بسم الله الرحمن الرحیم

CYSP 2023

دومین کنفرانس فضای سایبر

راهنما و چکیده مقالات

02230-21686

دانشگاه تهران

۹ تا ۱۱ آبان ۱۴۰۲

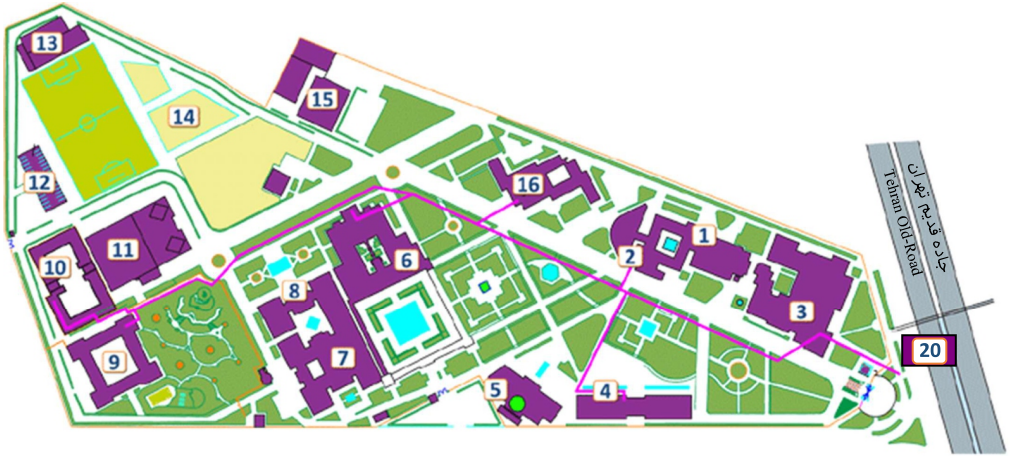
راهنما و چکیده مقالات
دومین کنفرانس ملی فضای سایبر (CYSP 2023)
برگزارکننده: دانشگاه تهران

تدوین: کاظم فولادی قلعه
با همکاری: علیرضا زینی، حسین عظیمی، محمدعلی شکوهیان‌راد

ناشر: دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
چاپ و صحافی: بوستان کتاب
تاریخ انتشار: ۸ آبان ۱۴۰۲

نشانی دبیرخانه: قم، بلوار دانشگاه، دانشکدگان فارابی دانشگاه تهران، دانشکده مهندسی
کد پستی: ۳۷۱۸۱۱۷۴۶۹
تلفن: ۰۲۵-۳۶۱۶۶۶۵۱
فکس: ۰۲۵-۳۶۱۶۶۶۵۲
ایمیل: cysp.conf@ut.ac.ir
وب‌سایت: http://cysp2023.ut.ac.ir
پیام‌رسان و شبکه‌های اجتماعی: @cysp_conf
همه‌ی پیوندها در یک جا: http://conf.cysp.ir/links

نقشه دانشکدگان
Map of College

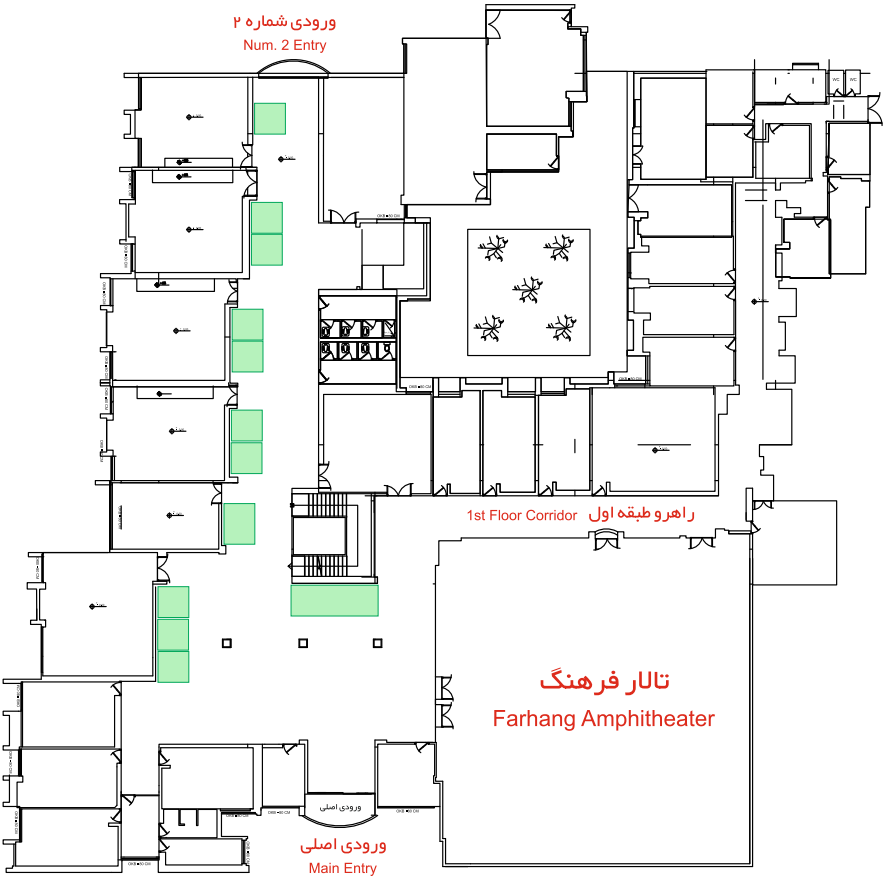


۱	سازمان مرکزی	Headquarter	1
۲	دانشکده حقوق	Faculty of Law	2
۳	دانشکده مهندسی	Faculty of Engineering	3
۴	دانشکده مدیریت و حسابداری	Faculty of Management & Accounting	4
۵	مسجد امام علی(ع)	Imam Ali Mosque	5
۶	کتابخانه مرکزی	Central Library	6
۷	سلف سرویس	Restaurant	7
۸	امور فرهنگی	Cultural Affairs	8
۹	خوابگاه حضرت معصومه(س)	Hazrat-e-Masoumeh Dorm	9
۱۰	خوابگاه حضرت زهرا(س)	Hazrat-e-Zahra Dorm	10

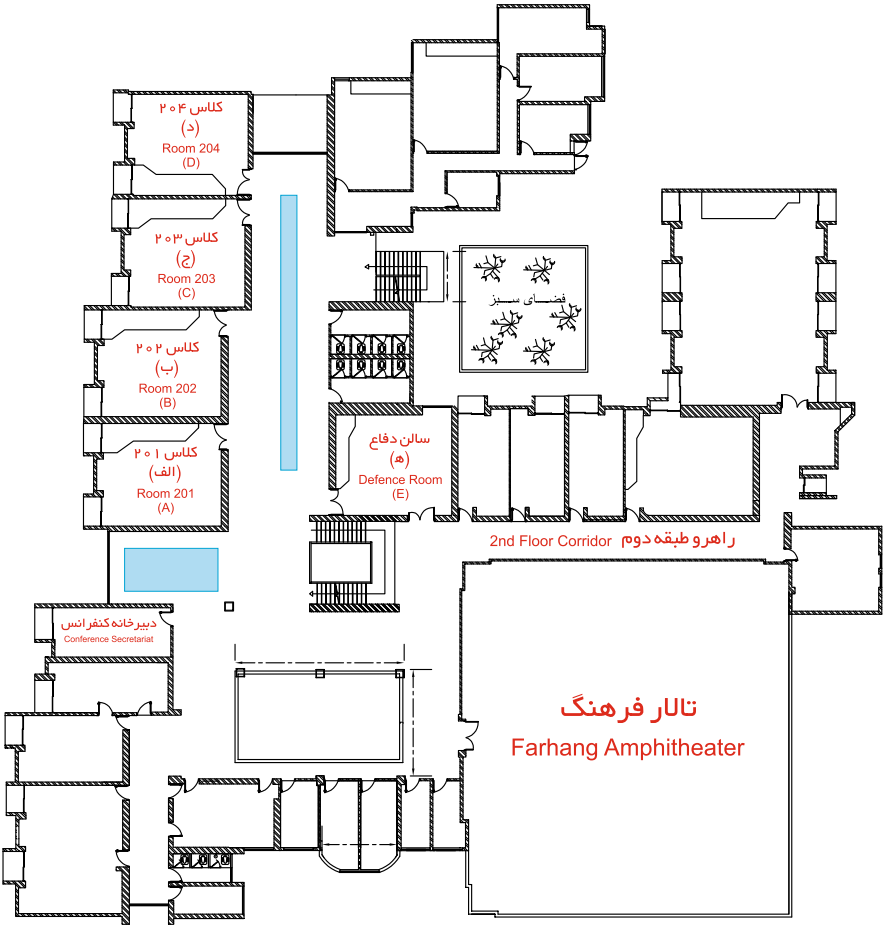
۱۱	اداره تربیت بدنی	Sport Handling	11
۱۲	اداره نقلیه	Vehicle Handling	12
۱۳	سالن ورزش	Sport Hall	13
۱۴	پارکینگ	Parking	14
۱۵	انبار	Warehouse	15
۱۶	دانشکده الهیات	Faculty of Theology	16
۱۷	خوابگاه دانش	Danesh Dorm	17
۱۸	خوابگاه اندیشه	Andisheh Dorm	18
۱۹	خوابگاه حکمت	Hekmat Dorm	19
۲۰	سر در / ورودی اصلی	Facade / Main Portal	20

CYSP 2023
The Second Conference on Cyberspace
دومین کنفرانس فضای سایبر
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

نقشه محل برگزاری برنامه و نشست‌ها
دانشکده مهندسی، طبقه اول
Floorplan, 1st Floor, Faculty of Engineering



نقشه محل برگزاری برنامه و نشست‌ها
دانشکده مهندسی، طبقه دوم
Floorplan, 2st Floor, Faculty of Engineering



CYSP 2023

THE SECOND CONFERENCE ON CYBERSPACE

دومین کنفرانس فضای سایر

۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

حامیان علمی
Scientific Sponsers

حامیان سازمانی
Organizational Sponsers

حامیان رسانه‌ای و نشر
Media & Publication Sponsers

برنامه کنفرانس

روز اول

سه‌شـــنبه ۹ آبان ۱۴۰۲						
زمان	برنامه					
۰۸:۴۵ – ۰۷:۳۰	**پذیرش**					
۰۹:۴۵ – ۰۹:۰۰	**مراسم افتتاحیه** (سالن فرهنگ)					
۱۰:۱۵ – ۰۹:۴۵	پذیرایی					
۱۱:۳۰ – ۱۰:۱۵	**سخنرانی سخنران ویژه و سخنران کلیدی** (سالن فرهنگ)					
۱۳:۰۰ – ۱۱:۳۰	ناهار و نماز					
۱۳:۳۰ – ۱۳:۰۰	**نشست ارائه مقالات پوستری** (راهروی طبقه اول)					
۱۵:۱۵ – ۱۳:۳۰	**نشست‌های تخصصی و کارگاه‌ها (۱)**					
	نشست ۱-الف (کلاس ۲۰۱)	نشست ۱-ب (کلاس ۲۰۲)	نشست ۱-ج (کلاس ۲۰۳)	نشست ۱-د (کلاس ۲۰۴)	نشست ۱-ه (سالن دفاع)	نشست ۱-و (تالار فرهنگ)
۱۵:۳۰ – ۱۵:۱۵	پذیرایی					
۱۷:۱۵ – ۱۵:۳۰	**نشست‌های تخصصی و کارگاه‌ها (۲)**					
	نشست ۲-الف (کلاس ۲۰۱)	نشست ۲-ب (کلاس ۲۰۲)	نشست ۲-ج (کلاس ۲۰۳)	نشست ۲-د (کلاس ۲۰۴)	نشست ۲-ه (سالن دفاع)	نشست ۲-و (تالار فرهنگ)

- برنامه‌ی روز اول (سه‌شنبه ۹ آبان) به‌صورت حضوری در شهر قم برگزار می‌شود.
- برنامه‌ی روز دوم (چهارشنبه ۱۰ آبان) به‌صورت مجازی و آن‌لاین برگزار می‌شود.
- برنامه‌ی روز سوم (پنجشنبه ۱۱ آبان) به‌صورت حضوری در شهر تهران برگزار می‌شود.
- محل برگزاری و جزئیات برنامه‌ی نشست‌های تخصصی و کارگاه‌ها در کانال و وب‌سایت کنفرانس درج شده است.

روز دوم و سوم

چهارشنبه ۱۰ آبان ۱۴۰۲

زمان	برنامه		
۰۸:۰۰ – ۰۹:۴۵	**نشست‌های ارائه مقالات شفاهی (۱) – مجازی**		
	نشست ۱-الف 1A	نشست ۱-ب 1B	نشست ۱-ج 1C
۰۹:۴۵ – ۱۰:۰۰	استراحت		
۱۰:۰۰ – ۱۱:۴۵	**نشست‌های ارائه مقالات شفاهی (۲) – مجازی**		
	نشست ۲-الف 2A	نشست ۲-ب 2B	نشست ۲-ج 2C
۱۱:۴۵ – ۱۳:۰۰	ناهار و نماز		
۱۳:۰۰ – ۱۴:۴۵	**نشست‌های ارائه مقالات شفاهی (۳) – مجازی**		
	نشست ۳-الف 3A	نشست ۳-ب 3B	نشست ۳-ج 3C
۱۴:۴۵ – ۱۵:۰۰	استراحت		
۱۵:۰۰ – ۱۶:۴۵	**نشست‌های ارائه مقالات شفاهی (۴) – مجازی**		
	نشست ۴-الف 4A	نشست ۴-ب 4B	نشست ۴-ج 4C
۱۶:۴۵ – ۱۸:۰۰	استراحت و نماز		
۱۸:۰۰ – ۱۹:۴۵	**نشست‌های ارائه مقالات شفاهی (۵) – مجازی**		
	نشست ۵-الف 5A	نشست ۵-ب 5B	نشست ۵-ج 5C

پنجشنبه ۱۱ آبان ۱۴۰۲

زمان	برنامه		
۰۸:۰۰ – ۰۹:۴۵	**نشست‌های تخصصی و کارگاه‌ها (۳)**		
	نشست ۳-الف 3A	نشست ۳-ب 3B	نشست ۳-ج 3C
۰۹:۴۵ – ۱۰:۰۰	پذیرایی		
۱۰:۰۰ – ۱۱:۴۵	**نشست‌های تخصصی و کارگاه‌ها (۴)**		
	نشست ۴-الف 4A	نشست ۴-ب 4B	نشست ۴-ج 4C
۱۱:۴۵ – ۱۳:۰۰	ناهار و نماز		
۱۳:۰۰ – ۱۴:۴۵	**نشست‌های تخصصی و کارگاه‌ها (۵)**		
	نشست ۵-الف 5A	نشست ۵-ب 5B	نشست ۵-ج 5C
۱۴:۴۵ – ۱۵:۰۰	پذیرایی		
۱۵:۰۰ – ۱۷:۰۰	**مراسم اختتامیه** (باشگاه دانشجویان)		

کد نشست

1A | ۱-الف

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۸ تا ۱۰

عنوان نشست: **فضای سایبر و هوش مصنوعی (۱)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۰۴	طراحی و پیاده‌سازی یک مدل هوشمند پرسش و پاسخ برای کووید۱۹ - صادق احمد آخوندی - سعید شیری قیداری - محمدحسن شیرعلی شهرضا
۱۰۱۸	شناسایی تروریست در شبکه‌های اجتماعی به‌وسیله اطلاعات منبع‌باز - مهدی کوره‌پز - رضا شیبانی
۱۰۶۹	بهبود بازشناسایی شخص با استفاده از یادگیری انتقالی و شبکه‌های سیامی - سجاد عموئی ششکل - کاظم فولادی قلعه - حسین آقابابا
۱۰۸۴	فراسوی GPS: موقعیت‌یابی بصری، سیستم مسیریابی مقاوم به تغییرات جغراسیاسی - عارف برهانی - کاظم فولادی قلعه - احسان رزاقی‌زاده
••••	-رزرو شده- -

کد نشست

1B	۱-ب

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۸ تا ۱۰

عنوان نشست: **فضای سایبر و جنبه‌های شناختی، روانی و اجتماعی**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۳۱	واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تأکید بر بلاگرها) – محبوبه موسیوند – فائزه ساکی
۱۰۳۸	تأملی در ماهیت و معنای آسیب‌زایی فضای مجازی – محمود مختاری
۱۰۸۶	بررسی نگرش‌ها نسبت به تحولات رفتاری زیست جنسی متأثر از ابژگی زنان در فضای مجازی – حمیده حسین‌زاده – محبوبه موسیوند – شهین قربانی
۱۰۸۷	راهکارهای رسانه‌ای مقابله با رویکرد ضدفرهنگی سلاح اجتماعی جوکر – حسن ضیائی جباری – حمیدرضا حسینی دانا – بی‌بی سادات میراسماعیلی
۱۰۱۱	تصویر مقصد ایران در اینستاگرام به روایت بلاگرهای غیرایرانی سفر – ندا رضوی‌زاده

کد نشست

1C	ج-۱

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۸ تا ۱۰

عنوان نشست: **فضای سایبر، حقوق و سیاست (۱)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۲۰	بررسی قانون‌گذاری هوش مصنوعی در جهان و ایران با تکیه بر مدل چندذی‌نفعی جهانی – علیرضا فخررحیمی – فربود تیموری
۱۰۲۷	جایگاه شبکه ملی اطلاعات در ایران بر اساس حقوق بین‌المللی ارتباطات – سید محمد علی مرتضوی شاهرودی
۱۰۵۲	توسل حق دفاع مشروع در حملات سایبری در حقوق بین‌الملل – مهدی کوره‌پز – رضا شیبانی
۱۰۵۵	اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل – سید حسین علوی – محمدرضا حسینی – مهراب رامک
۱۰۶۲	تبیین فضای سایبری و پیامدهای اجتماعی ناشی از آن در سیاست جنایی ایران – سودا آقامحمدزاده

کد نشست

۲-الف | 2A

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۰ تا ۱۲

عنوان نشست: **فضای سایبر و امنیت تکنیکی (۱)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۰۱	Improving Cybersecurity Systems Using Artificial Intelligence Techniques - *Ismail A. Humied*
۱۰۰۵	ارزیابی چالش‌های امنیت سایبری در محیط‌های واقعیت مجازی VR - علی ملک‌لی
۱۰۱۰	یک روش کارا جهت شناسایی حملات سیبل در شبکه‌های بین خودرویی - زهرا حرآبادی فراهانی
۱۰۱۲	ارتقای امنیت سیستم بانکی با استفاده از فناوری بلاک‌چین و رایانش ابری - رضا مدنی
۱۰۴۰	تشخیص میزان خطر امنیتی برنامه‌های موبایل با استفاده از مفهوم آنتروپی - محمود دی‌پیر - تکتم ذوقی

کد نشست

2B | ۲-ب

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۰ تا ۱۲

عنوان نشست: **فضای سایبر، امنیت ملی و دفاع سایبری**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۳۰	مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی - محمدرضامرادی - محمدرضا ولوی - متین مرادی
۱۰۵۰	کاربرد جنگ سایبری در جنگ‌های آینده - سجاد سلطانی رضایی سیر
۱۰۷۹	ابزارهای جنگ شناختی و راه‌کارهای مقابله با آن در حوزه سایبرنتیک - محمود اعتصامی فر
••••	-رزرو شده- -
••••	-رزرو شده- -

کد نشست

2C | ج-۲

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۰ تا ۱۲

عنوان نشست: **فضای سایبر و فلسفه (۱)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۰۲	تأملی بر نحوه‌ی وجود سایبر - احسان کیان‌خواه
۱۰۲۹	بازخوانی کارکرد دوسویه قوه خیال در سلطه‌ی سایبری بر مبنای علم النفس فلسفی - زهرا حبیبیان - عذرا جعفری موحد
۱۰۳۳	از گواهی تا باور مبتنی بر تکنولوژی: بررسی بر اساس تجربه‌گرایی انتقادی زمینه‌ای - محمدعلی عاشوری کیسمی
۱۰۴۹	مفهوم‌شناسی هوش دیجیتالی - مرضیه پورصالحی نویده - احمدرضا متین‌فر
••••	-رزرو شده- -

کد نشست

3A | ۳-الف

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۳ تا ۱۵

عنوان نشست: **فضای سایبر و هوش مصنوعی (۲)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۷۵	تشخیص وب‌سایت‌های اسپم فارسی با استفاده از پردازش زبان طبیعی - صبا حیدری‌دوست - امیرحسین کیهانی‌پور
۱۰۸۸	ارزیابی دادگان تجمیع رتبه‌بندی نتایج جستجو از منظر گراف - فاطمه پاک مهر - امیرحسین کیهانی‌پور
۱۰۸۹	بررسی و تحلیل دادگان تشخیص صفحات اسپم درمحیط وب بر اساس نظریه گراف - مهدیه رعیتی - امیرحسین کیهانی‌پور
۱۱۰۳	ارائه روشی برای تشخیص اجتماع در شبکه‌های پیچیده با الگوریتم بهینه‌سازی خرگوش‌های مصنوعی - آرش هدایتی - محسن محمودی
••••	-رزرو شده- -

کد نشست

3B	۳-ب

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۳ تا ۱۵

عنوان نشست: **فضای سایبر و امنیت تاکتیکی**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۱۷	راهبردهای مواجهه با فناوری‌های نوظهور از منظر امنیت سایبری - محمدحسن فرخی - خداداد هلیلی
۱۰۲۵	راه‌اندازی یک واحد پایش امنیت چابک در شرکت‌ها و سازمان‌ها - محمدمهدی قاسمی‌نیا - محمدحسن میرعارفین - حسین مرادی
۱۰۷۲	ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها - بهمن جهانی - سید نصیب‌اله دوستی‌مطلق
••••	-رزرو شده- -
••••	-رزرو شده- -

کد نشست

3C	۳-ج

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۳ تا ۱۵

عنوان نشست: **فضای سایبر و فلسفه (۲)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۵۸	پیشنهاد ریشه‌شناسی جدید برای مفهوم سایبر با استفاده از روش زبان‌شناسی تاریخی - محمد شمس‌الدینی - کاظم فولادی قلعه
۱۰۶۸	زندگی در ناواقعیتِ ماتریکس و فضای سایبری - مرتضی سعیدی ابواسحاقی - راضیه سعیدی ابواسحاقی
۱۰۷۰	تبیین نظری مؤلفه‌های نظام سایبرنتیک ومقایسه آن با مؤلفه‌های نظام ولایت - رضوان هامانی - زهرا حصارکی
۱۰۹۲	پیشرفت مطلق یا هدفمند هوش مصنوعی در اندیشه مقام معظم رهبری - حمید محسنی - کاظم فولادی قلعه
....	-رزرو شده- -

کد نشست

۴-الف | 4A

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۵ تا ۱۷

عنوان نشست: **فضای سایبر و فناوری‌های نو**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۰۶	تأثیر فناوری واقعیت افزوده در تعامل با محیط زیست - صادق عسگریلو - شکوه کرمانشاهانی
۱۰۰۷	آموزش زبان خارجی با کمک فناوری واقعیت افزوده - سونیا مظفری - حمیدرضا حمیدی
۱۰۱۵	اهمیت و کاربرد تحلیل کلان‌داده‌های زیرساخت ارتباطی-مخابراتی در کشور - احسان ترکمان منش
۱۰۳۹	چالش‌های رفتاری به‌کارگیری کلان‌داده در فضای سایبر - سید کمال واعظی - فرانک پاشایی
۱۰۴۵	مدیریت داده‌های پزشکی با کمک زنجیره بلوکی - زهرا امین مهر - فضل الله ادیب نیا

کد نشست

4B	۴-ب

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۵ تا ۱۷

عنوان نشست: **فضای سایبر و حکمرانی**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۱۴	تبیین حکمرانی فضای سایبر، با تکیه بر جایگاه قوای شناختی و مسئله معرفت - محسن ابراهیمی
۱۰۱۹	تأثیر حکمرانی داده بر کارآمدی هزینه‌کرد بودجه در پروژه‌ها - علیرضا فخررحیمی - فربود تیموری
۱۰۲۸	ارائه الگوی به‌کارگیری رسانه‌های اجتماعی در ارتقای روابط عمومی (مورد مطالعه: شهرداری نهاوند) - مریم کرمعلی - علی جعفری
۱۰۶۳	بررسی نقش و تاثیر قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی - محمدرضا حسینی - مهراب رامک - احسان کیان‌خواه - سید حسین علوی
۱۰۹۸	نسبت قلمرو حکمرانی با فضای سایبر - علی لکزائی - کاظم فولادی قلعه

کد نشست

4C	ج-۴

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۵ تا ۱۷

عنوان نشست: **فضای سایبر و دین**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۲۶	طراحی الگوریتم استدلال، اولویت گام دوم در ارتقای علوم اسلامی - محمدحسن احمدی
۱۰۳۴	دلیل عقلی جرم‌انگاری سایبری مبتنی بر قاعده اعانت بر اثم - محسن نادری - علی‌اکبر ایزدی فرد - محمدمهدی زارعی
۱۰۸۵	بررسی مسئولیت کاربران در فضای مجازی بر اساس قاعده اقدام - سیدرضا چوگان سنبل - مهدی طالبی چاهوکی
۱۱۰۵	نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر - محمدعلی عبدالهی - مسلم طاهری کل کشوندی - عاطفه اندرزا
۱۱۰۷	رویکرد فقهی به جامه‌شناسی پیام، با نگاهی به اینستاگرام - ابوالفضل امامی میبدی - مجتبی شیخی ده‌آبادی - مصطفی میرزایی فیروزآبادی

کد نشست

5A	۵-الف

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۸ تا ۲۰

عنوان نشست: **فضای سایبر و امنیت تکنیکی (۲)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۴۳	Image Hashing Algorithm: An Analysis and Improvement - *Seyed Amirhossein Tabatabaei*
۱۰۹۱	مطالعه‌ی ابزارهای برتر شنود شبکه و مقایسه کاربردی Wireshark و Cain and Abel - سارا سعادت - هایده باقری پور
۱۱۰۲	مدل‌سازی رفتاری مصرف منابع در بخش رمزنگاری فایل‌ها در باج‌افزارها - مهران گرمه - رجبعلی سجادیان فر - محمد شاه‌پسندی
۱۱۰۸	تشخیص بدافزارهای اندرویدی با استفاده از روش یادگیری ترکیبی پشته‌ای - مونا زارع - علیرضا رضوانیان
....	-رزرو شده- -

