# چالش‌های بین‌المللی امنیت فضای سایبری

دویچ، کرتیلا، ایوانکو[1]
مترجم: محمد تقوی نژاد[2]

فصلنامه علمی –تخصصی دانش انتظامی کهگیلویه و بویر احمد
سال دهم، شماره سوم(پیاپی ۲۸)، پاییز ۱۳۹۶
از صفحه ۵۳ تا ۶۶
تاریخ دریافت: ۱۳۹۶/۰۴/۰۹
تاریخ پذیرش: ۱۳۹۶/۰۷/۲۸

**چکیده**

فرصت‌هایی که فناوری اطلاعات و ارتباطات با تأکید ویژه‌ای بر اینترنت خلق کرده، تبدیل به یک بخش جدایی‌ناپذیر از زندگی شده است. با این حال، آیا ما به عنوان افراد، ملل یا جامعه بین‌المللی به اندازه کافی آگاه و آماده برای روبرو شدن با تهدیداتی که از فضای مجازی می‌آیند ازجمله تهدیدات تجاری و حتی جنگی آن هستیم؟ یعنی، باوجود تعداد روزافزون کاربران، اینترنت هنوز دارای کمترین قوانین مقررات است. در مورد فضای سایبری مسائل امنیتی وجود دارد که نمایانگر یک خط امنیتی است و همین مسئله عصر جدید را به چالش می‌کشد. توسعه و کاربرد فناوری اطلاعات و ارتباطات یک میدان جنگ جدید ایجاد کرده است. تروریسم سایبری به عنوان یک چالش جدی برای امنیت بین‌المللی ظهور کرده است. امنیت سایبری به‌طور قابل‌توجهی بر روابط بین‌الملل در قرن بیست و یکم تأثیر خواهد گذاشت. این مقاله خلاصه‌ای از مفاهیم و اصول تهدیدات سایبری را ارائه می‌دهد که بر ایمنی و امنیت یک بافت بین‌المللی تأثیر می‌گذارد.

**کلید واژه‌ها**

فضای سایبری، حمله سایبری، تروریسم سایبری و جرم و جنایت، امنیت بین‌المللی.

---

[1] عضو هیئت علمی دانشکده علوم انسانی، زاگرب، کرواسی
کارشناسی ارشد مطالعات ترجمه، دانشگاه اصفهان Mohammad.taghavi15@yahoo.com

**مقدمه**

جنگ سایبری و تروریسم حدومرزی نمی‌شناسند. مواجهه و اقدام علیه فضای سایبری مستلزم رد پیش‌فرض‌های معمول مربوط به زمان و فضا است، زیرا چنین حملاتی با استفاده از شبکه‌های اطلاعاتی و ارتباطات مدرن می‌تواند از هر نقطه در یک زمان بسیار کوتاه انجام شود. فرایندهای جهانی شدن بر روی دستاوردهای تمدن تأثیری نداشت، ولی بر توسعه تهدیدات جدید برای تمدن تأثیر گذاشت. واقعیت این است که تروریسم و تهدیدات ملی تحت تأثیر فرایند جهانی سازی و انقلاب اطلاعات اینترنت تغییریافته است. مزیت استراتژیک دیگر در قدرت مبارزه یا موقعیت جغرافیایی نیست بلکه در اطلاعات و دانش است. همکاری بین‌المللی و به اشتراک گذاری اطلاعات برای جلوگیری از تهدیدات سایبری ضروری است. باوجود اینکه تهدیدات اینترنتی در سال‌های اخیر به‌طور خاص در آموزه‌های نظامی مدرن قدرت‌های بزرگ و ناتو به‌طور خاص مورد تأکید قرارگرفته است، هنوز هم در قالب محرمانه قرار دارند.

هدف از این مقاله توجه کردن به تهدیدات اینترنتی است که امنیت کشورهای مدرن، سازمان‌ها و روابط بین‌الملل را تهدید می‌کند. این مقاله در نظر دارد فضای سایبری را از لحاظ چالش‌های امنیتی به عنوان بعدی که در آن روابط بین‌المللی گسترش می‌یابد، نشان دهد. لازم است موضوعات اصلی محیط بین‌المللی امنیت سایبر را تشخیص دهیم، اهدافشان را تجزیه و تحلیل کنیم و یک پارادایم چندوجهی فضای سایبری را تعیین کنیم و خاص بودن و اصول آن را تحلیل کنیم.

