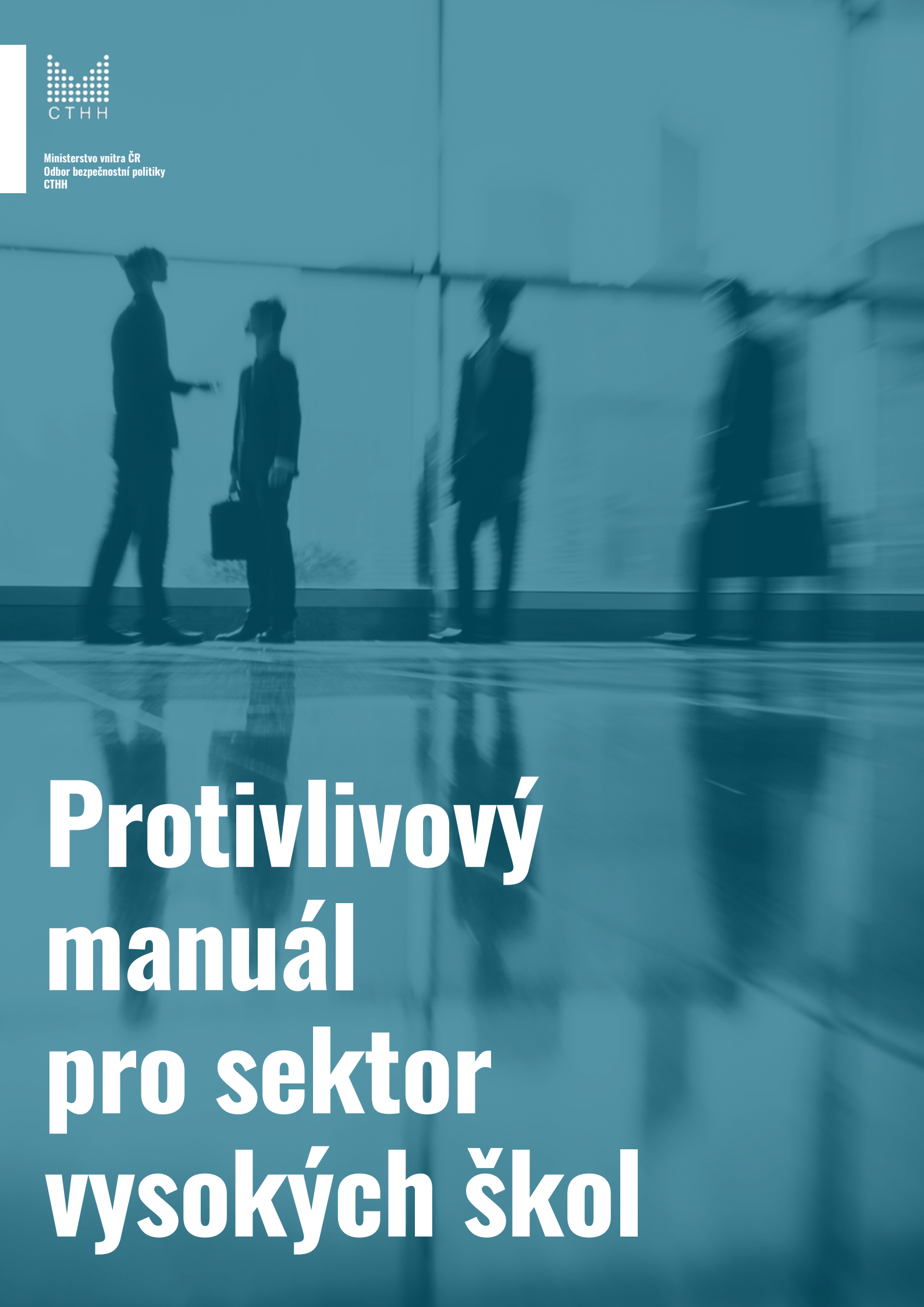


CTHH

Ministerstvo vnitra ČR
Odbor bezpečnostní politiky
CTHH

Protivlivový manuál pro sektor vysokých škol

Obsah

1

Úvod

Vážené akademičky, vážení akademici, vážení neakademičtí pracovníci sektoru vysokého školství, tento dokument vznikl v reakci na žádost Univerzity Karlovy, přičemž inspirací byly zejména události posledních let ve světě, ale i doma, kdy začíná být stále více jasné, že je potřeba začít řešit vlivové působení cizí moci na vysokých školách systematicky.

Nezpochybnitelnou součástí bezpečnostních zájmů ČR jako demokratického státu je mít silné a nezávislé vysoké školství včetně jeho schopnosti realizovat zákonem garantované akademické svobody a akademická práva, ale i zájem na transparentním financování sektoru vysokého školství. Akademické svobody a akademická práva jsou definována zákonem č. 111/1998 Sb., o vysokých školách, přičemž předpokládají vysokou míru osobní odpovědnosti členů akademické obce při jejich využívání, včetně implicitně obsažené povinnosti tato práva a svobody chránit. Vlivové působení cizí moci na sektor vysokých škol narušuje akademická práva a svobody zcela zásadním způsobem a ochrana proti němu by měla kombinovat osobní odpovědnost členů akademické obce s institucionálními opatřeními na úrovni vysokých škol.

Dostává se Vám do ruky dokument, jehož cílem je pomoci Vám **připravit se na to, že se můžete stát předmětem zájmu cizí moci**, a zároveň jak na danou situaci reagovat. Chceme Vám představit základní myšlenku a obecný návod, jak postupovat v rámci prevence, jaké otázky si klást, co by měly pokrývat Vaše interní pravidla, ale i jak nastalé situace řešit a jak ve spolupráci s dalšími subjekty sektoru vysokého školství budovat společné know-how ve snaze o **zvýšení odolnosti vůči vlivovému působení cizí moci**.

Dokument je členěn do dvou hlavních částí, přičemž první se věnuje nastavení systému pro zvýšení odolnosti vůči vlivovému působení cizí moci a druhá je určena **jednotlivcům**, s cílem naznačit jim, jakými způsoby na ně může cizí moc vlivově působit a jak se bránit.

Cílem rozhodně není uvalit na vysoké školy nové zákonné povinnosti, které by měly plnit; naopak realizace protivlivových opatření je ponechávána **na principech dobrovolnosti a osobní a institucionální odpovědnosti**. Plně respektujeme nezávislost vysokých škol a uvědomujeme si, že většina z nich již má nastavena interní bezpečnostní pravidla, nicméně hrozba vlivového působení cizí moci v nich nemusí být vždy uspokojivě pokryta.

Tento dokument představuje především **souhrn rad a doporučení** a zároveň **návod**, jak se vyrovnat se situacemi s přítomností vlivového působení cizí moci, jak reagovat a postupovat. Materiál si neklade za cíl zcela vyčerpávajícím způsobem popsat všechny možnosti, jak může vlivové působení cizí moci na vysoké školy a na akademickou obec probíhat, ale soustředí se na popis základních technik a postupů. V praxi se také ukazuje, že **ne vždy je možné předcházet všem hrozbám v jejich šíři a komplexnosti**, i když je dobré **být si jich vědom a připravit se na ně**.

Uvědomujeme si, že základem reputace a úspěchu našeho vysokého školství je jeho otevřenost a nezávislost. Podporujeme otevřenost různým myšlenkám, nápadům a trendům, studentům z různých socioekonomických skupin, ale i studentům ze zahraničí a nezávislost na politickém systému země a na nežádoucím vlivu ze strany cizí moci.

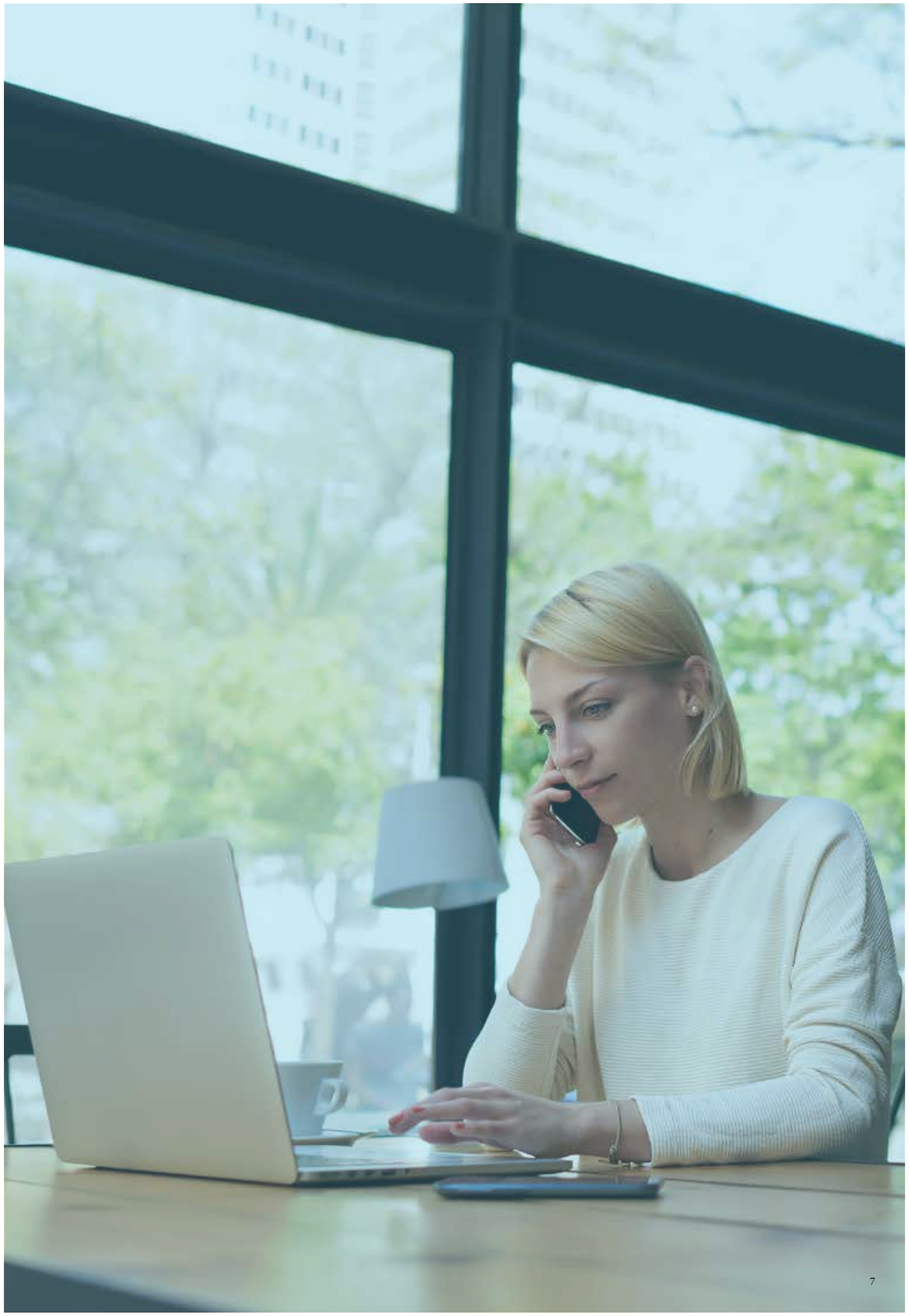
Spolupráce se zahraničními vysokými školami, ale i dalšími subjekty a organizacemi je nedílnou součástí dnešního komplexního akademického světa. V absolutní většině případů je taková spolupráce přínosná a neplynou z ní žádná další rizika či hrozby. V globálně propojeném

prostředí ale vznikají nové výzvy a hrozby, které ohrožují krom jiného duševní vlastnictví, počítačové systémy, ale i pověst vysokých škol a jejich zaměstnanců a zákonem garantované akademické svobody.