کد نشست

5B	۵-ب

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۸ تا ۲۰

عنوان نشست: **سایبرنتیک و کاربردهای آن**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۹۶	سایبودینامیک، قوانین جریان اطلاعات در چرخه‌ی سایبرنتیک - محمدعلی شکوهیان‌راد - سمانه کاتبی کوشالی
۱۱۱۱	نقش میدان‌های الکترومغناطیس درون‌زاد و برون‌زاد در پیشبرد تکوین جنین - سمیرا کاتبی کوشالی
۱۱۱۲	بازتعریف مفهوم شناخت و کارکردهای آن با رویکرد سایبرنتیکی - محمدعلی شکوهیان‌راد
۱۱۱۳	تغییرات اقلیمی، ابر پروژه‌ای برای کنترل جهان - عاطفه نصیری
••••	-رزرو شده- -

کد نشست

5C	۵-ج

چهارشنبه ۱۰ آبان ۱۴۰۲؛ ساعت ۱۸ تا ۲۰

عنوان نشست: **فضای سایبر، حقوق و سیاست (۲)**

کد مقاله	عنوان مقاله و نویسندگان
۱۰۰۸	بررسی تأثیر فناوری متاورس بر دگرگونی سنت روابط سیاسی کشورهای حاضر در ساختار نظام بین‌الملل - امید نوری - محمد لعل علیزاده
۱۰۸۲	شناسایی مالکِ داده‌ها در «هوش مصنوعی» و «اینترنت اشیاء» - محمد امینی - محمود رستگاری - سعید نصر
۱۰۹۹	مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب - علی عرب نجف‌آبادی
۱۱۰۹	حق دسترسی به فضای سایبری در تکوین افکار عمومی - ندا رستگاران - عبدالحمید فرزانه - روح الله رحیمی - مهدی شیخ موحد
••••	-رزرو شده- -

کد نشست

1P	۱-پ

نشست:

نشست پوستر

کد مقاله	عنوان مقاله و نویسندگان
۱۰۲۱	استراتژی تحول دیجیتال پارلمان در مسیر شفافیت و دموکراسی - یاشار ابری - احمد فرید اصیل
۱۰۲۳	بررسی و شناسایی کاربردهای فناوری بلاک‌چین و رمزارزها در حوزه‌ی هنرهای تجسمی دیجیتال و بازارهای مالی هنر در ایران - مهدی نصیری
۱۰۲۴	Vulnerability Analysis of Social Media Accounts Against Cyber Attacks *- Ahamd Farid Aseel - Yashar Abri*
۱۰۳۵	بررسی امکان جرم‌انگاری جرایم مرتبط با اعانت بر اثم در فضای مجازی - محسن نادری - علی‌اکبر ایزدی فرد - محمدمهدی زارعی
۱۰۳۷	اثر آموزش سواد رسانه‌ای بر هویت ملی - علیرضا بخشایش - مریم بابایی
۱۰۴۱	چالش‌های اجتماعی و امنیتی در توسعه متاورس - جمشید نصرت آبادی - مجید سلیمانی ساسانی - امیرمحمدشیرخدا
۱۰۵۱	اکوسیستم متاورس با محوریت جرائم مالی در آن - عباس ترکاشوند - رضا مالکی پور
۱۰۸۳	تشخیص نفوذ در امنیت سایبری به کمک یادگیری ماشین - سید محمد جواد نصراله
۱۱۰۰	پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری - علیرضا رضوانیان - سید مهدی وحیدی پور
۱۱۰۱	سایبرنتیک دروازه نوگشوده علم و تکنولوژی - زهرا بیگلری - زهرا عزتی نیا
۱۱۱۰	نیهلیسم فضای سایبری در همسخنی با نیچه - مرتضی سعیدی ابواسحاقی - راضیه سعیدی ابواسحاقی

اعضای کمیته اجرائی

۱. **دکتر حمید زارع**، دانشیار، رئیس دانشکدگان فارابی دانشگاه تهران: رئیس کنفرانس
۲. **دکتر کاظم فولادی قلعه**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: دبیر علمی
۳. **دکترامیرحسین کیهانی‌پور**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: دبیر اجرایی
۴. **دکتر احمد علی‌نژاد**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول نشست‌ها و کارگاه‌ها
۵. **مهندس محمدعلی شکوهیان‌راد**، پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران و مدرس مدعو دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول ارتباطات

همکاران کمیته اجرائی

۱. **مهندس علیرضا زینی**، دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران: مسئول امور مقالات
۲. **علیرضا میرزایی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول هماهنگی
۳. **مهندس محمدجواد خدمتی**، دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران: مسئول امور رسانه و خبرگزاری
۴. **مهدی حسومی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول پخش زنده اینترنتی
۵. **مهدی امامی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور چندرسانه‌ای
۶. **محمدحسین فرهادیان**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول تدوین ویدئویی
۷. **امیرحسین نصراللهی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور گرافیک
۸. **سجاد شکوه مسقانی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور نمایشگاه جانبی
۹. **سید محمدمهدی حسینی رکن‌آبادی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور پذیرش و تشریفات

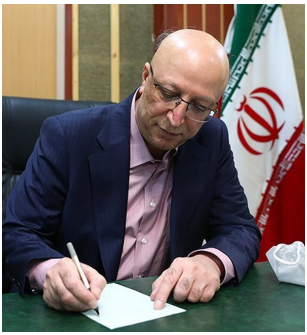
اعضای کمیته علمی

۱. **دکتر حسین آقابابا**، دانشیار، دانشگاه تهران
۲. **دکتر مهرنوش ابوذری**، استادیار، دانشگاه تهران
۳. **دکتر مهشید التماسی**، استادیار، دانشگاه تهران
۴. **دکتر سروناز تربتی**، استادیار، دانشگاه آزاد اسلامی
۵. **دکتر فاطمه ثقفی**، دانشیار، دانشگاه تهران
۶. **دکتر سید محمدباقر جعفری**، دانشیار، دانشگاه تهران
۷. **دکتر امیر جلالی بیدگلی**، استادیار، دانشگاه قم
۸. **دکتر حامد جلالی بیدگلی**، استادیار، دانشگاه صنعتی اصفهان
۹. **دکتر مهدی چم‌پور**، استادیار، دانشگاه صنعتی قوچان
۱۰. **دکتر محسن حاجی زین‌العابدینی**، استادیار، دانشگاه شهید بهشتی
۱۱. **دکتر سید احمد حبیب‌نژاد**، دانشیار، دانشگاه تهران
۱۲. **دکتر رحیم خانی‌زاد**، استادیار، دانشگاه علم و صنعت ایران
۱۳. **دکتر سید نصیب‌اله دوستی مطلق**، استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
۱۴. **دکتر مهدی ذاکری**، دانشیار، دانشگاه تهران
۱۵. **دکتر سعید روحانی**، دانشیار، دانشگاه تهران
۱۶. **دکتر محمدجواد شایگان‌فرد**، دانشیار، دانشگاه علم و فرهنگ
۱۷. **دکتر محمدحسن شیرعلی شهرضا**، استادیار، دانشگاه صنعتی امیرکبیر
۱۸. **دکتر سجاد شیرعلی شهرضا**، استادیار، دانشگاه صنعتی امیرکبیر
۱۹. **دکترمحمدحسین ظریفیان یگانه**، استادیار، دانشگاه تهران
۲۰. **دکتر سید سعیدرضا عاملی رنانی**، استاد، دانشگاه تهران
۲۱. **دکتر محمدعلی عبداللهی**، دانشیار، دانشگاه تهران
۲۲. **دکتر سید امید فاطمی**، دانشیار، دانشگاه تهران
۲۳. **دکتر کاظم فولادی قلعه**، استادیار، دانشگاه تهران
۲۴. **دکتر محمد کاشانی‌پور**، دانشیار، دانشگاه تهران
۲۵. **دکتر مسعود کوثری**، دانشیار، دانشگاه تهران
۲۶. **دکتر مهدی کارگهی**، استاد، دانشگاه تهران
۲۷. **دکتر محمدرضا کریمی قهرودی**، استادیار، دانشگاه صنعتی مالک اشتر
۲۸. **دکتر علی‌اصغر کیا**، استاد، دانشگاه علامه طباطبائی
۲۹. **دکتر امیرحسین کیهانی‌پور**، استادیار، دانشگاه تهران
۳۰. **دکتر احمد محمودی ازناوه**، استادیار، دانشگاه شهید بهشتی
۳۱. **دکتر محمود مختاری**، استادیار، دانشگاه شهید بهشتی

۳۲. **دکتر زهرا موحدی**، استادیار، دانشگاه تهران
۳۳. **دکتر عبدالرضا نوروزی چاکلی**، استاد، دانشگاه شاهد
۳۴. **دکتر خداداد هلیلی**، استادیار، دانشگاه علوم و فنون هوایی شهید ستاری
۳۵. **Dr. Christoph Stückelberger**، Professor، University of Basel

پیام وزیر علوم، تحقیقات و فناوری

به‌مناسبت برگزاری نخستین «کنفرانس فضای سایبر»



دکتر محمدعلی زلفی‌گل

۹ آبان ۱۴۰۱

بسم الله الرحمن الرحیم

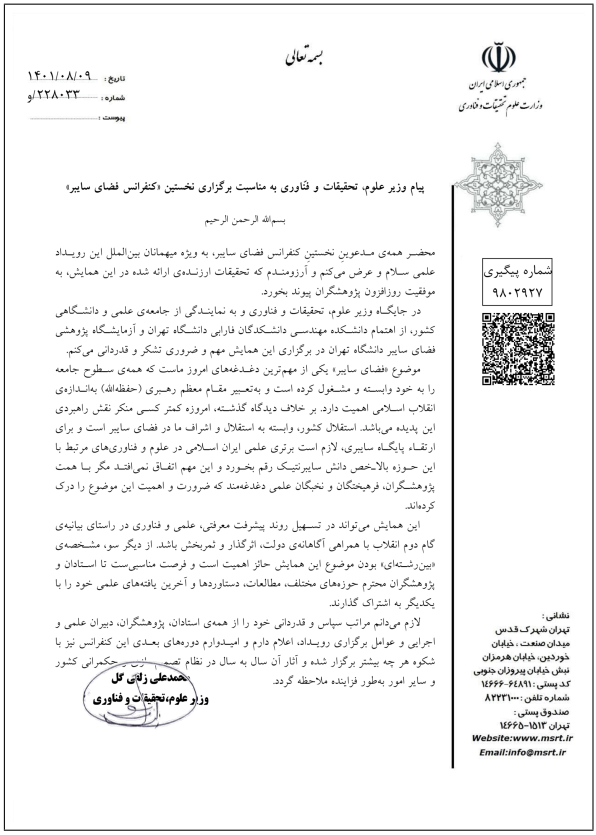
محضر همه‌ی مدعوین نخستین کنفرانس فضای سایبر، به ویژه میهمانان بین الملل این رویداد علمی سلام عرض می‌کنم و آرزومندم که تحقیقات ارزنده‌ی ارائه شده در این همایش، به موفقیت روزافزون پژوهشگران پیوند بخورد.

در جایگاه وزیر علوم، تحقیقات و فناوری و به نمایندگی از جامعه‌ی علمی و دانشگاهی کشور، از اهتمام دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران و آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران در برگزاری این همایش مهم و ضروری تشکر و قدردانی می‌کنم.

موضوع «فضای سایبر» یکی از مهم‌ترین دغدغه‌های امروز ماست که همه سطوح جامعه را به خود وابسته و مشغول کرده است و به تعبیر مقام معظم رهبری «حفظه الله» به اندازه‌ی انقلاب اسلامی اهمیت دارد. بر خلاف دیدگاه گذشته، امروزه کمتر کسی منکر نقش راهبردی این پدیده می‌باشد. استقلال کشور، وابسته به استقلال و اشراف ما در فضای سایبر است و برای ارتقاء پایگاه سایبری، لازم است برتری علمی ایران اسلامی در علوم و فناوری‌های مرتبط با این حوزه بالا-خص دانش سایبرنتیک رقم بخورد و این مهم اتفاق نمی‌افتد مگر با همت پژوهشگران، فرهیختگان و نخبگان علمی دغدغه‌مند که ضرورت و اهمیت این موضوع را درک کرده‌اند.

این همایش می‌تواند در تسهیل روند پیشرفت معرفتی، علمی و فناوری در راستای بیانیه‌ی گام دوم انقلاب با همراهی آگاهانه‌ی دولت،اثرگذار و ثمربخش باشد. از دیگر سو، مشخصه‌ی «بین رشته‌ای» بودن موضوع این همایش حائز اهمیت است و فرصت مناسبی‌ست تا استادان و پژوهشگران محترم حوزه‌های مختلف، مطالعات، دستاوردها و آخرین یافته‌های علمی خود را با یکدیگر به اشتراک گذارند.

لازم می‌دانم مراتب سپاس و قدردانی خود را از همه‌ی استادان، پژوهشگران، دبیران علمی و اجرایی و عوامل برگزاری رویداد، اعلام دارم و امیدوارم دوره‌های بعدی این کنفرانس نیز با شکوه هر چه بیشتر برگزار شده و آثار آن سال به سال در نظام تصمیم‌سازی و حکمرانی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.



بسمه تعالی

جمهوری اسلامی ایران
وزارت علوم تحقیقات و فناوری

تاریخ: ۱۴۰۱/۰۸/۰۹
شماره: ۲۲۸۰۳۳/و
پیوست:

شماره پیگیری
۹۸۰۲۹۲۷

پیام وزیر علوم، تحقیقات و فناوری به مناسبت برگزاری نخستین «کنفرانس فضای سایبر»

بسم‌الله الرحمن الرحیم

محضر همه‌ی مدعوین نخستین کنفرانس فضای سایبر، به ویژه میهمانان بین‌الملل این رویداد علمی سلام و عرض می‌کنم و آرزومندم که تحقیقات ارزنده‌ی ارائه شده در این همایش، به موفقیت روزافزون پژوهشگران پیوند بخورد.

در جایگاه وزیر علوم، تحقیقات و فناوری و به نمایندگی از جامعه‌ی علمی و دانشگاهی کشور، از اهتمام دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران و آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران در برگزاری این همایش مهم و ضروری تشکر و قدردانی می‌کنم.

موضوع «فضای سایبر» یکی از مهم‌ترین دغدغه‌های امروز ماست که همه‌ی سطوح جامعه را به خود وابسته و مشغول کرده است و به‌تعبیر مقام معظم رهبری (حفظه‌الله) به‌اندازه‌ی انقلاب اسلامی اهمیت دارد. بر خلاف دیدگاه گذشته، امروزه کمتر کسی منکر نقش راهبردی این پدیده می‌باشد. استقلال کشور، وابسته به استقلال و اشراف ما در فضای سایبر است و برای ارتقاء پایگاه سایبری، لازم است برتری علمی ایران اسلامی در علوم و فناوری‌های مرتبط با این حوزه بالاخص دانش سایبرنتیک رقم بخورد و این مهم اتفاق نمی‌افتد مگر با همت پژوهشگران، فرهیختگان و نخبگان علمی دغدغه‌مند که ضرورت و اهمیت این موضوع را درک کرده‌اند.

این همایش می‌تواند در تسهیل روند پیشرفت معرفتی، علمی و فناوری در راستای بیانیه‌ی گام دوم انقلاب با همراهی آگاهانه‌ی دولت، اثرگذار و ثمربخش باشد. از دیگر سو، مشخصه‌ی «بین‌رشته‌ای» بودن موضوع این همایش حائز اهمیت است و فرصت مناسبی‌ست تا استادان و پژوهشگران محترم حوزه‌های مختلف، مطالعات، دستاوردها و آخرین یافته‌های علمی خود را با یکدیگر به اشتراک گذارند.

لازم می‌دانم مراتب سپاس و قدردانی خود را از همه‌ی استادان، پژوهشگران، دبیران علمی و اجرایی و عوامل برگزاری رویداد، اعلام دارم و امیدوارم دوره‌های بعدی این کنفرانس نیز با شکوه هر چه بیشتر برگزار شده و آثار آن سال به سال در نظام تصمیم‌سازی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.

محمدعلی زلفی گل
وزیر علوم، تحقیقات و فناوری

نشانی:
تهران شهرک قدس
میدان صنعت، خیابان
خوردین، خیابان هرمزان
نبش خیابان پروزان جنوبی
کد پستی: ۱۴۶۶۶-۶۴۸۹۱
شماره تلفن: ۸۳۲۳۱۰۰۰
صندوق پستی:
تهران ۱۵۱۲-۱۴۶۶۵
Website:www.msrt.ir
Email:info@msrt.ir

سخن دبیر علمی

دکتر کاظم فولادی قلعه

عضو هیئت علمی دانشگاه تهران
سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

قرن جدید هجری شمسی را در شرایطی آغاز کردیم که دنیا موقعیت‌های بسیار متفاوتی را تجربه می‌کند و بدون شک بخش مهمی از این تفاوت‌ها متأثر از گسترش نفوذ فضای سایبر در جهان و اثرگذاری عمیق آن بر بیشتر جنبه‌های زندگی فردی و اجتماعی بشر است. اکنون می‌توانیم ادعا کنیم که «نظم جدید جهان» بدون شک وابسته به مقوله‌ی «فضای سایبر» است.

فضای سایبر، فضایی است که اطلاعات در آن به گردش در می‌آید؛ اما این گردش اطلاعات به‌صورت هدفمند و جهت‌مند انجام می‌گیرد و این تعبیر، همان چیزی است که در اصطلاح علمی به آن «کنترل» گفته می‌شود. بر این اساس، فضای سایبر، به‌عنوان فضایی که در آن نوعی کنترل رقم می‌خورد، درک می‌شود. این مهم‌ترین و ذاتی‌ترین ویژگی این فضاست که البته در ادبیات عمومی و علمی ما کمتر بدان توجه شده است و باعث شده است جنبه‌ی «مجازی» بودن این فضا در افکار عمومی برجسته‌تر جلوه کند. البته توجه به این نکته نیز مهم است که در اینجا مجازی (virtual) در مقابل واقعی نیست و مجازی بودن به نوعی واقعیت ناملموس اشاره دارد که در برابر واقعیت ملموس (actual) تعریف می‌شود.

فضای سایبر، مبتنی بر دانش «سایبرنتیک» شکل گرفته است. به‌طور ساده، دانش سایبرنتیک، دانش سلطه و حاکمیت است و این حاکمیت از طریق روش «کنترل» محقق می‌شود. بر این اساس، فضای سایبر را می‌توان یک قلمروی حاکمیتی دانست که هر پدیده‌ای که به آن وارد می‌شود، تحت نوعی سلطه از جنس کنترل قرار می‌گیرد. برای شکل‌گیری کنترل، باید متغیر کنترل در اختیار کنترل‌کننده قرار گیرد و بدیهی است که هر

نوع متغیر نیازمند دانش اختصاصی خود برای شیوه‌ی کنترل آن خواهد بود. شاخه‌های کاربردی دانش سایبرنتیک بر اساس انواع مختلف متغیرهای کنترل به جزئیات این موضوع می‌پردازند و آنها را به‌طور عمومی با عنوان X-cybernetics نامگذاری می‌کنیم که در آن X متغیر کنترل (کنترل‌کننده یا کنترل‌شونده) است. البته دانش‌های سایبری که با قالب کلی Cyber-X از آنها یاد می‌کنیم، شناخته‌شده‌تر هستند، چرا که این هدف دانش‌ها موضوع X است که در طبقه‌بندی متداول علوم به آن پرداخته شده است و صرفاً از ظرفیت «سایبر» برای هدف X استفاده می‌شود.

تنوع متغیرهای کنترل باعث می‌شود که طیف وسیعی از دانش‌ها در دامنه‌ی دانش سایبرنتیک واقع شوند یا به آن مرتبط شوند و به‌همین دلیل مطالعات بین رشته‌ای به‌صورت یک خصلت ذاتی در پژوهش‌های مرتبط با موضوع فضای سایبر و دانش پایه‌ی آن، یعنی دانش سایبرنتیک، شمرده می‌شود.

این کنفرانس قصد دارد زمینه‌ای را فراهم کند که مطالعات بین‌رشته‌ای بلکه فرارشته‌ای فضای سایبر به‌صورت منسجم شکل بگیرد و در قالب یک جریان علمی مؤثر و مفید به حرکت خود ادامه بدهد. برگزاری موفق نخستین دوره‌ی این کنفرانس در آبان ۱۴۰۱ و دستاوردهای آن انگیزه‌بخش پژوهشگران و دغدغه‌مندان موضوع این کنفرانس شد و به لطف الهی توفیق داریم دومین دوره‌ی این کنفرانس را در تاریخ ۹ الی ۱۱ آبان ۱۴۰۲ برگزار کنیم و امیدواریم برگزاری سالانه‌ی این کنفرانس هر چه بیشتر ما را به اهداف مشخص شده‌ی این رویداد نزدیک و نزدیک‌تر کند.

به‌علاوه، با توجه به رشد اهمیت فضای سایبر و کاربردهای آن، وسعت فراگیری و چالش‌های نوظهور حاکمیتی آن، ضرورت بررسی علمی ابعاد مختلف این پدیده در محیط دانشگاهی و هم‌اندیشی اندیشمندان مرتبط، بیش از پیش حس می‌شود. به‌همین منظور، دومین کنفرانس ملی فضای سایبر توسط دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران با محوریت «آزمایشگاه پژوهشی فضای سایبر» برگزار می‌شود. این کنفرانس محلی برای ارائه‌ی آخرین یافته‌های پژوهشگران و مباحثه پیرامون ایده‌های آنها در حوزه‌ی فضای سایبر، دانش سایبرنتیک و سیستم‌های سایبرنتیکی و مسائل مرتبط با آنها می‌باشد. متخصصان و پژوهشگران برای ارائه‌ی ایده‌های جدید و آخرین دستاوردهای خود به این کنفرانس دعوت شده‌اند و تمامی موضوعات مرتبط با حوزه‌ی فضای سایبر و دانش سایبرنتیک در سطوح استراتژیکی، تاکتیکی و تکنیکی در محدوده‌ی موضوعات مورد نظر این کنفرانس قرار می‌گیرد.

در برنامه‌ی دومین کنفرانس ملی فضای سایبر علاوه بر ۱۵ نشست ارائه‌ی مقالات شفاهی و نشست ارائه‌ی مقالات پوستری برای ارائه‌ی ۷۵ مقاله پذیرفته شده، بیش از ۲۰ نشست تخصصی/ میزگرد و کارگاه آموزشی پیش‌بینی شده است که شامل موضوعات پرکاربرد و پرمخاطب مرتبط با موضوع کنفرانس است. در اینجا جا دارد علاوه بر اعضای محترم کمیته‌های علمی و اجرایی، همکاران کمیته‌ها، پژوهشگران و نویسندگان مقالات، از سازمان‌ها، نهادها و شرکت‌های حمایت‌کننده از کنفرانس نیز تشکر ویژه داشته باشیم که غنای برنامه‌های تنظیم‌شده محصول همکاری این مجموعه‌ها با دبیرخانه‌ی کنفرانس

می‌باشد.

امیدواریم توفیق پیدا کنیم دوره‌های بعدی این کنفرانس را با کیفیت هر چه بهتر در سال‌های پیش رو داشته باشیم و آثار مفید این جریان پژوهشی در نظامات معرفتی، علمی، تصمیم‌سازی و اجرایی کشور بلکه جهان دیده شود، ان‌شاءالله. ۱ آبان ۱۴۰۲

محورهای مقالات

- چارچوب نظری و مفهومی زیرساخت فضای سایبر:
  - اطلاعات: محتوا، فلسفه‌ی اطلاعات و نظریه‌ی اطلاعات
  - کنترل: تغذیه‌ی اطلاعات، کنترل مهندسی و کنترل اجتماعی
  - ارتباطات: انتقال اطلاعات، ارتباطات مهندسی و ارتباطات اجتماعی
  - محاسبات: پردازش اطلاعات، ذخیره و بازیابی اطلاعات
- تئوری سیستم‌ها و سیستم‌های سایبرنتیکی
- دانش سایبرنتیک و شاخه‌های دانش سایبرنتیک
- فلسفه‌ی فضای سایبر، دیدگاه‌های فلسفی به فضای سایبر
- سیستم‌های مدیریت اطلاعات و سیستم‌های اطلاعاتی مدیریت
- جامعه‌ی اطلاعاتی
- روابط میان فضای ویرچوآل و فضای اکچوآل
- فضای سایبر و انسان
- حکمرانی فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر، حکمرانی در فضای سایبر
- جنگ سایبری، جنگ در فضای سایبر، جنگ به‌وسیله‌ی فضای سایبر
- قدرت سایبری، فضای سایبر و حاکمیت
- فرهنگ سایبری، فضای سایبر و فرهنگ، فضای سایبر و رسانه
- اقتصاد سایبری، فضای سایبر و اقتصاد
- جرائم سایبری، فضای سایبر و قانون
- روان‌شناسی سایبری
- فضای سایبر و هوش مصنوعی، کلان‌داده‌ها و یادگیری ماشینی
- فضای سایبر و اهداف توسعه پایدار سازمان ملل متحد (SDGs)
- سیستم‌های سایبر-فیزیکی و اینترنت اشیاء، انقلاب صنعتی چهارم
- سایبرنتیک کوانتومی، فضای سایبر کوانتومی، محاسبات و ارتباطات کوانتومی
- کاربردهای سایبری
- فضای سایبر و اینترنت
- فضای سایبر و شبکه‌های اجتماعی
- امنیت سایبری، فضای سایبر و امنیت
- بلاک‌چین (زنجیره‌بلوکی)، رمزارزها، ارز دیجیتال بانک مرکزی (CBDC)
- واقعیت ویرچوآل و واقعیت افزوده، متاورس و زندگی دوم
- سایر موضوعات مرتبط

چکیده مقالات فارسی

Code: CYSP2023-1002

تأملی بر نحوه‌ی وجود سایبر

احسان کیان‌خواه[1]
[1]پژوهشگاه فرهنگ و اندیشه اسلامی
ehsan@kiankhah.com

چکیده: فضای سایبر یا به تعبیر دیگر فضای مجازی با شتاب هیجان‌انگیزی در حال گسترش و سایبری کردن همهٔ امور است. جلوه‌های متنوعی از فضای سایبر در حال خودنمایی است و این تغییرات سریع، مناظر جذاب بیشتری را پدیدار خواهد کرد. از اطلاع‌رسانی، رسانه‌واری و شبکه‌های اجتماعی تا تلفیق مجاز با عالم واقعی نمایشی از این جذابیت هیجان‌انگیز است. این هم‌گرایی فناوری‌های اجتماعی شده عالم نوپدیدی را شکل خواهد داد که طلیعه‌های قابل‌مشاهده و با آینده‌نگری و ژرف‌اندیشی به‌وضوح ابعاد آن قابل‌درک است. وجود شناسی، فضای سایبر با این جلوه‌های متنوع موجب ابتناء صحیح سیاست‌ورزی سایبر خواهد شد. محقق با روش توصیفی – تحلیلی به وجود شناسی سایبر پرداخته است. در این مقاله تلاش می‌شود که از دستگاه فلسفی صدرالمتالهین (ره) برای اکتشاف نحوه وجود سایبر استفاده شود. در ابتدا مختصری از مبانی حکمت متعالیه که ناظر به بحث وجود شناسی است، بیان‌شده و در ادامه کلیاتی از معنا و مفهوم فضای سایبر ناظر به بحث تبیین شده تا بتوان اطلاق‌های متعدد از فضای سایبر را شناسایی کرد. بر این اساس از یک منظر فضای سایبر به‌مثابه وجود رابط و فاقد ماهیت است. از وجهی دیگر، فضای سایبر همانند عرض کیف است. در برداشت سوم سایبر به‌مثابه یکی از جواهر قابل دسته‌بندی است و در نگاه چهارم، سایبر ظرف جدیدی از تحقق هم‌تراز وجود ذهنی و خارجی است. این استنباط به درک صحیح صیرورت فضای سایبر کمک خواهد کرد تا سیاست‌گذاری نافذی برای جهت‌دهی به سایبر شکل گیرد.

