CYBER SECURITY ACADEMY
11.—15. ZÁŘÍ 2023 / ČSOB
RADLICKÁ 333/150, PRAHA 5

Prague Security Studies Institute

hlavní partneři

OBECNÉ INFORMACE

Dress code: Business Casual

Lokace: Sídlo ČSOB (Radlická 333/150, Praha 5). Sraz bude vždy v 8:30. Vzhledem k tomu, že na průchod budovou budeme muset vždy mít doprovod, je nutné, abychom na místě byli včas. **Místo setkání je u sochy Kaštan, přímo před výstupem z metra Radlická!**

Formát CSA 2023: Všechny naše přednášky se řídí pravidly **Chatham House**, což znamená, že účastníci mohou využít získané informace, ale neprozradí, od koho tyto informace získali.

Stravování: K dispozici na místě bude káva, čaj a drobné občerstvení. PSSI v rámci CSA 2023 nezajišťuje obědy. Je možné využít restauraci La Fresca, která sídlí přímo v prostorech ČSOB – je zde preferována platba kartou pro zajištění rychlejšího odbavení. Prostory nabízí také možnost ohřevu vlastního jídla, případně objednání dovozu dle vlastní preference.

Upozornění: V průběhu konání akademie budou pořizovány fotky a videa pro propagační účely.

PONDĚLÍ, 11. ZÁŘÍ, 2023

08:30 **Sraz u sochy Kaštan, přímo před výstupem z metra Radlická**

09:15–10:45 **Úvod do kybernetické bezpečnosti**
Veronika Kolek Netolická
Národní úřad pro kybernetickou a informační bezpečnost

Tato úvodní přednáška se zaměří na představení Národního úřadu pro kybernetickou a informační bezpečnost, jeho činnost a aktivity. Vysvětleny budou nejdůležitější pojmy a terminologie spojená s kybernetickou bezpečností, a také základní principy a koncepty kyberbezpečnosti.

Veronika Kolek Netolická na NÚKIB pracuje jako vedoucí oddělení národních strategií a politik, na které nastoupila před více jak šesti lety. Od října tohoto roku se zhostí nové pozice cyber attachée pro Indo-Pacifik na ambasádě ČR v australské Canbeře. Magisterský titul má z oboru Bezpečnostní a strategická studia, Fakulta sociální studií na Masarykové univerzitě, na níž nyní pokračuje v doktorském studiu se zaměřením na podrobnou analýzu kybernetických bezpečnostních hrozeb a jejich rizik. Na stejné škole vystudovala i bakalářský program Politologie – Bezpečnostní a strategická studia. V roce 2018 se zúčastnila dlouhodobého výzkumného pobytu ve Vietnamu na Ho Či Minově technické univerzitě. Kromě toho je absolventkou Programu studia kybernetické bezpečnosti v Centru George C. Marshalla v Německu či UN-Singapore Fellowship. V roce 2021 absolvovala roční mezinárodní program The Young Leaders Program na National Graduate Institute for Policy Studies (GRIPS) v Japonsku, kde získala magisterský titul v oboru veřejné politiky, po jehož absolvování se vrátila zpátky na NÚKIB.

11:00–12:30 **Kybernetická bezpečnost v avionice**
Tereza Toufarová
Velitelství kybernetických sil a informačních operací

Přednáška přináší stručné shrnutí principu vývoje avioniky, seznámení s principy certifikačních norem a požadavků na bezpečnost. Zaměřuje se na specifika cyber security tak, jak je uplatňována v leteckém vývoji a vyžadována certifikačními autoritami. V průběhu přednášky se dozvíte mimo jiné stručnou historii integrace principu kybernetické bezpečnosti do procesů používaných při certifikaci letadel a také o aktuálních novinkách z vývoje.