Základem následujícího textu jsou materiály zpracované k tomuto tématu ze strany Evropské unie (konkrétně ze strany Evropské komise[1, 2] a Evropského parlamentu[3, 4]), ale i národní dokumenty vydané vládami USA[5], Velké Británie[6, 7], Německa[8] a Austrálie[9] anebo některými zahraničními vysokými školami[10, 11, 12, 13]. Poznatky a doporučení z těchto vstupních materiálů jsou upravené pro české prostředí a doplněné o expertní znalosti a zkušenosti českých bezpečnostních odborníků.

Základní principy, které jsme zvolili pro tvorbu tohoto dokumentu, jsou:

- Akademické svobody a práva jsou garantované zákonem, což ale neznamená, že jsou zároveň dostatečně chráněné proti vlivovému působení cizí moci.
- Výzkum, spolupráce, smluvní vztahy a vzdělávací aktivity nesmí být v rozporu s právním řádem ČR.
- Bezpečnost je kolektivní záležitostí, nicméně každý má i určitou míru osobní odpovědnosti.
- Nároky na zajištění bezpečnosti by měly být proporcionální vzhledem k rizikům.
- Ochrana sektoru vysokého školství a jeho hodnot proti vlivovému působení cizí moci je důležitá.



2

Definice vybraných pojmů

Vzhledem k tomu, že cílem tohoto textu je poskytnout čtenáři alespoň základní vhled do problematiky škodlivého vlivového působení cizí moci se zaměřením na sektor vysokého školství, je nutné, aby byl čtenář seznámen se základními definicemi používaných pojmů.

I s ohledem na to, že vlivové působení cizí moci může nabývat různých podob, z nichž mnohé v jednotlivých krocích nijak neporušují platné zákony, bylo potřeba některé definice upravit přímo pro podmínky tohoto textu.

Agent zpravodajské služby – osoba vědomě a někdy i nevědomě jednající ve prospěch zpravodajské služby, která zpravidla plní jí zadané úkoly; nejedná se o zpravodajského důstojníka.

Akademický pracovník – pro potřeby této publikace jimi rozumíme profesory, docenty, další vědecké a odborné pracovníky a studenty.

Aktiva vysoké školy – v našem případě nehovoříme primárně o majetku, ale zejména o lidech (akademických pracovnících, výzkumnících, studentech doktorských programů, dalších studentech a zaměstnancích), know-how, duševním vlastnictví, výzkumných projektech, smlouvách s externími partnery, ale i o respektu, reputaci a postavení Vaší vysoké školy ve společnosti a v mezinárodním kontextu.

Cizí moc – český právní řád obsahuje definici pojmu v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů v § 2, písm. g) takto: „Cizí mocí se rozumí cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán." Pro účely tohoto textu definici rozšíříme i o jakékoliv další nestátní aktéry (fyzické či právnické osoby) bez ohledu na jejich státní příslušnost. Proto pokud v tomto textu budeme hovořit o „cizí moci", budeme tím rozumět jak české, tak zahraniční fyzické a právnické osoby (např. státy, jejich orgány, domácí a zahraniční firmy, politické strany atd.), které by mohly vysokou školu a její aktiva, včetně reputace, jakkoliv negativně ovlivňovat.

Due diligence – do češtiny bývá tento pojem nejčastěji překládán jako „náležitá pečlivost" anebo „náležitá opatrnost"; v našem případě se jedná o písemně či jiným záznamem doložitelné dohledání informací k subjektu šetření (tj. k představiteli cizí moci) sestávající minimálně z volně přístupných informací z otevřených zdrojů, dalších vysokoškolských a vědeckých databází, interních informačních zdrojů vysoké školy, informací a zkušeností získaných v rámci spolupráce mezi subjekty sektoru vysokého školství a analýzy rizik vyplývajících z těchto informací.

Ovlivňování[14] – všechny subjekty se snaží ovlivňovat jednání o záležitostech a otázkách, které jsou pro ně důležité; pokud jsou takové aktivity prováděny legálním a transparentním způsobem (kdy tyto subjekty otevřeně deklarují své záměry), pak jde o normální a běžnou aktivitu veřejnoprávních i soukromoprávních subjektů, včetně zahraničních, např. jako součást mezinárodních vztahů, diplomacie a PR a mohou pozitivním způsobem přispět do veřejné debaty.

Útočník – subjekt realizující vlivové působení vůči cílové osobě či instituci, přičemž se může jednat o zpravodajského důstojníka, agenta cizí zpravodajské služby, lobbistu, představitele privátní sféry apod., který se zpravidla za využití různých technik vlivového působení snaží ovlivnit cílový subjekt tak, aby nějak konal či nekonal.

Vlivové působení – nežádoucí a nepřípustná podoba ovlivňování, kterého se cizí moc dopouští,

pokud sama anebo prostřednictvím třetí strany vykonává zejména skryté, klamavé, vynucující či korupční aktivity směřující v tomto případě proti akademickým právům a svobodám a zájmům vysokých škol, jejich hodnotám a reputaci (včetně zájmu mít silné, nezávislé a transparentně financované vysoké školství atp.).

Vysoké školy – pro účely tohoto dokumentu si vystačíme primárně s definicí v zákoně č. 111/1998 Sb., o vysokých školách, v § 2, odst. 3, věta první: „Vysoké školy jsou univerzitní nebo neuniverzitní", nicméně tam, kde používáme pojem „vysoká škola", tím míníme i např. jednotlivé fakulty a další organizační jednotky, pokud jsou zřízeny.

Zpravodajská činnost – někdy též označovaná jako špionáž; v oblasti akademického a výzkumného prostředí se soustředí zejména na krádeže a transfer know-how, získání přístupu k citlivým informacím, výsledkům výzkumných projektů, inovativním řešením atp., mnohdy se ale v některých svých fázích zaměřuje i na sbírání podpůrných informací, jako jsou nálada na katedrách, slabiny či přednosti jednotlivých zaměstnanců, vztahy na pracovišti apod.; v konečném důsledku umožňuje cizí moci šetřit čas i vlastní zdroje.

Zpravodajský důstojník – příslušník zpravodajské služby, který může pracovat pod nejrůznějším krytím, např. jako diplomat, student, vědecký pracovník, obchodník apod., a který potřebuje pro svou činnost celou řadu kontaktů a osob, které využívá různým způsobem v zájmu svého vlastního státu.

Gender disclaimer: pro lepší přehlednost textu jsme se rozhodli uvádět osoby v mužském rodě, takže tam, kde píšeme o profesorech, docentech, akademicích, výzkumnících, studentech apod., myslíme samozřejmě i profesorky, docentky, akademičky, výzkumnice, studentky a další.

3

Proč je prostředí vysokých škol zajímavé pro cizí moc?

Se vstupem do akademického prostředí se stáváte osobou s přístupem k celé škále citlivých a pro cizí moc zajímavých informací. Disponujete mnohdy osobními informacemi stovek až tisíců studentů, z nichž by měly vzejít budoucí politické, společenské, kulturní a podnikatelské elity našeho národa, někteří z Vás mají přístup ke grantům a výzkumným projektům nebo máte možnost ovlivňovat obsah a formu výuky. Velmi často jste pak jako akademičtí pracovníci součástí veřejné, ale i odborné debaty k široké škále vnitropolitických anebo zahraničněpolitických témat. Udržujete si z podstaty své práce rozsáhlé kontakty na kolegy na jiných vysokých školách doma i v zahraničí, mnozí z Vás mají kontakty i na aktivní politiky, příslušníky bezpečnostních sborů, novináře a osoby ze světa byznysu. Je zcela přirozené, že takové přístupy a kontakty máte, neboť jsou základní součástí Vaší práce.[15]

Samotné uvědomění si toho, co takové informace a kontakty mohou pro někoho jiného znamenat a jak mohou být využitelné pro cizí moc, pokládáme za základní stavební kámen přístupu, který Vám zde chceme prezentovat.

Právě Váš přístup k procesům, funkcím a informacím, které mohou představovat potenciální zdroj informací pro osoby zastupující zájmy jiných států či nestátních subjektů, z Vás daleko častěji, než si možná uvědomujete, činí cíle zájmu cizí moci. Tyto zájmy nemusí být vůči ČR či organizacím, jichž je ČR členem, vždy přátelské.

Akademická sféra je velkým zdrojem informací, z nichž mnohé jsou samy o sobě nebo v souhrnu citlivé, utajované anebo je přístup k nim ze strany státu anebo na základě smluvního vztahu s určitou partnerskou stranou regulován.

Odborná reputace a akademické úspěchy Vaší vysoké školy jsou výsledkem dlouhodobé práce Vaší i mnoha Vašich kolegů. **Je Vaším zájmem přispět k ochraně dobrého jména Vaší vysoké školy, Vašeho pracoviště, duševního vlastnictví a informací, kterými disponujete a ke kterým máte přístup. Činy a aktivity každého z Vás přispívají k ochraně akademických práv a svobod a dalších zájmů, které se snažíme společným úsilím ochránit před vlivovým působením cizí moci.**

Záleží na vás. Jste důležití.

4

Nastavení systému obrany proti vlivovému působení cizí moci

Vysoké školy provádějí výzkum v širokém spektru různých oborů od umění, sociálních věd, lékařství až po technické vědy. Riziko vlivového působení cizí moci se bude pro jednotlivé obory lišit. I v rámci jednotlivých oborů bude docházet k dalšímu vnitřnímu členění na různé sekce a témata, které budou podléhat lišící se míře tohoto rizika.

Pokud o zaměstnance nebo studenty vysoké školy projeví cizí moc zájem, tak **cílem takového zájmu není s největší pravděpodobností daný člověk jako osoba, ale informace, přístupy či rozhodovací pravomoci, kterými disponuje.** Cíle potenciálních útočníků mohou být různé.[16] Může jít o pokus ovlivnit výuku nebo její část tak, aby odpovídala určitému vidění světa. Útočníci mohou chtít zjistit, čím se na Vašem pracovišti zabýváte či Vaším prostřednictvím získat v budoucnu potenciálně využitelné informace. V případě základního anebo aplikovaného výzkumu pak může útočník chtít získat přístup k výsledkům takového výzkumu a ušetřit tak své firmě nebo zemi tisíce hodin bádání, neúspěchů, hledání alternativních řešení, ale i nemalé finanční prostředky.

Potenciálním útočníkem nemusí být hned zahraniční zpravodajská služba, ale např. firma mající zájem na získání zakázek, právnická či fyzická osoba prosazující svůj zájem na změně rozhodnutí vydaného Vaším pracovištěm anebo subjekt zabývající se sběrem informací, které by mohl v budoucnosti zpeněžit. Může jít o hackera, který se jen baví, ovšem když narazí na zajímavé informace z Vašich databází, může se je pokusit zpeněžit. Takový hackerský útok může být i cílený. Dokonce si ho může útočník objednat na zakázku, pokud jeho IT dovednosti nejsou na úrovni, kdy by dokázal útok provést sám. Existují i jednotlivci a firmy, kteří na zakázku anebo s cílem budoucího využití kradou informace jiných. **Informace z vysokých škol a jimi založených či vlastněných právnických osob mají velkou cenu a lze o nich říct, že budou téměř s jistotou v budoucnosti využitelné.**

Základní postupy ke snížení rizika vlivového působení cizí moci by měly zahrnovat opatření, která jsou podrobněji rozepsána v kapitolách:

- Řízení rizik
- Due diligence
- Komunikace a vzdělávání
- Sdílení znalostí
- Kybernetická bezpečnost

4.1
Řízení rizik

Klíčem ke snížení rizika vlivového působení cizí moci v sektoru vysokého školství (ale i jinde) je **identifikace a řízení rizik**. Cílem pak je aplikovat procesy řízení rizik tak, aby došlo ke snížení zranitelnosti vůči vlivovému působení cizí moci ve všech spektrech činnosti vysokých škol, případně ke zmírnění dopadu takového působení. Zvláštní pozornost by měla být zaměřena na:

- ochranu duševního vlastnictví, výzkumných projektů a grantů, jejich obsahu a pokroku na nich,
- ochranu dobrého jména vysoké školy, členů akademické obce, partnerských subjektů a dalších zainteresovaných osob,
- rizika plynoucí od partnerských subjektů a z externího (mimorozpočtového) financování.