مفهوم استراتژیک ناتو که در پایان سال ۲۰۱۰ در نشست لیسبون تصویب شد، تعیین می‌کند که حملات سایبری بیشتر، سازمان‌یافته‌تر و هزینه‌بر شده‌اند و سبب آسیب به دولت، تجارت، اقتصاد و به‌طور بالقوه به حمل‌ونقل می‌شود. همچنین اظهار می‌شود که حملات سایبری می‌توانند به سطحی برسند که امنیت، ثبات و رونق ملی و یورو-آتلانتیک را به خطر بیندازند. سرویس‌های نظامی و اطلاعاتی خارجی، جنایتکاران سازمان‌یافته، تروریست‌ها و گروه‌های افراطی منشأ و منبع بالقوه چنین حملاتی هستند. همچنین درنتیجه نشست لیسبون تأکید شد که لازم است مهارت‌های پیشگیری، تشخیص، دفاع و بازیابی اطلاعات از حملات سایبری توسعه داده شوند. این امر با

استفاده از فرآیند برنامه‌ریزی ناتو برای پیشرفت و هماهنگی توانایی‌های ملی حفاظت سایبری محقق می‌شود. جمع‌آوری تمام سازمان‌های ناتو تحت حفاظت سایبری متمرکز و یکپارچه‌سازی بهتر از آگاهی‌های سایبری، هشدارها و پاسخ‌های مشترک کشورهای عضو بوده است.

باید توجه داشت که سرعت توسعه و پذیرش تکنولوژی ها از طریق استفاده از آن‌ها در زندگی روزمره فرصت‌های فراوانی برای مهاجمان ایجاد می‌کند. این مهاجمان در شکل‌های دولت‌ها، تروریست‌ها و جنایتکاران هستند زیرا آن‌ها همیشه در فضای سایبری به دنبال منافع خود هستند؛ بنابراین می‌توان نتیجه گرفت که مفهوم جدیدی از امنیت سایبری که در آن پیشگیری بخشی مهم است ایجادشده است.

فرض اولیه این است که فضای سایبری یک خطر امنیتی و چالش رو به رشد است. علاوه بر این، امنیت سایبری در قرن بیست و یکم به‌طور قابل‌توجهی بر روابط بین‌الملل تأثیر خواهد گذاشت، در حالی که تهدیدات و چالش‌ها به‌طور چشمگیری افزایش می‌یابد.

هدف این مقاله، تلفیق و تجزیه و تحلیل دانش مبتنی بر مرور مقاله‌های اخیر و مقالات تخصصی و علمی است که چالش‌های امنیتی بین‌المللی در فضای سایبری را بررسی می‌کنند. پژوهش علمی تلاش می‌کند فضای سایبری را به عنوان ابزاری عملی از روابط بین‌المللی از نظر چالش‌های امنیتی سایبری نشان دهد. با ساماندهی کردن استراتژی جنگ سایبری و روش‌های متنوع حمله مرتبط با اقدام برنامه‌ریزی‌شده از طریق استفاده از تکنیک‌ها، محاسبات و سیستم‌های شبکه‌ای تنظیم می‌شود.

## امنیت سایبری بین‌المللی

دامنه سایبری تأثیر زیادی بر تحول امنیت بین‌المللی و مفهوم امنیت دارد. بسیاری از نویسندگان ضرورت درک صحیح و ایجاد دکترین سایبری را مهم می‌پندارند.

