NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

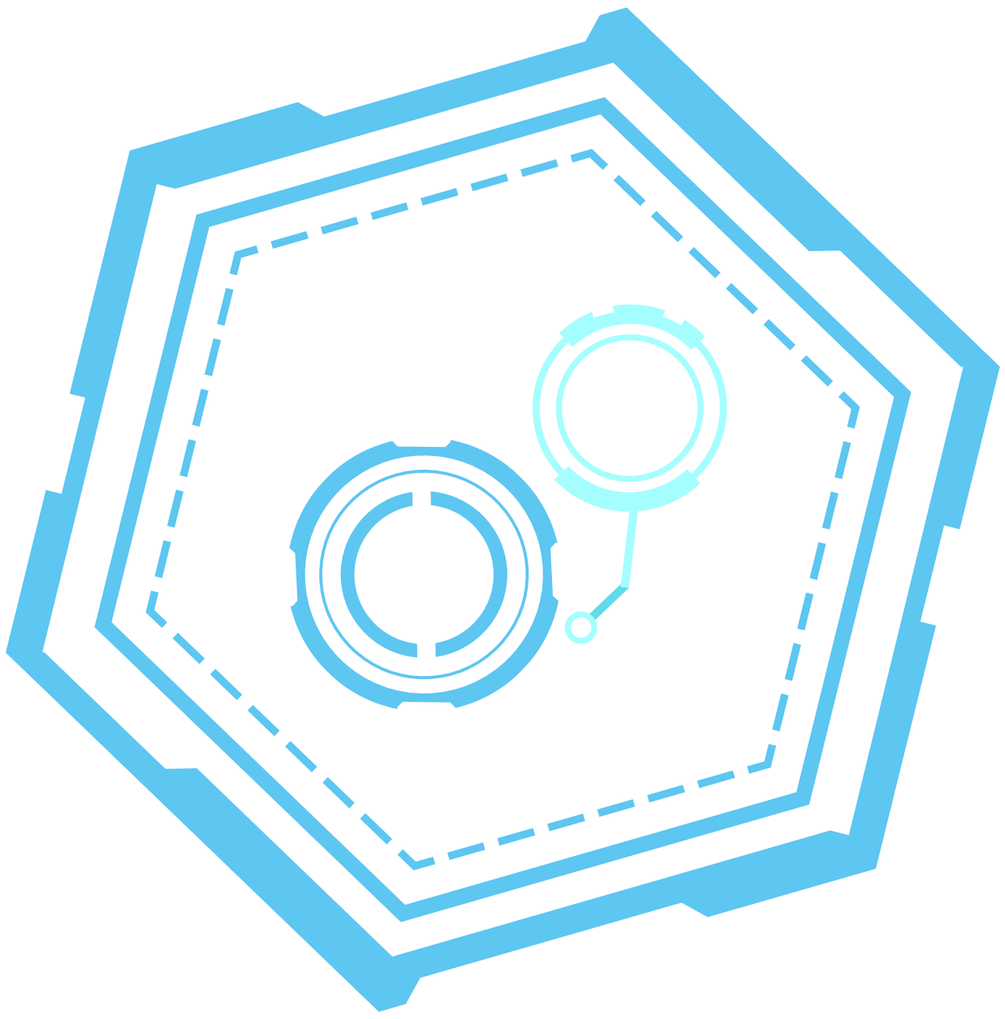
Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

