Archive of SID

فصلنامه امنیت ملی
سال نهم، شماره ۳۳، پاییز ۱۳۹۸
مقاله یازدهم از صفحه ۲۷۳ الی ۳۱٤

# مقاله پژوهشی: ارائه الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملّی جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری

مهراب رامک[۱]، محمدرضا ولوی[۲] و محمدرضا حسینی[۳]

**تاریخ دریافت: ۱۳۹۷/۷/۸** **تاریخ پذیرش: ۱۳۹۷/۹/۲۰**

**چکیده**

فضای مجازی کشور، فضایی متشکل از شبکه‌های ارتباطی است که در آن، محتوا و خدمات مفید، در چارچوب مبانی و ارزش‌های اسلامی و قوانین و مقررات کشور ارائه می‌شود و علی‌رغم محاسن بسیار، با ایجاد بستری برای وقوع جرائم سایبری، مخاطراتی را برای امنیت فضای مجازی و به‌تبع آن منافع ملی کشور، به دنبال دارد که پیگرد آن‌ها، نیازمند همکاری مراجع قانونی و پلیس سایبری همه کشورهای تحت تأثیر است (به دلیل ماهیت فرامرزی).

نظر به فقدان الگوی راهبردی مشخص در این خصوص، پژوهش توسعه‌ای- کاربردی حاضر با هدف دستیابی به الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملّی جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری به روش موردی- زمینه‌ای (با رویکرد آمیخته)، ضمن جمع‌آوری و مطالعه مبانی نظری مرتبط، مفاهیم قابل توجه (داده‌های کیفی) را به روش نظریه‌پردازی داده بنیاد (گراندد تئوری) توسط نرم‌افزار مکس‌کیودا، کدگذاری و مقوله‌سازی نموده (ابعاد، مؤلفه‌ها و شاخص‌ها) و مدل مفهومی پژوهش را ترسیم می‌نماید و سپس با مدل‌سازی معادلات ساختاری مربوطه در نرم‌افزار اسمارت پی.ال.اس و استخراج ٤ فرضیه اصلی و ۱۰ فرضیه فرعی جهت ارزیابی، خبره سنجی مدل را به روش گلوله برفی توسط پرسشنامه، از اعضاء هیئت‌علمی، مدیران عملیاتی و مدیران راهبردی آشنا به حوزه پژوهش (جامعه آماری) انجام و با تجزیه و تحلیل داده‌های کمی حاصل، برازش کلی مدل را قوی ارزیابی نمود.

نتایج پژوهش نشان داد که ۱۲ فرضیه مورد تأیید، ۲ فرضیه رد و شاخص‌های جهانی امنیت فضای مجازی (توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت‌های دولتی و خصوصی، مشارکت‌های بین‌المللی) نیز ابزارهای کارآمدی برای ارتقاء امنیت فضای مجازی است

**کلیدواژه‌ها**: الگوی راهبردی، همکاری بین‌المللی، ارتقاء امنیت فضای مجازی، منافع ملی جمهوری اسلامی ایران، مبارزه با جرائم سایبری

۱. دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبری، دانشگاه عالی دفاع ملی (نویسنده مسئول)- *M. Ramak@sndu.ac.ir*
۲. دانشیار دانشگاه صنعتی مالک اشتر
۳. استادیار دانشگاه عالی دفاع ملی

www.SID.ir

Archive of SID



**مقدمه:**

پیشرفت‌های نوین در عصر اطلاعات و توسعه فعالیت جوامع بشری در بستر فضای مجازی، سبب روبرو شدن دولت‌ها با پدیده‌های مجرمانه بین‌المللی جرائم سایبری شد و دولت‌ها در مواجهه با خطرات ناشی از جرائم دارای اثر فراملی، معیارهایی را تعیین کردند تا با اتکا بر آن‌ها، صلاحیت دادگاه‌های ملّی خود را به جرائم فراملی توسعه داده و امکان تعقیب در سطح بین‌المللی مرتکبان را فراهم آورند. امروزه، مجرم یا مجرمین سایبری از یک کشور، می‌توانند با کمترین هزینه امنیت یک یا چند کشور را در کمتر از یک ساعت به مخاطره اندازند.[1] لذا برقراری امنیت سایبری در نظام بین‌الملل، بدون تعامل و همکاری مطلوب کشورها در مبارزه با جرائم سایبری امکان‌پذیر نخواهد بود (بلدی، ۱۳۹۰) .

در سال ۲۰۰۰ کنوانسیون امنیت سایبری و محافظت از اطلاعات شخصی اتحادیه آفریقا با هدف ایجاد هماهنگی در قوانین مرتبط با امنیت سایبری و مبارزه با نقض حریم خصوصی (جمع‌آوری، پردازش، انتقال، ذخیره‌سازی داده‌های شخصی) تشکیل و قوانین کیفری مبارزه با جرائم سایبری، امنیت شبکه‌های رایانه‌ای و توسعه جامعه اطلاعاتی در آفریقا را مورد توجه قرار داد و دستورالعمل‌های گسترده‌ای ارائه و در سال ۲۰۱۲، قانون سایبری آفریقا را مشتمل بر چهار فصل معاملات الکترونیکی، حفاظت از اطلاعات شخصی، ارتقاء امنیت سایبری و مبارزه با جرائم سایبری و مقررات نهایی مصوب نمود و در ماده ۲۸، همکاری بین‌المللی را لازمه تحقق امنیت سایبری دانسته و چهار شاخص هماهنگی، کمک حقوقی متقابل، تبادل اطلاعات و ابزار همکاری را برای آن تعیین کرد (***AFRICAN UNION,*** ۲۰۱٤) .

نخستین معاهده‌ای که به جرائم سایبری پرداخت و همکاری بین‌المللی را بهبود بخشید نیز کنوانسیون جرائم سایبری بوداپست بود (۲۰۰۱) که با هدف دنبال نمودن یک سیاست رایج کیفری جهت حفاظت از جامعه در برابر جرائم سایبری، از طریق اتخاذ قوانین مناسب و گسترش همکاری‌های بین‌المللی توسط شورای اروپا تشکیل شد[2] و ضمن مدنظر قرار دادن جرائم دسترسی غیرقانونی، ره‌گیری غیرقانونی، ایجاد اختلال در اطلاعات، ایجاد اختلال در سیستم، سوءاستفاده از

---

۱- در سال ۲۰۱۷، باج افزار *WannaCry* توانست در ظرف چند ساعت بیش از ۱۰۰ کشور را آلوده و دچار مشکل کند.

۲- کنوانسیون جرائم سایبری در دانشنامه آزاد ویکی‌پدیا، ۱۹ فوریه ۲۰۱۵.

www.SID.ir

Archive of SID



دستگاه‌ها، جعل اسناد مرتبط با رایانه، کلاهبرداری مرتبط با رایانه، هرزه‌نگاری کودکان، کپی‌رایت و تروریسم سایبری، کشورهای عضو را به اتخاذ راه‌کارهایی جهت حفظ و ارتقاء امنیت و مبارزه با جرائم در فضای مجازی، ملزم نمود.

در سند چشم‌انداز جمهوری اسلامی ایران در افق ۱٤۰٤ هجری شمسی بر تعامل سازنده و متوازن در روابط بین‌الملل و در سیاست‌های کلی نظام در فضای تولید و تبادل اطلاعات کشور، بر ارتقای سطح همکاری‌های بین‌المللی در زمینه امنیت فضای مجازی تأکید شده است و این موضوع بیانگر ضرورت پرداختن به همکاری‌های بین‌المللی در حوزه سایبری است. لذا پژوهش حاضر، با هدف دستیابی به الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملّی جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری به مطالعه مبانی نظری مرتبط پرداخته و با استخراج ابعاد، مؤلفه‌ها و شاخص‌های قابل توجه با استفاده از روش نظریه‌پردازی داده بنیاد در نرم‌افزار مکس‌کیودا[1] (تحلیل کیفی)، مدل مفهومی پژوهش را ترسیم می‌نماید و با مدل‌سازی معادلات ساختاری مربوطه به روش حداقل مربعات جزئی (***PLS***) در نرم‌افزار اسمارت پی.ال.اس[2] (تحلیل کمی)، ٤ فرضیه اصلی و ۱۰ فرضیه فرعی را استخراج و مورد ارزیابی قرار می‌دهد و در نهایت، با ساختاربندی کلیه عوامل احصاء شده و برقراری روابط بین آن‌ها طبق حلقه تصمیم‌گیری «اودا-***OODA***» با چهار فاز، مشاهده، جهت‌دهی، تصمیم‌گیری و اقدام، الگوی راهبردی مورد نظر را طراحی و ارائه می‌نماید.

فضای مجازی کشور، فضایی متشکل از شبکه‌های ارتباطی است که در آن محتوا و خدمات مفید، در چارچوب مبانی و ارزش‌های اسلامی و قوانین و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی (از قبیل سن، جنس، شغل و تحصیلات) از محتوا و خدمات مورد نیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بمانند[3] و بر همین اساس نیز اکثر سرویس‌ها و خدمات خصوصی و دولتی از قبیل بانک، شهرداری، راهنمایی و رانندگی، قضایی و غیره در فضای مجازی کشور ارائه شده است که علاوه بر محاسن

---

۱- MaxQda ۲۰۱۸ (نرم افزار قدرتمند جهت تحلیل کیفی داده ها به روش‌های مختلف از جمله گراندد تئوری)

۲-SmartPLS V ۳.۰

۳- طرح جامع توسعه فضای مجازی سالم، مفید و ایمن که مرکز ملّی فضای مجازی کشور، در تاریخ ۱۳۹۳/۱۲/۱۰ تصویب نمود.

www.SID.ir

Archive of SID



بسیار زیاد، بستری را برای بروز جرائم سایبری با ماهیت فرامرزی مهیا نموده است که غالباً با همکاری نزدیک مجرمین در موقعیت‌های مختلف جغرافیایی صورت می‌گیرند و اگر مجرمان در کشورهای دیگر مستقر باشند، پیگرد این‌گونه جرائم با حمایت مراجع قانونی و همکاری پلیس همه کشورهای تحت تأثیر امکان‌پذیر خواهد بود و نظام همکاری قانونی دوطرفه مرسوم نیز ناکارآمد است (ممکن است که جرم فوق، دریکی از کشورهای درگیر، جرم محسوب نشود). از طرف دیگر، برقراری امنیت (سه عنصر پایه محرمانگی، یکپارچگی و در دسترس بودن) در فضای مجازی، کار بسیار دشواری است؛ زیرا از آن می‌توان به‌عنوان ابزاری متعارف برای حمله به تشکیلات دولتی، نهادهای مالی، زیرساخت‌های انرژی و حمل‌ونقل ملی و روحیه عمومی استفاده نمود. لذا ناامنی در فضای سایبری، صرفاً شامل ناامنی در سیستم‌های اطلاعاتی نیست؛ بلکه تمام زیرساخت‌هایی که به نحوی با فناوری اطلاعات در ارتباطند در برمی‌گیرد (همانند حمله سایبری به کشور توسط ویروس استاکس نت در سال ۲۰۱۰).

فضای مجازی، با توجه به ویژگی‌های ژئوپلیتیک همانند مدیریت و کنترل، هویت، همگرایی و همکاری، رقابت و ستیز، شکاف توسعه، تولید قدرت و حاکمیت ملی، می‌تواند در فرآیند رقابت بازیگران سیاسی و حکومت‌ها و نقش‌آفرینی در تولید قدرت و مناسبات آن در سیستم‌های جهانی و منطقه‌ای به کار گرفته شود. لذا تعامل و همکاری مطلوب و شایسته همه کشورها، در مبارزه با جرائم و ارتقاء امنیت سایبری می‌تواند اثربخش باشد؛ اما عواملی همچون تعارض قوانین داخلی کشورها، نبود نظام حقوقی منسجم جهانی برای مقابله با جرائم سایبری فراملی، حاکمیت مطلق آمریکا بر اینترنت و وابستگی زیرساخت‌های اصلی کشورها به چند کشور محدود، شرایطی را فراهم نموده است که اکثر کشورها و سازمان‌های بین‌المللی، باوجود اقدامات ارزشمند و مؤثر خود در مقابله با جرائم سایبری، موفقیت لازم را نداشته باشند.

به‌عنوان‌مثال، کنوانسیون جرائم سایبری بوداپست توسط اتحادیه اروپا در سال ۲۰۰۱ با هدف سازگار نمودن روش‌ها و ارتقاء همکاری بین‌المللی تشکیل شد و برخی از کشورها به آن پیوستند ولی در مقابل، بسیاری دیگر نیز آن را نپذیرفتند. طبق ماده ۳۲ کنوانسیون فوق، دسترسی فرامرزی به داده رایانه‌ای ذخیره شده در کشورهای عضو، باید در اختیار سایر اعضاء قرار گیرد تا بدون اخذ مجوز به آن‌ها دسترسی داشته باشند و این خواسته، منافع ملی کشور را مستقیماً مورد هدف قرار می‌دهد. لذا جمهوری اسلامی ایران نیز عضویت در کنوانسیون فوق را نپذیرفته است.

www.SID.ir

Archive of SID



با توجه به مطالب فوق‌الذکر، وقوع مداوم جرائم سایبری با ماهیت فراملی و اجتناب‌ناپذیر بودن تأثیر آن‌ها بر منافع ملی کشور (وحدت ملی، امنیت ملی و قدرت ملی)، همکاری بین‌المللی جهت مبارزه با جرائم (در راستای ارتقاء امنیت فضای مجازی کشور) را ایجاب می‌نماید که هنوز در جهان شکل نگرفته است و این مسئله را می‌توان، در عدم وجود الگوی راهبردی مشخص در این خصوص دانست که پژوهش حاضر به حل این مسئله خواهد پرداخت.

اهمیت و ضرورت پژوهش: پژوهش حاضر از این بابت حائز اهمیت است که اجرای آن می‌تواند فواید و پیامدهای مثبتی را در راستای تحقق اهداف سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) به دنبال داشته باشد:

- شناسایی منافع ملی جمهوری اسلامی ایران در فضای مجازی و روش‌های محافظت از آن‌ها.
- احصاء عوامل اثرگذار در همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی.
- احصاء عوامل اثرگذار در همکاری‌های بین‌المللی با رویکرد مبارزه با جرائم سایبری.
- شناسایی کنوانسیون‌ها و قوانین بین‌المللی در حوزه سایبر.

از سوی دیگر جرائم سایبری و سوءاستفاده‌های اقتصادی، فرهنگی، اجتماعی، سیاسی و غیره از فضای مجازی کشور در حال گسترش است و با کاهش اعتماد عمومی به فضای مجازی، اختلال جدی در کسب‌وکار کشور ایجاد خواهد شد و این امر نیز، موجبات آسیب‌پذیری زیرساخت‌های مهم، حساس و حیاتی کشور را فراهم می‌نماید و با پیشرفت فناوری نیز، مبارزه با آن‌ها روزبه‌روز دشوارتر خواهد شد. لذا ضرورت دارد پژوهش‌هایی در این خصوص صورت گیرد تا از عواقب و پیامدهای منفی آن‌ها پیشگیری شود.

سؤال‌های پژوهش: پژوهش با هدف اصلی پاسخگویی به این سؤال است که «الگوی راهبردی همکاری‌های بین‌المللی (ابعاد، مؤلفه‌ها و شاخص‌ها) برای ارتقاء امنیت فضای مجازی بر اساس منافع جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری چگونه است؟» انجام و سؤالات فرعی ذیل را نیز مورد توجه قرار می‌دهد.

