

NÚKIB

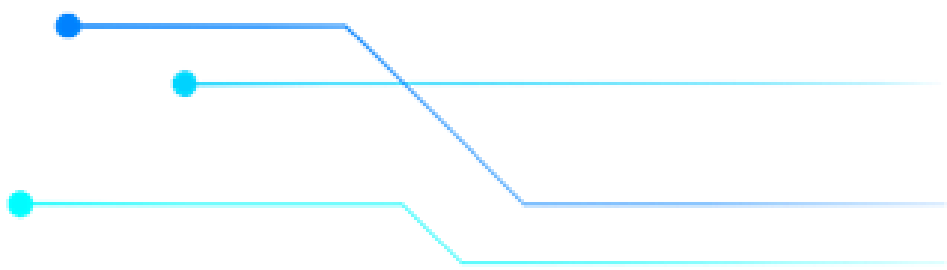


Národní úřad
pro kybernetickou
a informační
bezpečnost

Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

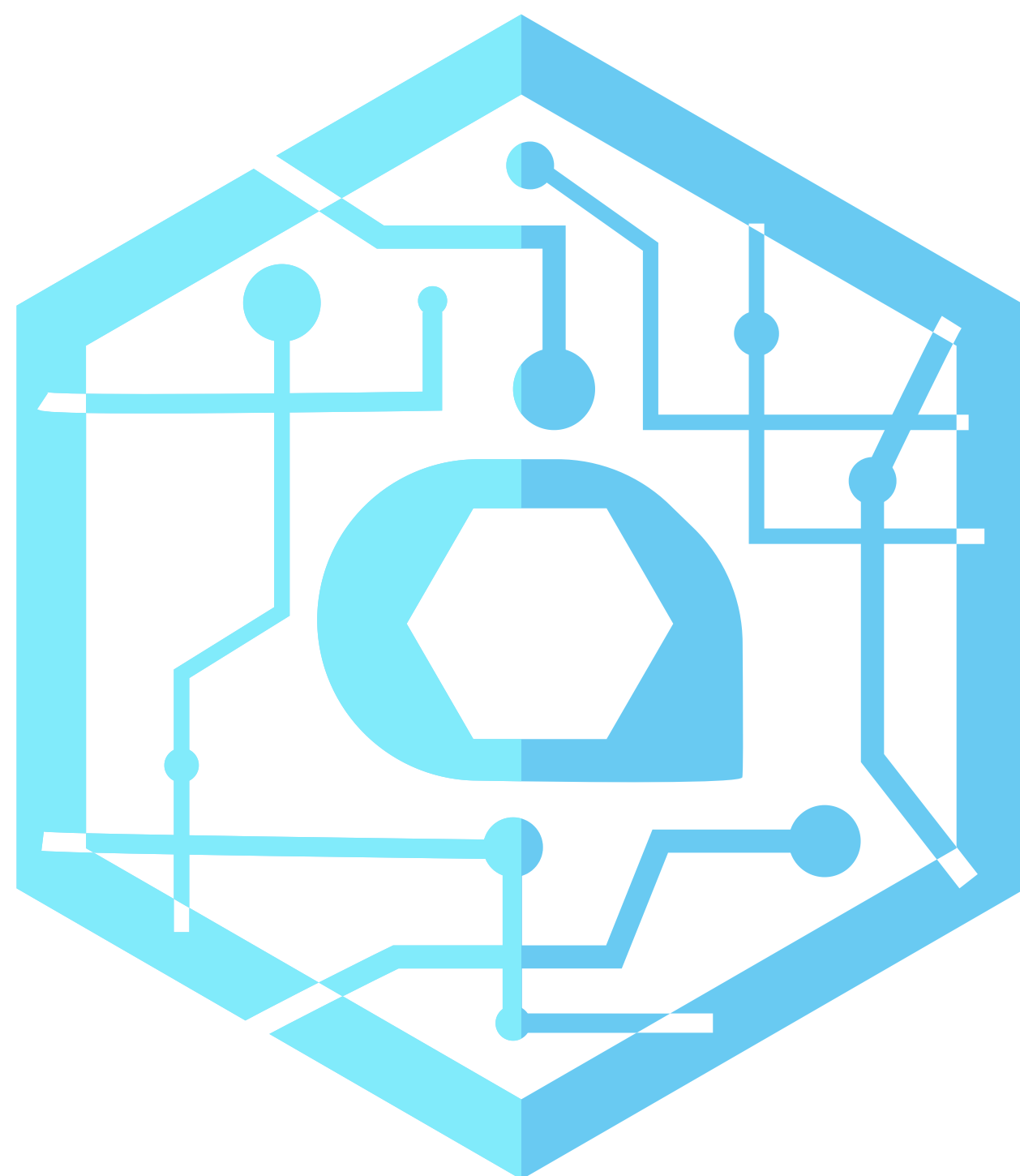
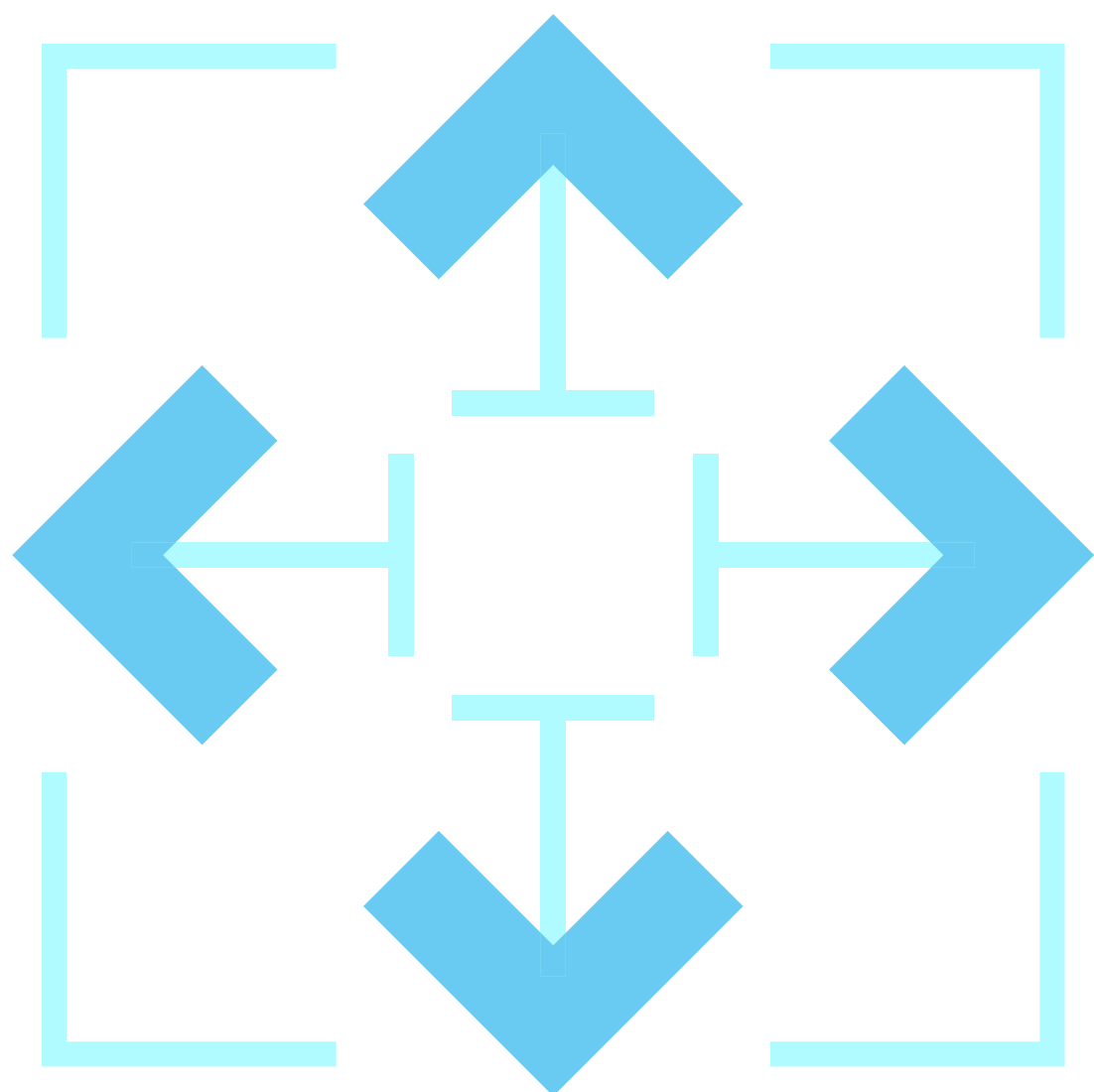
07/2023

