CYRIS Cyber Research and Inovations in Security

leden/2025

NEWSLETTER

AKTUALITY VE VÝZKUMU A VÝVOJI V KYBERNETICKÉ BEZPEČNOSTI

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

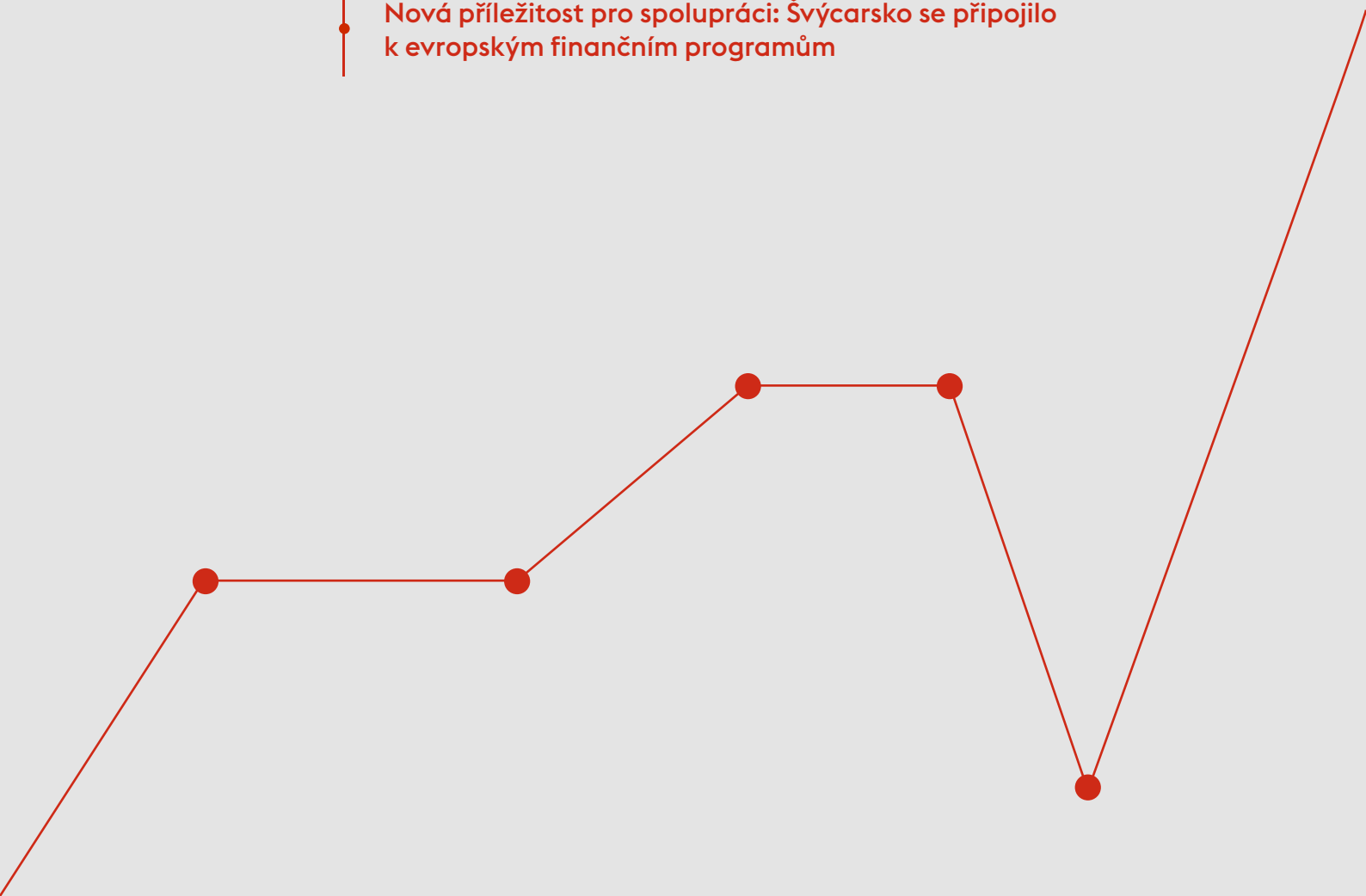
Aktuality, události a financování

3 Univerzita Tel Aviv nabízí stipendia pro hostující výzkumné pracovníky zaměřené na kyberbezpečnost

4 Eurostars-3 a MŠMT vyhlásili výzvu pro podporu malých a středních podniků

5 Vyhlášení 2. Výzvy Národního koordinačního centra „CyberCertification Boost“

Nová příležitost pro spolupráci: Švýcarsko se připojilo k evropským finančním programům



