**امنیت مخابرات،** شبکه یکپارچه پدافند هوایی و ایجاد بستری امن در مقابل سوء استفاده از مکالمات و ارتباطات.از ابتدای زندگی بشر، امنیت یکی از دغدغه‌های اصلی انسان‌ها بوده است. با اختراع تجهیزات ارتباطی و مخابراتی، روند رو به رشد و تأثیر این پدیده در زندگی روزمره مردم، خیلی‌زود جایگاه خود را پدیدار کرد؛ تا جایی که امروزه بیشترین تماس‌های مردم در کلیه امور روابط کاری و زندگی شخصی با استفاده از انواع تجهیزات ارتباطی انجام می‌شود. پیشرفت و توسعه این پدیده، به‌سرعت جایگاه ویژه خود را در بین سایر اختراعات و تسهیلات در بین مردم و جهت سهولت روابط کاری در تمامی سازمان‌های دولتی و غیر دولتی آشکار کرد؛ به‌طور‌ی‌که عدم وجود سامانه و تجهیزات ارتباطی در هر سازمان، انجام کارها را غیرِ ممکن می‌نمود (معاونت فاوا، 1396: 11). انواع تجهیزات ارتباطی که با تلگراف و تلفن‌های بسیار ساده، کار خود را در برقراری ارتباط بین مردم آغاز کردند؛ خیلی‌زود صاحب جایگاه ویژه‌ای در نیروهای نظامی و به یکی از ارکان اصلی ارتش‌ها تحت عنوان سلسله‌اعصاب در کنترل صحنه‌های نبرد تبدیل شدند (همان: 15). با پیشرفت روزافزون سامانه‌های مخابراتی و ارتباطی در انواع باسیم، بی‌سیم و ماهواره‌ها و نقش اساسی آن‌ها در زندگی مردم و ارتباطات سازمانی در ادارات، ارگان‌های دولتی و خصوصی و به‌ویژه در نیروهای نظامی، در مقابل بهره‌برداری از مبادلات اطلاعاتی در ارتباطات با شروع استراق سمع و یا ایجاد اختلال در سامانه‌های ارتباطی نیز رشد همگام پیدا کرد و به چالش بزرگی برای بهره‌وران از سامانه‌های ارتباطی تبدیل شد. امروزه با راه‌اندازی ارتباطات ماهواره‌ای و به‌ تبعِ آن بهره‌برداری از اینترنت و شبکه‌های اجتماعی، عدم امنیت در ارتباطات، درحجم وسیعی گسترش ‌یافته و به‌ نوعی نبرد نوینی تحت عنوان «سایبری» گریبان‌گیر تجهیزات ارتباطی و در هایت عدم وجود امنیت مخابرات در تمامی زمینه‌ها شده است (همان: 24). با پدیدارشدن سوء استفاده از اطلاعات و داده‌ها در ارتباطات تلفنی و سایر تجهیزات ویژه تبادلات اطلاعاتی، به‌ناچار نحوه مقابله با این پدیده نیز آغاز شد و در ابتدا با کدگذاری و رمز‌نمودن روش مکالمات و سپس با ابداع تجهیزات مقابله با استراق سمع، دستگاه‌های رمزکننده در کنار تجهیزات ارتباطی آغاز به کار کرد (همان: 32). در طول هشت سال دفاع مقدس نیز استراق سمع و بهره‌برداری از مکالمات نیروها و ارتباطات بین سازمانی برای طرفین درگیر، یکی از راهبردی‌ترین روش‌ها برای دستیابی به اطلاعات و تحرکات و آگاهی از چگونگی فعالیت‌های یکدیگر بود. استراق سمع و بهره‌برداری از مکالمات و ارتباطات به‌وسیلۀ سایت‌ها و هواپیماهای شنود الکترونیکی، صورت می‌گرفت و به‌منظور پوشش مناسب در عدم بهره‌برداری دشمن از مکالمات و ارتباطات سامانه‌ای، تجهیزات رمزکننده و کد و رمزگذاری در مکالمات و صدور دستورالعمل‌ها و روش‌های برقراری امنیت مخابرات در دستور کار قرار گرفت و فرماندهی پدافند هوایی نیز از این امر مستثنا نبود. در راستای برقراری امنیت مخابرات در جنگ تحمیلی به‌ویژه در سطح شبکه یکپارچه پدافند هوایی که ایجاد عدم سوء استفاده از مکالمات و ارتباطات تجهیزاتی از اهمیت خاصی برخوردار بود، ضمن بهره‌گیری از تجهیزات رمزکننده در تجهیزات تله‌تایپ و