- شاخص‌های منافع ملّی جمهوری اسلامی ایران چیست؟
- ابعاد و مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری چیست؟
- شاخص‌های بین‌المللی ارتقاء امنیت فضای مجازی چیست؟

www.SID.ir

Archive of SID



- تأثیر شاخص‌های بین‌المللی ارتقاء امنیت فضای مجازی بر مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری، چگونه است؟

**مبانی نظری:**

به‌منظور پاسخگویی به سؤالات لازم است که ابتدا با مطالعه مفاهیم کلیدی پژوهش و استخراج ابعاد، مؤلفه‌ها و شاخص‌های قابل توجه، مدل مفهومی پژوهش ترسیم گردد.

الگوی راهبردی: الگو، چارچوبی کلی شامل جنبه مفهومی (مفاهیمی که واقعیت متغیرها را به محقق نشان می‌دهد)، عنصر تئوری (مجموعه‌ای از سازه‌ها، مفاهیم و قضایای مرتبط جهت تشخیص، پیش‌بینی و تبیین روابط بین متغیرها) و قواعد تفسیری (سلسله قواعدی برای توصیف پدیده‌ها) است که زمینه مناسبی را برای طبقه‌بندی اطلاعات و سامان‌دهی آن‌ها فراهم می‌آورد (دیاری بیدگلی، ۱۳۹۳) و راهبرد، طرح، نقشه و دیدگاه‌هایی شامل تصمیمات محوری، دورنمایی جهت نگاه منسجم به جهان با تجهیز و به‌کارگیری نیروها و توانایی‌ها در جهت دستیابی به هدفی معین است. لذا الگوی راهبردی را می‌توان الگوی منسجمی دانست که با تنظیم منطقی عوامل و مؤلفه‌های اصلی راهبردی، روابط بین آن‌ها را به بهترین شکل ممکن ترسیم نموده و چگونگی دستیابی به اهداف را میسر سازد (حمیصی، ۱۳۹۱: ١٦) . به‌عبارت دیگر الگوی راهبردی، نمایشی از یک سیستم یا ایده به شکلی غیر از خود پدیده است که به نحوه کاربرد امکانات بالقوه و بالفعل در جهت رسیدن به اهداف راهبردی در سطح ملّی و با توجه به شرایط داخلی و خارجی کشور، اشاره دارد (کرم نیا، ۱۳۹۱: ١٦) .

منافع ملّی جمهوری اسلامی ایران: منافع ملّی[۱] مرکّب از کلمه «منافع» به معنای سود و «ملّی»، منسوب به ملّت است (روشندل، ١٣٩٤: ۳۳) . طبق اصل نهم قانون اساسی، «در جمهوری اسلامی ایران، آزادی و استقلال و وحدت و تمامیت اراضی کشور از یکدیگر تفکیک ناپذیرند و حفظ آن‌ها وظیفه دولت و آحاد ملت است». منافع ملّی، دستیابی به انرژی، منابع معدنی، فناوری جدید، توسعه اقتصادی، دفاع از اتباع خود در خارج از مرزها و غیره را نیز شامل شده (همان: ۳۸) و به منافع بنیادی، حیاتی، مهم و حاشیه‌ای[۲] (مرادیان، ۱۳۸۵: ۹۳) و در نگاهی جامع‌تر، به شش گروه منافع اولیه (منافع بنیادین و منافع حیاتی) ، منافع ثانویه (منافع مهم و منافع حاشیه‌ای) ، منافع

۱ -National interest

۲-FUNDEMENTAL INTERSTS & Vital INTERSTS & Important INTERSTS & Marginal INTERSTS

www.SID.ir

Archive of SID



پایدار، منافع متغیر، منافع مشترک و منافع خاص قابل دسته‌بندی است (شاه‌محمدی، ۱۳۹۲: ۱۷۹) و البته، تغییرات اجتماعی دهه‌های آینده، مدلی ترکیبی از راهبردها، متناسب با موقعیت‌های محیطی بوده و نقش «ولی‌فقیه و زعیم عالی نظام اسلامی» در تغییرات مطلوب اجتماعی، تأمین‌کننده حداکثر اهداف و منافع ملی جمهوری اسلامی ایران خواهد بود (عیوضی، ۱۳۹۳) . از نگاهی دیگر، هر یک از نقش‌های ملی جمهوری اسلامی، ارزش‌ها و منافع خاصی را ایجاد و ایجاب می‌کند که می‌تواند عناصر و ارکان منافع ملی را تشکیل دهد که در چهار دسته کلی منافع دفاعی- امنیتی، منافع بین‌المللی، منافع ایدئولوژیک و منافع اقتصادی قابل تقسیم‌بندی است (سلطانی‌فر، ۱۳۹۱: ۲۰۸) .

همکاری بین‌المللی: همکاری یک فرآیند مشارکت‌جویانه است که از طریق کار با یکدیگر و برای دستیابی به اهداف مورد نظر شکل‌گرفته و سبب اشتراک چشم‌انداز، دستیابی به نتایج مثبت برای مخاطبان و ساختن یک سیستم وابسته جهت پرداختن به مسائل و فرصت‌ها می‌شود و در واقع، فضای حمایتی جهت حل سامانمند مسائلی که حل آن‌ها به‌تنهایی توسط طرفین میسر نباشد، ایجاد می‌نماید. شکل‌گیری یک همکاری موفق درگرو عوامل متعدد ساختاری، محیطی و رفتاری است که مهم‌ترین آن‌ها می‌توان هدف، شرایط محیطی، ارتباطات، ویژگی اعضاء، ساختار و فرآیند و منابع برشمرد[1] (بهمنی، ۱۳۹۳: ٦٧) . از دیدگاه اسلام، همکاری کشورهای مسلمان و غیرمسلمان باید بر مبنای نگاه تکریم آمیز به انسان‌ها، همزیستی مسالمت‌آمیز، نفی اساس خشونت، پایبندی به اصول اخلاقی و عهد، گفتگو، مقابله‌به‌مثل و تجهیز قوا با هدف بازدارندگی شکل گیرد (علیخانی، ۱۳۹۰: ۱۳) .

حضرت امام خمینی (ره)، ویژگی اخلاق، حفظ صلح و امنیت بین‌المللی، عدم تجاوز به خاک کشورها، حسن هم‌جواری با همسایگان و همکاری با دولت‌ها بر مبنای احترام متقابل (غفرانی، ۱۳۹۱: ۲) و مقام معظم رهبری (مدظله‌العالی) ، انطباق با جهان‌بینی توحیدی و آموزه‌های اسلامی، تعاملات انسانی در سطح فردی، جمعی و جهانی[2] را برای همکاری بین‌المللی، برشمرده‌اند.

دولت‌ها در حقوق بین‌الملل و فضای مجازی ملّی و بین‌المللی، نقش دارند (***Wrange,*** ۲۰۱۳) و به‌منظور تأمین منافع آن‌ها، در کنوانسیون جرائم سایبری (ماده ۲۳) تأکید شده است که همکاری

---

۱- کارول لوکاس و ربکا اندریوز، با بررسی سوابق ۵۰ همکاری، عوامل مؤثر در همکاری شناسایی و در شش گروه دسته بندی و در مقاله‌ای تحت عنوان «*Four Keys to Collaboration Success*» منتشر کردند.

۲- دیدار با دانش‌آموزان و دانشجویان در آستانه سیزده آبان و روز ملی مبارزه با استکبار جهانی ۱۳۷۵/۸/۹

www.SID.ir

Archive of SID



بین‌المللی باید بر اساس توافقنامه‌های بین‌المللی در موضوعات کیفری و قانون‌گذاری متحدالشکل دوجانبه یا چندجانبه و قوانین داخلی انجام شود و تمامی جرائم مرتبط با رایانه و جمع‌آوری ادله الکترونیک را در برگیرد. البته باید توجه داشت که، دیپلماسی[۱] حاکم بر جامعه اطلاعاتی در قرن ۲۱، تحت تأثیر ویژگی ژئوپلیتیک فضای مجازی همچون مدیریت و کنترل، هویت، همگرایی و همکاری، رقابت و ستیز، شکاف توسعه، تولید قدرت، حاکمیتی ملی فضای مجازی (حافظنیا، ۱۳۹۰: ٤) قرار خواهد داشت (***Abeyagoonasekera & Ranasinghe,*** ۲۰۱۲) .

امنیت فضای مجازی (امنیت سایبری): جرائم سایبری، به شبکه‌ها، افراد و خانواده‌ها در زندگی آنلاین، آسیب می‌رساند ولی امنیت سایبری، از شبکه‌های دولتی و جهانی در مقابل هکرهایی که قصد بهره‌برداری از آسیب‌پذیری آن‌ها را دارند، محافظت می‌کنند ( ***Roderick S. Graham,*** ۲۰۱۷). حکومت‌ها تمامی تلاش خود را به کار می‌گیرند تا امنیت ملی کشور را برای عموم مردم فراهم ساخته و به پشتوانه آن، استقلال و تمامیت ارضی کشور را حفظ کنند (کوچی، ۱۳۹۳: ۱۳٦) لذا یکی از مصادیق مهم منافع ملّی را می‌توان حفظ امنیت فضای مجازی برشمرد (تقوی، ۱۳۹٤) .

امنیت در پارادایم فضای مجازی تابع دو عنصر کلیدی انسان (ویژگی‌ها و قابلیت‌هایش) و فضای سایبر (قابلیت‌ها و مبانی شکل‌گیری فضای سایبری) است و کنش و تعامل کنشگران این دو عامل، با ایجاد فضای تهدیدزا، ابعاد گسترده و متنوعی را در حوزه امنیت شکل می‌دهد ( ***Dutton,*** ۲۰۱۷**)**. امنیت سایبری، به‌تنهایی برای محافظت در مقابل تهدیدات سایبری مدرن کافی نیست بلکه نیازمند یک سیستم مدیریت امنیت اطلاعات[۲] بر مبنای سه رکن اساسی مردم، فرآیندها و تکنولوژی، به‌منظور تأمین سه عنصر اصلی امنیت است (محرمانگی[۳]، یکپارچگی[٤] و دسترس‌پذیری[۵]) (***Thriveni & Prashanth,*** ۲۰۱٤:۳) .

---

۱- دیپلماسی هنر مذاکره کردن است. دیپلمات کسی است که بتواند منافع ملی کشورش را در شرایط مختلف از جمله جنگ، مراودات اقتصادی، موضوعات فرهنگی، اختلافات منطقه‌ای و... از طریق گفتگو و مذاکره تأمین کند.

۲- ISMS (Information Security Management System): سیستم مدیریت امنیت اطلاعات

۳- محتوای داده‌های تبادل‌شده در فضای مجازی نباید توسط افراد غیر مجاز خوانده شود (Confidentaility).

٤- محتوا و داده‌های باید یکپارچه تبادل شوند تا امکان دستکاری شده و تغییر آنها توسط مهاجمین وجود نداشته باشد (Integrity).

۵- محتوا، اطلاعات و خدمات باید به گونه‌ای باشد که در دسترس افراد مجاز قرار گیرد و از دسترس افراد غیرمجاز خارج باشد (Availability).

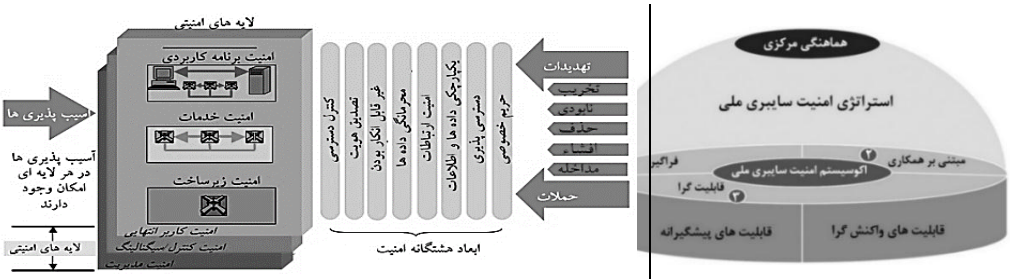
www.SID.ir

Archive of SID



در سال ۲۰۱۵، امنیت سایبری خاورمیانه مورد بررسی قرار گرفت و مدل اکوسیستم امنیت سایبری ملی با سه الزام راهبردی فراگیری، مبتنی بر همکاری و قابلیت گرایی ارائه شد (۰– الف) (***Tohme, Lindeyer, Harb, Papazian, & Ghaziri,*** ۲۰۱۵) . مرکز ملی فضای مجازی کشور، با توسعه امنیت در ابعاد محرمانگی، یکپارچگی، دسترسی‌پذیری، تصدیق هویت و کنترل دسترسی، ارتباطات امن، حریم خصوصی، مدل امنیت در شبکه ملّی اطلاعات کشور را ارائه نمود (۰– ب) (مرکز ملی فضای مجازی، ۱۳۹۶) .

**اکوسیستم امنیت سایبری ملی (*Lindeyer & Papazian*) و مدل مفهومی امنیت فضای مجازی کشور (مرکز ملی فضای مجازی)**




(الف) (ب)

راهبردهای امنیت سایبری در برخی از کشورهای جهان (مطالعه تطبیقی): عدم تأمین امنیت سایبری، در نهایت موجب بروز جنگ‌های سایبری می‌شود (***Schmitt,*** ۲۰۱۳) لذا کشورهای مختلف راهبردهای متفاوتی را در این خصوص اتخاذ نموده‌اند که مورد بررسی قرار گرفته و در برخی از آن‌ها نکات قابل توجهی در راستای اهداف پژوهش حاضر یافت شد که نمونه‌ای از آن‌ها عبارتند از (۰):