Vedení vysokých škol nese odpovědnost za **analýzu bezpečnostních rizik a vytváření strategií k jejich snižování**. Robustní bezpečnostní politika stojí na aktivním managementu, komunikaci a uvědomění si skutečnosti, že bezpečnost je dlouhodobým cílem, kterého lze dosáhnout jen systematickou a kontinuální prací. K jejímu vybudování je potřeba průběžně analyzovat existující rizika, která se v čase a podle okolností mění, nastavovat opatření k jejich snižování, komunikovat o těchto opatřeních, realizovat je a následně vyhodnocovat jejich efektivitu.

Otázky, které by si mělo vedení vysokých škol položit:

- Kdo ve vedení vysoké školy nese odpovědnost za vyhodnocování rizika vlivového působení cizí moci a za uplatňování náležitých protiopatření?
- Jaká máte interní pravidla, směrnice či nařízení řešící existenci rizika vlivového působení cizí moci a jak tyto dokumenty pomáhají manažerům, zaměstnancům a studentům pochopit, kdo, co, kdy a jak je vystaveno vyššímu riziku vlivového působení cizí moci?
- Jak jsou přesně analyzována rizika u jednotlivých výzkumných projektů? Máte nastavený centrální dohled, který by kromě vědeckého přínosu hodnotil i možná rizika?
- Máte stanoveny minimální požadavky na due diligence?
- Provádíte školení zaměstnanců a dalších osob (např. některých studentů) s cílem zvýšit jejich odolnost vůči vlivovému působení cizí moci? Je rozsah školení dostatečný?
- Máte nastavený systém interní komunikace s cílem hlásit incidenty na jednom místě tak, aby mohly být vyhodnocovány a mohla být přijímána adekvátní protiopatření?
- Jak jsou nastavena interní pravidla k řešení vzniklých incidentů s podezřením na vlivové působení cizí moci? Kdo tyto incidenty řeší? Jaké má k tomu postupy a nástroje?
- Kdo a kdy rozhoduje o zahájení spolupráce s bezpečnostními složkami, případně odpovědnými ministerstvy, za situace, kdy odhalíte možné vlivové působení cizí moci?
- Máte připravenou komunikační strategii a komunikační plány jak v rámci Vaší vysoké školy, tak i mimo ní, zahrnující postupy při situacích s přítomností vlivového působení cizí moci?
- Zapracováváte zkušenosti z vyhodnocených incidentů do Vašich interních pravidel, postupů, nařízení a školení? Sdílíte zkušenosti s ostatními vysokými školami?

Pokud si nejste jistí odpověďmi na výše položené dotazy, případně jste na některé z nich odpověděli negativně, pak je vhodné zapracovat na opatřeních proti vlivovému působení cizí moci na Vaší vysoké škole. **Rozhodněte, komu v nejvyšším managementu agendu ochrany proti vlivovému působení cizí moci přidělíte**. Uvědomte si, že i v rámci jedné vysoké školy budou existovat projekty, fakulty, katedry a další pracoviště, u nichž se **míra rizika vlivového působení cizí moci bude výrazně lišit.**

Proveďte analýzu aktiv Vaší vysoké školy s cílem odhalit, kdo z Vašich zaměstnanců by se mohl stát cílem vlivového působení cizí moci, zejména s ohledem na rozhodovací pravomoci a přístup k informacím, kterými disponuje např. o studentech, zaměstnancích a výzkumných projektech, ale i s ohledem na přístupy do médií, politických stran, bezpečnostních složek a do podnikatelské sféry. To samé proveďte ve vztahu ke studentům např. podle toho, jaké studují obory apod.

V dalším kroku **analyzujte Vaše stávající strategické dokumenty, bezpečnostní pravidla a procesy** a identifikujte, jak v nich je ošetřena ochrana osob, informací a IT systémů. Integrujte rizika vlivového působení cizí moci mezi Vámi zvažovaná rizika. **Nastavte procesy k identifikaci** oblastí Vaší činnosti se zvýšeným rizikem vlivového působení cizí moci, **nastavte dostatečná protiopatření** sloužící ke snížení těchto rizik a stanovte standardní postupy, kterými takové situace budete řešit.

Mezi tato opatření vždy **zahrňte minimální požadavky na due diligence, silnou a proaktivní komunikační strategii dovnitř i vně Vaší školy a systém školení** pro management, zaměstnance a studenty, přičemž ne vždy musí být pro všechny tyto skupiny rozsah školení shodný.

Ve většině případů není nutné, abyste se práce na projektu či spolupráce s partnerem, u kterého identifikujete zvýšené riziko vlivového působení cizí moci, vzdali. Danou situaci **můžete vyřešit třeba nastavením silnějších kontrolních mechanismů**, častějším auditem projektu a jeho přínosnosti, smluvním omezením aktivit a oprávnění partnerské strany apod.

Nastavení interních pravidel a směrnic by mělo specifikovat požadavky na jednotlivé zainteresované strany a subjekty, které je potřeba aplikovat v případě spolupráce s cizí mocí. **Na všech manažerských úrovních musí být jasně definovány standardní postupy realizované s cílem odhalit možné riziko vlivového působení cizí moci a musí být jasně stanovená odpovědnost za jejich realizaci.**

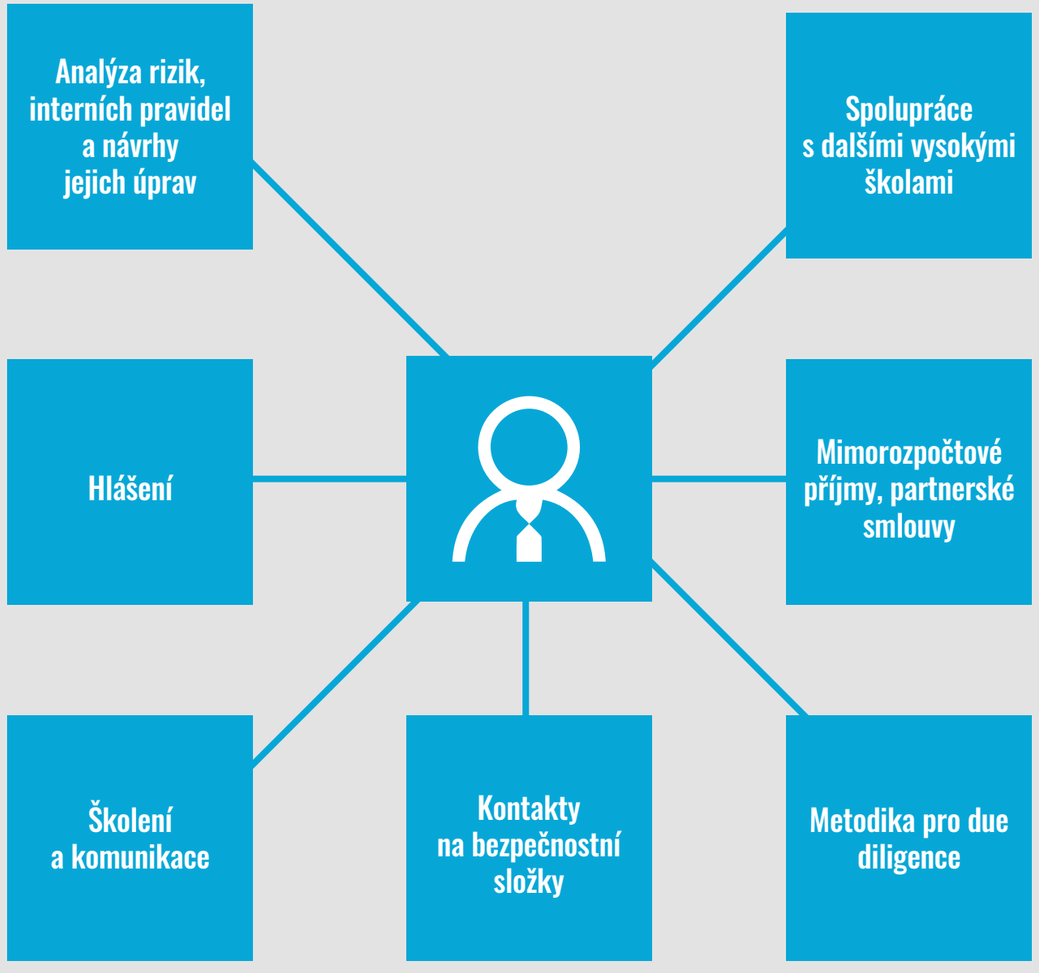
Systém interního nahlašování bezpečnostních incidentů a jeho vhodné nastavení umožňuje při dlouhodobém využívání snadněji vyhodnotit rizika, která se při Vaší práci nejčastěji vyskytují, včetně toho, kde Vámi nastavená opatření k jejich eliminaci a snížení fungují a kde ne.

Role a odpovědnost vedoucích pracovníků, co se týče spolupráce s cizí mocí, by měly být jasně a zřetelně stanoveny. Základní strategické dokumenty popisující pravidla a odpovědnost při spolupráci vysoké školy s cizí mocí by měly být sepsány tak, aby byl jejich výklad zřejmý a aby poskytovaly jednoznačné instrukce, jak postupovat a čeho se vyvarovat. Zároveň by měly obsahovat postupy, jak snížit rizika plynoucí pro vysokou školu ze spolupráce s cizí mocí.

Důležitým prvkem celého procesu je i uchování dokumentace související s vyhodnocením rizik vlivového působení cizí moci pro každou jednotlivou entitu (projekt, pracoviště, smlouva o spolupráci…). Podobně uchovávejte i dokumentaci pokrývající rozhodovací proces o přijatých opatřeních. Taková **dokumentace poskytuje velmi důležitý retrospektivní pohled**, zejména při uvědomění si faktu, že může nastat velmi rozdílné hodnocení daného rizika před případným incidentem a po něm.

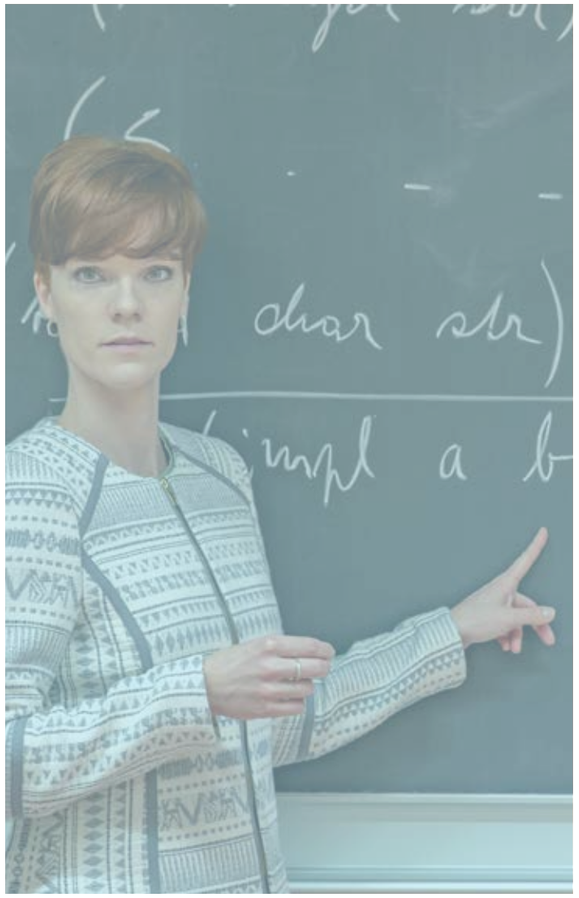
Z uvedeného vyplývá, že by měla být stanovena odpovědná osoba ve vedení vysoké školy, která bude mít na starosti celý proces od průběžného vyhodnocování rizik přes kontrolu dodržování nastavených opatření a školení zainteresovaných osob až po archivování veškeré dokumentace dokládající výše uvedené kroky. Vždy bude nakonec ale záležet na dané vysoké škole, zda tyto úkoly a odpovědnost za jejich realizaci přidá do agendy některého z manažerů, poskytne danému manažerovi v závislosti na rozsahu předpokládané práce tým lidí, anebo zřídí skupinu osob, které dostanou realizaci těchto úkolů na starosti.