ČERVENEC



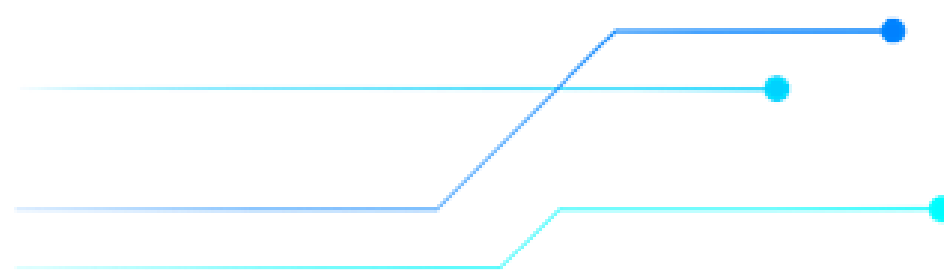
Španělsko v úvodu svého předsednictví v Radě EU klade důraz na kybernetickou bezpečnost

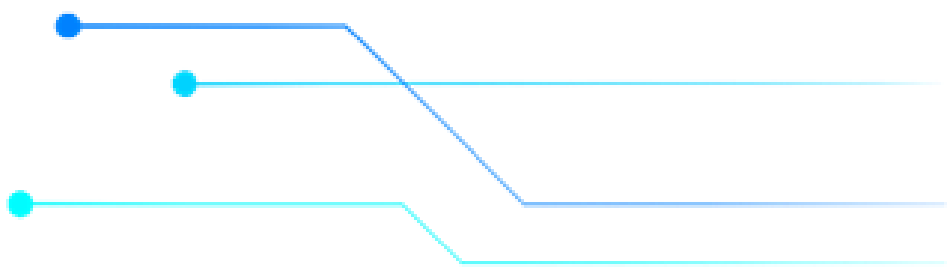
Španělské Národní koordinační centrum (NKC) spadající pod Španělský národní institut pro kybernetickou bezpečnost (INCIBE) uspořádal v průběhu července Workshop NKC o kybernetické bezpečnosti v rámci španělského předsednictví Rady EU. Iniciativy se v hybridním formátu zúčastnilo na 40 zástupců evropské sítě NKC, Evropské komise, Evropské agentury pro kybernetickou bezpečnost (ENISA), OECD a zástupců podniků působících v oblasti kybernetické bezpečnosti. Cílem semináře bylo zahájit hloubkový dialog s cílem posílit účast a váhu malých a středních podniků a inováčního ekosystému v iniciativách v oblasti kybernetické bezpečnosti, výzkumu, vývoje a inovací financovaných Evropskou unií.