Tereza Toufarová vystudovala na FEKT VUT obor komunikační technologie a HF JAMU obor dirigování sboru. Za sebou má devítiletou praxi ve vývoji avioniky v americké společnosti Honeywell, kde působila jako systémový inženýr, certifikační inženýr a projektový lídr. Na poslední jmenované pozici řídila integrační a aplikační úroveň vývoje, a to zejména letadel kategorie business jet. V průběhu této praxe byla přítomna nástupu integrace cyber security principu do avioniky. Od loňského roku působí v Armádě České republiky jako voják z povolání a své zkušenosti uplatňuje na Velitelství kybernetických sil a informačních operací.

12:30–13:45 **Obědová pauza**

14:00–15:30 **Vojenské implikace kyberprostoru**
Jakub Fučík
Velitelství kybernetických sil a informačních operací

Rozvoj komunikačních a informačních technologií vede nejen k novým možnostem a příležitostem, jak zlepšit blahobyt společnosti, ale také k závislosti na těchto technologiích. Ze strategického hlediska představuje kyberprostor novou dimenzi, kde státní a nestátní aktéři navzájem soutěží v prosazování svých vlastních zájmů – často na úkor jiných. Škodlivé kybernetické aktivity z tohoto pohledu představují nový druh hrozeb (a nástrojů), které mají negativní dopad nejen v této doméně, ale též v ostatních (fyzických) dimenzích. Kybernetická obrana a kybernetická bezpečnost se tak stávají nedílnou součástí veřejných a soukromých zájmů. Přednáška se zaměří na vojenské implikace kyberprostoru a jejich vlivu na charakter současných ozbrojených konfliktů.

Kpt. Mgr. et Mgr. Jakub Fučík, Ph.D. vystudoval mezinárodní vztahy a současně právo. Působil jako akademický pracovník Centra bezpečnostních a vojenskostrategických studií Univerzity obrany a jako tajemník odborného časopisu Obrana a strategie. Od roku 2021 je příslušníkem AČR na pozici vedoucí starší důstojník odboru plánování štábu Velitelství kybernetických sil a informačních operací. Absolvoval zahraniční kurz „International Law of Military Operations" na Defense Institute of International Legal Studies a výzkumnou stáž na NATO Defence College. Působí v rámci SAS/NATO STO panelů a workshopů a zastupuje Českou republiku v EDA Captech „Information".

16:00–17:00 **Kybernetická (ne)bezpečnost z pohledu klienta banky – Co na internetu hrozí a jak se efektivně bránit**
Petr Vosála
ČSOB

Tato přednáška se zaměří na kybernetickou bezpečnost z pohledu klienta banky. Vysvětlí různé hrozby a rizika, kterým jsou klienti vystaveni nejen při používání internetového bankovnictví a online platebních systémů. Budou diskutovány konkrétní hrozby a sociální inženýrství, a ukázáno, jak se těmto rizikům efektivně bránit. Přednáška poskytne praktické tipy a rady, jak chránit své bankovní účty a citlivé finanční údaje před kybernetickými útoky.

Petr Vosála vystudoval vysokou školu v oboru Elektronické obchodování, Informační technologie a management. V ČSOB pracuje od roku 1998, aktuálně na pozici Výkonný manažer útvaru Digital channels – Provoz a vývoj. Kybernetickou bezpečností se zabývá od roku 2010.

ÚTERÝ, 12. ZÁŘÍ, 2023

09:00–10:30 **Hacking jako řemeslo**
Martin Leskovjan
Binary Confidence

V přednášce zazní základní fakta o tématu penetračního testování neboli etického hackingu. Posluchači se seznámí s etickými a právními principy a metodologiemi, které se v této oblasti používají, dále s nejčastějšími typy testů, testovacími nástroji a postupy a také s nečekanými úskalími, které může tato činnost přinést. Samostatná část přednášky se bude věnovat nejúčinnějšímu typu kybernetického útoku, a tím je útok na wetware (člověka). V rámci něj si představíme základní postupy a principy testování metodami sociálního inženýrství.