Úkoly odpovědného manažera



4.2
Due diligence

Vysoké školy potřebují znát své partnery, a to i vzhledem k tomu, že jim od nich v některých případech může hrozit riziko vlivového působení cizí moci. Ve snaze o minimalizaci tohoto rizika je potřeba v co nejširší míře uplatňovat **zásadu „Poznej svého partnera“**.[17] Tuto zásadu je potřeba uplatňovat tak, aby v rámci procesu prověřování partnera a jeho důvěryhodnosti dospěla vysoká škola a její představitelé k dostatečnému poznání partnera **ještě předtím**, než dojde k navázání jakékoliv formální spolupráce.[18]



Spolupráce vysokých škol se třetími stranami je založena na kombinaci formálních, ale i neformálních vazeb se zahraničními a lokálními partnery. Absolutní většina této spolupráce je z hlediska samotných vysokých škol a ČR přínosná a žádaná a nevykazuje žádné znaky vlivového působení cizí moci. To je stav, který je ze strany státu a společnosti velmi podporovaný a žádoucí.

Akademici a další pracovníci sektoru vysokého školství mají povinnost jednat v souladu se zákony ČR, ale i v souladu s vnitřními předpisy svého zaměstnavatele. **Interní dokumenty a pravidla, která je upozorní na rizika vlivového působení cizí moci a na postupy, jak jim čelit, jim pak výrazně usnadní, aby dostáli svým povinnostem při ochranně akademických práv a svobod a nezávislosti.**[19]

V jakémkoliv partnerství záleží rozsah a míra rizika vlivového působení cizí moci do značné míry na povaze společné aktivity, která má být vykonávána. V mnoha případech se uplatní i konkrétní specifická legislativa či další smluvně zajištěné podmínky.

Riziko vlivového působení cizí moci se může také **s časem vyvíjet a měnit**, a proto by se u partnerů, se kterými vysoké školy uzavírají dlouhodobá partnerství, měl proces vyhodnocení tohoto rizika opakovat. Nelze nicméně zcela přesně určit, v jakém časovém horizontu by bylo vhodné proces zopakovat. Jako přijatelné doporučení se jeví provést kontrolu **jednou za jeden až dva roky**, jinak také **vždy při významné změně podmínek spolupráce a při zjištění nových informací**, které by mohly mít dopad na výsledek vyhodnocení tohoto rizika. Vždy je třeba postupovat v souladu se zásadou „Poznej svého partnera“ a vždy v rozsahu nutném pro posouzení rizika vlivového působení cizí moci odpovídajícího dané době, povaze a rozměru spolupráce. Zvažte i zapracování případného výhledu vývoje rizika vlivového působení cizí moci alespoň pro střednědobý horizont.

V mezidobí také **může dojít ke změně regulatorních požadavků ze strany vlády či zřizovatele**. Může dojít k nastavení nových pravidel, ale např. i k uvalení sankcí na některý ze subjektů, se kterým Vaše vysoká škola dosud spolupracovala. V takovém případě je potřeba zareagovat na nově vzniklou situaci a nejen upravit interní dokumenty vysoké školy vztahující se ke snižování rizika vlivového působení cizí moci, ale následně bez zbytečných odkladů provést úpravy i v dotčených smluvních vztazích, např. formou dodatku k původní smlouvě.

Vysoké školy by měly zvažovat i finanční rizika plynoucí ze spolupráce s cizí mocí a měly by se snažit tato rizika řídit a snižovat. Měly by ale také zvážit kroky, pomocí kterých by vyhodnotily potenciální reputační, politická, bezpečnostní a další rizika spjatá např. se zaměstnanci, sponzory, hostujícími akademiky a výzkumnými projekty, a následně rozhodovat na základě vyhodnocení i těchto rizik. Do analýzy rizik zahrňte i fakt, že mnozí zejména zahraniční spolupracovníci mohou mít i nezveřejněné vztahy a závazky anebo nemusí plně znát a respektovat pravidla, kterými jsou české vysoké školy povinny se řídit.

Vedení vysoké školy by mělo zajistit, aby byli její **zaměstnanci vyškoleni alespoň v základech rozpoznávání vlivového působení cizí moci a správných postupů při řešení podezření, že k něčemu takovému dochází**. U akademických a výzkumných pracovníků, u kterých vedení vysoké školy v rámci provedené analýzy zjistí zvýšené riziko vlivového působení cizí moci, by se mělo jednat o školení podrobnější. Taková školení by měla být pravidelně opakována v předem definovaných intervalech. Jako optimální vidíme školení jednou ročně u osob z vedení vysokých škol a u osob s identifikovaným rizikem vlivového působení cizí moci, u ostatních postačí jednou za dva roky. Minimální rozsah školení by měl obsahovat seznámení s interními dokumenty, pravidly a procesy k omezení vlivového působení cizí moci, dále návod, jak v konkrétních situacích postupovat, dále seznámení školených se základními vlivovými technikami, se kterými se mohou setkat (v rozsahu tohoto materiálu), a konečně případové studie a zkušenosti získané realizací protivlivových opatření.

4. 2. 1
Partnerské smlouvy a spolupráce s cizí mocí

Absolutní většina smluvních vztahů s jinými subjekty sektoru vysokého školství, se subjekty mimo tento sektor a se zahraničními subjekty je přínosem a obsahuje jen velmi malé riziko vlivového působení cizí moci.

V rámci partnerských a dalších smluv s domácími či zahraničními soukromými subjekty anebo státními, polostátními či nestátními subjekty z třetích zemí je vhodné před podpisem takových smluv hledat odpovědi na některé klíčové otázky. Jde vlastně o provedení zevrubné analýzy, během níž je potřeba vyhodnotit pozitiva, ale i možná negativa a dobrat se toho, zda taková smlouva bude pro Vaši vysokou školu skutečně přínosná a jaké hrozby a rizika s sebou přináší. Jen málokdy se asi stane, že by realita byla černobílá. Většinou budete čelit situaci, kdy bude potřeba

zvážit, zda pozitiva převládají nad negativy anebo naopak. Je třeba též počítat s tím, že čím dál tím častěji bude takové zvážení zřejmě požadováno ze strany akademiků, popřípadě ze strany médií a veřejnosti.[20]

Před formálním podepsáním smlouvy s cizí mocí by vysoká škola měla provést due diligence partnerského subjektu. Stejně tak by mělo dojít k přesnému specifikování oblasti a rozsahu spolupráce, včetně např. poskytnutí informací či záruk ze strany partnerského subjektu, které by mohly mít vliv na vyhodnocení rizika vlivového působení cizí moci. Tyto a další zákonné podmínky (např. povinnost dodržovat lidská práva a svobody, český právní řád, akademické svobody…) lze s budoucími partnerskými subjekty sjednat formou smluv o smlouvách budoucích či memorand o porozumění s jasnými následky jejich porušení.

Některé z otázek, které byste si před podpisem jakýchkoliv smluv s partnerskými subjekty měli položit:

- Jaké informace jsou známé o partnerském subjektu? Existují náznaky nějakých podezření? Existují informace o kontaktech a konexích, které by partner neměl mít? Jsou subjekt či instituce, s nimiž se chystáte navázat smluvní vztah, důvěryhodní? Existují veřejně dostupné informace o aktivitách takového subjektu či instituce, které by mohly znamenat budoucí ohrožení nezávislosti, dobrého jména či dalších zájmů Vaší vysoké školy?
- Snaží se partnerský subjekt o transparentnost, anebo jsou okolo jeho fungování tajnosti, pochyby a nejasnosti? Jak je partner transparentní při sdělování informací o svých dalších spolupracujících subjektech, majitelích, záměrech…, o kterých by Vaše vysoká škola měla předem vědět? Tyto mohou zahrnovat stávající vztahy s privátním sektorem, jinými vysokými školami a výzkumnými ústavy, ale i některými státními institucemi doma i v zahraničí.
- Trvá smluvní partner na tom, aby celá smlouva či její část byla neveřejná? U některých velmi specifických projektů, kde se pracuje s utajovanými skutečnostmi nebo jde o obchodní a jiné tajemství, to lze pochopit. Všude jinde by měly akademické instituce v zájmu prevence problémů usilovat o co možná největší transparentnost.
- Požaduje smluvní partner, aby vzájemná smlouva obsahovala pasáže, které do podobného typu smluv běžně nepatří? Trvá partner např. na tom, aby smlouva obsahovala různé zahraničněpolitické či jiné deklarace? Zvažte, zda jsou dané deklarace a prohlášení v gesci a zájmu Vaší vysoké školy, anebo zda patří do gesce některého z orgánů státní správy a zda je jejich existence ve Vámi sjednávané smlouvě nezbytná. Zvažujte a zjišťujte, proč je ve smlouvě partner chce mít.
- Má smluvní partner zájem na tom, aby ovlivňoval obsah diskuse na akademické půdě? Chce vybírat výukové materiály? Chce volit témata přednášek a seminářů? Má zájem na tom, aby se o určitých tématech nehovořilo anebo hovořilo jen určitým způsobem? Připouští i nesouhlasné názory či vysvětlující komentáře např. ze strany vyučujících či dalších expertů? Chce určovat, kdo bude přednášet a kdo ne?
- Existuje snaha partnerského subjektu sjednat smlouvu s Vaší vysokou školou tak, aby se dala jen velmi těžce či nedala vůbec vypovědět v situacích, kdy bude např. docházet k omezování akademických svobod či etického kodexu vysoké školy, nebo v případě, že vyjde najevo, že se partnerský subjekt stal předmětem exportních kontrol či sankcí? V jaké situaci se ocitnete, pokud se zjistí některá ze závažných negativních skutečností zmíněných výše? Budete moci ze smluvního vztahu bez vysokých ztrát odejít?
- Odpovídá kontrakt českému právu, anebo je partnerem prosazováno, že má odpovídat právu jeho domovského státu? Pak stojí za to zkoumat, zda taková pasáž ve smlouvě nebude v rozporu se základními lidskými právy a svobodami garantovanými Listinou základních práv a svobod nebo zda nebude omezovat akademické svobody garantované § 4 zákona č. 111/1998 Sb., o vysokých školách, případně zda není v rozporu s jinou částí českého právního řádu.

Vždy porovnávejte, co nabízíte a co za to získáte.,[22 23]

Vlády USA, Austrálie nebo Velké Británie již začaly pro své vysokoškolské sektory vydávat metodiky a doporučení ve snaze ulehčit jim identifikaci rizikového jednání ze strany partnerských subjektů. [24] Vláda Velké Británie vydala např. varování, že „výzkumná spolupráce s institucemi pocházejícími ze zemí, kde vládnou autoritářské režimy, může být náchylná ke zneužití ze strany organizací a institucí operujících v zemích, jejichž demokratické a etické hodnoty jsou odlišné od našich“.[25]

Jedním z vodítek může být **využívání sankčních seznamů vyhlašovaných vládou ČR, EU anebo OSN**. Tyto seznamy standardně zahrnují jednotlivce, skupiny, ale i organizace, kteří se podíleli či podílejí na porušování lidských práv, ilegálním obchodu se zbraněmi, terorismu či aktech extrateritoriálního násilí. Jako základní zdroje informací o sankcionovaných subjektech mohou posloužit webové stránky Ministerstva zahraničí[26], Ministerstva průmyslu a obchodu (Licenční správa)[27] a Finančního analytického úřadu.[28] Použít se ale dají i stránky americké nevládní iniciativy Organized Crime and Corruption Reporting Project, zpráva amerického Senátu o čínském vlivu na americké vysoké školy[30] anebo studie Australian Strategic Policy Institute.,[31, 32, 33] Zvýšenou pozornost by vysoké školy, podobně jako to dělají např. finanční instituce, měly věnovat i politicky exponovaným osobám a uzavírání smluvních vztahů s nimi.

