CYBER SECURITY ACADEMY

4—8/10/2021 / KPMG
POBŘEŽNÍ 648, PRAHA 1

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Prague Security Studies Institute

CYBER SECURITY ACADEMY

Prague Security Studies Institute

ve spolupráci:

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

hlavní partneři

NATO OTAN

US embassy

British Embassy Prague

KPMG

CYBEXER TECHNOLOGIES

partneři

Norwegian Embassy

Check Point SOFTWARE TECHNOLOGIES LTD

OBECNÉ INFORMACE

Dress code: Business Casual

Lokace: Sídlo KPMG (Pobřežní 648, Praha 1). Sraz bude vždy v 8:45 před vstupem do budovy. Vzhledem k tomu, že na průchod budovou budeme muset vždy mít doprovod, je nutné, abychom na místě byli vždy včas.

Formát CSA 2021: Všechny naše přednášky se řídí pravidly **Chatham House**, což znamená: „Pokud se setkání řídí pravidly Chatham House, tak účastníci mohou využít získané informace, ale neprozradí, od koho tyto informace získali."

Obědy: PSSI nezajišťuje obědy v rámci CSA 2021. Níže najdete vybrané restaurace v okolí

Lidová jídelna Těšnov (Těšnov 1635)
Veggie Garden (Pobřežní 394)
Pho Ha Noi (Křižíkova 275/7)
Gui Lin (Za poříčskou bránou 382)
Original Curry & Tandoor restaurant (Sokolovská 46)
Las Adelitas (Petrská 23)
Alforno (Petrské náměstí 4)

PONDĚLÍ, 4. ŘÍJNA, 2021

08:30 **Sraz před budovou KPMG (Pobřežní 648, Praha 1)**

09:00–09:15 **Přivítání + Úvodní slovo**
Zástupci PSSI a britské ambasády

09:15–10:30 **Ruská federace a její působení v kyberprostoru**
Michael Myklín, NÚKIB

Skupiny spjaté s Ruskou federací a jejími institucemi patří mezi nejaktivnější a nejschopnější aktéry v kyberprostoru a jejich aktivity se přímo dotýkají i České republiky a její národní bezpečnosti. V přednášce zazní detaily o teoretickém ukotvení ruských kybernetických ofenzivních kapacit v oficiálních dokumentech i pracích vojenských teoretiků, současné trendy ruských APT skupin a pozornost bude věnována i propojení ruského státu a kriminálního podsvětí v kyberprostoru.

Michael Myklín je vedoucím oddělení strategických a informačních analýz v Národním úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Oddělení je zodpovědné za analytické a informační materiály o významných kybernetických útocích a trendech pro vedení úřadu, čelní představitele českého státu a další domácí i zahraniční instituce. Michael získal magisterské vzdělání na Masarykově univerzitě v oboru bezpečnostních a strategických studií.

Reading list:
Russian Operational Art, New Type Warfare, and Reflexive Control

Understanding Russia's Cyber Strategy

10:45–12:15 **Budoucí výzvy kybernetické bezpečnosti**
Luboš Přikryl, NÚKIB

Přednáška se zaměří na nové technologie, které mají potenciál výrazně proměnit charakter kybernetické bezpečnosti, jako například sítě 5G, internet věcí (IoT) nebo umělá inteligence (AI).

Luboš Přikryl je analytikem NÚKIB se zaměřením na nejnovější technologie. Vystudoval Bezpečnostní a Strategická studia na Fakultě sociálních studií Masarykovy univerzity.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Čínské aktivity v kyberprostoru**
Monika Kutějová, NÚKIB

Jedna z nejaktivnějších zemí v kyberprostoru, Čínská lidová republika, využívá internet k dosažení svých národně-bezpečnostních, ekonomických a strategických geopolitických cílů. V přednášce budou představeny nástroje, taktiky a postupy (tzv. TTPs), skrze které chce Čína těchto cílů dosáhnout, a strategie i motivace čínské kybernetické špionáže a dalších typů útoků včetně konkrétních příkladů. Pro kontext bude přednáška doplněna vysvětlením struktury a vnitřního fungování čínských zpravodajských a bezpečnostních služeb a jejich vzájemné spolupráce.