بعد جدید سایبری روابط بین‌الملل یک چالش عمده برای نظریه‌های حفظ قدرت و ارعاب است. تهدیدات سایبری جدی، بی‌ثبات و در حال افزایش است. نظریه‌ها و استراتژی‌های ارعاب که در طول جنگ سرد طراحی‌شده و اجرا می‌شد نمی‌توانند در عرصه سایبری اجرا شوند. بسیاری از دانشمندان بر روی درک انقلاب سایبری در روابط

بین‌المللی کار می‌کنند. مقامات همچنین گام‌های خاصی را در همکاری، بخصوص در زمینه جرم و ایجاد CERT (تیم واکنش اضطراری رایانه‌ای) برداشته‌اند. تاتالویچ، گریزاند و کرتیلا اظهار داشتند که فرایندهای بین‌المللی سازی و جهانی سازی انسجام و تلاش بیشتری برای تنظیم یکپارچه نظم جهانی را به ارمغان آورده است. این در هسته سیاست‌های امنیتی ایالات‌متحده منعکس‌شده است. در این زمینه، یک مفهوم جدید - مفهوم امنیت انسان - در تئوری و عمل سیاسی پدیدار شد. برخلاف مفهوم سنتی امنیت ملی که در درجه اول بر امنیت یک فرد تأکید دارد و نه دولت. لین درباره امنیت سایبری نظریه‌ای ارائه کرده است. در نظریه وی مفهوم ارعاب، ایده اصلی استراتژی هسته‌ای است. با این حال، سؤال این است که آیا اصول ارعاب در فضای سایبری یک استراتژی قابل‌قبول است؟ باوجود اینکه سلاح‌های هسته‌ای و سایبری دارای یک ویژگی کلیدی مشترک هستند - برتر بودن حمله در مقایسه با دفاع - اما آن‌ها از بسیاری جهات متفاوت هستند. فقط چند کشور دارای سلاح‌های هسته‌ای هستند و شمار دشمنان احتمالی محدود است، همان‌گونه که در آن، تهدید ارعاب نیز مورداستفاده قرار می‌گیرد. وضعیت در فضای سایبری کاملاً متفاوت است. برخلاف سلاح‌های هسته‌ای، هر دولتی به سلاح‌های سایبری دسترسی دارد و چنین حملاتی نمی‌توانند قویاً با اقدامات دولت مرتبط باشند. حفاظت از زیرساخت‌های ملی علیه حمله می‌تواند یکی دیگر از منافع مشترک دولت‌ها باشد. کارشناسان و تحلیلگران برآورد می‌کنند که تلاش‌های روسیه و چین برای تسلط بر فضای مجازی طی چند سال گذشته بسیار زیاد شده است از این‌رو هرگونه تأخیر و عقب‌ماندگی در این حوزه می‌تواند به مشکل بزرگی برای غرب مدرن تبدیل شود.

حملات سایبری، هرچند که به عنوان یک چالش بین دولت‌ها، یک اقدام تروریستی یا یک حرکت جنایتکارانه رخ می‌دهد. حمله سایبری اینگونه تعریف می‌شود؛ حمله به فضای سایبری با هدف به خطر انداختن یک سیستم یا شبکه کامپیوتری و حتی به خطر انداختن سیستم‌های فیزیکی که بهترین مثال آن ویروس استاکس نت است. در اصطلاح عمومی که اغلب در رسانه‌ها استفاده می‌شود، از آن به عنوان حمله هکری نامبرده می‌شود. روش‌های مشابه حمله هکری برای اهداف نظامی و تروریستی مورداستفاده قرار می‌گیرد.

جانسزوسکی و کولاریک حملات سایبری را به چند فاز تقسیم کرده‌اند که از نظر آن‌ها اساساً همان فازهای جرائم متداول جنایی است:

• فاز اول این حمله، کشف قربانیان بالقوه است. با مشاهده فعالیت‌های معمول اهداف، اطلاعات مفیدی در مورد آن‌ها جمع‌آوری شده که از طریق برنامه‌های کاربردی و سخت‌افزاری مشخص می‌شوند؛

فاز دوم حمله نفوذ است. زمانی که مهاجم به سیستم وارد می‌شود، کار زیادی علیه هدف نمی‌تواند انجام دهد فقط می‌تواند در دسترسی به سرویس‌های خاصی که توسط هدف ارائه‌شده اختلال ایجاد کند؛

فاز بعدی شناسایی و انتشار فرصت‌های داخلی با بررسی منابع و حق دسترسی به بخش‌های محدود و مهم سیستم است؛

• در فاز چهارم مزاحم (هکر) به سیستم آسیب می‌رساند یا اطلاعات خاصی را سرقت می‌کند.