4. 2. 2
Donoři a finanční partneři

Finanční prostředky jsou jedním z mnoha způsobů, jak může cizí moc realizovat svůj vliv na vysoké školy. Pro cizí moc jde o cestu relativně snadnou a efektivní. Může se zaměřit na jednotlivce, výzkumný tým, fakultu anebo celou vysokou školu.

Cizí moc může projevit zájem na financování výzkumného projektu či studijního oboru. Může Vaší vysoké škole poskytnout sponzorský dar, nabídnout finanční partnerství anebo grant. Za takto investované peníze očekává cizí moc minimálně pozitivní dopad na svoji reputaci, ale mnohdy má zájem i na ovlivnění obsahu výuky anebo výstupu z vědeckého výzkumu tak, aby vyhovoval jejím zájmům. Cizí moc se nemusí snažit finančně ovlivnit celou vysokou školu anebo její organizační součást, ale může svoji pozornost zaměřit jen na jednotlivé členy akademické obce a další pracovníky sektoru vysokého školství.

Vždy hledejte odpověď na otázku, kdo je osoba či subjekt, kteří finanční prostředky poskytují.[34] U takové osoby či subjektu je potřeba provést plnohodnotnou analýzu rizik s cílem zjistit, zda se nejedná o subjekt, který by do budoucna mohl způsobit Vaší vysoké škole reputační či jiné potíže.[35, 36] Mějte na paměti, že transparentnost financování Vaší vysoké školy je jednou ze zcela zásadních částí její reputace.

Vhodným opatřením je i **vytvoření registru všech nerozpočtových finančních příjmů** Vaší vysoké školy (nemusíte zahrnovat poplatky studentů za nadstandardní dobu studia ani poplatky za studium u studentů samoplátců, peníze přijaté z Grantové agentury ČR[37], Technologické agentury ČR[38] anebo jednotlivých ministerstev a ústředních orgánů státní správy[39]). Ideálně v něm budou zaznamenány všechny příjmy vysoké školy přicházející od cizí moci. Takový registr by měl vzniknout při rektorátu (u nejvyššího managementu vysoké školy). Měl by obsahovat i informace o tom, jaké kroky byly podniknuty při prověřování přispívajícího či dárcovského subjektu, a záznam o průběhu schvalovacího procesu daného finančního příjmu ze strany Vaší vysoké školy. Tento registr lze využívat i k analýzám části finančních toků, ale také např. k ověření, zda se u obdobných finančních přispěvatelů postupovalo srovnatelným způsobem v rámci due diligence.

Očekávejte, že s nastavením transparentních pravidel pro přijímání finančních prostředků se část potenciálních útočníků přesune z pozice, kdy se snažili o navázání spolupráce v oficiálnější rovině, spíše do pozice, kdy budou usilovat o neoficiální kontakty s jednotlivými zaměstnanci.

Otázky, které si položte u mimorozpočtových příjmů Vaší vysoké školy:

- Jaká existují interní pravidla a postupy pro přijímání finančních prostředků ze zdrojů mimo vysokou školu? Kdo za jejich naplňování odpovídá? Schvalovací proces by neměl být v rukou jedné osoby, ale mělo by se na něm podílet více osob (vhodným minimem jsou tři).
- Máte vytvořený registr všech finančních příjmů Vaší vysoké školy přicházejících od cizí moci?
- Existuje zřejmý nepoměr mezi požadovaným výkonem a finančním ohodnocením za vykonanou práci? Pokud ano, pak se může jednat o snahu o diskreditaci příjemce peněz, resp. vytvoření situace pro budoucí vydírání takového příjemce.
- Požaduje plátce (donor) nějaké nestandardní pasáže ve smlouvě? Např. chce smluvně zajistit chování či jeho absenci, které fakticky znamenají rozpor s českým právním řádem a zákonem garantovanými akademickými svobodami?

4. 2. 3

Výzkum a ochrana duševního vlastnictví

Výzkum je silným tahounem růstu moderních ekonomik. To posiluje i jeho význam pro cizí moc, která se může pokusit kompromitovat integritu systému, ale i některé konkrétní výzkumné projekty.

Vysoké školy mají většinou nastavený systém, který se stará o ochranu jejich duševního vlastnictví. Je ale potřeba provést analýzu toho, zda tento systém dostatečně reaguje i na hrozby a rizika vyplývající pro výzkumnou činnost a ochranu duševního vlastnictví z vlivového působení cizí moci.[40] Klíčem k omezení vlivového působení cizí moci je opět proces identifikace a řízení rizik. Vysoké školy by měly aplikovat systém řízení rizik tak, aby došlo k minimalizaci dopadu vlivového působení cizí moci na jejich výzkumné aktivity a na ochranu duševního vlastnictví, které vytvářejí. Přitom platí předpoklad, že **vnímání rizik a jejich úrovně se může významně lišit před a po případném incidentu.**

Jedna z cest, jak si cizí moc může zajistit přístup k výzkumným projektům a duševnímu vlastnictví a v některých případech i vliv na ně, je přes různé formy smluv o financování, sponzorství a dary.[41] Další pak je snaha o získání si některého z členů výzkumných týmů či administrativní podpory formou darů, úplatků, vydírání anebo krádežemi dat.[42]

Ověřte si proto, jak jsou na Vaší vysoké škole nastavena pravidla pro identifikaci takových smluv k výzkumným projektům, kterým je třeba věnovat větší pozornost zejména s ohledem na předmět výzkumu anebo typ partnerství. Je žádoucí, aby tato pravidla byla jednoznačná a neumožňovala alternativní výklad. Požadavky na analýzu rizik při uzavírání smluvních partnerství k výzkumným projektům prováděným ve spolupráci se zahraničními subjekty anebo privátním sektorem musí být také jasně stanoveny. Za jejich implementaci, aktualizaci a proškolování cílových osob ohledně jejich obsahu musí být jasně stanovena odpovědná osoba.

V rámci řízení rizik u výzkumných projektů je ale potřeba zvážit i další věci. **Ne vždy je např. možné predikovat veškeré možné varianty budoucího využití výsledků výzkumu**. Nicméně strategie řízení rizik by měla obsahovat i **kroky k identifikaci a ochraně potenciálně citlivých výzkumů a z nich vzešlých technologií**. Mnohé z nových poznatků, technologií, ale i softwarů mohou sloužit jako tzv. zboží dvojího užití, přičemž tyto podléhají zpřísněné regulaci ze strany státu a EU (viz např. zákon č. 594/2004 Sb., jímž se provádí režim Evropských společenství pro kontrolu vývozu zboží a technologií dvojího užití). Jiné výzkumy a technologie mohou mít i budoucí vojenské využití.[44] V takových případech by vždy měla být věnována těmto projektům zvýšená pozornost a ochrana.

Zřejmé je i to, že výzkum mající budoucí široké komerční využití může čelit zvýšenému zájmu cizí moci, ať již ze strany různých privátních subjektů, či zahraničních zpravodajských služeb. Správně nastavená pravidla a jejich aplikace jsou klíčem k identifikaci slabých míst v ochraně duševního vlastnictví a ke snížení rizika jeho ztráty, zneužití či krádeže.

4.3 Komunikace a vzdělávání

Povaha sektoru vysokého školství může nabízet mnoho vstupních bodů pro vlivové působení cizí moci. Vysoké školy by proto měly proaktivně svým zaměstnancům a v některých případech i studentům **nabízet školení** s cílem poskytnout jim informace o tom, jak může probíhat vlivové působení cizí moci a **jak mu předcházet.**

Součástí takového školení by měl být **návod, jak postupovat** v případě, když se domnívají, že zaznamenali pokus o vlivové působení cizí moci, ať již vůči své osobě, kolegovi, výzkumnému projektu, fakultě či vysoké škole. Součástí tohoto proaktivního přístupu by měl být i zpracovaný **systém zpětné reakce**. Systém, ve kterém oznamovatel zašle svůj podnět, aniž by obdržel zpětnou vazbu, nebude nikdy dlouhodobě fungovat. Odpovědný pracovník vysoké školy by měl oznamovatele kontaktovat, sjednat si s ním osobní pohovor, doplnit další detaily, které např. oznamovatele nenapadly nahlásit, ale pro řešení situace mohou být velmi důležité, poskytnout informace o tom, jak bude dál postupováno, a poskytnout oznamovateli alespoň základní vodítka a rady, jak se v dané situaci dále chovat. Zejména v některých vyvíjejících se situacích je vhodné tento postup podle vývoje situace opakovat. S odstupem času je pak vhodné **oznamovatele seznámit se závěry a ponaučeními**, anebo pokud je to možné, tak i s celkovým řešením případu.

Každý takový případ by měl sloužit i k **zopakování analýzy rizik**, zejména s cílem odhalit, zda na daný případ pamatují Vaše postupy a pravidla, a zjednat nápravu, pokud tomu tak není. Tyto případy by pak měly být zahrnuty do následujících školení zaměstnanců a studentů tak, aby se snížila pravděpodobnost jejich opakování. Následně by takové případy měly být komunikovány i s dalšími vysokými školami, aby docházelo k žádoucí **multiplikaci zkušenosti a aby se snížila možnost opakování shodného problému** na dalších vysokých školách. Je totiž zcela běžné, že se útočník pokusí využít stejný modus operandi útoku i vůči dalším vysokým školám. V některých případech je pak vhodné varovat další vysoké školy již v rané fázi incidentu za účelem vytvoření širokého povědomí o daném problému s tím, že závěry a ponaučení budou následovat až později.

Součástí celého **systému školení ke zvýšení odolnosti** vůči vlivovému působení cizí moci by měla jednoznačně být i **pravidla pro následující oblasti**:

- etická pravidla pro formální, ale i neformální setkávání se se zástupci cizí moci včetně pravidel pro společenské příležitosti a pro přijímání darů, jakož i pro transparentnost o těchto stycích,
- doporučení pro bezpečné cestování do zahraničí,[45, 46, 47]
- systém přístupů na jednotlivá pracoviště, ale i do jednotlivých IT systémů, se kterými se na Vaší vysoké škole pracuje,
- pravidla pro používání telefonních přístrojů a internetu využívajících připojení placených Vaší vysokou školou,
- pravidla pro aktivity studentů na Vaší vysoké škole (a na kolejích) za účelem ochrany všech studentů před zásahy do jejich akademických a lidských práv a svobod.[48]

Hledejte odpovědi na následující dotazy:

- Jaká školení poskytuje Vaše vysoká škola s cílem zvýšit odolnost vůči vlivovému působení cizí moci? Je jejich formát co do obsahu, ale i časové dotace dostatečný pro jednotlivé skupiny školených podle míry rizika, která u nich byla určena analýzou rizika vlivového působení cizí moci?
- Jak máte nastavené postupy pro hlášení ze strany studentů, zaměstnanců a dalších osob o podezření na identifikaci vlivového působení cizí moci? Kdo hlásí co, komu, kdy a v jakém rozsahu? Jak takové hlášení vypadá? Co se s ním potom děje? Máte nastavenou zpětnou vazbu vůči oznamovateli? Využíváte vlastní závěry a ponaučení, ale i ty od spolupracujících vysokých škol?
- Jak mohou být nově nastavena či rozšířena současná interní pravidla Vaší vysoké školy týkající se např. etiky, společenských událostí, doporučení pro bezpečné cestování, přístupů k jednotlivým pracovištím, informačním systémům a internetu, aby zahrnovala řešení usnadňující identifikaci potenciálního rizika vlivového působení cizí moci?
- Jak může Vaše vysoká škola či výzkumná instituce ještě více podpořit výzkumníky a akademiky ve snaze proaktivně řídit riziko vlivového působení cizí moci, zejména tam, kde je identifikováno zvýšené riziko?