Česká republika se stala sídlem pro centrum excellence umělé inteligence

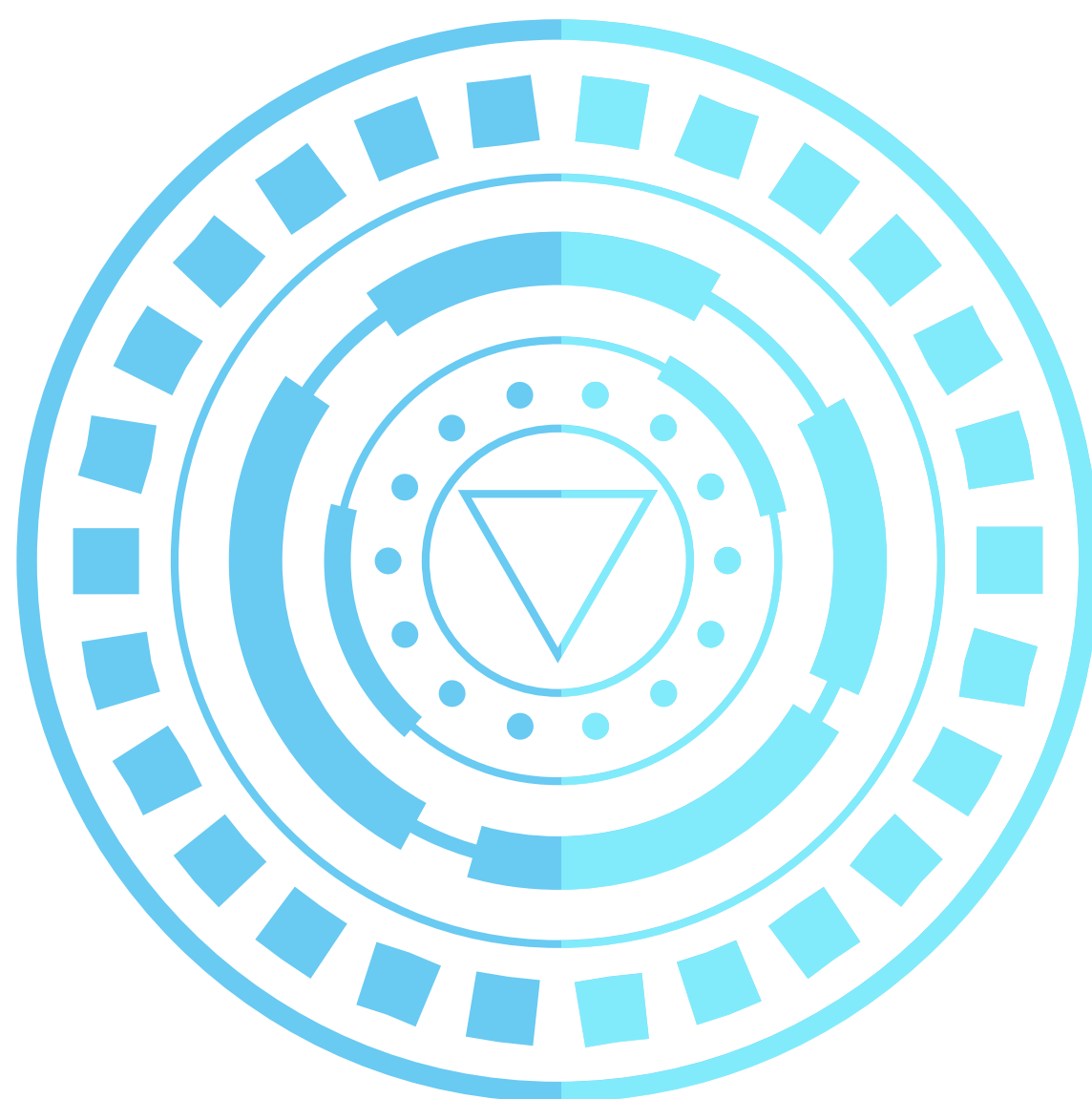
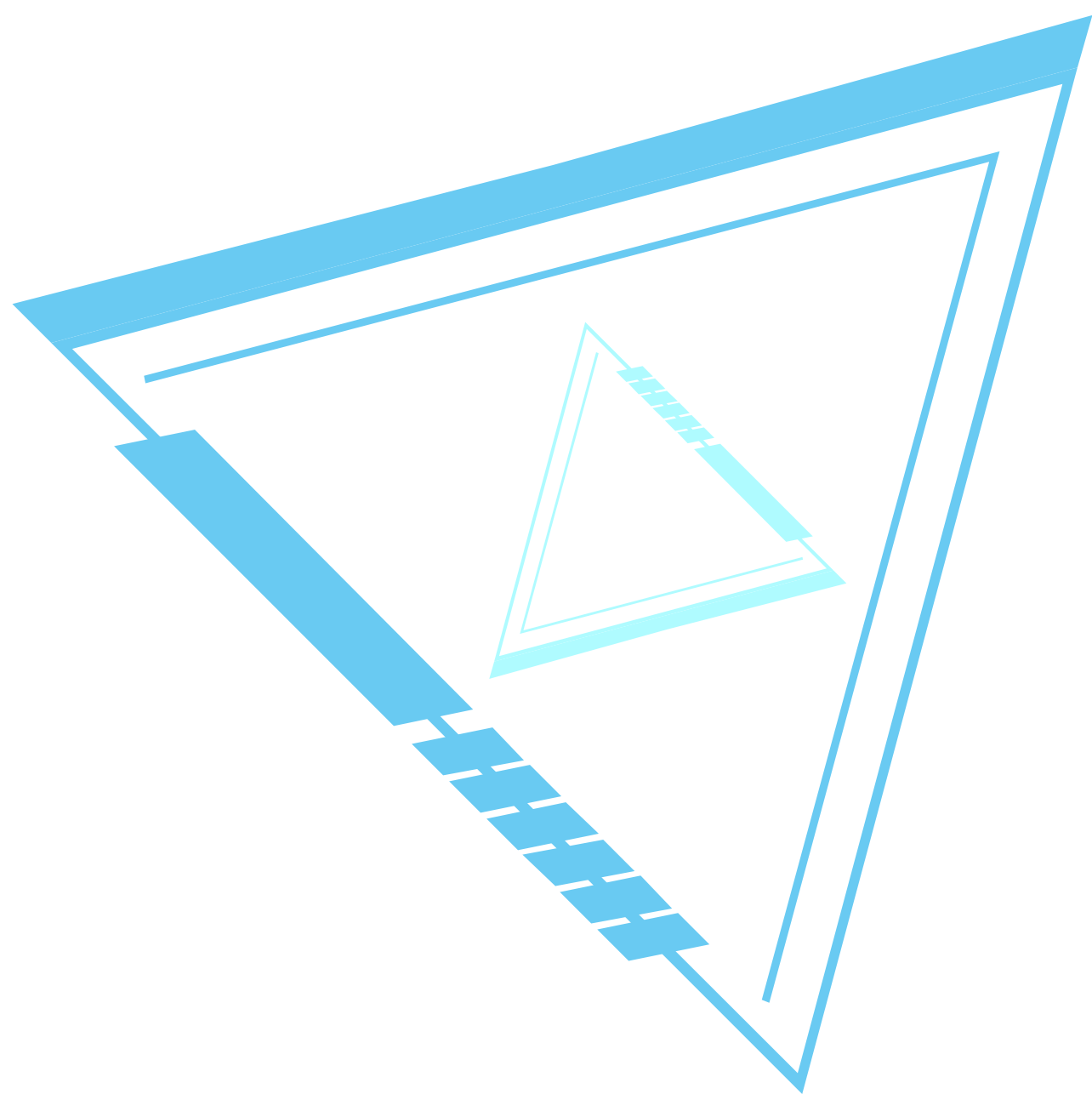
Nové centrum otevřela společnost IBM v Praze, a to se zaměřením na generativní umělou inteligenci. Cílem tohoto centra je pomoci českým firmám připravit se na éru pokročilých modelů strojového učení, které mají obrovský technologický i ekonomický potenciál. Pražské centrum se stalo součástí celosvětové sítě, kterou tvoří přibližně 1000 odborně zaměřených konzultantů, kteří se specializují na zvyšování produktivity informačních technologií a souvisejících aspektů.





