

عنوان مقاله:

مفهوم جنگ سایبری و تبیین نقش و کاربرد آن در جنگ های آینده

محل انتشار:

چهارمین کنفرانس ملی پدافند سایبری (سال: 1402)

تعداد صفحات اصل مقاله: 16

نویسندگان:

حسین بیگی - عضو هیئت علمی وابسته، گروه آموزشی حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

آیسان رضائی - دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

نسیمه امیرکار دوست - دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

خلاصه مقاله:

زمینه و هدف تحقیق: جنگ سایبری یکی از این مقوله هاست که در فضای مجازی بین تجهیزات ارتباطی، مخابراتی، شبکه های رایانه ای و سیستم های مبتنی بر رایانه با شدت تمام توسط کشورهای صاحب فناوری بر علیه سایرین در جریان است. پیشرفت روزافزون فناوری اطلاعاتی و گستردگی ابزار و تجهیزات سخت افزاری و نرم افزاری، شکل جدیدی از جنگ را پدید آورده است. مسلما به دلیل اجبار کشورها، ارتش ها در بهره برداری از آخرین دستاوردهای فناوری، شناسایی و ورود به موقع و صحیح در عرصه های نوین به یکی از دغدغه های طراحان و بازیگران حوزه راهبرد و دفاع تبدیل گردیده است. جنگ سایبری، حمله عمدی به زیرساخت های اطلاعاتی دشمن از طریق استفاده از تکنیک های نفوذگری به رایانه ها در عین جلوگیری کامل از انجام اقدامات مشابه از سوی دشمن است. هدف از این تحقیق راهکارهای پیشگیرانه در حوزه جنگ سایبری است که یکی از این راهکارها این است که حوزه سایبری نیازمند تدوین قوانین و اجرای اقدامات پیشگیرانه است. باید دستگاه ها ملزم شوند تا سامانه هایشان پیوست امنیتی داشته باشد. روش تحقیق: در این مطالعه روش توصیفی و تحلیلی است و جمع آوری اطلاعات با استفاده از کتاب ها، مقاله ها و صنایع الکترونیکی و پایگاه های اینترنتی صورت پذیرفته است که در آن به بررسی جنگ سایبری و اجرای اقدامات پیشگیرانه در حوزه سایبری است. یافته ها: اندیشکده مرکز عربی پژوهش و مطالعات سیاسی دوحه در گزارشی راهبردی به بررسی جنگ های مدرن سایبری و ابعاد و پیامدهای آن پرداخت و نوشت: در سال های اخیر طبق یافته های جدید، مفهوم فضای سایبری به مثابه میدان جنگ دچار تحولات چشمگیری شده است که مهم ترین آنها تاثیر مخرب مدنظر دولت ها، گروه ها و افراد از انجام این حملات است. مهم ترین نوع این حمله، هک کردن است که یکی از نگران کننده ترین موارد برای دولت ها و افراد به شمار می رود. ریشه اصلی این نگرانی حضور احزاب مختلف در این مسئله و سخت بودن ردیابی منشا آن است. یکی دیگر از دلایل همچنین به مشخص کردن پایگاه حمله و ارزیابی هزینه تاثیرات آن باز می شود. فضای گسترده وب، اکنون به محلی برای تنش، از جمله جاسوسی، ورود بدون مجوز و کنترل پایگاه های داده ای تبدیل شده که ممکن است امنیت ملی برخی کشورها را تحت الشعاع قرار دهد. به دلیل وقوع چنین پیشرفت هایی بیشتر دولت ها مسئله فضای سایبری را در اولویت خود قرار داده اند و بر بسط سازوکارهای جلوگیری کننده تمرکز نموده اند. نتیجه گیری: نتایج به دست آمده نشان می دهد که فضای سایبری به میدان جنگی جدید تبدیل شده که تهدیدی نو به فهرست تهدیدات متعارف پیش روی جهان امروز اضافه کرده است. بستر تاثیرات این تهدید از مرزهای جغرافیایی و سیاسی فراتر رفته و نکات ضمنی آن در حوزه امنیت ملی کشورها درآینده بسیار مهم است. هکرها اکنون قادرند سرورها را با تقاضاهای مکرر از کار بیندازند و عملکرد آنها را مختل کنند. بسیاری از ارزش های پیشرفته جهان، اقدامات خود را افزایش داده اند و در این زمینه تلاش بیشتری کرده اند. آن ها نقاط ضعف را مشخص کرده مثل برق، آب، حمل و نقل، سامانه دستور و کنتر ...

کلمات کلیدی:

جنگ، سایبر، شبکه، مخابرات، رایانه

لینک ثابت مقاله در پایگاه سیویلیکا:

