مرکز آپا دانشگاه سمنان

خبرنامه الکترونیکی ۷۴

مرکز تخصصی آپا دانشگاه سمنان

در این شماره می‌خوانید:

جنگ سایبری: جبهه جدید درگیری های مدرن

شماره هفتاد و چهار، سال هشتم، اسفند ۱۴۰۴ |کاری از تیم تولید محتوای مرکز تخصصی آپای دانشگاه سمنان

https://cert.semnan.ac.ir info.cert@semnan.ac.ir ۰۲۳-۳۱۵۳۵۰۲۱ @semcert

فهرست

خبر

مرکز آپا دانشگاه سمنان

اخبار امنیت سایبری

کشف آسیب پذیری در سرور eNet SMART HOME

آسیب‌پذیری CVE-۲۰۲۶-۲۶۳۶۹ در سرور eNet SMART HOME نسخه‌های ۲.۲.۱ و ۲.۳.۱ با شدت ۹.۳ به دلیل ضعف در کنترل مجوز (Authorization) در متد setUserGroup از طریق رابط JSON-RPC ایجاد شده است. در این نقص امنیتی، یک کاربر با سطح دسترسی پایین (UG_USER) می‌تواند با ارسال یک درخواست POST دستکاری‌شده به مسیر /jsonrpc/management، گروه کاربری خود را به UG_ADMIN تغییر دهد. این فرآیند بدون انجام بررسی‌های مناسب سطح دسترسی انجام می‌شود. در نتیجه مهاجم می‌تواند به قابلیت‌های مدیریتی کامل دست پیدا کند. این دسترسی شامل تغییر تنظیمات شبکه، مدیریت دستگاه‌های هوشمند، و اعمال تغییرات سیستمی در زیرساخت خانه هوشمند است. بهره‌برداری از این ضعف پیچیدگی فنی بالایی ندارد و می‌تواند منجر به کنترل کامل سامانه شود. با توجه به ماهیت سیستم‌های خانه هوشمند، این آسیب‌پذیری می‌تواند پیامدهای امنیتی و حتی فیزیکی قابل توجهی به همراه داشته باشد.

محصولات تحت تاثیر:

eNet SMART HOME Server

نسخه ۲.۲.۱ و نسخه ۲.۳.۱

سامانه‌هایی که رابط JSON-RPC مدیریت آن‌ها فعال و در دسترس شبکه قرار دارد.

محیط‌هایی که کاربران با سطح UG_USER امکان دسترسی به endpoint /jsonrpc/management را دارند.

توصیه های امنیتی:

به‌روزرسانی فوری نرم‌افزار به نسخه‌ای که وصله امنیتی را دریافت کرده است.

محدودسازی دسترسی شبکه‌ای به endpoint مدیریت (/jsonrpc/management) فقط برای IPهای مورد اعتماد.

فعال‌سازی تفکیک شبکه (Network Segmentation) برای جدا کردن سرور خانه هوشمند از شبکه عمومی یا اینترنت.

اعمال کنترل دسترسی مبتنی بر نقش (RBAC) در سطح سرور و بررسی صحت مجوزها در تمام متدهای JSON-RPC.

غیرفعال‌سازی دسترسی مستقیم مدیریتی از بیرون شبکه داخلی.

بررسی و ممیزی حساب‌های کاربری برای شناسایی هرگونه تغییر غیرمجاز در گروه‌های کاربری.

فعال‌سازی لاگ‌برداری دقیق از درخواست‌های JSON-RPC و پایش رفتارهای مشکوک.

کشف آسیب‌پذیری در افزونه midi-Synth وردپرس

افزونه midi-Synth با استفاده از کتابخانه‌های صوتی امکان ایجاد، ویرایش و پخش فایل‌های MIDI را درسیستم مدیریت محتوی وردپرس فراهم می‌کند. اخیراً آسیب‌پذیری بحرانی با شناسه CVE-۲۰۲۶-۱۳۰۶ و شدت بحرانی با امتیاز ۹.۸ در این افزونه شناسایی شده است. این آسیب‌پذیری از نوع آپلود فایل بدون احراز هویت است و به مهاجم اجازه می‌دهد با استخراج nonce از کد جاوااسکریپت سمت کاربر و ارسال یک درخواست HTTP دلخواه به عملیات export، فایل‌های مخرب خود را روی سرور قربانی آپلود کرده و در شرایط خاص، منجر به اجرای کد از راه دور گردد.

محصولات تحت تاثیر:

نسخه‌ی ۱.۱.۰ افزونه midi-Synth و تمامی نسخه های قبل از آن تحت تأثیر این آسیب‌پذیری قرار دارند.

توصیه های امنیتی:

به‌روزرسانی افزونه midi-Synth به نسخه وصله‌شده (در صورت انتشار) یا حذف و غیرفعال‌سازی کامل آن تا زمان ارائه وصله امنیتی.

کنترل آپلود فایل با استفاده از لیست سفید انواع فایل‌های مجاز، اعتبارسنجی پسوند فایل و بررسی MIME type.

مدیریت دسترسی پوشه آپلود بمنظور جلوگیری از اجرای فایل‌های آپلود شده.

کشف آسیب پذیری ربایش نشست واتساپ ناشی از افشای WebSocket بدون احراز هویت در پل واتساپ Nanobot

آسیب‌پذیری CVE-۲۰۲۶-۲۵۷۷ در مؤلفه WhatsApp bridge نرم‌افزار Nanobot با شدت ۱۰ به دلیل پیکربندی ناامن سرور WebSocket ایجاد شده است. این سرور به‌طور پیش‌فرض روی همه اینترفیس‌های شبکه (۰.۰.۰.۰) اجرا می‌شود و هیچ مکانیزم احراز هویتی برای اتصال‌های ورودی ندارد. در نتیجه، هر مهاجمی که به شبکه دسترسی داشته باشد می‌تواند بدون مجوز به سرور WebSocket متصل شود. پس از اتصال، مهاجم قادر است نشست واتساپ کاربر را در اختیار بگیرد. این موضوع امکان ارسال پیام به نام کاربر، مشاهده پیام‌ها و فایل‌های دریافتی به‌صورت لحظه‌ای، و حتی دریافت کدهای QR احراز هویت را فراهم می‌کند. چنین دسترسی‌ای عملاً کنترل کامل ارتباطات واتساپ را به مهاجم می‌دهد. بهره برداری از این ضعف ساده بوده و فقط به دسترسی شبکه نیاز دارد. در صورت سوءاستفاده، حریم خصوصی و امنیت ارتباطات کاربران به‌شدت به خطر می‌افتد.

محصولات تحت‌تأثیر:

مؤلفه WhatsApp Bridge در نرم‌افزار Nanobot

تمامی استقرارهایی که سرور WebSocket به‌صورت پیش‌فرض روی ۰.۰.۰.۰:۳۰۰۱ اجرا می‌شود و احراز هویت برای اتصال فعال نیست.

محیط‌هایی که پل واتساپ از شبکه داخلی یا اینترنت قابل دسترسی مستقیم است.

توصیه های امنیتی:

محدودسازی دسترسی شبکه‌ای به پورت ۳۰۰۱ فقط برای میزبان‌های مورد اعتماد (Firewall / ACL).

فعال‌سازی احراز هویت برای اتصال WebSocket یا استفاده از توکن‌های دسترسی امن.

Bind کردن سرویس فقط روی localhost یا شبکه داخلی امن به‌جای ۰.۰.۰.۰.

استفاده از Reverse Proxy امن همراه با TLS و کنترل دسترسی.

جداسازی شبکه (Network Segmentation) برای جلوگیری از دسترسی مستقیم خارجی.

بازنشانی نشست واتساپ و اسکن فعالیت‌ها در صورت احتمال سوءاستفاده.

به‌روزرسانی نرم‌افزار به نسخه‌ای که تنظیمات امن‌تری برای WebSocket اعمال می‌کند.

کشف آسیب‌پذیری در Tenable Security Center

اخیرا یک آسیب‌پذیری با شناسه CVE-۲۰۲۶-۲۶۳۰ و امتیاز ۸.۸ در ابزار Tenable Security Center شناسایی شده است. این ابزار بمنظور جمع‌آوری و تحلیل اسکن‌های امنیتی، مدیریت اسکنرهای Nessus و ارائه داشبوردهای جامع امنیتی در سازمان‌ها مورد استفاده قرار میگیرد و به‌عنوان هسته مرکزی پایش امنیت شبکه عمل می‌کند. این نقص به مهاجم احراز هویت شده امکان می‌دهد تا دستورات دلخواه خود را روی سرور اجرا کرده و کنترل کامل سامانه را به دست گیرد.

محصولات تحت تاثیر:

Tenable Security Center نسخه های ۶.۵.۱ ، ۶.۶.۰ و ۶.۷.۲ تحت تاثیر این آسیب پذیری قرار دارند.

برای این نسخه‌ها اصلاحیه‌های مستقل با شناسه‌های SC-۲۰۲۶۰۲.۱ و SC-۲۰۲۶۰۲.۲ منتشر شده است .

توصیه های امنیتی:

نسخه‌های آسیب‌پذیر (۶.۵.۱، ۶.۶.۰ و ۶.۷.۲) به آخرین نسخه‌های منتشر شده همراه با اصلاحیه‌های امنیتی SC-۲۰۲۶۰۲.۱ و SC-۲۰۲۶۰۲.۲ ارتقاء یابند.

Tenable Security Center باید تنها از شبکه‌های داخلی ایمن و سیستم‌های مجاز در دسترس باشد و دسترسی از اینترنت یا شبکه‌های غیرقابل اعتماد مسدود شود.

قبل از اعمال اصلاحیه‌ها و تغییرات پیکربندی، نسخه پشتیبان از داده‌ها و تنظیمات سامانه گرفته شود تا در صورت بروز مشکل، امکان بازگردانی وجود داشته باشد.

Acronis Cyber Protect

کشف آسیب‌پذیری در Acronis Cyber Protect ۱۵, ۱۶

Acronis Cyber Protect یک راهکار یکپارچه حفاظت از داده و امنیت سایبری است که قابلیت‌هایی مانند پشتیبان‌گیری، بازیابی اطلاعات، محافظت در برابر باج‌افزار، مدیریت نقاط پایانی و پایش امنیتی سیستم‌ها را در محیط‌های Windows و Linux فراهم می‌کند. این سامانه معمولاً در زیرساخت‌های سازمانی برای حفاظت از داده‌های حیاتی و مدیریت متمرکز امنیت مورد استفاده قرار می‌گیرد و دارای دسترسی به اطلاعات حساس و تنظیمات سیستمی است. اخیراً سه آسیب پذیری بحرانی با شناسه‌های CVE-۲۰۲۵-۳۰۴۱۲، CVE-۲۰۲۵-۳۰۴۱۱ و CVE-۲۰۲۵-۳۰۴۱۶ با شدت ۱۰ در این سامانه شناسایی شده است که ناشی از ضعف در مکانیزم‌های احراز هویت و کنترل مجوز دسترسی هستند. این نواقص می توانند به مهاجم اجازه دهند بدون طی فرآیندهای مجاز امنیتی، به داده‌های حساس دسترسی پیدا کرده و آن‌ها را تغییر دهد.

محصولات تحت تاثیر:

آسیب‌پذیری‌های فوق نسخه‌های زیر را تحت تأثیر قرار می‌دهند:

Acronis Cyber Protect ۱۶ (Linux / Windows) نسخه های قبل از Build ۳۹۹۳۸

Acronis Cyber Protect ۱۵ (Linux / Windows) نسخه های قبل از Build ۴۱۸۰۰

توصیه های امنیتی:

بروزرسانی سامانه به آخرین نسخه‌های ارائه‌شده توسط Acronis.

محدودسازی دسترسی به کنسول مدیریتی تنها از طریق شبکه داخلی یا VPN امن.

استفاده از احراز هویت دومرحله‌ای برای حساب‌های مدیریتی.

