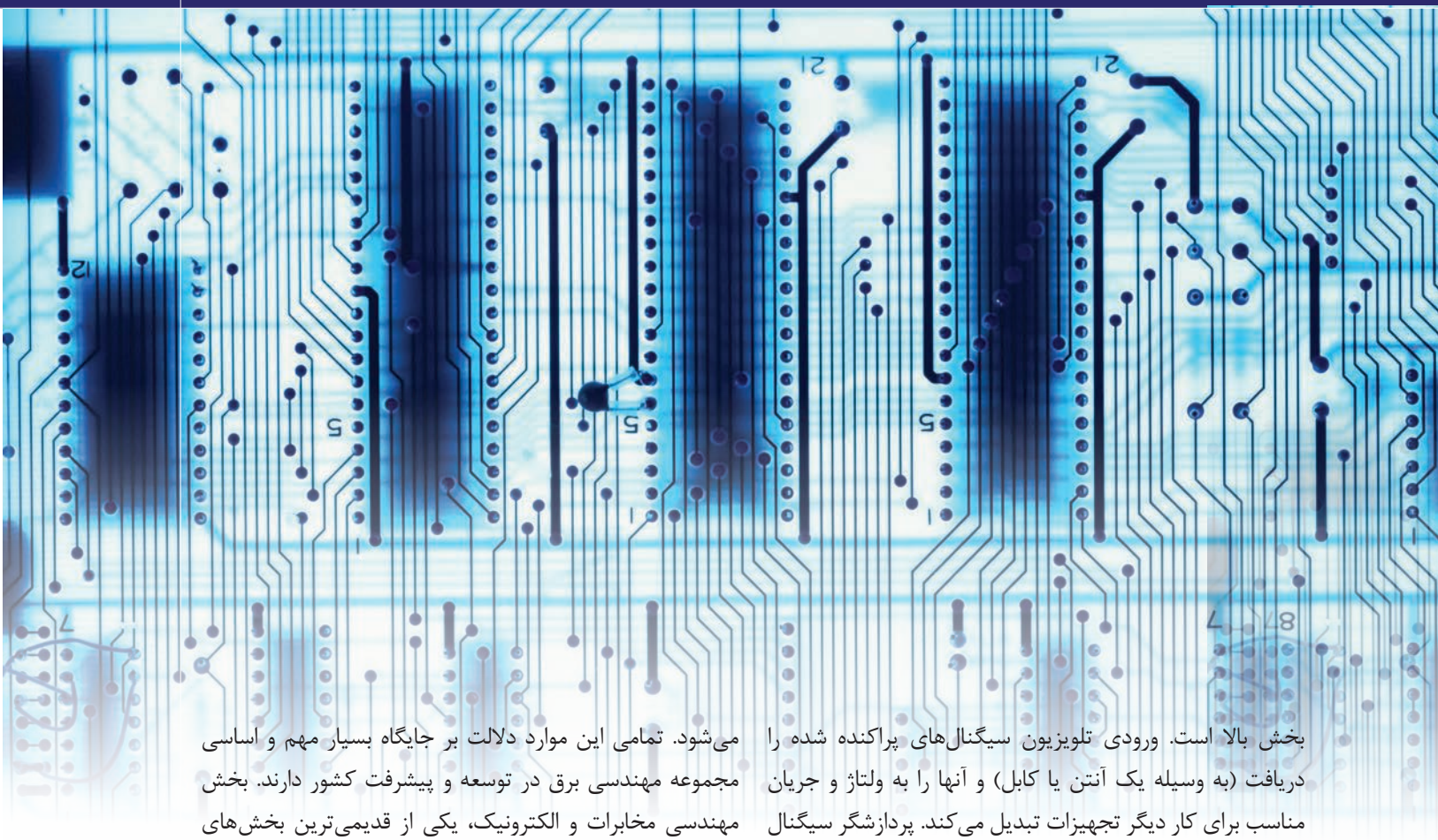
مدارهای الکترونیکی برای ایفا کردن وظایف مختلفی استفاده می‌شوند. کاربردهای اصلی مدارهای الکترونیکی عبارتند از: کنترل و پردازش داده‌ها؛ تبدیل و توزیع توان الکتریکی؛ اجرای عملیات خاص. همه‌ی این کاربردها با ایجاد و آشکارسازی میدان الکترومغناطیسی و جریان الکتریکی ارتباط دارند. از انرژی الکتریکی در سال‌های انتهایی قرن ۱۹ برای انتقال پیام به وسیله تلگراف و تلفن استفاده می‌شد اما بیشتر پیشرفت‌های مربوط به علم الکترونیک پس از ساخت رادیو شکل گرفت. در یک نگاه ساده، یک سیستم الکترونیکی را می‌توان به سه بخش تقسیم کرد:

• ورودی: حسگرهای الکترونیکی و مکانیکی (یا مبدل‌های انرژی). این تجهیزات سیگنال‌ها یا اطلاعات را از محیط خارج دریافت و سپس آنها را به جریان، ولتاژ یا سیگنال‌های دیجیتال تبدیل می‌کنند.

• پردازشگر سیگنال: این مدارها در واقع وظیفه اداره، تفسیر کردن و تبدیل سیگنال‌های ورودی برای استفاده آنها در کاربرد مناسب را بر عهده دارند. معمولاً در این بخش پردازش سیگنال‌های مرکب بر عهده پردازشگر سیگنال‌های دیجیتال است.

• خروجی: فعال کننده‌ها یا دیگر تجهیزات (مانند مبدل‌های انرژی) که سیگنال‌های ولتاژ یا جریان را به صورت خروجی مناسب در خواهند آورد (برای مثال با ایفای یک وظیفه فیزیکی مانند چرخاندن یک موتور).

برای مثال یک تلویزیون دارای هر سه



بخش بالا است. ورودی تلویزیون سیگنال‌های پراکنده شده را دریافت (به وسیله یک آنتن یا کابل) و آنها را به ولتاژ و جریان مناسب برای کار دیگر تجهیزات تبدیل می‌کند. پردازشگر سیگنال پس از دریافت داده‌ها از ورودی اطلاعات مورد نیاز مانند میزان روشنایی، رنگ و صدا را از آن استخراج می‌کند. در نهایت قسمت خروجی این اطلاعات را دوباره به صورت فیزیکی در خواهد آورد این کار به وسیله یک لامپ اشعه کاتدیک و یک بلندگوی آهنربایی انجام خواهد شد.

◄ پیشینه مهندسی الکترونیک در ایران

رشته مهندسی مخابرات و الکترونیک به منظور تربیت مهندسانی ایجاد شد که در فعالیت‌های صنعتی و تحقیقاتی در زمینه‌های یاد شده به فعالیت بپردازند. جهش‌های بزرگی که در فناوری‌های مختلف به وجود آمده ارتباط تنگاتنگی با رشته مهندسی برق و الکترونیک دارد. در کشور ما عمده فعالیت‌های صنعتی و پژوهشی مرتبط با گرایش‌های مختلف مهندسی برق توسط چهار وزارتخانه ارتباطات و فناوری اطلاعات، دفاع وزارت نیرو و صنایع انجام می‌شود و از این طریق درصد قابل توجهی از بودجه کل کشور صرف آبادانی و پیشرفت در عرصه‌های مختلف می‌شود. تمامی این موارد دلالت بر جایگاه بسیار مهم و اساسی مجموعه مهندسی برق در توسعه و پیشرفت کشور دارند. بخش مهندسی مخابرات و الکترونیک، یکی از قدیمی‌ترین بخش‌های دانشکده مهندسی دانشگاه شیراز است که در سال ۱۳۴۲، تأسیس گردید و شاخه‌ها و گرایش‌های متعددی را در مجموعه خود جای داده است. این بخش مهندسی در حال حاضر، در مقطع کارشناسی در گرایش‌های الکترونیک، مخابرات، در مقطع کارشناسی‌ارشد در گرایش‌های مخابرات سیستم، مخابرات میدان و الکترونیک و در مقطع دکترا در گرایش مخابرات، دانشجو می‌پذیرد. با تصویب هیئت رئیسه‌ی دانشگاه شیراز از سال ۱۳۸۷، بخش مهندسی مخابرات و الکترونیک در دانشکده مهندسی برق و کامپیوتر راه‌اندازی گردید.

منابع

۱- مهندسی الکترونیک [homepage] ۱۵ بهمن ۱۳۹۰ [online] <http://fa.wikipedia.org > [۱۵ بهمن ۱۳۹۰].

۲- آشنایی با رشته مهندسی برق [homepage] ۱۲ بهمن ۱۳۹۰ [online] <http://hupaa.com > [۱۱ بهمن ۱۳۹۰].

۳- برق و الکترونیک [homepage] ۱ بهمن ۱۳۹۰ [online] < danesh.bizhat.com/http:/> [۳ بهمن ۱۳۹۰].

۴- انجمن برق و الکترونیک ایران [homepage] ۵ بهمن ۱۳۹۰ [online] <www.iaeee.ir > [۸ بهمن ۱۳۹۰].

چه کسی می‌تواند این قاتل بزرگ را متوقف کند؟

• پروژه هارپ چیست؟

هارپ، پروژه‌ای مشترک میان نیروی هوایی و نیروی دریایی ایالات متحده‌ی امریکا در آلاسکا است. این پروژه برنامه‌ای تحقیقاتی است که برای مطالعه یونسفر طراحی شده تا فناوری تسلیحات جدید توسعه یابد.

سیستم هارپ برای دستکاری در یونسفر طراحی شده است. یونسفر لایه‌ای در حدود سی مایلی بالای زمین است. فرستنده یا دستگاه هارپ بر روی زمین، یک سیستم آنتنی چند فاز است، میدانی بزرگ از آنتن‌ها که برای کار و متمرکز ساختن انرژی فرکانس‌های رادیویی برای دستکاری یونسفر طراحی شده است. انرژی فرکانس رادیویی می‌تواند به روش‌هایی که هرگز برای سایر گیرنده‌ها امکان‌پذیر نیست، تابیده شود؛ شکل بگیرد یا تغییر کند. این دستگاه دارای قدرتی معادل یک میلیارد وات در زمان تکمیل فاز اول پروژه بود. از آن برای «توموگرافی نفوذ به زمین» (بررسی لایه‌های زمین برای استقرار تأسیسات زیرزمینی معادن)، ارتباط با زیردریایی‌ها، تغییر ارتباطات دیگران، رادار فوق افق، انتقال انرژی از یک بخش جهان به بخش دیگر بدون استفاده از سیم، ایجاد لایه‌ها یا سطوح پلاسما (انرژی) مصنوعی در یونسفر، تغییرات آب و هوایی یا یک سلاح ضد موشک استفاده می‌شود. داستان هارپ و فناوری‌های مرتبط با آن بخشی از معمای «تحول امور نظامی» است که دولت ایالات متحده‌ی امریکا آن را دنبال می‌کند.

