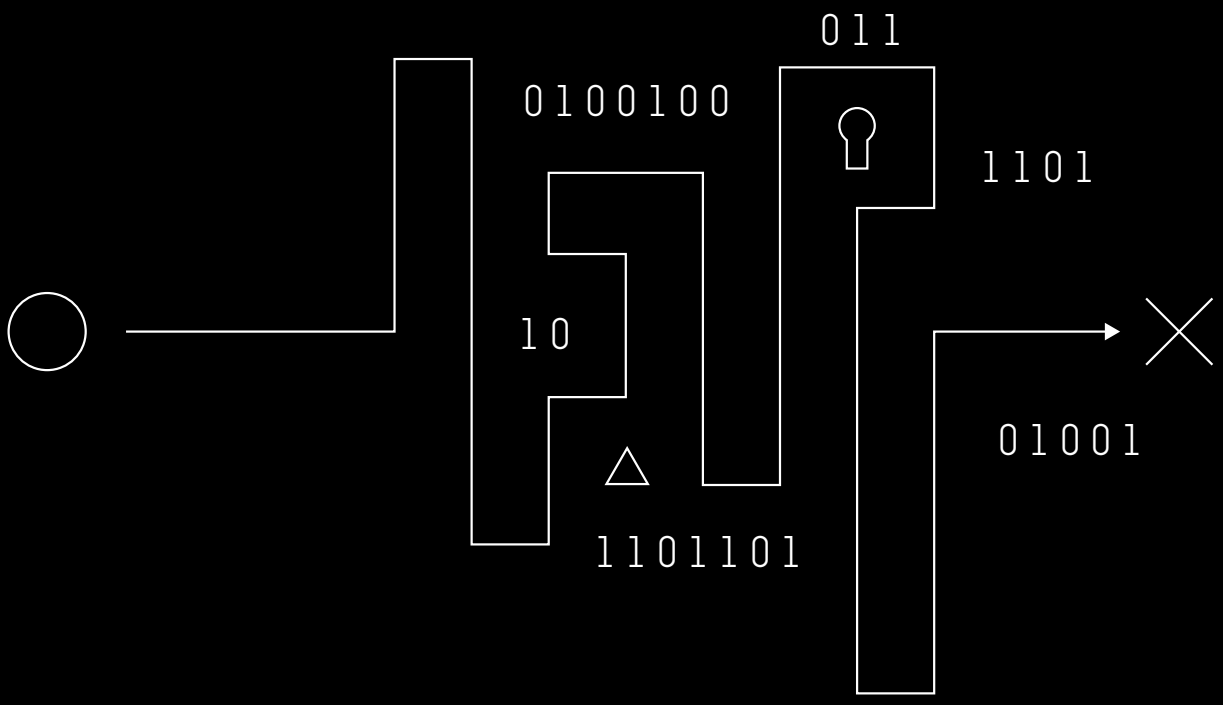
MUNI FI

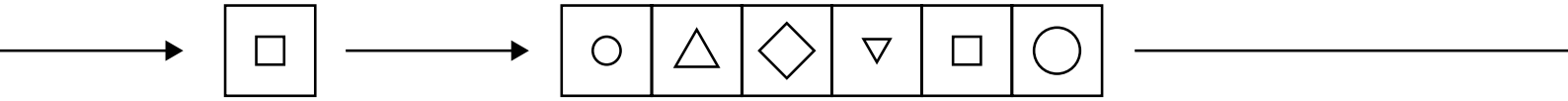
CERIT
CYQUAL




# Akční plán k Národnímu kvalifikačnímu rámci v kyberbezpečnosti[1]

Tato metodika byla schválena jako výsledek NmetS pověřeným ústředním správním orgánem – Národním úřadem pro kybernetickou a informační bezpečnost

1 Tento Akční plán vznikl v rámci projektu Národní kvalifikační rámec v kyberbezpečnosti. Program bezpečnostního výzkumu ČR 2015-2022 (VI20192022161). Masarykova univerzita. Investor: Ministerstvo vnitra ČR. Aplikační garant Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Jedná se o výsledek č. 3 v rámci tohoto projektu, který představuje metodiku NmetS, která byla schválena ústředním správním orgánem pro kybernetickou bezpečnost, kterým je Národní úřad pro kybernetickou a informační bezpečnost. Souhrnné informace o projektu jsou mj. dostupné na https://www.cyqual.cz/.



# 1. Úvod

Soudobý vývoj hrozeb v kyberbezpečnosti vyžaduje adekvátní reakci ze strany veřejného, soukromého a nevládního sektoru. Důležité je proto i dlouhodobé zajištění dostatečného počtu vzdělaných a kvalitních odborníků na různých pracovních pozicích v kyberbezpečnosti, jejichž znalosti a dovednosti budou na vysoké úrovni. Tuto vysokou úroveň je třeba garantovat a zajistit tím vhodné standardy pro pracovní pozice v oblasti kyberbezpečnosti. Obdobná úroveň znalostí a schopností pracovníků je žádoucí z hlediska zaměstnavatelů, kterým zajistí požadovanou míru kyberbezpečnosti i expertů na kyberbezpečnost samotných, kterým zvýší jejich cenu na pracovním trhu. Jedná se přitom o trend, u nějž se do budoucna očekává stále rostoucí tendence.

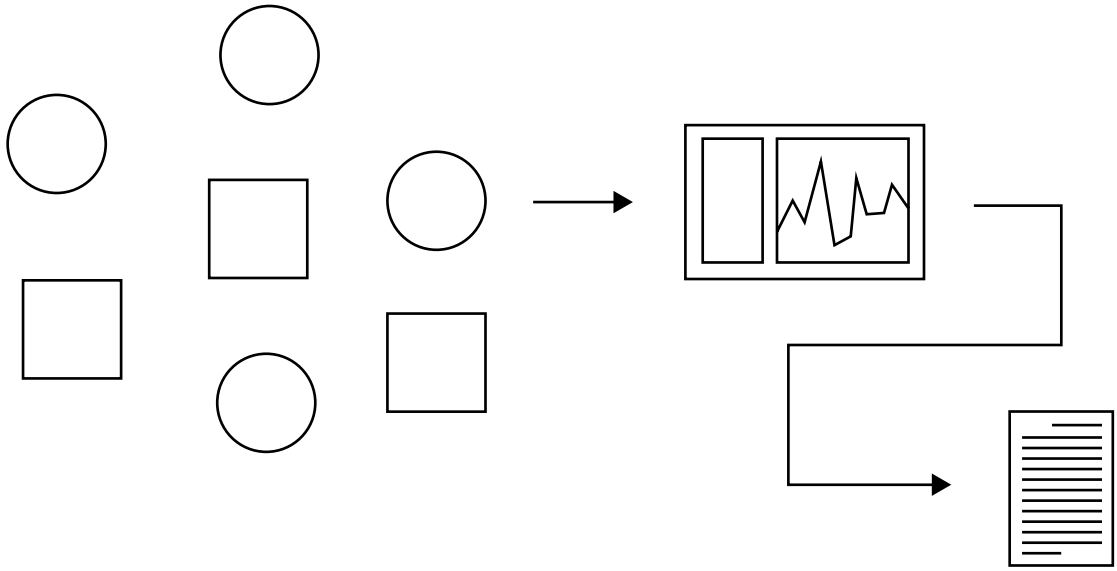
Z výše uvedených důvodů je v rámci stejnojmenného projektu vytvořen Národní kvalifikační rámec v kyberbezpečnosti a pro uvedení jeho podstatných aspektů do praxe je zpracován tento Akční plán k Národnímu kvalifikačnímu rámci v kyberbezpečnosti (dále Akční Plán). Jedná se o dokument určený ke koncepčnímu využití.[2] Respektuje základní východiska Metodiky přípravy veřejných strategií,[3] nicméně svým pojetím zapadá dominantně do rámce výše zmíněného projektu a potřeb NÚKIB coby aplikačního garanta.