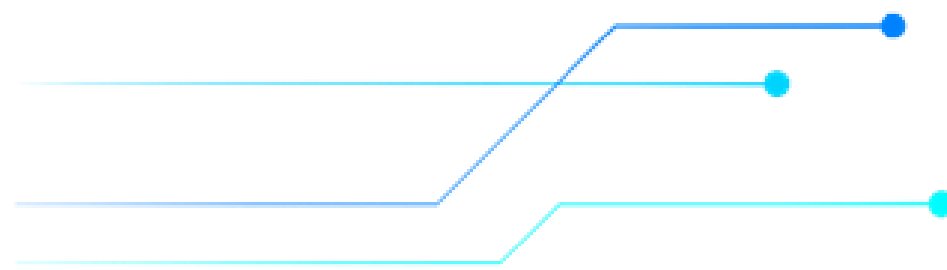
Cybertech Europe se vrací již na začátku října

Konference Cybertech Europe, zaměřená na sdílení nejnovějších inovací, výzev a řešení v digitálních technologiích, se uskuteční ve dnech 3.-4. října v italském Římě. Účastníci se mohou těšit na přednášky předních představitelů odvětví digitálních technologií z oblasti státního i soukromého sektoru, jakožto i na panelové diskuze expertů. Program se dále zaměří na aktuální trendy a směřování v oblasti kybernetické a informační bezpečnosti. Součástí akce je také prezentace partnerských subjektů působících v odvětví digitálních technologií. Registrace je možná přes oficiální stránky konference.