• بالابردن سقف جهان

کودکی در حین بازی در فضای باز با چشمانی پر از اعتماد به آسمان آبی بالای سرش نگاه می‌کند. مادرش کلاهی حصیری به سر او گذارده، به صورت او کرم ضد آفتاب زده و انتظار دارد به دلیل مصون نگاه داشتن فرزندش در برابر اشعه‌ی ماورای بنفش خورشید، او از این اشعه‌های مضر در امان باشد. اما آیا او در امان است؟ هم بدن او و هم سیاره‌اش، تحت ترکیبی نامشخص از اشعه‌های ساخته‌ی دست بشر هستند و هم اینک ارتش امریکا در نظر دارد تا این ترکیبات را بیشتر کند. این موضوع درباره‌ی مردمی است که به دنبال واقعیت درباره‌ی پروژه‌ی پنتاگون هستند که در نقطه‌ای بسیار دور افتاده در آلاسکا اجرا می‌شود. این پروژه‌ی ۳۰ میلیون دلاری که هارپ نامیده می‌شود برای تابش بیش از ۱/۷ گیگاوات (میلیارد وات) اشعه به یونسفر– لایه‌ی شارژ شده‌ی

الکتریکی بالای جو زمین استفاده می‌شود.

به زبان ساده، این دستگاه به مثابه‌ی یک تلسکوپ رادیویی وارونه یا معکوس است یعنی به جای گیرنده، فرستنده است. این امر باعث به جوش آمدن جو فوقانی می‌شود. بعد از اختلال در یونسفر، اشعه‌ها دوباره به صورت امواج بلند که درون کالبد ما، زمین و اقیانوس‌ها نفوذ می‌کنند، به زمین باز می‌گردند. آیا این تهاجم اشعه‌ای می‌تواند به حیات گیاهان و حیوانات بر روی زمین آسیب بزند؟ پژوهشگران معتقدند هارپ نمایانگر یک فناوری است که می‌تواند به کلاس جدیدی از تسلیحات بینجامد که می‌توانند دنیای ما را تغییر دهند یعنی ابزاری کاملاً نظامی. اگر از این ابزار سوء استفاده شود، می‌تواند آب و هوای جهان را به هم بریزد. می‌توان از این ابزار علیه بشریت استفاده کرد طوری که اندیشه‌ها، باورها و احساسات مردم عوض شوند. همچنین می‌توان از آن برای اهداف خوب یا بد استفاده کرد. مثلاً ساز موسیقی چنگ می‌تواند برای تولید موسیقی موتزارت یا ملودی مارش مرگ استفاده شود.

بسیاری از موضوع‌های فناوری را می‌توان از طریق آزمایش‌های نظامی هارپ دنبال کرد، مانند:

- تغییرات آب و هوای جهانی؛
- آسیب‌های اکوسیستم؛
- اخلال در ارتباطات الکترونیکی؛
- تغییرات رفتاری یا ذهنی.

پروژه‌هایی مانند هارپ می‌توانند ذاتاً دو عملکرد کاملاً متضاد از خود نشان دهند بسته به اینکه دست‌اندرکاران آن چه اندیشه‌ای را برای استفاده از آن در سر بپرورانند، یعنی پروژه هارپ همانگونه که می‌تواند فرصتی مغتنم باشد می‌تواند نوعی تهدید نیز برای نسل بشر به شمار آید. به‌طور کلی دانشمندان در هر پروژه‌ای یک انتها متصور می‌شوند ولی برای پروژه هارپ نمی‌توان هیچگونه حد و نهایتی قائل شد چرا که با پدیده‌هایی مانند اتمسفر زمین، فضا و انرژی‌های کیهانی مواجه هستیم و انتهای این پروژه می‌تواند سرآغاز نسلی جدید از ابرفناوری‌ها و به نوعی فتح باب و سر منشأ انقلاب صنعتی آینده و رنسانسی دیگر در جامعه بشریت باشد و همانند بسیاری از اختراع‌های بزرگ بشر مانند اختراع برق، تلفن، اینترنت و ... تحولی شگرف ایجاد نماید.

از منظری دیگر، پروژه‌هایی نظیر هارپ همانطور که می‌توانند برای بشریت مفید و سرمنشأ نسل جدیدی از ابرفناوری‌ها باشند به همان اندازه نیز می‌توانند برای کشورها تهدید بسیار جدی محسوب گردند و استفاده‌های نظامی بسیار مخربی داشته باشند و به قول برخی منتقدان آن، هارپ به نوعی حد نهایی سلاح ساخته دست بشر است به طوری که تسلیحات دیگر مانند انواع سلاح‌های هسته‌ای در برابر آن یک اسباب‌بازی ساده تلقی می‌شوند. در صورتی که بخواهیم به مختصری از کاربردهای انسانی و یا نظامی آن اشاره کنیم می‌توان موارد زیر را فهرست‌وار ذکر کرد، هر چند این پروژه دارای ابعاد بسیار وسیعی است که بسیاری از کاربردهای دیگر آن در آینده مورد استفاده قرار خواهد گرفت.

الف) برخی از کاربردهای انسان دوستانه پروژه هارپ

۱- انتقال برق و انرژی بدون استفاده از سیم به هر نقطه از زمین بدون اتلاف انرژی (بیش از ۲۰ درصد از برق تولیدی توسط نیروگاه‌ها به صورت گرما در خطوط انتقال برق شبکه تلف می‌شود)؛

۲- کنترل شرایط آب و هوا و ایجاد ابر و باران مصنوعی در مناطق خشک؛

۳- بهره‌گیری از انرژی بادهای خورشیدی و ایجاد انرژی پاک و بدون تشعشع به میزان ۱۰۰۰ برابر انرژی اولیه برای تحریک لایه یونسفر جو زمین؛

۴- استفاده پزشکی برای درمان بیماران با مشکلات روانی؛
۵- شارژ کردن باتری‌های ماهواره‌ها و سفینه‌ها از راه دور؛
۶- اکتشاف میادین نفتی و معادن زیرزمینی.

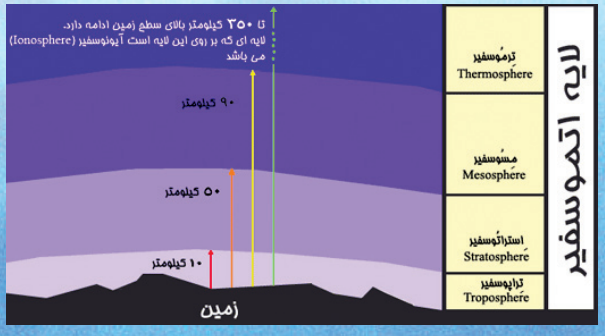
ب) برخی از کاربردهای نظامی پروژه هارپ

۱- ایجاد یک سپر ضد موشکی در لایه‌های جوی کشور مورد نظر؛
۲- ایجاد زمین‌لرزه‌های موضوعی با قدرت دلخواه در هر نقطه از جهان؛
۳- ایجاد انواع توفان، سیل و سونامی در هر نقطه از جهان؛
۴- مختل کردن کلیه ارتباطات رادیویی در طول جنگ بدون از دست دادن ارتباطات رادیویی خود؛
۵- مختل کردن و از کار انداختن کلیه تجهیزات الکترونیکی ادوات جنگی مانند رادارها، هواپیماها و ...؛
۶- نابودی هر نوع زیردریایی در اعماق اقیانوس‌ها؛
۷- نابودی انواع هواپیماها و ماهواره‌ها در آسمان و در مدار زمین؛
۸- ایجاد انفجاری بسیار مهیب در حد انفجارهای هسته‌ای بدون داشتن تشعشع؛
۹- ایجاد انواع ابر، مه و گرد و غبار برای مختل کردن حرکت نیروهای مقابل؛
۱۰- کنترل ذهن سربازان شامل ایجاد علائم غش، منگی و حالات خواب آلودگی؛
۱۱- ایجاد علائم افسردگی، هیجان‌های تصنعی، رخوت، عصبانیت کاذب و ... در افراد یک جامعه؛
۱۲- به وجود آوردن خشکسالی در هر منطقه از جهان؛
۱۳- کشف هر گونه پناهگاه، انبار مهمات، مکان‌های مخفی و ... در هر نقطه از جهان؛
۱۴- اندازه‌گیری مقدار ذخائر نفتی، معدنی و ... کشورهای دیگر برای برنامه‌ریزی‌های تجاری در آینده.

موارد بالا تنها بخشی از کاربردهای بسیار زیاد پروژه‌هایی با مکانیسم هارپ هستند و شاید به جرأت بتوان گفت این پروژه سرآغاز انقلاب صنعتی دیگر در جهان خواهد بود و به دلیل چنین جذابیت‌هایی بسیاری از کشورهای پیشرفته دنیا مانند روسیه (از زمان شوروی سابق تاکنون)، ژاپن، کانادا و اتحادیه اروپا، با صرف بودجه‌های کلان روی پروژه‌هایی با مکانیسم هارپ، سعی دارند از قافله چنین فناوری گرانبهایی عقب نیفتند.

• تعریف لایه‌ی یونسفر جو زمین

لایه‌ی یونسفر در بالاترین لایه‌ی اتموسفر قراردارد.



این لایه، تشعشعات خطرناک «ماورای بنفش» و «اشعه ایکس» خورشید را جذب می‌کند و مانند سقفی از ورود آنها به زمین جلوگیری می‌نماید تا زندگی بر روی کره زمین امکان‌پذیر گردد. همچنین به دلیل محیط الکتریکی موجود در یونسفر از این لایه برای انعکاس امواج رادیویی به اطراف زمین استفاده می‌شود. اگر این لایه به هر دلیل دچار اختلال شود تأثیرات بسیار زیادی بر روی زمین می‌گذارد و زیستن را مختل می‌کند.

نیکولا تسلا، مخترعی بزرگ بود که در هشتادمین سالگرد تولدش در ۱۰ ژوئیه، به نویسنده گفته بود آماده است دولت ایالات متحده‌ی امریکا را از راز نیروی الکترونیکی خود آگاه سازد که می‌توانست موتورهای یک هواپیما را در فاصله‌ی ۲۵۰ مایلی از کار بیاندازد و بنابراین یک دیوار دفاعی نامرئی همچون دیوار چین را به دور کشور احداث نماید.