کلمات کلیدی: وجودشناسی، فضای سایبر، جوهر، عرض، وجود خارجی، وجود ذهنی، وجود سایبری.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1004

طراحی و پیاده‌سازی یک مدل هوشمند پرسش و پاسخ برای کووید۱۹

صادق احمد آخوندی[۱]، سعید شیری قیداری[۲]، محمدحسن شیرعلی شهرضا[۲]
[۱] کارشناس ارشد علوم کامپیوتر، هوش مصنوعی و محاسبات نرم، دانشکده ریاضی و علوم کامپیوتر
دانشگاه صنعتی امیر کبیر (پلی تکنیک تهران)، تهران
sadegh.akhondi@aut.ac.ir
[۲] استادیار، دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیر کبیر (پلی تکنیک تهران)، تهران
{shiry,hshirali}@aut.ac.ir

چکیده: از زمان ظهور شیوع کووید ۱۹ در چین در سال ۲۰۱۹، این ویروس به سرعت در سراسر جهان گسترش یافته است و بیش از ۷۶۷/۵ میلیون نفر را تحت تأثیر قرار داده و به طور غم انگیزی جان بیش از ۶/۹ میلیون نفر را گرفته است. همانطور که مجلات علمی در تلاش هستند تا با انتشار اطلاعات جدید و دقیق در جهت مبارزه با این پاندمی جهانی اقدام نمایند. همزمان حجم انبوه مقالات و ادعاهای نادرست، چالش‌های مهمی را در دسترسی به داده‌های قابل اعتماد ایجاد کرده است. در این تحقیق، یک سیستم الگوریتمی خواننده-بازیاب دوگانه جدید با استفاده از مدل Pubmedbert توسعه داده شده است. این سیستم پیشرفته نیاز به اطلاعات دقیق را با پاسخ‌گویی مؤثر به سؤالات مرتبط با کووید ۱۹، کمک به شناسایی ویروس و بیماری، تسهیل اقدامات واکنش سریع، و مهار عفونت‌ها و انتقال بیشتر برطرف می‌کند. از طریق ادغام سیستم پاسخگویی به سؤال تدوین شده و مدل قدرتمند PubMedbert، این سیستم به نرخ دقت چشمگیر ٪۸۰/۱۴۸ دست یافته است. این نتایج عملکرد قوی سیستم را در پردازش و ارائه اطلاعات قابل اعتماد نشان می‌دهد، بنابراین در مبارزه با همه‌گیری و هدایت تصمیم‌گیری مبتنی بر شواهد مؤثر واقع خواهد شد.

کلمات کلیدی: هوش مصنوعی، سیستم پاسخ به پرسش، سیستم بازیابی سند، کووید ۱۹، مدل برت، مدل پابمد برت.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1005

ارزیابی چالش‌های امنیت سایبری در محیط‌های واقعیت مجازی VR

علی ملک‌لی[1]
[1] کارشناس ارشد مدیریت فناوری اطلاعات، دانشگاه تهران، مدرس دانشگاه
malekli.ali@gmail.com

چکیده: اگرچه واقعیت مجازی (VR) فناوری جدیدی نیست، اما به تازگی در حوزه های مختلفی به جز سرگرمی مورد استفاده قرار گرفته و این موضوع باعث شده است که جامعه پژوهشی امنیت اطلاعات، به تهدیدات جدید سایبری که با آن همراه است توجه کند. تنوع اجزای سیستم، سطح گستره ای از حملات سایبری را ممکن می سازد که می‌تواند مورد سوء استفاده و بهره برداری غیر مجاز توسط هکرها یا دشمنان شود. در عین حال، تأکید VR بر روی غرق شدن (immersion)، تعامل (interaction) و حضور (presence) به معنای آن است که می‌توان به صورت مستقیم کاربر را مورد هدف حمله سایبری قرار داد، ولی استفاده از دستگاه‌های نصب شده بر روی سر ممکن است، حس و مشاهده و درک این حمله را برای کاربر سخت کند. این مقاله با طبقه‌بندی سیستماتیک تهدیدات سایبری VR موجود در مقابل روشهای دفاعی سایبری مرسوم، به پژوهشگران با زمینه‌های مختلف برای شناسایی بهتر و درک هرچه بیشتر این مخاطرات کمک خواهد کرد.

کلمات کلیدی: واقعیت مجازی، حملات سایبری، امنیت سایبری، حریم خصوصی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1006

تأثیر فناوری واقعیت افزوده در تعامل با محیط زیست

صادق عسگریلو[1]، شکوه کرمانشاهانی[1]
[1]گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بین‌المللی امام خمینی(ره)، قزوین، ایران
kermanshahani@eng.ikiu.ac.ir ،sadeghasgarilou@gmail.com

چکیده: به دلیل آسیب‌های شدید وارده به منابع زیستی به ارتقای سطح آگاهی‌های عمومی برای حفاظت از محیط‌زیست بیش از پیش نیاز داریم. روش‌های سنتی آموزش محیط‌زیست، به دلیل نداشتن فاکتورهایی چون جان‌بخشی، حضور و تعلق به مکان، چندان کارا نبوده‌اند. این مقاله به بررسی استفاده از بازی فراگیر مبتنی بر واقعیت افزوده برای آموزش محیط زیست می‌پردازد و بعنوان نمونه کاربردی، باغستان تاریخی قزوین مورد بررسی قرار گرفته است. باغستان قزوین یکی از معدود نمونه‌های زنده بوم‌سازگان‌های اطراف شهر است که هنوز کارکرد، جامعیت، خصوصیات پیچیده و تا حد زیادی حکمرانی خرد مبتنی بر تعامل با شهر را حفظ کرده است. در عین حال باغستان در معرض تهدید جدی ناشی از عدم شناخت شهرنشینان و تصمیم‌گیران قرار دارد. در این پژوهش پس از بررسی ویژگی‌های باغستان سنتی قزوین و مطالعه پژوهش‌های نظری و برنامه‌های کاربردی مشابه، تاثیر بازی فراگیر مبتنی بر واقعیت افزوده در ایجاد حس تعلق به محیط زیست سنجیده شده است. نتایج نشان میدهد که استفاده از واقعیت افزوده شیوه تعاملی موثری برای افزایش حس تعلق به محیط زیست و رویکرد آموزشی و حساسیت‌زایی محیط زیست است.

کلمات کلیدی: آموزش محیط زیست، بازی فراگیر، واقعیت افزوده.

Code: CYSP2023-1007

آموزش زبان خارجی با کمک فناوری واقعیت افزوده

سونیا مظفری[۱]، حمیدرضا حمیدی[۱]
[۱]گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بین المللی امام خمینی(ره)
hamidreza.hamidi@eng.ikiu.ac.ir ،soniamozaffari@gmail.com

چکیده: بکارگیری فناوری اطلاعات در حوزه آموزش زبان خارجی بصورت ابزار کمکی بسیار مورد توجه است. در کلاس آموزش زبان خارجی، مکان تنها یک مفهوم انتزاعی است؛ جایی که در آن زبان از جامعه، فرهنگ و مکان‌هایی که در آنها مورد استفاده قرار می‌گیرد، جدا می‌شود. واقعیت افزوده فناوری است که در آن اجزای مجازی با محیط واقعی بصورت همزمان ترکیب شده و محتوای موردنیاز را نمایش می‌دهد. هدف ما در این پژوهش بررسی تأثیر واقعیت افزوده مبتنی بر مکان در آموزش زبان فارسی بعنوان یک زبان خارجی است. در این پژوهش پس از صحبت با اساتید حوزه آموزش زبان فارسی و بررسی پژوهش‌ها و کارهای مشابه به این نتیجه رسیدیم که برای آموزش زبان فارسی با استفاده از واقعیت افزوده کاری صورت نگرفته است. بنابراین طرح یک آزمایش انجام گرفت و سپس ارزیابی انجام شد. در ارزیابی از تعدادی زبان‌آموز استفاده شد. بازخوردهای زبان‌آموزان نشان می‌دهد که استفاده از واقعیت افزوده برای آموزش زبان فارسی باعث افزایش رضایتمندی، اشتیاق و تعامل با محیط و افراد می‌شود و همچنین فرآیند یادگیری و به‌خاطر سپاری مفاهیم را بهتر و مؤثرتر می‌کند.

کلمات کلیدی: واقعیت افزوده، آموزش زبان، زبان خارجی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1008

بررسی تأثیر فناوری متاورس بر دگرگونی سنت روابط سیاسی کشورهای حاضر در ساختار نظام بین‌الملل

امید نوری[۱]، محمد لعل علیزاده[۲]
[۱] کارشناسی ارشد علوم سیاسی، دانشگاه پیام نور، تهران
[۲] استادیار گروه علوم سیاسی، دانشگاه پیام نور، تهران
m.lalalizadeh@pnu.ac.ir

چکیده: امروزه با وجود فناوری‌های مختلف به‌عنوان ابزارهای مؤثر بر کمک و ارتقاء همه‌جانبه زندگی انسان‌ها، به‌طور مداوم شاهد پدیدار گشتن فناوری‌های ارتقاءیافته‌تر و بهینه‌تر هستیم. در حوزه فناوری‌های اطلاعاتی و ارتباطی، آخرین تحولی که صورت گرفته ظهور فناوری متاورس است؛ متاورس با دارا بودن ماهیت منحصربه‌فرد خود می‌تواند دگرگونی‌های متعددی را در حوزه‌های مختلف برای جوامع و روابط بین آن‌ها رغم زند که این پژوهش ارتباط بین این فناوری و نحوه اثرگذاری آن بر روابط سنتی شکل‌گرفته بین‌المللی را بررسی کرده است. ضمن بررسی مهم‌ترین یافته‌ها از منابع کتابخانه‌ای، به مطالعه نظرات و افکار اندیشمندان و متفکران در حوزه فناوری متاورس و روابط بین‌الملل پرداخته شد. نتیجه یافته‌های تحقیق نشان داد ارتباط و تأثیرگذاری قابل‌توجهی بین فناوری متاورس و روابط سنتی شکل‌گرفته بین کشورها در ساختار بین‌الملل وجود دارد. بنابراین فناوری مذکور علاوه بر ویژگی ذاتی و خاص خود، نشان داد که با رویکرد صحیح کشورها و سازمان‌های بین‌المللی، توانایی دگرگونی سازی قابل‌ملاحظه‌ای در حوزه‌های مختلف اقتصادی، سیاسی، فرهنگی، اجتماعی در بین کشورها را دارد و نقطه عطفی در روابط جاری بین کشورها تلقی می‌شود.

کلمات کلیدی: پیشرفت، دگرگونی روابط، فناوری متاورس، قدرت سیاسی، کشورهای توسعه‌نیافته و توسعه‌یافته، نظام بین‌الملل.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1010

یک روش کارا جهت شناسایی حملات سیبل در شبکه‌های بین خودرویی

زهرا حر آبادی فراهانی[1]
[1]دانشجوی کارشناسی ارشد مهندسی کامپیوتر - نرم افزار، دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران
zahrafarahany70@gmail.com

چکیده: محققین با معرفی شبکه‌های موردی بین خودرویی در صدد ایجاد بستر ارتباطی مناسب بین خودروها به منظور نیل به اهداف و کاربردهای مختلفی جهت رفاه حال مردم هستند. با پیشرفت تکنولوژی در قرن حاضر روز به روز بر کاربردهای این شبکه ها افزوده شده و شبکه‌های بین خودرویی بسیار مورد توجه شرکت‌های خودروسازی واقع شده‌اند. در شبکه‌های بین خودرویی، خودروها به صورت کاملا خودمختار با یکدیگر ارتباط برقرار کرده و یک شبکه غیرساختارمند بی‌سیم ایجاد می‌کنند. در شبکه‌های موردی بین خودرویی هیچ ایستگاه یا گره مرکزی، مدیریت و کنترل شبکه را برعهده ندارد و شبکه از یک سری خودرو تشکیل شده که متحرک بوده و جای ثابتی ندارند. این مساله باعث شده است که تهدیدات امنیتی فراوانی این شبکه‌ها را تهدید کند. بدین منظور در این مقاله روشی برای مقابله با حملات سیبل در شبکه‌های موردی بین خودرویی ارائه شده است. روش پیشنهادی با یارگیری گره‌ها و اثبات هویت گره‌ها بر مبنای تاییدیه گره‌های یار سعی در مقابله با نفوذ به این شبکه‌ها دارند. بدلیل پویایی بسیار بالای شبکه‌های بین خودرویی، مدت زمان همسایگی دو گره جهت یارگیری گره‌ها پارامتر بسیار مهمی است. بدین شکل که هدف انتخاب گره‌هایی است که مدت زمان زیادی مجاور یکدیگر باشند. لذا رویکرد اصلی در روش پیشنهادی این است که گره‌های یار بر مبنای جدول همسایگی گره‌ها تعیین گردند. به طوریکه روش پیشنهادی سعی می‌کند در روند یارگیری از گره‌هایی با مسیر یکسان و مدت زمان همسایگی بیشتر به عنوان گره‌های یار استفاده نماید. پس از تعیین گره‌های یار، روش پیشنهادی بر مبنای کلیدهای عمومی به واسطه گره‌های یار اقدام به تایید پیام‌های امن درون شبکه می‌نماید. به طوریکه اگر فرستنده پیام گره‌ای امن درون شبکه باشد، گره یار کلید عمومی خود را با پیام ارسالی گره فرستنده هش می‌نماید. نتایج شبیه‌سازی‌ها که با شبیه‌ساز ns-۲ پیاده‌سازی شده‌اند نشان می‌دهد که روش پیشنهادی به شکل کارایی گره‌های سیبل را درون شبکه شناسایی نموده و از انتشار بسته‌های جعلی ارسالی توسط آنها ممانعت می‌کند.

کلمات کلیدی: شبکه‌های موردی بین خودرویی، حملات سیبل، جداول همسایگی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1011

تصویر مقصد ایران در اینستاگرام به روایت بلاگرهای غیرایرانی سفر

ندا رضوی‌زاده[1]
[1]استادیار جامعه‌شناسی گروه جامعه‌شناسی گردشگری، پژوهشکده گردشگری جهاد دانشگاهی، مشهد
n.razavi@gmail.com

چکیده: تحولات گسترده تکنولوژیک در زمینه اطلاعات و ارتباطات و پوشش جهانی اینترنت، دگرگونی‌های وسیعی در فناوری‌های رسانه‌ای، و در نتیجه در فنون بازاریابی محصولات و خدمات پدیده آورده است. صنعت گردشگری نیز از این تحولات برکنار نمانده است. یکی از مهم‌ترین کاربردهای رسانه‌های جدید مبتنی بر اینترنت، به‌ویژه شبکه‌های اجتماعی، شناسایی وضع موجود، تقویت، اصلاح و بهبود تصویر مقصد است. پژوهش حاضر با تحلیل محتوای پست‌های ۲۰ بلاگر سفر در پلتفرم اینستاگرام می‌کوشد به این پرسش پاسخ دهد که: وضعیت تصویر مقصد ایران در شبکه اجتماعی اینستاگرام چگونه است؟ یافته‌ها نشان داد از نظر شناختی، منابع و جامعه میزبان بیش از هر چیز توجه گردشگران را به خود جلب کرده است. از نظر عاطفی نیز همین مؤلفه‌ها واکنش مثبت گردشگران را برانگیخته است و سهم واکنش‌های عاطفی منفی و خنثی نسبت به واکنش‌های مثبت ناچیز است. همچنین از نظر رفتاری، گردشگران در بیش از نیمی از پست‌های خود، ایران را به‌عنوان مقصدی جذاب به سایرین توصیه کرده‌اند و در حدود ۴۰٪ پست‌ها به سفر مجدد به ایران تمایل نشان داده‌اند. این وضعیت تصویری مثبت از مقصد ایران را در اجتماع بلاگرهای سفر شبکه اجتماعی اینستاگرام نشان داد که تمایز واضحی با تصویر ایران در رسانه‌های جریان اصلی دارد. بنابراین بهبود تصویر ایران، مستلزم اتخاذ استراتژی‌هایی برای بازاریابی مقصد ایران است که به‌طور وسیع بر محتوای تولیدشده توسط کاربر و تبلیغات دهان به دهان الکترونیک متمرکز شود.

کلمات کلیدی: تصویر مقصد، اینستاگرام، بازاریابی مقصد، مدیریت مقصد، محتوای تولیدشده توسط کاربر و تبلیغات دهان به دهان الکترونیک.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1012

ارتقای امنیت سیستم بانکی با استفاده از فناوری بلاک‌چین و رایانش ابری

رضا مدنی[1]
[1]دانشجوی کارشناسی ارشد، مهندسی فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران
rezamellat2005@gmail.com

چکیده: با توجه به حملات و تهدیدات امنیتی سیستم‌های بانکی و حریم خصوصی کاربران، استفاده از سرورهای متمرکز می‌تواند عاملی برای از دست دادن یا تحریف داده‌ها توسط مهاجمین باشد. بلاک‌چین یک دفتر غیرمتمرکز، توزیع‌شده و تغییرناپذیر دیجیتال است که معاملات را در یک شبکه جهانی رایانه‌ای ثبت می‌کند که اطلاعات از امنیت بالایی برخوردار هستند. از آنجا که ادغام آن با دامنه‌های دیگر مسائل مرتبط زیادی را حل کرده است، امکان حل مسائل مربوط به حریم خصوصی و امنیت در حوزه سیستم‌های بانکی وجود دارد. از بلاک‌چین به عنوان تأمین کننده‌ی امنیت و یکپارچگی فناوری‌هایی نظیر رایانش ابری استفاده می‌شود. بنابراین، استفاده از بلاک‌چین در حوزه رایانش ابری دامنه جدیدی از تحقیقات را به‌وجود می‌آورد. در این تحقیق ابتدا مفاهیم بلاک‌چین و رایانش ابری بررسی می‌شوند. سپس بلاک‌چین به‌عنوان خدماتی برای ارتقای امنیت سیستم بانکی در بستر رایانش ابری ارائه می‌شود تا نشان دهد چگونه می‌توان از ویژگی‌های مختلف فناوری بلاک‌چین و رایانش ابری به‌عنوان خدماتی برای امنیت سیستم بانکی استفاده نمود.

کلمات کلیدی: امنیت، سیستم بانکی، بلاک‌چین، رایانش ابری.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1014

تبیین حکمرانی فضای سایبر، با تکیه بر جایگاه قوای شناختی و مسئله معرفت

محسن ابراهیمی[1]
[1]دانش آموخته حوزهٔ علمیه قم، دکتری فلسفه دانشگاه اصفهان
mhnebr@gmail.com

چکیده: «بیانیه گام دوم انقلاب اسلامی» بر وظیفه سنگین دستگاه‌های حکومتی نسبت به «ابزارهای رسانه‌ای پیشرفته و فراگیر» تأکید دارد؛ و با توجه به این که بسیاری از این رسانه‌ها در فضای سایبر فعّالیت می‌کنند، واکاوی وظیفه یادشده با تأکید بر رسانه‌های سایبری، دارای نوآوری است. هدف پژوهش، پاسخ به این پرسش است که از منظر فقه سیاسی، وظیفه حکومت اسلامی نسبت به تأمین امنیّت در فضای سایبر کدام است و جایگاه این وظیفه در بیانیه گام دوم چیست. بنابر این با جستجو در منابع کتابخانه‌ای؛ مستندات حکم به وجوب تأمین امنیّت همه جانبه در فضای سایبر توصیف و با رویکرد فقه حکومتی تحلیل شده و دیدگاه مقام معظم رهبری پیرامون امنیّت فضای سایبر، در منظومه فکری ایشان بررسی شده تا جایگاه این وظیفه در بیانیه مشخّص گردد. در نتیجه، ایجاد امنیّتِ همه‌جانبه در فضای سایبر بر حکومت اسلامی واجب دانسته شده که مشمول مطالبه جدّی بیانیه گام دوم انقلاب اسلامی نیز می‌باشد.

کلمات کلیدی: حکمرانی فضای سایبر، قوای شناختی، متخیله و واهمه، قوه عاقله، معرفت.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1015

اهمیت و کاربرد تحلیل کلان‌داده‌های زیرساخت ارتباطی- مخابراتی در کشور

احسان ترکمان منش[1]
[1] کارشناسی ارشد هوش‌مصنوعی و پژوهشگر دانشگاه جامع امام حسین(ع)، تهران
ehsan.tr@email.com

چکیده: رشد فزاینده صنعت ارتباطات خصوصاً در دهه اخیر منجربه فراگیر شدن خدمات الکترونیک و افزایش ضریب نفوذ اینترنت گشته، که در نتیجه آن تولید انبوه داده‌هایی ارزشمند از فعالیت کاربران در صنعت مخابرات است. در حال حاضر روزانه صدها میلیون رکورد داده مخابراتی در کشور تولید می‌گردد، از دیگر سو با فراگیری نسل پنجم ارتباطی (5G) با تمرکز بر اینترنت اشیا و همچنین ادغام فناوری‌های ارتباطی با هوش‌مصنوعی در نسل ششم ارتباطی (6G) تحلیل کلان داده‌های مخابراتی در آینده‌ای نزدیک اهمیتی مضاعف خواهد یافت. لذا توجه جدی به تحلیل داده در سطح مدیریت راهبردی جامعه بسیار مهم می‌نماید. در حال حاضر داده‌های مخابراتی به چهار دسته داده‌های جزئیات تماس، داده‌های ثبت آی‌پی، داده‌های شبکه و داده مشتریان تقسیم می‌شوند که با بهره‌بردای صحیح از الگوریتم‌های داده‌کاوی نه تنها می‌توان گامی مهم در راستای تحقق حکمرانی سایبری کشور برداشت، بلکه با تطبیق سایر داده‌ها امکان بسط تحلیل‌ها به حوزه‌های کلان فرهنگی، سیاسی، امنیتی و اقتصادی وجود دارد.

کلمات کلیدی: تحلیل‌داده، حاکمیت داده، کلان داده، مخابرات، هوش‌مصنوعی، فضای سایبر، حاکمیت سایبری.

Code: CYSP2023-1017

راهبردهای مواجهه با فناوری‌های نوظهور از منظر امنیت سایبری

محمدحسن فرخی[۱]، خداداد هلیلی[۲]
[۱]دانشجوی دکتری امنیت سایبر، دانشگاه عالی دفاع ملی
mhf1364@gmail.com
[۲]استادیار، عضو هیات علمی دانشکده کامپیوتر، دانشگاه شهید ستاری، تهران
kh.halili@ssau.ac.ir

چکیده: همزمان با گسترش فضای سایبر و فناوری‌های مرتبط با آن، حملات و تهدیدات سایبری نیز مدام درحال‌توسعه هستند. در بسیاری از کشورها، امنیت سایبری به یکی از اولویت‌های اساسی در دستیابی به امنیت ملی تبدیل شده است. به‌منظور پیشگیری از آثار مخرب این حملات و جلوگیری از ایجاد خدشه در امنیت ملی، لازم است علاوه بر تمهیدات فنی، راهبردهای مناسبی در سطح ملی، تدوین و اجرا شود. هدف اصلی این مقاله بررسی راهکارهای مؤثر برای بهبود امنیت سایبری و ارائه راهبردهایی برای مواجهه هوشمند با فناوری‌های مورداستفاده در فضای سایبر، است. بدین منظور پس از بررسی فناوری‌های هوش مصنوعی، زنجیره‌بلوکی، اینترنت اشیا، رایانش ابری، بیومتریک و رباتیک و کاربردهای آن‌ها، راهبردهای پیشنهادی مطرح شده است. نتایج این تحقیق نشان می‌دهد توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری موجب بهبود امنیت سایبری می‌شود بدین منظور راهبردهایی مانند توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری در این مقاله موردتوجه و بررسی قرار گرفته است.

کلمات کلیدی: فضای سایبر، فناوری‌های نوظهور، امنیت سایبری، هوش مصنوعی.

Code: CYSP2023-1018

شناسایی تروریست در شبکه‌های اجتماعی به‌وسیله اطلاعات منبع‌باز

مهدی کوره‌پز[۱]، رضا شیبانی[۲]
[۱]گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد، ایران
Korehpaz65@gmail.com
[۲]استادیار انفورماتیک پزشکی، مدیر گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد مشهد، ایران
reza.shni@gmail.com

چکیده: در فعالیت های اطلاعاتی، امنیتی و انتظامی، برای شناسایی اهداف، از نظارت بر شبکه اجتماعی استفاده می شود. این رویکرد به تحلیلگران کمک می کند تا گروه های مخفی مانند یک شبکه ضد امنیتی، یک خانواده جنایتکار سازمان یافته یا یک باند تبهکار را با تحلیل داده ها شناسایی و از رشد افراط گرایی به هر شکل ممکن جلوگیری شود. فعالیت های تروریستی در سراسر جهان منجر به توسعه روش های پیچیده برای تجزیه و تحلیل گروه ها و شبکه های تروریستی شده است. تحقیقات فعلی و گذشته نشان داده است تجزیه و تحلیل شبکه های اجتماعی (SNA) رویکردی برای تجزیه و تحلیل شبکه های تروریستی و درک بهتر ساختار زیربنایی یک گروهک و شناسایی بازیگران کلیدی در گروه و پیوندهای آنها در سراسر سازمان است. در این رابطه مهم ترین چالش، حفظ حریم خصوصی برای دسترسی به اطلاعات است. این مقاله جنبه‌های مختلف تحلیل شبکه‌های اجتماعی را در مورد تروریسم، با در نظر گرفتن داده‌های تجربی و مطالعات مبتنی بر داده‌های منبع باز بررسی می‌کند. جمع آوری داده های باز بدون نیاز به داشتن مجوز از مراجع قضایی و با در نظر گرفتن اطلاعات منتشر شده توسط خود فرد در سطح وب صورت می گیرد. کار ما در درجه اول مطالعه ای بر روی انواع مختلف شبکه ها و گره های تروریستی غیرمتمرکز قابل دسترس بوسیله جمع آوری داده های باز است.