Akční plán začíná přehledem dostupných vzdělávacích kapacit a dostupné pracovní síly v ČR v evropském kontextu, včetně základního vymezení dosavadní úrovně kompetencí. Následně jsou identifikovány problémy se zajištěním dostatečného množství kvalitních odborníků v oblasti kyberbezpečnosti v ČR a zajištění dostatečného počtu a kvality odborníků KB. Následně jsou navrženy nástroje a postupy k posílení dostupnosti kvalifikované pracovní síly v kontextu Národního kvalifikačního rámce v kyberbezpečnosti, a to na základě vlastního výzkumu v ČR (včetně rozhovorů a dotazování se expertů ze soukromé sféry, z bezpečnostních složek a z akademického prostředí), zahraničních zkušeností a na základě využití evropských dokumentů, norem a praktických poznatků. Dále je vymezena role NÚKIB při využití Akčního plánu a nakonec jsou identifikováni jeho specifičtí uživatelé a navrženy osvětové a vzdělávací aktivity k realizaci tohoto plánu.

---

2 Jedná se přitom o šířeji pojatý dokument než pouze o „souhrn doporučených praktik a postupů schválených kompetenčně příslušným orgánem veřejné správy (NmetS)“ ve smyslu Metodiky 17+. Srov. Úřad vlády České repu bliky. Odbor rady pro výzkum, vývoj a inovace (2018): Metodika hodnocení výzkumných organizací a hodnocení programů účelové podpory výzkumu, vývoje a inovací Schváleno Usnesením vlády ČR ze dne 8. února 2017 č. 107. Praha: Úřad vlády ČR.

3 Ministerstvo pro místní rozvoj (2018): Metodika přípravy veřejných strategií.Dostupné z *https://www.mmr.cz/getmedia/70d00bf5-cec5-4ddd-9309-a3f54c216ea8/Metodika-pripravy-verejnych-strategii-plna-verze_1.pdf.aspx?ext=.pdf*



# 2. Analýza dostupné pracovní síly a dostupného vzdělávání v oblasti kyberbezpečnosti v ČR

ICT sektor, do kterého spadá i problematika kyberbezpečnosti, je z hlediska potřeb národní bezpečnosti i dalších oblastí státní i nestátní sféry, mimořádně důležitý. V současné době je pracovní trh na daném poli vysoce atraktivní a vyznačuje se výraznou převahou poptávaných pracovníků nad počtem reálně zaangažovaných expertů. Zajištění dostatečného počtu kvalifikovaných expertů je proto zásadním bezpečnostním zájmem ČR. Požadavky na kybernetickou bezpečnost vyplývají i z členství ČR v EU a NATO. Výrazný nárůst potřeby nových expertů je spojen s implementací směrnice EU tzv. „NIS 2".[4]

Podle materiálu Českého statistického úřadu (ČSÚ) pracovalo v roce 2020 v ICT sektoru celkem téměř 219,8 tisíc osob[5], což znamenalo 4% zaměstnanecké populace[6]. Počty oproti předchozí letům narůstaly a v době publikace tohoto akčního plánu lze předpokládat jejich další zvýšení o desítky tisíc pracovníků. I přes tuto skutečnost chybí na pracovním trhu zhruba 14 000 ICT pracovníků, jak vyplývá z průzkumu soukromých subjektů Coding Bootcam Praha a Techloop[7] (tento počet však podle méně exaktně získaných informací zjištěných v rámci našeho projektu může být až dvojnásobně vyšší). Kromě výrazné platové nerovnosti mezi veřejným a soukromým sektorem komplikuje situaci i fakt, že volná místa na takto specializovaných technických pozicích často ani nejsou evidována Úřadem práce, což dále ztěžuje efektivní

4 Evropský parlament (2020): Directive Of The European Parliament And Of The Council On Measures For A High Common Level Of Cybersecurity Across The Union. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN*

5 Český statistický úřad (2022): ICT odborníci – počty. Praha: ČSÚ, *https://www.czso.cz/csu/czso/ict-odbornici*

6 Český statistický úřad (2021): Lidské zdroje v informačních technologiích. Praha: ČSÚ, *https://www.czso.cz/csu/czso/cri/lidske-zdroje-v-informacnich-technologiich-2020*

7 Strojirenstvi.cz (2021): Proč je tak těžké sehnat IT specialistu? Aktuální data z trhu práce, dostupné z *https://www.strojirenstvi.cz/proc-je-tak-tezke-sehnat-it-specialistu-aktualni-data-z-trhu-prace*.

vyvažování nabídky s poptávkou[8]. Zatřiďování a popis v evidenci Úřadů práce již rovněž neodpovídá soudobým potřebám a ve státní sféře není vždy jasná představa o flexibilním přizpůsobení se aktuálním požadavkům v ICT-oblasti[9].

Kyberbezpečnost se prolíná celým ICT sektorem, i když samozřejmě vybrané specializace s kyberbezpečností souvisí silněji či jí týkají výhradně. Podle zjištění tohoto projektu patří v současnosti specialisté na kyberbezpečnost k nejžádanějším profesím na pracovním trhu a obecně je pak důležité, aby odpovídající znalosti a dovednosti z oblasti kybernetické bezpečnosti měli i další pracovníci ICT sektoru (a samozřejmě je třeba vzdělání a osvěta o kyberbezpečnosti v široké veřejnosti, což ale řeší jiné dokumenty než tento akční plán).

O úrovni kvalifikaci expertů v oblasti kyberbezpečnosti souhrnně nelze zjistit zcela přesné a exaktní informace. Je to dáno tím, že neexistovala dostatečně reprezentativní společná platforma pro identifikaci stavu a doposud ani jasná srovnávací kritéria pro úroveň kvalifikace (tento problém je odstraněn zpracováním hlavních výsledků projektu, v jehož rámci je vypracován tento plán). Důležité je i sjednocení názvů profesních specializací v kyberbezpečnosti. Jak vyplývá z poznatků projektu[10], jsou odborníci v ČR dobře vzdělaní a schopní v technických a programátorských znalostech a dovednostech, naopak slabší jsou jejich schopnosti zasazovat incidenty v oblasti kybernetické bezpečnosti do širšího kontextu a problematické jsou často i manažerské schopnosti.