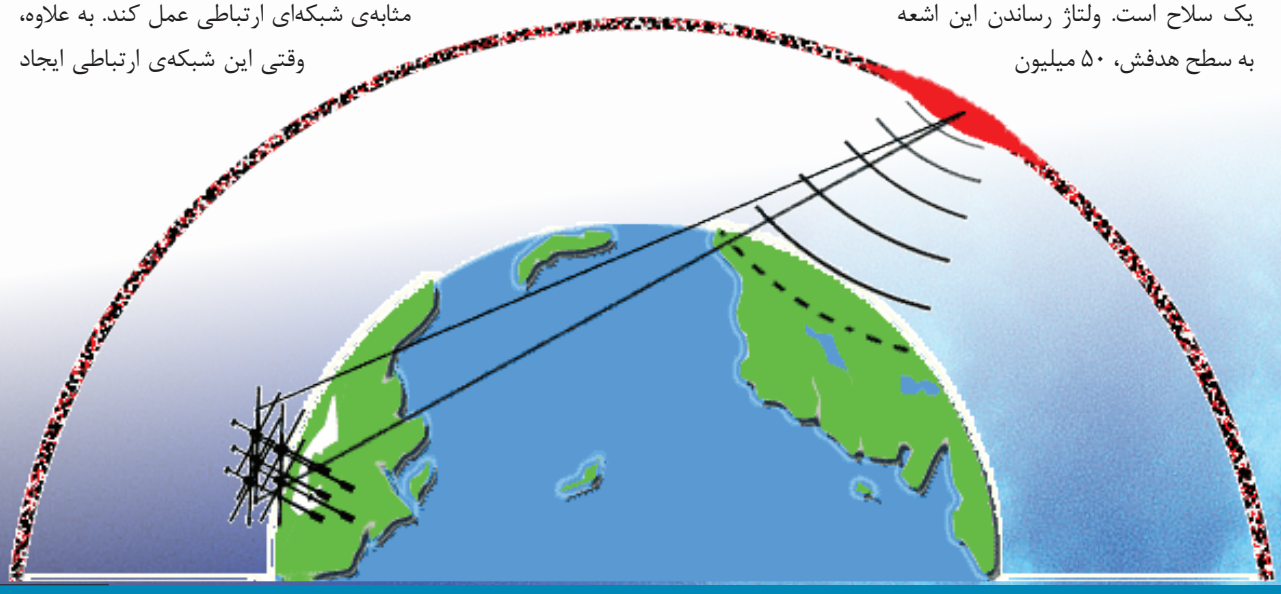
او معتقد بود این نیروی الکترونیکی مبتنی بر یک اصل کاملاً جدید فیزیکی است که تاکنون هیچ‌کس حتی در رؤیا نیز آن را تجسم نکرده است و متفاوت با اصول موجود در اختراع‌های او در ارتباط با انتقال برق از یک فاصله‌ی دور است که بابت آن چند پروانه‌ی انحصاری بهره‌برداری دریافت کرده بود. به گفته‌ی آقای تسلا، این نوع نیرو از طریق پرتویی ایجاد خواهد شد که یک صد میلیونیوم سانتیمتر مربع قطر دارد و می‌توان آن را از طریق دستگاه ویژه‌ای تولید کرد که بیش از ۲ میلیون دلار هزینه ندارد و ساخت آن تنها سه ماه زمان می‌برد.

به گفته‌ی او، این اشعه در برگیرنده‌ی چهار اختراع است که دو مورد از آنها قبلاً تست شده‌اند. یکی از آنها، روش و ابزاری برای تولید اشعه و دیگری برای تولید انرژی در هوای آزاد است که نیاز به میزان بالای خلأ را از میان می‌برد؛ دوم، روش و فرایندی برای تولید نیروی بسیار عظیم الکتریکی است؛ سوم، روشی برای تشدید این نیرو و چهارم روشی جدید برای تولید یک نیروی عظیم دافع الکتریکی است. این به مثابه‌ی یک سلاح است. ولتاژ رساندن این اشعه به سطح هدفش، ۵۰ میلیون ولت است.

ایده‌های تسلا باعث شکل‌گیری پرسش‌های زیادی در ذهن دانشمندان پیرامون «قانون و نظم» شدند که شاید پیش روی بسیاری از سازمان‌های دفاعی کنترل‌کننده‌ی چنین فناوری‌هایی قرار دارند. دانشمندان بر این باور بودند که اگر این فناوری در هر جایی به کار گرفته شود، باید صادقانه و شفافانه مطرح شود و تنها باید زمانی به کار گرفته شود که ایمن باشد. ایده‌ی آزادسازی چنین نیرویی در یونسفر سیاره، به شدت باعث آشفتگی او شده بود.

موضوع دیگری نیز وجود داشت که علاوه بر تأثیرات احتمالی هارپ، بر آب و هوا یا بر ارتباطات اضطراری در بوته‌زارهای آلاسکا نگران کننده بود. طی سال‌ها، مطالعات متعددی انجام شده بود که ثابت می‌کرد سطوح پایین امواج فرکانس‌های رادیویی می‌توانند بر ذهن، رفتار و فیزیولوژی انسان اثر گذار باشند. یکی از اسناد دیگر هارپ حکایت از آن داشت که «اثبات شده اختلال‌های یونسفری منجر به زمین لرزه‌هایی همچون زلزله‌ی ۲۸ مارس ۱۹۶۴ میلادی آلاسکا شده‌اند». دانشمندان به دنبال این موضوع بودند که آیا عکس این موضوع نیز صادق است یعنی آیا اختلال‌های عمدی در یونسفر می‌توانند باعث به حرکت درآمدن مواد درون زمین و ایجاد زمین‌لرزه شوند یا خیر.

توانایی استفاده و ارسال امواج الکترومغناطیسی در فرکانس‌های مختلف به نقاط مختلف زمین، نمایانگر یک توانایی منحصر به فرد برای مختل کردن همزمان تمامی شیوه‌های ارتباطی دریایی و یا هوایی است. این اختراع نمایانگر توانایی ایجاد حجم بی‌نظیری از نیرو در نقاط استراتژیک اتمسفر زمین و حفظ سطح تزریق نیرو به ویژه در صورت استفاده از تکانه‌های تصادفی به صورتی است که مراتب قابل کنترل‌تر و دقیق‌تر از روش‌های قبلی به ویژه تجهیزات هسته‌ای است. آنچه که برای اخلال ارتباط‌های دیگران استفاده می‌شود، می‌تواند خود به مثابه‌ی شبکه‌ای ارتباطی عمل کند. به علاوه، وقتی این شبکه‌ی ارتباطی ایجاد



شد، می‌توان از اثرات دور از ذهن آن برای از کار انداختن سیگنال‌های ارتباطی دیگران در راستای اهداف اطلاعاتی استفاده کرد.

• بالا در آسمان

خورشیدهای بی‌شمار در دیگر منظومه‌ها، اشعه‌های کیهانی را به طور مستمر در تمامی جهت‌ها منتشر می‌کنند. خورشید ما، اشعه‌ی گاما، اشعه‌ی ایکس و طول موج‌های کوتاه‌تر نور ماوراء بنفش را می‌تاباند. وقتی آنها با اشعه‌ی بیرونی اتمسفر زمین برخورد می‌کنند، این اشعه‌های کیهانی توسط اتم‌ها جذب می‌شوند اما در الکترون‌ها این فرایند از اتم‌ها خارج می‌شوند. بنابراین، جریان ثابتی از الکترون‌ها در این ارتفاع وجود خواهد داشت و اتم‌ها به شکل بار تغییر می‌کنند و به یون‌های باردار تبدیل می‌شوند. نام این فرایند، یونسفر است. ارتفاع رخ دادن این یونیزاسیون ۱۰۰۰ کیلومتر در بالاترین و ۵۰ کیلومتر در پایین سطح است، اما یون‌های دارای بار مثبت و منفی، در ارتفاع ۸۰ تا ۴۰۰ کیلومتری به فشرده‌ترین شکل خود در می‌آیند. براساس معیار غیرمتریک، یونسفر در ارتفاع حدودِ ۳۰ مایلی آغاز می‌شود و تا ۳۰۰ مایل یا حتی بیشتر بالا می‌رود.

این سپر الکتریکی شارژ شده‌ی طبیعی در اطراف زمین، طول موج‌های مضر اشعه‌ی خورشید را فیلتر می‌کنند و سطح زمین را در برابر بمباران پرتوها مصون نگاه می‌دارد.

با حرکت بادهای خورشیدی به سمت زمین، ذرات باردار شده‌ی الکتریکی در خطوط میدان مغناطیسی زمین جریان می‌یابند. در طول مسیر که حداقل مقاومت وجود دارد، ذرات پر انرژی به سمت قطب‌های زمین می‌روند و در آنجا مجتمع می‌شوند که این حالت الکتروجت نامیده می‌شود. گاهی اوقات الکتروجت به تدریج کاهش می‌یابد اما در

سایر موارد، سیلابی از تشعشعات خورشیدی ایجاد می‌گردد که باعث شکل‌گیری سیستمی از ذرات پر انرژی می‌شود، آسمان پر نور می‌گردد، پرده‌های شفق قطبی تغییر می‌کنند.

امواج قوی رادیویی، درجه حرارت و دانسیته‌ی الکترون‌ها را در یونسفر تغییر می‌دهند و سایر سیگنال‌های رادیویی که از منطقه‌ی اصلاح شده عبور می‌کنند، تحت تأثیر قرار می‌گیرند. دانشمندان به مدت سی سال بر روی این موضوع تحقیق کرده‌اند و به تدریج مشخص شد که هدایت امواج پر قدرت به یونسفر باعث بروز بی‌ثباتی می‌گردد. گرم کننده‌های یونسفری به طور عمده توسط دانشگاه‌ها و انستیتوهای تحقیقاتی فعالیت می‌کنند. انستیتو تحقیقات بین المللی استفورد اقدام به توسعه‌ی انبوهی از برنامه‌های انتقال فرکانس‌های بالا با بودجه‌ی آژانس دفاع هسته‌ای کرد. جدیدترین ابزار چند منظوره که برای هارپ ساخته شده، توسط پایگاه هوایی فیلیپس هدایت می‌شود.