جداسازی شبکه مدیریت پشتیبانگیری از شبکه کاربران عادی.t

کشف آسیب پذیری در .NET Remoting. نرم‌افزار DocLink

آسیب‌پذیری CVE-۲۰۲۶-۲۶۲۲۲ در نرم‌افزار Altec DocLink با شدت ۱۰ ناشی از در معرض بودن سرویس‌های .NET Remoting. بدون احراز هویت است. این سرویس از طریق ObjectURI مشخصی در دسترس قرار دارد و درخواست‌های دریافتی را بدون اعتبارسنجی مناسب پردازش می‌کند. به دلیل وجود مشکل در دیسریال‌سازی ناامن (Unsafe Deserialization)، مهاجم از راه دور می‌تواند اشیای مخرب ارسال کند. این موضوع امکان خواندن فایل‌های دلخواه از سیستم، نوشتن فایل در مسیرهای حساس و حتی اجبار سیستم به ارسال احراز هویت SMB را فراهم می‌کند. در صورتی که مسیرهای قابل نوشتن در دسترس وب‌سرور IIS باشند، مهاجم می‌تواند به اجرای کد از راه دور (RCE) دست پیدا کند. همچنین بازنویسی فایل‌های سیستمی می‌تواند باعث اختلال در سرویس یا از کارافتادن کامل آن شود. از آنجا که این نقص بدون نیاز به احراز هویت قابل بهره‌برداری است، سطح ریسک آن بسیار بالا ارزیابی می‌شود. اصلاح پیکربندی و به روزرسانی نسخه آسیب‌پذیر برای جلوگیری از سوءاستفاده ضروری است.

محصولات تحت تاثیر:

Altec DocLink (در حال حاضر تحت نگهداری Beyond Limits Inc.)

نسخه مشخص‌شده آسیب‌پذیر: ۴.۰.۳۳۶.۰

سرویس درگیر: Altec.RDCHostService.exe

Endpoint آسیب‌پذیر: .NET Remoting با ObjectURI به نام doclinkServer.soap

استقرارهایی که سرویس را روی TCP یا HTTP/SOAP در دسترس شبکه (به‌ویژه اینترنت) قرار داده‌اند

محیط‌هایی که DocLink را پشت Microsoft IIS اجرا می‌کنند و مسیرهای قابل‌نوشتن وب دارند

توصیه های امنیتی:

به‌روزرسانی فوری به نسخه اصلاح‌شده (در صورت انتشار Patch رسمی از سوی Beyond Limits)

غیرفعال‌سازی یا محدودسازی دسترسی به .NET Remoting. در صورت عدم نیاز

اعمال احراز هویت و کنترل دسترسی شبکه (ACL / Firewall) برای محدود کردن دسترسی به پورت‌های مربوطه