Monika Kutějová se v začátku své kariéry v NÚKIB věnovala kybernetickým hrozbám proti nadnárodním sektorům (např. proti energetickému průmyslu, zdravotnictví či vysokému školství). V posledních měsících se začala zaměřovat na regionální problematiku kybernetických hrozeb pocházejících především z Číny. Před nástupem na NÚKIB pracovala jako projektová koordinátorka v neziskovém sektoru. Vystudovala Mezinárodní teritoriální studia na brněnské Mendelově univerzitě a Evropskou ekonomickou integraci na pražské VŠE.

15:30–17:00 **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.

Tereza Toufarová vystudovala 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 posledně jmenované pozici řídila integrační a aplikační úroveň vývoje zejména business jet letadel. V průběhu této praxe byla přítomna nástupu integrace cyber security principu do avioniky. Od letošního roku nastoupila do Armády České republiky jako voják z povolání a své zkušenosti uplatňuje na Velitelství kybernetických sil a informačních operací.

ÚTERÝ, 5. ŘÍJNA, 2021

09:00–10:30 **Kybernetická bezpečnost v mezinárodních vztazích**
Daniel Bagge

Přednáška se zaměří na důležitost kybernetické bezpečnosti v oblasti mezinárodních vztahů a při vedení války, a vysvětlí, proč jde o nezbytnou součást technologické dominance. Daniel Bagge zprostředkuje jednotlivé aspekty na příkladech a zkušenostech z Washingtonu, kde působil jako kyberatašé v letech 2018–2021.

Daniel P. Bagge zastával funkci kyberatašé České republiky ve Washingtonu D.C., kde byl odpovědný za bilaterální spolupráci v oblasti kybernetické bezpečnosti a to vůči USA a Kanadě. Byl vyslán Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) České republiky. Pozici ve Washingtonu předcházela funkce ředitele odboru kybernetických bezpečnostních politik nejprve v Národním bezpečnostním úřadu, a posléze v NÚKIBu. V těchto pozicích byl odpovědný za tvorbu a implementaci systému ochrany kritické informační infrastruktury ČR, koncepci informační a analytické činnosti v oblasti hrozeb v kyberprostoru, národních a mezinárodních cvičení a Národní strategie kybernetické bezpečnosti 2015-2020, jejímž je spoluautorem. Je jedním z architektů Pražské 5G bezpečnostní konference a tzv. Pražských návrhů.

Reading list:
Technology Adoption: Are we too late to the party?

10:45–12:15 **Bezpečnost v moderním světě**
Miloslav Lujka, Check Point Software Technologies

Miloslav pracuje dvanáctým rokem pro Check Point Software Technologies, světového lídra v oblasti kybernetické bezpečnosti. Má za sebou přes 20 let zkušeností v mezinárodních firmách, klíčové projekty vedl například pro Cisco Systems a Vodafone. Strategické řízení si osvojil během studia MSc. a MBA na The Nottingham Trent University.

Je zakladatelem neziskového vzdělávacího projektu www.digitalnipevnost.cz, kde se věnuje mj. bezpečnosti běžných lidí. Můžete ho pravidelně vídat v televizi, kde komentuje aktuální bezpečnostní dění. V roce 2019 se zařadil mezi TEDx speakery s přednáškou: „Vaše soukromí neexistuje…“

12:30–13:30 **Obědová pauza**

13:45–15:15 **Vlivové operace s použitím kybernetických nástrojů**
Alžběta Bajerová, Asociace pro mezinárodní otázky

Alžběta Bajerová je analytička Výzkumného centra AMO. Zaměřuje se na informační operace, kybernetickou bezpečnost a vlivové působení cizích mocí. V současnosti pracuje jako analytička v Bruselu, kde v roce 2019 absolvovala stáž v NATO HQ. Předtím působila jako novinářka a i nadále přispívá na serveru Voxpot. Mezi její pracovní zkušenosti patří například stáž v expertním centru NATO CCD v Estonsku, na Národním úřadě pro kybernetickou a informační bezpečnost (NÚKIB), nebo na českém velvyslanectví v Číně. Je spoluzakladatelkou iniciativy Zvol Si Info, která bojuje vzděláním proti dezinformacím. Alžběta získala magisterský titul z Bezpečnostních a strategických studií na Masarykově univerzitě, kde vystudovala také bakalářský program Mezinárodní vztahy. Při studiu absolvovala semestr na National Taiwan University na Tchaj-wanu.