**راهبردهای امنیت سایبری برخی از کشورها (به تفکیک قاره)**

| ردیف | کشور | راهبردهای امنیت سایبری | منبع |
|---|---|---|---|
| ۱ | ترکیه (آسیا) | بر پایه هفت شاخص اصلی گزارش‌های رسمی، چارچوب قانونی، مسئولیت‌پذیری و سازمان‌دهی، برنامه‌های امنیت سایبر، فعالیت‌های امنیت سایبری در نیروهای مسلح، همکاری بین‌المللی ملی/فراملی، تدوین شده است. | *Senturk, Çil, & Sağıroğlu, (۲۰۱۲:۱۱۳* |
| ۲ | هندوستان (آسیا) | پیش‌بینی حملات و هشدار به‌موقع، حفاظت از سامانه‌های حیاتی در مقابل حملات سازمان‌یافته اقتصادی، به‌کارگیری سازمان‌های | *Bamrara, (۲۰۱۲* |

www.SID.ir

Archive of SID



| ردیف | کشور | راهبردهای امنیت سایبری | منبع |
|---|---|---|---|
| | | زیرساختی برای ایمن‌سازی فضای سایبری را مدنظر قرار داده است. | |
| ۳ | آلمان (اروپا) | بر حفاظت از زیرساخت‌های حیاتی، به‌کارگیری مرکز ملی پاسخگویی سایبری، تشکیل شورای امنیت ملی سایبری، کنترل مؤثر جرائم سایبری، اقدام مؤثر هماهنگ برای امنیت سایبری اروپا و جهان، توسعه کارکنان و تأمین ابزاری برای پاسخگویی به حملات سایبری، تمرکز نموده است. | *Federal ) Ministry of the (Interior, ۲۰۱۱* |
| ٤ | انگلستان (اروپا) | امنیت فضای سایبر را برای سلامت جامعه و امنیت ملی خود حیاتی دانسته و در چشم‌انداز ۲۰۲۱، «انگلستانی امن و مقاوم در برابر تهدیدات سایبر، موفق و هماهنگ با دنیای دیجیتال» را تصویر می‌نماید و برای تحقق چشم‌انداز فوق، سه هدف کلان دفاع[۱]، بازدارندگی[۲] و توسعه[۳] را مدنظر قرار داده و سه راهبرد کلان کاهش خطر استفاده از فضای سایبری، بهره‌برداری از فرصت‌ها در فضای سایبر و بهبود قابلیت‌های تصمیم‌گیری را دنبال می‌کند. | *Government of ) the United (Kingdom, ۲۰۱٦* |
| ٥ | استرالیا (اقیانوسیه) | مبارزه مؤثر با جرائم سایبری را لازمه محیط دیجیتال امن و مطمئن دانسته و سیاست‌های امنیت فضای سایبری خود را بر پایه حفظ محیط عملیاتی ایمن، انعطاف‌پذیر و قابل اعتماد در راستای امنیت ملی، تدوین نموده است. | *Commonwealth ) of Australia, (۲۰۱۳, pp. ٦-۸* |
| ٦ | نیوزلند (اقیانوسیه) | در سه حوزه افزایش آگاهی و امنیت آنلاین، حفاظت از سیستم‌های دولتی و اطلاعاتی و برنامه‌ریزی برای پاسخگویی به حوادث، اولویت‌بندی شده است. | *New Zealand's ) Cyber Security (Strategy, ۲۰۱۱* |
| ۷ | کانادا (آمریکا) | بر سه محور تأمین امنیت سیستم‌های دولتی، ایمن‌سازی سیستم‌های حیاتی و برقراری بستر امن آنلاین استوار است. | *Canada & ) Public Safety (Canada, ۲۰۱۰* |
| ۸ | جامائیکا (آمریکا) | چشم‌انداز امنیت سایبری خود را در حال تکامل دانسته و از طریق پیاده‌سازی راهبردهای پیشگیرانه در خطرات بالقوه و آسیب‌پذیری‌ها، در چهار محور اصلی محافظت از زیرساخت‌های اطلاعاتی حیاتی، مردم، قوانین نظارتی و کنترل‌های فنی، چارچوب امنیت سایبری خود را تدوین نموده است[٤]. | *Dennis, Jones, ) Kildare, & (Barclay, ۲۰۱٤* |
| ۹ | کنیا | حفاظت از زیرساخت حیاتی، اطلاع‌رسانی و آموزش، تدوین چارچوب | *Government of )* |

۱-DEFEND
۲-DETER
۳-DEVELOP
٤-JNCF

www.SID.ir

Archive of SID



| ردیف | کشور | راهبردهای امنیت سایبری | منبع |
|---|---|---|---|
| | (آفریقا) | حاکمیتی جامع امنیت سایبری و ارتقاء آگاهی دولت و مـردم کنیـا از امنیـت سایبری را مورد توجه قرار داده است. | *(Kenya, ۲۰۱٤* |

شاخص جهانی امنیت سایبری[۱]، توسط اتحادیه بین‌المللی مخابرات و شـرکت ***ABI***، بـا هـدف تقویت یک فرهنگ جهانی امنیت سایبری و ادغام آن با فناوری اطلاعات و ارتباطات ارائه شد. این شاخص، یک نظرسنجی برای تعیین میزان تعهد کشورهای عضو در کمک برای افزایش آگـاهی در خصوص امنیت سایبری است. نتایج اخذشده از همه ۱۹۳ کشور عضو در سال ۲۰۱۷، نشان داد که تعهد لازم برای بهبود همکاری، ظرفیت‌سازی و اقدامات سازمانی در راستای ارتقای امنیت سایبری در جهان وجود دارد (***GCI,*** ۲۰۱۱) . در سال ۲۰۱۷، نسخه ارتقاءیافته شاخص‌های فوق ارائه و در بخش پنجم آن (همکاری) ، پنج شاخص توافق‌های دوجانبه، توافق‌های چندجانبه، مشـارکت‌هـای سازمانی، مشارکت بخش‌های دولتی و خصوصـی، مشـارکت‌هـای بـین‌المللـی، بـرای مشـارکت و همکاری بین‌المللی در شبکه‌ها تعیین شد (***ITU,*** ۲۰۱۷:٤) .

فرآیند ارتقاء امنیت سایبری (امنیت فضای مجازی): تلاش زیادی توسـط سـازمان همکـاری و توسعه اقتصادی و اتحادیه بین‌المللی مخابرات برای ترویج و ارتقاء امنیت فضای سایبری صـورت گرفت (***McDowell, Nensey, & Steinberg,*** ۲۰۱٤) و در نهایت، مؤسسه ترند میکرو[۲] (۲۰۱۷)، اجزای ضروری نسل آینده امنیت سایبری را موردمطالعه قرار داد و مـدل فرآینـدی جـامعی بـرای ساماندهی مراحل ارتقاء امنیت سایبری ارائه نمود که در آن، تحلیل ریسک و برآورد خطرات، طبق چرخه دمینگ[۳] (***Wamala,*** ۲۰۱۱:۹۳) و نظارت و مقابلـه بـا تهدیـدات سـایبری (رسـیدگی بـه رویدادهای غیرمنتظره و حوادث، با تمرکز بر پاسخ سریع) طبق حلقه بوید[٤] یا «اودا»، طراحـی‌شـده است) ۰) (***Trend Micro,*** ۲۰۱۷:۲۰) .

---

۱-Global Cybersecurity Index (GCI)

۲-rend Micro Incorporated

۳-Deming cycle (PDCA): Plan برنامه‌ریزی؛ Do انجام دادن؛ Check چک کردن؛ Act عمل کردن

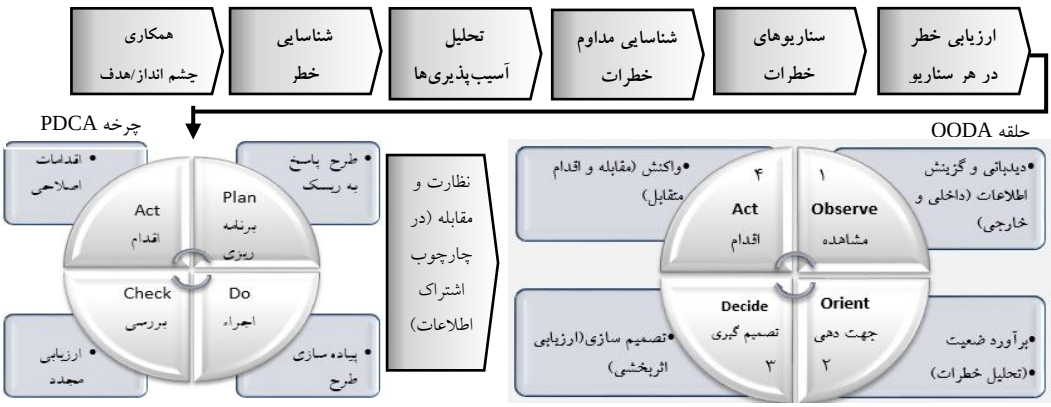
٤- Boyd's Loop or OODA در سال ۱۹۸۷، حلقه «اودا» شامل چهـار مرحلـه مشـاهده Observe؛ جهـت‌دهـی Orient؛ تصمیم‌گیری Decide؛ اقدام Act؛ توسط استراتژیست‌های نظامی آمریکا و سرهنگ جان بوید ارائه شد.

www.SID.ir

Archive of SID



**مراحل ارتقاء امنیت سایبری (Trend Micro, ۲۰۱۷:۲۰)**




جرائم سایبری: در دنیای واقعی، انسان‌ها در طول زمان و در چارچوب مکان محصورند، اما در فضای مجازی، با استفاده از فناوری‌های نوین ارتباطی و رایانه‌ها، نقاط ضعف انسان که همانا سرعت، دقّت، حافظه و خستگی و غیره پوشش داده‌شده و با سرعتی نزدیک به‌سرعت نور خواسته‌ها و پاسخ‌ها به مقصد و مبدأ منتقل می‌گردد (***Tabansky,*** ۲۰۱۱:۷٦). ویژگی‌هایی چون تعدد زیاد بازیگران، هزینه کم، سرعت و تأثیرگذاری بالا، ناشناس ماندن، دشواری در ردیابی، کمرنگ شدن نقش جغرافیا ***(Kahn et al.,*** ۲۰۱۱: ۲۸-۲۰) و از سوی دیگر، فقدان مرزهای فیزیکی، عدم انطباق با استانداردهای جهانی حقوق کیفری، یکنواختی قوانین در حوزه‌های اصلی قانون‌گذاری و غیرمادی بودن رفتارهای ارتکاب یافته (قاجار قیونلو، ۱۳۹۱: ۲۱۳)، موجب می‌گردد که برخلاف جرائم سنتی که مجرم باید در محل وقوع جرم حضورداشته باشد، جرم در یک دنیای مجازی در ابعاد بین‌المللی اتفاق افتد (خلیلی، ۱۳۹۱: ۷) و مجرمین به دارایی‌های مادی (زیرساخت، سازه و سامانه‌های سایبری، محتوا، داده و اطلاعات سایبری) و معنوی (فردی و جمعی/ملّی) کشور در فضای مجازی دست‌درازی کنند (جلالی فراهانی، ۱۳۹۰: ۳۸) و عوامل اقتصادی، فرهنگی، سیاسی، مشکلات روحی نظیر عصبانیت، حسادت، انتقام‌جوئی، تفریح و سرگرمی، رقابت و غیره نیز می‌توانند در شکل‌گیری آن جرائم مؤثر باشند (پیکان‌پورفرد، ۱۳۹۵: ۲) .

سازمان پلیس جنایی بین‌المللی (اینترپل)، جرائم رایانه‌ای را به شش گروه دستیابی غیرمجاز، تغییر داده‌های رایانه‌ای، کلاهبرداری رایانه‌ای، تکثیر غیرمجاز، سابوتاژ (خرابکاری) رایانه‌ای و سایر

www.SID.ir

Archive of SID



جرائم رایانه‌ای و بخش یکم قانون جرائم رایانه‌ای کشور (جرائم و مجازات) آن را به جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، سرقت و کلاهبرداری مرتبط با رایانه، جرائم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب، مسئولیت کیفری اشخاص حقوقی و سایر جرائم دسته‌بندی نموده‌اند (حاجی ده‌آبادی ، ۱۳۹۳) .

پیشگیری از وقوع جرائم سایبری: به اقدام علمی جهت کاهش بزه‌کاری و ناامنی، اطلاق شده و از روش‌های پیشگیری عام و خاص (کیفری) و پیشگیری اجتماعی و وضعی (غیر کیفری و اجتماعی همانند جرائم سایبری) در این خصوص استفاده می‌شود (خانعلی‌پور، ۱۳۹۰: ۱۰).

پیشگیری اجتماعی: تدابیر آموزشی، فرهنگی و اجتماعی دولت و سازمان‌های مردم‌نهاد در سالم‌سازی محیط اجتماعی و فیزیکی برای حذف یا کاهش عوامل اجتماعی وقوع جرم است و به‌صورت جامعه‌مدار و رشدمدار انجام می‌شود (محمد نسل، ۱۳۸۷) .

پیشگیری وضعی: با افزایش بهای ارتکاب جرم از طریق حذف موقعیت‌های دارای خطر و بهره‌گیری از راهبردهای پیشگیرانه ایجابی و سلبی انجام می‌شود (بهره‌مند، ۱۳۹۳: ۱۵۵) .

مبارزه با جرائم سایبری: جرائم سایبری می‌تواند تهدیدی برای امنیت ملّی باشد ( ***Peritz & Sechrist,*** ۲۰۱۰, ***pp.*** ۵-۷) (آمریکا، این حملات را به‌عنوان جنگ تلقی می‌کند) . هر اقدام مجرمانه در فضای مجازی (ایجاد اختلال، کاهش کیفیت یا نابودی اطلاعات سامانه هدف) ، طبق فرآیند شناسایی، پویش، دسترسی، ارتقاء، اختفاء، یورش و تثبیت انجام می‌شود و برای دفاع از دارایی‌ها در مقابل آن‌ها، باید مراحل تشخیص و پیشگیری[۱] (شناسایی راه‌های نفوذ، جهت افزایش ضریب امنیت، پایداری سامانه‌ها و متوقف نمودن حملات) ، مدیریت حادثه و محدود کردن خرابی‌ها[۲] (تعیین آثار، نشانه‌ها و هشدارها، پایدار کردن سامانه‌ها، خاموشی و تخصیص مجدد) و پشتیبانی[۳] (باید قبل از هر حمله‌ای، اطلاعات را جمع‌آوری نمود و از آن‌ها نسخه پشتیبانی تهیه شود) ، را مورد توجه قرار داد (حسینی، ۱۳۹۲: ٤٨) .

به علت فرامرزی بودن جرائم سایبری و برابری حاکمیت‌ها، دادگاه داخلی یک کشور اصولاً نمی‌تواند علیه جرائم ارتکابی کشوری دیگر حکم صادر کند. لذا بهترین روش مبارزه، رجوع به

۱- Prevention: Embed Security into design & Ban attacks
۲ -Incident management & damage limitation: harden the system & Shutdown and reallocation & real time
۳ -Backup

www.SID.ir

Archive of SID



محاکم بین‌المللی و ایجاد همکاری پلیسی و حقوقی در سطح بین‌المللی است (سازمان همکاری و توسعه اقتصادی (***OECD***)، اتحادیه بین‌المللی مخابرات (***ITU***)، مجمع جهانی نوآوری (***IGCI***)، سازمان ملل متحد (***UN***)، انجمن بین‌المللی حقوق جزا، یونسکو (***UNESCO***)، اتحادیه اروپا (***EU***) و بسیاری سازمان دیگر، در حوزه مبارزه فراملی با جرائم سایبری و غیره) و در این راستا، ترکیب اقدامات فنی و غیر فنی و تصویب قوانین جدید ملّی و بین‌المللی مبارزه با جرائم سایبری و فارنزیک (پزشکی قانونی) رایانه‌ای می‌تواند مفید باشد (***Arora, Bhatt, & Pant,*** ۲۰۱۲) .

ترسیم مدل مفهومی پژوهش: به‌منظور ترسیم مدل مفهومی لازم است که مفاهیم قابل توجه (داده‌های کیفی) را از مستندات جمع‌آوری‌شده استخراج (فیش‌برداری، علامت‌گذاری، نام‌گذاری یا کدگذاری) و بر اساس میزان تکرار مفاهیم مشابه، آن‌ها را جمع‌بندی (تحلیل کیفی) و عوامل قابل توجه در مدل مفهومی را تعیین نماییم که این مهم در پژوهش حاضر، به روش نظریه‌پردازی داده بنیاد یا گراندد تئوری[1] و توسط نرم‌افزار مکس‌کیودا انجام می‌شود. طبق روش فوق، کلیه مستندات پژوهش در نرم‌افزار فوق درج و مفاهیم قابل توجه، کدگذاری شد (کدگذاری باز) و با دسته‌بندی کدهای مشابه یا تکراری و مقوله سازی از آن‌ها در چندین مرحله (اختصاص نام یا کدی کلان‌تر به کدهای دسته‌بندی‌شده)، شاخص‌ها، مؤلفه‌ها و ابعاد طبق ۰ احصاء گردید (ستون تکرار، نشان‌دهنده تعداد تکرار یا تأکید مفهوم فوق در مستندات است).

