

هوش مصنوعی و امنیت سایبری

مؤلفین

لورنزو پاپیلو، استفانوفانتین، آفونسو فریرا، کارولینپولتو

مترجمین

پرند خوزاده، الهه جمشیدی، یویک حاجی سید جواد





عنوان و نام پدیدآور

هوش مصنوعی و امنیت سایبری/ مولفین لورنزو پاپیلو ... [و دیگران]؛ مترجمین پرند خوزاده، الهه جمشیدی، پوپک حاجی‌سیدجواد؛ ویراستاران ادبی معصومه مهدی‌پور، مریم رازجو؛ ویراستار علمی هادی باغبانی؛ ناظر ویراستار مرتضی چشمه‌نور.

مشخصات نشر

تهران: انتشارات پشتیبان، ۱۴۰۰.

مشخصات ظاهری

۱۸۵ص: مصور (رنگی).

شابک

۸۰۰۰۰۰ ریال 978-622-255-477-4

وضعیت فهرست نویسی

فبیا

یادداشت

عنوان اصلی: Artificial Intelligence and Cybersecurity: technology governance and policy challenges.

یادداشت

مولفین لورنزو پاپیلو، استفانو فانتین، آفونسو فریرا، کارولینو لتو.

موضوع

هوش مصنوعی

Artificial intelligence

فضای مجازی -- تدابیر ایمنی

Cyberspace -- Security measures

شبکه‌های کامپیوتری -- تدابیر ایمنی

Computer networks -- Security measures

پوپیلو، لورنتسو ام.

شناسه افزوده

Pupillo, Lorenzo M.