یکی از کاربردهای نظامی این دانش، آلوده کردن ترکیبات شیمیایی، هوا یا دیگر امکانات در حین جنگ است. کاربرد دیگر این فناوری، ایجاد توازن مجدد در خصایص شیمیایی افراد با استفاده از ترکیب سطوح پایین مواد شیمیایی با فرستنده‌های تنظیم شده است. این مورد، یک روش درمانی در اروپا و آسیا از طریق روش‌های الکترولیزری طب سوزنی است که توسط پژوهشگران این حوزه تکمیل شده است.

با وجود تمامی هشدارهای بیولوژیکی، متأسفانه هارپ به راه خود ادامه می‌دهد. برخی پژوهشگران معتقدند منع استفاده از فناوری‌های رادیویی و ریز موج‌ها غیر ممکن و غیر واقع‌بینانه است، اما در واقع خطرات به میزان زیادی نادیده گرفته می‌شوند. در راه رسیدن به هدف، متفکران باید به دیگر انسان‌ها کمک کنند. آنها باید درباره‌ی این موضوع تحقیق کنند که آیا یک محیط به شدت استرس‌آمیز الکترومغناطیسی، بر قدرت تفکر انسان تأثیر می‌گذارد یا نه. اگر چنین است، آنگاه نادیده گرفتن این واقعیت باعث می‌شود که ما شاهد انبوهی از سیاستگذارانی باشیم که غیر منطقی تصمیم‌گیری می‌کنند. انسان منابع کافی برای تغییر فناوری‌ها را در اختیار دارد البته اگر سیاست‌گذاران بخواهند چنین اتفاقی رخ دهد. افرادی که دانشمند نیستند، باید سطح اطلاعات خود را در این خصوص بالا ببرند.

منابع:

۱- بجیک، نیک.(۱۳۸۹). فرشتگان این چنگ را نمی‌نوازند. ترجمه‌ی آرش پازکی. انتشارات بیت الاحزان فاطمه (س).
۲- چوسودوسکی، میشل.(۲۰۰۷) Weather warfale، نشریه اکولوژیست.
۳- هارپ چیست؟[homepage] ۱۲ اسفند ۱۳۹۰[online] www.shia-news.com]۱۴ اسفند ۱۳۹۰[.

دکتر علی‌اکبر جلالی، بنیانگذار اولین روستای الکترونیکی در ایران

درباره اینکه ایشان متولد کجا و چه سالی هستند در اینترنت مطالعات زیادی انجام دادم ولی روایت‌های مختلفی وجود داشت، بنابراین تصمیم گرفتم که از خود ایشان این مطلب را بپرسم، چنین شد که برای ایشان در سایت خودشان پیام گذاشتم که مطلب صحیح را به بنده بفرمایند ایشان نیز با لطف بسیار زیاد در اسرع‌وقت به من چنین پاسخ دادند که ایشان متولد ۱۳۳۳، در شهر دامغان هستند و نیز چند سایت دیگر مربوط به زندگی‌نامه‌شان و همچنین کتابی که درباره زندگی ایشان چاپ شده است را به من معرفی کردند. جالب است بدانید که دکتر خود را شاهکویی می‌داند یعنی جایی که پدر و مادر ایشان متولد و اهل آنجا هستند.

تخصص دکتر جلالی، کنترل است. ایشان لیسانس مهندسی برق الکترونیک را در سال ۱۳۶۴، از دانشگاه خواجه نصیرالدین طوسی و کارشناسی ارشد، دکترا و فوق دکترایشان را از دانشگاه‌های اوکلاهما و وست ویرجینیا در سال‌های ۱۳۶۸ و ۱۳۷۳دریافت کرده‌اند. دکتر جلالی جزء پژوهشگران آینده‌نگر هستند و نظریه موج چهارم، عصر مجازی را برای اولین بار در دنیا مطرح کرده‌اند. ایشان تاکنون چند پروژه ICT را در سطح ملی در زمینه‌های مختلف توسعه فناوری اطلاعات و ارتباطات انجام داده‌اند.

لیست بخشی از خدمات ایشان به شرح زیر است:

۱- طراحی شهر الکترونیک کیش (این پروژه در سال ۱۳۷۹ شروع شد و در فرهنگ سازی توسعه ICT کشور نقش مؤثری داشت و هم اکنون توسط یک شرکت ایرلندی دنبال می‌شود)؛

۲- طراحی همایش جهانی شهرهای الکترونیکی و اینترنتی (این همایش نقطه عطفی در توسعه ICT کشور گردید)؛

۳- طراحی همایش کاربرد فناوری اطلاعات و ارتباطات در روستا (آغازگر فعالیت‌های ICT روستایی در کشور گردید).

۴- طراحی اولین مرکز جامع خدمات کاربردی اینترنت در ایران؛

۵- طراحی اولین روستای اینترنتی ایران «شاهکوه» که تاکنون بیش از یک میلیون نفر از سراسر جهان از طریق وب‌سایت از آن بازدید کرده‌اند و اغلب رسانه‌های جهان آن را مورد توجه قرار داده‌اند.

۶- طراحی اولین مرکز جامع خدمات کاربردی فناوری اطلاعات و ارتباطات روستایی کشور؛

۷- طراحی مقدماتی کریدور ICT شمال کشور (شامل استان‌های گیلان، گلستان و مازندران)؛

۸- مجری تدوین سند راهبردی شهر الکترونیک مشهد با محوریت شهرداری؛ سند راهبردی ICT روستایی کشور، سند راهبردی ICT استان مازندران و قم؛ RFP سند راهبردی ICT سازمان گسترش و نوسازی معادن و صنایع معدنی ایران؛

۹- مجری، تهیه نرم‌افزار آموزش مجازی ضمن خدمت دبیران کشور در وزارت آموزش و پرورش؛

۱۰- مجری پروژه دولت الکترونیکی و پروژه کار از راه دور در شرکت فولاد مبارکه اصفهان؛

۱۱- ارائه دهنده اولین درس مجازی بر روی شبکه اینترنت در ایران؛

۱۲- عضو مستقل یونسکو در آموزش و فناوری منطقه آسیا و اقیانوسیه، عضو کمیته آموزش مجازی کشور، عضو هیئت مدیره انجمن ICT ایران، عضو هیئت مدیره انجمن ایرانی مطالعات جامعه اطلاعاتی، عضو شورای پژوهشی آموزش و پرورش کشور؛

۱۳- پژوهشگر نمونه سال‌های ۷۸ و ۷۹ دانشگاه علم و صنعت ایران، پژوهشگر برتر صنعت IT کشور در سال ۱۳۸۲؛

۱۴- استاد نمونه دانشکده برق دانشگاه علم و صنعت ایران در سالهای ۷۶ و ۷۵، پژوهشگر نمونه‌ی دانشکده برق در سال ۱۳۸۲ ، ۱۳۸۴ و ۱۳۸۵؛

۱۵- مؤلف و مترجم بیش از صد مقاله و ۲۶ کتاب در زمینه مهندسی برق و ICT که کتاب PLC ایشان مقام اول ترجمه کتاب سال ۱۳۷۸، را در سطح کشور را داشته است، و کتاب Reduced Order Systems ایشان به زبان انگلیسی در سال ۲۰۰۶، توسط انتشارات Springer در آمریکا به چاپ رسیده است و در NASA و دانشگاه‌های معتبر جهان به عنوان کتاب مرجع استفاده می‌شود؛

۱۶- کسب جایزه eASIA ۲۰۰۷، منطقه آسیا و اقیانوسیه در نوآوری و خلاقیت در پروژه اولین مرکز ICT روستایی کشور از طرف AFACT ، سازمان ملل و یونسکو و نیز برگزیده بزرگترین جایزه بین‌المللی روابط عمومی سال ۲۰۰۹، توسط انجمن تخصصی روابط عمومی ایران و مؤسسه کارگزار روابط عمومی.

برخی از سوابق شغلی آموزشی و غیر آموزشی

۱- مشاور رئیس و مدیرکل دفتر ریاست، روابط عمومی و بین‌الملل در دانشگاه علم و صنعت ایران از سال ۱۳۷۷ تا ۱۳۷۹؛

۲- عضو شورای دانشگاه، شورای هماهنگی اجرائی دانشگاه و هیئت ممیزه دانشگاه علم و صنعت ایران؛

۳- معاون پژوهشی پژوهشکده‌ی الکترونیک؛

۴- مدیر امور پژوهشی و بین‌الملل دانشگاه علم و صنعت ایران؛

۵- عضو هیئت علمی، مدیر گروه کنترل، مدیر فوق برنامه فرهنگی- دانشجویی، مسئول مرکز کامپیوتر و مدیر دوره‌های کوتاه مدت مهندسی برق.

در حال حاضر ایشان به عنوان دانشیار در دانشکده برق دانشگاه علم و صنعت ایران و پژوهشکده الکترونیک مشغول به تدریس و پژوهش و نیز استاد پاره‌وقت دانشگاه ویرجینیای غربی هستند.

منابع

۱- آشنایی با زندگی‌نامه دکتر علی‌اکبر جلالی [homepage] ۱۸ بهمن ۱۳۹۰ [online]
< www.tarikhaneh.com > [۱۹ بهمن ۱۳۹۰].

۲- دانشکده برق دانشگاه علم و صنعت تهران [homepage] ۱۷ بهمن ۱۳۹۰ [online]
< http://www.iust.ac.ir > [۱۶ بهمن ۱۳۹۰].

۳- زندگی‌نامه دکتر علی‌اکبر جلالی [homepage] ۱۹ بهمن ۱۳۹۰ [online]
< www.csee.wvu.edu > [۲۰ بهمن ۱۳۹۰].

۴- وب‌سایت رسمی دکتر علی‌اکبر جلالی [homepage] ۱۸ بهمن ۱۳۹۰ [online]
< www.drjalali.ir > [۱۹ بهمن ۱۳۹۰].

نام کتاب: امنیت اطلاعات: از آگاهی تا آموزش

نویسندگان: دکتر محمد حسن‌زاده،

مهندس نرگس جانگیری

ناشر: نشر کتابدار

نویسندگان کتاب در پیشگفتار بیان کرده‌اند که امروزه کمتر کسی را می‌توان یافت که اطلاعاتی برای از دست رفتن نداشته باشد. همه ما در معرض از دست دادن اطلاعاتی هستیم که ممکن است به دست آوردن آنها دیگر امکان‌پذیر نباشد. از سوی دیگر نوعی از دزدی و ناامنی در محیط‌های کاری رواج یافته است که ریشه در گسترش فناوری اطلاعات و ارتباطات و آسیب‌های همراه آن دارد.