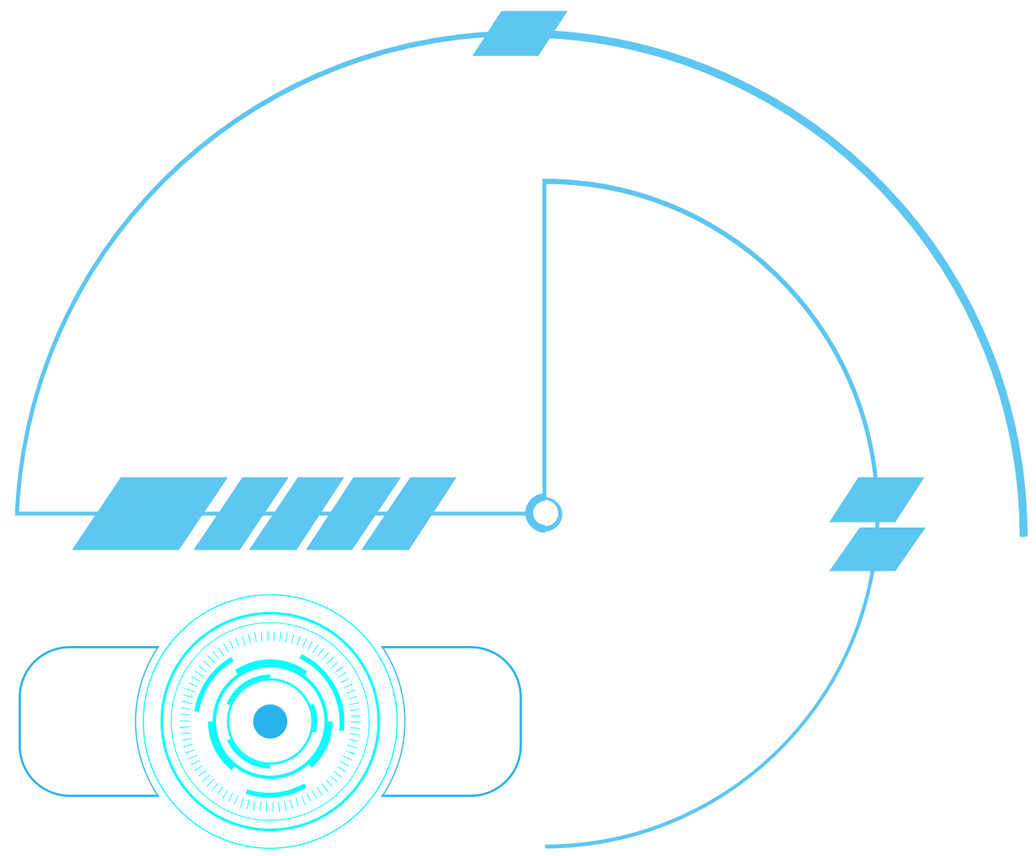
08/2023

SRPEN

Info dny Evropské komise k programu Horizon Europe

Dvoudenní akce zaměřená na sdílení možností financovaní výzkumu z Horizon Europe se uskuteční ve dnech 11.-12. října 2023. Tyto informační dny jsou věnovány pracovnímu programu Klastr 4 Digital Industry and Space na období let 2023-2024, jenž se zaměřuje mimo jiné např. na digitální technologie a průmysl. Přizvaní hosté budou přednášet nejen o jednotlivých tématech výzvy, ale také přiblíží systém hodnocení přihlášených projektů. Chybět nebude ani prostor pro otázky hostů a vzájemnou diskuzi. Akce se uskuteční online, k účasti je ovšem nutná bezplatná registrace.