علاوه بر این، آن‌ها نشان می‌دهند که امروزه حملات سایبری عمدتاً شامل موارد زیر است:

• بدافزار از طریق پیوست ها در مرورگر اینترنت، ایمیل یا سایر آسیب‌پذیری‌های سیستم

حمله منع سرویس (DoS) به منظور جلوگیری استفاده از سیستم‌های کامپیوتری و شبکه‌ها؛

• حذف یا انتقال؛ (گذاشتن یک پیام) به دولت و وب‌سایت‌های تجاری برای تبلیغات اهداف یا به منظور ایجاد اختلال در اطلاع‌رسانی؛

• نفوذ غیرمجاز به سیستم: برای سرقت اطلاعات محرمانه و / یا اختصاصی، به خطر انداختن اطلاعات و یا استفاده از سیستم برای شروع حمله به سایر سیستم‌ها.

در چنین شرایطی از دگرگونی و دیدگاه‌های مختلف و درک امنیت و امنیت بین‌المللی به صورت کلی، تهدیدات سایبری این اصطلاحات را از نو تعریف می‌کنند. در راستای

تلاش برای تضمین امنیت از یک‌سو و ویژگی‌های تهدیدات سایبری و انگیزه‌های هکران از سوی دیگر، لازم است که یک پارادایم جدید امنیتی بین‌المللی در عصر سایبری را ایجاد کنیم.

چندوجهی فضای سایبری

ایالات‌متحده، روسیه و چین کشورهایی هستند که به خاطر واحدهای سایبری نظامی ماهرشان معروف هستند. فرانسه و اسرائیل علاوه بر دولت‌های مذکور درحال‌توسعه قابلیت‌های سایبری خود هستند. افسران اطلاعاتی آمریکا بر این باورند که ۲۰ تا ۳۰ ارتش جهان ازجمله تایوان، ایران، استرالیا، کره جنوبی، هند، پاکستان و چندین کشور عضو ناتو داری توانایی‌های بالقوه برای جنگ سایبری هستند. فرماندهی سایبری ایالات‌متحده، همراه با آژانس‌هایی که با آن‌ها کار می‌کنند، از باهوش‌ترین و وطن‌پرست‌ترین افراد نظامی غیرنظامی برخورداری هستند که این افراد برنامه‌ها و توانایی‌های خود را برای سلطه در فضای مجازی با هدف حفظ امنیت ملی و صلح پی‌ریزی می‌کنند.

تسلط استراتژیک بر فضای مجازی هنوز توسط هیچ یک از نهاد های بین‌المللی محقق نشده است. بدون شک هدف بسیاری از کشورها مانند ایالات‌متحده آمریکا، چین و روسیه سلطه بر فضای سایبری است. با این حال، همان قدر که بر روی سیستم دفاعی و توان تهاجمی خود سرمایه‌گذاری می‌کنند، نتوانستند سیستم به عنوان قدرت جهانی ایجاد کنند. همان‌طور که در مقابل تقسیم بلوک جهان به دو مرکز قدرت در طول جنگ سرد ایستادند، ارعاب بر اساس توان تهاجمی در فضای سایبری خیلی مهم نیست چون‌که مراکز قدرت زیادی در آن وجود دارد. قدرت آن ملت‌ها بیشتر به امکان ایجاد یک سیستم دفاع دائمی بستگی دارد که آن‌هم تحت تأثیر وابستگی آن‌ها به زیرساخت‌های اطلاعاتی است. وابستگی به زیرساخت‌های اطلاعاتی با سطح آسیب‌پذیری کشورهای دیجیتالی توسعه‌یافته اقتصادی و نظامی مرتبط است.

با توجه به خصوصیت فضای سایبری، به ویژه عدم تقارن با زمان و فضا واقعی و عوامل ژئواستراتژیک، یک چالش امنیتی جدید که نیازمند مفاهیم نظامی جدید است پیش روی دولت‌ها و سازمان‌ها قرارگرفته است. به ویژه ضروری است علاوه بر تدوین دکترین

دفاعی مخصوص، طرح‌های تهاجمی برای مقابله با اقدامات در فضای سایبری نیز تدوین شود.