بدون شک شاه بیت امنیت اطلاعات، آگاهی است. در صورتی که همه ما از جوانب مختلف امنیت اطلاعات آگاه باشیم، کمتر دچار ضرر و زیان می‌شویم. ساده‌ترین و مؤثرترین راه برای دستیابی به آگاهی، آموزش است؛ بنابراین آموزش امنیت اطلاعات یکی از مهم‌ترین مباحثی است که باید در سطح فردی، سازمانی و ملی به آن پرداخته شود.

این کتاب به عنوان دستاوردی از نگاه جامع به امنیت اطلاعات، با این هدف تدوین شده است که دانش مناسبی از امنیت اطلاعات، اهمیت آن، مدل‌ها و مبانی نظری آن ارائه نماید و سپس با تأکید بر اهمیت آگاهی و کسب آن از رهگذر آموزش، چهارچوبی برای این مفهوم فراهم آورد. در ضمن با ارائه‌ی خلاصه‌ای از یافته‌های یک تحقیق میدانی، آموزه‌هایی عملی از امنیت اطلاعات را به خوانندگان عرضه می‌کند. فصل‌های نه‌گانه در این کتاب، مفهوم امنیت اطلاعات را از آگاهی تا آموزش پوشش می‌دهد.

در فصل اول، کلیت امنیت اطلاعات تبیین شده است. فصل دوم، به مؤلفه‌های تشکیل‌دهنده امنیت اطلاعات به همراه مصداق-ها و واژه‌های آنها به تفصل پرداخته شده است. فصل سوم کتاب به مدل‌های امنیت اطلاعات اختصاص دارد و در فصل چهارم، عوامل تأثیرگذار بر امنیت اطلاعات بررسی و بر نقش عوامل انسانی در ارتقای امنیت اطلاعات تأکید شده است. فصل‌های پنجم و ششم به آگاهی از امنیت اطلاعات و آموزش آن اختصاص یافته است تا به صورت توأمان دو مفهوم کلیدی این کتاب را تبیین کند. فصل هفتم نمونه‌ای از یک مطالعه موردی گزارش شده که در یک مؤسسه مالی به انجام رسیده است. در نهایت فصل‌های هشتم و نهم کتاب به ارائه‌ی راهکارهای عملیاتی در حوزه‌ی ارتقای امنیت اطلاعات به تفکیک نقاط آسیب‌پذیر پرداخته است.

این کتاب برای سه گروه از افراد تدوین شده است: کسانی که به مبحث امنیت اطلاعات علاقمند هستند؛ کسانی که به صورت حرفه‌ای با فناوری اطلاعات و ارتباطات کار می‌کنند و دانشجویان رشته‌های کتابداری و اطلاع‌رسانی، مدیریت فناوری اطلاعات و پژوهشگران حوزه‌ی منابع اطلاعاتی.

نفوذگران در جنگ سایبری چه کسانی هستند؟

۱- گروه نفوذگران کلاه سفید، هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. هکرهای کلاه سفید متخصصان شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا می‌کنند و به مسئولان گزارش می‌دهند.

۲- گروه نفوذگران کلاه سیاه، اشخاصی هستند که وارد کامپیوتر قربانی خود می‌شوند و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن ویروس و غیره می‌پردازند.

۳- گروه نفوذگران کلاه خاکستری، اشخاصی هستند که حد وسط دو تعریف بالا می‌شوند.

۴- گروه نفوذگران کلاه صورتی، این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

ایست بازرسی فرکانس‌ها چیست؟

مهره یا چوک فریت؛ این اسم برجستگی‌های استوانه‌ای شکلی است که نزدیک به انتهای برخی کابل‌های متصل به رایانه (و البته کابل بعضی وسایل الکترونیکی دیگر) دیده می‌شود. اگر یکی از این برجستگی‌ها را در یک کابل به درد نخور بشکنید (یا یکی از انواع دو تکه آنها را باز کنید) می‌بینید که زیر آنها یک استوانه فلز مانند و خاکستری رنگ قرار دارد که کابل از میان آن رد شده است. جنس این استوانه از فریت است؛ یک ماده نیمه مغناطیسی که از مخلوط کردن اکسید آهن با چند فلز دیگر به دست می‌آید و در خیلی موارد مانند ساخت هسته آنتن‌های درونی رادیو به کار می‌رود. فریت در واقع یک فیلتر انتخابی است که بسته به ترکیباتش می‌تواند بخش خاصی از امواج الکترومغناطیسی را به دام بیندازد و جذب کند.

از این خاصیت برای کاهش اثر تداخل نویزهای الکترومغناطیسی و به ویژه امواج رادیویی در کار وسایل الکترونیکی حساس مثل رایانه استفاده می‌شود؛ اما این نویزها و امواج مزاحم از کجا می‌آیند؟

رایانه‌ها وسایل نویزداری هستند. مادربوردِ رایانه، کریستالی دارد که با فرکانسی بین ۳۰۰ تا ۴۰۰۰ مگاهرتز پیوسته در حال نوسان است. کارت گرافیکی هم برای تغذیه اطلاعاتی مانیتور از نوسانگرهای دیگری استفاده می‌کند. به همین ترتیب ابزارهای دیگر هم اغلب پردازنده و فرکانس کار خاص خودشان را دارند.

همه این نوسانگرها می‌توانند در فرکانس کار خودشان سیگنال‌های رادیویی تابش کنند که بیشتر این تشعشعات به وسیله کِیس فلزی رایانه جذب و خنثی می‌شود؛ اما یک منبع دیگر برای تولید و انتقال نویز وجود دارد و آن، کابل‌های متصل به رایانه است.

این کابل‌ها برای جریانی که حمل می‌کنند، درست حکم یک آنتن بلند و قدرتمند را دارند و امواجی با همان فرکانس را در فضا پراکنده می‌کند که این سیگنال‌ها می‌تواند در کار رادیو و تلویزیون‌های نزدیک به کابل، اختلال ایجاد کند. به همین ترتیب، کابل‌های اتصال، توانایی جذب سیگنال‌های رادیویی موجود در محیط و انتقال آنها همراه با جریان‌های اصلی به درون مدارهای الکترونیکی رایانه را نیز دارند. اینجاست که یک استوانه فریت مناسب با احاطه کردن کابل در یک انتهای آن، این بخش مزاحم از فرکانس‌ها را جذب و به گرما تبدیل می‌کند در حالی که به جریان‌های اصلی که فرکانس متفاوتی دارند، اجازه عبور می‌دهد؛ یک ایست بازرسی برای فرکانس‌های قاچاق.

منابع

۱- موسسه آموزشی و تحقیقاتی صنایع دفاعی [homepage] ۱۵ بهمن ۱۳۹۰ [online]
<www.tridi.ir> [۱۵ بهمن ۱۳۹۰].

۲- مرکز هوافضا و هوانوردی [homepage] ۱۲ بهمن ۱۳۹۰ [online]
<www.aerocenter.ir> [۱۱ بهمن ۱۳۹۰].

۳- مافی، کتایون، جام جم آنلاین [homepage] ۱۳ بهمن ۱۳۹۰ [online]
<www.jamejamonline.ir> [۱۴ بهمن ۱۳۹۰].

سحابی سر اسب

یک سحابی تاریک در ابر مولکولی شکارچی است که نزدیک به شرقی‌ترین نقطه‌ی صورت فلکی شکارچی (ستاره نطاق) قرا گرفته‌است و ۱۵۰۰ سال نوری تا زمین فاصله دارد. این جرم همچون دندانه‌ای تیره در میان سحابی نشری قرمز رنگ خودنمایی می‌کند. چهره‌ی تیره‌ای از سر اسب در سحابی آشکار است و که این جرم در حقیقت غباری کدر است که در جلوی سحابی نشری و پرنوری قرار گرفته است. این جرم نیز همچون ابرهای جو زمین به صورت اتفاقی چنین شکلی را به خود گرفته است. بعد از چند هزار سال، بخش داخلی سحابی به دلیل حرکت دگرگون می‌شود. انتشار سحابی به رنگ قرمز به علت آمیخته شدن الکترون با پروتون‌های اتم هیدروژن است. همچنین در تصویر، سحابی بازتابی آبی رنگی مشاهده می‌شود که به گونه‌ای ممتاز نور آبی ستاره همدم را بازتاب می‌کند.

مثلث تابستانی چیست؟

مثلث تابستانی تشکیل شده از سه ستاره‌ی پر نور شب‌های تابستان که این ستاره‌ها عبارت‌اند از: ستاره آلفای شلیاق، ستاره آلفای دجاجه و ستاره آلفای عقاب که سه راس این مثلث را تشکیل می‌دهند. هر یک از این سه ستاره نام خاص دیگری نیز دارند. به آلفای شلیاق «نسر واقع یا کرکس نشسته یا وگا»، به آلفای دجاجه «دنب – ردف» و به آلفای عقاب «نسر طائر یا کرکس پرنده» می‌گویند.

(توضیح: روش عمومی نام‌گذاری ستارگان این است که در هر صورت فلکی، پرنورترین ستاره با حرف آلفای یونانی، ستاره بعدی با حرف بتا و ... نامیده می‌شود. به عنوان مثال، آلفا دجاجه یعنی پرنورترین ستاره صورت فلکی دجاجه. البته حدود ۲۰۰ ستاره آسمان، اسامی خاص دارند که با هر دو نام شناخته می‌شوند).

صورت فلکی دجاجه (مرغ یا ماکیان): نام یک صورت فلکی در نیمکره شمالی آسمان. دجاجه صورت فلکی روشن و وسیعی است که هم یادآور نام سنتی خود یعنی قو است و هم اسم غیر رسمی‌اش، صلیب شمالی را دارد. این صورت فلکی که پهنه‌ای از راه شیری را در تابستان پوشش می‌دهد دارای خوشه‌های ستاره‌ای فراوان به همراه سحابی‌های زیادی است. این صورت فلکی صلیب گونه در میانه راه شیری واقع است. نورانی‌ترین ستاره دجاجه (آلفای دجاجه) که در دم قرار دارد ردف یا دنب نامیده می‌شود و یکی از سه رأس مثلث تابستانی را شکل داده است. در کنار این ستاره، شکاف تاریکی در راه شیری دیده می‌شود که به گونی ذغال مشهور است.

صورت فلکی شلیاق (چنگ رومی): شلیاق صورت فلکی کوچکی است ولی به علت دارا بودن ستاره درخشان «نسر واقع یا کرکس نشسته» از اهمیت ویژه‌ای برخوردار است. این ستاره بعد از شعرای یمانی، درخشان‌ترین ستاره آسمان نیمکره شمالی است و همچنین پنجمین ستاره پر نور آسمان شلیاق که از فراز چنگ رومی با رنگ سفید می‌درخشد.