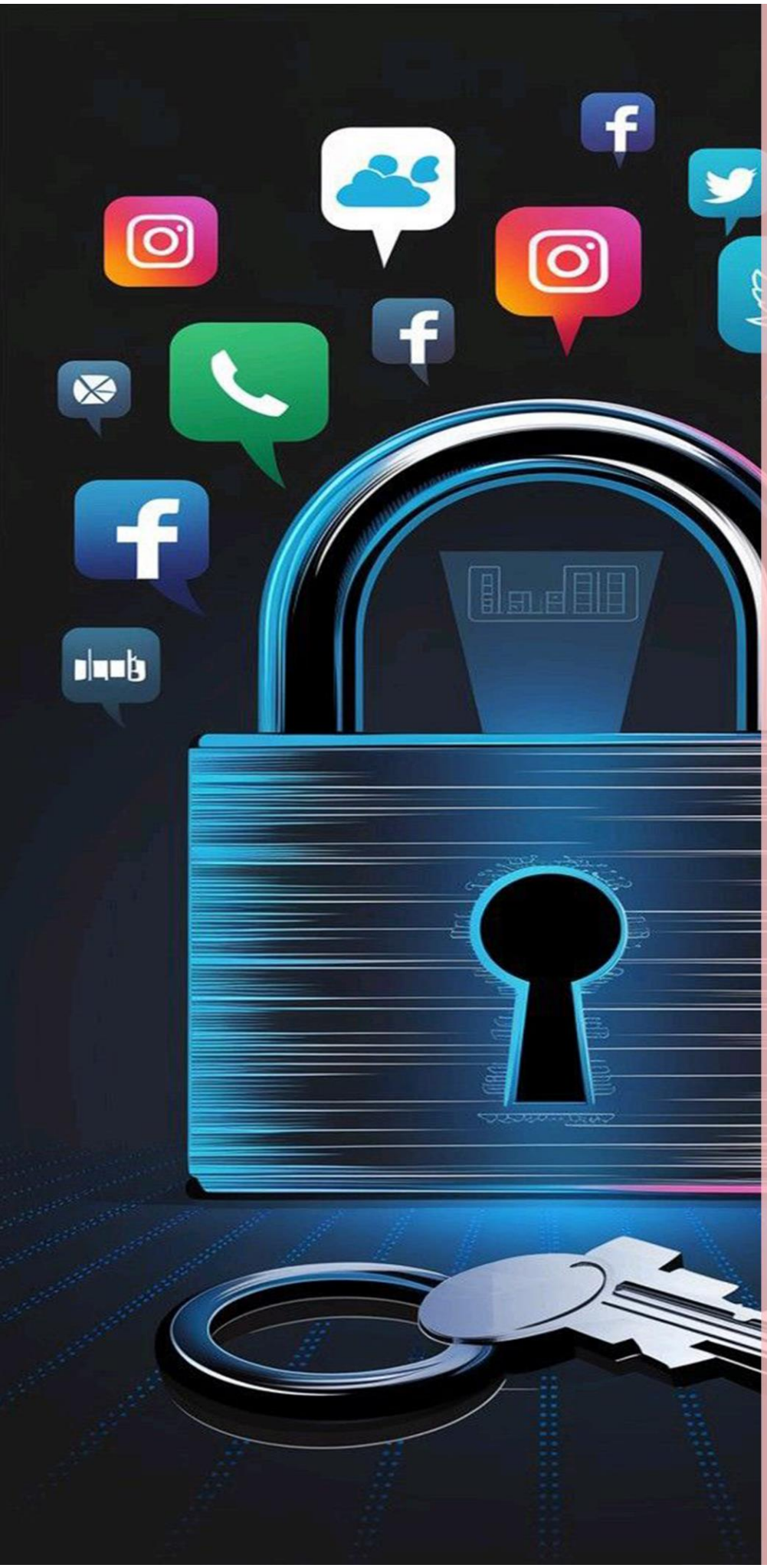
جلوگیری از دسترسی عمومی به پورت‌های Remoting (مانند ۸۹۰۰ یا پورت‌های سفارشی مشابه)

اجرای سرویس با حداقل سطح دسترسی (Least Privilege)

مسدودسازی مسیرهای UNC خروجی برای جلوگیری از SMB Coercion

مانیتورینگ لاگ‌ها برای شناسایی درخواست‌های SOAP یا Remoting مشکوک

اطمینان از اینکه مسیرهای قابل‌نوشتن تحت IIS قابلیت اجرای فایل (execute permission) نداشته باشند.



مرکز آپا دانشگاه سمنان

جنگ سایبری

جنگ سایبری: جبهه جدید درگیری های مدرن

مقدمه

در دنیای امروز، درگیری ها دیگر محدود به مرزهای جغرافیایی و میدان های نبرد سنتی نیستند. یک جبهه جدید و حیاتی در حال گسترش است: جنگ سایبری. این حملات که اغلب نامرئی و ناشناس باقی می مانند، میتوانند تأثیراتی به مراتب گسترده تر و عمیق تر از درگیری های نظامی کلاسیک داشته باشند. این تحلیل به بررسی اهمیت فزاینده جنگ سایبری، چالش های آن و نقش پیشبینی شده اش در آینده درگیری ها می پردازد.