Český fond na podporu startupů podpoří rozvoj umělé inteligence

Pražský AI Startup Incubator otevírá fond pod názvem Look AI Ventures (LAIV), který se zaměřuje výhradně na startupy působící v oblasti umělé inteligence. Cílová částka, kterou by měl fond naplnit, je 20 milionů eur směřovaných do AI startupů v rané fázi vývoje, ale s vysokým potenciálem růstu a uplatněním technologie umělé inteligence v klíčových sektorech. Investice do jednoho startupu může dosáhnout výše 250 tisíc eur s možností reinvestice až do úrovně jednoho milionu eur. Reinvestice budou uskutečněny do startupů, které v portfoliu LAIV ukáží v následujících letech největší potenciál výnosu. LAIV by měl být tvořen alespoň z pětatřiceti startupů. V současné době je však ještě v procesu fundraisingu.



Displej se schopností měnit tvar v budoucnu umožní dotek s digitálními objekty

Vědci z University of Colorado Boulder vyvinuli unikátní displej schopný měnit svůj tvar. Zobrazovací jednotka je tvořena mřížkou měkkých robotických „svalů“, jež dokáží vnímat tlak a na jeho základě vytvářet vzory. Tato inovace vychází z technologie tzv. měkkých robotů (soft robots – robotické mechanismy z měkkých, flexibilních materiálů, jenž mají svým vzhledem a funkcí připomínat živé organismy), konkrétně ze třídy nazývané hydraulicky zesílené elektrostatické aktátory (Hydraulically Amplified Self-Healing Electrostatic – HASEL). Takovýto 3D displej má potenciál přenášet na dálku nejen třírozměrný vzhled zobrazovaného objektu, ale také přináší možnost se objektu přímo dotknout, a tím získat hmatový vjem. Displej může generovat širokou škálu objektů od rolovacího textu až po konkrétní předměty, u kterých je schopen navíc simulovat jejich případné pohyby. Ačkoli se v současné době jedná o prototyp, který vznikl na základě výzkumu syntetických biologických orgánů, může tato technologie v budoucnosti nalézt široké spektrum využití od prostého vytváření 3D modelů až po senzorické rukavice pro virtuální realitu.

Věděli jste, ŽE...

...ČVUT v Praze, Masarykova univerzita v Brně, Vysoká škola Ambis a iniciativa prg.ai společně pracují na projektu mapování rizik, příležitostí a regulace umělé inteligence v kontextu lidských práv. Cílem projektu je identifikovat příčiny porušení lidských práv umělou inteligencí a sestavit sadu doporučení, jak tyto technologie vyvíjet, používat a regulovat tak, aby nedošlo k ohrožení lidských práv, ale naopak pomohli je chránit. Projekt financovaný TAČR mimo jiné podtrhává multioborový charakter moderních digitálních technologií.

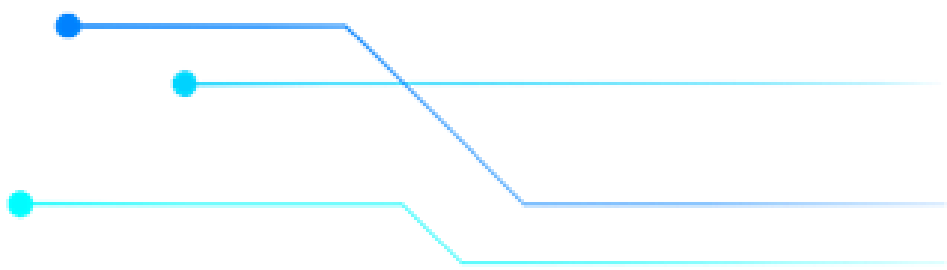
Technologie AI.X zvyšuje zabezpečení proti zneužití biometrických údajů skrze deepfakes

Společnost Daon specializující se na biometrická a identifikační řešení představila technologii AI.X pro odhalování deepfakes (technologie na bázi umělé inteligence, která shromažďováním modelů lidského chování, fotografií a skenů lidských tváří a zvukových nahrávek hlasů umožňuje napodobňovat skutečné osoby a nechat je simulovat libovolné chování). Generativní technologie pro vytváření deepfakes představují výraznou hrozbu jakožto nástroje na odcizení identity, a to zejména při obcházení zabezpečení skrze ověřování hlasu, skenu obličeje nebo snímků identifikačních průkazů. Technologie AI.X se tedy soustřeďuje na odhalování tzv. prezentačních útoků zaměřených na napodobování lidského hlasu (cloned voice) – takové útoky jsou typické prezento-

váním deepfakes nástroji pro snímání biometrických údajů s cílem neoprávněně do něj vniknout a odcizit zpřístupněná data. Model od společnosti Daon je díky umělé inteligenci schopen hlasové deepfakes nejen detekovat, ale také zamezit případnému vpuštění do služby nebo aplikace, do které se uživatel přihlašuje prostřednictvím biometrických údajů. Algoritmy AI.X identifikují jedinečné hlasové vzory v deepfake, které ovšem mohou být pro lidské ucho zcela nerozpoznatelné.