**مقوله‌های قابل توجه (مؤلفه‌ها)**

| شاخص‌ها | تکرار | مؤلفه‌ها | ابعاد |
|---|---|---|---|
| تدابیر آموزشی و آگاه‌سازی عمومی (جامعه مدار) | ۳ | پیشگیری اجتماعی از وقوع جرم | پیشگیری از وقوع جرم |
| امن‌سازی زیرساخت‌های فنی کشور (جامعه مدار) | ٤ | | |
| تدریس مواد درسی مرتبط در مدارس (رشد مدار) | ۲ | | |
| استمرار در اجرای برنامه‌های پیشگیری (رشد مدار) | ٥ | | |
| افزایش دشواری ارتکاب جرم (ایجابی) | ۳ | پیشگیری وضعی از وقوع جرم | |
| افزایش خطر ارتکاب جرم (ایجابی) | ٦ | | |
| کاهش دستاوردها جرم (سلبی) | ٤ | | |
| کاهش عوامل محرک جرم (سلبی) | ۳ | | |
| شورای عالی فضای مجازی کشور | ۷ | سیاست‌گذاری و اجرا در سطح ملی | سیاست‌گذاری (قانونی – |
| مراکز مدیریت امداد و هماهنگی عملیات رخدادهای | ۳ | | |

۱- *Grounded Theory* در نهایت نظریه و یا فرضیه مورد نظر را ارائه می‌نماید.

www.SID.ir

Archive of SID



| شاخص‌ها | تکرار | مؤلفه‌ها | ابعاد |
|---|---|---|---|
| رایانه‌ای (ماهر) | | | اجرایی) |
| گروه‌های واکنش هماهنگ رخداد (گوهر) | ٤ | | |
| پلیس (اینترپل و فتا) | ۹ | | |
| سازمان همکاری و توسعه اقتصادی (OECD) | ٥ | سیاست‌گذاری و اجرا در سطح فراملی | |
| اتحادیه بین‌المللی مخابرات (ITU) | ۲ | | |
| مجمع جهانی نوآوری (IGCI) | ٤ | | |
| سازمان ملل متحد (UN) | ۳ | | |
| انجمن بین‌المللی حقوق جزا | ۲ | | |
| یونسکو (UNESCO) | ٥ | | |
| اتحادیه اروپا (EU) | ٥ | | |
| قانون جرائم رایانه‌ای | ٤ | مقررات‌گذاری در سطح ملی | مقررات-گذاری |
| قانون تجارت الکترونیک | ٥ | | |
| قانون دادرسی الکترونیکی | ٥ | | |
| کنوانسیون جرائم سازمان‌یافته (پالرمو) | ٤ | مقررات‌گذاری در سطح فراملی | |
| کنوانسیون جرائم سایبری (بوداپست) | ۳ | | |
| ثبت رخدادهای امنیتی | ٤ | رصد و پایش جرائم سایبری | برخورد قضایی و پلیسی |
| جمع‌آوری و ذخیره‌سازی | ۳ | | |
| تحلیل و هشدار دهی | ٥ | | |
| علیه نفوذ مبتنی بر شبکه (NIDS) | ٥ | شناسایی و تعقیب مجرمین | |
| علیه نفوذ مبتنی بر میزبان (HIDS) | ٦ | | |
| علیه نفوذ توزیع‌شده (DIDS) | ۷ | | |
| در مراجع قانونی ملی | ۳ | رسیدگی و مجازات | |
| در مراجع قانونی بین‌المللی | ۲ | | |
| در سطح منطقه‌ای | ٤ | استرداد و معاضدت قضایی | |
| در سطح بین‌المللی | ۳ | | |

ابعاد، مؤلفه‌ها و شاخص‌های مبارزه با جرائم سایبری برای ارتقاء امنیت فضای مجازی یا به‌عبارت‌دیگر، بستر یا زمینه شکل‌گیری همکاری بین‌المللی مشخص شد و با بهره‌گیری از توانمندی ابزارهای پنج‌گانه شاخص جهانی امنیت سایبری، توافق‌های دوجانبه، توافق‌های

www.SID.ir

Archive of SID



چندجانبه، مشارکت‌های سازمانی، مشارکت بخش‌های دولتی و خصوصی، مشارکت‌های بین‌المللی، روابط اثربخش با ملت‌ها، دولت‌ها و سازمان‌های بین‌المللی در عرصه فضای سایبر جهانی برقرار می‌گردد. با تجمیع موارد فوق در یک مدل خورشیدی[۱]، مدل مفهومی پژوهش مشتمل بر ٤ لایه ترسیم می‌گردد (۰).

مدل مفهومی فوق، در چهار لایه ابعاد، مؤلفه‌ها، زیرمؤلفه‌ها و شاخص‌ها (به ترتیب از داخل به بیرون) ترسیم گردید و طبق آن، همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران و با رویکرد مبارزه با جرائم سایبری باید در ٤ مرحله به‌هم‌پیوسته، پیشگیری از وقوع جرم (پیشگیری اجتماعی و پیشگیری وضعی)، سیاست‌گذاری و اجرا (در سطح ملی و فراملی)، مقررات گذاری (در سطح ملی و فراملی) و برخورد قضایی و پلیسی (رصد و پایش جرائم سایبری، شناسایی و تعقیب مجرمین، رسیدگی و مجازات، استرداد و معاضدت قضایی) صورت گیرد. لایه سوم (با پس‌زمینه سفید)، زیرمؤلفه‌های قابل توجه در هر مؤلفه را نشان می‌دهد که برای ارتقاء امنیت سایبری در زمینه هر یک از آن‌ها، می‌توان از ابزارهای پنج‌گانه همکاری بین‌المللی (توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت بخش‌های دولتی و خصوصی، مشارکت‌های بین‌المللی)، استفاده نمود (به این دلیل در مدل، چرخان ترسیم شده‌اند).

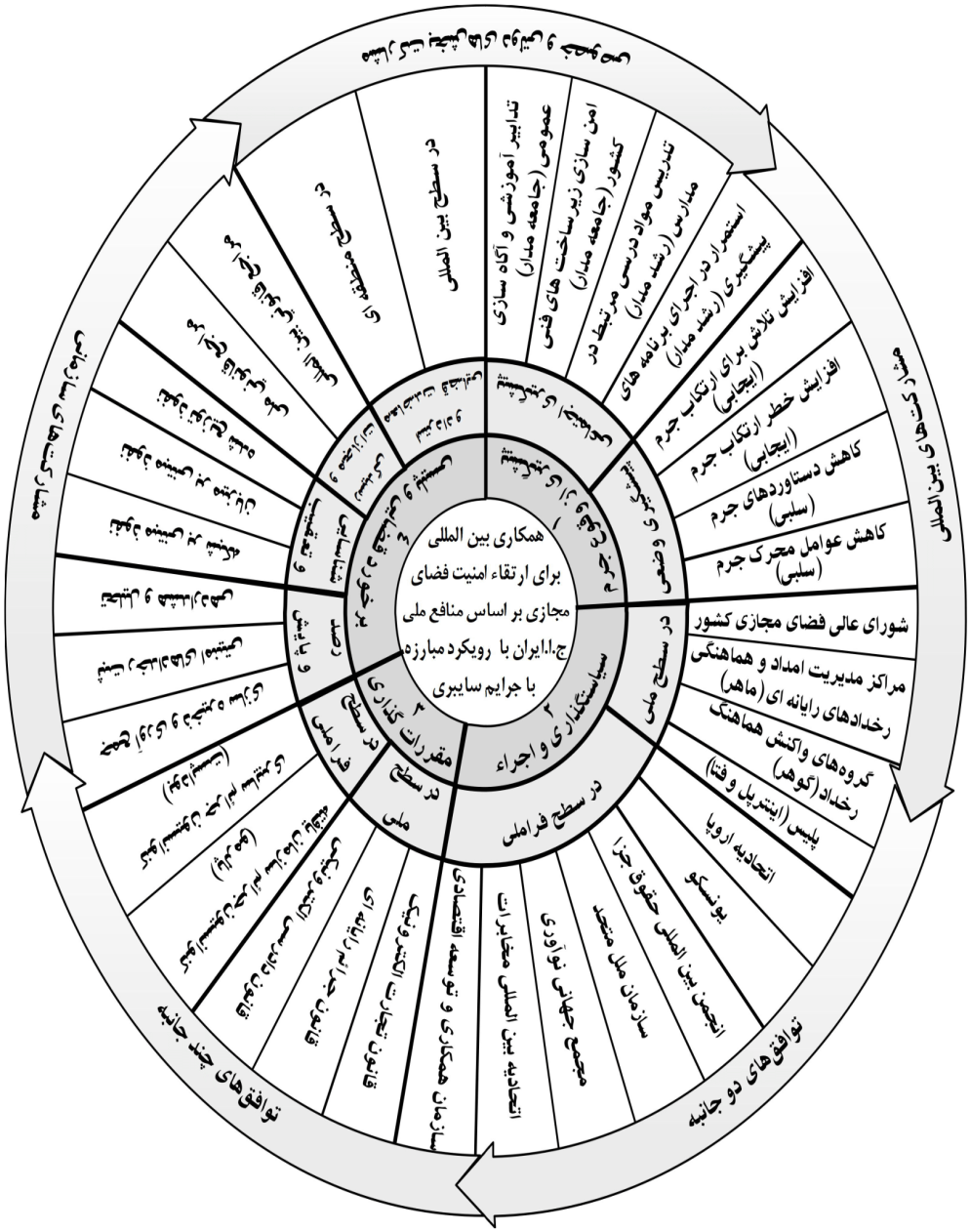
۱-SunBurst

www.SID.ir

Archive of SID



**مدل مفهومی پژوهش (محقق ساخته)**




www.SID.ir

Archive of SID



## روش تحقیق

پژوهش توسعه‌ای حاضر با رویکرد آمیخته (تحلیل کیفی- تحلیل کمی) انجام شد. در مرحله اول (تحلیل کیفی)، مبانی نظری پژوهش در نرم‌افزار تحلیل کیفی مکس‌کیودا درج و به روش نظریه‌پردازی داده بنیاد (گراندد تئوری) کدگذاری و تحلیل‌شده و با استخراج ابعاد، مؤلفه‌ها و شاخص‌ها، مدل مفهومی پژوهش ترسیم می‌گردد. در مرحله دوم (تحلیل کمی)، با مدل‌سازی معادلات ساختاری[۱] (بررسی هم‌زمان اثر یک یا چند متغیر مستقل بر یک یا چند متغیر وابسته - ۰) مدل مفهومی پژوهش در نرم‌افزار تحلیل کمی اسمارت پی.ال.اس و استخراج فرضیه‌های پژوهش، نظر خبرگان در خصوص مدل فوق توسط پرسشنامه، مصاحبه و جلسات کانونی اخذ می‌گردد و با اعمال اصلاحات لازم بر اساس نتایج تجزیه و تحلیل داده‌های کمی حاصل با روش حداقل مربعات جزئی[۲] (*PLS*) (دارای قابلیت ویژه در تحلیل نمونه‌های کم) بر روی مدل مفهومی و ساختاربندی کلیه عوامل احصاء شده و برقراری روابط بین آن‌ها طبق حلقه تصمیم‌گیری «اودا- *OODA*» با چهار فاز، مشاهده، جهت‌دهی، تصمیم‌گیری و اقدام، الگوی راهبردی مورد نظر طراحی و ارائه می‌شود[۳].

**فرآیند مدل‌سازی معادلات ساختاری (SEM (داوری و رضا زاده، ۱۳۹۲: ۲۷)**


در این روش باید، برازش (مناسب بودن) مدل از ۳ جنبه اندازه‌گیری، ساختاری و کلی مورد ارزیابی قرار گیرد (محسنین و اسفیدانی، ۱۳۹۳) لذا اطلاعات از طریق سایت‌های داخلی[٤]،

---

۱- Structural Equation Modeling (SEM) منصور مؤمنی در کتاب «مدل سازی معادلات ساختاری با تأکید بر سازه های بازتابنده و سازنده» به این موضوع پرداخته است (مؤمنی، ۱۳۹۲) .

۲- Partial least squares (PLS) path modeling

۳- داوری و رضازاده در کتاب «مدلسازی معادلات ساختاری با نرم افزار **PLS**»، روند اجرای کار را تشریح نموده‌اند (داوری و رضازاده، ۱۳۹۲: ۲۷) .

٤ SID. ir, Elearnica. ir, IranDoc. ac. ir,Civilica. com, sci. isc. gov. ir, ensani. ir, noorlib. ir, elearnica. Ir,...

www.SID.ir

Archive of SID

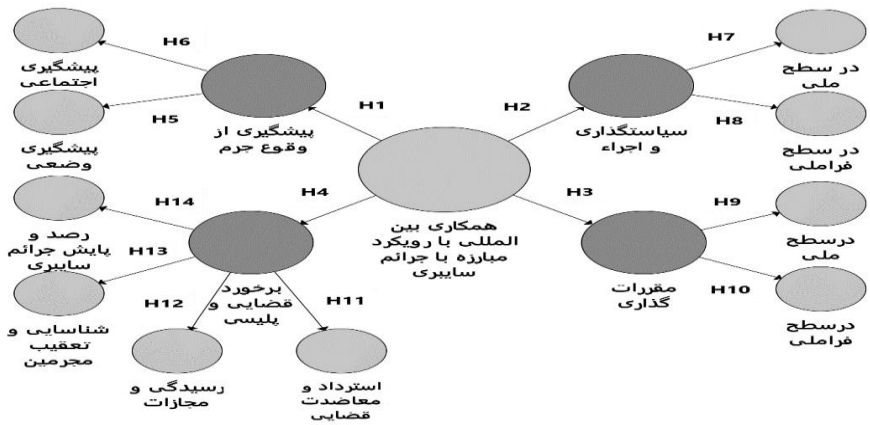


سایت‌ها و موتورهای جستجوی علمی خارجی[۱]، مستندات کاغذی و الکترونیکی و غیره (برای تسریع در فیش‌برداری، از نرم‌افزار مکس‌کیودا[۲] استفاده شد) ، جمع‌آوری و توسط نرم‌افزار پژوهیار[۳] ساماندهی گردید. به‌منظور ذخیره‌سازی توصیف‌های آماری داده‌های پرسشنامه (پایایی یا آلفای کرونباخ، روایی، فراوانی و غیره) ، از نرم‌افزار ***SPSS*** ۲۵ و از نرم‌افزار ***SmartPLS*** ۳ جهت تجزیه و تحلیل داده‌های کمی (مستخرج از پرسشنامه، مصاحبه و جلسات کانونی) به‌منظور تأیید عاملی مدل مفهومی، ارزیابی فرضیه‌ها و پاسخگویی به سؤال‌های پژوهش، و در نهایت نیز الگوی راهبردی مورد نظر طبق مراحل حلقه «اودا»، در نرم‌افزار ***EdrawMAX*** ترسیم گردید.

## تجزیه و تحلیل داده‌ها و یافته‌های تحقیق:

ابتدا، مدل معادلات ساختاری مدل مفهومی پژوهش را در نرم‌افزار تحلیل کمی اسمارت پی.ال.اس ترسیم می‌کنیم[٤].

**ترسیم روابط ابعاد و مؤلفه‌های پژوهش به‌منظور شناسایی فرضیه‌ها (محقق ساخته)**




۱-scholar. google. com, sciencedirect. com, springer. com, ieee. Org,...

۲-MaxQDA

۳- نرم‌افزار کاملاً ایرانی پژوهیار، امکان جمع‌آوری، ساماندهی و استناددهی مستندات (نوشتار، تصویر، صوت و غیره) را فراهم می‌نماید.