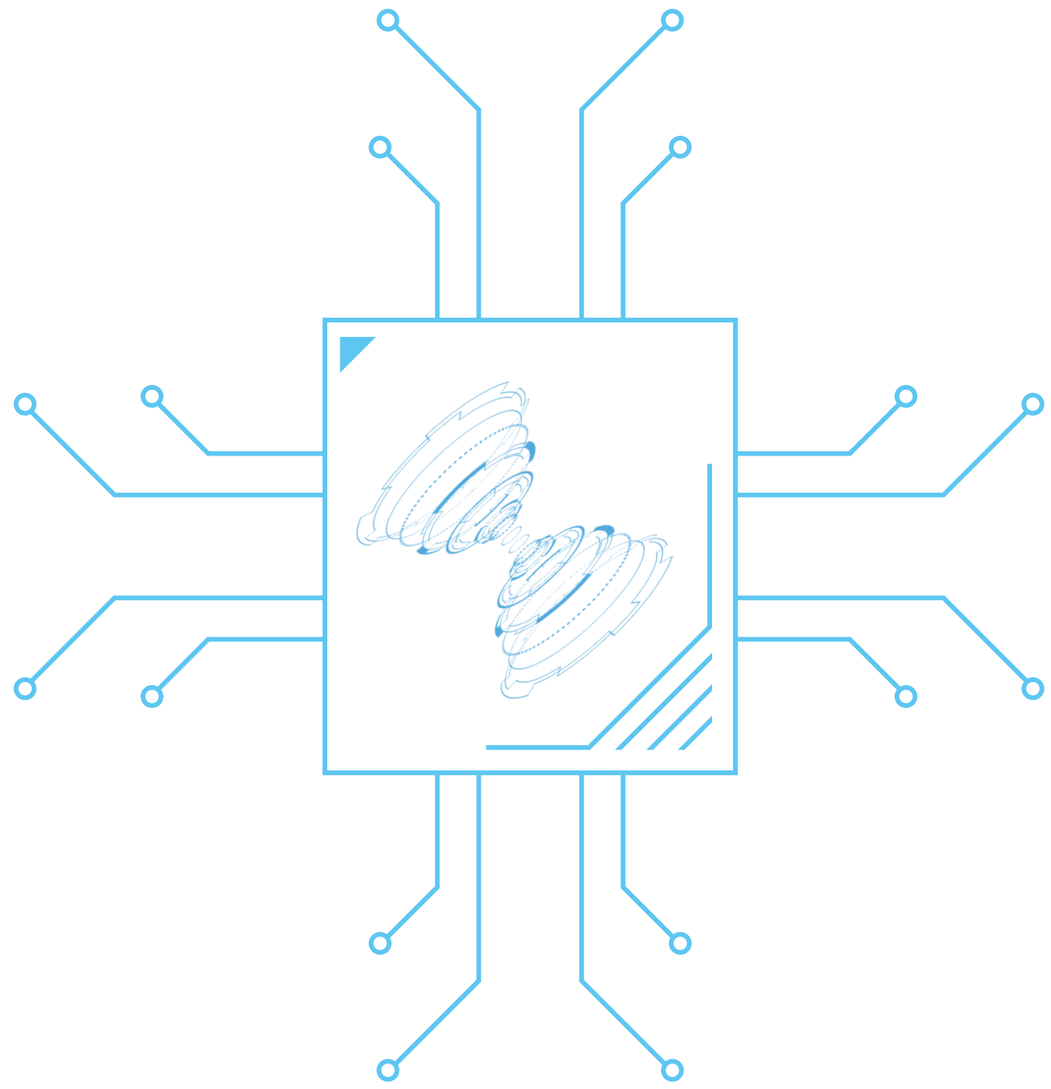




Indie hostila setkání ministrů pro digitalizaci G20

Jednání ministrů pro digitalizaci zastupující země s největšími a nejrychleji rostoucími ekonomikami v oblasti digitálních technologií se uskutečnilo v rámci indického předsednictví G20. Ze setkání, které se uskutečnilo 19. srpna 2023 ve městě Bangalore, vzešla dohoda o přípravě společného prohlášení na podporu digitálních inovací a začleňování digitálních dovedností a bezpečnosti do digitální ekonomiky. Digitální veřejná infrastruktura by měla podporovat inovace a hospodářskou soutěž a zároveň respektovat lidská práva, přičemž na globální úrovni by měla přinést efektivnější a inkluzivnější veřejnou správu ve službách občanů. Evropskou unii zastupoval Roberto Viola, generální ředitel DG CONNECT (Generální ředitelství pro komunikace, sítě, obsah a technologie) Evropské komise.

Mezinárodní kyberbezpečnostní výzvu ovládl Tým Evropa



Prvenstvím v druhém ročníku této mezinárodní soutěže se pyšní Tým Evropa, jenž tak obhájil své loňské vítězství při premiéře této soutěže. Akce proběhla 4. srpna 2023 v americkém San Diegu, kde proti sobě stálo celkem 7 týmů z Afriky, Asie, Kanady, Evropy, Latinské Ameriky, Oceánie a Spojených států amerických. Soutěžící z 65 států soupeřili v aktivitách jako Capture the Flag nebo Attack and Defence. Za Týmem Evropy skončila na druhém místě Oceánie, třetí místo obsadila Asie. Akce má za cíl otevřít přístup do světa kybernetické bezpečnosti mladým talentům a podporovat rozvoj jejich dovedností a kreativního myšlení při řešení komplexních situací.