„Značné jsou také potenciální dopady (AI) na samotného uživatele a je otázkou času, kdy se i v ČR objeví první stížnosti a žaloby na porušení lidských práv...”

Lukáš Kačena
výkonný ředitel prg.ai



Výzkumníci z Univerzity Palackého v Olomouci spolupracují na vývoji superrychlých kvantových počítačů

Zástupci olomoucké univerzity jsou součástí mezinárodního konsorcia, v rámci kterého spolupracují s kolegy z University of Tokyo, Australian National University a University of New South Wales na vývoji superrychlých optických kvantových počítačů. Česká část vědecké skupiny se soustřeďuje na nelineární měření propagujícího se elektromagnetického pole. Právě nelineárnost operací, tedy násobení určitých kvantových stavů, představuje základ pro optické kvantové počítače. Nelinearity výzkumníci dosáhli prostřednictvím kombinace rychlých nelineárních výpočtů v digitálních elektronických obvodech a nových stavech světla se silně kvantovými vlastnostmi snižujícími šum v nelineárních obvodech. Pomocí měření na velkém vzorku různých

stavů světla následně výzkumníci ověřili, že měřicí obvod skutečně provádí požadovanou nelineární operaci. Daná metoda podle vědců umožňuje vysokou rychlost obvodu a je s ní spojena potřeba pouze malého optického zpoždění a nízkých ztrát. Čeští vědci využili tuto metodu měření jako první na světě. Hlavní výhodou optických řešení je, že mohou operovat za pokojové teploty s vysokými opakovacími frekvencemi. Optické kvantové počítače lze navíc díky moderním technologiím klasické optické komunikace propojovat i na velkou vzdálenost. Experiment dokázal funkčnosti flexibilní a rychlé nelineární dopředné vazby, na jejímž základě bude možné sestavit technologii pro optické kvantové výpočty.

Tipy na zajímavé akce

Září

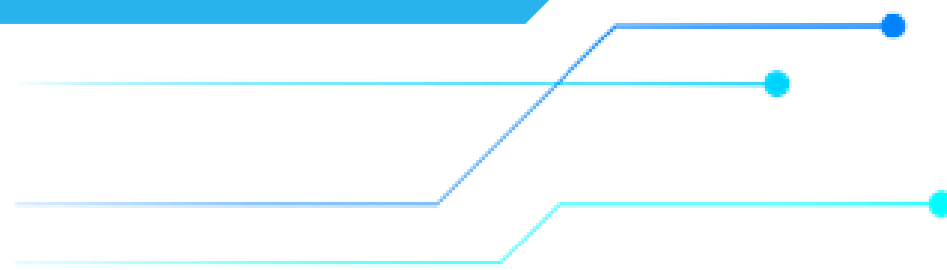
13. – 2023 CTI-EU Conference powered by ENISA