کلمات کلیدی: تحلیل شبکه‌های اجتماعی، اسینت، جرم کاوی، داده کاوی، هوش مصنوعی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1019

تأثیر حکمرانی داده بر کارآمدی هزینه‌کرد بودجه در پروژه‌ها

علیرضا فخررحیمی[۱]، فربود تیموری[۲]
[۱]دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران؛ امور نظام فنی، اجرایی مشاورین و پیمانکاران، معاونت فنی و زیربنایی، سازمان برنامه و بودجه کشور، تهران
alirfrahimi@iran.ir
[۲]دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران
fa.teimouri01@sndu.ac.ir

چکیده: هدف این مقاله بررسی تأثیر حکمرانی داده بر کارآمدی هزینه‌کرد بودجه در پروژه‌های ایران است. حکمرانی داده به‌عنوان یک ابزار مدیریتی، توانایی تجزیه و تحلیل داده‌های پروژه را فراهم می‌آورد و از طریق بهبود برنامه‌ریزی و کنترل هزینه‌ها، به بهبود عملکرد پروژه‌ها و افزایش کارآمدی کمک می‌کند. بررسی نتایج این مقاله نشان می‌دهد که حکمرانی داده، ابزاری قدرتمند برای بهبود کارآمدی هزینه‌کرد بودجه در پروژه‌های عمرانی و غیرعمرانی است و می‌تواند به کشورها در ارتقاء زیرساخت‌ها و توسعه‌بخشی کمک کند.بدیهی است شرایط تحریم، تکانه‌های اقتصادی و سایر فشارهای بین‌المللی از یک سو، الزام به طی نمودن مسیر توسعه کشور و سعی در تداوم شتاب توسعه در ایران، لزوم استفاده از حکمرانی داده را بیش از بیش مهم می‌نماید. بدیهی است استفاده از حکمرانی داده پیش از هر چیز نیاز به برخی الزامات و معیارها دارد که در این مقاله به اختصار مورد بررسی قرار گرفته‌اند.

کلمات کلیدی: حکمرانی داده، هزینه، بودجه، پروژه‌های عمرانی، هزینه کرد، پایش.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1020

بررسی قانون‌گذاری هوش مصنوعی در جهان و ایران با تکیه بر مدل چندذی‌نفعی جهانی

علیرضا فخررحیمی[۱]، فربود تیموری[۲]
[۱] دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران؛ امور نظام فنی، اجرایی مشاورین و پیمانکاران، معاونت فنی و زیربنایی ، سازمان برنامه و بودجه کشور، تهران
alirfrahimi@iran.ir
[۲] دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران
fa.teimouri01@sndu.ac.ir

چکیده: قانون‌گذاری هوش مصنوعی در کشور جمهوری اسلامی ایران ضروری است تا بهره‌برداری امن و اخلاقی از این فناوری را تضمین کند. هوش مصنوعی، با آثاری نظیر تأثیر بر اشتغال، اقتصاد، و امنیت مخاطبین اجتماعی، نیازمند استانداردها و مقرراتی است که مانع مشکلات احتمالی ناشی از استفاده ناصواب از آن شود. قوانین باید حریم خصوصی شهروندان، انسان‌مندی هوش مصنوعی و پیشگیری از تبعیض‌های اجتماعی را در بر داشته باشند. با توجه به اهمیت آموزش، تحقیقات و ایجاد همکاری‌های بین‌المللی، کشور باید برنامه‌ریزی و ارتقاء نیروهای متخصص در این حوزه را به‌عنوان اولویت مدنظر قرار دهد. توسعه فناوری هوش مصنوعی می‌تواند در مواجهه با چالش‌های جامعه مؤثر باشد، اما نیازمند قوانین محافظتی و همکاری بین‌المللی است. فقدان قوانین و مقررات مناسب برای هوش مصنوعی می‌تواند به تأثیرات منفی و پیش‌بینی نشده این فناوری در جامعه منجر شود. تأثیرات اصلی این فقدان قانون به صورت‌هایی نظیر عدم حمایت از حقوق شهروندان، عدم اطمینان در استفاده از هوش مصنوعی، تأثیرات اجتماعی و اقتصادی ناخواسته، عدم کنترل مسئولیت‌ها، نقض اخلاقیات، و سایر موارد ، بروز خواهد کرد.

کلمات کلیدی: هوش مصنوعی، قانون گذاری، مقررات، حاکمیت.

Code: CYSP2023-1021

استراتژی تحول دیجیتال پارلمان در مسیر شفافیت و دموکراسی

یاشار ابری[1]، احمد فرید اصیل[1]
[1]دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
faridaseel.4all@gmail.com ،yasharabri@ut.ac.ir

چکیده: در این دوران دیجیتالی، سازمان‌های عمومی، مانند مجلس‌ها، ملزم به توسعه استراتژی‌های دیجیتالی هستند تا با متحول کردن عملکردها خود را بهبود دهند. این استراتژی باید از فناوری‌های دیجیتال استفاده کند تا با ایجاد شفافیت امکانات مهمی را هم برای شهروندان و هم برای نمایندگان مجلس در فرآیند سیاست‌گذاری فراهم کند. مجلس‌ها می‌توانند با استفاده از دانشی که در طول چرخه‌های زندگی مجلس از جمع‌آوری داده در جامعه به دست می‌آید تصمیمات سیاست‌گذاری مبتنی بر شواهد (EBP) را در انتخاب، تدوین و ارزیابی سیاست‌های عمومی دخیل کنند. این مقاله پیشنهاد می‌دهد که از ابزارهای دیجیتال در همه مراحل تصمیم‌گیری در مجلس استفاده شود. یک مسیر برنامه‌ریزی ارائه شده است، که در زمینه چارچوب تحول دیجیتال مبتنی بر کاربر و فناوری‌های دیجیتال آن قرار دارد. جنبه‌هایی که تحلیل می‌شوند، شرایط محدودیت برای ایجاد محیط دیجیتال EBP را نیز شامل می‌شود. راهکار دموکراسی مدرن با این سازوکارهای شفافیت مبتنی بر داده‌های دریافتی از جامعه موجب افزایش اطمینان مردم به آینده کشور خواهد شد.

کلمات کلیدی: شفافیت پارلمانی، سیاست‌گذاری مبتنی بر شواهد، استراتژی دیجیتال، تحول دیجیتالی پارلمان.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1023

بررسی و شناسایی کاربردهای فناوری بلاک‌چین و رمزارزها در حوزه‌ی هنرهای تجسمی دیجیتال و بازارهای مالی هنر در ایران

مهدی نصیری[1]
[1] کارشناس ارشد رشته‌ی تاریخ هنر جهان اسلام، گروه مطالعات عالی هنر، دانشکده‌ی هنرهای تجسمی دانشکدگان هنرهای زیبا، دانشگاه تهران، ایران
nasiri.mehdi@ut.ac.ir

چکیده: خرید و فروش آثار هنرهای تجسمی دیجیتال بر بستر فناوری‌های نوینی مانند بلاک‌چین و رمزارزها، باعث شده‌است که هنرمندان و علاقه‌مندان به هنر در ایران اسلامی، امکان خلق، انتشار، خرید و فروش آثار خود را به‌صورت دیجیتال بر بستر بلاک‌چین با استفاده از رمزارزها داشته‌باشند. این مقاله به بررسی کاربردها، مزایا و چالش‌های این فناوری‌های نوین در حوزه‌ی هنرهای تجسمی دیجیتال و تأثیر آن بر بازار هنر دیجیتال در کشور می‌پردازد. با توجه به رشد سریع حوزه‌ی بلاک‌چین و NFT در سطح جهانی، این مقاله به‌دنبال پاسخ به این پرسش است که کاربردهای مهم فناوری بلاک‌چین و رمزارزها در حوزه‌ی هنرهای تجسمی دیجیتال چه هستند؟ و شرایط لازم برای ایجاد و راه‌اندازی یک رمز ارز ملی-ایرانی در حوزه‌ی هنرهای تجسمی در داخل کشور بر بستر بلاک‌چین چگونه است؟ بدین‌منظور با استفاده از روش تحقیق توصیفی-تحلیلی، پس از پژوهش و واکاوی در حوزه‌های ذکر شده مشخص گردید که استفاده از فناوری بلاک‌چین و رمزارزها می‌تواند باعث افزایش اعتماد و شفافیت در معاملات هنری، ردیابی منشأ اثر هنری، رهگیری تاریخچه‌ی مالکیت و فروش‌های ثانویه، امنیت خرید و فروش در معاملات هنری، قراردادهای هوشمند، توسعه و رشد بازارهای دیجیتال هنر در ایران شود.

کلمات کلیدی: بلاک‌چین، رمز ارز، NFT، بازار دیجیتال هنر، هنرهای تجسمی دیجیتال.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1025

راه‌اندازی یک واحد پایش امنیت چابک در شرکت‌ها و سازمان‌ها

محمدمهدی قاسمی‌نیا[۱]، محمدحسن میرعارفین[۲]، حسین مرادی[۳]
[۱] کارشناسی ارشد علوم کامپیوتر، دانشگاه یزد، یزد، ایران
ghaseminya@gmail.com
[۲] کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه علم و صنعت، تهران، ایران
m_mirarefin@iust.ac.ir
[۳] دانشجوی کارشناسی ارشد مدیریت، دانشگاه تهران، تهران، ایران
ho3in14741@gmail.com

چکیده: ضرورت پیاده‌سازی یک واحد امنیت برای مقابله با تهدیدات محیطی و افزایش ایمنی سازمان، امری غیرقابل انکار است. گسترش روزافزون تهدیدات و پیشرفت‌های نرم و سخت‌افزاری، سازمان‌های بزرگ و کوچک را مجبور به حفاظت بیش از پیش از داده‌ها، سرویس‌ها و دارایی‌هایشان کرده و در این بین، وجود یک تیم منسجم و ساختارمند که بر روی این موضوع متمرکز باشند، امری ضروری است. واحد عملیات امنیت به همین منظور و در جهت مقابله با تهدیدات خارجی و افزایش ایمنی در سازمان تشکیل شده است. مقاله‌ی پیش رو، در آغاز به بررسی و مرور کارها و تحقیقات انجام گرفته در این حوزه می‌پردازد. سپس به شناخت اجزای سازنده‌ی واحد عملیات امنیت در قالب ساختار PPTGC که متشکل از افراد، فرایندها، تکنولوژی، قوانین و رویه‌هاست، پرداخته است. در انتها موارد مستعد تحقیق در این حوزه عنوان شده است.

کلمات کلیدی: واحد عملیات امنیت، امنیت سیستم‌های کامپیوتری، چارچوب پاسخگویی به حادثه، ساختار PPTGC.

Code: CYSP2023-1026

طراحی الگوریتم استدلال، اولویت گام دوم در ارتقای علوم اسلامی

محمدحسن احمدی[1]
[1]دانشیار دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
ahmadi_mh@ut.ac.ir

چکیده: پژوهش‌های بسیاری است که در آنها پژوهشگر نسبت به مبانی و پیش‌فرض‌ها -یی که چه بسا خود به‌صورت مستقیم یا غیرمستقیم (با اتکا به مبانی دیگران) آنها را مفروض گرفته- بی‌توجه است. از سوی دیگر، متغیرهای به‌کارگرفته شده در تحلیل متون، بر اساس استاندارد خاصی تعیین نمی‌شوند. تحلیل‌های کمی هم که به مدد فراوری شدن متون، شیوع پیدا کرده است. این همه، گویای آن است که لازم است پیشنهاد طراحی الگوریتمی داده شود تا همواره به‌روزرسانی شده و در پیشخوان پژوهش‌ها قرار گیرند. روشن است که نه حافظه عادی پژوهشگر مجال این فرآیند به‌روزرسانی را دارد و نه اساساً حجم پژوهش‌های کنونی، اجازه پرداختن به این حوزه گسترده از مبانی و متغیرها را می‌دهد.این پژوهش بر آن است تا به مدد هوش مصنوعی و با وجود آسیب پژوهش‌های جاری از جهت عدم جامعیت نسبت به ابعاد موضوع، به تدوین الگوریتمی در این خصوص دست یازد تا نتایج پژوهش‌های مبتنی بر استدلال‌های متنی، به الگوی معیار نزدیک‌تر شود.

کلمات کلیدی: هوش مصنوعی، پیش‌فرض، روش تحقیق، حافظه، الگوریتم استدلال.

Code: CYSP2023-1027

جایگاه شبکه ملی اطلاعات در ایران بر اساس حقوق بین‌الملل ارتباطات

سید محمد علی مرتضوی شاهرودی[1]
[1]دانشجوی کارشناسی ارشد علوم ارتباطات اجتماعی، دانشگاه صدا و سیما
m.shahroudy90@gmail.com

چکیده: تکنولوژی ارتباطی در حال توسعه است و نقش دولت در کنترل امور، به‌ویژه جریان اطلاعات، روز به روز ضعیف‌تر می‌شود. فضای سایبر به دلیل پیشرفت ارتباطات و فراگیر شدن آن در سراسر جهان، به یک مسئله مهم تبدیل شده است. این فضا همچنین، همراه با مزایای فراوان، در بردارنده آفت‌ها و سوء استفاده‌هایی نیز است. فضای مجازی سبب دگرگونی ریخت جامعه و اخلال در نظام ارزشی، گسترش جاسوسی نوین و توسعه نبردهای هیبریدی شده و از این جهت، تهدیدات امنیتی جدی را شکل داده است. تضمین استقلال و امنیت کشور در فضای سایبر بسیار حائز اهمیت است که به تحقق شبکه ملی اطلاعات در سه بعد زیرساخت، سرویس و محتوا وابستگی دارد. بسیاری از کشورهای صاحب قدرت سایبری برای مدیریت فضای سایبر خود مبادرت به طراحی و اجرایی نمودن شبکه ملی اطلاعات بومی نموده‌اند. در این پژوهش، با استفاده از روش تحقیق کیفی و توصیفی-تحلیلی، به تبیین مؤلفه‌های مطلوبیت استقرار شبکه ملی اطلاعات در کشور با استفاده از تجربیات سایر کشورهای پیشرفته مثل روسیه و چین و کشورهای حامی حقوق بین‌الملل ارتباطات پرداخته شده است. در این مقاله، به بررسی این مسئله پرداخته شده است که آیا حقوق بین‌الملل ارتباطات می‌تواند به تمام نیازهای کشورها از جمله جمهوری اسلامی ایران در حفظ و صیانت سایبرنتیک پاسخ دهد یا نیازمند قوانین داخلی هستند؟ به طور کلی، تحقیقات در این حوزه نشان می‌دهد که حفاظت از فضای سایبر برای حفظ امنیت و استقلال کشورها بسیار حائز اهمیت است و تحقق حکمرانی این فضا برای مدیریت کلان جامعه دارای اهمیت حیاتی است.

کلمات کلیدی: شبکه ملی اطلاعات، اینترنت ملی، حقوق بین‌الملل ارتباطات، آزادی بیان.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1028

ارائه الگوی به‌کارگیری رسانه‌های اجتماعی در ارتقای روابط عمومی (مورد مطالعه: شهرداری نهاوند)

مریم کرمعلی[۱]، علی جعفری[۲]
[۱] دانشجوی دکتری علوم ارتباطات، دانشگاه آزاد اسلامی واحد اردبیل، اردبیل، ایران
maryamk1366@yahoo.com
[۲] استادیار پژوهشگاه مطالعات آموزش و پرورش، سازمان پژوهش و برنامه‌ریزی آموزشی، تهران، ایران
alijafari.researcher@gmail.com

چکیده: هدف این پژوهش، بررسی تأثیر رسانه‌های اجتماعی بر روابط عمومی سازمان‌های خدماتی است.با پیشرفت رسانه‌های اجتماعی، بخش‌های مختلفی از جمله روابط عمومی نیز تحت تأثیر قرارگرفته‌اند. به‌همین دلیل، تخصصی‌های روابط عمومی باید توانایی سازگاری با محیط دیجیتال را داشته باشند تا با تغییرات چشم‌گیر این فضا همراهی کنند. این پژوهش با هدف طراحی یک الگوی استفاده از رسانه‌های اجتماعی در بهبود اثربخشی روابط عمومی سازمان‌های خدماتی به‌صورت آمیخته (کیفی و کمی) انجام شده است. روش تحلیل پژوهش به صورت کاربردی و با رویکرد اکتشافی آمیخته بوده است. در مرحله اول، با استفاده از تحلیل محتوا و مصاحبه‌های عمیق، مؤلفه‌های الگو شناسایی شدند. شرکت‌کنندگان این مرحله از بین ۱۶ نفر از خبرگان دانشگاهی و مدیران ارشد شهرداری نهاوند به‌صورت هدفمند انتخاب شدند. در مرحله دوم، با استفاده از روش مدل‌سازی معادلات ساختاری، الگوی طراحی‌شده بررسی شد. نمونه آماری این پژوهش شامل ۲۰۳ نفر از مدیران و کارشناسان شهرداری نهاوند بود که به‌صورت تصادفی طبقه‌ای انتخاب شدند. ابزار جمع‌آوری داده‌ها پرسشنامه بود که روایی و پایایی آن تأیید شده است. تحلیل داده‌ها با استفاده از نرم‌افزار لیزرل انجام شد. نتایج بخش کیفی نشان می‌دهد که رسانه‌های اجتماعی در سه جنبه ارتباطات رسانه‌ای، سهولت استفاده و اطلاع‌رسانی تأثیرگذار هستند. در بخش کمی نیز مشخص شد که استفاده از رسانه‌های اجتماعی با ارتقای روابط عمومی سازمان‌های خدماتی رابطه‌ای معنادار دارد و الگوی طراحی شده متناسب است. از این رو، مدیران و سیاست‌گذاران روابط عمومی سازمان‌های خدماتی می‌توانند با بهره‌گیری از نتایج این پژوهش و استفاده از ظرفیت‌های رسانه‌های اجتماعی، بستر مناسبی را برای توسعه و بهبود اثربخشی فعالیت‌های روابط عمومی سازمان فراهم کنند.

کلمات کلیدی: رسانه اجتماعی، روابط عمومی، سازمان خدماتی، شهرداری نهاوند.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1029

بازخوانی کارکرد دوسویه قوه خیال در سلطه‌ی سایبری بر مبنای علم النفس فلسفی

زهرا حبیبیان[1]، عذرا جعفری موحد[2]
[1] دانش‌آموخته سطح سه فلسفه اسلامی جامعة الزهرا سلام‌الله علیها، قم و دانشجوی کارشناسی ارشد فلسفه و کلام اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
habibian213@gmail.com
[2] دانش‌آموخته سطح سه فلسفه اسلامی جامعة الزهرا سلام‌الله علیها، قم و فارغ‌التحصیل دکتری کلام امامیه، دانشگاه قرآن و حدیث، قم
jafarimovahed97@gmail.com

چکیده: در طول تاریخ، کنترل و سلطه بر دیگران دغدغه‌ی اصلی سلطه‌جویان بوده است. دانش سایبرنتیک محصول علم مدرن، با خاستگاه اومانیستی، به‌معنای کنترل و حاکمیت از طریق جریان اطلاعات است که در انسان با محوریت خیال رقم خورده و بستری نرم و نوین در اعمال سلطه محسوب می‌شود. قوهٔ خیال به تحلیل علم‌النفس فلسفی دو ساحت سلطه‌پذیر و سلطه‌گریز دارد. از یک سو سلطهٔ‌سایبری با تخدیر خیال، ذائقه‌شناسی و ذائقه‌سازی در انسان، فاعلیت عقلانی نفس را زایل ساخته و نفس آدمی را با ایجاد کثرت در ارضای امیال شهوانی تا سر حد تسخیر در جهت اهداف سلطه پیش می‌برد. از سوی دیگر خیال در جنبه سلطه‌گریز خود پلی برای استقرار عقل بوده و در پرتو هدایت تکوینی و تشریعی، با قدرت زیبایی‌شناختی، عامل اصلی عزم، طریقی ضروری در سلوک و سپری در مقابل اعمال سلطه‌ی سایبری به شمار می‌رود. در سلطه‌ی سایبری، نوعی تسخیر باطل ایجاد می‌شود که به‌نحو علی بر انسان مؤثر نبوده و به فاعلیت بالقصد او ضربه‌ای وارد نمی‌سازد؛ بلکه مسیر اختیار را با بازداشتن تمسک به تفکر و تعقل، یک‌طرفه ساخته و در مسیری خلاف مصلحت او سوق می‌دهد. بر این مبنا روش کنترل در سلطه‌ی سایبری با تعالی انسان در تقابل است. شناخت ساحت دوگانه‌ی خیال در سلطه‌ی سایبری، در پیشگیری و دفاع در برابر آسیب‌های نظام سلطه و نیز تنظیم نظامی متعالی مبتنی بر مبانی اسلامی، مؤثر است.

کلمات کلیدی: کنترل، سلطه‌ی سایبری، اومانیسم، خیال، فاعلیت بالتسخیر، زیبایی‌شناسی، هدایت.

Code: CYSP2023-1030

مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی

محمدرضا مرادی[۱]، محمدرضا ولوی[۲]، متین مرادی[۳]
[۱] دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران
mr.moradi@sndu.ac.ir
[۲] دانشیار دانشگاه صنعتی مالک اشتر، تهران
valavi@mut.ac.ir
[۳] دانشجوی مهندسی نرم‌افزار کامپیوتر، دانشگاه شاهد ، تهران
matinmoradi1401@gmail.com

چکیده: دکترین در حقیقت، فلسفه را که اغلب ابهام‌آلود و نظری است، می‌گیرد و آن را عملیاتی می‌کند تا از دل آن، سیاست‌هایی خاص بیرون بیاید. در خصوص مفهوم دکترین در دنیا، تفاوت دیدگاه وجود دارد. رویکرد ج.ا.ا. به دکترین نیز، با دو رویکرد غالب شرقی و غربی تا حدودی متفاوت است. دکترین عمدتاً در امور دفاعی-امنیتی به‌کار می‌رود. کشورهای دنیا، برای تدوین دکترین از مدل‌های مشخصی بهره می‌برند که عموماً نیز این مدل‌ها به‌صورت واضح تشریح نمی‌گردند. فضای سایبر، پدیده نوظهوری است که دارای ویژگی‌های خاص خود می‌باشد. این فضا چند سالی است که رسماً به‌عنوان یکی از عرصه‌های جنگ تعریف گردیده است. بنابراین چنانچه در نظر داشته باشیم برای این فضا در حوزه دفاعی-امنیتی دکترین تدوین نماییم، نیازمند یک مدل خاص‌منظوره می‌باشیم. مدل فرآیندی معرفی شده، مختص فضای سایبر جمهوری اسلامی ایران است و برگرفته از یک کارپژوهشی گسترده (با بهره‌گیری از نظر خبرگان و تعیین اعتبارسنجی آن) است که نتیجه آن ارائه شده است. هدف این پژوهش که برگرفته از یک رساله دکتری می‌باشد آن است که مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی-امنیتی احصا شود.

کلمات کلیدی: دکترین، فضای سایبر، دفاعی امنیتی، تدوین مدل.

Code: CYSP2023-1031

واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تأکید بر بلاگرها)

محبوبه موسیوند[۱]، فائزه ساکی[۲]
[۱] استادیار گروه مطالعات علوم اجتماعی و توسعه، پژوهشکده زنان، دانشگاه الزهرا، تهران، ایران
m.moosivand@alzahra.ac.ir
[۲] کارشناسی ارشد مطالعات زنان، دانشگاه الزهرا، تهران، ایران
sakifaezeh7@gmail.com

چکیده: فضای سایبر و شبکه‌های اجتماعی علیرغم مزایای قابل توجه و بی‌شمار، آسیب‌ها و مشکلاتی را هم برای کاربران به‌دنبال داشته است که نیازمند بحث و بررسی است، به‌همین منظور این پژوهش با هدف واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تأکید بر بلاگرها) با استفاده از روش توصیفی-تحلیلی انجام شده است که نتیجه این پژوهش بدین شرح است که ترویج سبک زندگی متعارض با سبک زندگی ایرانی-اسلامی و ترویج تفکر کسب درآمد و شهرت از فضای سایبر و شبکه‌های اجتماعی به هر طریقی، دو آسیب عمده در این حوزه به‌شمار می‌رود. در مجموع به‌منظور کاهش آسیب‌های فردی و اجتماعی فضای سایبر و شبکه‌های اجتماعی به‌ویژه در حوزه بلاگرها پیشنهاد می‌شود که علاوه بر ارتقا دانش رسانه افراد، سیاست‌گذاری‌ها و اقدامات مناسبی جهت مقابله با بعضی آسیب‌های فضای مجازی انجام شود.

کلمات کلیدی: فضای سایبر، فضای مجازی، شبکه‌های اجتماعی، آسیب، بلاگر.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1033

از گواهی تا باور مبتنی بر تکنولوژی: بررسی بر اساس تجربه‌گراییِ انتقادیِ زمینه‌ای

محمدعلی عاشوری کیسمی[1]
[1]فلسفه، دانشگاه علامه طباطبائی، تهران، ایران
m_ashori@atu.ac.ir

چکیده: هدف این پژوهش بررسی معرفت‌شناختی خروجی‌های هوش مصنوعی در برابر پرسشهای علمی است. با توجه به اینکه در هوش مصنوعی، از اطلاعات و داده‌های متخصصان و دانشمندان برای یادگیری استفاده میشود؛ ممکن است این تصور پدید آید که میتوان خروجیهای به‌دست‌آمده در برابر پرسش‌های علمی را نوعی گواهی گروهی در نظر گرفت. این پژوهش با استفاده از روش تحلیلی-انتقادی دیدگاه‌های موجود را مورد ارزیابی قرار میدهد که در این راستا از رویکرد تجربه‌گرایی انتقادی زمینه‌ای هلن لانجینو استفاده شده است. نتایج پژوهش حاضر نشان میدهد رویکردهای سنتی و ابزاری امکان بررسی خروجی هوش مصنوعی تحت عنوان گواهی را ندارند. رویکرد شبه-گواهی بر معرفت‌شناسی اجتماعی جریان اصلی متکی است که بررسی‌ها نشان میدهد استدلالها و انتقادات این رویکرد بر پایه شناخت روند تولید دانش علمی استوار نیست. دیگر نتایج پژوهش نشان می‌دهند که کماکان خروجی هوش مصنوعی در برابر پرسشهای علمی را نمی‌توان گواهی گروهی متخصصان دانست و اصطلاح «باور مبتنی بر تکنولوژی» بهتر آن را تبیین میکند.