Na nedostatek ICT pracovníků, včetně specialistů na kyberbezpečnost, se snaží reagovat i vzdělávací systém a jednotlivé instituce v ČR. Jak vyplývá z již zmíněné analýzy ČSÚ, dochází v průběhu času k výkyvům v absolutním počtu studentů ICT. V roce 2020 činil počet studentů ICT oborů 21 660 osob, z nějž 72% studovalo bakalářský, 24% magisterský a 4% doktorský studijní program[11]. Dvě třetiny studentů však studovali program Vývoj a analýza softwaru, tedy ne program dominantně zaměřený na kyberbezpečnost (i když samozřejmě kyberbezpečnostní aspekty obsahuje).

Celkově je v České republice podle databáze CyberHEAD (vede ji ENISA) možné studovat dva bakalářské programy specializované na kyberbezpečnost (na FI MU a VUT FIT) a čtyři magisterské (opět na FI a VUT FIT)[12]. Další akreditovaný magisterský studijní obor „Kybernetická bezpečnost" je uváděn na Univerzitě obrany. Databáze nově akreditovaných programů MŠMT uvádí k 28. listopadu 2022 dále uvádí celkem 46 studijních programů/studijních oborů českých vysokých škol v oblasti vzdělávání

---

8 Drmola, J.- Kasl, F. - Loutocký, P. - Mareš, M. - Pitner, T. – Vostoupal, J. (2021): The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework. In The 16th International Conference on Availability, Reliability and Security (ARES 2021), *https://doi.org/10.1145/3465481.3469186*

9 Tyto problémy jsou nicméně de facto podobné i v rámci celé Evropské unie. K tomu více viz jednotlivé výstupy například v rámci evropského projektu H2020 Sparta. Sparta (nedat.): Deliverables: *https://www.sparta.eu/deliverables/*

10 Jedná se o poznatky získané z neformalizovaných expertních rozhovorů a dlouhodobého monitoringu situace.

11 Český statistický úřad (2021), s. 1-3.

12 CyberHEAD (2022): Czech Republic.
*https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=cze* Pro srovnání dostupnosti vzdělávání na mezinárodní úrovni viz Sparta (nedat.): Study programs, https://www.sparta.eu/study-programs/.

„Kybernetika a 279 SP/SO v oblasti vzdělávání „Informatika“[13].

Česká republika samozřejmě využívá i experty v ICT oblasti, včetně kyberbezpečnosti, kteří do ČR přišli po dokončení vzdělání ze zahraničí, ať již ze zemí Evropské unie nebo mimo ni. Celá ICT oblast, a zvláště pak oblast kyberbezpečnosti, je sektorem potenciálně citlivým na úniky informací a na interní zabezpečení. Přitom u všech pracovníků na kritických pozicích, a zejména u pracovníků ze zemí, u nichž existuj zvýšené riziko vystupování proti bezpečnostním zájmům ČR, mohou hrát roli zvýšené požadavky na jejich bezpečnostní prověření, což dále negativně ovlivňuje nabídku na tomto specifickém trhu práce.

Analýzu dostupné pracovní síly a dostupného vzdělávání v oblasti kyberbezpečnosti v ČR lze tedy shrnout do následujících hlavních bodů:

— kyberbezpečnost je jednou z nejvíce poptávaných specializací v rámci ICT sektoru;

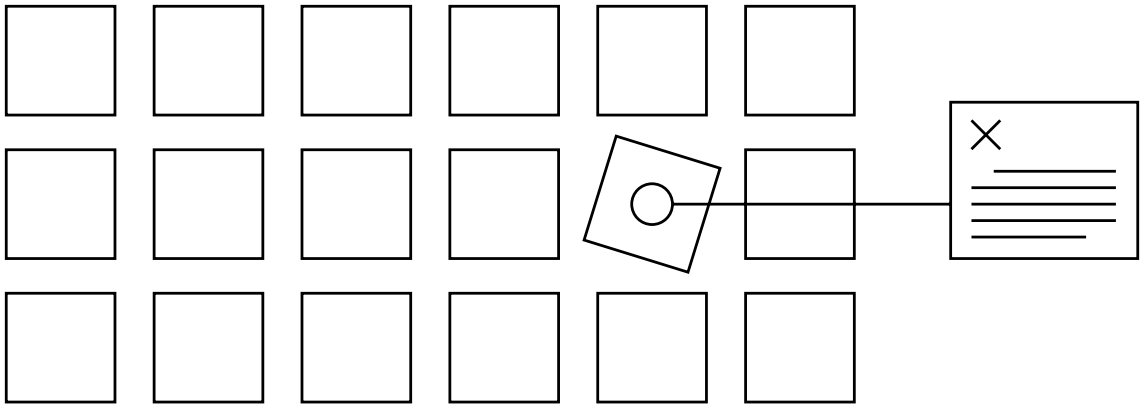
— tento sektor obecně a specifiky v oblasti kyberbezpečnosti poptává velké množství expertů;

— doposud neexistovala jasná kritéria pro kvalifikaci v oblasti kyberbezpečnosti, ani platforma pro srovnání (tento deficit je řešen Národním kvalifikačním rámcem v kyberbezpečnosti, dále Kvalifikační rámec);

— IT-schopnosti a dovednosti v kyberbezpečnosti na technologické úrovni se na základě dílčích poznatků jeví jako celkově dobré, chybí však využití dalších aktivit předpokládaných Kvalifikačním rámcem;

— V ČR existuje několik specializovaných kyberbezpečnostních programů na vysokých školách a jeden pokusně ověřovaný středoškolský RVP zaměřený na kybernetickou bezpečnost (na dvou středních školách), ty však nejsou schopny pokrýt potřeby z hlediska národní bezpečnosti i z hlediska širších zájmů veřejného i soukromého sektoru.

13 Ministerstvo školství, mládeže a tělovýchovy (2022): Registr vysokých škol a uskutečňovaných studijních programů, *https://regvssp.msmt.cz/registrvssp/csplist.aspx*



# 3. Identifikace problémů při zajištění chybějících pracovních kapacit a nepokrytých vzdělávacích kapacit

Hlavním problémy při zajištění kybernetické bezpečnosti vyplývají z celkového nedostatku ICT expertů, včetně specialistů na kyberbezpečnost. Z toho je následně odvozen problém zajištění expertů pro práci na pozicích důležitých z hlediska národní bezpečnosti ve veřejném sektoru za situace, kdy v soukromém sektoru mají výrazně vyšší příjmy. Dalším problémem jsou nejasné nároky na kvalifikaci těchto expertů v kyberbezpečnosti celkově i v jednotlivých kyberbezpečnostních specializacích (např. správců bezpečnostních IT-systémů a rozhraní, specialistů na hodnocení a testování IT-systémů, auditorů kybernetické bezpečnosti atd.) vyplývající mimo jiné i z neexistence jednotné taxonomie povolání v oblasti kybernetické bezpečnosti.