اهمیت فزاینده جنگ سایبری:

تعریف: جنگ سایبری به استفاده از حملات دیجیتال علیه دشمنان (کشورها، سازمان ها یا افراد) برای کسب مزیت استراتژیک اطلاق میشود. این حملات میتوانند شامل نفوذ به سیستم ها، اختلال در عملکرد آنها، سرقت اطلاعات، یا انتشار اطلاعات نادرست باشند .

چرا مهم است؟ در عصر دیجیتال، وابستگی شدید جوامع به زیرساخت های فناوری اطلاعات و ارتباطات، جنگ سایبری رابه ابزاری قدرتمند تبدیل کرده است. اختلال در این زیرساخت ها می تواند منجر به فلج شدن ا قتصاد، خدمات عمومی، و حتی توان دفاعی یک کشور شود.

تأثیرگذاری همتراز با حملات نظامی:

زیرساخت های حیاتی: حملات سایبری میتوانند شبکه های برق، سیستم های تأمین آب، شبکه های حمل و نقل، سیستمهای بانکی، و زیرساخت های ارتباطی را هدف قرار دهند. اختلال در هر یک از این حوزه ها می تواند پیامدهای فاجعه باری داشته باشد .

مثال: قطع گسترده برق در یک منطقه، اختلال در سیستم های مالی، از کار افتادن ارتباطات اضطراری .

هزینه و ریسک: در مقایسه با حملات نظامی سنتی، حملات سایبری اغلب هزینه کمتری دارند و ریسک شناسایی مستقیم و پاسخ نظامی متقابل کمتری را به همراه دارند. این موضوع، جذابیت آن را برای مهاجمان افزایش می دهد.

جنگ سایبری: جبهه جدید درگیری های مدرن

چالش های شناسایی و مقابله:

ابهام در منشأ: یکی از بزرگترین چالش ها، دشواری ردیابی دقیق منشأ حملات سایبری است. مهاجمان می توانند از تکنیک های پیچیده ای برای پنهان کردن هویت و موقعیت خود استفاده کنند(مانند استفاده از پراکسی ها، شبکه های ناشناس، یا سرورهای واسطه).

مسئولیت پذیری: تعیین مسئولیت یک حمله سایبری میتواند بسیار دشوار باشد. این ابهام، امکان پاسخگویی و ایجاد بازدارندگی را پیچیده میکند .

سرعت تحولات: حوزه سایبری دائماً در حال تغییر است. تهدیدات جدید به سرعت ظهور می کنند و فناوری های دفاعی باید همگام با آنها به روز شوند، که این امر نیازمند سرمایه گذاری مداوم و نیروی انسانی متخصص است.

نقش جنگ سایبری در درگیری های آینده:

جبهه جدایی ناپذیر: پیشبینی میشود که جنگ سایبری به بخشی جدایی ناپذیر از هرگونه درگیری نظامی در آینده تبدیل شود. کشورها و گروه ها به طور فزایندهای از قابلیت های سایبری خود برای تضعیف دشمن، جمع آوری اطلاعات، و پیشبرداهداف استراتژیک استفاده خواهند کرد .

جنگ اطلاعاتی و روانی: جنگ سایبری اغلب با جنگ اطلاعاتی و روانی همراه است. انتشار اخبار جعلی، دستکاری افکارعمومی، و ایجاد بی ثباتی اجتماعی، اهداف رایجی هستند که از طریق کانال های دیجیتال دنبال میشوند .

بازدارندگی سایبری: توسعه و حفظ قابلیت های دفاع سایبری قوی، به یک عنصر کلیدی در استراتژی های بازدارندگی ملی تبدیل خواهد شد.

نتیجه‌گیری:

جنگ سایبری دیگر یک مفهوم تئوریک نیست، بلکه واقعیتی انکارناپذیر در عرصه ژئوپلیتیک و امنیت بین الملل است. درک پیچیدگی ها، چالش ها، و پتانسیل این نوع جنگ، برای دولت ها، سازمان ها و حتی افراد، امری حیاتی است تا بتوانند در برابر تهدیدات احتمالی خود را محافظت کنند و از منافع خود در این عرصه نامرئی دفاع نمایند.

ما را در تلگرام دنبال کنید :

@semcert