کلمات کلیدی: گواهی گروهی، هوش مصنوعی، معرفت‌شناسی اجتماعی، هلن لانجینو، تجربه‌گراییِ زمینه‌ای انتقادی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1034

دلیل عقلی جرم‌انگاری سایبری مبتنی بر قاعده اعانت بر اثم

محسن نادری[۱]
[۱]دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
mnnnnarsenal9085@gmail.com
علی‌اکبر ایزدی فرد[۲]
[۲]عضو هیئت علمی دانشگاه و استاد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
izadifard@umz.ac.ir
محمدمهدی زارعی[۳]
[۳]استادیار و عضو هیئت علمی گروه فقه و مبانی حقوق اسلامی دانشگاه مازندران
m.zarei@umz.ac.ir

چکیده: امروزه عقل ابر لزوم بهره‌گیری از فضای مجازی جهت تسهیل در امور مختلف اتفاق نظر دارند. برای کارآیی و بهره‌گیری مطلوب از این فضا مدیریت و سازماندهی قانونی فضای مجازی امری عقلانی و شایان توجه است. پژوهش حاضر با روش توصیفی-تحلیلی و مراجعه به کتب فقهی و آراء فقها، همراه با توجیه، تبیین، استدلال و استنتاج است. فرصت‌ها و چالش‌های فضای مجازی با عنایت به لزوم حفظ امنیت عمومی جامعه ضمن احترام به حرمت و حریم خصوصی اشخاص حقیقی و حقوقی موجب نگرانی و دغدغه در شیوه حکمرانی منطقی و اصولی بر این فضاشده است. ارائه چارچوب و ضابطه عقلایی مبتنی بر فرهنگ و عقاید جامعه جهت ورود و استفاده از فضای مجازی امری لازم و ضروری است و لزوم و اقتضای این مهم را عقل مستقلا درک می کند. از یافته‌های پژوهش حاضر می‌توان به ضرورت عقلانی بهره‌گیری از عامل تنظیم‌کننده و سازمان‌دهنده استفاده از فضای مجازی اشاره کرد که همان «قانون» نام دارد و عدم وجود آن موجب هرج و مرج، نابسامانی و اختلال در امنیت روانی جامعه می‌شود و در نهایت استفاده از قواعد کاربردی فقهی نظیر قاعده اعانت بر اثم با رویکرد تبیینی-تنبیهی می‌توانند در ساماندهی بیش از پیش فضای سایبری مؤثر باشند.

کلمات کلیدی: فضای مجازی، اعانت بر اثم، مجازات، علم فقه، پیشگیری.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1035

بررسی امکان جرم‌انگاری جرایم مرتبط با اعانت بر اثم در فضای مجازی

محسن نادری[۱]
[۱]دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
mnnnnarsenal9085@gmail.com
علی‌اکبر ایزدی فرد[۲]
[۲]عضو هیئت علمی دانشگاه و استاد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
izadifard@umz.ac.ir
محمدمهدی زارعی[۳]
[۳]استادیار و عضو هیئت علمی گروه فقه و مبانی حقوق اسلامی دانشگاه مازندران
m.zarei@umz.ac.ir

چکیده: قوانین جزایی جامعه ایران به‌لحاظ محتوایی برگرفته از فقه و حقوق اسلامی است. برای برخی از جرایم و گناهان در فقه و حقوق اسلامی توسط شارع مجازات معینی تعیین شده است که باید عیناً همان حکم توسط محکمه اجرا شود. در مقابل نسبت به برخی از موارد شارع مجازات معینی را تعیین نکرده است. یکی از این موارد اعانت بر اثم است. اعانت بر اثم حرام است و هر آنچه که حرام بوده و قابلیت مجازات دنیوی را داشته باشد محکمه می‌تواند مجازات تعزیری را برای آن در نظر بگیرد. پژوهش حاضر با روش توصیفی-تحلیلی و مراجعه به کتب فقهی و آراءفقها، همراه با توجیه، تبیین و استدلال و استنتاج است. مستنداتی برای حرمت اعانت بر اثم توسط فقها مطرح شده است. بررسی این مستندات و تعمیم آن نسبت به فضای مجازی این امکان که بتوان جرایم مرتبط با اعانت بر اثم را در فضای سایبری جرم‌انگاری کرد را فراهم می کند. خلاصه این که با استدلال و تبیین این مستندات حرمت اعانت بر اثم اعم از فضای حقیقی و فضای مجازی اثبات می شود و با توجه به حکم حرمت محاکم قضایی می‌توانند از جنبه تعزیری مجازات متناسبی را برای موارد مختلف اعمال کنند.

کلمات کلیدی: اعانت بر اثم، مستندات، فضای مجازی، فضای حقیقی، امکان مجازات.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1037

اثر آموزش سواد رسانه‌ای بر هویت ملی

علیرضا بخشایش[۱]، مریم بابایی[۲]
[۱]عضو هیئت علمی بخش‌های روان‌شناسی و علوم تربیتی دانشکده روان‌شناسی و علوم تربیتی دانشگاه یزد
abakhshayesh20@yahoo.com
[۲]دانشجوی کارشناسی ارشد روان‌شناسی عمومی دانشگاه یزد
mary.babaei@yahoo.com

چکیده: هویت از مهم‌ترین موضوعات و مفاهیم علوم انسانی است که در عصر اطلاعات دستخوش تغییر و دگرگونی شده است. هویت ملی از جمله مفاهیمی است که به‌علت اهمیت ویژه‌ی آن برای دولت و ملت‌ها، حفظ آن ضروری است. رسانه‌ها نیز از جمله عواملی هستند که می‌توانند، این نوع هویت را به نفع خود تقویت یا تضعیف کنند. اما در صورتی که مخاطب مجهز به سواد رسانه‌ای باشد، تحت تأثیر ظاهر پیام‌ها قرار نمی‌گیرد و از هویت ملی خود محافظت می‌کند. هدف و روش: هدف از نگارش این مقاله بررسی یافته‌هایی بود که هویت ملی، تأثیرپذیری آن از رسانه و فایده‌ی سواد رسانه‌ای در حفظ هویت ملی را مورد بررسی قرار داده بودند، به‌همین دلیل به روش کتابخانه‌ای (تحلیلی- اسنادی) و با استفاده از کتاب ها، منابع الکترونیکی و بانک‌های اطلاعاتی این کار انجام شد. نتیجه‌گیری: با بررسی‌های به‌عمل آمده نتیجه می‌گیریم که هویت ملی متأثر از رسانه‌های جمعی و فناوری اطلاعات و ارتباطات است و راه محافظت از این تأثیرات، مجهز بودن به سواد رسانه‌ای است.

کلمات کلیدی: هویت ملی، رسانه، بحران هویت، عصر ارتباطات، سواد رسانه‌ای.

Code: CYSP2023-1038

تأملی در ماهیت و معنای آسیب‌زایی فضای مجازی

محمود مختاری[1]
[1]استادیار فلسفه علم و فناوری، پژوهشکده مطالعات بنیادین علم و فناوری، دانشگاه شهید بهشتی، تهران
ma_mokhtari@sbu.ac.ir

چکیده: در خصوص آسیب‌زایی اینترنت و فضای مجازی، عبارات و مضامینی از این قبیل دیده (یا شنیده) می‌شود که «فضای مجازی بلای خانمان‌سوز است»، «شبکه‌های اجتماعی، باعث توسعه انحرافات جنسی شده‌اند»، و غیره. این رویکرد عام به اثرگذاری فضای مجازی، حاکی از باور به چیزی است که آن را، «عاملیت فضای مجازی» می‌نامیم. مباحث و مناقشات حوزه مطالعات نظری فناوری، نشان می‌دهد که تلقی فوق از ارتباط بین فناوری و جامعه، بسیار ساده‌انگارانه است. نه‌تنها پذیرش گزاره مزبور، به‌سهولت ممکن نیست بلکه بررسی و ارزیابی آن نیز با مشکلاتی مواجه است. هدف مقاله حاضر این است که با طرح و بررسی طیف رویکردهای مطرح درباره عاملیت اجتماعی فناوری (با تأکید بر فناوری فضای مجازی) و با توجه به نتایج سیاست‌گذارانه هر رویکرد، به این پرسش پژوهشی پاسخ دهد که «آیا و به چه معنا می‌توان از آسیب‌زایی فضای مجازی سخن گفت؟» ادعای مقاله آن است که در بین مهمترین دیدگاه‌ها (که شرح و بررسی خواهد شد)، «نظریه سیستمی» (یا همان سیستم‌های فنی-اجتماعی) هم از جنبه نظری و هم از جنبه سیاست‌گذارانه، پاسخ واقع‌بینانه‌تری برای پرسش پژوهشی این مقاله فراهم می‌کند.

کلمات کلیدی: فضای مجازی، تحولات اجتماعی، عاملیت فناوری، جبر فناوری، وساطت فناوری، کنش گر-شبکه، سیستم‌های فنی-اجتماعی.

Code: CYSP2023-1039

چالش‌های رفتاری به‌کارگیری کلان‌داده در فضای سایبر

سید کمال واعظی[۱]، فرانک پاشایی[۲]
[۱]دانشیار، دانشکدگان مدیریت دانشگاه تهران، تهران
vaezi_ka@ut.ac.ir
[۲]دانشجوی دکتری، پردیس بین‌المللی کیش دانشگاه تهران، کیش
faran.pahaei@gmail.com

چکیده: این مقاله تلاش می‌کند تا سهمی انتقادی در بحث چالش‌های رفتاری بکارگیری کلان‌داده در فضای سایبر ارائه دهد و برای بررسی این موضوع از بینش‌های اقتصاد رفتاری استفاده کرده تلنگرها را به عنوان ابزاری برای اصلاح چالش‌های رفتاری معرفی می‌کند. علاوه بر مطالعه فرصت‌ها و چالش‌های استراتژی‌های کلانداده برای دولت، جامعه و سیاست‌گذاری، این مقاله بررسی می‌کند که چگونه کلان‌داده پتانسیل سوءاستفاده یا همسوبودن با اهداف سیاست‌گذاران را دارد یا ممکن است تأثیرات منفی بر جامعه داشته باشد و نتیجه‌گیری می‌کند با اینکه کلان‌داده یک جایگزین کاربردی در محیط‌های نامطمئن تصمیم‌گیری با ایجاد بینش عمیق‌تر در مورد مسائل اجتماعی و تصمیم‌گیری است، ممکن است نتواند بین مهم‌ترین ارزش‌های انسانی مانند حریم خصوصی، برابری، محرمانه بودن، شفافیت، هویت، انتخاب آزاد و تبعیض و استفاده قانع‌کننده از کلان‌داده تعادل برقرار کند. این موضوع در کشورهای درحال‌توسعه به‌دلیل شکاف دیجیتالی در کاربردهای کلان‌داده، با خطر افزایش نابرابری بین نهادهایی که به داده‌ها دسترسی دارند و آنان که دسترسی ندارند، جدی‌تر است. این تحقیق، چهار نوع تلنگر سنتی، دیجیتال، بیش‌تلنگر و تاریک در سه ساختار مختلف سوگیری بازخورد، طرفدار اجتماع و طرفدار خود معرفی می‌کند تا راهحل مناسب چالش‌های رفتاری نسبت به کلان‌داده را معرفی کند و در انتها بر بیش‌تلنگرها تأکید دارد.

کلمات کلیدی: کلان‌داده، تلنگر، سو گیری شناختی، رفتار، فضای سایبر.

Code: CYSP2023-1040

تشخیص میزان خطر امنیتی برنامه‌های موبایل با استفاده از مفهوم آنتروپی

محمود دی‌پیر[۱]، تکتم ذوقی[۲]
[۱]دانشیار دانشکده رایانه و فناوری اطلاعات، دانشگاه هوایی شهید ستاری، تهران، ایران
mdeypir@ssau.ac.ir
[۲]استادیار گروه مهندسی کامپیوتر و برق، دانشکده شریعتی، دانشگاه فنی و حرفه‌ای، تهران، ایران
t.zoughi@shariaty.ac.ir

چکیده: امنیت دستگاه‌های همراه با توجه به افزایش کاربرد آنها نقش مهمی در امنیت فضای سایبری دارد. با گسترش کاربرد آنها، بدافزارهای زیادی نیز برای سوء استفاده از کاربران آنها توسط نفوذگران ارائه شده است. شناختن سطح خطر امنیتی هر نرم‌افزار می‌تواند در اطلاع‌رسانی به کاربر درباره استفاده از نرم‌افزارهای مخرب، تأثیرگذار باشد. می‌توان به‌صورت تقریبی خطرات امنیتی نرم‌افزارهای اندروید را از طریق بررسی مجوزهایی که آنها درخواست می‌دهند، تخمین زد. در این بررسی بر اساس تعریف مجوزهای بحرانی و با تجزیه و تحلیل مجوزهای درخواستی توسط نرم‌افزارهای خبیث و نرم‌افزارهای قابل اعتماد و شناخته شده، معیار جدیدی به منظور اندازه‌گیری خطر امنیتی برنامه‌های اندروید ارائه شده است. در این معیار مجوزهایی اثر بیشتری در محاسبه مقدار خطر امنیتی دارند که آنتروپی بیشتری در تشخیص برنامه‌های مخرب از برنامه‌های کاربردی داشته باشند. همچنین میزان خطر هر برنامه موبایل برابر با مجموع بهره اطلاعاتی مجوزهای درخواستی آن است. آزمایش‌های صورت گرفته روی داده‌های واقعی نشان‌دهنده نرخ تشخیص بالاتر معیار پیشنهادی در مقایسه با استانداردهای گذشته قرار دارد.

کلمات کلیدی: مجوز، ارزیابی ریسک امنیتی، معیار امنیتی، داده‌کاوی، آنتروپی، بهره اطلاعاتی، تحلیل ایستا، تحلیل پویا.

Code: CYSP2023-1041

چالش‌های اجتماعی و امنیتی در توسعه متاورس

جمشید نصرت آبادی[۱]، مجید سلیمانی ساسانی[۲]، امیرمحمدشیرخدا[۳]
[۱]استادیار و عضو هیئت علمی دانشگاه فارابی، تهران، ایران
dr.nosratabadi110@gmail.com
[۲]استادیار و عضو هیئت علمی دانشگاه تهران، تهران، ایران
msoleimani@ut.ac.ir
[۳]دانشجوی کارشناسی ارشد، دانشگاه فارابی، تهران، ایران
ariadata@ymail.com

چکیده: با توجه به گسترش روز افزون دانش و فناوری، مفاهیم و واژگان جدیدی جای واژگان قدیمی را پر می‌کنند. پس از شکست پروژه زندگی دوم، آرزوها و دست‌نیافتنی‌های واقع در ذهن بشر تمام نشد، بلکه جای خود را با مفهومی کامل‌تر و جامع‌تر به نام متاورس تکمیل کرد. توجه به پیوست اجتماعی و اخلاقی تکنولوژی‌های نوظهور از مهم‌ترین عوامل رشد و توسعه آنها می‌باشد. اما در متاورس فعلی فقط شاهد تغییر در تجارت دارایی‌های مجازی به‌صورت آنلاین و در بازی‌های آنلاین هستیم، جایی که کاربران می‌توانند دارایی‌های دیجیتال مانند لوازم جانبی برای آواتارها را ایجاد و یا خرید و فروش کنند. ما در این پژوهش ضمن بازخوانی مفاهیم مطرح شده برای کلیدواژه متاورس و تکنولوژی‌های در دسترس، به بیان چالش‌ها و مشکلات اجتماعی و امنیتی که در راه تکامل این تکنولوژی و یا مفهوم آن به‌کار می‌آید با دسته‌بندی کپی‌رایت، حریم‌خصوصی، نگهداری و حفاظت از داده‌ها در بخش امنیتی و هویت افراد، تبعیض و سوگیری، سلامت افراد، قطبیت در جامعه، آزادی، قوانین و حکومت‌ها در بخش اجتماعی می‌پردازیم. لازم به ذکر است این مقاله با استفاده از مطالعات کتابخانه‌ای مقالات معتبر متعدد در این حوزه تنظیم شده است.

کلمات کلیدی: متاورس، چالش‌های متاورس، اخلاق در متاورس، فراجهان، دنیاهای مجازی، واقعیت مجازی، هوش‌مصنوعی، حریم‌خصوصی.

Code: CYSP2023-1045

مدیریت داده‌های پزشکی با کمک زنجیره بلوکی

زهرا امین مهر[۱]، فضل الله ادیب نیا[۲]
[۱]دانشجوی کارشناسی ارشد شبکه‌های کامپیوتری، فناوری اطلاعات، دانشگاه یزد، یزد
zahraaminmehr@stu.yazd.ac.ir
[۲]دانشیار دانشکده مهندسی کامپیوتر، فناوری اطلاعات، دانشگاه یزد، یزد
fadib@yazd.ac.ir

چکیده: در سال‌های اخیر، صنعت مراقبت‌های بهداشتی شاهد تحولی انقلابی با ادغام دستگاه‌های پزشکی به هم پیوسته، تجزیه و تحلیل داده‌ها و اتصال به اینترنت بوده است. اینترنت اشیاء پزشکی به شبکه‌ای از دستگاه‌های پزشکی، حسگرها، برنامه‌های کاربردی نرم‌افزاری و سیستم‌هایی اشاره دارد که برای بهبود ارائه مراقبت‌های بهداشتی، نظارت بر بیمار و رفاه کلی، به هم مرتبط هستند. این زیست‌بوم به هم پیوسته به دستگاه‌های پزشکی اجازه می‌دهد تا به طور یکپارچه با یکدیگر ارتباط برقرار کنند، اطلاعات مهم سلامتی را جمع آوری و تبادل کنند. با این حال، این داده‌ها بسیار حساس هستند و به یک سیستم ذخیره‌سازی و مدیریت ایمن و قابل اعتماد، نیاز دارند. در اینترنت اشیاء پزشکی چالشی که وجود دارد بحث امنیت و صحت داده‌ها و همچنین احراز هویت پزشکان و بیماران است. جهت برطرف نمودن این چالش، روش‌های مختلفی ارائه شده که هرکدام مزایا و معایبی دارند. معماری پیشنهادی در این مقاله ترکیبی از زنجیره بلوکی و پایگاه‌داده MongoDB است و معایب روش‌های دیگر را بهبود می‌بخشد. از جمله مزایای این مدل پیشنهادی مقیاس‌پذیری، کاهش سربار محاسباتی، حفظ حریم خصوصی و افزایش امنیت است.

کلمات کلیدی: امنیت، اینترنت اشیاء پزشکی، زنجیره بلوکی، محاسبات مه، MongoDB.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1049

مفهوم‌شناسی هوش دیجیتالی

مرضیه پورصالحی نویده[۱]، احمدرضا متین‌فر[۲]
[۱]استادیار، گروه روان‌شناسی، دانشگاه آزاد اسلامی واحد تهران شرق، تهران
m_poursalehy@yahoo.com
[۲]استادیار، گروه فناوری، دانشگاه امام حسین(ع)، تهران
a_vizand@yahoo.com

چکیده: هدف از پژوهش حاضر معرفی چهارچوب نظری هوش‌دیجیتالی بود. هوش‌دیجیتالی مجموعهٔ کاملی از شایستگی‌های دیجیتالی است که برای پیشرفت در انقلاب‌صنعتی‌چهارم موردنیاز است. صلاحیت اساسی هوش‌دیجیتالی، شهروندی دیجتال است که افراد را قادر می‌سازد از فناوری به‌طور ایمن، مسئولانه و به روشی اخلاقی استفاده کنند.این مجموعهٔ جامع از صلاحیت‌های دیجیتالی، ریشه در ارزش‌های اخلاقی همگانی دارد تا از افراد برای استفاده، کنترل و ایجاد فناوری برای پیشبرد بشریت استفاده کنند. هوش دیجیتالی قصد دارد با تهیهٔ نسخه‌ای جهانی برای مهار فناوری برای آیندهٔ مشترک در طی انقلاب صنعتی چهارم، نیازهای سیستم‌های آموزشی، صنایع و دولت‌ها را پوشش دهد. هوش‌دیجیتالی دربرگیرنده ۸ حوزه با عنوان ۱) هویت دیجیتالی؛ ۲) مصرف دیجیتالی؛ ۳) ایمنی دیجیتالی؛ ۴) امنیت دیجیتالی؛ ۵) هوش‌هیجانی دیجیتالی؛ ۶) ارتباط دیجیتالی؛ ۷) سواد دیجیتالی و ۸) حقوق دیجیتالی است. مهارت‌های دیجیتالی ماهیتی متوالی و شرطی دارند به این معنا که آن‌ها بر یکدیگر بنا نهاده می‌شوند. هوش‌دیجیتالی، افراد را قادر به تعامل موفقیت‌آمیز در زیست‌بوم دیجیتالی نموده و حل مسائل مورد نیاز در محیط‌های مجازی را ممکن می سازد. برای تبدیل‌شدن افراد به شهروندان دیجیتالی خردمند، شایسته و آمادهٔ آینده که با موفقیت از فناوری استفاده نمایند، توجه به هوش‌دیجیتالی از ضروریات است.

کلمات کلیدی: هوش، هوش‌دیجیتالی، سوادرسانه، مهارت دیجیتالی، شایستگی دیجیتالی.

Code: CYSP2023-1050

کاربرد جنگ سایبری در جنگ‌های آینده

سجاد سلطانی رضایی سیر[1]
[1]دانشگاه تهران
sajadsoltani222@yahoo.com

چکیده: امروزه انسان‌ها به این فکر افتاده‌اند که سلاح را به‌طور کامل از دستان هم‌نوعانشان بیرون بکشند و این بار سنگین را به دوش کامپیوترها بیندازند. مهم‌ترین اقدام در این زمینه ترقی سیستم‌های اطلاعاتی کامپیوتری است که با تکثیر سیستم‌های خودکار و نیمه‌خودکار سیار مثل روبات‌ها ترکیب شده است. اهمیت اطلاعات در جنگ‌ها حتی بیشتر از اهمیت سربازان و سلاح‌ها و دیگر استانداردهای قدیمی‌است. جنگ اطلاعاتی نشانه‌ای از دوران مدرن ماست. دنیای مدرن ما شدیداً وابسته به انواع فناوری‌ها و به‌خصوص کامپیوتر است. جایی هم که وابستگی وجود داشته باشد، سطح آسیب‌پذیری بالاتر می‌رود. جنگ سایبری یکی از این مقوله‌هاست که در فضای مجازی بین تجهیزات ارتباطی، مخابراتی، شبکه‌های رایانه‌ای و سیستم‌های مبتنی بر رایانه با شدت تمام توسط کشورهای صاحب فناوری بر علیه سایرین است. آینده جنگ سایبری را همه کشورها دنبال می‌کنند و در این راستا بارها اندیشمندان آینده‌پژوهی از حملات سایبری به‌عنوان تهدید آینده یاد کرده‌اند. در این مقاله در پی پاسخ به این سؤال هستیم که کاربرد جنگ سایبری در جنگ‌های آینده چگونه است؟ فرضیه ما نیز این است که سال‌ها است که استفاده از تکنولوژی‌های آینده‌نگرانه در ساخت سلاح‌های پیشرفته مورد توجه قرار گرفته و تکنولوژی‌های عجیب و غریب بسیار بیشتری نیز در راه است که سلاح‌های استفاده شده در فیلم‌های علمی-تخیلی را به واقعیت تبدیل خواهند کرد.

کلمات کلیدی: سایبر، الکترونیک، جنگ، رایانه، سلاح، ارتباط، آینده.

Code: CYSP2023-1051

اکوسیستم متاورس با محوریت جرائم مالی در آن

عباس ترکاشوند[۱]، رضا مالکی پور[۲]
[۱] کارشناسی مهندسی فناوری اطلاعات، دانشگاه پیام نور تهران
abbas.38947@gmail.com
[۲] کارشناسی مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد ملایر
hajiradmehr2023@gmail.com

چکیده: متاورس، دریچه‌ای به روی فضاها و ایجاد هویت جایگزین برای تجربیات انسانی بازکرده است. اهمیت روزافزون متاورس در دنیای مجازی و تداوم دنیای دیجیتال برای بسیاری از کاربران به‌عنوان یک مفهوم خیالی و یا غیرممکن شناخته شده است، اما حقیقت این است که ما در حال حاضر در میان متاورس‌های اولیه زندگی می‌کنیم و آینده قبل از اینکه واقعاً برای ایجاد آن آماده باشیم، وجود دارد. اکوسیستم متاورس به‌سرعت در حال رشد است و نوآوران و شرکت‌های بزرگ فناوری در این اکوسیستم قرار دارند. اگر متاورس یک دنیای مجازی باشد، برای کنترل کلاه‌برداری‌ها و جرائم مالی به نسخه مجازی از پلیس نیاز است. با توجه به برنامه‌های متاورس، به نظر می‌رسد حمایت از برنامه‌های ضد پول‌شویی به همان اندازه که در دنیای واقعی اهمیت دارد، در دنیای مجازی نیز اهمیت دارد. در این مقاله سعی در معرفی اجزای تشکیل‌دهنده اکوسیستم متاورس، سرمایه‌گذاری در آن و در نهایت جرائم و تخلفات ابزارهای مالی در متاورس تشریح شده است.

کلمات کلیدی: متاورس، NFT، مالی، جرائم، هویت، رمز ارز.

Code: CYSP2023-1052

توسل حق دفاع مشروع در حملات سایبری در حقوق بین‌الملل

علی حیدری، بیژن حیدری
ali.heydari.4001@gmail.com

چکیده: یکی از شیوه‌های نوین تخاصم درصحنه بین‌المللی، حملاتی است که در بستر فضای سایبری صورت می‌گیرد، هرچند این حملات پتانسیل ایجاد تلفات گسترده و خسارات وسیع را دارند اما سرعت بالای تغییرات در این حوزه موجب گردیده است که حقوق بین‌الملل از وضع قواعد جدید متناسب با فضای سایبری عاجز بماند. استفاده از فضای سایبری برای دستیابی سریع و مؤثر به اهداف راهبردی، امروزه به ابزار جدید جنگی و مهم برای همه بازیگران دولتی و غیردولتی تبدیل شده است. شناسایی قلمرو حقوقی آن نیز با موانعی در شرایط مختلف و از جمله حقوق جنگ و حق دفاع مشروع رو به روست که ورود حقوق بین‌الملل به بحث را با چالش مواجه کرده است. در این پژوهش با رویکرد توصیفی و استفاده مطالعات پیشین سعی شده است تا به بررسی ابعد موضوع مطرح شده پرداخته شود.

کلمات کلیدی: جنگ سایبری، حقوق بین‌الملل، حملات سایبری، دفاع مشروع.