Martin Leskovjan je certifikovaný auditor managementu informační bezpečnosti a působí jako bezpečnostní konzultant při teamu Binary Confidence, dříve český team společnosti Citadelo zaměřené na penetrační testování a audity. Spoluzaložil také organizaci Paralelní polis zabývající se novými formami správy společenských vztahů. Profesní deformace ho vede k hledání slabin ve všech systémech, proto se začal zabývat také kryptoměnami, ochranou soukromí na internetu a antifragilními strukturami jako jsou např. anonymní kryptomarkety.

10:45–12:15 **Atribuce kybernetických útoků**
Jana Marešová

Atribuce kybernetických útoků je od roku 2020 jedním z hlavních témat bezpečnostní komunity v České republice. Svým rozsahem se jedná o velmi komplexní proces, který často zahrnuje všechny relevantní aspekty, tj. nejen technická data, ale i zpravodajské, právní, zahraničně politické a ekonomické vstupy. Veřejná atribuce kybernetických útoků, tj. oznámení, kdo je považován za odpovědné, často není zcela snadná a státy nemusí být vždy ochotné takové oznámení učinit a to i z důvodu rozdílných technických a zpravodajských informací, které mají k dispozici. Co si však pod pojmem kybernetická atribuce představit, čím je pro český stát tak důležitá a jaké jsou její hlavní metody a možná úskalí, bude předmětem této přednášky.

Mgr. Jana Marešová, MBA je analytička kybernetické bezpečnosti. Je absolventkou magisterského studia mezinárodních vztahů na Metropolitní univerzitě v Praze a bezpečnostně právního studia na Policejní akademii. V roce 2022 dokončila postgraduální studium v oboru Management a kybernetická bezpečnost na CEVRO Institutu, kde se zaměřila v rámci své závěrečné práce na téma Atribuce kybernetických útoků.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Kybernetická bezpečnost v mezinárodních vztazích**
Richard Kadlčák
Ministerstvo zahraničních věcí ČR

Přednáška na téma „Kybernetická bezpečnost v mezinárodních vztazích“ zkoumá vliv kybernetických hrozeb na mezinárodní diplomacii a politiku. Bude se zabývat různými typy kybernetických útoků a jejich dopady na suverenitu států. Dále se zaměří na mezinárodní reakce a normy v oblasti kybernetické bezpečnosti, včetně konkrétních příkladů a budoucích trendů v této oblasti.

Richard Kadlčák v současnosti zastává roli zvláštního zmocněnce pro kybernetický prostor a ředitele Odboru kybernetické bezpečnosti na Ministerstvu zahraničních věcí ČR. Jeho role zahrnuje koordinaci vnitrostátní a mezinárodní spolupráce v oblasti kybernetické bezpečnosti a reprezentování ČR na mezinárodních jednáních s tématikou dotýkající se kybernetického prostoru. Na Ministerstvu zahraničních věcí ČR působí jako diplomat více než 20 let a v minulosti vykonával mimo jiné funkci mimořádného a zplnomocněného velvyslance ČR v Estonsku.

15:45–17:15 **Čínské aktivity v kyberprostoru**
Monika Kutějová
Specialistka kybernetické bezpečnosti

Čínská lidová republika využívá kyberprostor k dosažení svých geopolitických cílů. V přednášce budou představeny motivace i strategie čínské kybernetické špionáže, včetně nástrojů, taktik a postupů (tzv. TTPs), skrze které chce ČLR těchto cílů dosáhnout. Pro ucelený obrázek se podíváme na strukturu a vnitřní fungování čínských zpravodajských a bezpečnostních služeb a zaměříme se na aktuální témata a hrozby s nimi spojené.

Monika Kutějová působí v oblasti kybernetické bezpečnosti čtvrtým rokem. Zkušenosti v oboru získala na mezinárodním Letišti Václava Havla v Praze jako SOC analytička a předtím v NÚKIB, kde se věnovala regionální problematice kybernetických hrozeb pocházejících z Čínské lidové republiky. Vystudovala Mezinárodní teritoriální studia na brněnské Mendelově univerzitě a Evropskou ekonomickou integraci na pražské VŠE.