٤- عادل آذر و همکارانش، مدلسازی معادلات ساختاری را در کتاب «مدلسازی مسیری – ساختاری در مدیریت» تشریح نموده اند (آذر، غلامزاده، و قنواتی، ۱۳۹۱).

www.SID.ir

Archive of SID



متغیرهای پنهان (ابعاد و مؤلفه‌ها) در مدل معادلات ساختاری و روابط بین آن‌ها را نشان می‌دهد و صحت هر رابطه (تأیید/ رد) باید بررسی شود و می‌تواند فرضیه پژوهش باشد لذا ۱٤ فرضیه قابل توجه است (۰).

**فرضیه‌های پژوهش**

| فرضیه | عنوان |
|---|---|
| اصلی | H۱– شناخت و پیشگیری از جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد.<br>H۲ – سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد.<br>H۳ – تدوین مقررات مبارزه با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد.<br>H٤ –برخورد قضایی و پلیسی با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد. |
| فرعی | H۵ – پیشگیری اجتماعی از وقوع جرم، تأثیر معنی‌داری بر پیشگیری از وقوع جرم دارد.<br>H٦ – پیشگیری وضعی از وقوع جرم، تأثیر معنی‌داری بر پیشگیری از وقوع جرم دارد.<br>H۷ – سیاست‌گذاری در سطح ملی، تأثیر معنی‌داری بر سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری دارد.<br>H۸ – سیاست‌گذاری در سطح فراملی، تأثیر معنی‌داری بر سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری دارد.<br>H۹ – مقررات‌گذاری در سطح ملی، تأثیر معنی‌داری بر مقررات گذاری مبارزه با جرائم سایبری دارد.<br>H۱۰ – مقررات‌گذاری در سطح فراملی، تأثیر معنی‌داری بر مقررات گذاری مبارزه با جرائم سایبری دارد.<br>H۱۱ – رصد و پایش جرائم سایبری، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد.<br>H۱۲ – شناسایی و تعقیب مجرمین سایبری، تأثیر معنی‌داری در برخورد قضایی و پلیسی با جرائم سایبری دارد.<br>H۱۳ – دستگیری و مجازات مجرمین سایبری، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد.<br>H۱٤ –استرداد مجرمین سایبری و معاضدت قضایی، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد. |

به‌منظور اخذ نظر خبرگان جهت ارزیابی مدل مفهومی احصاء شده از جمع‌بندی ادبیات و مبانی نظری پژوهش (فصل ۲)، پرسشنامه‌ای بر اساس طیف لیکرت ۵ گزینه‌ای (۱=خیلی کم، ۲=کم، ۳=متوسط، ٤=زیاد، ۵=خیلی زیاد) تنظیم گردید. به‌منظور اعتبارسنجی (روایی و پایایی)، پرسشنامه فوق در اختیار ۱۰ نفر از خبرگان قرار گرفت و نظرات تخصصی به‌صورت حضوری اخذ و اشکالات مطرح‌شده، اصلاح گردید و سپس داده‌های حاصل از پرسشنامه در نرم‌افزار ***SPSS*** درج و آلفای کرونباخ مناسب اخذ شد (۰.۸۸۲ بزرگ‌تر از ۰.۷) و سپس، پرسشنامه نهایی در اختیار ٤۰ نفر از صاحب‌نظران قرار گرفت (کاغذی و الکترونیکی) و در نهایت نیز ۲۸ پرسشنامه جمع‌آوری شد.

www.SID.ir

Archive of SID



اطلاعات جمعیت شناختی: ۵۳ درصد از پاسخگویان آشنایی خود را متوسط و ۳۵ درصد زیاد و ۷ درصد خیلی زیاد اعلام نموده‌اند و این مطلب با توجه به چهار مفهوم مطرح در پژوهش (همکاری بین‌المللی، منافع ملی جمهوری اسلامی ایران، ارتقاء امنیت فضای مجازی و مبارزه با جرائم سایبری) دور از انتظار نبود ولی باید توجه داشت که محققین معمولاً خود را پایین‌تر از میزان واقعی در نظر می‌گیرند. ۳۲ درصد از پاسخگویان، سابقه کار ۱۱ تا ۱۵ سال و ۳۲ درصد دیگر نیز سابقه کار ٦ تا ۱۰ سال را داشته‌اند که بیشترین فراوانی را تشکیل می‌دهند. ٤۳ درصد از پاسخگویان کارشناس فنی، ۲۱ درصد مدیر عملیاتی، ۱۸ درصد عضو هیئت‌علمی، ۱۱ درصد مدیر راهبردی و ۷ درصد نیز مدیر میانی بوده‌اند (۰).

**اطلاعات جمعیت شناختی پاسخگویان (تحصیل محقق توسط نرم‌افزار SPSS)**


بررسی ابعاد و مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری:

با ثبت نظر اخذشده از خبرگان در نرم‌افزار و اجرای الگوریتم حداقل مربعات جزئی[۱]، نتایج طبق ۰به دست آمد.

۱-PLS Algorithm

www.SID.ir

Archive of SID



**نتایج محاسبات (محقق ساخته)**

| | آلفای کرونباخ[۱] | پایایی ترکیبی[۲] | متوسط واریانس (AVE)[۳] | ضریب تعیین ($R^2$) | نتیجه برازش | $Q^2$ | نتیجه برازش |
|---|---|---|---|---|---|---|---|
| پیشگیری از وقوع جرم | ۰.۷۳۱ | ۰.۸۸۱ | ۰.۷۸۸ | ۰.۰۱۱ | ضعیف | ۰.۰۰٦ | ضعیف |
| پیشگیری اجتماعی | ۰.۷٦٤ | ۰.۸٤٤ | ۰.۵۷۷ | ۰.۲۸ | متوسط | ۰.۰٤۷ | متوسط |
| پیشگیری وضعی | ۰.٦۵۵ | ۰.۷۸٤ | ۰.٤۸ | ۰.۲۷۸ | متوسط | ۰.۰۳۱ | متوسط |
| سیاست‌گذاری و اجرا | ۰.۸۱٤ | ۰.۹۱۵ | ۰.۸٤۳ | ۰.۳۷ | قوی | ۰.۲۲٤ | قوی |
| سیاست‌گذاری و اجرا در سطح ملی | ۰.۷۱٤ | ۰.۸۲ | ۰.۵۳۷ | ۰.۱۱۸ | ضعیف | ۰.۰۰۷ | ضعیف |
| سیاست‌گذاری و اجرا در سطح فراملی | ۰.۷۸۲ | ۰.۸۳۹ | ۰.٤۳۷ | ۰.٤۵۱ | قوی | ۰.۱۱۲ | متوسط |
| مقررات گذاری | ۰.۸٦۳ | ۰.۹۳٦ | ۰.۸۸ | ۰.۰۵۹ | ضعیف | ۰.۰۵٤ | ضعیف |
| مقررات گذاری در سطح ملی | ۰.۸۸۵ | ۰.۹۲۱ | ۰.۷۹٦ | ۰.۰۹۷ | ضعیف | ۰.۰۱٤ | ضعیف |
| مقررات گذاری در سطح فراملی | ۰.۷۸۲ | ۰.۹۰۲ | ۰.۸۲۱ | ۰.٤۸۵ | قوی | ۰.۳۲۸ | قوی |
| برخورد قضایی و پلیسی | ۰.۷۲ | ۰.۸۲۱ | ۰.۵٤۷ | ۰.۵۲۸ | قوی | ۰.۲۰۹ | قوی |
| رصد و پایش جرائم سایبری | ۰.۸٤٦ | ۰.۹۰۷ | ۰.۷٦٤ | ۰.۵۸۱ | قوی | ۰.۳۰۳ | قوی |
| شناسایی و تعقیب مجرمین | ۰.۸۱٦ | ۰.۸۸۷ | ۰.۷۲٤ | ۰.۱۷۷ | ضعیف | ۰.۰۸۱ | متوسط |
| رسیدگی و مجازات | ۰.۷۵۳ | ۰.۸۹ | ۰.۸۰۱ | ۰.۳٤۷ | قوی | ۰.۲۳۲ | قوی |
| استرداد و معاضدت قضایی | ۰.۸۲٦ | ۰.۹۱۹ | ۰.۸۵ | ۰.۱۹ | متوسط | ۰.۱۲۱ | متوسط |

بررسی برازش مدل اندازه‌گیری (بررسی روابط متغیرهای آشکار (مستطیل) با متغیرهای پنهان مرتبط (دایره‌های متصل)): پایایی مدل اندازه‌گیری از ۳ دیدگاه بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی مورد ارزیابی قرار می‌گیرد.

۱-Cronbachs Alpha

۲-Composite Reliability

۳ -*AVE: Average Variance Extracted*

www.SID.ir

Archive of SID



- بارهای عاملی (اعداد محاسبه و درج‌شده بر روی پیکان‌های متصل به مستطیل‌ها): بارهای عاملی نباید کمتر از ۰/٤ باشند که همان‌طور که در ۰ مشاهده می‌شود، همه بارهای عاملی بیشتر از ۰/٤ بوده و برازش مناسب است.
- پایایی ترکیبی (مشترک): همان‌طور که در ۰ مشاهده می‌شود، پایایی ترکیبی (مشترک) همه عوامل بیشتر از ۰.٦ است که حکایت از پایایی مناسب مدل دارد.
- آلفای کرونباخ: آلفای کرونباخ همه عوامل بیشتر از ۰.۷ است که حکایت از پایا بودن مدل دارد (۰).

روایی مدل از دو دیدگاه روایی همگرا و روایی واگرا مورد ارزیابی قرار گرفت.

- روایی همگرا (متوسط واریانس استخراج‌شده یا ***AVE***): همان‌طور که در ۰ مشاهده می‌شود، مقادیر همه عوامل بیشتر از ۰.٤ است که حکایت از روایی همگرای مناسب مدل دارد.
- روایی واگرا: ماتریس فورنل و لارکر مدل، قابل قبول بودن روایی واگرای مدل را نشان داد.

بررسی برازش مدل ساختاری (ارزیابی روابط بین متغیرهای پنهان (دایره‌ها)): به‌منظور ارزیابی روابط بین متغیرهای پنهان (دایره‌ها) انجام می‌شود (طبق محاسبات بوت استرپینگ[۱] یا خود راه‌اندازی):

- معیار ***R Squares*** یا $R^2$ (ضریب تعیین): میزان تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا را نشان می‌دهد و مقادیر تا ۰/۱۹ و تا ۰/۳۳ و تا ۰/٦۷، به ترتیب برازش ضعیف، متوسط، قوی را نشان می‌دهند (داوری، ۱۳۹۲: ۹۳) . با توجه به مقادیر ستون ضریب تعیین در ۰، برازش معیار $R^2$ مدل ساختاری، متوسط تا قوی است.
- ضرایب معناداری ***z*** (مقادیر ***t-values***): ضرایب معناداری ***z*** بیشتر از ۱.۹٦ و بیشتر از ۲.۵۸ و بیشتر از ۳.۲۷، سطح معناداری ۹۵٪ و ۹۹٪ و ۹۹.۹٪ رابطه بین عوامل در نشان می‌دهد (رستم‌زاده، ۱۳۹۵: ٦۱) . طبق ۰، فقط ابعاد پیشگیری از وقوع جرم و مقررات گذاری، از روابط معناداری برخوردار نیستند ولی مؤلفه‌های آن‌ها، از روابط معناداری برخوردارند که این مسئله در ارزیابی فرضیه‌ها، مورد بررسی دقیقی قرار خواهد گرفت.

۱-BootStrapping

www.SID.ir

Archive of SID



- معیار $Q^2$ [۱]: نشان‌دهنده قدرت پیش‌بینی مدل است. سه مقدار ۰.۰۲ و ۰.۱۵ و ۰.۳۵ نشان‌دهنده برازش ضعیف، متوسط و قوی مدل ساختاری است[۲]. با توجه به ۰، برازش مدل را در این معیار می‌توان متوسط تا قوی ارزیابی نمود.

بررسی برازش مدل کلی: معیار ***GOF***: این مقدار (***GOF***)، از جذر حاصل‌ضرب میانگین ستون «متوسط مشترک ***AVE***»[۳] و میانگین «ضریب تعیین $R^2$» حاصل می‌گردد (۰) و مقدار ۰.۰۱ و ۰.۲۵ و ۰.۳۶، برازش ضعیف، متوسط و قوی مدل را نشان می‌دهد.

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{۰.۷۰۳ \times ۰.۲۸٤} = ۰.٤٤۷$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰.٤٤۷ بوده و چون از ۰.۳٦ بیشتر است، برازش مدل را قوی ارزیابی نموده و با استفاده از نتایج حاصل، فرضیه‌های پژوهش را ارزیابی می‌نماییم.

ارزیابی فرضیه‌های پژوهش: به‌منظور ارزیابی ٤ فرضیه اصلی (***H*۱** تا ***H*٤**) و ۱۰ فرضیه فرعی (***H*۵** تا ***H*۱٤**)، از نتایج معناداری ***z*** برای تأیید یا رد رابطه (رابطه تأیید با مقادیر بیشتر از ۱.۹٦) و از مقادیر ضریب مسیر برای تشخیص شدت رابطه (یک واحد تغییر در سمت چپ هر رابطه، باعث تغییر به میزان ضریب مسیر در سمت راست آن رابطه خواهد شد)، استفاده می‌کنیم (۰).

**ضریب مسیر و ضریب معناداری روابط بین سازه‌ها (تحصیل محقق)**

| فرضیه | روابط | ضریب مسیر | ضرایب z | تأیید یا رد |
|---|---|---|---|---|
| H۱ | همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری - پیشگیری از وقوع جرم | ۰.۱۰۷ | ۰.۷٦٤ | رد |
| H۵ | پیشگیری از وقوع جرم - پیشگیری اجتماعی | ۰.۵۲۹ | ۳.۵۹۱ | تأیید |
| H٦ | پیشگیری از وقوع جرم - پیشگیری وضعی | ۰.۵۲۷ | ۳.٦٦٦ | تأیید |
| H۲ | همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری - سیاست‌گذاری و اجرا | ۰.٦۰۹ | ۲.۹۳٦ | تأیید |
| H۷ | سیاست‌گذاری و اجرا - در سطح ملی | ۰.۳٤۳ | ۲.۱٤۲ | تأیید |

۱-Stone-Geisser Criterion

۲- از طریق ستون SSE/SSO-۱ در جدول Indicator Crossvalidated Redundancy از تحلیل Blindfolding نرم افزار SmartPLS بدست می‌آید

۳- Communality: این عنوان به صورت مشخص در نسخه ۲ نرم افزار وجود دارد ولی در نسخه ۳ نرم‌افزار از مقدار AVE استفاده می شود.

www.SID.ir

Archive of SID



| فرضیه | روابط | ضریب مسیر | ضرایب z | تأیید یا رد |
|---|---|---|---|---|
| H۸ | سیاست‌گذاری و اجرا - در سطح فراملی | ۰.٦۷۱ | ۷.۹۷۰ | تأیید |
| H۳ | همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری – مقررات‌گذاری | ۰.۲٤۳ | ۱.۲۸۰ | رد |
| H۹ | مقررات‌گذاری - در سطح ملی | ۰.۳۱۲ | ۲.۱٥٥ | تأیید |
| H۱۰ | مقررات‌گذاری - در سطح فراملی | ۰.٦۹۷ | ٤.۳۷۸ | تأیید |
| H٤ | همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری - برخورد قضایی و پلیسی | ۰.۷۲۷ | ۷.٥٤٤ | تأیید |
| H۱۱ | برخورد قضایی و پلیسی - رصد و پایش جرائم سایبری | ۰.۷٦۲ | ۱۰.۷٤۱ | تأیید |
| H۱۲ | برخورد قضایی و پلیسی - شناسایی و تعقیب مجرمین | ۰.٤۲۰ | ۳.٤۷٤ | تأیید |
| H۱۳ | برخورد قضایی و پلیسی - رسیدگی و مجازات | ۰.٥۸۹ | ۳.٤۳۱ | تأیید |
| H۱٤ | برخورد قضایی و پلیسی - استرداد و معاضدت قضایی | ۰.٤۳۳ | ۲.۱۹۲ | تأیید |

فرضیه اصلی ***H*۱** (شناخت و پیشگیری از جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد).