Důležité je přitom zajistit experty jak pro „běžné zajištění“ kyberbezpečnosti, tak i vysoce kvalifikované experty pro speciální problematiky a identifikaci a zvládání nových hrozeb. S potřebou specializovaných expertů na všech úrovních pak souvisí i nutnost dostatečného počtu vědeckých a výzkumných pracovníků v oblasti kyberbezpečnosti, odpovídající podpora výzkumu a jeho propojení s praxí. I když se řada pracovišť snaží o dosažení těchto cílů, z celkového pohledu jsou zde stále deficity. Přetrvává i nepochopení problematiky kyberbezpečnosti ze strany některých státních orgánů a nezajištění dostatečných prostředků pro rozvoj v této oblasti. I když nelze opomíjet problematiku různých hrozeb v kyberprostoru (dezinformace, nenávistné projevy, dětská pornografie apod.), kybernetická bezpečnost je problematikou technologicko-informatického charakteru (byť samozřejmě s přesahem do dalších oblastí) a musí být takto prioritně vnímána a podporována. Žádoucí je multidisciplinární přístup k této problematice (propojení s právem, sociálními vědami, forenzními disciplínami apod.), který se daří v akademickém a částečně i v praktickém prostředí prosazovat, i když i zde existuje potenciál k dalšímu rozvoji.

Jak již bylo uvedeno, v oblasti „skutečné kyberbezpečnosti" chybí pracovníci v soukromé i ve veřejné sféře. Ve vazbě na národní bezpečnost je pak nedostatek patrný v několika oblastech. Jedná se o zajištění expertů pro hlavní správní úřad v dané oblasti – tedy NÚKIB – kde existuje relativně velká fluktuace (způsobená odchodem pracovníků do soukromé sféry, přičemž motivací je často finanční ohodnocení). Konkrétně za rok 2021 to byla fluktuace technických i netechnických pracovníků 12% a do 30. 11. 2022 13% technických pracovníků a 9% netechnických[14]. Přes dočasnou stabilizaci je stále žádoucí personální expertní posilování ve vojenské oblasti, tedy především v jednotkách spadajících pod Velitelství informačních a kybernetických sil a v Národním centru kybernetických operací Vojenského zpravodajství. Experty v kyberbezpečnosti zaměřené na plnění speciálních úkolů v rámci jejich působnosti stabilně potřebují i další dvě zpravodajské služby, tedy Bezpečnostní informační služba a Úřad pro zahraniční styky a informace.

Chybí i policejní specialisté na kybernetickou bezpečnost v rámci Policie ČR, ať již v sekci kybernetické kriminality v rámci Národní centrály proti organizovanému zločinu (NCOZ) nebo na odděleních kybernetické kriminality na jednotlivých krajských ředitelstvích. Specializované potřeby se v oblasti kyberbezpečnosti se objevují i u dalších bezpečnostních sborů, ať se již jedná o Celní správu, Vězeňskou službu[15], Generální inspekci bezpečnostních sborů i Hasičský záchranný sbor[16].

Kyberbezpečnostní experti jsou potřeba do CERT/CSIRT týmů na mnoha úrovních. Obecně roste potřeba manažerů kybernetické bezpečnosti a dalších specializovaných profesí ve vládní, soukromé i neziskové sféře. I v rámci soukromého sektoru lze přitom identifikovat podstatné sektory z hlediska důležitých národních zájmů, především v oblasti energetiky, telekomunikačních technologií, dopravy apod., včetně soukromých bezpečnostních společností.

Několik případů v ČR již ukázalo i na možnost zneužití IT schopností pro různá nežádoucí narušení kyberbezpečnosti, ať se již jednalo o kriminální anebo extremisticky motivovaný hacking či špionážní aktivity ve prospěch soukromých subjektů a cizích mocností. Jako nejvýznamnější příklady lze uvést třeba útoky na české nemocnice[17] nebo na Ministerstvo zahraničních věcí[18]. Je tedy třeba zabránit i tomu, aby experti na kyberbezpečnost zneužívali svoje znalosti a schopnosti pro účely zločinu, extremismu, špionáže a jiných aktivit ve prospěch cizích mocností apod. Nicméně tato problematika nespadá do Akčního plánu s výjimkou potřeby manažerů i řadových pracovníků identifikovat případné nežádoucí insidery a jejich aktivity v prostředí, kde mohou výše uvedenou nežádoucí činnost páchat.

---

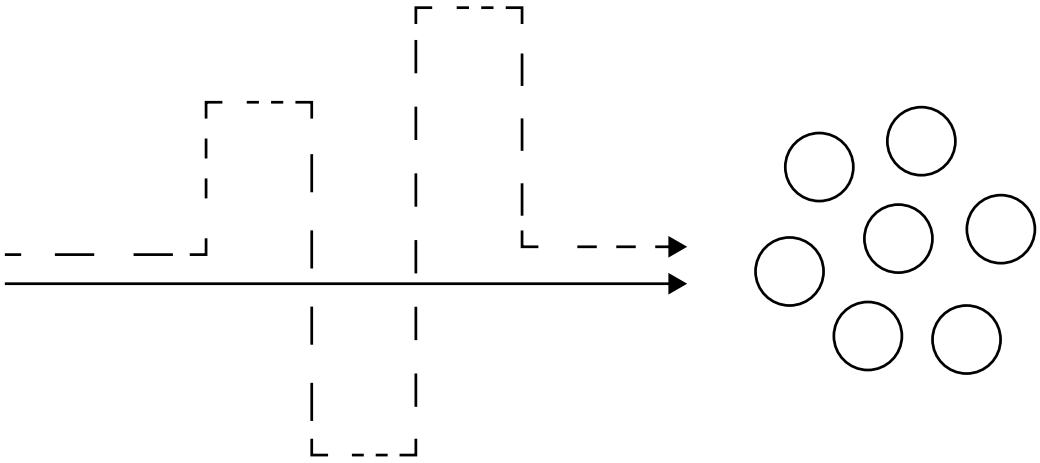
14 Data byla sdělena autorskému týmu projektu od pracovníků NÚKIB dne 24. 11. 2022.

15 Mimo jiné kvůli nelegálnímu průniku digitálních zařízení mezi vězněné osoby i kvůli možným útokům na databáze a elektronické zabezpečení na vězeňská zařízení.

16 U HZS hraje specifickou roli i kybernetická ochrana zařízení sloužících Integrovanému záchrannému systému, za který HZS zodpovídá.