15:30–17:00 **Norský pohled na kybernetickou bezpečnost**
Ministerstvo zahraničí, Norsko

STŘEDA, 6. ŘÍJNA, 2021

09:00–09:30 **Důležitost kybernetické obrany v mezinárodním kontextu**
Karel Řehka, NÚKIB

Karel Řehka se dlouhodobě za zabývá tématem hybridní války a vojenských informačních operací. Vystudoval vojenské gymnázium v Opavě a Vysokou vojenskou školu pozemního vojska ve Vyškově, absolvoval roční důstojnický kurz ve Velké Británii a absolvoval prestižní kurz rangers v USA. Zúčastnil se vojenských misí na Balkáně a v Afghánistánu, v Armádě ČR působil u 601. skupiny speciálních sil generála Moravce, které od roku 2010 velel. Od listopadu 2014 stál v čele Ředitelství speciálních sil ministerstva obrany až do roku 2020, kdy byl jmenován ředitelem Národního úřadu pro kybernetickou a informační bezpečnost.

09:30–10:30 **Hacking jako řemeslo**
Martin Leskovjan, Citadelo

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 člen boardu společnosti Citadelo zaměřené na penetrační testování a audity, která působí v ČR, na Slovensku a ve Švýcarsku. Vystudoval Právnickou fakultu UK a následně se zaměřil na oblasti práva související s bezpečností informací a autorskými právy na internetu ve spojení s praxí etických hackerů, které nejprve obchodně zastupoval a následně v roce 2017 založil český team. 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 **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.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Identita. Identifikace. Autentizace. Podepisování.**
Jiří Bulan, Společník & CEO RaulWalter CZ

Dříve papír, dnes počítače. Jak ale identitě v době internetu věřit? Jak věřit tomu, že jste ten, za koho se vydáváte? Jiří Bulan vám vysvětlí, na jakém principu funguje digitální podpis. Jak funguje cestovní pas nebo čipový občanský průkaz. Ukáže vám příklad Estonska, kde s digitální identitou opravdu každodenně pracují. Dokonce díky ní mohou volit v demokratických volbách on-line.

Jiří Bulan je společníkem a ředitelem ve společnosti RaulWalter CZ, která se specializuje na „identity solutions" pro veřejný a soukromý sektor. Jiří se zaměřuje zejména na oblast digitální identity, kryptografie a chytrých karet. Spolupracoval na technologických řešení pro biometrické pasy a další formy e-ID ve Velké Británii, Irsku, Švédsku, Libanonu a Jordánsku. Před příchodem do privátní sféry Jiří pracoval pro různé státní a vládní úřady.

Reading list:
Regulation on on electronic identification and trust services for electronic transactions in the internal market

Nařízení o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie

Do dvou let bude mít občanský průkaz v sobě nový čip. Stejně jako cestovní pas

Volit korespondenčně nebo po internetu jde. Vnitro ale nechce

15:30–17:00 **Proměny kybernetického konfliktu**
Andrew Dwyer, Durham University

Přednáška se zaměří na současný vývoj útočných kybernetických operací, které ukazují stále chaotičtější terén konfliktu. Ačkoliv mnoho státních aktérů formalizovalo své aktivity v národních „kybernetických silách" – například ve Velké Británii – terén kybernetických konfliktů je stále méně přehledný. Tento terén 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.

Andrew Dwyer je výzkumný pracovník na Durham University a zároveň se podílí na výzkumu v Centre for Technology and Global Affairs Oxfordské univerzity. Pracuje také jako zástupce editora v odborném žurnálu Big Data & Society a je součástí redakce časopisu Digital Geography and Society. V minulosti pracoval jako výzkumný pracovník v Cyber Security Group na University of Bristol.

18:00–20:00 **Recepce na Britské ambasádě v Praze**
180/14 Thunovská, Praha 1

ČTVRTEK, 7. ŘÍJNA, 2021

09:00–10:30 **Kybernetické útoky v bankovním sektoru**
Milan Zrcek, ČSOB

Přednáška se zaměří na kybernetické útoky ve všech možných digitálních kanálech. Velká část bude věnována současným taktikám podvodníků jako jsou „phishingové" stránky nebo různé aplikace. Tyto konkrétní 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.

