امنیت در فضای سایبری و مجازی

امنیت، یکی از اصلی ترین نیازهای بشری در تمامی اعصار و قرون بوده و در آینده نیز خواهد بود.

در این تردیدی نیست که همگان نیازمند امنیت هستند.

در این تردیدی نیست که همگان نیازمند امنیت هستند، اما در اینکه مصداق ناامنی چیست.

منابع تهدید کننده امنیت براساس شرایط و ساختاری مختلف، دگرگون شده و مصداق ها تابعی از شرایط زمانی و مکانی هستند.

هرچند که جنگ از قدیمی ترین منابع تهدیدکننده امنیت در طول تاریخ بوده، ولی صد سال پیش، از جنگ های الکترونیک خبری نبود.

بیست سال پیش کسی از امنیت فضای سایبر و مجازی سخنی نمیگفت، ولی اکنون امنیت فضای مجازی به عضوی جدا نشدنی از امنیت بین المللی تبدیل شده است.

اهمیت امنیت در فضای سایبری

امنیت فضای سایبری به خاطر اتکای بیش از حد تمامی بازیگران سیاسی به آن، بی تردید مقوله ای استراتژیک قلمداد میشود.

به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه ای امنیتی شده است.

شایان ذکر است که ناتو از چندی پیش تعدادی از نخبگان امنیت ملی و سیاست خارجی را تحت رهبری آلبرایت وزیر خارجه پیشین آمریکا گرد هم آورد.

تا به این سؤال پاسخ دهند که امنیت کشورهای عضو ناتو در آینده و دهه ای که در پیش است، چگونه و با تأثیر از چه منابعی مورد تهدید واقع می شود.

معنا و تاریخچه فضای سایبر

به مجموعه هایی از ارتباطات درونی انسان ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

به طور مثال یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل، اینستاگرام، تلگرام و ... با یکدیگر ارتباط برقرار کنند.

بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدهای کیبرد یا گوشی های هوشمند یا حرکت موس صورت می گیرد.

مشتق شده است لغت یونانی Kybernetes به معنی سکان دار یا راهنما مشتق شده است.

سایبرنتیک را نوربرت وینر در سال 1948 استفاده نمود. نوربرت وینر یک ریاضی دان بود.

نویسنده داستان های علمی تخیلی ویلیام گیبسون از این واژه در داستان هایش استفاده نموده است.

واژهCyber

سایبر پیشوندی است برای توصیف یک شخص، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است.

در طی توسعه اینترنت واژه های ترکیبی بسیار از این کلمه سایبر به وجود آمده است.

فضای سایبر.Cyberspace

شهروند سایبر.Cybercitizen

پول سایبر.Cybercash

فرهنگ سایبر.Cyberculture

راهنمای فضای سایبر.CyberCoach

تجارت سایبر.Cyberbussiness

کانال سایبر. Cyberchannel

جرائم سایبری

در اواسط دهه 90 با گسترش شبکه های بین المللی و ارتباطات ماهواره ای، نسل سوم جرایم کامپیوتری، تحت عنوان جرایم سایبری یا جرایم در محیط سایبر شگل گرفت.

به این ترتیب جرایم اینترنتی را می توان مکمل جرایم کامپیوتری دانست.

بخصوص اینکه جرایم نسل سوم کامپیوتری که به جرایم در محیط مجازی معروف است.

طبیعت این جرایم و سو استفاده های مرتکب شده در این دنیای مجازی جدید هیچگاه در دنیای حقیقی دیده نشده است.

امنیت ناکافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می دهد.

در ایران نیز روزانه با توجه به گسترش اینترنت به جرایم سایبری افزوده می شود.

جرایم سایبری در سال 1400 به شرح زیر است:

توهین و هتک حیثیت افراد و نشر اکاذیب.

کلاهبرداری در فضای مجازی.

هک (دسترسی غیر مجاز).

تخریب و اختلال در داده ها و سیستم ها.

انگیزه در جرایم گزارش شده:

کسب منابع مالی.

ضد اخلاقی.

انقام جویی.

جنگ جهانی سوم جنگ سایبری است

در این جنگ جهانی نه از ارتش کلاسیک خبری است نه از تسحیلات مرگبار.

در این جنگ فقط رایانه یا کامپیوتر است و کابل و ایده.

در سال سال های 1397 لغایت 1400 شاهد حمله های دو جانبه بین ایران و ایالات متحده امریکا بودیم.

همچنین خرابکاری هایی در فضای سایبری توسط اشغالگران فلسطین به کشور عزیزمان ایران انجام شد.

که متاسفانه بخشی از آن ها به ثمر رسید و باعث بروز اختلالاتی در فضای اینترانت کشور شد.

مانند کرم رایانه ای استاکس نت که یک ویروس تمام عیار سیاسی محسوب می شود.

از این رو می توان علل وقوع جرایم رایانه ای را به چند دسته تقسیم نمود.

نا اشنایی کاربران با ویژگی های فضای سایبر.

بی توجهی و کم توجهی به امنیت فناوری اطلاعات.

افزایش میزان کاربری رایانه و بهره گیری از شبکه های رایانه ای.

پیچیده تر شدن فعالیتهای متخلفین و مجرمین فضای سایبر.

فقدان قوانین خاص جرم رایانه ای.

فقدان همکاریهای بین المللی در مقابله با جرایم رایانه ای.

نتیجه گیری مقاله امنیت سایبری

هدف ما از این است که بتوانیم برای شبکه ه و محیط های اینترنتی خود امنیت سایبری به وجود بیاوریم و از این جرایم جلوگیری کنیم.

که بهترین را برای جلوگیری از وقوع اکثر جرایم رایانه ای یا غیررایانه ای به آکاهی ما بستگی دارد.

اگر تعداد بیشتری از مردم از اشکال و روش های فعلی جرایم سایبریآگاهی یابند، قربانیان کاهش خواهد یافت.

این آموزش ها می بایست از دوران ابتدای تحصیل در کتاب های درس قرار گیرند.

زیراامروز در سال 2021 میلادی یا 1400 خورشیدی و با توجه به شیوع ویروس کرونا اکثر امور در فضای اینترنت انجام می شود.

از این رو با افزایش گستره استفاده از اینترنت فرصت های مجرمین نیز افزایش پیدا می کند.

امروز پس از گذشت دو سال از شرایط درگیری ویروس کرونا کسب و کارها به استفاده از ارائه خدمات آنلاین بیش از گذشته رو آورده اند.

به طور مثال یک شرکت باغبانی و جابجایی درخت مجبور شده است به جای ارائه خدمات حضوری به غیرحضوری روی اورد و همه کسب و کارها برای خود وب سایت مورد نیاز خود را در پلتفرم های مختلف تهیه نموده اند.

اماکسبه و حتی دانش آموزان آموزش های کمی دیده اند و بعضا در دو سال اخیر شاهد افزایش جرم اینترنتی بوده ایم که هدف اصلی مجرم کسب درآمد بوده است.