17 Horákova, Veronika (2021): Nemocnice se z kyberútoku otřepává celý rok, hrozbu hackerů bere vážněji. iDnes, 25. 3. 2021. *https://www.idnes.cz/brno/zpravy/kyberutok-fakultni-nemocnice-hrozba-hackeri-nukib.A210324_600537_brno-zpravy_krut*

18 Lipská, Jana (2019): Byl to útok cizí státní moci, uvedl NÚKIB k napadení serverů ministerstva zahraničí. Seznam Zprávy, 13. 8. 2019. *https://www.seznamzpravy.cz/clanek/byl-to-utok-cizi-statni-moci-rekl-nukib-k-napadeni-serveru-ministerstva-zahranici-77215*



# 4. Opatření k posílení dostupnosti kvalifikované pracovní síly potřebné pro zajištění národní kyberbezpečnosti

Opatření k posílení kvalifikované pracovní síly potřebné pro zajištění národní kyberbezpečnosti lze vymezit ve vzájemně se prolínajících rovinách kvantity a kvality, přičemž v kvalitativní rovině je výrazně potřebný a využitelný i Kvalifikační rámec. Je přitom třeba vycházet i z požadavků Evropské unie v dané oblasti, které byly zpracovány především Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA).

Tyto dokumenty obsahují doporučení i srovnání jednotlivých zemí EU v oblasti schopností v kyberbezpečnosti v rámci toho, co je nazýváno „vyšším vzděláváním" („higher education")[19]. ENISA požaduje společný rámec týkající se kyberbezpečnosti v EU, který se bude zabývat rolemi, kompetencemi, schopnostmi a znalostmi. Upozorňuje přitom na existující European Cybersecurity Skills Framework[20]. Je zde mimo jiné kladen důraz na větší diverzifikaci (ve smyslu plurality) oborů vzdělávání, na podporu pod-reprezentovaných skupin lidí v kyberbezpečnosti a na spolupráci členských států a Evropské unie v této oblasti. ENISA provozuje i projekt CyberHEAD, kde jsou obsaženy data o vzdělávacích programech v kyberbezpečnosti v EU a tento projekt je dále rozvíjen a precizován[21]. ČR může najít dílčí inspiraci v zahraničí (mj. v USA[22] či v Itálii[23]), nicméně její vlastní zpracovaný kvalifikační rámec má průkopnický a modelový charakter v globálním rámci.

---

19 Nurse, Jason R. C. – Adamos, Konstantinos – Grammatopoulos, Ahanasios - Di Fabio, Franco Di (2021): Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. Chalandri : European Union Agency for Cybersecurity.

20 Tamtéž. Blíže viz ENISA (nedat): European Cybersecurity Skills Network, *https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework*

21 Tamtéž. Blíže viz ENISA (nedat): CyberHEAD - Cybersecurity Higher Education Database, *https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead*

22 Cyber Seek (nedat): Hack the Gap, *https://www.cyberseek.org/*

23 Osservatorio delle Competenze Digitali (nedat.): Schede delle professioni ICT, *https://competenzedigitali.org/osservatorio-delle-competenze-digitali/schede-delle-professioni-ict/*

Česká republika musí být aktivní na evropské úrovni, primárně však musí hájit svoje zájmy a zajistit vlastní potřeby. ČR hodlá posilovat bezpečnost kybernetického prostoru v EU, což vyplynulo i z programu českého předsednictví v roce 2022[24]. Z hlediska zájmů České republiky je podstatné, aby subjekty ve veřejné, soukromé i neziskové sféře v ČR měly pro potřeby zajištění národní bezpečnosti dostatek kvalifikovaných a spolehlivých odborníků v oblasti kybernetické bezpečnosti. Důležité je i to, aby soukromá sféra neabsorbovala natolik velkou část expertů v kyberbezpečnosti, která by znemožnila adekvátní obsazení pracovních pozic v důležitých složkách státní správy z hlediska národní bezpečnosti. Pro tento účel je třeba zajistit zvláštní platové tarify pro experty na kyberbezpečnost v jasně vymezených státních složkách (ozbrojené síly, bezpečnostní sbory, zpravodajské služby, vybrané ústřední orgány státní správy) a propagovat obecné benefity těchto složek (výsluhy, zvláštní zdravotní péči apod.). Motivací může být i pomoc při vzdělávání a zvláštní certifikace pro pracovní pozice vyplývající z rolí v Kvalifikačním rámci.

Do potřeb vzdělávání a získávání nových pracovníků je tedy třeba integrálně včlenit kritéria z Kvalifikačního rámce a sjednotit i terminologii při vymezení rolí a pracovních pozic na různých úrovních zajištění kyberbezpečnosti. Nad rámec personálního posilování je třeba rozvíjet i vědecké poznání kyberbezpečnosti v různých dimenzích aplikovaného i základního výzkumu[25].

Kvantitativní nárůst expertů v oblasti kyberberbezpečnosti je možné zajistit především posílením různých forem vzdělávání v dané oblasti, dále pak vhodnou migrační politikou, širším zapojením skupin obyvatelstva s malým podílem odborníků v oblasti kybernetické bezpečnosti (ženy a dívky, což je aktuální prioritou NÚKIB), alokací zvýšených finančních zdrojů pro vzdělávání odborníků v oblasti kybernetické bezpečnosti a vzájemnou kombinací všech přístupů, z nichž vzdělání má dominantní charakter.

---

**V zásadě lze tedy:**

— podporovat vysokoškolské programy na vysokých školách v ČR, které budou primárně zaměřené na kyberbezpečnost nebo v nich bude tato problematika výrazným způsobem obsažena (hlavně se musí jednat o programy a obory v rámci fakult informatiky a obdobných, nicméně důležité je zahrnutí kyberbezpečnosti i do programů jiného zaměření, tedy např. práva, managementu, sociálně-vědních bezpečnostních studií apod.). Tyto programy by měly být koncipovány tak, aby odpovídaly rolím a požadavkům Kvalifikačního rámce;

— podporovat zvýšení počtu profesně zaměřených vysokoškolských studijních programů v kybernetické bezpečnosti;

— podporovat rekvalifikační a specializační programy u již vystudovaných expertů v IT-technologiích anebo v jiných programech a oborech příbuzných ke kyberbezpečnosti, se zohledněním rolí vymezených v Kvalifikačním rámci;

---

24 Program českého předsednictví v Radě Evropské unie.
*https://czech-presidency.consilium.europa.eu/media/edkb5w41/program-cz-pres.pdf*
25 Rada vlády pro výzkum, vývoj a inovace (nedat): Základní pojmy výzkumu a vývoje v OECD a EU, *https://www.vyzkum.cz/FrontClanek.aspx?idsekce=932*

— zvýšit limit celkové finanční částky, kterou můžou Úřady práce vynaložit na rekvalifikaci jednoho uchazeče o zaměstnání nebo zájemce o zaměstnání;

— vysílat experty z ČR za prostředky z veřejné podpory anebo s podporou od specializovaných soukromých subjektů na úplné specializované vysokoškolské studium kyberbezpečnosti do zahraničí (prestižní univerzity v oboru), přičemž výběr studijních programů by bral do úvahy i role a požadavky Kvalifikačního rámce (za tímto účelem je možné vytipovat vhodné uchazeče již na středních školách a zřídit pro tento účel zvláštní stipendium);