STŘEDA, 13. ZÁŘÍ, 2023

9:00–10:30 **Čínské (kyber)aktivity proti Taiwanu**
Michal Thim
Ericsson

Tato přednáška se soustředí na kybernetický rozměr čínských aktivit namířených proti Taiwanu. Stručně zmíněn bude historický kontext konfliktu mezi Čínou a Taiwanem, a poté se hlouběji zaměříme na současný kybernetický boj, jako jeden z bezpečnostních faktorů v této situaci. Přednáška analyzuje čínské kybernetické útoky a operace, které směřují k infiltraci taiwanských systémů, odcizení citlivých informací a narušení kritické infrastruktury. Přednáška rovněž diskutuje o budoucím vývoji této kybernetické konfrontace a jejím významu pro globální bezpečnostní paradigma v kontextu zkušeností z kybernetického rozměru ruské agrese proti Ukrajině.

Michal Thim je analytik kybernetických hrozeb a specialista na oblast východní Asie. V minulosti pracoval v Národním úřadu pro kybernetickou a informační bezpečnost České republiky, kde měl na starosti monitorování a analýzu státem sponzorovaných kybernetických hrozeb pocházejících z regionu východní Asie. Je absolventem magisterského studia politologie na Fakultě sociálních věd Univerzity Karlovy v Praze. V letech 2007–2010 pracoval Michal jako ředitel Výzkumného centra Asociace pro mezinárodní otázky. V letech 2010–2012 studoval asijsko-pacifická studia na National Chengchi University (NCCU) v Tchaj-peji. V roce 2014 se na NCCU vrátil jako hostující vědecký pracovník Taiwan Fellowship.

10:45–12:15 **Kybernetické útoky v bankovním sektoru**
Milan Zrcek
ČSOB

Přednáška se zaměří na kybernetické útoky ve všech možných digitálních kanálech, které budou demonstrovány na jednotlivých příkladech. Velká část bude věnována současným taktikám podvodníků jako jsou „phisingové“ stránky nebo různé aplikace. Tyto příklady budou detailně rozebrány tak, aby se jim účastníci mohli v budoucnu bránit a porozuměli metodám těchto podvodníků.

Milan Zrcek je zkušeným expertem v oblasti informační bezpečnosti, kde se zaměřuje na vymýšlení bezpečnostní IT strategie, koordinaci kybernetické bezpečnosti a kontrolních programů, hodnocení rizik a implementaci Data Loss Prevention řešení. V minulosti pracoval jako konzultant a auditor informačních systému v PwC. Vystudoval informační management na VŠE v Praze.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Využití AI ve vlivových operacích**
Jindřich Karásek
Trend Micro

Tato přednáška se zaměřuje na využití umělé inteligence (AI) ve vlivových operacích. Bude zkoumáno, jak AI může být použita k optimalizaci a zlepšení strategií vlivových operací, které se často provádějí ve sféře politiky, ekonomiky a veřejného mínění. Přednáška se zaměří na konkrétní příklady a techniky, které umožňují lepší porozumění a ovlivnění cílového publika.

Jindřich Karásek je vedoucím výzkumníkem kybernetických hrozeb ve společnosti Trend Micro. Jeho výzkumná práce se zaměřuje na oblasti kognitivní války, kybernetické špionáže a kybernetických hrozeb či zpravodajství. Je také vědcem zabývajícím se bezpečnostními daty, známým jako tzv. 4n6strider.