Univerzita Tel Aviv nabízí stipendia pro hostující výzkumné pracovníky zaměřené na kyberbezpečnost

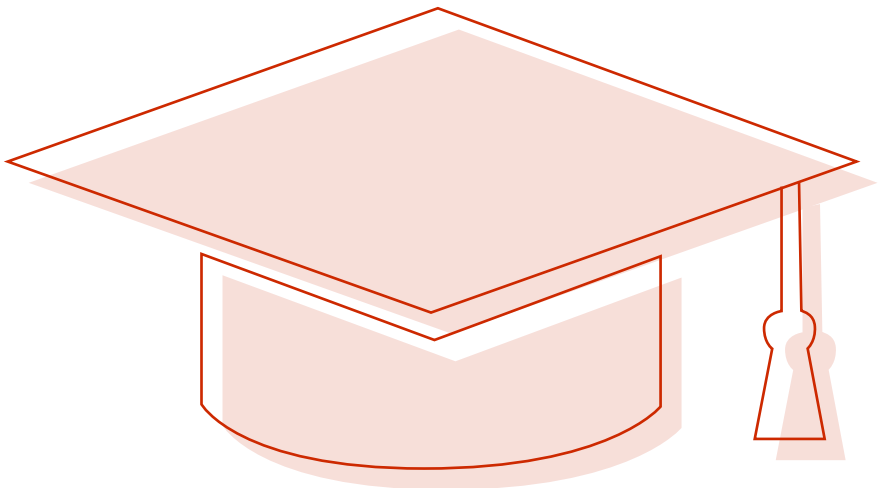
Blavatnikovo mezioborové centrum pro kybernetický výzkum na Tel Avivské univerzitě hledá zájemce o stipendia pro hostující výzkumné pracovníky.

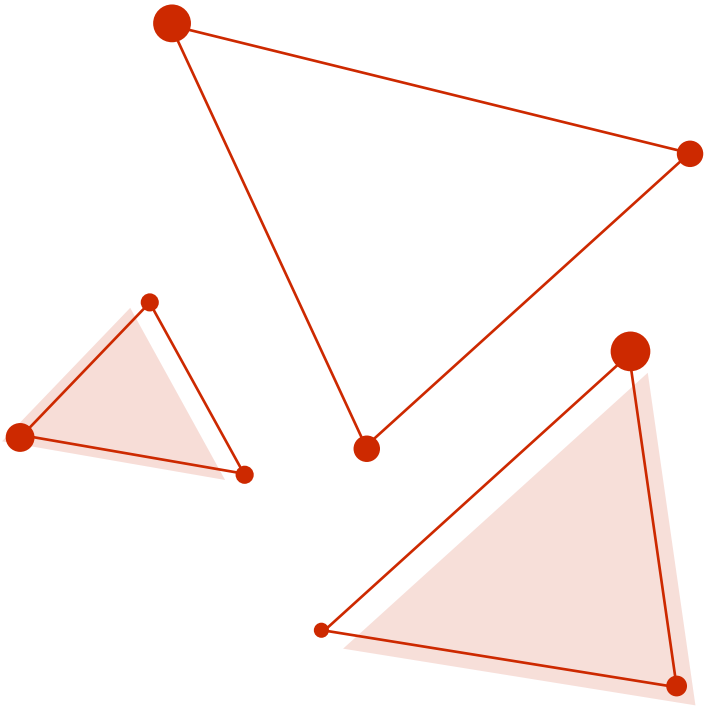
Program je určen pro vědce a postgraduální studenty zaměřující se na **kybernetickou bezpečnost, umělou inteligenci a příbuzné obory**.

Role hostujícího výzkumného pracovníka nabízí příležitosti pro realizaci vlastního výzkumu za využití univerzitních kapacit a technologií, navazovaní spolupráce s izraelskými výzkumníky působícími v oboru či účast na vědeckých i komerčních akcích, včetně celosvětově známé akce CyberWeek.

Zájemci se mohou hlásit prostřednictvím online formuláře.

tc.cz





Eurostars-3 a MŠMT vyhlásili výzvu pro podporu malých a středních podniků

Evropské partnerství pro inovativní malé a střední podniky (Eurostars-3) ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy (MŠMT) vyhlásilo **8. výzvu zaměřenou na podporu inovativních malých a středních podniků**.