— vysílat experty z ČR za prostředky z veřejné podpory anebo s podporou od specializovaných soukromých subjektů na specializované kyberbezpečnostní kurzy a stáže na prestižní zahraniční a mezinárodní pracoviště v kyberbezpečnosti, přičemž by tato pracoviště byla vybírána podle potřeby precizovat a doplňovat znalosti a schopnosti u vybraných rolí dle Kvalifikačního rámce;

— podporovat příchod zahraničních expertů na kyberbezpečnost do ČR (již po studiu a případně praxi v zahraničí), kteří by obsadili především pracovní pozice vázané k nedostatkovým rolím z hlediska Kvalifikačního rámce a svoje schopnosti a znalosti by adaptovali pro potřeby těchto rolí;

— podporovat příchod zahraničních studentů na studia kyberbezpečnosti do ČR, a to takových, u kterých existuje jasná perspektiva (stvrzená i odpovídajícími závazky), že po ukončení studia budou pracovat v ČR na pozicích důležitých z hlediska rolí poptávaných dle Kvalifikačního rámce;

— podporovat získávání odborníků ze skupin obyvatelstva s malým zastoupením v oblasti kybernetické bezpečnosti (ženy a dívky apod.);

— podporovat kooperaci, propojování a výměnu informací mezi aktéry, experty a stakeholdery na poli kyberbezpečnosti, a to zejména mezi vzdělávacími institucemi, akademický experty, zástupci soukromé sféry, veřejnou správou i bezpečnostními složkami.

U všech výše uvedených skupin je třeba identifikovat nejen prvoplánové zájemce, ale je třeba aktivní přístup k motivování lidí k takovýmto studiím a rekvalifikacím, včetně podpory doposud pod-reprezentovaných skupin (rovné genderové zastoupení, podpora etnických menšin, zdravotně znevýhodněných osob apod.). O existenci Kvalifikačního rámce je možné informovat i v kampaních a iniciativách zaměřených na širokou veřejnost[26], aby o něm existovalo široké povědomí.

Jak již bylo uvedeno, pro zajištění národní bezpečnosti je třeba vytvořit i odpovídající výzkumnou základnu, která bude umožňovat adekvátní reakci na nové hrozby v kyberbezpečnosti, včetně adaptace na nové technologické podmínky (mj. očekávaný příchod kvantových počítačů). Ve výzkumu je vysoce žádoucí i multidisciplinarita, mimo jiné ve vazbě ICT věd na právní či sociální vědy. Zásadní je i internacionalizace

26 Uvažovat je možné i o stabilní celonárodní vzdělávací platformě, příkladem může být řecká Digitální akademie občana. Jākobsone, Māra (2021): Greece - Citizen's Digital Academy, Digital Skills and Job Platforms, *https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/greece-citizens-digital-academy*

výzkumu. Obecně musí být výzkum v oblasti kyberbezpečnosti jednou z hlavních priorit státní politiky vědy a výzkumu. Ty by měla zohledňovat i potřeby pro zkvalitnění znalostí expertů na jednotlivých pracovních pozicích vymezených Kvalifikačním rámcem.

I v oblasti výzkumu kyberbezpečnosti samotné je třeba zajistit dostatek vědců a lidí, kteří jim vytváří zázemí. Aktivně je třeba podporovat mladé výzkumníky i zkušené experty, kteří po odchodu z praxe odejdou do vědecko-výzkumných zařízení. Proto jsou důležité finanční stimuly i jiné benefity, mimo jiné perspektiva smysluplné práce ve špičkově vybaveném a příznivém pracovním prostředí.

Za tímto účelem je třeba dlouhodobě podporovat stabilní výzkumná centra, která budou na jednu stranu moci dlouhodobě a na základě vlastní iniciativy bádat a na druhu stranu budou permanentně komunikovat se státními i soukromými kyberbezpečnostními složkami o potřebách národní bezpečnosti. Takováto centra mohou vznikat i spoluprací vícero vysokých škol či výzkumných organizací[27], a to i na mezinárodní úrovni.[28] Výzkum kyberbezpečnosti je samozřejmě možné rozvíjet i na méně prestižních pracovištích, excelentní centra a týmy by však měly být preferovány. Nedílnou součástí aplikovaného výzkumu také musí být úzká spolupráce se zainteresovanými státními institucemi a soukromými subjekty.

Důležitá je v daném kontextu i stabilní finanční podpora kyberbezpečnostního výzkumu, přičemž pro jistotu a dlouhodobou schopnost budovat stabilní týmy je důležitá institucionální podpora směřovaná do dané oblasti. I nadále musí hrát výraznou roli střednědobá a krátkodobá projektová činnost z grantů, včetně těch od grantových agentur TAČR a GAČR (kde by měly brát oborové komise do úvahy potřebnou multioborovost výzkumu). Výzkum kyberbezpečnosti je samozřejmě třeba podporovat i v rámci obranného výzkumu (v gesci Ministerstva obrany) a v rámci bezpečnostního výzkumu (v rámci Ministerstva vnitra). Výzkumné aktivity již v současné době umožňují podřazení výzkumu do některého ze stupňů utajení,[29] nicméně ve vysoce závažných problematikách (včetně kyberbezpečnosti) je ohrožením už samotné zveřejnění názvu a základního abstraktu výzkumného projektu. Proto se jeví jako žádoucí mít pro potřeby specifických garantů a uživatelů výsledků výzkumu (zvláště zpravodajské služby a specializované policejní složky a pro specifickou mezinárodní spolupráci) vyčleněné i prostředky na projekty, které (včetně jejich výsledků) nebudou vykazovány běžným způsobem v RIV-RVVI, ale pouze v utajené neveřejné databázi.

---

27 Příkladem je CyberSecurity Hub z.s., na kterém se podílí Masarykova univerzita, Vysoké učení technické a České vysoké učení technické.

28 K dílčí aktivitě v rámci zakládání evropských digitálních hubů více viz: *https://digital-strategy.ec.europa.eu/en/activities/edihs*

29 Ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

**Celkově je tedy možné opatření k posílení dostupnosti kvalifikované pracovní síly potřebné pro zajištění národní kyberbezpečnosti shrnout v následujících bodech:**

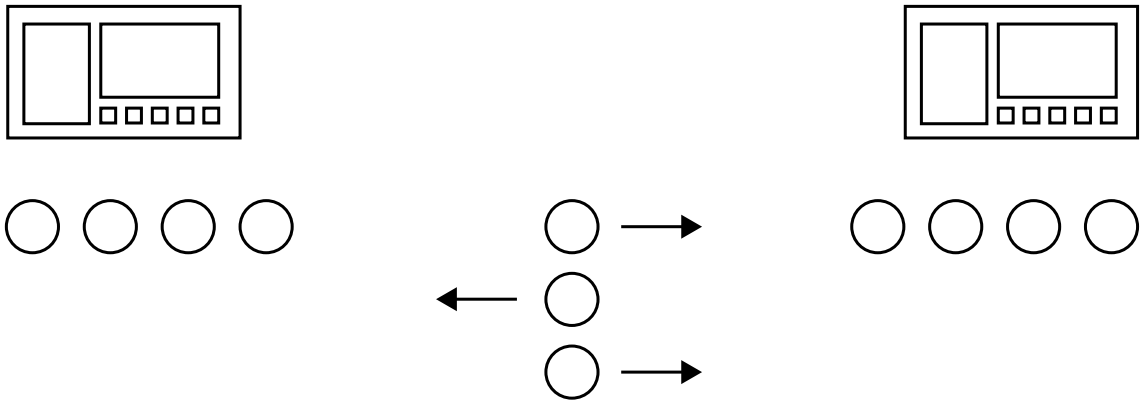
— zajištění speciálních platových podmínek a jiných benefitů pro kyberbezpečnostní experty na pozicích zásadních z hlediska národní bezpečnosti;