Code: CYSP2023-1055

اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل

سید حسین علوی[۱]، محمدرضا حسینی[۲]، مهراب رامک[۳]
[۱] دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
h.alavi@aut.ac.ir
[۲] دانشیار گروه مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
rezahsn88@gmail.com
[۳] دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
m.ramak@aut.ac.ir

چکیده: در ابتدای شکل‌گیری فضای سایبر، برخی نظریه‌پردازان بر این باور بودند، توسعه فضای سایبری و برقراری تعاملات اقتصادی، سیاسی و فرهنگی در سطح جهانی، با تعابیری از قبیل مرززدایی، سرزمین‌زدایی، قلمروزدایی و حاکمیت‌زدایی همراه خواهد بود اما هم اکنون به‌طور گسترده‌ای پذیرفته شده است که فضای سایبری یک منطقه عاری از قانون نیست که در آن هر کس بتواند با رفتار بدون ضابطه و بدون در نظر گرفتن قوانین، مقررات و قواعد پذیرفته شده بین‌المللی، هر گونه فعالیت خصمانه‌ای انجام دهد. مسئله اصلی این پژوهش این است که آیا اصول و قواعد حقوق بین‌الملل حال حاضر، با قاطعیت و شفافیت از اقدامات خصمانه سایبری که حاکمیت کشورها بر قلمرو سایبری را نقض می‌کنند، جلوگیری می کند و این اصول و قواعد قابل اتکا در صیانت از حاکمیت کشورها بر قلمرو سایبری ملی هستند؟ این نوشتار با مرور و بررسی اسناد، اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی که با استفاده از روش تحلیل محتوای کیفی و ابزار نرم‌افزار مکس‌کیودا انجام پذیرفته است نتیجه می‌گیرد، اصول و قواعد حقوق بین‌الملل حال حاضر از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و عموماً اقدامات ناقض حاکمیت سایبری ملی با شدت متوسط و کم (اعم از: توسل به زور، مداخله غیرمجاز و ...) فاقد پیگرد قانونی هستند. از این رو این قواعد و اصول در مقابل اقدامات مخرب و ناقض حاکمیت سایبری ملی از بازدارندگی لازم برخوردار نیستند.

کلمات کلیدی: قلمرو سایبری، حاکمیت ملی سایبری، اصول و قواعد حقوق بین‌الملل.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1058

پیشنهاد ریشه‌شناسی جدید برای مفهوم سایبر با استفاده از روش زبان‌شناسی تاریخی

محمد شمس‌الدینی[۱]، کاظم فولادی قلعه[۲]
[۱]پژوهشگر آینده‌پژوهی، پژوهشکده حضرت ولیعصر (عج)، دانشگاه جامع امام حسین (ع)
shams.m@chmail.ir
[۲]استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده: یکی از روش‌های فهم دقیق معانی الفاظ، ریشه‌شناسی آنهاست. در ریشه‌شناسی مفهوم سایبرنتیکز، هیچ پژوهشگری تا کنون، ریشه‌ی آن را به مفهومی غیر از کوبرنتس (kybernetes) در زبان یونانی نبرده است؛ اما تقریباً همه‌ی این پژوهشگران، پیش از آن را بررسی نکرده‌اند و به نظر می‌رسد که با مطالعه‌ی پیش از یونان، معانی مهم‌تری از این مفهوم، روشن می‌شود. در این پژوهش، برای رسیدن به معنای دقیق‌تری از مفهوم سایبرنتیکز و به‌طور خاص مفهوم سایبر، با استفاده از روش زبان‌شناسی تاریخی و به‌طور مشخص، ریشه‌شناسی و عبارت‌شناسی، سعی شده است تا ریشه‌های پیش‌تری از این مفهوم را در نزد متفکرانی که این مفهوم را استفاده کرده‌اند، کاوش کنیم. در نتیجه با ریشه‌شناسی مفهوم سایبر و مفاهیم نزدیک به آن مانند جبر، زمینه‌های جدیدی از ریشه و معنای تاریخی سایبر پیشنهاد شده است. نهایتاً با دسته‌بندی شواهد و طرح ۶ محور مفهومی به‌عنوان شاهد برای هم‌ریشگی دو مفهوم سایبر و جبر، مدعی شده‌ایم که سایبر، برگرفته از مفهوم جبر است و به‌لحاظ کارکردی نیز، اراده‌ای که در پس جهان سایبر قرار گرفته است، همان اراده‌ای است که در بنیاد معنایی مفهوم جبر نشسته است.

کلمات کلیدی: ریشه‌شناسی، سایبر، جبر، زبان‌شناسی تاریخی.

Code: CYSP2023-1062

تبیین فضای سایبری و پیامدهای اجتماعی ناشی از آن در سیاست جنایی ایران

سودا آقامحمدزاده[1]
[1] کارشناسی حقوق، دانشگاه آزاد اسلامی، واحد شبستر، ایران
sevda81amzd@gmail.com

چکیده: با توجه به رشد تکنولوژی رایانه‌ای و تحول اطلاعات وهمچنین گسترش ارتباطات در فضای سایبری و متعاقباً سهولت ارتکاب جرایم مرتبط با فناوری‌های نوین، بحث روزآمد شدن و لزوم تدوین قوانین بسیار ضروری است. هدف این تحقیق ارائه راهبردهایی برای پیشگیری از آسیب‌های فضای مجازی است. در این پژوهش که به روش توصیفی–تحلیلی می‌باشد سعی بر آن شد سیاست جنایی ایران در رابطه با فضا و تدابیر پیشگیری از جرم در حوزه پدافند سایبری مورد بررسی قرار بگیرد که یافته‌ها نشان از آن دارد که در زمینه راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی، ابعاد حذف توجیه‌کننده‌ها، کاهش منافع حاصل از جرم، افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم و افزایش خطرهای مدنظر برای ارتکاب جرم به‌ترتیب بالاترین تا پایین‌ترین میانگین رتبه‌ای تأثیر در پیشگیری از آسیب‌های فضای مجازی را دارند. مهم‌ترین نتیجه این تحقیق، استخراج تدابیری در قالب راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی است که استفاده از آنها می‌تواند تاثیر زیادی در پیشگیری از آسیب مجازی، کاهش جرایم، حبس‌زدایی، و غیره داشته باشد.

کلمات کلیدی: آسیب‌های فضای مجازی ، پیشگیری ، سیاست جنایی ایران ، فضای سایبر.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1063

بررسی نقش و تاثیر قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی

محمدرضا حسینی[۱]، مهراب رامک[۲]، احسان کیان‌خواه[۳]، سید حسین علوی[۴]
[۱] دانشیار گروه مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
rezahsn88@gmail.com
[۲] دکترای تخصصی مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
m.ramak@aut.ac.ir
[۳] دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
e.kiankhah@sndu.ac.ir
[۴] دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
h.alavi@aut.ac.ir

چکیده: با گسترش روزافزون بهره‌برداری از فناوری‌ها و تجهیزات سایبری در زندگی فردی و اجتماعی انسان‌ها، شاهد توجه بیش از پیش کشورها به پدیده قلمرو سایبر ملی با هدف اعمال حاکمیت و ممانعت از تسلط بیگانگان در فضای سایبری ملی هستیم. این پژوهش با بررسی ادبیات مرتبط با حاکمیت بر قلمرو سرزمینی و چگونگی انطباق اصول و قواع حقوق بین‌الملل مرتبط با حاکمیت ملی بر فضای سایبر ملی به تحقیق پیرامون نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی می‌پردازد. تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی است و روش تحقیق مورداستفاده در این پژوهش توصیفی-تحلیلی است که برای گردآوری اطلاعات، از منابع کتابخانه‌ای و اینترنتی استفاده شده است و سعی شده تا مبانی لازم جهت تبیین موضوع از منابع به روز داخلی و خارجی استخراج گردد. محققین پس از تجزیه و تحلیل اطلاعات نتیجه‌گیری کردند قلمروگذاری و مرزبانی فضای سایبری می‌تواند نقش بسزایی در اعمال حاکمیت بر فضای سایبر ملی داشته باشد و برخورداری از اصول و قواعد حقوق بین‌الملل، پیگیری‌های قانونی و دفاع از فضای سایبر ملی مستلزم تعریف و اعلان قلمرو سایبری ملی و مرزبانی مؤثر این فضا می‌باشد. به‌علاوه تعریف نشدن قلمرو و مرز ملی در فضای سایبری، رفتار قانون‌مند کنشگران خصوصی و دولتی در یک فضای قانونی را به همراه نخواهد داشت و منجر به تضعیف نظام حاکم و امنیت ملی خواهد شد. نتایج حاصل از این تحقیق گسترش دانش و شناخت بهتر تصمیم‌گیران و متولیان امر در کشور را به همراه خواهد داشت.

کلمات کلیدی: اصول و قواعد حقوق بین‌الملل، حاکمیت ملی، قلمرو گذاری و مرزبانی فضای سایبری.

Code: CYSP2023-1068

زندگی در ناواقعیتِ ماتریکس و فضای سایبری

مرتضی سعیدی ابواسحاقی[۱]، راضیه سعیدی ابواسحاقی[۲]
[۱]دانشجوی دکتری فلسفه دانشگاه تهران، پژوهشگر پژوهشگاه فضای مجازی
morteza.saeidi@ut.ac.ir
[۲]دانش آموخته کارشناسی تعلیم و تربیت، دانشگاه فرهنگیان
raziyesaeedi9819@gmail.com

چکیده: فیلم ماتریکس (۱۹۹۹) انسان‌ها را به‌نحوی تصویر می‌کند که در فضایی کامپیوتری اسیر شده‌اند و بدن آنها در خمره‌ای لزج و مغذی به‌عنوان منبع انرژی ماتریکس قرار دارد و ماتریکس جهانی می‌سازد و به ذهن انسان‌ها این را القاء می‌کند که همین، واقعیت است. فضای ماتریکس را با فضای سایبری و شبکه‌های مجازی مقایسه کرده‌ایم که در فضای مجازی نیز واقعیتی شبیه به ماتریکس در حال رقم خوردن است و انسان‌ها در حال تخدیر شدن هستند، تا جایی که زندگی در ماتریکس و زندگی در فضای سایبری همانند زندگی در ناواقعیت است. ناواقعیتی که انسان‌ها به دلیل تخدیر و احساس لذت خیلی وقت ها نمی‌خواهند از آن آزاد شوند. در این مقاله بیان شده است که این امکان بر اساس حقیقت سوبژکتیوته و ریاضیاتی شدن جهان و ابژه شدن انسان وقوع پیدا می‌کند، و فیلم ماتریکس را تذکری هوشمندانه از طرف هنر برای انسان‌ها می‌دانیم.

کلمات کلیدی: ماتریکس، سوبژکتیویته، فضای سایبری، ابژه، انسان.

Code: CYSP2023-1069

بهبود بازشناسایی شخص با استفاده از یادگیری انتقالی و شبکه‌های سیامی

سجاد عموئی ششکل[۱]، کاظم فولادی قلعه[۲]، حسین آقابابا[۳]
[۱]دانش‌آموخته کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
sajad.amouei@ut.ac.ir
[۲]استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir
[۳]دانشیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
aghababa@ut.ac.ir

چکیده: بازشناسایی شخص در جامعه تحقیقاتی محبوبیت بالایی به‌دست آورده و دلیل آن افزایش کاربردها و اهمیت آن در صنعت نظارت است. بازشناسایی شخص به‌دلیل وجود تغییرات درون‌کلاسی و بین‌کلاسی در دوربین‌های مختلف همچنان به‌عنوان یک مسئله‌ی چالشی مورد بررسی قرار می‌گیرد. در این مقاله یک شبکه از نوع سیامی معرفی می‌شود که جفت تصاویر را دریافت کرده و سپس با استفاده از شبکه پیش‌آموزش داده شده، ویژگی‌های تصاویر را استخراج می‌کند و در نهایت خروجی توسط یک تابع اتلاف تصدیق تعیین می‌شود. به‌منظور به‌دست آوردن ویژگی‌های عمیق‌تر از تصاویر عابران پیاده، از شبکه پیش‌آموزش داده شده EfficientNet B0 برای استخراج ویژگی‌ها استفاده کردیم. آزمایش‌ها را روی مجموعه داده CUHK01 برای نشان دادن دقت روش پیشنهادی انجام دادیم. دقت روش پیشنهادی در رتبه ۱، رتبه ۵، رتبه ۱۰، رتبه ۱۵ و رتبه ۲۰ به ترتیب ٪۷۰، ٪۹۵، ٪۹۹، ٪۹۹ و ٪۹۹ می‌باشد. نتایج نشان می‌دهد که روش ارایه شده نسبت به روش‌های به‌روز دارای عملکرد بهتری است.

کلمات کلیدی: بازشناسایی شخص، شبکه سیامی، اتلاف تصدیق، EfficientNet B0.

Code: CYSP2023-1070

تبیین نظری مؤلفه‌های نظام سایبرنتیک ومقایسه آن با مؤلفه‌های نظام ولایت

رضوان هامانی[۱]، زهرا حصارکی[۲]
[۱]طلبه سطح چهار حکمت متعالیه جامعة الزهراء سلام الله علیها و دانشجوی د کتری فلسفه فیزیک دانشگاه باقرالعلوم، قم
rezvanhamani1402@gmail.com
[۲]طلبه سطح چهار کلام اسلامی جامعة الزهراء سلام الله علیها، کارشناسی ارشد فلسفه اسلامی دانشکده هدی، کارشناس و پژوهشگر دوره نقد وهابیت جامعة الزهراء سلام الله علیها، قم
z.hesaraki.chmail.ir

چکیده: تئوری سیستم‌ها نظریه‌ای برای درک و تحلیل کلیت جهان هستی و وقایع و منظومه‌های درون آن است که توان تصمیم‌سازی، تصمیم‌گیری و کنترل‌گری را به شکل چشم‌گیری افزایش داده و به‌عنوان یک روش میان‌رشته‌ای تحولات زیادی را در بستر وسیع سازمان‌های جهان کنونی رقم‌زده است. این تئوری با ایجاد یک تفکر کل‌نگرانه در مدیریت سازمانها، نقش بسیار مهمی در پیدایش نظام سایبرنتیکی و الگوی مدیریت جامع آن داشته است. استفاده از این سیستم در پدیده‌های شناختی و روان‌شناختی برای کنترل و مدیریت جوامع انسانی و سلطه بر حاکمیت‌های محلی، با هدف رسیدن به نظم نوین جهانی، نظام سلطه را در جهان امروز رقم زده است. در مقابل سیستم مدیریت نظام توحیدی علاوه بر هدایت تکوینی عامه، که نظام و سازمان خلقت براساس آن تکوّن یافته و هدایتی همگانی و متحد به‌سوی غایتی است، و هدایت تکوینی خاص، که از طریق عقل و فطرت نوع بشریت را رهنمون است، هدایت تشریعی عامه را در ظرف اختیار و توان کنشگری انتخابی انسانها قرار داده، تا در سیستمی ورای تئوری سیستم‌های حاکم بر هدایت تکوینی، به تنظیم‌گری جامعه و هدایت انسان‌ها برای رسیدن به اهداف متعالی خلقت رهنمون باشد. در این پژوهش با تعریف تئوری جامع سیستم‌ها و با تاکید بر طبقه‌بندی بلدینگ، نظام سایبرنتیکی برآمده از آن معرفی شده و با روشی تحلیلی- توصیفی و بر مبنای هستی‌شناسی حاکم بر فلسفه اسلامی طبقه‌بندی سیستمی که می‌تواند توصیف‌گر نظام ولایت باشد، ارائه گردیده و با بهره از آیات قرآن به مقایسه نظام ولایت با نظام سایبرنتیک پرداخته شده است.

کلمات کلیدی: تئوری سیستم‌ها، نظام سایبرنتیک، نظام ولایت، کنترل، هدایت.

Code: CYSP2023-1072

ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها

بهمن جهانی[۱]، سید نصیب‌اله دوستی‌مطلق[۲]
[۱] دانشجوی دکتری مدیریت راهبردی فضای سایبر گرایش امنیت سایبری، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
bhjahani@gmail.com
[۲] استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
doustimotlagh@chmail.ir

چکیده: نتایج بدست آمده از تحقیقات مراکز پژوهشی و خدمات امنیت سایبری نشان می‌دهد که توسعه فناوری‌های زیرساختی، تدوین و ابلاغ دستورالعمل‌های امنیت سایبری و تربیت متخصصین این حوزه، در دفع تهدیدات چندان موفق نبوده و همچنان خسارت و آسیب به سرمایه‌های سایبری سازمان‌ها رو به افزایش است. یافته‌های این تحقیقات نشان می‌دهد که کارکنان در ایجاد تهدیدات امنیت سایبری سازمان‌ها یا تأمین آن نقش بسیار مهمی دارند که عدم توجه به این موضوع از مهمترین دلایل شکست برنامه‌های امنیت سایبری است. براین‌اساس حوزه جدیدی تحت عنوان فرهنگ امنیت سایبری، به جهت کلیدی بودن فرهنگ در شکل‌دهی به رفتار کارکنان، مطرح گردیده است. این تحقیق در پی یافتن ابعاد و مؤلفه‌های کلیدی و اثرگذار در ایجاد و ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها است. این پژوهش از نوع کاربردی بوده و با استفاده از روش توصیفی تحلیلی با استناد به منابع کتابخانه‌ای، و تحلیل و بررسی اسناد این حوزه و بهره‌گیری از نظرات خبرگان، به دنبال ابعاد و مؤلفه‌های کلیدی ایجاد فرهنگ امنیت سایبری است. نتایج حاصل از تحقیق در سطح راهبردی ۵ بعد و ۱۶ مؤلفه، سطح عملیاتی ۷ بعد و ۱۸ مؤلفه و سطح تکنیکی ۴ بعد و ۸ مؤلفه را بر فرهنگ امنیت سایبری سازمان‌ها مؤثر دانسته است.

کلمات کلیدی: فرهنگ امنیت سایبری، مدل فرهنگ امنیت سایبری، فرهنگ سازمانی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1075

تشخیص وب‌سایت‌های اسپم فارسی با استفاده از پردازش زبان طبیعی

صبا حیدری‌دوست[۱]، امیرحسین کیهانی‌پور[۲]
[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
saba.heydaridoost@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده: تولید صفحات اسپم به عنوان یکی روشهای جلب توجه کاربر به محتوای غیر مطلوب، یکی از چالشهای عمده در حوزه بازیابی اطلاعات به ویژه در محیط وب، بشمار میرود و طی سالهای گذشته، الگوریتمهای مختلفی برای تشخیص آنها مطرح شده است. بر این اساس، روشهای تولید اسپم نیز همزمان با پیشرفت فناوری، تغییر شکل می‌دهند. امروزه، یکی از روش‌های غیرقانونی افزایش رتبه وب سایت، استفاده از وب سایت‌های اسپم است. در این مقاله، ابتدا انواع اسپم و روش‌های شناسایی وب سایت‌های اسپم مورد بررسی قرار گرفته است. سپس یک مجموعه داده شامل وب سایت‌های اسپم و غیر اسپم در وب فارسی، معرفی شده و با استفاده از این مجموعه داده، یک مدل Multinomial Naïve Bayes آموزش دیده است. در این مدل، متون این وب سایت‌ها با توجه به تکنیک‌های پردازش زبان طبیعی، مورد بررسی قرار گرفته است و نهایتاً هر وب سایت، در یکی از دو دسته اسپم و غیر اسپم، دسته‌بندی می‌شود. نتایج ارزیابی روش پیشنهادی روی مجموعه داده متشکل از حدود هزار وبسایت در محیط وب فارسی، حاکی از برتری عملکرد آن نسبت به روش مرجع مورد مقایسه، بر اساس شاخص ارزیابی F-Score و به میزان حدود ٪۲۰٫۲۵ میباشد.

کلمات کلیدی: وب‌سایت‌های اسپم، مدل Multinomial Naïve Bayes، پردازش زبان طبیعی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1079

ابزارهای جنگ شناختی و راه‌کارهای مقابله با آن در حوزه سایبرنتیک

محمود اعتصامی فر[1]
[1]سطح سه تخصصی مدیریت اسلامی و کارشناس ارشد مدیریت رسانه
mimalef69@mail.ir

چکیده: یکی از تحولات دوران معاصر در عرصه نظام بین الملل، انقلاب اطلاعات و فناوری ارتباطات است. تحت تاثیر این فناوری‌ها، جنگ تغییر و تحولات گسترده‌ای به خود دیده که از آن جمله می‌توان به جنگ نرم و تحول مفاهیمی چون امنیت در فضای سایبرنتیک اشاره کرد. امروزه کشور ایران پس از چهار مرحله جنگ سرد، جنگ سخت، نیمه سخت و نرم، وارد پنجمین جنگ سلطه جویان با عنوان جنگ شناختی-ادراکی شده است. جنگ شناختی به معنای هدف قرار دادن قوه شناخت عموم مردم و نخبگان جامعه هدف با تغییر هنجارها، ارزش‌ها، باورها، نگرش‌ها و رفتارها، از طریق مدیریت ادراک و برداشت است. پژوهش حاضر کاربردی و آینده‌نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. نتایج پژوهش نشان می‌دهد که برای مقابله با جنگ شناختی در حوزه سایبرنتیک نیازمند به استفاده از راهبردهای ویژه در مورد اقوام و اقلیت‌ها، شفافیت، اطلاع‌رسانی دقیق و بصیرت افزایی به جامعه، ارتقای سواد رسانه‌ای مخاطبان با استفاده از تمام وسایل ارتباط جمعی، ایجاد راه‌های مشروع برای ارضاء نیازهای مردم، افزایش محصولات فرهنگی تأثیرگذار بر جامعه و جوانان می‌باشد.

کلمات کلیدی: فضای سایبرنتیک، جنگ شناختی، عصر اطلاعات، عملیات روانی.

Code: CYSP2023-1082

شناسایی مالکِ داده‌ها در «هوش مصنوعی» و «اینترنت اشیاء»

محمد امینی[۱]، محمود رستگاری[۲] سعید نصر[۲]
[۱]دانشجوی دکتری حقوق خصوصی، دانشگاه اصفهان، ایران
m.aminiphdlaw74@ase.ui.ac.ir
[۲]دانش‌آموخته کارشناسی ارشد حقوق خصوصی، دانشگاه اصفهان، ایران
{m.rastegari1994,saeednasr11}@gmail.com

چکیده: مالکیت از مفاهیم فقهی – حقوقی با سابقه‌ای است که مردم با آن آشنا بوده و متعلق آن را بیشتر اشیاء مادی تصور می‌کنند و وقتی با لفظ مالک مواجه می‌شوند، بی‌درنگ این لفظ را برای انسان معتبر می‌دانند. ولی به مرور زمان و فرض یا اعطای شخصیت به بعضی از عناوین یا نهادها، وصف ملکیت و مالک شدن برای آن‌ها نیز معقول شناخته شد. امروزه با پیشرفت تکنولوژی و فناوری‌های ارتباطات، برنامه‌ها و ابزارهای نوینی ظهور یافته که از جمله‌ی آنها، هوش مصنوعی (AI) و اینترنت اشیا (IOT) می‌باشد. براین‌اساس پرسش اصلی در تحقیق حاضر آن است که آیا می‌توان هوش مصنوعی و اینترنت اشیا را مالک داده‌هایشان دانست؟ در این خصوص آیا میان این دو تفاوت وجود دارد؟ نگارندگان با روش توصیفی – تحلیل و تدقیق در پژوهش‌های انجام شده و قوانین موجود به این مهم دست یافتند که در هوش مصنوعی با وجود وصف خودمختاری و امکان اعطای شخصیت، می‌توان آن را مالک آفرینه‌های ایجادی‌اش دانست، ولی در اینترنت اشیا، مالک داده‌های ارسالی از سوی شیئ، همان برنامه‌نویس، طراح و کنترل‌کننده‌ای است که این اطلاعات مستقیماً برای او فرستاده می‌شود.

کلمات کلیدی: اینترنت اشیا، شخصیت، مالک (مالکیت)، وصف خودمختاری، هوش مصنوعی.

Code: CYSP2023-1083

تشخیص نفوذ در امنیت سایبری به کمک یادگیری ماشین

سید محمد جواد نصراله[1]
[1]دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
m.javad.nasrolla@gmail.com

چکیده: با گسترش اینترنت، حملات سایبری به‌سرعت در حال تغییر هستند و وضعیت امنیت سایبری خوش‌بینانه نیست. این مقاله، تحقیقات کلیدی در زمینه یادگیری ماشین (ML) و روش‌های یادگیری عمیق (DL) را برای برای تحلیل شبکه و تشخیص نفوذ تشریح می‌کند و شرح مختصری از هر روش ML/DL ارائه می‌دهد. از آنجا که داده‌ها در روش‌های ML/DL بسیار مهم هستند، برخی از مجموعه داده‌های رایج شبکه مورد استفاده در ML/DL را توصیف می‌کنیم و سپس چالش‌های استفاده از آن در امنیت سایبری را توضیح خواهیم داد و پیشنهادهایی را برای تحقیق ارائه می‌کنیم.

کلمات کلیدی: امنیت سایبری، یاد گیری عمیق، یاد گیری ماشین.

Code: CYSP2023-1084

فراسوی GPS: موقعیت‌یابی بصری، سیستم مسیریابی مقاوم به تغییرات جغراسیاسی

عارف برهانی[۱]، کاظم فولادی قلعه[۲]، احسان رزاقی‌زاده[۳]
[۱]دانش‌آموخته مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
rf.borhani@gmail.com
[۲]استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir
[۳]متخصص حوزه یادگیری ماشینی و بینایی ماشین، تهران
ehsanrazaghizade22@gmail.com

چکیده: وابستگی فزاینده به سیستم موقعیت یاب جهانی (GPS) برای مسیریابی، یک آسیب‌پذیری بحرانی را در کاربردهای مختلف نشان داده است، به خصوص زمانی که سیستم‌های مسیریابی سنتی، مانند GPS، به‌دلیل عوامل مختلفی از جمله دستکاری سیگنال، سیگنال‌دهی ضعیف و موارد دیگر در دسترس نیستند. در پاسخ به این چالش، این مقاله پتانسیل «موقعیت‌یابی بصری» را به عنوان یک راه‌حل مسیریابی جایگزین بررسی می‌کند که در برابر محدودیت‌های جغراسیاسی و دستکاری سیگنال قابل اتکا است. هدف این مقاله ارائه یک مرور جامع از تحقیقات موقعیت‌یابی بصری و بررسی قابلیت‌های آن در استفاده به‌عنوان یک راهکار مسیریابی قابل اعتماد است. این مقاله چالش‌ها و محدودیت‌های سیستم‌های کنونی مبتنی بر GPS، اصول و تکنیک‌های زیربنایی اودومتری بصری، و پیشرفت‌های اخیر در این زمینه را مورد بحث قرار می‌دهد. علاوه بر آن، این مقاله نتایج شبیه‌سازی‌های نشان‌دهنده اثربخشی موقعیت‌یابی بصری در سناریوهای مختلف دنیای واقعی را ارائه و ظرفیت آن را به‌عنوان یک جایگزین مناسب برای سیستم‌های مسیریابی مبتنی بر GPS برجسته می‌کند.