15:30–17:00 **Kybernetická bezpečnost – konkrétní zkušenosti a překážky**
David Pikálek
KPMG

Jak KPMG Česká republika přistupuje ke kybernetické bezpečnosti? David Pikálek vysvětlí, proč je důležité klást důraz na rovnováhu mezi různými typy bezpečnostních opatření, jako je organizace, technologie a bezpečnostní povědomí. Na základě svých zkušeností upozorní na problémy ve společnostech, které snižují efektivitu bezpečnostních opatření a celkovou úroveň kybernetické bezpečnosti.

David Pikálek má za sebou více než 30 let zkušeností v oboru informačních technologií, přes 15 let v oboru bankovnictví a široký rozsah zkušeností s řízením projektů, řízením informační bezpečnosti, přípravou strategií informační bezpečnosti i rozvojem IS/IT, a to nejen v bankách. Podílel se na budování první internetové banky v ČR a na modernizaci bezpečnosti on-line bankovnictví České spořitelny a dalších bank. David se převážně zaměřuje na řízení informační bezpečnosti, ISMS, řízení rizik IT, správu kybernetické bezpečnosti, ochranu dat a fyzické zabezpečení. Rovněž se orientuje v rámcích kontroly zabezpečení architektury a životního cyklu bezpečnostního rozvoje.

ČTVRTEK, 14. ZÁŘÍ, 2023

09:00–10:30 **Proměny kybernetického konfliktu (ENG)**
Andrew Dwyer
Royal Holloway, University of London

Tato přednáška se zaměří na současný vývoj útočných kybernetických operací. Ačkoliv mnoho státních aktérů formalizovalo své aktivity v národních „kybernetických silách" – například ve Velké Británii – prostředí kybernetických konfliktů je stále méně jasnější. Toto prostředí není výhradní doménou států, ale jeho součástí jsou i soukromé společnosti, zločinecké skupiny a další aktéři. Přednáška blíže popíše případy WannaCry (2017), NotPetya (2017), Sunburst (2020 – také známý jako hack SolarWinds) a Microsoft Exchange (2021), na kterých demonstruje vývoj a proměny současného kybernetického prostoru, a to včetně přesahu do aktuálně probíhající války na Ukrajině.

Andrew Dwyer je přednášejícím v oboru informační bezpečnosti na Royal Holloway, University of London. Ve svém nedávném výzkumu se zabýval rozhodovacími procesy, úlohou státních kybernetických operací a schopností a také „kritickými" přístupy ke studiu kybernetické bezpečnosti. Je vedoucím britské pracovní skupiny pro ofenzivní kybernetiku a dříve působil na výzkumných pozicích na Bristolské univerzitě a Durhamské univerzitě poté, co v roce 2019 dokončil doktorát (Ph.D.) na Oxfordské univerzitě.

10:45–12:15 **Digitální a kybernetické rozměry ozbrojených konfliktů (ENG)**
Alexi Drew
International Committee of the Red Cross

Alexi Drew je poradkyní pro technologickou politiku Mezinárodního výboru Červeného kříže v londýnské delegaci. Také působila jakovedoucí analytička v oblasti obrany, bezpečnosti a infrastruktury ve společnosti RAND Europe, výzkumná analytička v The Policy Institute (King's College London) a spolupracovnice Centra pro vědecká a bezpečnostní studia (CSSS) na King's a Globální sítě pro extremismus a technologie (GNET). Ve své práci se zaměřuje na nové technologie, mezinárodní normy, a jejich dopad na mezinárodní vztahy a geopolitiku. Alexi je poradkyní britské pobočky Women in International Security (WIIS), členkou poradního sboru organizace Minorities in Peace and Security (MiPS) a mentorkou organizace Girl Security. V současné době je politickou referentkou zvláštní skupiny Asociace politických studií (PSA) pro technologickou a internetovou politiku a také členkou Královské společnosti umění a členkou Chartered Institute for IT nebo British Computing Society. Jejím specifickým zájmem jsou informační operace, správa platforem, kontrola zbrojení, algoritmická moc, kybernetická bezpečnost a umělá inteligence. Za její profesní dráhu může příliš mnoho Star Treku v době dospívání.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Cvičení kybernetické bezpečnosti**
Irena Adler Pavelková
Národní úřad pro kybernetickou a informační bezpečnost