Výzva cílí na mezinárodní výzkumné, vývojové a inovační projekty, jejichž **výsledkem bude nový produkt, proces nebo služba pro komercionalizaci na evropských a globálních trzích**.

Maximální výše podpory pro projekt činí až 160 000 EUR na rok, přičemž projekty můžou trvat až 3 roky. Výzva byla vyhlášena v pátek 10. ledna 2025 na webových stránkách sítě Eureka a **uzávěrka proběhne ve čtvrtek 13. března 2025 ve 14:00 hodin**.

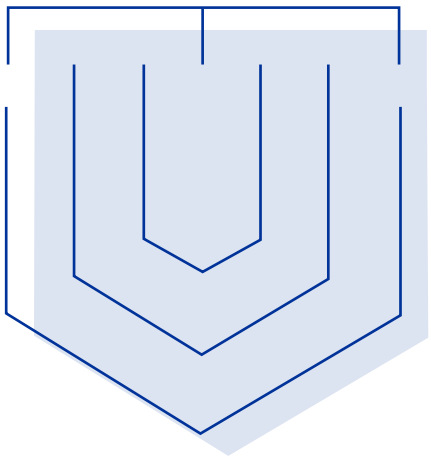
tc.cz

Vyhlášení 2. Výzvy Národního koordinačního centra „CyberCertification Boost“

NÚKIB v roli NKC vyhlásil **2. Výzvu k podávání projektů „CyberCertification Boost: Podpora rozvoje certifikačních kapacit v kybernetické bezpečnosti“**.

Cílem výzvy je podpořit rozvoj a posílení certifikačních kapacit v oblasti kybernetické bezpečnosti v České republice.

Příjem žádostí bude ukončen 31. března 2025. Podrobnosti k výzvě a podmínkám podávání žádostí naleznete na webu NÚKIB.

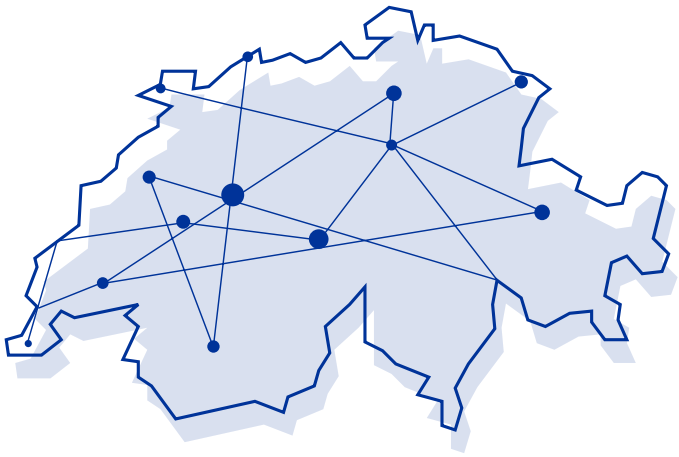


Nová příležitost pro spolupráci: Švýcarsko se připojilo k evropským finančním programům

Švýcarsko se připojilo jako **asociovaná země** k programu **Digitální Evropa** (DEP), který podporuje rozvoj klíčových digitálních technologií, jako jsou superpočítače, umělá inteligence nebo **kybernetická bezpečnost**.

Nová dohoda umožní Švýcarsku také účast na několika unijních programech, včetně Horizon Europe, Euratom Research, ITER/F4E, Erasmus+ nebo EU4Health.

Tento krok přináší nové příležitosti pro spolupráci na inovativních řešeních mezi členskými státy EU a Švýcarskem, přičemž švýcarským subjektům bude umožněno účastnit se výzev od 1. ledna 2025.