صورت فلکی عقاب: نام یک صورت فلکی لوزی شکل در نیمکره شمالی آسمان و یکی از ۴۴ صورت فلکی معرفی شده توسط بطلمیوس است. ستاره آلفا ستاره‌ای سه تایی است. ستاره بتا با نام الشاهین نیز ستاره‌ای سه تایی است. ستاره گاما با نام شاهین رازو یا Trazed شناخته می‌شود. ستاره اپسیلون نیز با نام دنب‌العقاب شناخته می‌شود. نیز ستاره زتا این صورت فلکی از نوع متغیر قیفاووسی است.

ستاره آلفای عقاب «کرکس پرنده» از جمله ستارگان درخشان آسمان است و در وسط سه ستاره تشکیل دهنده بال عقاب قرار گرفته است.

منابع

۱- آسمان شب ایران [homepage] ۱۸ بهمن ۱۳۹۰ [online] <www.nightsky.ir> [۱۹ بهمن ۱۳۹۰].

۲- مرکز علوم و ستاره شناسی تهران [homepage] ۱۷ بهمن ۱۳۹۰ [online] <http://sactehran.com> [۱۸ بهمن ۱۳۹۰].

۳- پایگاه اطلاع رسانی علوم ستاره شناسی و فضایی [homepage] ۱۰ بهمن ۱۳۹۰ [online] <www.persianstar.com> [۱۳ بهمن ۱۳۹۰].

رودخانه‌ها، گاز دی‌اکسیدکربن تولید می‌کنند

متخصصان علوم جوی درآمریکا تأکید کردند که رودخانه‌ها و نهرها منابع تولید گاز گلخانه‌ای دی‌اکسیدکربن هستند. این متخصصان در آزمایش‌های جدیدی دریافته‌اند که جویبارها و رودخانه‌ها، حجم قابل ملاحظه‌ای از گاز دی‌اکسیدکربن را وارد اتمسفر زمین می‌کنند. آنها تأکید کردند که این یافته باید در مطالعات مدل‌سازی جوی مورد توجه قرار بگیرد. این مطالعه که با تلاش کارشناسان دانشگاه ییل در آمریکا صورت گرفته می‌تواند روی نحوه بررسی‌ها و ارزیابی‌های متخصصان از حرکت کربن در چرخه زمین، آب و اتمسفر تأثیر بگذارد.

دیوید بوتمن از متخصصان برجسته دانشکده «مطالعات جنگلداری و محیط زیست» در این دانشگاه تشریح کرد: رودخانه‌ها و نهرها درست همانطور که ما در بازدم خود دی‌اکسیدکربن تولید می‌کنیم، منبع تولید این گاز هستند اما این واقعیت تاکنون در محاسبات دانشمندان روی منابع تولید گازهای گلخانه‌ای در نظر گرفته نشده است. این در حالی است که با توجه به یافته جدید، مناطق وسیعی مثل آمریکا می‌توانند نقش به سزایی در تولید حجم بالایی از این گاز داشته باشند.

آشنایی با لیست قرمز سازمان جهانی حفاظت از منابع طبیعی

سازمان جهانی حفاظت از منابع طبیعی در سال ۱۹۶۳، جامع‌ترین لیست وضعیت نگهداری از منابع طبیعی گیاهی و جانوری را به وجود آورد. سازمان بین‌المللی حفاظت از طبیعت و منابع طبیعی معتبرترین سازمان اعلام نظر در مورد وضعیت گونه‌ها است. این لیست قرمز (لیست داده‌های سرخ) بر روی ضوابط دقیقی برای ارزیابی خطر انقراض هزاران گونه و زیر گونه استوار شده است. این ضوابط مربوط به همه گونه‌ها در تمام مناطق دنیا می‌شود. هدف از تدوین این لیست جلب توجه مردم، تصمیم‌گیران و همچنین اجتماع‌های بین‌المللی به موضوع حفاظت از منابع طبیعی است تا از این طریق از روند رو به رشد انقراض گونه‌های گیاهی و جانوری جلوگیری شود. اصلی‌ترین ارزیاب‌ها و سنجش‌گران گونه‌ها در دنیا، انجمن مطالعه بر زندگی حیوانات لندن، مؤسسه مطالعه بر زندگی حیوانات، مرکز جهانی نظارت بر منابع طبیعی و بسیاری از گروه‌های تخصصی هستند که با کمیسیون بقای گونه‌های سازمان جهانی حفاظت از منابع طبیعی کار می‌کنند. به طور کلی تاکنون ارزیاب‌های این سازمان و گروه‌ها حدود نیمی از گونه‌های در خطر انقراض را گزارش کرده‌اند. یکی دیگر از اهداف این سازمان، به دست آوردن دسته‌های هر گونه و ارزیابی آنها در صورت امکان هر ۵ سال و یا هر ۱۰ سال است. در بازبینی گونه‌ها در سال ۲۰۰۶، بیش از ۷ هزار گونه زنده برای درج در لیست قرمز شناسایی شد. این گونه‌ها تا سال ۱۹۹۶ سنجیده نشده بودند. این سازمان در آخرین ارزیابی‌اش در ۱۲ سپتامبر سال ۲۰۰۷، گونه‌های لیست قرمز خود را تا ۱۶ هزار و ۳۰۶ گونه در معرض انقراض بالا برده است. این رقم ۱۸۸ گونه بیشتر از آخرین ارزیابی در سال ۲۰۰۶، است.

منابع:
۱- انجمن‌های تخصصی محیط زیست [homepage] ۱۵ بهمن ۱۳۹۰ [online]
<www.mohit-zist.com > [۱۵ بهمن ۱۳۹۰].
۲- زیست‌شناسی [homepage] ۱۲ بهمن ۱۳۹۰ [online]
<www.zist.gidital.com> [۱۱ بهمن ۱۳۹۰].
۳- گیاهان دارویی [homepage] ۱۳ بهمن ۱۳۹۰ [online]
< http://fa.parsiteb.com > [۱۴ بهمن ۱۳۹۰].

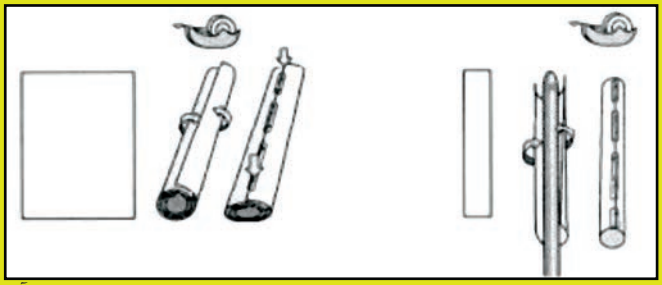
آزمایش لوله‌های کاغذی شگفت‌انگیز

مغز شما اطلاعات دریافت شده توسط چشمتان را به طور شگفت‌انگیزی با هم ترکیب می‌کند.

هنگامی که به اطراف خود می‌نگرید، امکان دارد اطلاعاتی که توسط دو چشم خود دریافت می‌کنید، با هم مغایر باشند. آیا می‌دانید در اینگونه موارد مغزتان چگونه رفتار می‌کند؟ آیا گیرنده‌هایی که در مغز قرار دارند مستقل از هم عمل می‌کنند یا متأثر از یکدیگر هستند؟ با انجام آزمایش زیر خواهید فهمید که هر یک از دو چشم چگونه بر دیگری تأثیر می‌گذارند.

وسایل مورد نیاز

یک پرده‌ی سفید کاملاً روشن، یا دیوار سفید یا ورق سفید کاغذ؛ چند ورق کاغذ سفید مثل کاغذ فتوکپی یا کاغذ تایپ؛ نوار شفاف.



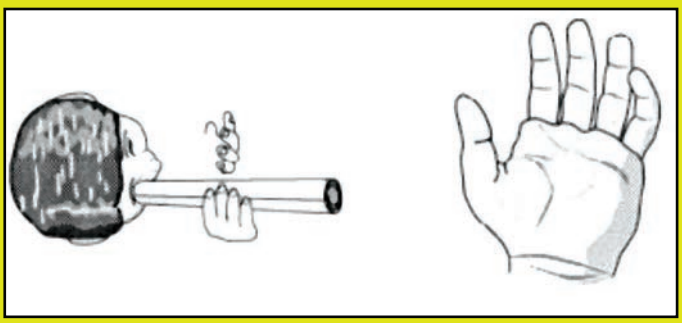
سه ورق کاغذ را به صورت لوله‌هایی به طول ۲۸ سانتی‌متر و قطر تقریبی ۱/۵ سانتی‌متر درآورید. برای جلوگیری از باز شدن کاغذها آنها را چسب بزنید. یکی از لوله‌ها را طوری فشار دهید که سطح مقطع آن به صورت یک بیضی پهن درآید (همانند شکل روبه‌رو).

تکه‌ای کاغذ را به صورت نواری به عرض تقریبی ۶/۴ سانتی‌متر و طول تقریبی ۲۸ سانتی‌متر ببرید. این نوار را پیچانید و با آن لوله‌ای به قطر ۱/۵سانتی‌متر و طول ۲۸ سانتی‌متر بسازید. با این لوله‌های کاغذی می‌توانید چهار آزمایش انجام دهید:

سوراخی روی دست؛ همپوشانی نقاط؛ دایره‌ها یا بیضی‌ها؛ روشن‌تر یا تاریک‌تر؟

سوراخی روی دست

شرح آزمایش



یکی از لوله‌های کاغذی را (که با یک ورق کامل ساخته‌اید) در دست راست خود نگه‌دارید. در حالی که هر دو چشم خود را باز نگه‌داشته‌اید، با چشم راست به درون لوله نگاه کنید. حال کف دست چپ خود را جلوی صورت بیاورید و همانند شکل زیر، در سمت چپ لوله نگه‌دارید.

در کف دست خود یک سوراخ خواهید دید.

چه اتفاقی در حال وقوع است؟

یکی از چشم‌ها یک دست، و دیگری یک سوراخ می‌بیند. چشم و مغز شما دو تصویر را با هم ترکیب می‌کند و یک دست با سوراخی در وسط آن می‌آفرینند!