Digitalizace, AI a kybernetická bezpečnost tématem pražské konference

Dne 21. září 2023 se v Praze uskuteční konference s názvem Změní AI svět kolem nás? Návštěvníci se ovšem kromě umělé inteligence budou moct dozvědět také o potenciálu pro zlepšení života skrze digitální technologie obecně a o jejich dopadu na zvyšování efektivity práce. Spolu s tím vyvstane také příležitost pro sdílení dobré praxe v uvedených oblastech, a to zejména s ohledem na kybernetickou bezpečnost provozovaní moderních technologií. Registrace na konferenci je otevřená a bezplatná.

Nejnovější bloková šifra zvyšuje ochranu dat ve vyrovnávací paměti

Mezinárodní tým vědců z Tohoku University dosáhl významného pokroku v oblasti kybernetické bezpečnosti, a to vytvořením vysoce účinné šifry pro randomizaci rychlé vyrovnávací paměti (tzv. cache neboli přechodné ukládaní nejčastěji používaných dat pro urychlení jejich načítání). Nová šifra se zaměřuje na hrozbu útoků postranními kanály* na vyrovnávací paměti, skrze které je možné nepozorovaně získávat citlivé informace z počítačových systémů, včetně hesel a ověřovacích klíčů. Obrana proti takovému typu útoku je násobně obtížnější než při klasické kryptoanalýze (získávání obsahu z šifrovaných informací – opak kryptografie). Právě randomizace vyrovnávací paměti se ukazuje jako slibné protiopatření a konkrétní takovou architekturou je nově vyvinutý SCARF (bloková šifra s nízkou latencí pro bezpečnou randomizaci vyrovnávací paměti). Tato specializovaná bloková šifra s délkou bloku 10 bitů dokáže oproti stávajícím architekturám SCARF dokončit proces randomizace s poloviční latencí oproti stávajícím kryptografickým technikám. SCARF je navržen tak, aby byl kompatibilní s různými zařízeními pro automatizované zpracování dat, což zajišťuje širokou použitelnost a potenciál významně zvýšit bezpečnost výpočetní techniky a chránit citlivé údaje všech uživatelů.

**Side channel útoky, neboli útoky postranními kanály, se na rozdíl od klasické kryptoanalýzy nesnaží najít teoretické slabiny v matematické struktuře algoritmu, ale pokouší se o zneužití informací, které unikají přímo z fyzické implementace systému během běhu kryptografického algoritmu.*

Bezdrátová sluchátka budoucnosti umožní jejich ovládání skrze mozkové vlny

Technologickou novinku zaměřenou na zlepšení ovladatelnosti bezdrátových sluchátek připravuje společnost Apple. Nově vyvíjený senzorový systém pro sluchátka AirPods v sobě kombinuje řadu aktivních elektrod, jež jsou schopny měřit elektrické biosignály v mozku uživatele. Logika těchto měření vychází z medicínských poznatků především z oblasti elektroencefalografie (záznam elektrické aktivity mozku), ale také z elektromyografie (sledování elektrické aktivity svalů), elektrokardiogramu (monitorování elektrického potenciálu srdce), pulsu krve a dalších. Použité elektrody se dle svých schopností měřit různé typy biosignalů dělí do několika podskupin, z nichž každá je vhodná pro sledování konkrétního druhu aktivity. Využitelnost různých druhů elektrod je navíc individuálně konfigurovatelná dle fyziologických parametrů uživatele. V praxi by tak díky měřením senzorů chytré zařízení poznalo, např. jakým způsobem uživatel vnímá právě přehrávanou skladbu a buďto by ji přímo přeskočilo nebo třeba upravilo playlist tak, aby aktuální náladě uživatele více vyhovoval. V širším náhledu na využitelnost této technologie ji bude možné propojit se stávajícími funkcemi chytrých zařízení pro sledování zdraví. Hudbou vzdálené budoucnosti je potom sledování biomarkerů pro včasnou detekci závažných neurologických onemocnění, jako je například Alzheimerova choroba. Kromě bezdrátových sluchátek by v budoucnu mohl být obdobný senzorový systém aplikovaný také např. v chytrých brýlích, hodinkách či jiných zařízeních, která umožňují skrytí měřicích elektrod.

Připomínáme!

Již 26. září končí lhůta pro podání návrhů projektů v rámci právě vypsaných výzev v programu Digitální Evropa Kyberbezpečnost, z nichž některé se zaměřují například na koordinaci mezi civilní a obrannou sférou v oblasti kybernetické bezpečnosti, implementaci EU legislativy a národních strategií v této oblasti, standardizaci, posilování digitálních schopností a další.

NASA a IBM se spojili za účelem zlepšení sledování klimatických změn s pomocí AI

Výzkumu v oblasti změny klimatu má pomoct open-source model umělé inteligence vytvořený americkým Národním úřadem pro letectvo a vesmír (NASA) a technologickým gigantem IBM. Model má pomoct především při sledování a předpovídání povodní a požárů. Model byl vytvořen na základě dat nashromážděných z harmonizovaných družic NASA Landsat a Sentinel-2, což představuje další významný krok pro oblast aplikace umělé inteligence do praxe. Cílem nasazení této technologie je sledování změn ve využití půdy (transformace přírodních ploch na hospodářské), monitorování přírodních katastrof a předpovídání výnosů plodin. Očekává se také, že bude mít zásadní význam pro pochopení důsledků klimatických změn jak na transformaci Země, tak na ekonomiku jednotlivých regionů a lidskou společnost jako takovou. IBM odhaduje, že model dokáže analyzovat geoprostorová data až čtyřikrát rychleji než současné nejmodernější modely hlubokého učení, jenž pracují pouze s polovičním rozsahem dat. IBM plánuje později v tomto roce představit také komerční verzi modelu jako součást své platformy pro umělou inteligenci a platformy Watson (mnohoúčelová umělá inteligence vyvíjená společností). Tento geoprostorový model umělé inteligence je volně přístupný skrze portál Hugging Face, veřejné úložiště pro modely strojového učení.

Vědeli jste, ŽE...

čeští vědci vyvinuli speciální papír pro balení elektroniky? Tento druh papíru je schopen efektivně odvádět elektřinu a tím eliminovat účinky statické elektřiny, jež mohou elektronická zařízení trvale poškodit. Balicí papír je možno vyrábět ve třech variantách: první vodivý papír zamezuje vzniku statického náboje, druhý odvádí náboj od baleného zboží a třetí představuje substrát pro flexibilní elektroniku. Modifikovaná celulóza, která balicí papír tvoří, je navíc recyklovatelným produktem z obnovitelných zdrojů, čímž na rozdíl od běžných plastových obalů snižuje zátěž pro životní prostředí.

Inovace technologie tenkovrstvých baterií eliminuje nedostatky nejrozšířenější konstrukce současnosti

Lithium-iontové baterie představují jednou z nejdůležitějších současných technologií v širokém spektru každodenního využití a jsou součásti takřka všech běžně používaných elektronických zařízení. I přesto mají ovšem celou řadu nedostatků. Kromě toho, že při každém nabití a vybití zkracují svoji kapacitu a nabíjí se relativně pomalu, jsou také značně náchylné k vzplanutí. Výzkumníci ze Švýcarské federální laboratoře pro vědu a technologii materiálů proto vyvinuli nové tenkovrstvé baterie, které jsou bezpečnější, mají delší životnost a lze je opakovatelně nabít již během pouhé minuty. Výroba těchto baterií je navíc mnohem šetrnější k životnímu prostředí. Technologie tzv. tenkovrstvé polovodičové baterie, tedy pokrývaní nosného komponentu neboli substrátu tenkou vrstvou komponentů bateriových článků (elektrolytu, katody a anody), přitom není úplnou novinkou, jelikož je známá již od 80. let 20. století. Přelomové je ovšem skládání vrstev článků silných jen několik mikrometrů na sebe, a tím zvyšovaní objemu energie, kterou jsou baterie schopny uschovat. Tenkovrstvé články se vyrábějí pomocí vakuového povlakování (tj. rozprašovaní elektrolytické vrstvy ve vakuové komoře v přesně kontrolované míře na cílový substrát). Jelikož tenkovrstvé baterie nevyužívají kapalný, ale pevný elektrolyt, při jejich poškození nedochází k úniku výparů, které se můžou vznítit, nebo dokonce explodovat. Aktuálně největším nedostatkem této konstrukce je velikost baterií, jelikož dvě vrstvy článků nanesené na ploše o maximální velikosti 1 x 3 milimetry, které jsou výzkumníci zatím schopni nanést, není pro praktické využití postačující.