وابستگی به شبکه‌های رایانه‌ای و ارتباطات کامپیوتری ایالات‌متحده را در مقابل حمله‌های احتمالی آسیب‌پذیر می‌کند که این دنیای سایبری را تبدیل به منبع عظیمی از شک و تردید می‌کند. آسیب‌پذیری نسبت به حملات و امکان مقابله توسط کلارک و نیکاک به عنوان قدرت سایبری ملی تعریف شده است. بر طبق گفته آن‌ها قدرت سایبری ملی، برآورد خالص توانایی یک کشور برای هزینه در یک جنگ سایبری است . قدرت ملی سایبری سه عامل را در نظر می‌گیرد: قابلیت‌های تهاجمی سایبری، وابستگی ملی به شبکه‌های سایبری و توانایی کشور برای کنترل و دفاع از فضای سایبری خود، با اجرای اقداماتی مانند توقف ترافیک در خارج از کشور. بر اساس این سه عامل، نویسندگان یک ارزیابی کلی از قدرت سایبری ایالات‌متحده، روسیه، چین، ایران و کره شمالی تدوین کردند. برای تسهیل مقایسه و تحلیل، نتایج ارزیابی در جدول زیر دسته‌بندی شدند. مقیاس اندازه‌گیری از ۱ تا ۱۰ است، ارزش کوچک‌تر نشان‌دهنده ارزیابی بدتر و ارزش بالاتر است که نشان‌دهنده ارزیابی بهتر است.

**جدول ۱: ارزیابی قدرت سایبری کشورها**

| کشور | ایالات‌متحده آمریکا | روسیه | چین | ایران | کره شمالی |
|---|---|---|---|---|---|
| قدرت تهاجمی | ۸ | ۷ | ۵ | ۴ | ۲ |
| وابستگی به شبکه‌های سایبری | ۲ | ۵ | ۴ | ۵ | ۹ |
| قدرت دفاعی | ۱ | ۴ | ۶ | ۳ | ۷ |

آن‌ها بیشتر توضیح می‌دهند که چرا ایالات‌متحده، بر اساس ارزیابی انجام شده، قدرت برتر فضای سایبری نیست. اگر کل قدرت سایبری ملی تنها بر اساس توانایی‌های تهاجمی سنجیده شود، ایالات‌متحده آمریکا در جایگاه اول است. با این حال، نتیجه یک جنگ سایبری تنها به توانایی‌های تهاجمی بستگی ندارد. بخش مهم وابستگی یک ملت به سیستم‌ها در فضای سایبری است. برخلاف ایالات‌متحده آمریکا، چین درحال‌توسعه قابلیت‌های سایبری تهاجمی خود است، اما بر دفاع نیز متمرکز است. جنگجویان سایبری ارتش چین هر دو وظیفه تهاجمی و دفاعی در فضای مجازی را بر عهده دارند و در مقایسه با ارتش آمریکا هنگام صحبت در مورد دفاع، آن‌ها نه تنها به دفاع از شبکه‌های نظامی کشور می‌پردازند بلکه به دفاع از شبکه‌های غیرنظامی نیز می‌پردازند. در چین، شبکه‌هایی که زیرساخت اینترنت را تشکیل می‌دهند، تحت کنترل دولت هستند. دولت چین دارای قدرت و ابزاری است که می‌تواند بخش چینی اینترنت را از بقیه جهان خاموش کند که احتمالاً در صورت وقوع درگیری با ایالات‌متحده این اتفاق به وقوع خواهد پیوست. از سوی دیگر، ایالات‌متحده هیچ برنامه یا ظرفیتی برای انجام این کار ندارد، زیرا ارتباطات سایبری آن‌ها عمدتاً خصوصی است. چین می‌تواند است استفاده از فضای مجازی را در مواقع بحرانی محدود کند و از دسترسی کاربران خاصی جلوگیری کند. ولی ایالات‌متحده آمریکا قادر به انجام چنین کاری نیست. از لحاظ دفاع و وابستگی کم به زیرساخت شبکه کره شمالی بالاترین امتیاز را می‌گیرد؛ به عبارت دیگر، این کشور می‌تواند اتصالات محدود خود به فضای سایبری را آسان‌تر و مؤثرتر از چین از بین ببرد. کره شمالی سیستم‌های کمی دارد که وابسته به فضای سایبری هستند که حتی یک حمله سایبری وسیع به آن سیستم‌ها تأثیر چندانی بر آن‌ها ندارد. نویسندگان هشدار می‌دهند که باید در نظر داشته باشیم که وابستگی سایبری به معنی اینکه چند درصد از خانواده‌ها از اینترنت استفاده می‌کنند و یا تعداد افرادی که از گوشی‌های هوشمند استفاده می‌کنند نیست بلکه وابستگی سایبری یعنی میزانی که زیرساخت‌های حیاتی مثل (برق، راه‌آهن و زنجیره‌های عرضه و تقاضا) وابسته به سیستم‌های شبکه هستند. به این ترتیب، یک دولت که تا حد زیادی وابسته به سیستم‌های فضای سایبری است، چالش‌های بیشتری در ایجاد یک دفاع ملی سایبری