شناسه افزوده

خوزاده، پرند، ۱۳۷۸-، مترجم

شناسه افزوده

جمشیدی، الهه، ۱۳۶۳-، مترجم

شناسه افزوده

Jamshidi, Elaheh

شناسه افزوده

حاجی‌سیدجواد، پوپک، ۱۳۵۵-، مترجم

شناسه افزوده

Haji Seyed Javad, Poopak

شناسه افزوده

باغبانی، هادی، ۱۳۵۶-، ویراستار

شناسه افزوده

Q۳۳۵

رده بندی کنگره

۰۰۴/۳

رده بندی دیویی

۸۷۲۹۳۳

شماره کتابشناسی ملی

اطلاعات رکورد کتابشناسی

فبیا

نام کتاب: هوش مصنوعی و امنیت سایبری

مؤلفین: لورنزو پاپیلو، استفانو فانتین، آفونسو فریرا، کارولینو لتو

مترجمین: رند خوزاده، الهه جمشیدی، پوپک حاجی‌سیدجواد

ویراستاران ادبی: معصومه مهدی‌پور، مریم رازجو

ویراستار علمی: هادی باغبانی

ناظر ویراستار: مرتضی چشمه‌نور

صفحه‌آرا: علی مهدی‌زاده

طراح جلد: زهرا مهدوی

نوبت چاپ: اول - ۱۴۰۰

ناشر: انتشارات پشتیبان

شمارگان: ۵۰۰ نسخه

قیمت: ۸۰۰۰۰۰ ریال



تلفن تماس: ۰۲۱-۸۶۰۳۶۴۲۳ / تلفکس: ۰۲۱-۸۶۰۳۶۴۲۸

صندوق پست الکترونیک: Pub.Poshtiban@chmail.ir

تارنمای انتشارات پشتیبان: www.PoshtibanPress.ir

فهرست مطالب

چالش‌های فناوری، حکومت و سیاست	۹
پیشگفتار	۹
خلاصه اجرایی	۱۰
توصیه‌های خط‌مشی از گروه کار	۱۲
هوش مصنوعی برای امنیت سایبری	۱۲
امنیت سایبری برای هوش مصنوعی	۱۵
فصل اول: مقدمه	۱۹
اروپا در مورد بحث هوش مصنوعی و امنیت سایبری در کجا قرار دارد؟	۲۴
برخی از تعاریف	۲۶
هوش مصنوعی برای امنیت سایبری و امنیت سایبری برای هوش مصنوعی	۲۹
فصل دوم: هوش مصنوعی در امنیت سایبری	۳۱
مقدمه	۳۲
پشتیبانی سیستم‌های هوش مصنوعی از امنیت سایبری	۳۳
استحکام سیستم	۳۶
استفاده‌های مخرب هوش مصنوعی	۵۲
گسترش تهدیدات موجود	۵۲
ویژگی‌های حملات مبتنی بر هوش مصنوعی	۵۷
معرفی تهدیدات جدید	۵۸
دیپفیک‌ها	۵۹
پرنوگرافی	۶۲
سیاسی	۶۳
جرم و جنایت و امنیت سایبری	۶۵
نظامی	۶۶
شکست کپچا	۶۸
حملات ازدحامی	۶۸
تغییرات در ویژگی معمولی تهدیدها و اشکال جدید آسیب‌پذیری در سیستم‌های هوش مصنوعی	۶۹
ملاحظات اخلاقی مرتبط با هوش مصنوعی در امنیت سایبری	۷۴
عدم تقارن در تعامل هوش مصنوعی و امنیت سایبری	۷۸
عدم تقارن در توسعه استانداردهای اخلاقی هوش مصنوعی	۸۰
عدم تقارن حمله/دفاع	۸۱

۸۲	قابلیت اعتماد در مقایسه با قابلیت اطمینان هوش مصنوعی
۸۷	خطرات امنیت سایبری مرتبط با انسان‌سازی هوش مصنوعی
۹۰	داتروپومورفیزم و ابهام‌زدایی از هوش مصنوعی
۹۲	بحث سلاح‌سازی و حمله در مقابل دفاع
۹۹	فصل سوم: امنیت سایبری برای هوش مصنوعی
۱۰۱	مقدمه
۱۰۵	سیستم‌های یادگیری ماشینی سطح حمله بزرگ‌تری دارند
۱۰۷	دیدگاه سطح بالا از چشم‌انداز تهدید
۱۰۷	حملات ورودی
۱۱۰	حملات سمی
۱۱۲	یک مدل تهدید هوش مصنوعی
۱۱۲	لایه زیرساختی
۱۱۲	لایه داده
۱۱۳	لایه مدل
۱۱۴	لایه الگوریتمی
۱۱۴	لایه عملیاتی
۱۱۵	نقش عاملان انسانی
۱۱۶	ایمنی و امنیت زیرساخت‌های باز، مستقل و مبتنی بر هوش مصنوعی و تکامل زمان اجرا آن
۱۲۲	کاهش ناامنی شبکه از آنجایی که مرتبط با هوش مصنوعی است
۱۳۰	مرحله ایده‌پردازی
۱۳۱	مرحله برنامه‌ریزی
۱۳۱	مرحله طراحی
۱۳۱	مرحله ساخت
۱۳۲	مرحله استقرار
۱۳۳	فصل چهارم: مسائل و توصیه‌های سیاست
۱۳۵	مقدمه
۱۳۵	قوانین فعلی و آینده هوش مصنوعی: پاسخ‌گویی، قابلیت حسابرسی و اعمال نظارتی
۱۳۸	چارچوب‌های قانونی موجود: امنیت سایبری اتحادیه اروپا
۱۴۰	مسائل عمده سیاست
۱۴۰	تفویض کنترل
۱۴۲	باز بودن تحقیق
۱۴۶	خط‌مشی‌های ارزیابی ریسک و تست تناسب

چالش‌های فناوری، حکومت و سیاست

مرکز مطالعات سیاسی اروپا^۱ یک مؤسسه تحقیقاتی مستقل در زمینه سیاست‌گذاری است که در بروکسل مستقر است. وظیفه این مرکز ارائه تحقیقات تحلیلی قوی است که منجر به راه‌حل‌های سازنده برای چالش‌های پیش روی اروپا در حال حاضر می‌شود.