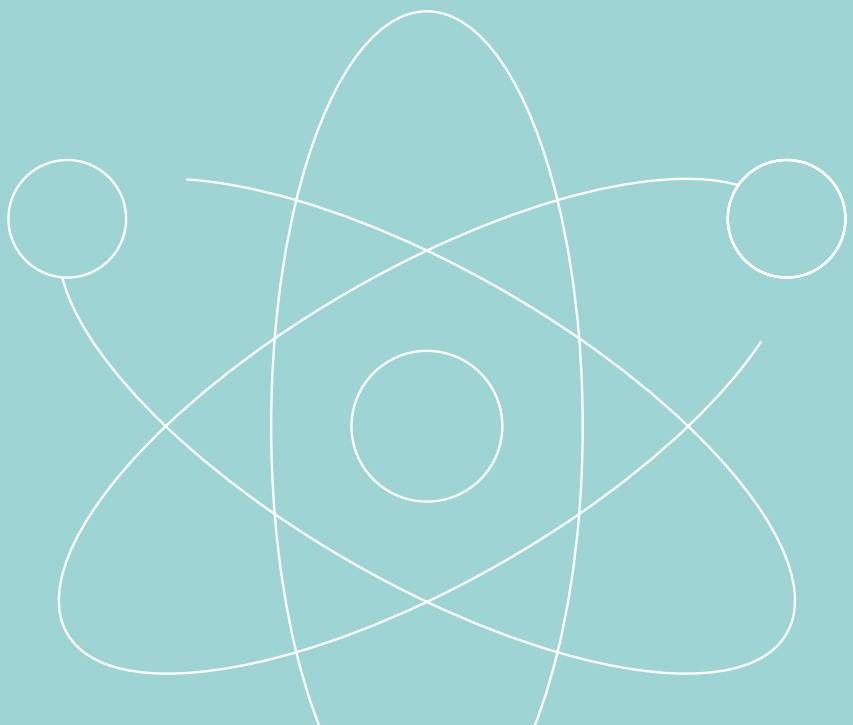
NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

Spolufinancováno Evropskou unií

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Podpořeno z programu Digitální Evropa v rámci projektu National Coordination Centre in the Czech Republic (č. 101127941). Názory a stanoviska uvedené vyjadřují pouze názory autora(ů) a nemusí nutně odrážet názory Evropské unie ani Evropského centra kompetencí pro kybernetickou bezpečnost. Evropská unie ani poskytovatel dotace nenesou za tyto názory odpovědnost.

Technologické novinky, objevy a zprávy



Čeští výzkumníci vytvořili výjimečnou datovou sadu pro analýzu síťového provozu

Vědecký tým ze sdružení CESNET a Fakulty informačních technologií ČVUT v Praze vytvořil unikátní datovou sadu, která zachycuje **roční síťový provoz v národní akademické síti**.

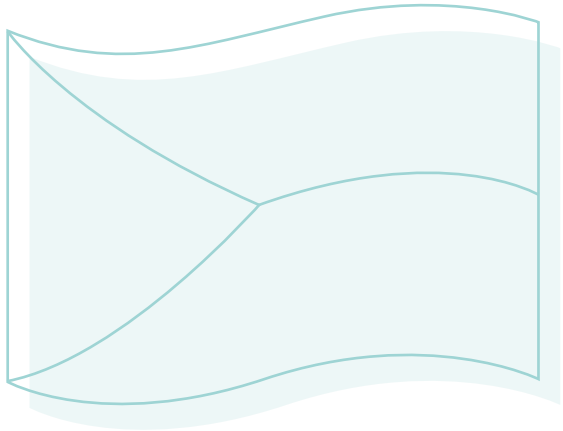
Tato anonymizovaná datová sada, publikovaná v prestižním časopise Nature Scientific Data, představuje významný krok ve výzkumu kybernetické bezpečnosti a detekce hrozeb.

Tradiční datové sady obvykle pokrývají pouze několik dní síťového provozu, což **omezuje možnost zkoumat časově proměnné jevy**. To často vede k situaci, kdy algoritmy strojového učení, navržené na základě těchto krátkodobých dat, selhávají při reálném nasazení kvůli tzv. datovému posunu – jevu, kdy modely ztrácejí přesnost vlivem změn v síťovém provozu, například po aktualizaci softwaru.

Nově vytvořená datová sada **umožňuje hlubší analýzu vlivu času na výkon algoritmů strojového učení**. Tím poskytuje cenný nástroj pro vývoj robustnějších detektorů kybernetických hrozeb, které jsou schopny adaptace na dynamicky se měnící síťové prostředí.