Reading list:
Internet Organised Crime Threat Assessment (IOCTA) 2020

10:45–12:15 **Mezinárodní jednání o stabilizaci kybernetického prostoru**
Richard Kadlčák, Ministerstvo zahraničních věcí

Záměrem přednášky je poskytnout vhled do aktuálních mezinárodních jednání usilujících o stabilizaci kybernetického prostoru. Ty v současnosti probíhají na mnoha různých fórech jako jsou OSN, OBSE, EU nebo NATO. Zaměří se na pět klíčových tematických okruhů: 1) aplikace mezinárodního práva v kyberprostoru, 2) principy, pravidla a normy zodpovědného chování států v kyberprostoru, 3) opatření k posílení důvěry, 4) budování kapacit a 5) hrozby nových technologií.

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.

Reading list:
Open-ended working group on developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

12:30–13:30 **Obědová pauza**

13:45–15:15 **Vojenské implikace kyber prostoru**

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“

Reading list:
Technologický vývoj 2020

15:30–17:00 **Cvičení kybernetické bezpečnosti**
Alena Leciánová, NÚKIB

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.

Alena Leciánová se přípravou jak národních, tak mezinárodních cvičení kybernetické bezpečnosti zabývá od roku 2016, kdy se stala zaměstnancem Národního centra kybernetické bezpečnosti pod Národním bezpečnostním úřadem. Po oddělení a vzniku Národního úřadu pro kybernetickou a informační bezpečnost ve své činnosti dále pokračuje, od roku 2020 již jako vedoucí oddělení, jehož hlavní náplní je nejen příprava cvičení od počátku do konce, ale i spolupráce s ostatními celky organizace, či přednášková činnost v oblasti. Kromě toho je součástí Core Planning Team aliančního cvičení Cyber Coalition, kde v týmu zvaném Scenario Development přispívá k tvorbě zastřešujícího scénáře cvičení. Přednášející je absolventkou Fakulty sociálních studií Masarykovy univerzity v oboru Bezpečnostní a strategická studia.

Reading list:
Národní úřad pro kybernetickou a informační bezpečnost – Publikace (nukib.cz)

Exercises (ccdcoe.org)

PÁTEK, 8. ŘÍJNA, 2021

09:00–12:30 **Strategické cvičení kybernetické bezpečnosti**
Lucie Kadlecová a Kari Rannikko, CybExer Technologies

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 Kari Rannikko a jako spolumoderátorka Lucie Kadlecová. Pro tento typ cvičení nejsou potřeba žádné technické znalosti.

Kari Rannikko je plukovníkem ve výslužbě, který v CybExer Technologies zastává pozici Senior Strategy Advisor se zaměřením na hybridní hrozby a strategické rozhodování. V roce 2019 působil jako manažer v kanceláři předsedy vlády Finska během finského předsednictví EU. Byl zde mimo jiné zodpovědný za projekt Scenario Based Policy Discussions on Countering Hybrid Threats, který byl určen pro ministry vnitra EU, Policy Directors ministerstev obrany a zahraničí zemí EU. Má více jak 30 let zkušeností z obranného sektoru ve finských službách. Působil v mezinárodních misích OSN, EU i NATO. Jeho akademický zájem se soustředí na integrovaný přístup k řešení krizí, který realizuje jako vedoucí instruktor na Finnish Defence College.

Lucie Kadlecová pracuje jako senior associate (strategie a threat intelligence) a současně CybExer Technologies zastupuje na českém trhu. Dokončuje také doktorské studium na Univerzitě Karlově v Praze. Dříve působila jako výzkumný pracovník na Massachusetts Institute of Technology (MIT) v Cambridge, USA v rámci Fulbrightova stipendia. Pracovala také v Národním centru kybernetické bezpečnosti ČR a byla stážistkou v sekci kybernetické obrany v sídle NATO a v kabinetu komisaře pro rozšíření a evropskou politiku sousedství v Evropské komisi. Je autorkou a spoluautorkou několika publikací a příležitostně přednáší na vysoké škole nebo na konferencích souvisejících s kybernetickou bezpečností. Magisterský titul získala na katedře válečných studií, King's College London.

12:30–13:30 **Závěrečné vyhodnocení (+vyplnění online dotazníku)**

13:30 **Udělení certifikátů, ukončení**