پیشگفتار

این گزارش بر اساس بحث‌های انجام‌شده در گروه کاری مرکز مطالعات سیاسی اروپا در زمینه هوش مصنوعی و امنیت سایبری است. این گروه کاری متشکل از کارشناسان صنعت، نمایندگان اتحادیه اروپا و نهادهای بین‌المللی، دانشگاهیان، سازمان‌های جامعه مدنی و پزشکان بود (لیست شرکت‌کنندگان در ضمیمه II را ببینید). فعالیت گروه در پاییز ۲۰۱۹ میلادی آغاز شد، در چهار مورد جداگانه ملاقات کرد و در طول شکست کووید - ۱۹ تا مارس ۲۰۲۱ میلادی به صورت آنلاین ادامه یافت.

به عنوان هماهنگ‌کننده گروه کاری، من خواهم از مشارکت ارزشمند همه شرکت‌کنندگان در این کار قدردانی کنم. تشکر ویژه از اعضای هیئت مشورتی: جونا برایسون^۲ در مدرسه حکمرانی هرتی، برلین، ماریاروساریا تادئو^۳ در دانشگاه کسنفورد، ژان مارک ریکلی^۴ در مرکز سیاست‌های امنیتی ژنو و مارک استوکلین^۵ در مرکز تحقیقات ماشین‌های تجاری بین‌المللی^۶، زوریخ. من همچنین مایلم از کار قابل توجهی که توسط گزارشگران همکارم، استفانو فانتین^۷، افونسو فریرا^۸ و کارولینا پولیتو^۹ انجام شده است، قدردانی کنم. این کار یک تلاش جمعی بوده است و همان‌طور که در خود متن نشان داده شده است، سایر

1- CEPS: The Centre for European Policy Studies.

2- Joanna Bryson.

3- Mariarosaria Taddeo.

4- Jean-Marc Rickli.

5- Marc Ph. Stoecklin.

6- IBM: International Business Machines.

7- Stefano Fantin.

8- Afonso Ferreira.

9- Carolina Polito.

مشارکت‌کنندگان در گروه کاری یا اعضای هیئت مشورتی با تهیه پیش‌نویس بخش‌های منتخب گزارش. یعنی جوانا برایسون، ماریاروساریا تادئو، ژان مارک ریکلی، دیوید کلارک^۱، راب اسپایگر^۲، کریس هاجینز^۳، مت والمزلی^۴، سباستین گرلاچ^۵ و ماتی آکسلا^۶. همچنین از اعضای که داوطلبانه نسخه‌های قبلی این گزارش را مرور کردند، به‌ویژه مارک رادیس^۷، کارول ماتز^۸، الکس سانگرس^۹، راشل آزافرانی^{۱۰}، فیلیپ گرافن^{۱۱}، جوزپه جیوانی داکینو^{۱۲}، فدریکا روسو^{۱۳}، نیتا پولمی^{۱۴}، واید هوگنوت^{۱۵} و میگوئل گونزالس-سانچو-بودرو^{۱۶}، قدردانی می‌کنم. همچنین از سخنرانان دعوت‌شده که در بحث گروه کاری مشارکت داشتند تشکر می‌کنم.

خلاصه اجرایی

مرکز مطالعات سیاست‌های اروپایی در پاییز سال ۲۰۱۹ میلادی کارگروهی در زمینه هوش مصنوعی^{۱۷} و امنیت سایبری راه‌اندازی کرد. هدف این کارگروه جلب توجه به چالش‌های فنی، اخلاقی، بازار و حکمیت ناشی از تقاطع هوش مصنوعی و امنیت سایبری بود. این گروه کاری، از نظر طراحی چند ذی‌نفع، متشکل از هفده سازمان خصوصی، هشت نهاد اتحادیه اروپا^{۱۸}، یک سازمان بین‌المللی و یک سازمان چندجانبه، پنج دانشگاه و

1- David Clark.

2- Rob Spiger.

3- Chris Hutchins.

4- Matt Walmsley.

5- Sebastian Gerlach.

6- Matti Aksela.

7- Mare Radice.

8- Carol Mezat.

9- Alex Sangers.

10- Rachel Azafrani.

11- Philip Graefen.

12- Giuseppe Giovanni Daquino.

13- Federica Russo.

14- Nineta Polemi.

15- Wide Hogenhout.

16- Miguel Gonzales-Sancho-Bodero.

17- AI: Artificial Intelligence.

18- EU: European Union.