دارد. به همین دلیل است که ایالات‌متحده آمریکا در ارتباط با جنگ سایبری آسیب‌پذیرتر از روسیه و چین است. مطمئناً خطر جنگ سایبری برای آمریکا بسیار بیشتر از خطر آن برای کشوری کوچک مانند کره شمالی است. سه نهاد بزرگ دارای روابط بین‌الملل (ایالات‌متحده آمریکا، چین و روسیه) و تعادل قدرت در فضای سایبری، همه‌ی قدرت سایبری دو کشور که به خاطر توتالیتاریسم و مشکلات هسته‌ای تهدیدی برای جهان هستند، مورد تجزیه و تحلیل قرارگرفته است. کلارک و نیکاک تخمین می‌زنند که آن‌ها توان تهاجمی زیادی ندارند، اما در سوءاستفاده از فضای سایبری شرکت دارند.

به خاطر برنامه‌های هسته‌ای، ایران در ماه ژوئن ۲۰۱۰ هدف حمله کرم کامپیوتری به نام استاکسنت قرار گرفت. این کرم برای آلوده ساختن سیستم‌های صنعتی ساخته شد و ثابت شد قدرت خرابکاری در برنامه هسته‌ای ایران را داراست. علاوه بر برنامه هسته‌ای ایران، ویروس استاکسنت هزاران کامپیوتر و تجهیزات صنعتی را در سراسر جهان آلوده کرده است. کرم استاکسنت می‌تواند در فضای سایبری برای مدت طولانی پنهان شود. تحلیلگران اعلام کردند که ویروس پیچیده استاکسنت به‌طور خاص برای نفوذ و کنترل سیستم‌های کامپیوتری تأسیسات هسته‌ای نطنز در ایران طراحی‌شده بود. این ویروس در فضای سایبری برای مدت طولانی به‌خوبی از خود مراقبت می‌کند. کارشناسان استاکسنت را به عنوان یک قطعه پیچیده نرم‌افزاری با نیم میلیون خط کد توصیف می‌کنند. برای چنین نرم‌افزارهای مخرب پیچیده‌ای، لازم است که دانش و اطلاعاتی از انواع خاصی از سیستم‌های کنترل صنعتی استفاده شود که موردحمله قرار می‌گیرند داشته باشیم و به نظر می‌رسد که کد توسط یک تیم متخصص و نه تنها یک نفر نوشته‌شده است؛ بنابراین، یک‌سوء ظن وجود دارد که توسط برنامه نویسان آمریکایی یا اسرائیلی انجام شده است. در مقاله‌ای که در نیویورک تایمز منتشر شد، سنجر می‌نویسد که رئیس‌جمهور آمریکا اوباما دستور حمله سایبری به ایران (حمله به سانتریفیوژهای مورداستفاده برای غنی‌سازی اورانیوم) را داده است.