Tipy na zajimavé akce

Říjen

2.-6. - Týden kybernetické bezpečnosti v Haagu

3.-4. - CyberTech Europe 2023 v Římě

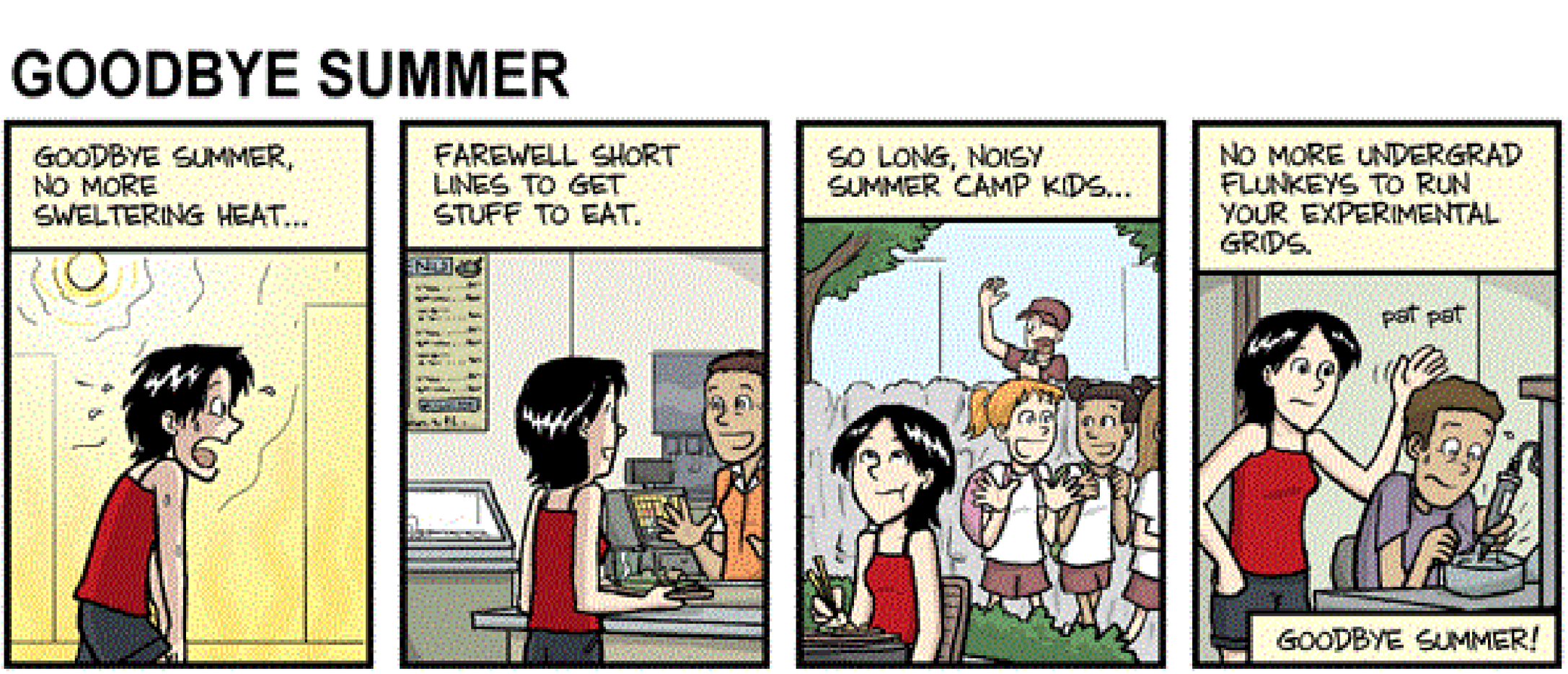
3.-5. - Critical Infrastructure Protection and Resilience Europe v Praze

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

08/2023



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