Projekt nesoucí název Analýza šifrovaného provozu pomocí síťových toků, financovaný z výzvy IMPAKT 1 Ministerstva vnitra ČR otevírá nové možnosti pro zlepšení bezpečnosti v digitálním světě a zároveň zdůrazňuje důležitost dlouhodobého sběru dat pro pokročilý výzkum v oblasti kybernetické bezpečnosti.

vedavyzkum.cz



Deset let nástrojů priority Widening v Česku: nejsilnějšími regiony jsou Praha a Brno

V uplynulém desetiletí se nástroje priority Widening, zaměřené na šíření excelence a rozšiřování účasti v evropských výzkumných programech, v České republice soustředily převážně do Prahy a Jihomoravského kraje, zejména Brna.

Tyto dvě metropole, klasifikované jako silní inovátoři podle Regional Innovation Scoreboard 2023, **výrazně profitovaly z projektů Widening**, což je v evropském kontextu spíše výjimečné.

Nedávné diskuse o možném přesunu zaměření Wideningu z národní na regionální úroveň vyvolaly obavy, že by inovačně silné regiony mohly být z těchto programů vyloučeny. To by mohlo negativně ovlivnit právě Prahu a Brno, které z těchto nástrojů dosud významně těžily.

Česká národní pozice proto **podporuje zachování Wideningu na národní úrovni, aby byla zajištěna kontinuita podpory pro klíčová výzkumná centra**.

Analýza Technologického centra Praha ukazuje, že **ČR efektivně využívá nástroje Widening**, přičemž hlavní část získaných prostředků směřuje do programů ERA Chairs, Teaming a Twinning. Zvýšená aktivita v těchto oblastech vedla k **násobnému nárůstu získaných finančních prostředků** oproti předchozímu programu Horizont 2020.

Pro posílení výzkumných kapacit je významný také nástroj **Excellence Hubs**, který podporuje spolupráci mezi akademickou sférou a soukromým sektorem – takovýmto projektem je i projekt The Cyber-security Excellence Hub in Estonia and South Moravia (CHESS), jehož součástí je v roli asociovaného partnera také NÚKIB.

vedavyzkum.cz

Umělá inteligence DeepSeek: Technologický pokrok nesoucí možná bezpečnostní rizika

Čínská společnost DeepSeek v lednu uvedla na trh svůj model umělé inteligence R1, který svým výkonem a efektivitou konkuruje západním jazykovým modelům jako je ChatGPT, Copilot nebo Gemini.

Posun ve vývoji umělé inteligence představuje především jeho **schopnost generovat výsledky s výrazně nižší energetickou náročností, a tudíž i s výrazně levněji**, a to při zachování všech vlastností, které nabízí konkurence. Tento technologický pokrok však zároveň vyvolává bezpečnostní a etické obavy.

Odborníci zjistili, že DeepSeek R1 je **náchylný k poskytování nebezpečných informací**, včetně návodů na výrobu zbraní, podpory sebepoškozování nebo vytváření malwaru.

Tyto nedostatky v bezpečnostních opatřeních mohou vést k manipulaci s názory uživatelů. Kromě toho DeepSeek R1 navíc vykazuje silnou zaujatost ve prospěch čínské vlády, což vyvolává **otázky ohledně cenzury a šíření propagandy**.

Kromě toho aplikace DeepSeek **shromažďuje a odesílá údaje** o uživatelích na servery v Číně, což vzbuzuje další obavy z možného zneužití těchto informací. V reakci na tato rizika již některé instituce, včetně amerického námořnictva, zakázaly používání aplikace DeepSeek ve svých služebních zařízeních.

Model R1 společnosti DeepSeek je zřetelným příkladem situace, kdy technologický pokrok přichází za cenu značných potenciálních bezpečnostních rizik. Z těchto důvodů je využívaní takových technologií nutné pečlivě zvážit.

theguardian.com

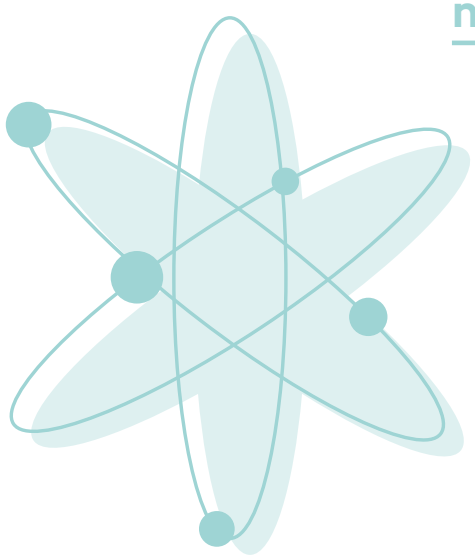
Budovaní kvantových spojů může vést ke stabilizaci kvantových sítí, důležitý je ovšem jejich správný počet

Fyzici z Northwestern University navrhli **novou strategii pro udržení komunikace v neustále se měnících kvantových sítích**. Kvantová provázanost fotonů slibuje revoluci v oblasti výpočetní techniky a komunikace, vedoucí k bezprecedentně rychlé a bezpečné výměně informací. Významným problémem však je, že tyto provázané stavy se po překonání určité vzdálenosti ztrácejí, čímž v podstatě dochází ke zhroucení sítě.