کره شمالی با توجه به پیشرفت تکنولوژیکی ضعیف آن، به سیستم‌های فضای مجازی زیاد وابسته نیست؛ و به دلیل این عدم وابستگی ارزیابی توانایی‌های دفاعی آن‌ها بسیار خوب است. اگرچه توانایی‌های تهاجمی پیشرفته‌ای ندارند، ولی واضح است که نقش

فعال و مهمی در فضای مجازی بازی می‌کنند. در واقع، در جولای ۲۰۰۹ چندین وب‌سایت آمریکایی، ازجمله وب‌سایت کاخ سفید، تحت حمله DDoS (انکار سرویس) قرار گرفتند. مظنون کره شمالی بود. این وضعیت پس از حمله به کره جنوبی تائید شد. رسانه‌های کره جنوبی و مقامات دولتی آشکارا همسایه شمالی خود را متهم کرده‌اند و مقامات ایالات‌متحده به منظور ارسال یک پیام قوی و محکم» از یک حمله سایبری تلافی‌جویانه حمایت می‌کنند. در نوامبر ۲۰۱۴ گروهی که خود را GOP یا سربازان صلح می‌نامیدند، شرکت «سونی پیکچرز» را هک کرده و اطلاعاتی از قبیل اطلاعات شخصی کارکنان و خانواده‌هایشان، ایمیل‌های بین کارکنان، اطلاعات در مورد حقوق مدیران در شرکت، کپی از فیلم‌های منتشرنشده سونی و سایر اطلاعات را سرقت کردند. هدف از حمله که به کره شمالی نسبت داده شد این بود که سونی را از انتشار یک فیلم که (به درستی) در آن رهبر کره شمالی به تمسخر گرفته شده و تصویرسازی رژیم کره شمالی و رهبر آن، کیم جونگ اون با طعنه و تمسخر صورت گرفته بود، منع کند.

## نتیجه‌گیری

موضوع مقاله، یعنی چالش‌های بین‌المللی امنیت سایبری، به‌وضوح یک عنوان جالب و چالش‌انگیز در حوزه‌ی تحقیق است. از دلایل مهم برای اثبات این ادعا این است که این حوزه تا به حال به اندازه کافی مورد بررسی قرار نگرفته است، به خصوص در کشور کرواسی با توجه به توسعه فزاینده روابط بین‌الملل در فضای مجازی، مطابق با سرعت توسعه فن‌آوری‌ها و اجرای آن‌ها در روابط دولت‌ها، سازمان‌ها و افراد، این حوزه همیشه جالب و چالش‌برانگیز خواهد بود. این نتیجه‌گیری از تغییر دائمی نگرش‌ها و تکنولوژی ها حاصل می‌شود. این دقیقاً همان بی‌ثباتی است که نشان می‌دهد که از این رشته تخصصی، بین‌رشته‌ای، در یک دوره ۵ یا ۱۰ ساله محتمل است نتیجه‌های جدیدی را به دست آید و بر اساس آن پارادایم‌ها و دکترین جدیدی شکل گیرد. کار می‌گوید که جنگ سایبری در حدود یک دهه آغازشده، اما هنوز به‌خوبی مشخص نیست. هیچ توافقنامه بین‌المللی معتبر وجود ندارد که تعریف قانونی از عمل تجاوز سایبری ارائه کند. در واقع، کل حوزه قانون سایبری بین‌المللی هنوز مبهم است. توسعه و در دسترس بودن فن‌آوری‌های اطلاعاتی و ارتباطاتی و تنش‌های موجود در بین دولت‌های مختلف سیاسی و ایدئولوژیک، روابط بین‌المللی را در فضای مجازی را تحت تأثیر قرار داده است.