— podpora specializovaných kyberbezpečnostních programů na vysokých školách a vyšších odborných školách, rámcového vzdělávacího programu kybernetické bezpečnosti pro střední školy a dalších vzdělávacích aktivit („reskilling and upskilling“);

— vhodná stimulace pracovní migrace do ČR za účelem posílení kyberbezpečnosti;

— zajištění vhodné výzkumné základny v oblasti kyberbezpečnosti.

— Ve všech těchto bodech je třeba zohledňovat evropeizaci (zvláště dokumenty ENISA) a klást důraz na pomoc pracovním rolím vymezeným v Kvalifikačním rámci.



# 5. Vymezení role MU a NÚKIB při využití Akčního plánu

NÚKIB je aplikačním garantem projektu, na jehož základě vzniknul i Kvalifikační rámec. Ten je určen všem subjektům v ICT sektoru, které jsou důležité pro bezpečnostní zájmy ČR na poli kyberbezpečnosti. Národní kvalifikační rámec v kyberbezpečnosti bude udržován ze strany Masarykovy univerzity za podpory NÚKIB (tato podpora bude spočívat v propagačně-informační a poradní roli ve vztahu k Národnímu kvalifikačnímu rámci v kyberbezpečnosti). Konkrétní aktivity správců Národního kvalifikačního rámce v kyberbezpečnosti budou:

---

1/ **V organizačně-správní oblasti:**

- udržovat a aktualizovat Kvalifikační rámec jako veřejně přístupný materiál;
- podporovat znalost a schopnost vysvětlovat důležité atributy Kvalifikačního rámce u příslušných zaměstnanců MU a NÚKIB;
- ve spolupráci NÚKIB a MU organizovat a koordinovat společnou platformu složenou ze zástupců orgánů státní správy relevantních z hlediska národní bezpečnosti aplikující Kvalifikační rámec, vzdělávacích institucí využívajících Kvalifikační rámec a z dalších subjektů soukromé, neziskové i veřejné sféry. Tato platforma bude diskutovat a vyhodnocovat poznatky z aplikace Kvalifikačního rámce a navrhovat aktualizace a zlepšení. Pracovní název je Koordinační platforma k Národnímu kvalifikačnímu rámci v kyberbezpečnosti). Dílčí otázky mohou řešit sekce v rámci platformy, a to a) sekce národní kyberbezpečnosti (SNKB a) sekce pro vzdělávání (SPV), b) sekce specifických uživatelů (SSU). Pro řešení specifických a průřezových otázek mohou být vytvořeny ad hoc skupiny (ADS).

2/ **V oblasti vzdělávání:**

— vést jednání za podpory NÚKIB s Národním akreditačním úřadem o prosazení požadavků z Kvalifikačního rámce do obsahu studijních programů zaměřených na ICT a specifiky na kyberbezpečnost;

— v jednání s vysokými školami aktivně podporovat vznik nových specializovaných oborů ve vazbě na pracovní pozice a role vymezené Kvalifikačním rámcem a nabízet experty do výuky v dané oblasti;

— ve spolupráci s vzdělávacími institucemi ozbrojených sil, bezpečnostních sborů a zpravodajských služeb prosazovat do přípravy specialistů v těchto silách, sborech a službách požadavky z Kvalifikačního rámce v příslušných vzdělávacích programech.

3/ **V oblasti praxe:**

— prosazovat matérii obsaženou v Kvalifikačním rámci do strategických a dalších dokumentů, které vznikají v působnosti NÚKIB (Národní strategie kybernetické bezpečnosti ČR a na ni navazující dokumenty) a do šířeji zaměřených strategických dokumentů, které obsahují problematiku kyberbezpečnosti garantovanou od NÚKIB (Audit národní bezpečnosti, Bezpečnostní strategie ČR);

— aktivně napomáhat naplňování standardů vyžadovaných Kvalifikačním rámcem a kontrolovat je u subjektů důležitých z hlediska národní bezpečnosti (zpravodajské služby, bezpečnostní sbory, správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury a případně vybraní správci a provozovatelé významných informačních systémů a vybraní provozovatelé základní služby nebo správci a provozovatelé informačního systému základní služby apod.);

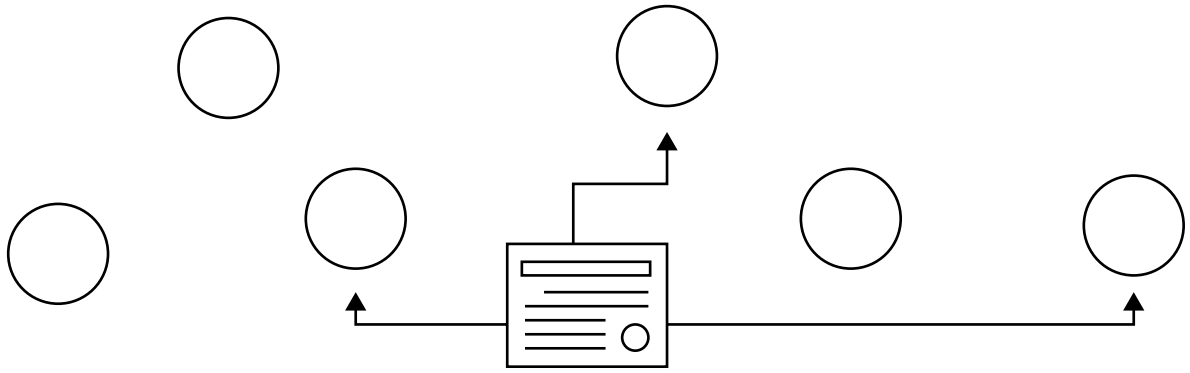
— jednat se zástupci dalších veřejných, soukromých a nevládáních subjektů (včetně profesních asociací v oblasti ICT a specifiky kyberbezpečnosti) o zapracování standardů vyžadovaných Kvalifikačním rámcem do jejich pracovních struktur a aktivity a napomáhat s jejich aplikací a kontrolou.