ضریب ***z*** کمتر از ۱.۹٦ است (۰.۷٦٤) لذا فرضیه رد شده و نشان می‌دهد که از نظر خبرگان، این رابطه از معناداری مناسبی برخوردار نیست ولی در ذیل این فرضیه، دو فرضیه فرعی ***H*٥** و ***H*٦** مطرح است که باید بررسی شود:

***H*٥**: پیشگیری اجتماعی از وقوع جرم، تأثیر معنی‌داری بر پیشگیری از وقوع جرم دارد: ضریب ***z*** بیشتر از ۱.۹٦ است (۳.٥۹۱) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

***H*٦**: پیشگیری وضعی از وقوع جرم، تأثیر معنی‌داری بر پیشگیری از وقوع جرم دارد: ضریب ***z*** بیشتر از ۱.۹٦ است (۳.٦٦٦) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

با رد فرضیه اصلی H۱ و تأیید فرضیه‌های فرعی H٥ و H٦، می‌توان نتیجه گرفت که خبرگان، تمرکز اقدامات پیشگیری اجتماعی و پیشگیری وضعی از وقوع جرم را ضروری نمی‌دانند و اقدامات فوق باید در دو ساختار و سازمان مجزا انجام شود.

فرضیه اصلی ***H*۲** (سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد).

www.SID.ir

Archive of SID



ضریب **z** بیشتر از ۱.۹٦ است (۲.۹۳۹) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد. در ذیل این فرضیه دو فرضیه فرعی **H**۷ و **H**۸ مطرح‌شده‌اند:

**H**۷– سیاست‌گذاری در سطح ملی، تأثیر معنی‌داری بر سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۲.۱٤۲) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

**H**۸– سیاست‌گذاری در سطح فراملی، تأثیر معنی‌داری بر سیاست‌گذاری و اجرای اقدامات مبارزه با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۷.۹۷۰)، فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

فرضیه اصلی **H**۳ (تدوین مقررات مبارزه با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد)

ضریب **z** کمتر از ۱.۹٦ است (۱.۲۸۰) لذا فرضیه رد شده و نشان می‌دهد که از نظر خبرگان، این رابطه از معناداری مناسبی برخوردار نیست **T** ولی در ذیل این فرضیه، دو فرضیه فرعی **H**۹ و **H**۱۰ مطرح است که باید بررسی شود:

**H**۹– مقررات‌گذاری در سطح ملی، تأثیر معنی‌داری بر مقررات‌گذاری مبارزه با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۲.۱۵۵) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

**H**۱۰– مقررات گذاری در سطح فراملی، تأثیر معنی‌داری بر مقررات گذاری مبارزه با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (٤.۳۷۸) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

با رد فرضیه اصلی **H**۳ و تأیید شدن فرضیه‌های فرعی **H**۹ و **H**۱۰ می‌توان نتیجه گرفت که خبرگان، تمرکز اقدامات مقررات گذاری در سطح ملی و در سطح فراملی را ضروری نمی‌دانند و اقدامات فوق باید در دو ساختار و سازمان مجزا انجام شود.

فرضیه اصلی **H**٤ (برخورد قضایی و پلیسی با جرائم سایبری، تأثیر معنی‌داری بر همکاری بین‌المللی برای ارتقاء امنیت فضای مجازی دارد)

ضریب **z** بیشتر از ۱.۹٦ است (۷.۵٤٤) لذا فرضیه تأیید شده و نشان می‌دهد که این رابطه از معناداری مناسبی برخوردار است. در ذیل این فرضیه چهار فرضیه فرعی **H**۱۱ و **H**۱۲ و **H**۱۳ و **H**۱٤ مطرح‌شده‌اند:

www.SID.ir

Archive of SID



***H*۱۱**– رصد و پایش جرائم سایبری، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹۶ است (۱۰.۷٤۱) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

***H*۱۲**– شناسایی و تعقیب مجرمین سایبری، تأثیر معنی‌داری در برخورد قضایی و پلیسی با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۳.٤۷٤) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

***H*۱۳**– دستگیری و مجازات مجرمین سایبری، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۳.٤۳۱) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

***H*۱٤**– استرداد مجرمین سایبری و معاضدت قضایی، تأثیر معنی‌داری بر برخورد قضایی و پلیسی با جرائم سایبری دارد: ضریب **z** بیشتر از ۱.۹٦ است (۲.۱۹۲) لذا فرضیه تأیید شده و معناداری مناسب رابطه فوق را نشان می‌دهد.

تأثیر شاخص‌های بین‌المللی امنیت فضای مجازی (پنج‌گانه) بر مؤلفه‌های پژوهش: اثر هر یک از شاخص‌های جهانی امنیت فضای مجازی (توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت‌های دولتی و خصوصی، مشارکت‌های بین‌المللی) در تحقق زیرمؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جریم سایبری، توسط پرسشنامه سنجش شد (بر اساس طیف لیکرت) و نتایج نشان داد که شاخص‌های پنج‌گانه فوق را باید به‌عنوان ابزارهایی کارآمد، در راستای ارتقاء امنیت فضای مجازی در همکاری‌های بین‌المللی، مورداستفاده قرار داد.

## نتیجه‌گیری:

نظر به اینکه در پژوهش حاضر، ابعاد، مؤلفه‌ها و شاخص‌های مورد نظر با روشی هدفمند (نظریه‌پردازی داده بنیاد یا گراندد تئوری) احصاء و مدل مفهومی پژوهش ترسیم گردید و سپس، توسط پرسشنامه‌ای حاوی سؤال‌های بسته طبق طیف لیکرت (خیلی زیاد، زیاد، متوسط، کم و خیلی کم) جهت اخذ نظر خبرگان در خصوص صحیح بودن انتخاب عوامل احصاء شده (حذف عوامل اضافی) و سؤال‌های باز جهت اخذ نظریه تشریحی در خصوص عواملی که از سوی محقق دیده نشده و مغفول مانده خبره سنجی گردید، می‌توان ادعا نمود که نتایج پژوهش حاضر، جامع

www.SID.ir

Archive of SID



(هر چه لازم بوده، در اینجا جمع است) و مانع (از ورود موارد زائد، ممانعت به‌عمل‌آمده است) است (البته، با توجه به پیشرفت لحظه‌ای فناوری اطلاعات، گسترش روزافزون فضای سایبر و تولید لحظه‌ای هزاران مقاله علمی در سطح جهان، این ادعا می‌تواند نسبی باشد؛ زیرا محققین با نقد و بررسی یافته‌های سایر محققین و جمع‌بندی آن‌ها، نتایج جدیدی را ارائه نموده یا به عبارتی توسعه می‌دهند و با تجمیع یافته‌های محققین، تولید علم صورت می‌گیرد) لذا می‌تواند به چهار سؤال فرعی مطرح در پژوهش پاسخ داد و بر آن اساس، ضمن پاسخگویی به سؤال اصلی پژوهش، الگوی راهبردی مورد نظر را ترسیم کرد.

پاسخ سؤال فرعی اول: شاخص‌های منافع ملّی جمهوری اسلامی ایران چیست؟

طبق مبانی نظری پژوهش، شاخص‌های منافع ملی جمهوری اسلامی ایران، شناسایی و در چهار گروه کلی منافع دفاعی- امنیتی (حفظ موجودیت نظام جمهوری اسلامی، استقلال و تمامیت ارضی، قدرت ملی، وحدت ملی و امنیت ملی)، منافع بین‌المللی (ایجاد جامعه عدل اسلامی، وحدت جهان اسلام، تغییر یا اصلاح نظم و وضع بین‌المللی موجود، اعتبار بین‌المللی، عدم شکل‌گیری هژمونی منطقه‌ای رژیم صهیونیستی، برابری عملی دولت‌ها در عدالت جهانی)، منافع ایدئولوژیک (حفظ موجودیت اسلام و مذهب تشیع، حفظ ارزش‌های دینی و انقلاب اسلامی، دفاع از امت اسلامی، مبارزه با ظلم، نفی سلطه‌پذیری و سلطه‌گری، استکبارستیزی، حمایت از مستضعفین و مظلومین، عزت‌نفس و آزادی سیاسی) و منافع اقتصادی (توسعه و رفاه اقتصادی، معیشت ضروری مردم، دسترسی به سرمایه و بازار جهانی، صادرات و واردات مواد اولیه و کالاهای صنعتی) دسته‌بندی گردید.

پاسخ سؤال فرعی دوم: ابعاد و مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری چیست؟

در طی پژوهش، ابعاد و مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری، طبق ۰ شناسایی و استخراج گردید.

www.SID.ir

Archive of SID



**ابعاد، مؤلفه‌ها و زیرمؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری (محقق ساخته)**

| ابعاد | مؤلفه‌ها | زیرمؤلفه |
|---|---|---|
| پیشگیری از وقوع جرم | پیشگیری اجتماعی | تدابیر آموزشی و آگاه‌سازی عمومی (جامعه‌مدار) – امن‌سازی زیرساخت‌های فنی کشور (جامعه‌مدار) – تدریس مواد درسی مرتبط در مدارس (رشدمدار) – استمرار در اجرای برنامه‌های پیشگیری (رشدمدار) |
| | پیشگیری وضعی | افزایش تلاش برای ارتکاب جرم (ایجابی) – افزایش خطر ارتکاب جرم (ایجابی) – کاهش دستاوردها جرم (سلبی) – کاهش عوامل محرک جرم (سلبی) |
| سیاست‌گذاری و اجرا | در سطح ملی | شورای عالی فضای مجازی کشور – مراکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر) – گروه‌های واکنش هماهنگ رخداد (گوهر) – پلیس اینترپل و سایبری (فتا) |
| | در سطح فراملی | سازمان همکاری و توسعه اقتصادی (OECD) – اتحادیه بین‌المللی مخابرات (ITU) – مجمع جهانی نوآوری (IGCI) – سازمان ملل متحد (UN) – انجمن بین‌المللی حقوق جزا یونسکو (UNESCO) – اتحادیه اروپا (EU) |
| مقررات-گذاری | در سطح ملی | قانون جرائم رایانه‌ای – قانون تجارت الکترونیک– قانون دادرسی الکترونیکی |
| | در سطح فراملی | کنوانسیون جرائم سازمان‌یافته (پالرمو) کنوانسیون جرائم سایبری (بوداپست) |
| برخورد پلیسی و قضایی | رصد و پایش جرائم سایبری | ثبت رخدادهای امنیتی – جمع‌آوری و ذخیره‌سازی – تحلیل و هشدار دهی |
| | شناسایی و تعقیب مجرمین | نفوذ مبتنی بر شبکه (NIDS) –نفوذ مبتنی بر میزبان (HIDS) – نفوذ توزیع شده (DIDS) |
| | رسیدگی و مجازات | در مراجع قانونی ملی – در مراجع قانونی بین‌المللی |
| | استرداد و معاضدت قضایی | در سطح منطقه‌ای – در سطح بین‌المللی |

پاسخ سؤال فرعی سوم: شاخص‌های بین‌المللی ارتقاء امنیت فضای مجازی چیست؟

امروزه، سنجش جهانی امنیت سایبری در پنج محور اقدامات قانونی، اقدامات فنی، اقدامات سازمانی، ظرفیت‌سازی و همکاری صورت می‌گیرد (***ITU,*** ۲۰۱۷:٤) و در محور پنجم

www.SID.ir

Archive of SID



(همکاری)، پنج شاخص توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت بخش‌های دولتی و خصوصی، مشارکت‌های بین‌المللی، به‌منظور همکاری بین‌المللی برای ارتقاء امنیت سایبری، مورد توجه قرار گرفته است که شاخص‌های مورد نظر این سؤال است.

پاسخ سؤال فرعی چهارم: تأثیر شاخص‌های بین‌المللی ارتقاء امنیت فضای مجازی بر مؤلفه‌های همکاری بین‌المللی با رویکرد مبارزه با جرائم سایبری، چگونه است؟

با اتکا به نتایج نظرسنجی و تجزیه و تحلیل انجام‌شده، می‌توان ادعا نمود که شاخص‌های پنج‌گانه همکاری بین‌المللی برای ارتقاء امنیت سایبری (توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت‌های دولتی و خصوصی، مشارکت‌های بین‌المللی)، ابزارهای کارآمدی به‌منظور تحقق اهداف تک‌تک اجزا الگو خواهد بود و باید به‌صورت فراگیر جهت ارتقاء امنیت فضای مجازی در همکاری‌های بین‌المللی، مورد استفاده قرار گیرد.

ارائه الگوی راهبردی (پاسخ به سؤال اصلی):

الگو باید با توجه به جنبه‌های مفهومی (مستقیم یا غیرمستقیم)، عناصر تئوریک (روابط مفاهیم، سازه‌ها و متغیرهای مرتبط با یکدیگر به‌منظور پیش‌بینی و تبیین پدیده‌ها) و قواعد تفسیری، چارچوبی را برای طبقه‌بندی اطلاعات و سامان‌دهی منطقی اجزا و روابط ترسیم نماید (دیاری بیدگلی، ۱۳۹۳) و الگوی راهبردی نیز باید با تنظیم منطقی عوامل و مؤلفه‌های اصلی راهبردی، روابط بین آن‌ها ترسیم گردد و چگونگی دستیابی به اهداف را میسر سازد (حمیصی، ۱۳۹۱: ۱۶) .

در سال ۲۰۰۵، مدل کاربردی حلقه اودا در فضای سایبر، توسط برنادت برهمر[۱]، ارائه شد (***Brehmer,*** ۲۰۰۵:۳) و پس از ۱۰ سال (۲۰۱۵)، وینسنت لندرز و همکارانش[۲] با هدف سرعت بخشیدن به چرخه «اودا» جهت مشاهده، پردازش و واکنش سریع به رویدادها، مدل فوق را توسعه داده و چارچوب مفهومی فرماندهی و کنترل در حوزه فضای سایبری را مشتمل بر چهار مرحله مشاهده، جهت‌دهی، تصمیم‌گیری و اقدام با روابط تعاملی، نظارتی و بازخوردی برای ارتقاء امنیت فضای سایبر با رویکرد مبارزه با تهدیدات سایبری ارائه نمودند (۰) ( ***Lenders, Tanner, &*** ***Blarer,*** ۲۰۱۵) و در سال ۲۰۱۷ نیز برادران زاگر، با بهره‌گیری از مدل فوق برای دفاع سایبری در

۱ -Berndt Brehmer

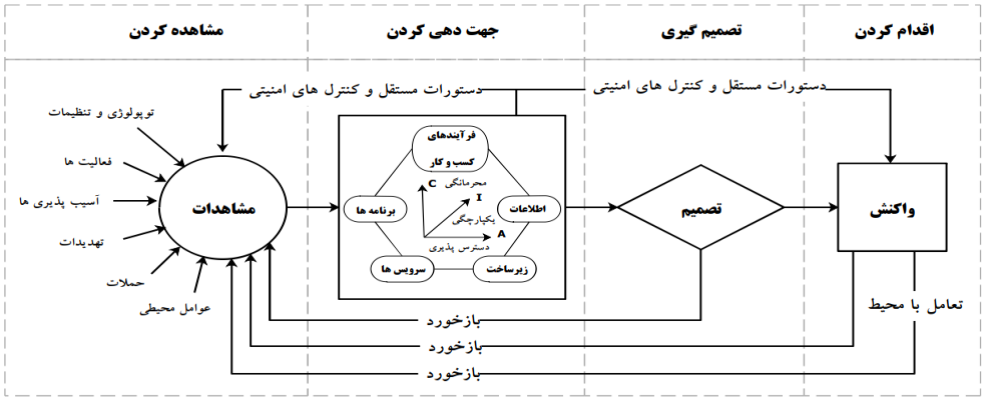
۲ -Vincent Lenders, Axel Tanner, Albert Blarer: Gaining an Edge in Cyberspace with Advanced Situational Awareness

www.SID.ir

Archive of SID



مقاله «حلقه اودا در فضای سایبر : یک مدل جدید در دفاع سایبری[۱]»، بر کاربردی بودن حلقه فوق تأکید نمودند (***Zager & Zager,*** ۲۰۱۷:۵).