کلمات کلیدی: بینایی ماشین، مسیریابی، موقعیت‌یابی بصری (VO)، سیستم موقعیت‌یاب جهانی (GPS).

Code: CYSP2023-1085

بررسی مسئولیت کاربران در فضای مجازی بر اساس قاعده اقدام

سیدرضا چوگان سنبل[۱]، مهدی طالبی چاهوکی[۲]
[۱]طلبه سطح ۲ حوزه علمیه و کارشناسی ارشد مهندسی فناوری اطلاعات و ارتباطات
chogan65@gmail.com
[۲]طلبه سطح ۲ حوزه علمیه، کارشناسی ارشد مهندسی مکانیک
mehditalebich@gmail.com

چکیده: هرگاه شخصی با آگاهی و اختیار، مالش را در معرض تلف قرار دهد، طبق قاعده فقهی اقدام، مسئولیت این کار به عهده وی خواهد بود. پس از توسعه اینترنت و گسترش فناوری‌های نوین ارتباطی، فضای مجازی به بستری برای فعالیت‌های جدید و متنوع تبدیل شده است. با توجه به اینکه در موارد متعددی، کاربران با آگاهی و اختیارخود فعالیت‌هایی در این فضا انجام می‌دهند که امکان بهره‌برداری و سوء استفاده دیگران را فراهم می‌آورد، پاسخ به این مسئله ضروری است که اگر کاربران، آگاهانه اقدام به فعالیتی نمایند که منجر به ورود زیان به ایشان گردد، آیا این اقدام می‌تواند مسئولیت زیان‌زننده را سلب نماید یا خیر. در این پژوهش با روش کتابخانه‌ای، در ابتدا به بررسی قاعده فقهی اقدام و مفاهیم مال و مالکیت در فضای مجازی به‌عنوان دو مفهوم کلیدی در قاعده مزبور پرداخته شد و سپس برخی اقدامات آگاهانه کاربران در فضای مجازی مورد بررسی قرار گرفت و در نهایت بیان گردید که هرگاه شخصی در بستر فضای مجازی اقدامی در جهت اتلاف مالش انجام دهد، مسئولیت آن به عهده خودش است و هرگاه اقدامی غیر مالی انجام دهد که مورد سوء استفاده دیگران واقع شود، نمی‌توان سوءاستفاده‌گر را از مسئولیت مبرا دانست.

کلمات کلیدی: قاعده اقدام، فضای مجازی، اقدام در فضای مجازی، مال و مالکیت در فضای مجازی، مسئولیت زیان در فضای مجازی.

Code: CYSP2023-1086

بررسی نگرش‌ها نسبت به تحولات رفتاری زیست جنسی متأثر از ابژگی زنان در فضای مجازی

حمیده حسین‌زاده[۱]، محبوبه موسیوند[۲]، شهین قربانی[۳]
[۱] کارشناسی‌ارشد رشته مطالعات زنان گرایش زن و خانواده، دانشکده علوم اجتماعی دانشگاه الزهرا (س)، تهران، ایران
hi.hosseinzadeh@gmail.com
[۲] استادیار گروه مطالعات اجتماعی و توسعه، عضو هیئت علمی پژوهشکده زنان دانشگاه الزهرا (س)، تهران، ایران
m.moosivand@alzahra.ac.ir
[۳] دانشجوی کارشناسی‌ارشد رشته مطالعات زنان گرایش زن و خانواده، دانشکده علوم اجتماعی دانشگاه الزهرا (س)، تهران، ایران
hana.qorbani@gmail.com

چکیده: یکی از وسایل ارتباط جمعی که از اهمیت و تأثیرگذاری بالایی برخوردار است، پلتفرم اینستاگرام می‌باشد که در عصر امروز به‌طور گسترده‌ای فراگیر شده و مورد استقبال قرار گرفته است؛ از این رو این مطالعه با هدف بررسی نگرش‌ها نسبت به تحولات رفتاری زیست جنسی متأثر از ابژگی زنان در فضای مجازی به روش کیفی صورت گرفته است؛ نمونه‌ی هدف ۱۱ خانم ۱۶ تا ۳۵ بوده است، که جمع‌آوری اطلاعات از طریق مصاحبه‌های نیمه‌ساختاریافته صورت پذیرفته است. نتایج شامل چهار مضمون اصلی شامل نگرش‌های جنسی، جامعه‌پذیری رفتاری، سایبرسکس و آواتاریسم و ایماژ بدنی است، نتایج نشان داد که علاوه بر استفاده از محتواهای تولید شده توسط دیگران که به‌آسانی و راحتی قابل دسترس است، هر شخص می‌تواند تولیدات تصویری و شخصی خود را با دیگران جهت استفاده به اشتراک بگذارد و درک افراد از جهان پیرامون تحت تاثیر تصاویری است که از طریق رسانه‌های گوناگون در ذهنشان شکل می‌گیرد و از طریق مشاهده‌ی آن می‌توان به بخشی از رویاها، ارزش‌ها، ایدئولوژی‌ها و کاستی‌های موجود در جامعه دست یافت.

کلمات کلیدی: زیست جنسی، تحولات رفتاری، ابژگی، شبکه‌های اجتماعی.

Code: CYSP2023-1087

راهکارهای رسانه‌ای مقابله با رویکرد ضدفرهنگی سلاح اجتماعی جوکر

حسن ضیائی جباری[۱]، حمیدرضا حسینی دانا[۲]، بی‌بی‌سادات میراسماعیلی[۲]
[۱]دانشجوی دکتری، گروه مدیریت رسانه‌ای، دانشکده علوم انسانی و هنر، واحد دماوند، دانشگاه آزاد اسلامی، دماوند، ایران
tash.ziaee@yahoo.com
[۲]استادیار، گروه مدیریت رسانه‌ای، دانشکده علوم انسانی و هنر، واحد دماوند، دانشگاه آزاد اسلامی، دماوند، ایران
{hhoseinidana,f.miresmaili}@gmail.com

چکیده: امروزه رسانه‌ها می‌توانند عامل توسعه فرهنگی یا تهاجم فرهنگی باشند. چالش جدید جوامع در دنیا، استفاده از رسانه برای تقویت سلاح نرمی بنام «سلاح اجتماعی جوکر» می‌باشد. این سلاح نرم به‌واسطه محتوای جعلی خبری و فیک‌نیوزها در راستای ایجاد ناهنجاری‌های فرهنگی پشتیبانی می‌شود. هدف اصلی این مقاله بررسی راهکارهای رسانه‌ای جهت مقابله با ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر می‌باشد. سئوال اصلی این است که آیا بین راهکارهای رسانه‌ای و ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر رابطه معنی‌داری وجود دارد؟ این پژوهش فرض را بر این گرفته که بین راهکارهای رسانه‌ای و ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر رابطه معنی داری وجود دارد. با توجه به اهداف این تحقیق و موضوع پژوهش، از روش پژوهش آمیخته یا ترکیبی از روش‌های کمی و کیفی استفاده شده است.نهایتاً گزاره‌ها در یک دسته‌بندی کلی، سازماندهی و تجزیه و تحلیل شدند و راهکارهای رسانه‌ای حاصل؛ در قالب سه مقوله شامل فناوری‌های شناخت محتوای خبری جعلی، فرهنگ‌سازی شناخت و راهکارهای حکمرانی معرفی شدند. بنابراین و با استناد به مقوله‌های به‌دست آمده، افراد ومخاطبان رسانه می‌توانند با استفاده از راهکارهای ارائه شده با آسیب‌های فرهنگی سلاح اجتماعی جوکر مقابله کنند.

کلمات کلیدی: ناهنجاری‌های فرهنگی، فیک‌نیوزها، راستی‌آزمایی محتوای خبری، سلاح اجتماعی جوکر.

Code: CYSP2023-1088

ارزیابی دادگان تجمیع رتبه‌بندی نتایج جستجو از منظر گراف

فاطمه پاک مهر[۱]، امیرحسین کیهانی‌پور[۲]
[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
f.pakmehr@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده: با افزایش اهمیت شبکه‌ها در زندگی امروزه، تحلیل دادگان بر اساس نظریه شبکه به منظور استخراج ویژگیهای پنهان در مجموعه داده، به عنوان یک رویکرد تحقیقاتی جدید، مورد توجه جامعه محققان قرار گرفته است. از سوی دیگر، این روش تحلیل، امکان مقایسه بین مجوعههای داده مختلف را نیز فراهم میآورد. در این پژوهش، دو مجموعه داده تجمیع رتبه‌بندی نتایج جست‌وجو یعنی MQ2007-agg و MQ2008-agg، از منظر گراف مورد بررسی قرار گرفته است. برای این‌کار، ابتدا دادگان را به‌وسیله شاخص کندال به گراف شباهت ویژگی تبدیل کرده و ویژگی‌هایی از جمله اندازه اجزا، طول مسیر، اثر دنیای کوچک، توزیع درجه، قوانین توانی و ضرایب خوشه‌بندی را برای این شبکه‌ها محاسبه می‌شود و سپس بررسی تحلیلی ویژگی‌های به‌دست آمده در هر مجموعه داده، صورت گرفته است. نتایج بررسی‌ها نشان می‌دهد که گراف هیچ کدام از دادگان مورد ارزیابی، از نوع گراف‌های بدون مقیاس نبوده و تنها گراف متناظر با مجموعه MQ2007-agg از نوع دنیای کوچک است.

کلمات کلیدی: تحلیل داده، نظریه گراف، تحلیل شبکه، ویژگی‌های گراف، شاخص کندال.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1089

بررسی و تحلیل دادگان تشخیص صفحات اسپم درمحیط وب بر اساس نظریه گراف

مهدیه رعیتی[۱]، امیرحسین کیهانی‌پور[۲]
[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
mahdieh.raeyati@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده: نظریه گراف که به مدل‌سازی روابط موجود بین عناصر مختلف مسئله مورد بررسی می‌پردازد، ابزار مفیدی را برای ساده‌سازی بخش‌های یک سیستم فراهم می‌کند. پیچیده‌تر شدن مسائل دنیای پیرامونی، به‌کارگیری نظریه گراف را به یک ضرورت تبدیل نموده است. این مقاله قصد دارد مجموعه دادگان عرضه شده به‌منظور شناسایی تشخیص صفحات اسپم در محیط وب را از منظر گراف مورد بررسی قرار دهد. برای این منظور، ابتدا گراف شباهت ویژگی‌های مجموعه داده، ایجاد می‌شود و سپس، گراف حاصل به‌لحاظ شاخص‌های ساختاری مختلف، مورد بررسی قرار خواهد گرفت. برای ارزیابی روش پیشنهادی، گراف شباهت به‌ازای دو دسته از ویژگی‌های متنی و پیوندی به‌ازای مجموعه داده WEBSPAM-UK2007 ایجاد گردید و بر اساس شاخص‌های فوق مورد مقایسه تحلیلی قرار گرفت. نتایج به‌دست آمده نشان می‌دهد که علیرغم بزرگ‌تر بودن و تراکم نسبی بالاتر گراف شباهت ویژگی‌های مبتنی بر متن، نسبت به گراف شباهت ویژگی‌های مبتنی بر پیوند، بر اساس شاخص‌های ضریب خوشه‌بندی، گراف شباهت ویژگی‌های مبتنی بر پیوند، انسجام نسبی بیشتری را دارا می‌باشد. این موضوع با توجه به اندازه نسبی بزرگ‌ترین مؤلفه همبند نیز تأیید می‌شود. این رویکرد، امکان مقایسه تحلیلی دادگان مختلف را فراهم می‌آورد. علاوه بر آن، می توان از نتایج این پژوهش به‌منظور طراحی دادگان جدید نیز استفاده نمود.

کلمات کلیدی: نظریه گراف، دادگان تشخیص صفحات اسپم، ویژگی‌های گراف، شاخص کندال.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1091

مطالعه‌ی ابزارهای برتر شنود شبکه و مقایسه کاربردی Cain and Abel و Wireshark

سارا سعادت[۱]، هایده باقری پور[۱]
[۱]دانشجوی دکتری رشته مهندسی فناوری اطلاعات، پردیس بین‌المللی ارس دانشگاه تهران
{ssaadat,bagheripou}@ut.ac.ir

چکیده: این مقاله مطالعه‌ای بر روی بهترین ابزارهای نفوذ شبکه می‌باشد که از بین آنها Wireshark و Cain and Abel انتخاب‌شده‌اند و اینکه چگونه می‌توان حفره‌های امنیتی و انجام حملاتی مانند شکستن رمز عبور، حمله مرد میانی، شنود ترافیک کاربران و غیره را با این ابزارها آشکار کرد. آزمایش‌ها برای شواهد عملی از طریق ایجاد آزمایشگاه مجازی انجام شده‌است. هدف از این مقاله برای نشان دادن این مهم بود که چگونه می‌توان با آشکار کردن حفره‌های امنیتی مختلف در سیستم مبتنی بر ویندوز، سیستم شخص را به‌راحتی هک کرد. نتایج نشان‌می‌دهد که در صورت کم‌توجهی، سوءاستفاده از یک سیستم یا کشف رمز عبور چقدر ساده است و به‌راحتی می‌توان به امنیت و ایمنی سیستم خدشه وارد کرد. از آنجایی که سیستم‌ها هرگز نمی‌توانند همیشه از حملات در امان باشند، بنابراین دانستن این تهدیدات و استفاده از مکانیسم‌های امنیتی مناسب به‌گونه‌ای که مورد سوء استفاده قرار نگیرد برای افراد مفید خواهد بود.

کلمات کلیدی: شنود شبکه، نفوذ به شبکه، هک، ابزارهای نفوذ، تهدیدات سایبری، حملات رمز عبور، Wireshark، Cain and Abel.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1092

پیشرفت مطلق یا هدفمند هوش مصنوعی در اندیشه مقام معظم رهبری

حمید محسنی[۱]، کاظم فولادی قلعه[۲]
[۱] دکتری حکمت متعالیه از مؤسسه آموزشی و پژوهشی امام خمینی (ره)، قم
h.mohseni1297@mailfa.com
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده: از منظر برخی اندیشمندان و متفکران در آینده نه‌چندان دور هوش مصنوعی در مسئله حکمرانی دنیا و جوامع نقشه بسزایی خواهد داشت. به همین دلیل اخیراً مقام معظم رهبری بر پیشرفت در حوزه هوش مصنوعی تأکید کرده‌اند. اما برای مواجهه درست و دقیق با دیدگاه معظم له، می‌بایست اندیشه وی دراین‌باره تبیین و بررسی شود. ازاین‌رو مسئله اصلی تحقیق حاضر این است که آیا نگرش واقعی رهبری در حوزه هوش مصنوعی به‌طور مطلق و در هر شرایطی بوده یا هدفمند و جهت‌دار است؟ با تأمل و واکاوی اندیشه مقام معظم رهبری مشخص شد همان‌طور که ایشان بر اصل ضرورت پیشرفت در حوزه فناوری هوش مصنوعی تأکید کرده‌اند بر هدفمندی و جهت گذاری صحیح هوش مصنوعی نیز تأکید دارند. اصل توحیدمحوری یکی از جنبه‌های هدفمندی در پیشرفت هوش مصنوعی است. هدف مهم دیگر تحقیق حاضر این بود که مسئله هوش مصنوعی یک فناوری صرف نبوده، بلکه می‌تواند تأثیرات مهم فرهنگی، دینی تمدنی و حکمرانی داشته باشد. ازاین‌رو پیشرفت این نوع فناوری در نظام و تمدن اسلامی می‌بایست هدفمند و بر محور توحید باشد. افزون براین از منظر رهبری پیشرفت هر نوع علم و فناوری مبتنی بر مباحث فکری و فلسفی است. درنتیجه، با تبیین نگرش واقعی رهبری بسیاری از ابهامات برای مسئولان و قانون‌گذاران و محققان در مواجهه با پیشرفت هوش مصنوعی برطرف خواهد شد.

کلمات کلیدی: ضرورت پیشرفت، اصل هدفمندی، اصل توحید، مقام معظم رهبری.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1096

سایبودینامیک، قوانین جریان اطلاعات در چرخه‌ی سایبرنتیک

محمدعلی شکوهیان‌راد[۱]، سمانه کاتبی کوشالی[۲]
[۱]مدرس دانشگاه تهران و پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
cm@shokoohian.ir
[۲]دانش‌آموخته‌ی دکتری شیمی - فیزیک، دانشگاه کاشان
sahab135@gmail.com

چکیده: تلقی انسان از جهان و ارکان سازنده‌ی آن در طول تاریخ، چنین بوده که صرفاً ماده و انرژی سازندگان پایه‌ی جهان هستند. لذا دانش‌هایی که بتوانند ماهیت، کارکرد، قوانین حاکم و نحوه‌ی کنترل ماده و انرژی را توضیح دهند، برای فهم جهان کفایت می‌کنند. اما عصر اطلاعات که با وقوع انقلاب صنعتی سوم آغاز شد، فضای فهم و ادراک از جهان را به‌سمت مؤلفه‌ی نوینی سوق داد که در گذر زمان اثبات شد حتی ماده و انرژی نیز تحت سیطره‌ی آن هستند: اطلاعات. همچنین به‌دلیل استیلای اطلاعات بر ماده و انرژی، دانش سایبرنتیک -دانش تخصصی کنترل جریان اطلاعات- نیز بر دانش فیزیک سلطه دارد. به‌تدریج مشخص گردید اطلاعات در حالی که می‌تواند ماده و انرژی را کنترل نماید، به‌دلیل ماهیت متفاوتی که دارد از قوانین حاکم بر ماده و انرژی پیروی نمی‌کند. این مهم آغاز یکی از بزرگترین انقلاب‌های علمی جهان شد که مبنای اکثر دانش‌ها را از ماده و انرژی به اطلاعات تغییر داد؛ تغییری که بر پایه‌ی دانش سایبرنتیک رقم خورد و کماکان ادامه دارد. از سوی دیگر، ثبات‌مندی و پایداری بسیار بالای جریان اطلاعات حاکی از قانون‌مندی روند آن است. بدین سبب جریان‌مندی اطلاعات، قطعاً از قوانین مشخصی پیروی می‌کند؛ قوانینی که در دانش فیزیک مطالعه نشده و باید کشف شوند. در این راستا، طی نسبت‌شناسی میان مؤلفه‌ی گرما در پویایی ماده و انرژی که قوانین ترمودینامیک بر پایه‌ی آن تدوین شده، با مؤلفه‌ی سایبر که جریان اطلاعات را در چرخه‌ی سایبرنتیک ایجاد و کنترل می‌نماید، برای نخستین بار «قوانین پویایی جریان اطلاعات» با عنوان سایبودینامیک مورد مطالعه قرار گرفت.

کلمات کلیدی: سایبرنتیک؛ سایبودینامیک؛ قوانین جریان اطلاعات؛ مثلث اطلاعات، ماده و انرژی (مثلث اِما).

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1098

نسبت قلمرو حکمرانی با فضای سایبر

علی لک‌زائی[۱]، کاظم فولادی قلعه[۲]
[۱]دانشجوی کارشناسی ارشد گرایش امنیت سایبری، دانشکده برق و کامپیوتر، دانشگاه تربیت مدرس؛ دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
lakzaei.ali@modares.ac.ir
[۲]استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده: موضوع حکمرانی از مباحثی است که در شرایط کنونی ذهن دانشمندان و سیاست‌مداران را به شکل توأمان درگیر کرده است. حکمرانی، از آن حیث که هم دانش است و هم کنش، از گستره وسیعی برخوردار بوده و آنچه باعث اهمیت بیشتر آن شده است، نقش و تأثیر آن در پیشرفت و عقب‌ماندگی کشورها است؛ آنچه امروزه بر پیچیدگی الگوهای حکمرانی افزوده است، افزوده شدن فضای سایبر به‌عنوان عنصری تعیین‌کننده در این عرصه می‌باشد. از این رو تعیین نسبت قلمرو حکمرانی با فضای سایبر از اهمیت مضاعف برخوردار است و اتخاذ هر رویکردی در باب قلمرو حکمرانی مستقیما بر گستره حکمرانی و سیاست‌های اتخاذ شده در این زمینه و در نتیجه بر امنیت ملی و بلکه تمامی ساحت‌های زندگی فردی و اجتماعی هر کشوری اثرگذار است؛ از این رو پرسش اصلی مقاله حاضر نسبت قلمرو حکمرانی با فضای سایبر است. فرضیه مورد بررسی این است که نسبت قلمرو حکمرانی با فضای سایبر سه عرصه را در بر می‌گیرد. ۱- حکمرانی در فضای سایبر ۲- حکمرانی بر فضای سایبر ۳- حکمرانی با فضای سایبر، مهم‌ترین دست‌آورد مقاله این است که غفلت از هر یک از سه عرصه مذکور موجب ناقص دیده شدن نسبت قلمرو حکمرانی با فضای سایبر بوده و به‌جای فرصت‌سازی، چالش‌خیز، تهدیدساز و بحران‌آفرین خواهد بود.

کلمات کلیدی: حکمرانی در فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر، قلمرو حکمرانی، سایبرنتیک.

Code: CYSP2023-1099

مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب

علی عرب نجف‌آبادی[1]
[1]دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
ali.arab5965889@gmail.com

چکیده: استفاده ابزاری نادرست از رسانه‌ها در فضای سایبر در صورتی که منجر به ورود ضرر و زیان به مخاطبان شود از موجبات احراز مسئولیت حقوقی است که این مسئولیت ممکن است در نتیجه توهین و پخش ادعاهای واهی، هتک حرمت، انتشار ویروس‌های رایانه‌ای، تبلیغات دروغین، بی‌مبالاتی در تولید نرم‌افزارها و مواردی از این قبیل ایجاد شود. با وجود اینکه فرامرزی بودن، دشواری‌های کنترل و هویت پنهان بازیگران حاضر در این فضا می‌تواند موجب دشواری اثبات مسئولیت افراد گردد، اما در حالت احراز از جنبه حقوقی بیشتر نظریه تقصیر در باب مبنای مسئولیت حقوقی رسانه‌ها و نظریه خطر در باب مبنای مسئولیت همزمان مخاطب از توجه بیشتری برخوردار است. در این میان و در راستای استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان، می‌توان به احراز مسئولیت در مقابل مخاطبین و بعضا مسئولیت همزمان مخاطب اشاره نمود چرا که اگر استفاده از رسانه سایبر بر اساس سیاستی متناسب، معقول، منطقی و مبانی مستحکم صورت نگیرد نه فقط پیامدهای مطلوبی نخواهد داشت بلکه خود سبب ایجاد گرفتاری-ها و معضلات اجتماعی و حقوقی زیادی خواهد گشت. بر همین اساس این مقاله از نوع نظری بوده و روش آن، توصیفی تحلیلی و کتابخانه‌ای می‌باشد و با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

کلمات کلیدی: مسئولیت حقوقی، مخاطبان، رسانه سایبر.

Code: CYSP2023-1100

پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری

علیرضا رضوانیان[۱]، سید مهدی وحیدی پور[۲]
[۱]استادیار، گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران
rezvanian@usc.ac.ir
[۲]استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه کاشان، کاشان
vahidipour@kashanu.ac.ir

چکیده: تردیدی نیست که فراوانی استفاده از منابع دیجیتالی و پدیدار شدن فناوری‌های نوظهور در زندگی روزانه افراد رو به افزایش است و همچنین گستردگی محتوا و اطلاعات متنوع، امکان نفوذ و سوء استفاده از افراد و سازمان‌ها را روز به روز افزایش می‌دهد. مطالعات و پژوهش‌های گوناگونی نیز برای حفاظت از منابع دیجیتالی و ارائه راه‌کارهای امنیت سایبری از جنبه‌های مختلف پژوهشی تا صنعتی توسط پژوهشگران و صنعتگران در سال‌های اخیر ارائه شده است. بنابراین، با توجه به اهمیت موضوع امنیت در فضای سایبری، در این مقاله پایش کتابشناختی علم با بررسی مقالات منتشر شده و پایش فناوری با بررسی ثبت اختراعات، مورد بررسی قرار گرفته است. برای بررسی مقالات از منابع نمایه‌شده موجود در پایگاه علمی اسکپوس استفاده شده است و برای بررسی ثبت اختراعات از داده‌های موجود در لنز استفاده شده است. در نهایت گزارش‌های مختلف به تفکیک آمار به‌دست آمده از زوایای مختلف و بر اساس شاخص‌های مختلف ارائه شده است.

کلمات کلیدی: امنیت سایبری، تحلیل کتابشناختی، پایش علم، پایش فناوری.

Code: CYSP2023-1101

سایبرنتیک دروازه نوگشوده علم و تکنولوژی

زهرا بیگلری[۱]، زهرا عزتی نیا[۲]
[۱]دانشجوی کارشناسی ارشد، مؤسسه شناخت
biglari110@gmail.com
[۲]دانشجوی دکتری مدیریت رسانه، دانشگاه آزاد اسلامی واحد علوم تحقیقات، تهران
pasia529@yahoo.com

چکیده: ارتباط ناگسستنی علم و تکنولوژی و سیر تاریخی کاربردی‌شدن علم در زندگی بشری زمینه‌ساز پیدایش مفهوم تکنوساینس گردید. به گونه‌ای که می‌توان شیء تکنیکی را برون‌داد همکاری دانشمندان و مهندسین به‌شمار آورد. فناوری فراگیر که در عصر کنونی با گسترش فناوری اطلاعات و هوش مصنوعی چهره‌ای بی‌بدیل به نمایش گذاشته است مسبب چالش‌ها و فرصت‌های تازه‌ای است؛ به‌گونه‌ای که ساحت فکر و اندیشه‌ی انسانی را نیز تحت سیطره‌ی القائات و ادراکات جدیدی از مفاهیم قرار داده است. فرایند تلاش‌های گروهی سیستم علمی، اکنون به جایگاهی رسیده که گونه‌ای جدید از سیستم بازخورد و کنترل به نام «سایبرنتیک» را معرفی نموده است. سایبرنتیکِ برآمده از انبوه اطلاعات و دستگاه‌های محاسباتی، نرم‌افزاری فراهم آورده که هدف نهایی آن پیدایشِ یک ماشین به تقلید از انسان نیست، بلکه به‌عکس، انسان سخت‌افزاری است که نرم‌افزار او در این سیستم علمی پردازش می‌شود؛ به‌گونه‌ای که پیچیدگی دنیای علم می‌تواند بازخورد و بازنمایی همه اهداف خود را در رفتار انسانی نظاره کند. مقاله پیش‌رو می‌کوشد با روش توصیفی- تحلیلی رابطه فناوری و گام‌های نخستین در شبکه علمی را برای دستیابی به دانش سایبرنتیک تبیین کند. برای این منظور نخست سیر تحول فناوری از ابزاری در دست انسان تا خلق ماشینی دارای قدرت تفکر و تکلم را بررسی می‌کند. سپس نشان می‌دهد که این ایده دکارتی در نسخه‌های جدید خود چگونه به تسلط ماشین بر کالبد انسان از راه کنترل قوه تفکر و تکلم می‌پردازد.