همپوشانی نقاط

شرح آزمایش

دو لوله‌ی کاغذی بردارید و روی دو چشم خود نگه‌دارید و از درون آنها به پرده‌ی سفید (یا دیوار سفید) نگاه کنید. ابتدا یکی از دو چشم را ببندید، سپس باز کنید و دیگری را ببندید. آیا روشنی نقطه‌ای که از درون لوله‌ها می‌بینید، با هر دو چشم یکسان است؟

لوله‌های کاغذی را حرکت دهید تا قسمتی از دونقطه روشن روی هم بیفتد. توجه کنید که آن قسمت پرنورتر است. نقطه‌ها را به طور کامل روی هم بیاندازید. آیا نقطه‌ی ترکیبی روشن‌تر از نقاط تنها به نظر می‌رسد؟ با بستن یک چشم این موضوع را تحقیق کنید.

چه اتفاقی در حال وقوع است؟

وقتی فقط بخشی از دو نقطه را روی هم می‌اندازید، چشم و مغز شما نتیجه می‌گیرند که مجموع دو نقطه‌ی روشن باید از یک نقطه‌ی تنها روشن‌تر به نظر برسند. وقتی دو نقطه به طور کامل روی هم می‌افتند، به نظر می‌رسد که مغز شما یکی از آنها را نادیده می‌گیرد.

دایره‌ها یا بیضی‌ها

شرح آزمایش

یکی از لوله‌های کاغذی مدور را روی یک چشم و لوله‌ای که سطح مقطع آن را به صورت بیضی درآورده‌اید را روی چشم دیگر بگذارید. با دو لوله به دیوار سفید نگاه کنید و نقاط روشن را روی هم قرار دهید. دایره می‌بینید یا بیضی؟ جای لوله‌ها را با یکدیگر عوض و آزمایش را تکرار کنید. اگر شما در ابتدا فقط دایره را می‌دیدید، حال فقط بیضی را می‌بینید.

چه اتفاقی در حال وقوع است؟

مغز و چشمان شما در ادغام کردن تصاویر مشکل دارند. بیشتر اشخاص یک چشم غالب دارند. مغز این افراد تصویری که از چشم غالب می‌آید را انتخاب می‌کند. بعضی از افراد هم چشم غالب ندارند و بنابراین دو شکل روی هم افتاده را می‌بینند. بهترین بازیکنان بیس‌بال چشم غالبی ندارند.

روشن‌تر یا تاریک‌تر؟

شرح آزمایش

یکی از لوله‌هایی را که با ورق کاغذ کامل ساخته‌اید را بردارید و جلوی یکی از چشمانتان بگیرید و در حالی که هر دو چشمتان باز است، به دیوار سفید نگاه کنید. توجه کنید که نقطه‌ی نوری را که از درون لوله می‌بینید، روشن‌تر از بدنه‌ی لوله به نظر می‌رسد.

همین کار را با استفاده از لوله‌ای انجام دهید که از نوار باریک کاغذی درست کرده‌اید. توجه کنید که نقطه‌ی روشن، این بار تاریک‌تر از بدنه‌ی لوله است.

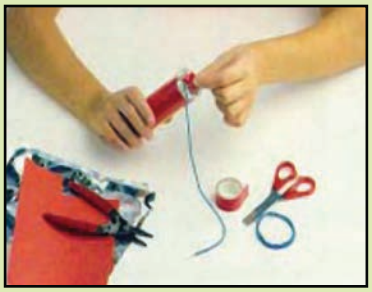
چه اتفاقی در حال وقوع است؟

گیرنده‌های نوری درون چشم شما، به محض دریافت نور، سیگنالی به مغزتان می‌فرستند. گیرنده‌ای که نور را دریافت می‌کند، به گیرنده‌های مجاور نیز سیگنال‌هایی می‌فرستد که باعث می‌شود حساسیتشان را نسبت به نور از دست بدهند. وقتی بدون لوله به دیوار سفید می‌نگرید، یک زمینه با روشنایی یکنواخت می‌بینید. زیرا همه‌ی گیرنده‌ها به طور مساوی تحریک شده‌اند. زمانی که شما از درون لوله‌ای نگاه می‌کنید که با ورق کاغذی کامل درست شده است، نقطه‌ی روشن با حلقه‌ی تاریک محاصره شده است. چون گیرنده‌های مرکز شبکیه توسط سیگنال‌های حلقه‌ی تاریک بازداشته نشده‌اند، نقطه روشن‌تر به نظر می‌رسد. در مقابل از دیواره‌های لوله‌ی ساخته شده از نوار باریک کاغذی، نور می‌تابد. وقتی از طریق این لوله (با دیواره‌های نازک) نگاه می‌کنید، نقطه تاریک‌تر به نظر می‌رسد. زیرا نوری که از دیواره‌های لوله می‌تابد، حساسیت گیرنده‌های مرکز شبکیه‌ی شما را می‌کاهد.

منبع

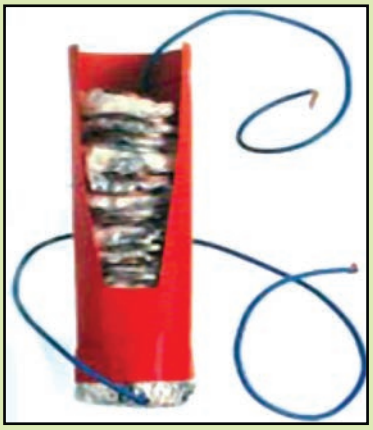
۱- لوله‌های کاغذی شگفت‌انگیز [homepage] ۱۸ بهمن ۱۳۹۰ [online]
< http://daneshnameh.roshd.ir > [۱۹ بهمن ۱۳۹۰].

باتری بسازیم



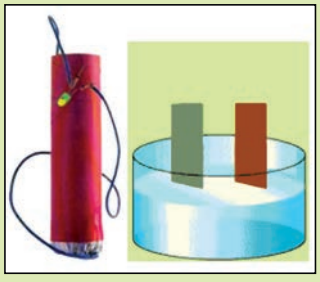
◄ با مقوا یک استوانه بسازید و در زیر آن ورق آلومینیوم بچسبانید. سپس به ورق آلومینیوم سیمی وصل کنید.

◄ مقداری پنبه را به آب نمک یا آبلیمو آغشته کنید و در داخل قوطی قرار دهید. در مرحله بعد سکه‌ای تمیز روی پنبه قرار دهید. سپس به ترتیب ورق آلومینیوم، پنبه آغشته به آبلیمو و سکه را روی هم قرار دهید و این کار را چند بار تکرار کنید.



◄ سرانجام سیمی را به طرف دیگر سکه وصل کنید.

◄ دو طرف دیگر سیم‌ها را به زبانتان بزنید چه احساسی دارد؟ آنها را به لامپی وصل کنید چه مشاهده می‌کنید؟



◄به شکل‌های زیر توجّه کنید

ساخت فرستنده‌ی رایانه‌ای

چقدر مایل هستید تا متن پیامی را بدون سیم، بدون «ارتباط اینترنت و بدون کارمزد» به یکی از دوستانتان بفرستید؟

در این پروژه ما یک فرستنده‌ی رادیویی ساده می‌سازیم که به پورت سریال کامپیوترتان وصل می‌شود. کامپیوتر به کمک یک برنامه‌ی ساده اطلاعات کلمه‌ای که شما تایپ می‌کنید را به سیگنال‌های رادیویی تبدیل می‌کند. این سیگنال توسط کامپیوتر دیگر رمزگشایی می‌شود. کامپیوتر دیگر این کار را به کمک یک مدار گیرنده‌ی رادیویی ارزان و کارت صدا انجام می‌دهد. با کمی مطالعه درمی‌یابید که شما حتی به کامپیوتر دیگر نیز نیاز ندارید زیرا سیگنال رادیویی به صورت کدهای مورس ارسال می‌شوند که هر کسی با کمی تمرین می‌تواند رمزگشایی آن را یاد بگیرد. همچنین می‌توان از آن به عنوان یک زبان رمز یا به عنوان راهی برای ارسال پیام به نقاط دور (مثلاً به کمک یک آینه) در نظر گرفت.

وسایل مورد نیاز

۱- اسیلاتور (نوسان‌ساز) یک مگاهرتز: اگر شما رادیویی دارید که می‌تواند بسامدهای دیگر را دریافت کند می‌توانید از اسیلاتور با بسامدهای دیگر استفاده کنید.

۲- اتصال پورت سریال: ما از اتصال ۹ پین RS۲۳۲ استفاده می‌کنیم. شما می‌توانید یک کابل سریال قدیمی را باز کنید یا از فروشگاه الکترونیک یا رایانه، یک اتصال نو بخرید.

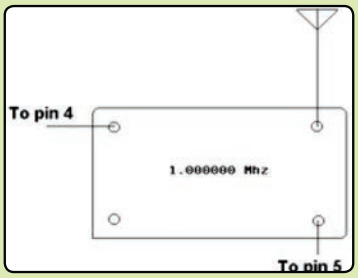
۳- مقداری سیم روکش‌دار به عنوان آنتن: تقریباً هر سیمی برای این کار مناسب است، هرچه بلندتر بهتر.

۴- سیم سوسماری: این یک تکه سیم با سرهای سوسماری (در هر طرفش) است.

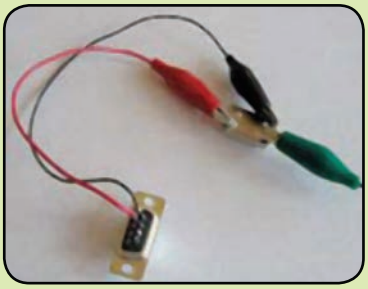
برای ساخت طرح اولیه‌ی فرستنده‌مان، ما قطعه‌ها را با سیم سوسماری به هم وصل می‌کنیم. این کار به ما امکان تعویض اسیلاتور یک مگاهرتز با اسیلاتور دیگر و در نتیجه تغییر بسامد را می‌دهد. سپس ما نسخه‌ای از پروژه که با مدار چاپی (سوکت برای اسیلاتور و LED برای روشن و خاموش شدن هم‌زمان با کد مورس) روشن ساخته می‌شود را به شما نشان خواهیم داد.

قدم اول دو نیم‌کردن سیم‌سوسماری است. در تصویر بالا، دو سیم‌سوسماری سیاه و قرمز را بریده‌ایم تا سیم‌کشی و ارتباطات مدار را راحت‌تر بتوان دید. کمی از روکش عایق انتهای سیم‌ها را بردارید و یکی از سیم‌ها را به پین ۵ و دیگری را به پین ۴ لحیم کنید.

پین ۵ اتصال پورت سریال (سیم سیاه در تصویر بالا) به پین زمین اسیلاتور وصل می‌شود. پین ۴ اتصال پورت سریال به پین تغذیه‌ی اسیلاتور وصل می‌شود. تصویر زیر طرحی از نحوه‌ی سیم‌کشی را نشان می‌دهد.