هنوز هیچ کشوری نتوانسته بر فضای سایبری بین‌المللی سلطه استراتژیک داشته باشد. تعداد زیادی از نهادهای بین‌المللی حضور و تمایل خود را فعالیت برای در فضای مجازی نشان دادند. این نشان می‌دهد که فضای سایبری یک بعد چند قطبی است که بسیار بعید است سلطه یا تقسیم بلوک در آن رخ دهد. دلایل این امر در عدم اعتماد متقابل و ترس از جاسوسی در ارتباط با سیستم‌های دفاعی است. با این حال، کشورهایی که دارای بیشترین نفوذ هستند آنهایی اند که از بیشترین قدرت اقتصادی و نظامی برخوردار هستند و در عین حال بیشترین وابسته به زیرساخت‌های سایبری را دارند مثل آمریکا، روسیه و چین. ناتو نیز نقش مهمی ایفا می‌کند. می‌توانیم نتیجه‌گیری کنیم که در سال‌های اخیر، مفهوم جدید امنیت سایبری را می‌توان به عنوان یک پارادایم چندضلعی فضای سایبر تعریف کرد. اکثر نویسندگان افزایش چالش‌ها و فعالیت‌های جاسوسی در فضای مجازی را پیش‌بینی می‌کنند که فرضیه اولیه این مقاله را تائید پشتیبانی می‌کند. آن‌ها اظهار می‌کنند که حملات سایبری یکی از بزرگ‌ترین تهدیدات امنیتی بین‌المللی است. برخلاف تعارض متعارف، چنین حملاتی به‌طور فزاینده‌ای شایع می‌شوند و آن‌ها به عنوان یک حمله متعارف، ی توانند باعث انهدام در مقیاس بزرگ، حتی با عواقب مرگبار شوند؛ بنابراین ضروری است که یک دفاع مؤثر ایجاد شود که در آن نقش کلیدی پیشگیری، همکاری بین‌المللی و پذیرش استانداردهای بین‌المللی شناخته شده و قانونی است. با توجه به افزایش تروریسم و جرائم اینترنتی، ضروری است آموزش‌های سیستماتیک و نیروی نظامی، اطلاعاتی و مراکز مدنی برای دفاع از حملات سایبری ساماندهی شود. اگر تمام اظهارت گفته شده در متن و تائید فرضیه ابتدایی را در نظر بگیریم، می‌توان نتیجه گرفت که امنیت سایبری به یکی از پیش‌نیازهای مفهوم دموکراتیک زندگی در جامعه مدرن تبدیل‌شده است.

**منابع**

[۱]NATO, “Strategic concept for the defence and security of the members of North Atlantic Treaty Organization,” 2010, Available: http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (3.2.2017.)

[2] N. Choucri and D. Goldsmith, “Lost in cyberspace: harnessing the Internet, international relations, and global security,” Bulletin of the Atomic Scientists, vol. 68, no. 2, 2012, pp. 70-77.

[3] S. Tatalović, A. Grizold, and V. Cvrtila, Suvremene sigurnosne politike. Zagreb: Golden marketing-Tehnička knjiga, 2008.

[4] H. Lin, “A virtual necessity: some modest steps toward greater cybersecurity,” Bulletin of the Atomic Scientists, vol. 68, no. 5, 2012, pp. 75-87.

[5] L. J. Janczewski and A. M. Colarik, Cyber warfare and cyber terrorism. Hershey: Information Science Reference, 2008.

[6] J. S. Nye, “Cyber war and peace,” 2012, Available: http://www.project-syndicate.org/commentary/cyber-war-andpeace (3.2.2017.)

[7] J. Carr, Inside cyber warfare, 1st ed. Sebastopol, CA: O’Reilly Media, 2010.

[8] R. A. Clarke and R. K. Knake, Cyber war: the next threat to national security and what to do about it. New York: Ecco, 2010.

[9] Risk Based Security, “A Breakdown and Analysis of the Sony Hack,“ 2014, Available: https://www.riskbasedsecurity.com/2014/12/a-breakdown-andanalysis-of-the-december-2014-sony-hack/#thebeginning (9.4.2017.)

[10] G. Siboni and D. Siman-Tov, “Cyberspace Extortion: North Korea versus the United States, “ INSS Insight No. 646, 2014, Available: http://www.inss.org.il/uploadImages/systemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf (9.4.2017.)

[11] M. Petrović, “Obrana od cyber-napada”, Hrvatski vojnik, vol. 9, no. 385, 2012, pp. 26-29. [12] D. E. Sanger, “Obama order sped up wave of cyberattacks against Iran,” The New York Times, 2012, Available: www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html?pagewanted=1 (3.2.2017.)