Dalším vhodným opatřením je detailně připravený komunikační plán, který by měl řešit zejména, kdo komunikuje co, vůči komu a v jaký okamžik. Omezíte tak situace, kdy není jasné, kdo by měl danou událost komunikovat vůči zaměstnancům a studentům, ale i vůči veřejnosti, pokud se jedná o případ, kdy by veřejnost měla být informována. Vhodná a přiměřená komunikace je nedílnou součástí řešení nejen případů vztahujících se k vlivovému působení cizí moci. I prosté prohlášení ve formě „Stalo se to a to, situaci řešíme, aktuálně nemůžeme sdělit nic dalšího“ je z hlediska vysoké školy jako instituce a jejího dlouhodobého renomé lepší než mlčení, které dá prostor různým fabulacím a někdy i vzniku konspiračních teorií.[49]

Několik tipů ke zvážení:[50]

Pro vnější komunikaci s veřejností, médii a ostatními vysokými školami

- Na komunikační aktivity vyčleňte dostatečné množství osob a prostředků.
- Ujasněte si, jakým způsobem a prostřednictvím koho chcete informace přijímat (tok informací dovnitř) a jak chcete naopak vnější subjekty informovat (tok informací ven).
- Vždy berte v potaz sociální sítě; využijte jejich sílu a dosah ve Váš vlastní prospěch. Snažte se zamezit šíření hoaxů a falešných zpráv, které Vám mohou uškodit. Ve fázi po incidentu budou velmi pravděpodobně v informačním prostoru přítomny.
- Prvotní informace může být i stručná, na detaily a rozbory bude více času později.
- Pro komunikaci s veřejností si ideálně dopředu připravte texty zpráv pro různé typy incidentů, které pak upravíte podle konkrétní situace. Ušetříte tak čas a vyhnete se případným komunikačním chybám.

Pro vnitřní komunikaci s akademickými pracovníky, studenty a dalšími zaměstnanci

- Dopředu si ujasněte, jakým způsobem chcete s touto skupinou osob komunikovat. Informujte je také o tom, jakým způsobem budete jako organizace ve fázi po incidentu postupovat a jaký způsob komunikace mohou očekávat.
- Prvotní informace nemusí být obsáhlá, na detaily a rozbory bude více času později.
- Zvolte si takový komunikační nástroj, který je spolehlivý, umíte jej používat a máte jistotu, že se informace, kterou se snažíte sdělit, dostane k recipientům.
- Zvažte nejefektivnější způsoby komunikace. Např. svolání akademických pracovníků, studentů či dalších zaměstnanců do konferenční místnosti a informování o dalším postupu napřímo může být v některých situacích lepším řešením než posílání e-mailu anebo telefonát.

4.4
Sdílení znalostí

Vysoké školy a výzkumné instituce by podobně jako v jiných oblastech své činnosti měly **sdílet své poznatky a zkušenosti vztahující se k neustále se vyvíjejícímu riziku vlivového působení cizí moci**. To v sobě zahrnuje jak debatu nad tvorbou indikátorů sloužících na dané vysoké škole k odhalování vlivového působení cizí moci, tak přístup k řízení rizik, systému školení a práci s hlášeními oznamovatelů, dále úpravy pravidel externího financování výzkumu a výuky, pravidla pro ekonomickou aktivitu zaměstnanců mimo výkon práce pro svého zaměstnavatele (vysokou školu či výzkumný ústav) a další. Taková informační výměna by měla zahrnovat také sdílení konkrétních poznatků o odhaleném vlivovém působení cizí moci, ale i vzájemné informování se o způsobu řešení jednotlivých incidentů, případové studie a analýzy. Výměna těchto poznatků by měla probíhat např. formou setkání ustavené pracovní skupiny anebo definované online platformy uvnitř vysoké školy či výzkumné instituce a i napříč sektorem vysokého školství.

Tam, kde existuje podezření na porušení zákona, které přesahuje možnosti řešení interními akty řízení, případně postup např. podle zákoníku práce (zákon č. 262/2006 Sb.), je potřeba kontaktovat Policii ČR[51] či Bezpečnostní informační službu[52] se žádostí o pomoc. Proaktivní přístup k řešení problematiky rizika vlivového působení cizí moci je klíčem ke snížení dopadů případných jednotlivých vlivových operací útočníka.

4.5
Kybernetická bezpečnost

Kybernetická bezpečnost je nedílnou součástí mixu opatření ke snížení rizika vlivového působení cizí moci. **Významná část vlivového působení cizí moci je totiž s kybernetickým světem nějakým způsobem spjata**. Krádeže dat či narušení jejich integrity anebo narušení dostupnosti a spolehlivosti IT sítí patří mezi techniky vlivového působení cizí moci.[53] Vysoké školy by proto měly zaměřit svoji pozornost i na zkvalitnění svého přístupu ke kybernetické bezpečnosti.[54]

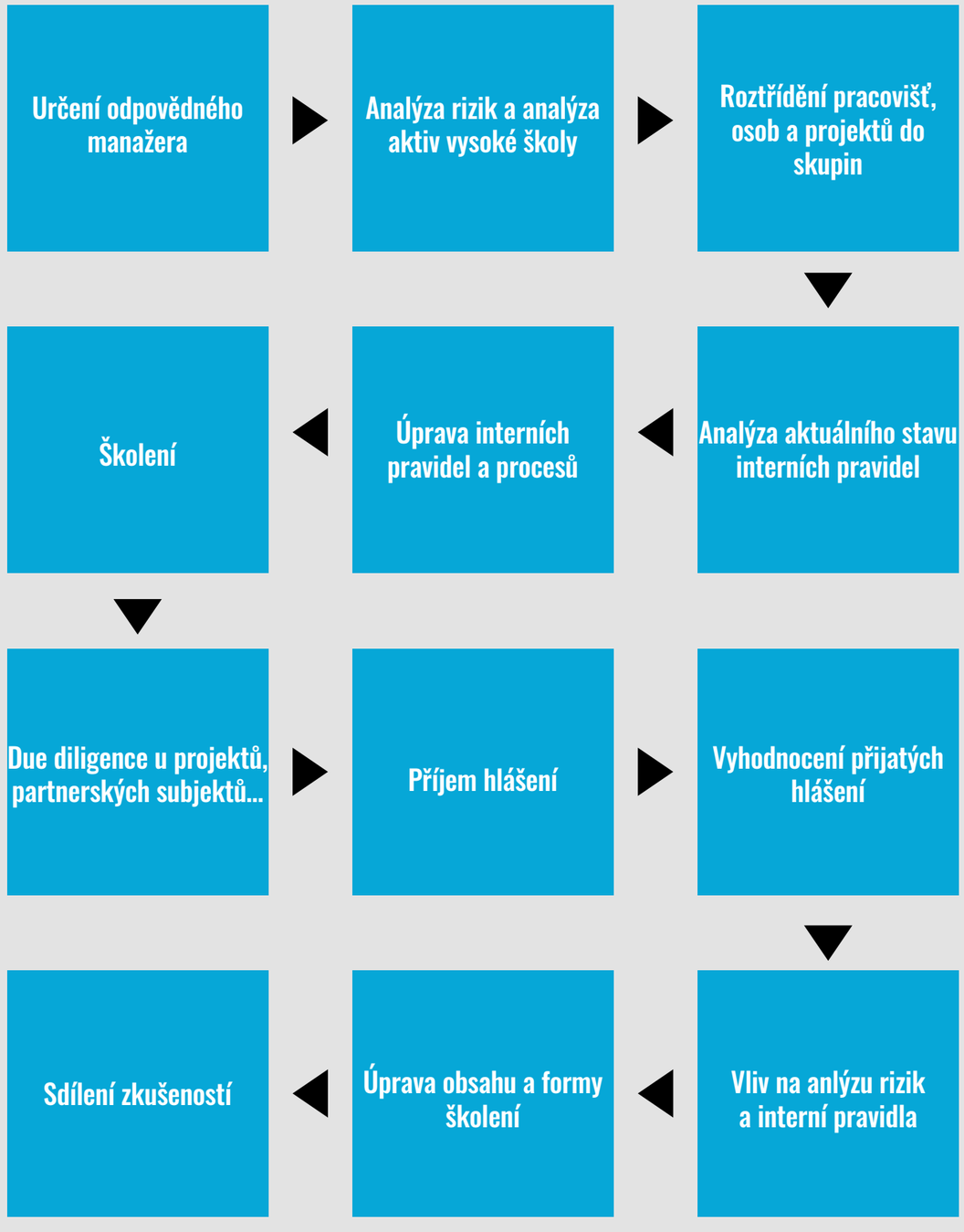
Národní úřad pro kybernetickou a informační bezpečnost zveřejňuje na svých stránkách celou řadu doporučení[55, 56], metodik[57], školicích materiálů[58] a aktuálních informací k různým kybernetickým hrozbám.[59]

Největší slabinou IT systémů bývají lidé, kteří s nimi pracují. Proto je potřeba je náležitě pro bezpečný pohyb v kybernetickém světě školit. Využít lze např. školení „Dávej kyber“.[60]

Pokud již dojde ke kybernetickému bezpečnostnímu incidentu, pak by vysoká škola měla mít nastavené postupy, jak takové situace řešit.

I v oblasti kybernetické bezpečnosti se čistě z pohledu snížení rizika vlivového působení cizí moci jeví jako podstatný prvek nastavení jasných a komplexních pravidel.[61] Neméně důležité jsou i včasné reakce na kybernetické bezpečnostní incidenty, komunikace a sdílení poznatků a zkušeností a školení zaměstnanců a studentů.

Zjednodušené grafické znázornění procesu nastavení systému ochrany proti vlivovému působení cizí moci



5

Shrnutí

Ke zvýšení odolnosti vůči vlivovému působení cizí moci v sektoru vysokého školství lze doporučit následující kroky:

- Uvědomte si, že riziko vlivového působení cizí moci vůči vysokým školám a jejich zaměstnancům je reálné.
- Určete osobu, která bude na Vaší vysoké škole odpovědná za snižování rizika vlivového působení cizí moci.
- Do analýzy rizik zahrňte riziko vlivového působení cizí moci a toto vyhodnoťte pro jednotlivé úrovně (nejvyšší manažeři, pracovníci s identifikovaným zvýšeným rizikem vlivového působení cizí moci a ostatní pracovníci a studenti), ale i organizační součásti a projekty (budou čelit rozdílné míře rizika podle toho, čemu se věnují).
- Proveďte analýzu stávajících bezpečnostních pravidel a doporučení.
- Stanovte strategii pro snižování vlivového působení cizí moci; nastavte kontrolní mechanismy.
- Zahrňte zásadu „Poznej svého partnera“ do své běžné činnosti.
- Připravte systém školení pro zaměstnance a studenty.
- S odstupem času opakujte analýzu rizik, protože riziko vlivového působení cizí moci se může s časem měnit.
- Sledujte regulatorní požadavky ze strany státu či zřizovatele a v souladu s nimi upravujte svoje vnitřní pravidla proti vlivovému působení cizí moci.
- Vytvořte registr finančních příjmů vysoké školy od cizí moci.
- Pravidelně vyhodnocujte informace, které máte k vlivovému působení cizí moci; závěry a poučení využívejte k dalšímu zdokonalení systému snižování rizika vlivového působení cizí moci.
- Připravte si komunikační plán pro případ incidentu s přítomným vlivovým působením cizí moci.
- Sdílejte svoje zkušenosti s dalšími vysokými školami.
- Stanovte jasná pravidla pro bezpečné cestování do zahraničí, přijímání darů, chování se při jednáních s cizí mocí, ale i pro politické aktivity studentů a zaměstnanců.

6

Techniky vlivového působení cizí moci na jednotlivce

V další části textu se pokusíme zmínit nejčastější techniky vlivového působení cizí moci. Jedná se tedy o výčet demonstrativní, přičemž jednotlivé techniky prezentujeme tak, abyste je v případě, že se s nimi osobně setkáte, byli schopni identifikovat. Popis nezahrnuje veškeré současné a budoucí možnosti působení cizí moci proti Vám, ale vybírá nejčastěji využívané možnosti. Stejně tak, jak se vyvíjí hrozby a rizika, vyvíjí se i techniky vlivového působení cizí moci na jednotlivce.