4/ **V oblasti mezinárodní spolupráce:**

— prosazovat požadavky Kvalifikačního rámce do obdobných mezinárodních dokumentů, zvláště pak na úrovni NATO a EU. V rámci EU je třeba zajistit soulad mezi dokumenty ENISA a Kvalifikačním rámcem;

— podporovat mezinárodní spolupráci v oblasti vzdělávání a výzkumu v oblasti kyberbezpečnosti, včetně zapojení českých subjektů do CyberHEAD;

— zahrnout ve spolupráci s ministerstvem zahraničích věcí matérii z Kvalifikačního rámce do zahraniční rozvojové politiky a nabízet v jejím rámci vybrané získané zkušenosti.



# 6. Identifikace specifických uživatelů Akčního plánu a způsobu práce s nimi, včetně osvětových a vzdělávacích aktivit o plánu

NÚKIB je nejvýznamnější správní institucí z hlediska kybernetické bezpečnosti, která koordinuje ve spolupráci s MU využití Kvalifikačního rámce. Pro úspěšné uvedení do praxe je však třeba, aby se do této aktivity zapojily i další subjekty. Jak již bylo uvedeno, jejich zástupci budou jednat v KP a jednotlivých sekcích. Nejprve je však třeba jednotlivé složky identifikovat a informovat o základních atributech Kvalifikačního rámce a následně poskytnout podrobnější školení.

Pro potřeby komunikace a osvěty týkající se Kvalifikačního rámce budou MU ve spolupráci s NÚKIB zpracovány následující materiály ke Kvalifikačnímu rámci.

---

**Bude se jednat o:**

— základní deskriptivní materiál o Kvalifikačním rámci, který shrne jeho obsah a objasní interaktivní práci s ním. Bude umístěn na internetové platformě;

— manuál pro práci přihlášených uživatelů (s právem změny údajů v databázi platformy);

— vzor zprávy o aplikační praxi Kvalifikačního rámce, který bude sloužit k vyhodnocení aplikace dokumentu a platformy.

Proškolení správců uskuteční Masarykova univerzita, mohou být proškoleni i zástupci NÚKIB MU ve spolupráci s NÚKIB uspořádá i úvodní tiskovou konferenci pro novináře, ke které budou připraveny tiskové zprávy o Kvalifikačním rámci. Další základní informace budou na speciálním workshopu představeny zájemcům z řad politických reprezentantů (ve spolupráci s Parlamentním institutem) a vybraným úředníkům veřejné správy (ve spolupráci s Institutem pro veřejnou správu).

---

**Na představení platformy na tomto workshopu budou pozváni i zástupci následujících institucí (potenciálních uživatelů platformy):**

— Ozbrojené síly ČR (zvláště KySIO);

— Zpravodajské služby ČR (VZ – NCKO, ÚZSI, BIS);

— Vybrané bezpečnostní sbory ČR (zvláště PČR – NCOZ, GIBS a vybrané složky HZS;

— Vybraná ministerstva a ústřední orgány státní správy (MVČR- CTHH, MO, NBÚ, Úřad vlády, v případě ustavení i z úřadu Poradce pro národní bezpečnost[30]);

— Správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury a případně vybraní správci a provozovatelé významných informačních systémů a vybraní provozovatelé základní služby nebo správci a provozovatelé informačního systému základní služby;

— Zástupci vybraných významných soukromých komerčních subjektů aktivních na poli kybernetické bezpečnosti a profesních asociací;

— Zástupci vybraných vzdělávacích a výzkumných institucí.

Proškolení pracovníci MU a případně NÚKIB budou dále rozvíjet a kontrolovat využití Kvalifikačního rámce na svých pracovištích a školit v užívání platformy její uživatele.

Příslušná ministerstva a ústřední orgány státní správy budou požádána, aby do strategických a dalších dokumentů zpracovávaných v jejich působnosti, které se výrazně prolínají s kyberbezpečností, byly zapracovány odkazy a případně další text týkající se Kvalifikačního rámce.

MVČR tak může učinit v případě zpracování komplexní Strategie vnitřní bezpečnosti a dále při aktualizaci Strategie boje proti terorismu, Strategie prevence kriminality a případně dalších dokumentů po konzultaci s NÚKIB.

MO tak může učinit v případě aktualizace Strategie kybernetické obrany, Akčního plánu k Národní strategii pro čelení hybridnímu působení a případně dalších dokumentů po konzultaci s NÚKIB.

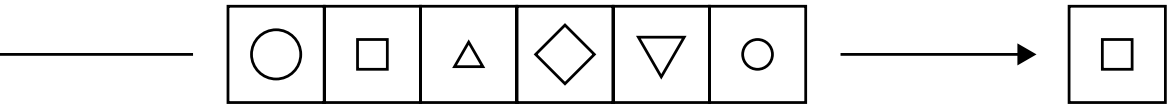
Další ministerstva tak mohou učinit v případě strategických dokumentů, které budou po konzultaci s NÚKIB vyhodnoceny jako relevantní z hlediska národních zájmů v kybernetické bezpečnosti.

MŠMT ve spolupráci s Národním akreditačním úřadem může zajistit aplikaci matérie z Kvalifikačního rámce do požadavků na akreditaci u vysokoškolských programů zaměřených na kyberbezpečnost a jejich kontrolu.

MŠMT ve spolupráci s NÚKIB a dalšími orgány státní správy může aktivně stimulovat vznik specializovaných programů, jejichž absolventi budou odpovídat profilům pracovních pozic a rolí z Kvalifikačního rámce.

---

30 Vláda ČR (2022): Programové prohlášení vlády, *https://www.vlada.cz/cz/programove-prohlaseni-vlady-193547/*



# 7. Závěr

Akční plán je dokumentem, který umožňuje uvést Kvalifikační rámec do praxe v širším kontextu politiky v oblasti kybernetické bezpečnosti. Kolem Kvalifikačního rámce je třeba vytvořit živoucí a aktivně pracující expertní komunitu, která bude prosazovat závěry Kvalifikačního rámce do praxe a odpovídajícím způsobem je vyhodnocovat a aktualizovat. Identifikovaná opatření by měla sloužit k tvorbě a zavádění nových studijních programů, oborů, učebních plánů a inovativních prvků výuky v oblasti kybernetické bezpečnosti. Celkovým cílem je kvalitativní posílení expertů v oblasti kyberbezpečnosti, které je a bude v zájmu národní bezpečnosti ČR, a to i z hlediska jejího zapojení do NATO, EU a dalších mezinárodních organizací a struktur.

MUNI FI

CERIT
CYQUAL

Tento Akční plán vznikl v rámci projektu Národní kvalifikační rámec v kyberbezpečnosti. Program bezpečnostního výzkumu ČR 2015-2022 (VI20192022161). Masarykova univerzita. Investor: Ministerstvo vnitra ČR. Aplikační garant Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Jedná se o výsledek č. 3 v rámci tohoto projektu, který představuje metodiku NmetS, která byla schválena ústředním správním orgánem pro kybernetickou bezpečnost, kterým je Národní úřad pro kybernetickou a informační bezpečnost. Souhrnné informace o projektu jsou mj. dostupné na *cyqual.cz*.