دورنگار، از کدگذاری جهت کلیه تجهیزات و سامانه‌های پدافند هوایی و مکالمات مورد استفاده در تبادل اطلاعات استفاده شد. دراین‌رابطه در ابتدا کدها به‌صورت چند ورق و خیلی مختصر تهیه می‌شد. با گستردگی عملیات‌ها و گسترش متعدد مراکز کنترل و فرماندهی و مراکز حساس و حیاتی و حساسیت حفظ امنیت مخابرات، کدهای مورد نظر در قالب کتاب به‌صورت ماهانه و در مقاطعی به علت ضرورت، هفتگی تهیه می‌شد و در اختیار یگان‌های بهره‌ور قرار می‌گرفت و یگان‌ها ملزم بودند در مکالمات عملیاتی و آمادی و گاه اداری، حتماً از کدهای مربوطه در مکالمات جهت امنیت مخابرات استفاده کنند (همان: 77). جهت عدم کشف مکالمات فی‌مابین مراکز کنترل و فرماندهی و یگان‌های عمل‌کننده پدافند هوایی و هواپیماهای طرح پدافندی، در هنگام انجام اقدامات تاکتیکی و یا در موقع اعلام وضعیت عملیاتی و غیر عملیاتی‌بودن سامانه‌ها و چگونگی گسترش‌ها، از کدهای مربوطه استفاده می‌شد. ضمن اینکه کلیه امور عملیاتی، آمادی، پشتیبانی و اداری که می‌بایستی توسط ارتباط تلفنی و دورنگار انجام شود نیز از کدهای مورد نظر بهره‌برداری می‌کرد. برای آشنایی با چگونگی این روند، به ذکر چند مثال پرداخته می‌شود: به‌عنوان‌ مثال هواپیمای طرح پدافندی، هواپیمای شکاری ره‌گیری می‌باشد که جهت درگیری هوایی با هواپیمای مهاجم، از پایگاه هوایی خودی پرواز می‌کند و در اختیار شبکه راداری قرار می‌گیرد تا شبکه راداری با هدایت و کنترل این هواپیما، علیه هواپیمای مهاجم اقدام تاکتیکی انجام دهد. این هواپیما با یک معرف مانند «پردیس 1» به پرواز در می‌آید و ایستگاه رادار مربوطه با استفاده از این معرف، با هواپیما تماس برقرار می‌کند و بقیه امور عملیاتی، در لحظات رهگیری و درگیری نیز در حدِّ ممکن که از سرعت اقدامات تاکتیکی کاسته نشود، با کدهای تعیین‌شده، انجام می‌شود. به‌عنوان ‌مثال برد: قاسم، ارتفاع: محمود، سمت: بهزاد، هواپیمای مهاجم: کرکس و .... در مورد تجهیزات پدافند هوایی نیز با همین روند، امور مکالمات برای برقراری امنیت مخابرات صورت می‌گرفت که می‌توان به نمونه‌هایی از آن همانند سامانه هاک: شاهین، موشک هاک: قُمری، رادار جست‌وجوکننده: امید، رادار تعقیب هدف: نگاه، عملیاتی: عمران، غیر عملیاتی: بلوط و ... اشاره کرد که این امر در حفظ امنیت مخابرات و عدم کشف مکالمات مورد تبادل در امور عملیاتی در طول هشت سال دفاع مقدس، بسیار سازنده و مؤثر واقع می‌شد و هرگونه عدول و سرپیچی از این روش‌ها و دستورالعمل‌ها، با توجه به توان شنود بالای عراق که باید کمک سایر کشورهای منطقه و فرا‌منطقه‌ای توسط سایت‌های شنود زمینی و هواپیماهای شنود و رادارهای پرنده را در کمک به آن اضافه کرد، موجب دستیابی عراق به اطلاعات مورد نیاز از اقدامات و عملکرد نیروهای ایران می‌شد. این موضوع در طراحی عراق برای اقدام علیه ایران بسیار کارساز بود و عملکرد نیروهای ایرانی به‌ویژه در شبکه یکپارچه پدافند هوایی با استفاده از دستگاه‌های رمزکننده و بهره‌برداری از کدهای تعیین‌شده، سد محکمی در جلوگیری از استراق سمع دشمن شد. سوابق و اسناد موجود، گویای این امر می‌باشد (همان: 112 و 113). **مآخذ:** معاونت فاوا، نقش ارتباطات و فنّاوری اطلاعات پدافند هوایی در دوران دفاع مقدس، تهران: نیروی پدافند هوایی، 1396.