Strategií pro vyřešení tohoto problému je při propojovaní komunikačních uzlů **přidávat větší množství spojů v menší vzdálenosti od sebe**. Tento přístup umožňuje dosáhnout stabilizace sítě. Problematické je ovšem nalezení správného počtu spojů. Příliš mnoho spojů zatěžuje zdroje, zatímco příliš málo spojů vede k fragmentaci sítě a nedochází k efektivnímu řešení původního problému.

Průlomové je zjištění, že správný počet nových spojů lze odvodit jakožto odmocninu z počtu uživatelů. Například pro milion uživatelů je potřeba přidat 1 000 spojů na odeslání každého jednoho qubitu po síti. Tento objev se může stát základem pro **vytvoření optimálního návrhu stabilní kvantové sítě** schopné realizovat rychlé výpočty a ultra-bezpečnou komunikaci.

news.northwestern.edu



Připomínáme

V minulém čísle jsme vás informovali o **přípravách partnerských burz** k navazování kontaktů pro projekty připravované do výzev programu Horizont Evropa. Tyto zpravidla dvoudenní akce nabízí příležitost setkat se se zástupci desítek mezinárodních organizací, která mají zájem o předložení žádosti o financovaní projektu v rámci některé z nadcházejících výzev programu Horizont Evropa. V uplynulých letech tato akce **vedla ke vzniku mnoha řešitelských konsorcií, která následně realizovala velice úspěšné výzkumné projekty**. Většina partnerských burz probíhá fyzicky v Bruselu, Düsseldorfu, či Paříži, přičemž náklady na cestu lze pokrýt cestovním grantem až do výše 1000 €.

tc.cz

Věděli jste, že

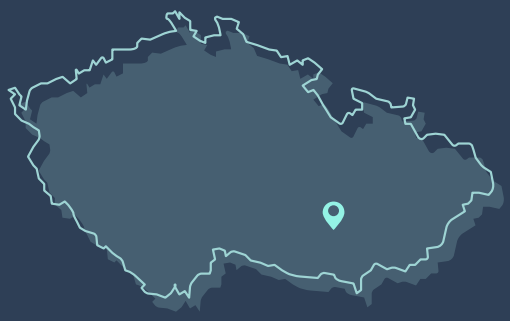
AI se může učit podobně jako malé dítě? Malý Sam nosil dvakrát týdně, od šesti měsíců do dvou let, na hlavě kameru, kterou zachycoval svět kolem sebe. Záznam zachycoval veškeré aktivity Sama jako je hraní, čtení či konzumaci jídla. Vědci pak tyto záznamy použili k tréninku umělé inteligence. **AI se učila jako dítě, bez předchozích znalostí, jen spojením slov a obrazů**. A překvapivě -to fungovalo! Výzkum poukazuje na skutečnost, že vývoj dětí nemusí být výrazně závislý na vrozené schopnosti učit se jazyk, ale tím nejvýznamnějším je schopnosti vidět a spájet si obrázkové a zvukové vjemy.

vedavyzkum.cz

Kontaktní informace

Národní úřad pro kybernetickou a informační bezpečnost

Oddělení vědy, výzkumu a inovací



Mučednická 1125/31
616 00 Brno
Tel.: +420 541 110 777
P. O. BOX 17, Brno 16, CZ 616 00

Olšanská 36/9
130 00 Praha
Tel.: +420 607 032 806
e-mail: vyzkum@nukib.gov.cz

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Zaregistrujte se ke členství

Naskenuj mě

Tato datová sada nám poskytla příležitost analyzovat vliv času na výkon algoritmů, což je pro oblast kyberbezpečnosti zásadní. Můžeme díky tomu lépe pochopit, jaké faktory způsobují datový posun a jak tomu předejít,

Ing. Jan Luxemburk, výzkumník z FIT ČVUT