Postupně Vám představíme následující techniky vlivového působení cizí moci: verbování, nevědomé vytěžování informací, zneužití osobních informací z otevřených zdrojů, nebezpečné nabídky, ovlivňování na zahraničních cestách, vydírání, nátlak a lobbing a ovlivňování na jednáních.

6.1 Verbování

Každý se může stát předmětem zájmu cizí moci. Záleží jen na tom, čeho chce cizí moc dosáhnout.

Jde o techniku[62] nejčastěji využívanou zpravodajskými službami.[63] Zpravodajská služba[64] se za využití různých postupů pokusí získat člověka[65], který pro ni má nějakou hodnotu, k vědomé spolupráci[66]. K tomu nejčastěji zvolí přímé oslovení zpravodajským důstojníkem, může ale použít i prostředníky nebo různá krytí. V akademickém prostředí využívá útočník ve svůj prospěch také často nejrůznější legitimní anebo zdánlivě legitimní subjekty, jako jsou např. vědecko-technické knihovny, vědecké instituty a think-tanky, dále organizace zaměřené na expertní výměny či transfer know-how v rámci oficiálních výměnných a talentových programů, konzultační společnosti apod.

Zpravodajským důstojníkem pod krytím může být osoba vydávající se za diplomata, podnikatele, vědeckého pracovníka, studenta atp. Může k Vám přistoupit tzv. „pod cizí vlajkou“, protože si např. uvědomuje, že spolupráce nebo i jen kontakt s někým z jejich země pro Vás mohou být problematické.[67] Pokud se bude vydávat za osobu z jiné, pro Vás výrazně méně problematické země, budete možná méně ostražití a budete mít větší zájem si dotyčného vyslechnout a navázat spolupráci.

Je také možné, že se dostanete do situace, kdy budete útočníkovi nějak zavázáni – pomůže Vám např. ve chvíli nouze či v nějaké krizové situaci.[68] Může se k Vám dostat také jako přítel někoho z rodiny nebo známých.

Podobných technik, i když mnohdy výrazně méně sofistikovaných, využívají i jiné subjekty při snaze o prosazování svých zájmů. I mnohé privátní subjekty disponují obrovskými finančními, technologickými i lidskými zdroji a ve větší či menší míře neváhají tyto techniky využít ve svůj prospěch, zejména ve snaze získat konkurenční výhodu a silnější postavení na trhu či ve snaze ochránit svoje zájmy. Jak ale cizí moc konkrétně verbování provede?

Útočník ví, čeho chce dosáhnout, a bude hledat způsoby, kterými toho dosáhne co nejsnáze. Zahájí proto svoji činnost procesem **tipování a sbírání informací**, které by mohly být využitelné k samotnému verbování. Čím lépe útočník svoji potenciální oběť pozná, tím více výhod pak bude mít v dalších fázích procesu verbování. V procesu tipování jsou velmi často útočníkem shromažďovány informace, které se na první pohled mnohdy jeví jako bezcenné a nijak ohrožující.[69]

Historie vztahů, ale i drobných hříchů jednotlivých akademických pracovníků, lidí ve vedoucích pozicích, ale i dalších osob, jejich majetkové a rodinné poměry, charakterové vlastnosti, zájmy a koníčky, rozhodovací pravomoci, příprava veřejných zakázek a jejich zadávací dokumentace, dotační tituly a granty, složení různých komisí rozhodujících o výběrových řízeních a mnoho dalšího – to jsou přesně ty informace, o které potenciálním útočníkům jde.

Když má útočník dostatečné množství informací o své potenciální oběti, pak přistoupí k **navázání prvotního kontaktu**. Většinou půjde o nějaké krátké setkání, jehož jediným cílem je přesvědčit Vás k dalšímu setkání. Někdy Vás útočník osloví napřímo, jindy se nechá představit někým, koho již znáte, protože to zvyšuje útočníkovy šance, že s dalším setkáním s ním budete souhlasit. V některých situacích sehraje útočník doslova divadelní scénku s cílem Vás zaujmout, abyste to byli Vy sami, kdo útočníka osloví. Následuje fáze **rozvoje přátelských vztahů**, kdy se útočník zaměří na budování přátelské vazby mezi Vámi a jím. Z útočníkovy strany jde vždy o předstíraný zájem o Vaši osobu. Útočník se začne zajímat i o Vaši práci a může se stát, že Vás požádá o zpracování nějaké analýzy či o názor, přičemž může trvat na tom, aby se jednalo jen o veřejně dostupné informace. Za Vaši práci Vám dobře zaplatí nebo Vám poskytne jinou protihodnotu. V určitém momentu pak útočník přistoupí k samotnému **aktu zverbování**, který může proběhnout písemně, ústně anebo konkludentně. Postupně po Vás bude útočník vyžadovat **sdělování citlivých informací** a Vy už nebudete moci říct ne, protože budete mít na výběr jen mezi pokračováním ve spolupráci s útočníkem, anebo pracovněprávním a případně i trestněprávním postihem. Tomu se ale nevyhnete, ani pokud s útočníkem budete spolupracovat.

V některých případech postupuje cizí moc dlouhodobě a pokusí se získat danou osobu ke spolupráci již v rané fázi její kariéry.

Získávání informací je dlouhodobá činnost. Útočník vyhledává osoby, které mají přístup k určité informaci, nebo osoby, které mají přístup k někomu, kdo hledanou informací disponuje. Nezáleží na tom, jestli si Vy sami namlouváte, že nejste důležití. Pokud bude potenciální útočník považovat útok na Vás za něco, co ho posune k jeho cíli, pak se o to pokusí. Zároveň platí, že **každá instituce je tak zranitelná, jak zranitelný je její nejslabší článek**. Nestaňte se bránou, skrze kterou útočník pronikne do Vaší instituce.[70]

Kdokoliv, s kým se seznámíte mimo okruhy svých ověřených přátel a kolegů, může pracovat v zájmu cizí moci. To nelze nikdy spolehlivě vyloučit ani u lidí, které znáte delší dobu, neboť pro cizí moc mohli začít pracovat až v průběhu doby, kdy se vzájemně znáte. V tomto případě zaměřte svoji pozornost zejména na nápadnou změnu chování a probíraných témat.

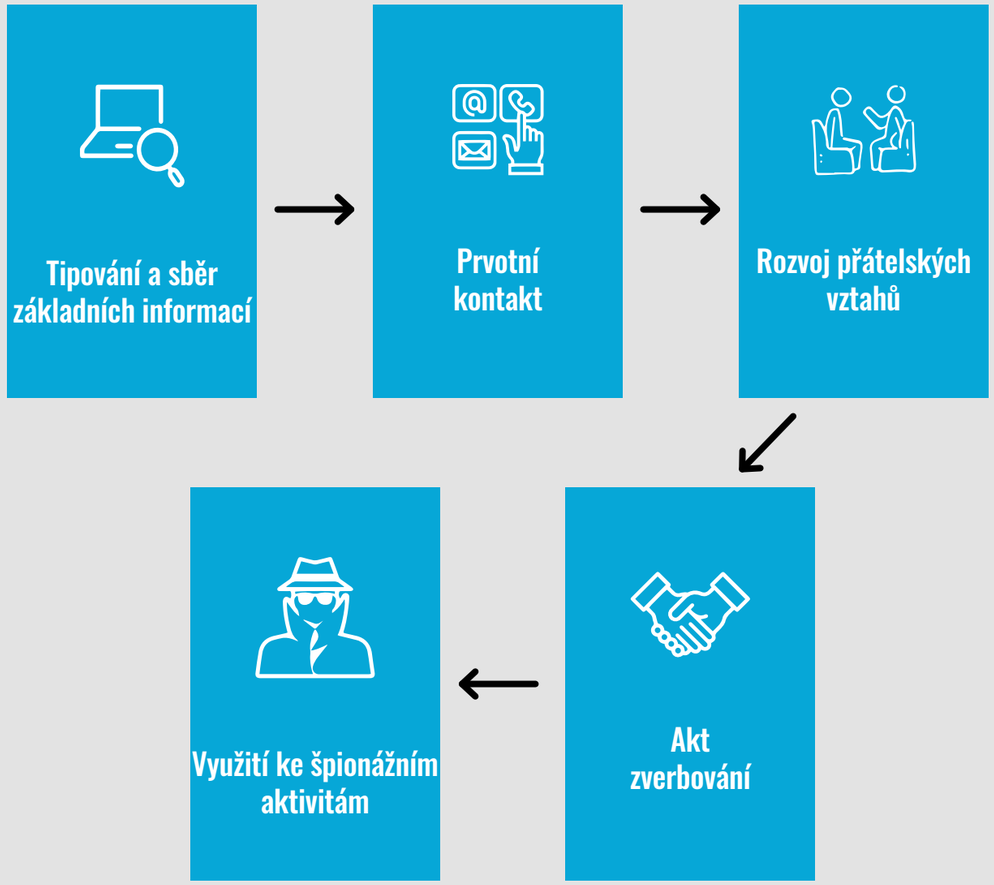
Věnujte čas tomu, abyste si promysleli:

- které informace o sobě a o své práci nebudete sdělovat, příp. je budete probírat jen s nadřízenými, nejbližšími kolegy či rodinou,
- které informace o sobě a o své práci budete sdělovat a probírat pouze v kruhu přátel,
- které informace o sobě a o své práci můžete sdělit i v okruhu cizích lidí,
- témata, o kterých se budete bavit, když se dostanete „do úzkých“.

To, že si Vás útočník vybere za cíl svých aktivit, nemusí být vůbec Vaše chyba. Zaznamenáte-li znaky toho, že může docházet k pokusu o Vaše zverbování, neotálejte a kontaktujte svého nadřízeného, bezpečnostního manažera, Policii ČR anebo Bezpečnostní informační službu. **Nesnažte se situaci řešit úplně sami**. Z hlediska Vašeho budoucího života a Vaší kariéry se může jednat o zcela zásadní problém. Rozhodnost a včasnost, s jakou začnete situaci aktivně řešit, jsou nesmírně důležité. Mohou se stát tím, co Vás ochrání před pracovněprávním anebo trestněprávním postihem.

Proces verbování lze pro ilustraci vizualizovat následujícím způsobem: [71, 72]

Zjednodušený popis procesu verbování



V případě, že zaznamenáte pokus o zverbování Vaší osoby zástupcem cizí moci, postupujte následovně:

- Věnujte zvýšenou pozornost tomu, co po Vás zástupce cizí moci chce.
- Pamatujte si pokud možno co největší množství detailů (jak proběhl Váš kontakt, kdo oslovil koho, kdo byl prostředníkem, na co se útočník ptal, o co měl zájem…).
- Na takovou nabídku ke spolupráci s cizí mocí reagujte ideálně jasným a zřetelným „ne“. Vaši odpověď si protistrana nebude moci vykládat jako „možná“, „podmíněné ano“ či „ano“. Vaše jasná a zřetelná zamítavá reakce by měla protistranu odradit od dalších pokusů Vás naverbovat.
- Neříkejte, že si vše musíte rozmyslet, a ani nevtipkujte. V takovém případě si Vaši reakci může protistrana vykládat jako „možná“ anebo jako „podmíněné ano“, velmi pravděpodobně se pokusí kontaktovat Vás znovu a již Vaše vzájemné první setkání může použít k Vašemu vydírání.
- Útočníka informujte o tom, že o situaci budete informovat nadřízené a bezpečnostního manažera. Útočníka tím odradíte od dalších pokusů Vás naverbovat, a navíc mu tím říkáte, že budou existovat kompetentní osoby, které o jeho aktivitách budou vědět a budou zvažovat protiopatření.
- Bez zbytečných průtahů informujte nadřízené a bezpečnostního manažera. Pokud tak neučiníte, útočník vycítí šanci pokusit se o Vaše zverbování znovu. Navíc neinformování nadřízeného a bezpečnostního manažera Vám může později být přičítáno ze strany zaměstnavatele k tíži a může např. ohrozit i získání či obnovení bezpečnostní prověrky od Národního bezpečnostního úřadu nebo od zaměstnavatele, pokud o ni požádáte.
- Výjimku z výše uvedeného postupu interakce s útočníkem představuje stav, kdy Vám útočník implicitně anebo explicitně vyhrožuje. Pokud jde o výhrůžku, kterou vnímáte jako reálnou, a máte oprávněný strach se útočníkovi postavit a spolupráci jasně odmítnout, pak se nesnažte situaci řešit sami. V takovém případě se naopak pokuste získat si čas (i předstíraným vzetím si času na rozmyšlenou). Následně bez zbytečných průtahů informujte nadřízené a bezpečnostního manažera. Pokud jste v zahraničí, svůj pobyt obratem ukončete a vraťte se domů. Prostřednictvím bezpečnostního manažera si vyžádejte asistenci českých bezpečnostních složek, ideálně Bezpečnostní informační služby. Její zástupci jakožto profesionálové, kteří mají s popsanými situacemi zkušenosti, následně určí další postup.