: مدل وینسنت لندرز (فرماندهی و کنترل در حوزه سایبر) (**Lenders, Tanner, & Blarer,** ۲۰۱۵)

نظر به تطابق کامل مدل فوق با موضوع پژوهش حاضر، الگوی راهبردی مورد نظر بر اساس مدل لندرز در ٤ مرحله طراحی گردید (۰).

- مرحله ۱؛ مشاهده (دیده‌بانی): در مرحله نخست باید، جرائم سایبری (با ماهیت‌های سیاسی، اقتصادی، دفاعی و امنیتی، اجتماعی و فرهنگی) شناسایی و تحلیل‌های لازم برای تشخیص ماهیت، اثرات مخرب، نقاط آسیب‌پذیری، روش‌های پیشگیری و مقابله و غیره انجام شود. از طرف دیگر، باید اقدامات پیشگیرانه‌ای صورت گیرد تا وقوع جرم کاهش‌یافته و امکانات، تجهیزات و منابع کشور، پاسخگوی مبارزه با حجم زیاد جرائم سایبری باشد:
  - پیشگیری اجتماعی از وقوع جرم: با استفاده از اقدامات جامعه‌محور همانند برای ارتقاء سطح دانش و آگاهی کنونی جامعه و امن‌سازی زیرساخت‌های سایبری کشور (کوتاه‌مدت) و رشدمدار همانند تدریس مواد درسی مرتبط در مدارس و همچنین استمرار اجرای برنامه‌های پیشگیری و یا هر روش همسان دیگر، باید وقوع جرم کاهش یابد.
  - پیشگیری وضعی از وقوع جرم: با اقدامات پیشگیرانه ایجابی همانند افزایش تلاش برای ارتکاب جرم و افزایش خطر ارتکاب جرم و سلبی همانند کاهش دستاوردها جرم و کاهش عوامل محرک جرم و روش‌های همسان دیگر، زمینه‌های لازم برای وقوع جرم و عواید حاصل از آن کم شده و وقوع جرائم کاهش یابد.

۱- OODA Loops in Cyberspace: A New Cyber-Defense Model

www.SID.ir

Archive of SID



- مرحله دوم؛ جهت‌دهی (تصمیم‌سازی): در این مرحله (هسته اصلی و مغز متفکر الگو)، ضمن رعایت محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات در راستای حفظ منافع ملی جمهوری اسلامی ایران (منافع ایدئولوژیک، منافع اقتصادی، منافع دفاعی و امنیتی، منافع اقتصادی) و توجه ویژه به بهره‌گیری از توانمندی ابزارهای بین‌المللی توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت بخش‌های دولتی و خصوصی، مشارکت‌های بین‌المللی (شاخص‌های جهانی امنیت سایبری)، اطلاعات دریافتی از بخش مشاهده را مورد تجزیه و تحلیل‌ها قرار داده و ضمن اخذ نظرات، پیشنهادها و طرح‌های ضروری مورد نظر در سطح ملی و فراملی (از زیر بخش‌های سیاست‌گذاری در سطح ملی و سیاست‌گذاری در سطح فراملی) و جمع‌بندی یافته‌ها، سیاست‌های لازم جهت تنظیم مقررات قانونی و اجرایی لازم برای برخورد با جرائم سایبری تدوین و به مرحله بعد (مقررات‌گذاری) ارسال می‌کند.
  - سیاست‌گذاری و اجرا در سطح ملی: بر اساس پاسخگویی ملی به جرائم تعیین شده از سوی هسته سیاست‌گذاری الگو، سیاست‌ها (با محوریت شورای عالی فضای مجازی و مرکز ملی فضای مجازی در ذیل آن) و شیوه‌های اجرایی مبارزه با جرائم سایبری در کشور (مراکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)، گروه‌های واکنش هماهنگ رخداد (گوهر)، پلیس اینترپل، پلیس فتا و سازمان‌های همسان) را مورد بازنگری قرار گرفته و نظرات، پیشنهادها و طرح‌های ضروری جهت ارتقاء و یا تدوین سیاست‌های جدید به هسته سیاست‌گذاری الگو، عودت می‌گردد.
  - سیاست‌گذاری و اجرا در سطح فراملی: بر اساس پاسخگویی فراملی به جرائم تعیین شده، سیاست‌ها و شیوه‌های اجرایی مطرح‌شده در مذاکرات، اجلاس‌ها و همچنین ارائه شده توسط سازمان‌های بین‌المللی فعال در عرصه مبارزه با جرائم سایبری از قبیل سازمان همکاری و توسعه اقتصادی (***OECD***)، اتحادیه بین‌المللی مخابرات (***ITU***)، مجمع جهانی نوآوری (***IGCI***)، سازمان ملل متحد (***UN***)، انجمن بین‌المللی حقوق جزا، یونسکو (***UNESCO***)، اتحادیه اروپا (***EU***) و سازمان‌های همسان، مورد بازنگری قرار گرفته و نظرات، پیشنهادها و طرح‌های ضروری جهت مشارکت در مذاکرات و حضور در اجلاس‌ها در راستای حفظ و حراست از منافع ملی جمهوری اسلامی ایران در جهان، به هسته سیاست‌گذاری الگو، عودت می‌گردد.

www.SID.ir

Archive of SID



- مرحله سوم؛ تصمیم‌گیری: در این مرحله بر اساس سیاست‌های تعیین‌شده از سوی هسته سیاست‌گذاری الگو، مقررات لازم برای برخوردهای قضایی و پلیسی در سطح ملی و در سطح فراملی، تدوین می‌گردد.
  - مقررات‌گذاری در سطح ملی: بر اساس سیاست‌های تعیین‌شده از سوی هسته سیاست‌گذاری الگو، قوانین، مقررات و شیوه‌های قضایی و اجرایی کشور (قانون جرائم رایانه‌ای، قانون تجارت الکترونیک و قانون دادرسی الکترونیکی و غیره) در برخورد با جرم سایبری فوق، مورد بازنگری قرار گرفته و نظرات، پیشنهادها و طرح‌های ضروری جهت ارتقاء و یا تدوین قوانین و مقررات جدید کشور، با هسته سیاست‌گذاری الگو هماهنگ شده و نهایی می‌گردد.
  - مقررات گذاری در سطح فراملی: بر اساس سیاست‌های تعیین‌شده از سوی هسته سیاست‌گذاری الگو، مقررات و کنوانسیون‌های منطقه‌ای و بین‌المللی (کنوانسیون جرائم سازمان‌یافته (پالرمو)، کنوانسیون جرائم سایبری (بوداپست) و غیره)، مورد بازنگری دقیق قرار گرفته و نظرات، پیشنهادها و طرح‌های ضروری جهت مشارکت در کنوانسیون‌های بین‌المللی جهت اعمال‌نفوذ در راستای تنظیم مقررات منطبق با منافع ملی جمهوری اسلامی ایران، با هسته سیاست‌گذاری الگو هماهنگ شده و نهایی می‌گردد.
- مرحله چهارم؛ اقدام (واکنش): در این مرحله (نهایی)، بر اساس مقررات تعیین‌شده در بخش مقررات‌گذاری (در سطح ملی و فراملی)، برخوردهای قضایی و پلیسی با مجرمین سایبری در ٤ فرآیند به‌هم‌پیوسته انجام می‌شود:
  - رصد و پایش جرائم سایبری: این بخش را تجهیزات الکترونیکی و رایانه‌ای (سامانه و سرویس‌دهنده) خاص تشخیص، شناسایی و ذخیره‌سازی رخدادهای سایبری فضای تبادل اطلاعات و ارتباطات، تشکیل می‌دهند که به‌طور غیرمتمرکز در ارگان‌ها، سازمان‌ها، وزارتخانه‌ها و غیره نصب‌شده و بر اساس وظایف، به سه گروه تقسیم می‌گردند:
    - رخدادهای سایبری در حوزه هر سازمان، در سامانه‌ها و سرویس‌دهنده‌های همان سازمان ذخیره می‌گردد.

www.SID.ir

Archive of SID



- رخدادهای سایبری جمع‌آوری‌شده در سامانه‌ها و سرویس‌دهنده‌های سازمانی، توسط سامانه‌های کشوری جمع‌آوری‌شده و در سرویس‌دهنده‌های مرکزی کشور، ذخیره‌سازی می‌گردند.
- رخدادهای سایبری جمع‌آوری‌شده در سرویس‌دهنده‌های مرکزی توسط سامانه‌های خاص، مورد تجزیه و تحلیل و داده‌کاوی قرار گرفته و ضمن هشداردهی‌های لازم به بخش‌های دیگر، جرائم قطعی را مشخص نموده و ادله الکترونیک مربوطه را جهت شناسایی و تعقیب مجرمین، به بخش بعد ارسال می‌کند.

- شناسایی و تعقیب مجرمین: در این بخش، منشأ جرائم شناسایی‌شده (مبتنی بر شبکه (***NIDS***) و یا مبتنی بر میزبان (***HIDS***) و یا توزیع‌شده (***DIDS***)) و بر آن اساس نیز، مجرمین تحت تعقیب قرار می‌گیرند و در نهایت نیز دستگیر می‌شوند. اگر مجرمین در کشور دیگری مستقر باشند و امکان دستگیری مستقیم وجود ندارد، موارد از طریق هسته برخورد قضایی و پلیسی الگو، به بخش چهارم (استرداد و معاضدت قضایی مجرمین) ارجاع شده و موضوع از آن طریق پیگیری می‌شود.
- رسیدگی و مجازات مجرمین: مجرمین دستگیرشده در مرحله قبل را می‌توان در مراجع قانونی ملی (قوه قضائیه کشور) و مراجع قانونی بین‌المللی، رسیدگی و مجازات نمود (نظر به اینکه، فضای سایبر فاقد یک مرجع و اقتدار مرکزی در جهان است، قوانین بین‌المللی لازم در خصوص رسیدگی و مجازات جرائم سایبری در سطح بین‌الملل تدوین‌نشده است و دادگاه بین‌المللی اختصاصی ملموس نیست لذا کشورها غالباً به دنبال استرداد و یا معاضدت قضایی هستند).
- استرداد و معاضدت قضایی مجرمین: اگر مجرمین در کشورهای دیگری مستقر باشند باید، اقدامات استرداد مجرمین از طریق همکاری پلیس اینترپل کشورها انجام شود (کریمی، ۱۳۹۰) و با انعقاد توافقنامه‌های دوجانبه یا چندجانبه و معاضدت قضایی (مشارکت مراجع قضایی یک یا چند کشور در رسیدگی به جرائم) ، به جرائم رسیدگی و مجرمین مجازات گردند.

بازخوردها، نظارت و کنترل در الگوی راهبردی: در الگوی راهبردی فوق، علاوه بر روابط تعامل و همکاری در بین اجزا (پیکان‌های ضخیم مشکی‌رنگ)، روابط بازخوردی و همچنین

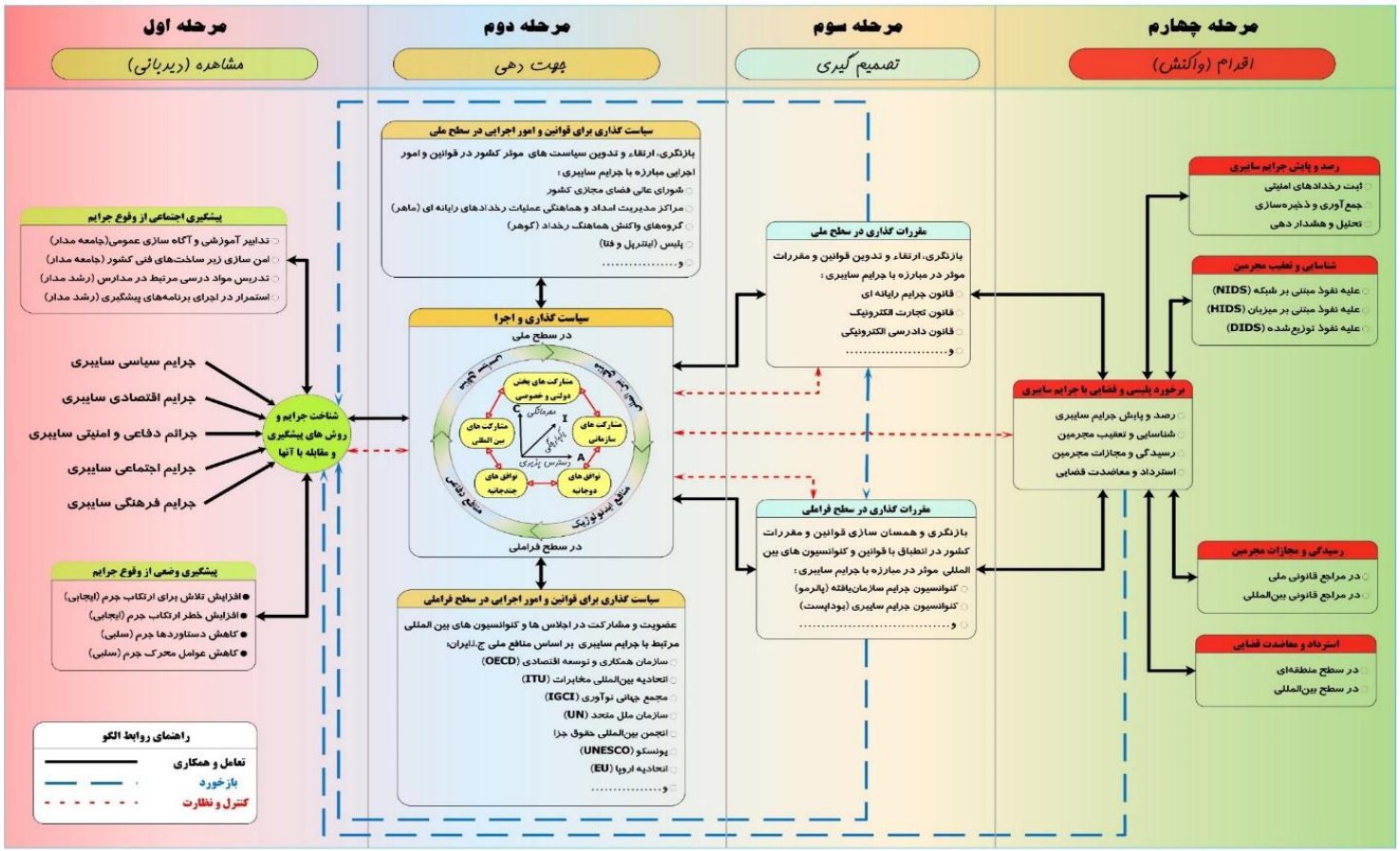
www.SID.ir

Archive of SID



نظارتی و کنترلی به‌منظور بهبود عملکرد الگو وجود دارد. بخش‌های مقررات‌گذاری در سطح ملی و فراملی، علاوه بر بازخورد نظرات، پیشنهادها و طرح‌های ضروری خود به یکدیگر جهت هماهنگی، نکات کلیدی استخراج‌شده را که می‌تواند به شناخت جرائم و روش‌های مقابله و پیشگیری از آن‌ها کمک کند، به مرحله مشاهده، بازخورد می‌نماید. با اجرایی نمودن مقررات تدوین‌شده در برخورد پلیسی و قضایی با مجرمین سایبری، اطلاعات مفیدی در خصوص نحوه وقوع جرم، نقاط مورد اثر و غیره حاصل خواهد شد شود که می‌تواند کمک شایانی به شناخت بهتر جرائم و روش‌های مقابله و پیشگیری از آن‌ها داشته باشد لذا موارد استخراج‌شده فوق به مرحله مشاهده بازخورد می‌گردد. بخش سیاست‌گذاری و اجرا، نقش محوری و مغز متفکر الگو را بر عهده دارد لذا به‌منظور هماهنگ‌سازی عملکرد بخش‌ها و به‌تبع آن بهبود سیاست‌های تدوین‌شده، عملکرد بخش‌های اصلی را تحت نظارت گرفته و اختلالات احتمالی الگو را با صدور دستورات کنترلی رفع می‌کند.