کلمات کلیدی: فناوری، شیء تکنیکی، انسان، سایبرنتیک.

Code: CYSP2023-1102

مدل‌سازی رفتاری مصرف منابع در بخش رمزنگاری فایل‌ها در باج‌افزارها

مهران گرمه‌ء[۱]، رجبعلی سجادیان فر[۲]، محمد شاه‌پسندی[۲]
[۱]استادیار گروه مهندسی کامپیوتر دانشگاه بجنورد
m.garme@ub.ac.ir
[۲]دانشجوی کارشناسی ارشد مؤسسه آموزش عالی اشراق
{sajadianfar,m.shahpasandi}@ub.ac.ir

چکیده: امروزه باج‌افزارها بدترین چالش مدیران و مسئولین فناوری اطلاعات سازمان‌ها هستند. سازندگان محصولات ضدویروس و تحلیل‌گران بدافزار دشواری‌های زیادی برای شناسایی و کالبدشکافی یک بدافزار پیچیده متحمل می‌شوند. یکی از نکات کلیدی موجود در این فرآیند، سرعت تشخیص و پاسخگویی به یک حمله باج‌افزاری می باشد که این امر گاهی سرنوشت‌ساز بوده و علاوه بر مقدار داده از دست رفته و سرعت انتشار باج‌افزار، بر امکان رمزگشایی اطلاعات نیز تأثیرگذار خواهد بود. با توجه اینکه امکان دور زدن تکنیک‌های سنتی شناسایی همواره وجود دارد، استفاده از روش‌های نوین تشخیص باج‌افزار کمک شایانی به مدافعین این حوزه خواهد کرد. این پژوهش با رویکرد بررسی میزان مصرف منابع سیستم (پردازنده، حافظه و دیسک) نمونه‌هایی از پنج خانواده از باج‌افزارها با تاریخ انتشار حداکثر سه سال گذشته انجام گرفته است که در نهایت با تحلیل نتایج به‌دست آمده، رفتار باج‌افزارها نسبت به نحوه مصرف منابع، مدل‌سازی و گزارش شده است. نتایج به‌دست آمده از این تحقیق نشان می‌دهد که ساختار کد و الگوی رمزنگاری در بین باج‌افزارهای هم‌خانواده تشابهات زیادی دارد. بنابراین با استفاده از مدل به‌دست آمده خواهیم توانست سایر باج‌افزارهای یک خانواده را شناسایی کرده و دقت و سرعت تشخیص را بمراتب بالاتر ببریم.

کلمات کلیدی: Ransomware، Detection، Responding، Obfuscation.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1103

ارائه روشی برای تشخیص اجتماع در شبکه‌های پیچیده با الگوریتم بهینه‌سازی خرگوش‌های مصنوعی

آرش هدایتی[1]، محسن محمودی[1]
[1]پژوهشگر پژوهشگاه علوم انتظامی و مطالعات اجتماعی فراجا، تبریز
mohsen.nahmoudi98@email.com ،waro.info@gmail.com

چکیده: شبکه پیچیده نگاهی جدید به پدیده‌های می‌باشد که با توجه به ارتباط اجزای آن و همچنین ارتباط با دیگر پدیده‌ها، دارای پیچیدگی بالایی بوده و رفتار جمعی متفاوتی از خود نشان می‌دهند. تشخیص اجتماع یک چالش مهم در این شبکه‌ها می‌باشد. در این مقاله برای تشخیص اجتماع در شبکه‌های پیچیده از رویکرد فرا اکتشافی و الگوریتم بهینه‌سازی خرگوش مصنوعی استفاده شد. روش پیشنهادی در محیط نرم‌افزاری متلب پیاده‌سازی شده و کارایی آن در چهار مجموعه داده حقیقی (باشگاه کاراته زاخاری، شبکه فوتبال کالج آمریکایی، شبکه دلفین‌های، شبکه پول بوکز) با شاخص‌های پیمانگی و NMI مورد تجزیه‌وتحلیل قرار گرفت. تجزیه‌وتحلیل نتایج نشان داد که در مجموعه داده‌های حقیقی بالاترین مقدار پیمانگی به‌صورت میانگین برای مجموعه داده Polbooks و پایین‌ترین مقدار آن برای مجموعه داده Karate می‌باشد. این در حالی است که در مجموعه داده حقیقی بالاترین میزان NMI برای مجموعه داده Dolphins و کمترین مقدار برای مجموعه داده Karate به‌دست‌آمده است.

کلمات کلیدی: شبکه پیچیده، شبکه اجتماعی، تشخیص اجتماع، الگوریتم بهینه‌سازی خرگوش مصنوعی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1105

نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر

محمدعلی عبدالهی[۱]، مسلم طاهری کل‌کشوندی[۲]، عاطفه اندرزا[۳]
[۱]دانشیار گروه فلسفه، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
abdllahi@ut.ac.ir
[۲]استادیار گروه شیعه شناسی و معارف اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
muslimtaheri@ut.ac.ir
[۳]دانشجوی دکتری مدرسی معارف اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
andarza.a313@ut.ac.ir

چکیده: ظهور فناوری‌های نوین ارتباطی در عصر حاضر، به همراه نوآوری‌هایی که در فضای سایبر به وجود آمده، موجب تحولات بنیادی درنهاد خانواده گشته است.در این مقاله کوشیده‌ایم تا نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر را نشان دهیم. سؤال اصلی مقاله این است که، نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر چیست؟ تلاش می‌کنیم در پاسخ این پرسش نشان دهیم که اعتقادات مذهبی می‌تواند نقش مهمی در توانمندسازی خانواده‌ها در مواجهه با فضای سایبر داشته باشد. باورهای دینی در صورتی‌که با بصیرت و آگاهی همراه شود می‌تواند در افراد به‌ویژه هسته‌ی اصلی خانواده احساس هدف‌مندی، امید به کمال انسانی و توجه به جاودانگی ایجاد کند . چنین باورهایی که از منابع دینی سرچشمه می‌گیرد به خانواده‌ها کمک می‌کند تا با حفظ روابط و ارزش‌های قوی، چالش‌های زندگی مدرن را پشت سر بگذارند. پژوهش حاضر به روش توصیفی - تحلیلی ارائه شده است.

کلمات کلیدی: باورهای دینی، توانمندسازی، خانواده، فضای سایبر.

Code: CYSP2023-1107

رویکرد فقهی به جامه‌شناسی پیام، با نگاهی به اینستاگرام

ابوالفضل امامی میبدی[۱]، مجتبی شیخی ده‌آبادی[۲]، مصطفی میرزایی فیروزآبادی[۳]
[۱] دانش‌آموخته حوزه و دکترای فقه سیاسی و روابط بین‌الملل، جامعة المصطفی (ص)، قم
abolfazlemami@chmail.ir
[۲] دانش‌آموخته حوزه و دکترای علوم اقتصادی، مؤسسه آموزشی و پژوهشی امام خمینی (ره)، قم
msheikhy97@chmail.ir
[۳] دانشجوی کارشناسی ارشد، علوم تربیتی گرایش برنامه‌ریزی درسی، دانشگاه پیام نور، تفت
mmfabadi@gmail.com

چکیده: همانگونه که برای برآوردن نیاز بدن به آهن، نمی‌توان نبشی را گاز زد، برای نیازهای روان نیز، «جامه پیام» باید با دستگاه گوارش و پردازش روان سازگار باشد. از آنجا که شناخت لایه‌ها و ویژگی‌های انسان و جامعه، فراتر از توان اندیشه و دانش اندک ما است، باید روش فقهی را برای دستیابی به آن برگزید. فقه، ریشه همرسانی دیدپایه را به کژی‌های یهود برمی‌گرداند و بازپخش امروزی آن در اینستاگرام را به ما هشدار می‌دهد. فقه، همچنین «الگوی تراز جامه پیام» را، کاربست متوازن هر پنج لایه «عقل، فکر، قلب، حس و عضو» انسان و هر «پنج حسّ» لایه عضو می‌داند؛ چیزهایی که در «رفتار اسلامی و مخلصانه» یافت می‌شود. دستاورد این نوشته، آشکارسازی «تباهگری پنهان همرسانی دیدپایه» است که به «مهجوریت و هذیان‌پنداری قرآن» و دگرگونی ذائقه همرسانی، از واژه‌پایگی و خودآگاهی به ناخودآگاه‌سالاری می‌انجامد. ازاین‌رو باید در سامانه همرسانی تراز، افزون بر گسترش «رفتارپایگی» در جامعه، در ساماندهی شبکه‌های اجتماعی ملی نیز، از دیدپایگی جلوگیری کرد و توازن عناصر حسی را در جامه پیام سامان بخشید.

کلمات کلیدی: فقه ارتباطات، قالب پیام، جامه‌شناسی اینستاگرام، رسانه دیداری، گناه نگاه، رفتار مخلصانه.

Code: CYSP2023-1108

تشخیص بدافزارهای اندرویدی با استفاده از روش یادگیری ترکیبی پشته‌ای

مونا زارع[1]، علیرضا رضوانیان[1]
[1]گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران
monazare754@gmail.com، rezvanian@usc.ac.ir

چکیده: بدافزارها، برنامه‌هایی هستند که رفتار مخربی دارند و برای آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری طراحی شده‌اند. بدافزارها، تنوعی از کارهای مخرب از سرقت اطلاعات حساس تا از بین بردن کل سیستم‌ها را با اهداف مختلفی چون تجاری، اجتماعی، اقتصادی، سیاسی، نظامی یا شخصی را انجام می‌دهند. با توجه به پیچیده‌تر شدن ساختار و رفتار بدافزارها در سیستم‌های اندروید، رویکردهای سنتی، تکرارگرا و آماری عملا کارساز نبوده و در گذر زمان منسوخ شده است. در این مقاله، بعد از آماده سازی و نرمالسازی داده‌ای، از یک روش یادگیری ترکیبی به صورت پشته‌سازی برای تشخیص بدافزارهای اندرویدی استفاده شده است؛ به این صورت که درخت تصمیم (DT)، بیز ساده (NB) و رگرسیون خطی (LR) به‌عنوان یادگیرنده‌های ضعیف و ماشین بردار پشتیبان (SVM) به‌عنوان یادگیرنده قوی منظور شده است. نتایج آزمایش‌ها بر روی داده‌های سیستم‌های اندرویدی براساس معیارهای دقت، بازخوانی و صحت حاکی از بهبود نتایج روش پیشنهادی نسبت به نتایج روش‌های پایه و چند روش اخیر دارد.

کلمات کلیدی: تشخیص بدافزار، اندروید، یاد گیری ماشین، پشته‌سازی، درخت تصمیم، ماشین بردار پشتیبان.

Code: CYSP2023-1109

حق دسترسی به فضای سایبری در تکوین افکار عمومی

ندا رستگاران[۱]، عبدالحمید فرزانه[۲]، روح الله رحیمی[۳]، مهدی شیخ موحد[۳]
[۱]دانشجوی دکتری حقوق عمومی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
neda_rastegaran@yahoo.com
[۲]استادیار فقه و مبانی حقوق اسلامی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
farzaneh2139@gmail.com
[۳]استادیار حقوق عمومی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
mr5661@gmail.com ،rahimi.mehr48@yahoo.com

چکیده: ظهور و گسترش فضای سایبری مشارکت عموم در گفتمان حوزه عمومی را فراهم نموده است این امر تأثیرگذاری افکار عمومی در کنترل قدرت را منجر شده است. شناخت حق دسترسی به فضای سایبری، باعث مطالبه‌گری عموم می‌گردد و نقش کارگزاری سیاسی عموم را برجسته‌تر می‌سازد. خلاء تعریف دقیق فضای سایبری در نظام حقوقی جمهوری اسلامی ایران مشهود می‌باشد. با الگوبرداری از قوانین و مقررات سایبری در کشورهای موفق و بومی‌سازی آن مبتنی بر ویژگی‌های فرهنگی-حقوقی جمهوری اسلامی ایران، می‌توان فقدان قوانین بنیادین در این حوزه را مرتفع نمود. بر طبق یافته‌ها توجه به قوانین بنیادین و مقررات‌زدایی از سایر قوانین و مقررات در حوزه فضای سایبری پیشنهاد می‌گردد. زیرا در پارادایم لیبرالیسم امکان تکوین افکار عمومی در معنای علمی محتمل‌تر است. حاکمیت موظف است به صورت مستمر قوانین و مقررات را مطابق با نوآوری‌های این فضا بررسی نموده و با تفوق مقررات‌زدایی و خط‌مشی گذاری مبتنی بر نیاز، سیر استعلایی جامعه را در راستای گسترش حقوق و آزادی‌های بنیادین تأمین نماید.

کلمات کلیدی: افکار عمومی، حقوق عمومی، حوزه عمومی، فضای سایبری.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1110

نیهلیسمِ فضای سایبری در همسخنی با نیچه

مرتضی سعیدی ابواسحاقی[۱]، راضیه سعیدی ابواسحاقی[۲]
[۱]دانشجوی دکتری فلسفه دانشگاه تهران، پژوهشگر پژوهشگاه فضای مجازی
morteza.saeidi@ut.ac.ir
[۲]دانش‌آموخته کارشناسی تعلیم و تربیت، دانشگاه فرهنگیان
raziyesaeedi9819@gmail.com

چکیده: نیچه در اشاره به زمانه‌اش می‌گوید: ما در عصری آشفته زندگی می‌کنیم، و به همین خاطر، شورانگیز نیست. این عصر مدام خودش را گرم می‌کند، زیرا احساس می‌کند گرم نیست، بلکه اساساً یخ‌زده است. در زمانه‌ی ما رویدادها یا وقایع صرفاً با استفاده از پژواک روزنامه‌ها [یا رسانه‌ها] عظمت [پوشالی‌شان] را به دست می‌آورند. در این مقاله تلاش بر این است که این سخن نیچه در نسبت با فضای سایبری و اینترنت و شبکه‌های مجازی بررسی شود و پوچ‌گرایی و نیست‌انگاری یا نیهلیسمی که در فضای سایبری و شبکه‌های مجازی شدت یافته را متذکر شویم و در ادامه در همسخنی و همدلی با نیچه و هایدگر این امر بیان شود که رخداد نیهلیسم و ظهورات کامپیوتر و فضای سایبری برآمده از تاریخ غرب است و در صورتی که این امر در ادامه تاریخی غرب دیده نشود امکان فهم درست آن نخواهد بود. در انتها راه برون‌رفت از این مهلکه را از نظر نیچه و هایدگر در هنر معرفی کردیم، از نظر هایدگر هنر بزرگ امکان گذار و تغییر را فراهم می‌کند و می‌تواند جهانی نو بسازد که انسان را از نیهلیسم و پوچ‌گرایی نجات دهد. این تحقیق در حیطه مطالعات بنیادین قرار دارد و روش آن از سنخ روش‌های پژوهش کیفی است که روش تحلیل مضمون یا تحلیل تم (Thematic Analysis) برای آن به کار می‌رود. از آنجا که تحلیل مضمون هم برای بیان واقعیت و هم برای تبیین آن به کار می‌رود و در این پژوهش به‌دنبال تبیین و توصیف درست و عمیقی از نتایج فضای سایبری هستیم، روش تحلیل مضمون مناسب آن است.

کلمات کلیدی: نیچه، فضای سایبری، نیهلیسم، هنر، شبکه های مجازی، تخدیر.

Code: CYSP2023-1111

نقش میدان‌های الکترومغناطیس درون‌زاد و برون‌زاد در پیشبرد تکوین جنین

سمیرا کاتبی کوشالی[1]
[1] دکتری زیست‌شناسی گرایش سلولی تکوین، دانشگاه اصفهان
sahab135@gmail.com

چکیده: درک عوامل موثر در تکوین سلول تخم از دیرباز ذهن محققان را به خود مشغول داشته است . آنچه طی سالیان دراز از فرایندهای دخیل در قطبیت، ریخت‌زایی و اندام‌زایی جنین به‌دست آمده، ناشی از تلاش بی‌وقفه‌ی محققان در عرصه زیست‌شناسی مولکولی، بیوشیمی و ژنتیک بوده است. در این میان میدان‌های الکترومغناطیس و تابش‌ها به‌عنوان یکی از شاخه‌های مهم بیوفیزیک در رابطه با جنین‌شناسی نادیده گرفته شده است. به‌موازات پیشرفت علوم سلولی مولکولی و الکتروفیزیولوژی، دریچه‌ای تازه به‌روی محققان زیست‌شناسی تکوینی گشوده شد که به نقش بسیار مهم میدان‌های الکترومغناطیس در پیشبرد صحیح فرایندهای تکوین در موجودات زنده اشاره داشت. آزمایش‌های انجام شده طی نیم قرن بیانگر این است که جنین قادر به تولید میدان‌های الکترومغناطیس و تابش‌هایی بسیار ضعیف است که در ایجاد قطبیت، مهاجرت سلول‌ها و ریخت‌زایی فوق العاده حائز اهمیت‌اند. در مقاله حاضر به اهمیت میدان‌های الکترومغناطیس طبیعی و مصنوعی در پیشبرد فرایندهای تکوین جنین پرداخته شده است.

کلمات کلیدی: میدان‌های الکترومغناطیسی، جنین، تکوین، ریخت‌زایی.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1112

بازتعریف مفهوم شناخت و کارکردهای آن با رویکرد سایبرنتیکی

محمدعلی شکوهیان‌راد[1]
[1]مدرس دانشگاه تهران و پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
cm@shokoohian.ir

چکیده: مفهوم شناخت، مفهومی است که به‌واسطه‌ی فراگیری و همه‌گستری اطلاعات، در چند سال اخیر به یکی از پرکاربردترین مفاهیم در ادبیات علمی، نظامی، سیاسی، اقتصادی و حتی فرهنگی و اجتماعی تبدیل شده است؛ خصوصاً از منظر بسترسازی نوع جدیدی از منازعات که به منازعات شناختی (با تعبیر عامیانه‌ی جنگ شناختی) شهرت یافته است. در این بین، آسیب جدی و اثرگذاری که رخ داده است، پرداختن به حوزه‌ی منازعات شناختی بدون توجه به خودِ مفهوم شناخت، سپس دانش شناختی و نهایتاً قدرت برآمده از دانش شناختی است (قدرت شناختی). این خلأ مهم باعث شده است به دلیل عدم توجه به مبانی پایه‌ی مفهومی و نظری، از سویی در حوزه‌های مذکور به سمت تأثیرپذیری از جریان فکری غرب سوق یابیم و از سوی دیگر، دچار اختلافات متعدد در تعریف منازعات شناختی بشویم. همچنین خلأ مذکور باعث شده است تا نسبت‌شناسی میان دانش شناختی و دانش کنترل‌کننده‌ی جریان اطلاعات (دانش سایبرنتیک) که عملا بسترساز و گسترانندهی مفهوم شناخت است، مغفول واقع شود. برای رفع خلأ مذکور، ابتدا مبناشناسی مفهوم شناخت بر اساس عنصر اطلاعات انجام شد و نسبت‌یابی آن با دانش سایبرنتیک به سرانجام رسید، به‌گونه‌ای که مشخص شد دانش شناختی در پاسخ به دو پرسش اساسی سایبرنتیک برای کنترل پدیده‌های مُدرک از طریق جریان اطلاعات کاربرد یافته است. سپس طی چهار گام، تعاریف کارکردی برای مفهوم شناخت، دانش شناختی، قدرت شناختی و نهایتاً منازعات شناختی ارائه گردید به‌طوری که جامع، راهبردی و قابل استفاده در اقدامات عملی باشند.

کلمات کلیدی: سایبرنتیک؛ شناخت، دانش شناختی، منازعات شناختی، جهان‌بینی، اطلاعات.

دومین کنفرانس فضای سایبر
THE SECOND CONFERENCE ON CYBERSPACE
CYSP 2023
۹ تا ۱۱ آبان ۱۴۰۲ – دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

Code: CYSP2023-1113

تغییرات اقلیمی، ابر پروژه‌ای برای کنترل جهان

عاطفه نصیری[1]
[1] کارشناس ارشد مهندسی منابع طبیعی، دانشگاه آزاد اسلامی، واحد تهران شمال
nasiry.atefeh@gmail.com

چکیده: سابقه‌ی طرح مفهوم تغییرات اقلیمی، به دو قرن پیش باز می‌گردد، هرچند که عبارت خاص «تغییرات اقلیمی» از ۱۹۷۵ وارد ادبیات علمی شد. علت تغییرات اقلیمی، به انباشت گازهای گلخانه‌ای و به خصوص CO_2 و عنصر کربن نسبت داده می‌شود. مروری پیش‌بینی‌های اسبق درباره‌ی تغییرات اقلیمی و گرمایش زمین، حاکی از آن است که عمده‌ی آنها، هرگز محقق نشدند. آیا نظریه‌ها و پیش‌بینی‌های امروزی تغییرات اقلیمی و آینده‌ی آب و هوایی زمین هم به سرنوشت پیش‌بینی‌های پیشین، دچار خواهند شد؟ برای کنترل همه جا، باید از عاملی استفاده کرد که در همه جا حضور داشته باشد و جهان شمول باشد. همچنین باید در نظر داشت که اساس تغییرات آب و هوایی بر مواردی است که برای مردم، قابل اندازه‌گیری نیست. از سوی دیگر، برخورد درست با پدیده‌های اقلیمی و محیط زیستی، منوط به داشتن داده‌های درست است. هرگونه داده‌پردازی یا ارائه‌ی داده‌های نادرست، سبب واکنش‌های نادرست شده، که خود می‌تواند عامل بحران اقلیمی و زیست محیطی باشد، بدون آن‌که در اصل و در واقعیت، بحرانی وجود داشته باشد. به نظر می‌رسد که هدف تمامی این موارد –که نظریه‌های علمی پشتیبان‌شان، تاکنون به اثبات دقیق نرسیده‌اند– کنترل نمودن جریان اقتصاد و انرژی کشورها و ملت‌ها، به بهانه‌ی تغییرات اقلیمی است.

کلمات کلیدی: تغییرات اقلیمی، کنترل، جهان، گازهای گلخانه‌ای، کربن، سایبرنتیک، اکوسایبرنتیک، اطلاعات.

Code: CYSP2023-1043

Image Hashing Algorithm: An Analysis and Improvement

Seyed Amirhossein Tabatabaei[1]
[1]*Department of Computer Science, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran*
amirhossein.tabatabaei@guilan.ac.ir

Abstract: Image authentication code algorithms are schemes wherein the authenticity of an image is considered in a robust war. As the images are mainly subjected to some authorized modifications, such schemes must be able to accept the authorized changes while rejecting the malicious ones. This article analyzes an image authentication algorithm based on error detection code. The image authentication scheme utilizes a type of error detection code in order to encode the mixed most significant bits (MSB) intensity value of each image pixel. The secrecy of system is based on two secret keys. The algorithm provides an acceptable robustness and elaborate design however, it suffers from some security features that leave a gap for improvement. These features are analyzed and will be employed to show the vulnerabilities of the scheme. Also, some solutions are proposed to elaborate the algorithm more. The solutions will increase the strength of the scheme while keeping the robustness.

Keywords: *Image Authentication, Robustness, Image Hashing, Error detection and correction.*

Code: CYSP2023-1024

Vulnerability Analysis of Social Media Accounts Against Cyber Attacks

Ahamd Farid Aseel[1], Yashar Abri[1]
[1]*M.Sc. Student, Information Technology Engineering, Faculty of Engineering, College of Farabi, University of Tehran*
faridaseel.4all@gmail.com, yasharabri@ut.ac.ir

Abstract: This article examines the vulnerability of social media accounts against cyber attacks. With the increasing number of users on these platforms and the accumulation of sensitive information in user accounts, the security of these networks is facing cyber threats. The article analyzes phishing attacks and brute-force attacks as penetration methods and investigates the weaknesses of social media networks against these attacks. Additionally, social engineering, as a deception-based and psychological attack on individuals within social networks, is analyzed. Through a questionnaire, users' attitudes and behaviors regarding security measures are evaluated. The results indicate that some users use strong passwords but do not change them regularly, and users' awareness of security practices is inadequate. The security of social media accounts is of utmost importance, and this article emphasizes that increasing users' and administrators' awareness of cyber threats and countermeasures is crucial to strengthening the security of these platforms. The information presented in this article can contribute to enhancing the security of accounts and protecting users' personal information against cyber attacks.

Keywords: *Cyber Attacks, Social Networks, Phishing, Brute Force, Penetration.*

Code: CYSP2023-1001

Improving Cybersecurity Systems Using Artificial Intelligence Techniques

Ismail A. Humied[1]
[1]*Associate Professor, Faculty of Police, Policy Academic, Ministry of Interior, Sana'a, Yemen*
dr.ismail_humied@yahoo.com

Abstract: Cyberattacks and threats are in complexity every day. With the number of attacks growing every day around the world, there are a variety of methods and strategies for penetrating business systems and individual devices. Individual attackers, organizations, and whole nations are responsible for these attacks. Attack resources are growing and cyberattacks can have severe global impact and consequences. These variables make it difficult for security teams to keep pace, so smarter solutions are needed. This research provides an overview of how two areas of artificial intelligence (AI), machine learning and deep learning, can be used to meet cybersecurity challenges. The research can also show how existing AI technologies can improve cybersecurity. Security systems can use AI to automate time-consuming manual security operations and make detection and response more proactive and predictive. As part of this research, a workshop was held with official from government and private agencies, who are responsible for network monitoring and security. During this workshop, a discussion occurred what problems individuals had at work. Thus, this research includes potential AI-based remedies for identifying issues.

Keywords: *Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Cyber-attacks, Cybercrime, Detect.*

English Papers Abstracts

Book of Abstracts & Participant's Guide
The Second Conference on Cyberspace (CYSP 2023)
Organizer: University of Tehran

Preparation: *Kazim Fouladi-Ghaleh*
with: *Alireza Zeini, Hussein Azimi, Mohammad-Ali Shokoohian-Rad*

Publisher: Faculty of Engineering, College of Farabi, University of Tehran
Printing: Boostan-e-Ketab
Publishing Date: October 29, 2023

Secretariat Address: Faculty of Engineering, College of Farabi, University of Tehran, Old Qom-Tehran Road, Qom, Iran, Postal Code: 3718117469.
Telephone: 025-36166651
Fax: 025-36166652
E-mail: `cysp.conf@ut.ac.ir`
Web: `http://cysp2023.ut.ac.ir`
Messengers: `@cysp_conf`
All links in one: `http://conf.cysp.ir/links`

بسم الله الرحمن الرحیم

IN THE NAME OF ALLAH

CYSP 2023

The Second Conference on Cyberspace

Book of Abstracts

ISC Islamic World Science Citation Center 02230-21686

University of Tehran

31 October, 1-2 November 2023