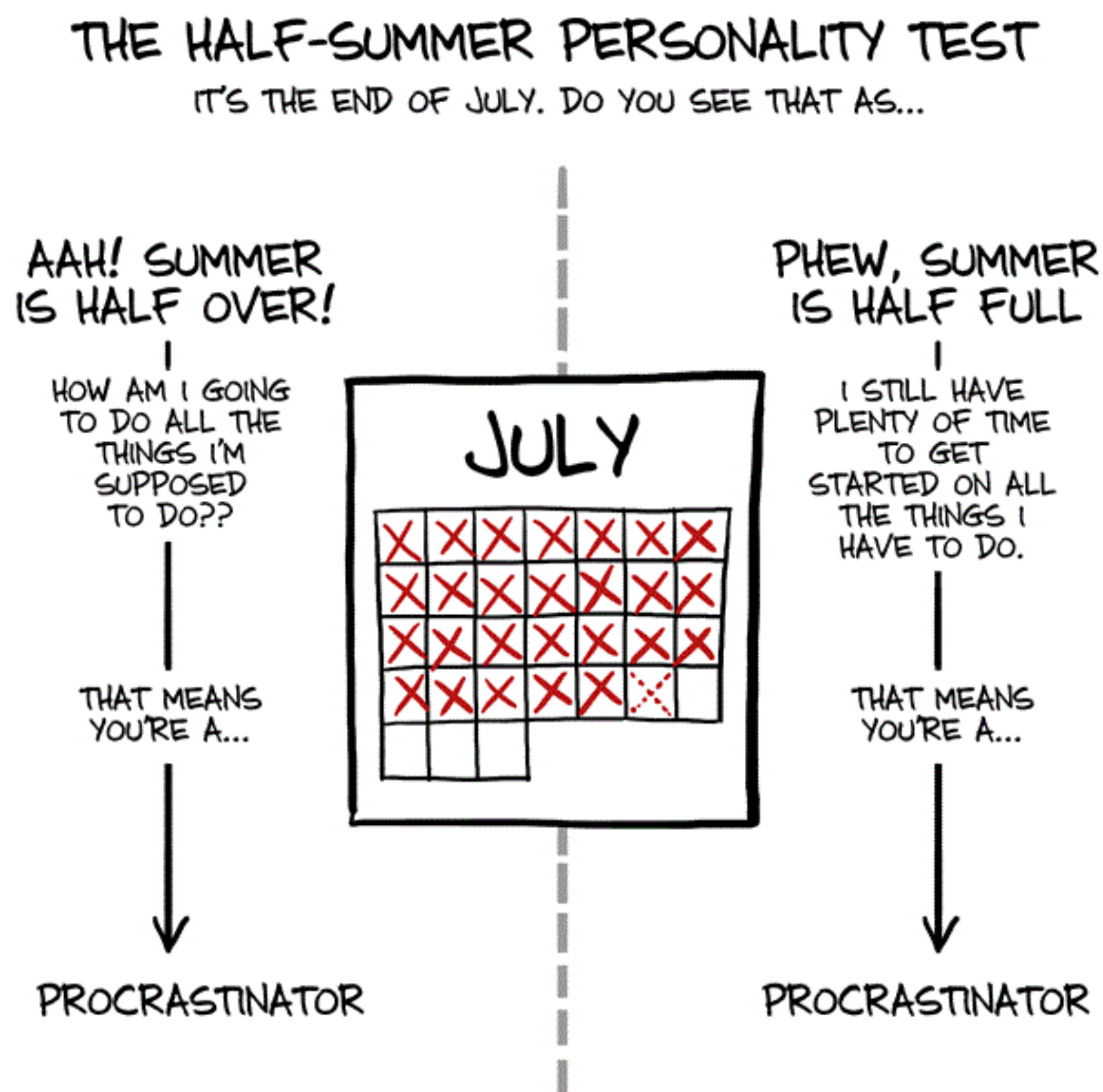
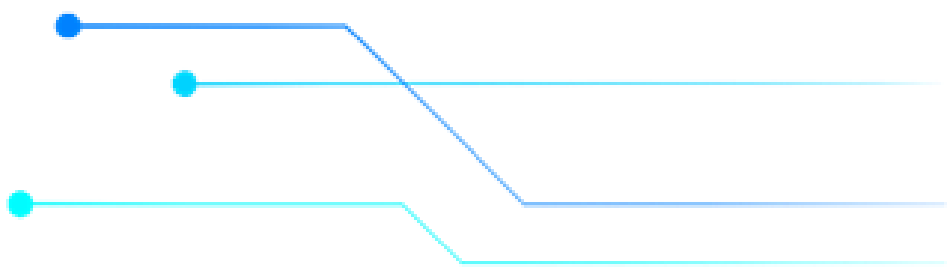
21. – Digitalizace, umělá inteligence a kybernetická bezpečnost

21.-22. – European Cybersecurity Skills Conference 2023

Říjen

11.-12. – Evropské infodny k výzvám 2024 v Klastru 4 Digitalizace, průmysl a vesmír





Národní úřad
pro kybernetickou
a informační bezpečnost

Mučednická 1125/31

616 00 Brno

Tel.: +420 541 110 777

P.O. BOX 17, Brno 16, CZ 616 00

Oddělení vědy, výzkumu
a inovací



Olšanská 36/9

130 00 Praha

Tel.: +420 607 032 806

e-mail: vyzkum@nukib.cz