در تصویر زیر اسیلاتور به طور وارونه دیده می‌شود و سیم‌کشی را به وضوح می‌توانید ببینید.



سیم سوسماری سبز به آنتن وصل است که می‌تواند هر سیم بلندی باشد. این به پین خروجی اسیلاتور وصل می‌شود. پین باقی مانده‌ی اسیلاتور (نزدیکترین به گوشه‌ی تیز) بدون استفاده رها می‌شود. به این ترتیب فرستنده‌ی رایانه‌ای شما کامل است.

منبع:

محسنی، مریم و فروزان‌کیا. مرکز یادگیری سایت تبیان، [homepage] ۵ بهمن ماه ۱۳۹۰ [online]
<www.tebyan.net> [۶ دی ۱۳۹۰].

چهارمین دوره کنفرانس و مسابقه ملی «اوریگامی» برگزار می‌شود

چهارمین دوره کنفرانس و مسابقه ملی اوریگامی در روزهای ۱۹ تا ۲۱ اردیبهشت‌ماه سال آینده در دانشکده ریاضی و علوم کامپیوتر دانشگاه امیرکبیر برگزار خواهد شد.

اوریگامی یا «هنر کاغذ و تا» یکی از کاردستی‌های محبوب ژاپنی است که امروزه در سراسر جهان طرفداران زیادی دارد. هدف این هنر، آفریدن طرح‌های جالب با تا زدن‌های کاغذ است.

اوریگامی هنر و اندیشه تا زدن کاغذ یا صفحه‌هایی از جنس پلاستیک، فلز و مواد دیگر برای خلق شکل‌های مختلف است. این شکل‌ها تعداد زیادی از حیوانات، پرندگان، ماهی‌ها، وسایل بازی، سقف استادیوم‌ها و وسایل تزیینی، شکل‌های هندسی و اشکالی در ارتباط با گرافیک، معماری، صنعت و ... را شامل می‌شوند. به عنوان مثال با استفاده از این هنر، دانشمندان می‌توانند فضاپیماهای مدرن‌تری را با تا زدن به روش اوریگامی به فضا بفرستند. اوریگامی، دنیای ریاضیات، مهندسی، علوم و هنرهای دیگر را دچار تحول‌های کارامدی کرده است. اوریگامی طیف بسیار گسترده‌ای از کودکان دبستانی تا استادان دانشگاه را در بر می‌گیرد. تمام مردم می‌توانند از آن لذت ببرند و با خلق طرح‌های جدید به تاریخ اوریگامی بپیوندند. آخرین مهلت ارسال مقالات، ۱۹ فروردین ماه و زمان اعلام نتایج، اول اردیبهشت ماه سال آینده خواهد بود. موضوع مقاله‌های ارائه شده به این کنفرانس «ریاضیات اوریگامی»، «اوریگامی در علوم تربیتی و آموزش»، «اوریگامی در صنعت و مهندسی»، «کاربرد اوریگامی در زیباسازی شهری»، اوریگامی در علوم پایه»، «طراحی»، «هنر»، «نحوه آموزش اوریگامی»، «کارهای برش»، «تا کردن (Folding)»، «اوریبوتیک (Oribotic)» و «اوریفابریک (Ori-fabric)» اعلام شده است. علاقمندان می‌توانند برای کسب اطلاعات بیشتر به نشانی اینترنتی .http://cg.aut ac.ir/origami مراجعه کنند.

نخستین کنفرانس بین‌المللی «نظریه‌پردازی و پیشرفت علوم انسانی» برگزار می‌شود

نخستین کنفرانس بین‌المللی «نظریه‌پردازی و پیشرفت علوم انسانی» با حضور اندیشمندان و صاحبنظران داخلی و خارجی حوزه علوم انسانی، ۱۱ و ۱۲ آذرماه سال آینده در دانشگاه آزاد اسلامی واحد گرگان برگزار می‌شود.

نخستین کنفرانس بین‌المللی «نظریه‌پردازی و پیشرفت علوم انسانی؛ مفاهیم و موانع و ضرورت‌ها» با حمایت معاونت پژوهش و فناوری دانشگاه آزاد و دبیرخانه هیئت حمایت از کرسی‌های نظریه‌پردازی برگزار می‌شود.

هدف از برگزاری این کنفرانس ایجاد فرصت برای طرح نظرات و نقدهای جدید در فضاهای علمی و حمایت از اندیشمندانی است که نظریه‌هایی دارند و از پشتوانه علمی قوی برخوردار هستند.

رئیس شورای آموزشی منطقه ۱۰ دانشگاه آزاد با اشاره به محورهای مقدماتی کنفرانس بین الملل «نظریه‌پردازی و پیشرفت علوم انسانی» گفت: «تبیین مبانی فرایند و سازوکارهای نظریه‌پردازی»، «توسعه و گسترش تفکر و فرهنگ نقد و نظریه‌پردازی»، «شناسایی موانع و راهکارهای نظریه‌پردازی در ایران»، «تبیین نقش کرسی‌های نظریه‌پردازی در پیشرفت فرهنگ و تمدن اسلامی»، «تدوین و توسعه نظریه‌های بومی از طریق کرسی‌های نظریه پردازی» و «ارائه الگوی ایرانی اسلامی نظریه‌پردازی و نقد» از محورهای این کنفرانس است. این کنفرانس همزمان با ایام دهه فجر رونمایی می‌شود، گفت: علاقمندان برای کسب اطلاعات بیشتر می‌توانند به سایت دبیرخانه کنفرانس به نشانی http://gorganconf.ir مراجعه کنند.

نخستین مسابقه «عکس متالوگرافی» برگزار می‌شود

نخستین مسابقه «عکس متالوگرافی»، ۱۳ و ۱۴ اردیبهشت ماه سال آینده در دانشکده مهندسی معدن و متالورژی دانشگاه صنعتی امیرکبیر با حمایت شبکه آزمایشگاهی فناوری نانو برگزار می‌شود.

پیشرفت علم تحلیل ریزساختار، ایجاد فرصت برای ارائه آثار مربوط به علم و خواص مواد و تبادل اطلاعات در زمینه متالوگرافی از جمله اهداف برگزاری این مسابقه عنوان شده است.

مسابقه عکس متالوگرافی در شش محور «میکروسکوپ الکترونیکی»، «میکروسکوپ نوری»، «متالوگرافی رنگی»، «مینرالوگرافی»، «سراموگرافی» و «عکاسی هنری علمی» برگزار می‌شود. بر اساس اعلام دبیرخانه این مسابقه، شرکت‌کنندگان می‌توانند عکس‌های خود را برای شرکت در بخش‌های آزاد، هنری، موضوعی و نرم‌افزار متالوگرافی به دبیرخانه مسابقه ارسال کنند.

ثبت نام برای شرکت در نخستین مسابقه عکس متالوگرافی که در دانشگاه صنعتی امیرکبیر برگزار می‌شود از مهرماه آغاز شده است و تا پایان اسفند ماه سال جاری ادامه دارد. عناوین عکس‌های راه یافته به بخش نمایشگاه، فروردین ماه سال آینده بر روی پایگاه اینترنتی مسابقه قرار می‌گیرد. نتایج نهایی داوری نیز ۱۴ اردیبهشت ماه در مراسم اختتامیه نمایشگاه اعلام خواهد شد. افراد می‌توانند برای کسب اطلاعات بیشتر و شرکت در مسابقه به پایگاه اینترنتی مسابقه به نشانی http://imc2012.ir مراجعه کنند.

دانشگر را از خودتان بدانید

دانشگر نشریه‌ای علمی است که با هدف ترویج علم و فناوری و اطلاع‌رسانی از تازه‌های دانش و فناوری منتشر می‌شود. اما تدوین و انتشار این نشریه تنها بخش کوچکی از این راه است.

مهم‌تر از آن همراهی شما مخاطبان عزیز با دانشگر است.

این صفحه مربوط به شماست. برای دانشگر نامه بنویسید و آن را به نشانی نشریه یا پست الکترونیکی آن بفرستید.

از کدام بخش نشریه بیشتر بهره برده‌اید؟ به نظرتان چه بخش‌هایی خیلی مهم نیست یا چه بخش‌هایی باید به نشریه اضافه شود؟

خلاصه اینکه هیچ بخشی از نشریه را از نگاه تیزبین خود محروم نکنید، از طرح روی جلد تا مقالات.

شما می‌توانید برای نشریه مطلب هم بنویسید. این مطالب پس از بررسی و تأیید تحریریه به نام خودتان در نشریه منتشر می‌شود.

دانشگر می‌تواند میعادگاهی برای همه دوست‌داران ترویج علم و فناوری در ایران عزیزمان باشد.

برگ اشتراک ماهنامه علمی دانشگر

◀بهای اشتراک و هزینه پست:

یکساله (دوازده شماره)۲۰۰/۰۰۰ ریال　　شش ماهه (شش شماره): ۱۰۰/۰۰۰ ریال

بهای اشتراک برای دانش آموزان و دانشجویان (با ۳۰٪تخفیف)

یک ساله (دوازده شماره)۱۴۰/۰۰۰ریال　　شش ماهه (شش شماره): ۷۰/۰۰۰ ریال

◀نحوه پرداخت:

برای اشتراک یک ساله یا شش ماهه ماهنامه مبلغ حق اشتراک را به حساب سیبا به شماره ۲۱۷۲۰۴۹۰۰۱۰۰۲ قابل پرداخت در کلیه شعب بانک ملی ایران به نام مرکز تحقیقات سیاست علمی کشور واریز نمایید.

◀مشخصات مشترک:

نام و نام‌خانوادگی:　　سازمان/ دانشگاه/ مدرسه:

◀نشانی و اطلاعات تماس:

شهر:　　آدرس دقیق پستی:

کدپستی :

تلفن تماس:　　تلفن همراه:

پست الکترونیکی:

◀نحوه ارسال:

فیش بانکی را به همراه این فرم به نمابر ۸۸۰۶۹۷۶۰ ارسال کرده و در اولین فرصت اصل فیش بانکی را برای تکمیل اشتراک به نشانی زیر پست کنید:

تهران: میدان ونک، خیابان ملاصدرا، خیابان شیرازجنوبی، خیابان سهیل، شماره ۹ کدپستی: ۱۴۳۵۸-۹۴۴۶۱

صندوق پستی: ۵۵۴-۱۳۱۴۵

برای استفاده از تخفیف ارسال کپی کارت معتبر دانش‌آموزی یا دانشجویی الزامی است.