www.SID.ir




الگوی راهبردی همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران با رویکرد مبارزه با جرائم سایبری

Archive of SID
www.SID.ir

Archive of SID



بر اساس نتایج حاصل از پژوهش، پیشنهادهای زیر ارائه می‌گردد:

۱- ایجاد و بهره‌گیری از سازمان همکاری‌های بین‌المللی سایبری جمهوری اسلامی ایران به‌منظور سیاست‌گذاری و مقررات‌گذاری‌های مورد نیاز کشور در سطح بین‌المللی (این سازمان باید، کلیه اجلاس‌ها، کنوانسیون‌ها و دیگر اقدامات سایبری در سطح بین‌المللی را مورد بررسی مداوم قرار داده و مقدمات حضور کشور در آن‌ها را فراهم نماید تا همکاری‌های منطقه‌ای و بین‌المللی دوجانبه، چندجانبه و مشارکتی در حوزه سایبر شکل گیرد).

۲- تقویت توان و اختیارات مرکز ملی فضای مجازی کشور جهت کنترل و مدیریت مؤثر رخدادهای فضای مجازی کشور

۳- الگوی راهبردی فوق با محوریت شورای عالی فضای مجازی کشور پیاده‌سازی و اجرایی شود (مسلماً الگوی پیشنهادی کامل و جامع نیست بلکه می‌تواند به‌عنوان سطح صفر یا زیربنای اولیه مورد توجه قرار گیرد و با پژوهش‌های مرتبط بعد، کامل‌تر گردد).

٤- آموزش‌های همگانی در رسانه‌های ملی، مدارس، دانشگاه‌ها و مراکز آموزشی جدی گرفته شود.

۵- قانون جرائم سایبری به‌طور خاص و سایر قوانین مرتبط به‌طور عام، مورد بازنگری قرار گرفته و ابهامات و کاستی‌های آن‌ها مرتفع گردد.

در طی پژوهش، مواردی مشاهده شد که می‌تواند زمینه مطالعاتی مناسبی برای پژوهش‌های آتی باشد که به‌اختصار عبارتند از:

- اجرای پژوهش‌های توسعه‌ای- کاربردی در راستای تعیین ساختار و وظایف سازمان همکاری‌های بین‌المللی سایبری جمهوری اسلامی ایران و حوزه فعالیت آن.
- شناسایی روش‌های نوین و اثربخش پیشگیری اجتماعی و پیشگیری وضعی از وقوع جرائم سایبری.
- شناخت دقیق منافع ملی کشور در فضای مجازی و روش‌های حفظ و حراست از آن‌ها در همکاری‌های بین‌المللی.
- مطالعه تطبیقی اقدام سازمان‌های بین‌المللی در خصوص مبارزه با جرائم سایبری و ارتقاء امنیت فضای مجازی و استخراج زمینه‌های مناسب جهت مشارکت کشور در آن‌ها

www.SID.ir

Archive of SID



- مطالعه تطبیقی در خصوص شناخت روش‌های نوین برخوردهای قضایی و پلیسی با جرائم سایبری
- طراحی نظام مقابله با رخدادها و حوادث سایبری در شرایط عادی، ویژه امنیتی و جنگ.
- معماری وظایف و نگاشت نهادی ساختارهای ملی در نظام همکاری‌های بین‌المللی برای ارتقاء امنیت فضای مجازی بر اساس منافع ملی جمهوری اسلامی ایران با رویکرد مبارزه با جرائم سایبری.

www.SID.ir

Archive of SID



## منابع:


- ***قرآن کریم***
- کتب و بیانات ***حضرت امام خمینی (ره)***
- کتب و بیانات ***حضرت امام خامنه‌ای (مدظله‌العالی)***
- آذر، عادل؛ غلامزاده، رسول؛ قنواتی، مهدی؛ (۱۳۹۱)، ***مدل‌سازی مسیری - ساختاری در مدیریت***، انتشارات نگاه دانش.
- بلدی، زینب، (۱۳۹۰)، ***بررسی مسئولیت بین‌المللی دولت‌ها در قبال نقض قواعد آمره حقوق بین‌الملل***، (پایان‌نامه کارشناسی ارشد)، دانشگاه مؤسسه آموزش عالی شهید اشرفی اصفهانی.
- بهره‌مند، حمید؛ کوره‌پز حسین‌محمد؛ سلیمی، احسان؛ (۱۳۹۳)، ***راهبردهای وضعی پیشگیری از جرائم سایبری***، آموزه‌های حقوق کیفری، شماره ۷، صفحات ۱۷۶-۱٤۷.
- بهمنی، محمدرضا، (۱۳۹۳)، ***مدل سیاست‌گذاری گسترش همکاری‌های بین‌المللیِ مراکز دین‌پژوهی کشور***، راهبرد فرهنگ، شماره ۲۷.
- تقوی؛ تقی؛ محمدی، علی، (۱۳۹٤)، ***مطالعه موردی در خصوص تأثیرات مثبت و منفی شبکه‌های اجتماعی بر امنیت ملی کشورها***، مقاله ارائه شده در پدافند سایبری، پایگاه اطلاع‌رسانی پدافند سایبری کشور.
- جلالی‌فراهانی، امیرحسین، (۱۳۹۰)، ***بایسته‌های حقوق دفاع مشروع سایبری***، مقاله ارائه شده در نخستین همایش دفاع سایبری.
- حاجی ده‌آبادی، احمد؛ سلیمی، احسان، (۱۳۹۳)، ***اصول جرم‌انگاری در فضای سایبر (با رویکردی انتقادی به قانون جرائم رایانه‌ای)***، فصلنامه مجلس و راهبرد، شماره سال ۲۱ شماره ۸۰.
- حافظ‌نیا، محمدرضا، (۱۳۹۰)، ***مفهوم‌سازی ژئوپلیتیک اینترنت و فضای مجازی***، ژئوپلیتیک، شماره ۲۱.
- خانعلی‌پور؛ اجارگاه، سکینه، (۱۳۹۰)، ***پیشگیری فنی از جرم***، نشر میزان.
- خلیلی‌پور رکن‌آبادی، علی؛ نورعلی‌وند، یاسر، (۱۳۹۱)، ***تهدیدات سایبری و تأثیر آن بر امنیت ملی***، فصلنامه مطالعات راهبردی، شماره ٥٦.
- داوری، علی؛ رضازاده، آرش، (۱۳۹۲)، ***مدل‌سازی معادلات ساختاری با نرم‌افزار*** PLS، تهران: جهاد دانشگاهی.
- دیاری بیدگلی، محمدتقی؛ غفوری‌نیا، سجاد، (۱۳۹۳)، ***الگوی راهبردی قرآن در ایجاد گرایش روحی به پیامبر اکرم (ص) و اهل‌بیت (ع)***، کتاب قیم، جلد ٤، شماره ۱۱.
- رستم‌زاده، رضا؛ علیمحمدی سیابان، اصغر، (۱۳۹٥)، ***اثرات عوامل محیطی بر عملکرد بازاریابی سبز؛ مطالعه موردی: شرکت شیرین عسل***، مدیریت زنجیره ارزش.


www.SID.ir

Archive of SID




- روشندل، جلیل، (۱۳۹٤)، ***امنیت ملی و نظام بین‌المللی***، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- شاه‌محمدی، محمد؛ توحیدی‌فام، محمد، (۱۳۹۲)، ***رابطه امنیت و منافع ملی***، مطالعات حفاظت و امنیت انتظامی، شماره ۲٦.
- علیخانی، علی‌اکبر، (۱۳۹۰)، ***مبانی و اصول روابط بین‌الملل در اسلام***، پژوهش‌های روابط بین‌الملل، جلد ۱، شماره ۱.
- عیوضی، محمدرحیم؛ ترقی، علیرضا، (۱۳۹۳)، ***الگوی راهبردی مدیریت تغییرات اجتماعی در دهه آینده بر اساس اهداف و منافع ملّی جمهوری اسلامی ایران***، فصلنامه مطالعات دفاعی استراتژیک، شماره ۵۵.
- غفرانی، لیلا، (۱۳۹۱)، ***روابط بین‌الملل و سیاست خارجی مبتنی بر صلح از دیدگاه امام خمینی (ره)*** (جلد ۱، صفحه ۷)، مقاله ارائه شده در همایش ملی حقوق بین‌الملل در آیینه علوم روز.
- قاجار قیونلو، سیامک، (۱۳۹۱)، ***مقدمه حقوق سایبر***، تهران: میزان.
- کریمی، انوشیروان، (۱۳۹۰)، ***استرداد مجرمین از طریق اینترپل*** (پایان‌نامه ارشد)، دانشگاه آزاد واحد تهران مرکزی؛ دانشکده حقوق.
- کوچی، سعید، (۱۳۹۳)، ***جایگاه امنیت در فضای سایبری***، مطالعات حفاظت و امنیت انتظامی، شماره ۳۱.
- مؤمنی، منصور، (۱۳۹۲)، ***مدل‌سازی معادلات ساختاری با تأکید برسازه‌های بازتابنده و سازنده***، گنج شایگان.
- محسنین، شهریار؛ اسفیدانی، محمدرحیم، (۱۳۹۳)، ***معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی به کمک نرم‌افزار*** Smart-PLS، کتاب مهربان.
- محمد نسل، غلامرضا، (۱۳۸۷)، ***پلیس و سیاست پیشگیری از جرم***، انتشارات دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.
- مرادیان، محسن، (۱۳۸۵)، ***درآمدی بر ابعاد و مظاهر تهدیدات***، تهران: انتشارات راشا.
- ***مرکز ملی فضای مجازی***، (۱۳۹٦)، شبکه ملی اطلاعات [ملی].

- AFRICAN UNION. (۲۰۱٤). AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION. AFRICAN UNION.
- Arora, Amarpreet S. Bhatt, Susheel Ch; & Pant, Anamika. (۲۰۱۲). Forensics computing-technology to combat cybercrime. *International journal of advanced research in Computer Science and software Engineering*, ۲(۷).
- Boyd, J.R. (۱۹۸۷). *A Discourse on Winning and Losing*. The Author.
- Brehmer, Berndt. (۲۰۰۵). The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control.


www.SID.ir

Archive of SID



Presented at the ۱۰th International Command and Control Research and Technology.

- Canada; & Public Safety Canada. (۲۰۱۰). *Canada's cyber security strategy: for a stronger and more prosperous Canada.* Ottawa, Ont.: Govt. of Canada [Public Safety Canada] = Gouvernement du Canada Sécurité publique Canada.
- Dennis, Antonio; Jones, Rohan; Kildare, Duane; & Barclay, Corlane. (۲۰۱٤). A Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica. *The Electronic Journal of Information Systems in Developing Countries*.
- Dutton, Julia. (۲۰۱۷). Three pillars of cyber security – IT Governance Blog. Retrieved November ۲۷, ۲۰۱۷, from https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security/
- Federal Ministry of the Interior. (۲۰۱۱). Cyber Security Strategy for Germany. Federal Ministry of the Interior.
- GCI. (۲۰۱۱). Global Cybersecurity Index (GCI). GCI.
- Gercke, Marco. (۲۰۱۱). Understanding Cybercrime. A Guide for Developing Countries. *International Telecommunication Union (Draft)*, ۸۹, ۹۳.
- Government of Kenya. (۲۰۱٤). kenya-national-cybersecurity-strategy.pdf. Ministry of Information Communications and Technology.
- Government of the United Kingdom. (۲۰۱٦). NATIONAL CYBER SECURITY STRATEGY ۲۰۱٦-۲۰۲۱. United Kingdom: Government of the United Kingdom.
- Halaweh, Mohanad. (۲۰۱۲). Integration of grounded theory and case study: An exemplary application from e-commerce security perception research. *JITTA: Journal of Information Technology Theory and Application*, ۱۳(۱), ۳۱.
- ITU. (۲۰۱۷). Global Cybersecurity Index (GCI) ۲۰۱۷.
- Kahn, Robert E. McConnell, Mike; Nye Jr, Joseph S. Schwartz, Peter; Daly, Nova J. Fick, Nathaniel; … others. (۲۰۱۱). America's cyber future - ۱. *Center for a New American Security, Washington, DC, Tech.*
- Lenders, Vincent; Tanner, Axel; & Blarer, Albert. (۲۰۱۵). Gaining an Edge in Cyberspace with Advanced Situational Awareness. *IEEE Security & Privacy*.
- *New Zealand's Cyber Security Strategy electronic resource*. (۲۰۱۱). Wellington: New Zealand Government.
- Peritz, Aki J. & Sechrist, Michael. (۲۰۱۰). Protecting Cyberspace and the US National Interest. *Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School*.
- Schmitt, Michael N. (ed). (۲۰۱۳). *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at*

www.SID.ir

Archive of SID



*the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press.

- Senturk, Hakan; Çil, Zaim; & Sağıroğlu, Şeref. (۲۰۱۲). Cyber security analysis of turkey. *International Journal of Information Security Science*, *۱* (٤), ۱۱۲–۱۲٥.
- Tabansky, Lior. (۲۰۱۱). Basic concepts in cyber warfare. *Military and Strategic Affairs*, *۳*(۱), ۷٥–۹۲.
- Thriveni, T K; & Prashanth, C S R. (۲۰۱٤). The need for a Dynamic, Multi-layered Cloud Security. *International Journal of Recent Advances in Engineering & Technology (IJRAET)*.
- Tohme, Walid; Lindeyer, Jeremy; Harb, Imad; Papazian, Sevag; & Ghaziri, Ramzi. (۲۰۱٥). Cyber security in the Middle East. Strategy& Formerly Booz & Company.
- Trend Micro. (۲۰۱۷). Cyber Security in ۲۰۲۰. Trend Micro Incorporated.
- Wamala, Frederick. (۲۰۱۱). ITUNationalCybersecurityStrategyGuide.pdf. ITU.
- Wrange, P\a al. (۲۰۱۳). Intervention in national and private cyber space and international law.
- Zager, Robert; & Zager, John. (۲۰۱۷). OODA Loops in Cyberspace: A New Cyber-Defense Model. Small Wars Journal.

www.SID.ir