Přednáška poskytne vhled do oblasti cvičení kybernetické bezpečnosti. Pokryje celý cyklus cvičení od definice jeho cílů, přes tvorbu scénáře, až po jeho exekuci a vyhodnocení. Účastníci budou seznámeni jak s různými typy cvičení a přístupy k nim obecně, tak s konkrétními případy a výstupy. V rámci přednášky se rovněž dozví, jaké jsou hlavní přínosy cvičení a s jakými výzvami se setkávají jejich organizátoři jak v rámci NÚKIB, tak i mimo něj.

Irena Adler Pavelková je absolventkou Právnické fakulty Masarykovy univerzity a Zahradnické fakulty Mendelovy univerzity. Již při studiu pracovala jako projektový manager v resortu zemědělství a věnovala se řízení projektů zaměřených na rozvoj a posílení institucí veřejné správy, které byly po vstupu ČR do EU zodpovědné za zavádění legislativy EU do národního právního systému. Posléze působila jako právní metodik v resortu zeměměřictví a katastru. Od roku 2021 se na oddělení cvičení NÚKIB věnuje přípravě a realizaci národních i mezinárodních cvičení kybernetické bezpečnosti (NATO, EU). Od začátku roku 2023 toto oddělení vede.

15:30–17:00 **Kybernetická bezpečnost v mezinárodních vztazích, zpravodajství a technologie**
Daniel Bagge
Strider Technologies

Přednáška se zaměří na důležitost kybernetické bezpečnosti v oblasti mezinárodních vztahů, vedení války a také jako nezbytnou součást technologické dominance. Daniel Bagge zprostředkuje jednotlivé aspekty na příkladech a zkušenostech z Washingtonu, kde v letech 2018–2021 působil jako kyberatašé a pohovoří o svých zkušenostech z pozice stratéga Vojenského zpravodajství, kterou zastával v roce 2022–2023.

Daniel Bagge aktuálně působí jako Senior Intelligence Specialist v Strider Technologies. V minulosti založil a vedl Odbor kybernetických bezpečnostních politik Národního centra kybernetické bezpečnosti na Národním bezpečnostním úřadu), a posléze byl jeho ředitelem i na NÚKIBu. V letech 2018–2021 působil jako kyberatašé ČR ve Washingtonu. V minulých letech také pracoval jako stratég Vojenského zpravodajství pro oblast nastupujících a převratných technologií, kde se zabýval dopadem moderních technologií na obranu a bezpečnost. Studoval v Praze, Izraeli a Německu. Přednášel na Joint Advanced Warfighting School v americkém Norfolku i na civilních univerzitách v USA a Evropě. Je autorem knihy o informačních operacích v kyberprostoru.

18:30–20:30 **Recepce na Britské ambasádě v Praze, 180/14 Thunovská, Praha 1**

PÁTEK, 15. ZÁŘÍ, 2023

09:00–12:15 **Strategické cvičení kybernetické bezpečnosti (ENG)**
Tauno Tamm & Markus Münzer
RiskSight

Během tohoto cvičení budou účastníci řešit scénář postupně eskalující mezinárodní krize v kybernetickém prostoru. Mohou si tak v praxi vyzkoušet své teoretické znalosti, které získali v předchozích dnech Cyber Security Academy. Cvičením bude jako hlavní moderátor provázet Markus Münzer a jako spolumoderátor Tauno Tamm. Pro tento typ cvičení nejsou potřeba žádné technické znalosti.

12:15–13:00 **Závěrečné vyhodnocení, vyplnění online dotazníku, udělení certifikátů, oficiální ukončení**

13:00–15:00 **Číše vína na terase a setkání s ČSOB experty, komentovaná prohlídka budovy**
(tato část programu je již dobrovolná)