Zaznamenali jste náznaky toho, že se o vás zajímá cizí moc? Věřte své intuici. Nečekejte a obraťte se na profesionály s žádostí o pomoc.

Možné znaky toho, že se vás někdo snaží verbovat přes sociální sítě

- Přes sociální síť (nejčastěji LinkedIn, ale i Facebook, Twitter a další) Vám přijde zpráva od zahraniční vysoké školy, výzkumného institutu anebo firmy.
- Profil, který Vás kontaktuje, bude mít velmi pravděpodobně západně znějící křestní jméno, ale příjmení odpovídající zemi původu. Velmi často bude obsahovat falešnou profilovou fotografii, někdy generovanou umělou inteligencí, a abstraktní a mnohdy významově ne zcela jasný popis organizace, jejímž jménem Vás profil kontaktuje. Velmi často daná organizace (ani osoba pod profilem, jenž Vás kontaktoval) nemá žádnou historii, nebo dokonce ani reálně neexistuje. Text bude psaný slabou angličtinou s množstvím chyb. K profilu, který Vás osloví, bude zpravidla navázáno poměrně velké množství spojení a kontaktů, ty ale budou většinou trpět podobnými vadami jako profil, ze kterého Vám přišla původní zpráva.
- Žádost o poskytnutí rady anebo konzultace (zprvu velmi nevinné, zpravidla v rozsahu otevřených zdrojů). Následovat bude pozvání k pracovní návštěvě (v zemi „původu“ profilu) s tím, že veškeré výlohy budou placené zvoucí stranou.
- Pokud nabídku přijmete, přijde na řadu setkání s osobou stojící za profilem, z nějž jste byli kontaktováni, kterému budou velmi pravděpodobně přítomni i další kolegové této osoby. Postupně proběhne několik setkání podobajících se běžným pracovním schůzkám. Většinou se odehrají v drahých hotelech.
- Požadavek na zpracování analytického zhodnocení trendů v určité oblasti, na sumarizaci veřejně dostupných a postupně i veřejně nedostupných a citlivých informací (mnohdy strategických a vojensky využitelných).
- Za Vaši práci Vám bude nabídnuta odměna předem (většinou ve formě peněz v hotovosti a většinou u předání peněz bude více než jedna osoba ze zvoucí strany). S vysokou pravděpodobností bude z předání odměny pořízen i skrytý videozáznam s cílem Vás s ním v budoucnosti vydírat.
- Požadavek zvoucí strany na důvěrnost spolupráce.
- Další komunikace bude probíhat spíše elektronicky (primárně přes aplikace, jako jsou WeChat, Signal či WhatsApp, ale třeba i e-mailem). Po nějaké době snaha o další osobní setkání, ideálně opět v zemi, odkud pochází zvoucí strana. Veškeré cestovní výlohy budou opět hrazené zvoucí stranou.
- Postupné plné zapojení do různých špionážních aktivit.[73, 74]

6.2
Nevědomé vytěžování informací

Nevědomé vytěžování[75, 76], patří mezi základní zpravodajské techniky. Vychází z přirozené manipulace, kterou používá do určité míry v běžném životě každý. Jedná se o způsob, jak získat od cílové osoby co největší množství informací, aniž by si vytěžovaná osoba uvědomila, že je sděluje. V tom se zásadně liší od verbování, které je jednoznačnou nabídkou spolupráce, což znamená, že při verbování většinou není pochyb o tom, co se děje, a verbovaný má možnost říct „ne“.

Dobrý manipulátor, který se Vás může pokusit tzv. vytěžit, na Vás bude většinou působit jako velmi příjemná osoba. K tomu bude využívat práci s očním kontaktem, komplimenty (ve snaze vzbudit dojem, že Vás považuje za schopného a chytrého člověka), empatické naslouchání, občasné přikyvování, zájem o to, co říkáte, a vyvolávání pocitu, že jeho zájmy jsou blízké Vašim. Použití této techniky není omezené pouze na osobní kontakt, ale v určité míře ji lze provádět i přes telefon, či dokonce v psané formě (e-maily, chatovacími aplikacemi, SMS…).

Proč techniky nevědomého vytěžování fungují? Protože útočník, který je používá, si je vědom kulturních a osobnostních predispozic, které bývají lidem vlastní, a snaží se jich zneužít.

Přirozené chování člověka jako sociálního jedince, na které se útočníci zaměří, nejčastěji zahrnuje:[77]

- Snahu být nápomocný a slušný, a to i k úplným cizincům.
- Snahu vypadat jako někdo, kdo je velmi dobře informovaný.
- Snahu získat uznání a víru v to, že člověk přispívá k něčemu dobrému.
- Tendenci rozhovořit se k tématu, pokud člověk získá kladnou odezvu.
- Sklon šířit klepy a pomluvy.
- Snahu opravovat ostatní.
- Tendenci podcenit hodnotu sdělovaných informací, speciálně v situacích, kdy člověk není schopen vyhodnotit komplexně, jak by takové informace mohly být využity.
- Tendenci věřit tomu, že všichni lidé jsou v podstatě dobří a čestní.
- Snahu odpovídat pravdivě, pokud má člověk pocit, že otázka, která mu byla položena, je v dobré víře a s dobrým úmyslem.
- Snahu přesvědčit někoho jiného o své pravdě.

Útočník Vás zpravidla kontaktuje zdánlivě náhodně, případně s velmi věrohodnou záminkou. Může proběhnout i více takovýchto „náhodných“ setkání pro posílení důvěry. V akademickém prostředí dochází i k situacím, kdy informace tímto způsobem sbírá osoba, která se ve Vašem prostředí pohybuje oprávněně a oficiálně, jako např. tlumočník při jednání se zástupci protistrany či kontaktní osoba při návštěvě delegace u partnerské instituce. Pomocí připravené komunikační strategie z Vás útočník dokáže dostat postupně velké množství informací, aniž byste si všimli něčeho podezřelého. Má vytvořenou vlastní smyšlenou identitu, legendu, která má zpravidla podpořit Váš zájem o další setkávání s ním. Útočník s Vámi může ze začátku mluvit především o sobě a o Vás se jakoby nezajímat. Cílem je vmanipulovat Vás do situace, kdy sami od sebe začnete sdělovat tu nějaké osobní informace, tu zase nějakou drobnost z Vaší práce.

Nejlepší obranou proti těmto technikám je **zdravá nedůvěra** a **zvýšená obezřetnost**. Uvědomte si, které z informací, jimiž disponujete, jsou citlivé nebo mohou být citlivé při jejich dosazení do širšího kontextu. O těchto informacích se pak nezmiňujte, pokud k tomu nemáte velmi pádný důvod. Určete si, které informace (o Vaší práci, rodině apod.) můžete sdělovat komukoliv „na potkání“ a které už je vhodné sdělovat jen osobám prověřeným a důvěryhodným.[78]

Důležité je pamatovat si, že útočníkovi nikdy nejde o Vaše osobní kvality, ale vždy o informace, které máte. Rovněž nezapomeňte, že nemusíte nikomu vůbec nic sdělovat. Nenechte se z pocitu slušnosti vmanipulovat do situace, ve které se stanete obětí útočníka.

Konverzaci, u které máte podezření na probíhající pokus o Vaše vytěžování, můžete dostat zpět pod svoji kontrolu následujícími způsoby:[79]

- Ve Vašich odpovědích se odkazujte na veřejně přístupné informace (webové stránky, články v novinách, tiskové zprávy…).
- Ignorujte jakoukoliv otázku či vyjádření, u kterých máte pocit, že vzhledem ke konverzaci a jejímu obsahu nejsou vhodné anebo se snaží změnit téma hovoru.
- Na otázku, kterou vnímáte jako nevhodnou, reagujte svojí vlastní otázkou.
- Reagujte slovy „Proč se na to ptáte?“.
- Poskytněte odpověď, která není zcela konkrétní.
- Nebojte se říct, klidně i v rozporu s faktickým stavem věci, že takovou informaci nemáte a danou věc prostě nevíte.
- Deklarujte, že budete muset takovou diskusi nahlásit nadřízeným anebo bezpečnostnímu manažerovi.
- Na rovinu řekněte, že o této věci se s danouosobou nebudete anebo nesmíte bavit.

6.3
Zneužití osobních informací z otevřených zdrojů

Ke zveřejňování informací o sobě a svých blízkých online přistupujte velmi obezřetně.

Útočník uskuteční skoro vždy svoje první kroky online.[80] Zaměří se na to, co se dá o Vás z dostupných webových stránek najít. Především sociální sítě[81] (Facebook, Twitter, Instagram, LinkedIn, YouTube, TikTok, Twitch apod.) jsou dobrým zdrojem osobních informací např. o tom, kam jezdíte na dovolenou, kam chodíte do kavárny, jaké máte zvyky, kde jste studovali, kde pracujete a žijete či odkud pocházíte.[82] Jsou obrazem alespoň části vztahů mezi lidmi, se kterými se setkáváte, a to nejen prostřednictvím seznamu přátel, ale i pomocí fotografií a videí, které jsou umístěné nejen na Vašem profilu, ale také na profilech desítek (a možná stovek) Vašich přátel a rodinných příslušníků. Analýzou přístupných vizuálních informací a viditelných vzkazů a komentářů lze mnohdy získat základní přehled využitelný útočníkem pro další hledání doplňujících poznatků.

Samy sociální sítě uchovávají obrovské množství informací o uživatelích a jejich zvycích. Jejich business model je postaven na tom, že mnohé z těchto informací v anonymizované podobě prodávají dalším subjektům, které si u nich zadávají inzerci. S touto praxí uživatelé vyjadřují souhlas potvrzením podmínek při založení účtu. Sociální sítě a jejich provozovatelé o svých uživatelích většinou shromažďují nejen informace, které jim přímo sdělí (např. při založení účtu), ale i takové, které vyplývají přímo a nepřímo z chování uživatele na dané sociální síti. Jsou to např.: bydliště, věk, pohlaví, svatba, nedávné stěhování, očekávání dítěte, stáří auta, dary charitám, hraní her, používání debetních karet, nakupování potravin a jakého druhu, příjem, vlastnictví nemovitosti a její hodnota, vztah na dálku, pracovní prostředí, hraní her v prohlížečích, používání herních konzolí, zájem o nákup kosmetiky, preferovaný typ restaurací, zájem o sportovní události a mnoho dalšího.[83]

Na sociálních sítích může útočník velmi dobře vyhledávat podle stanovených kritérií. Lze také porovnávat dva různé profily osob – co mají společného a jejich vazby. Lze vyhledávat informace podle zaměstnavatele, místa bydliště, náboženství apod. Známy jsou i rozsáhlé úniky osobních dat uživatelů sociálních sítí a jejich zneužití.[84]

Další veřejně přístupné informace lze dohledat v některých databázích státních institucí, jako jsou živnostenský rejstřík, registr podnikatelských subjektů, katastr nemovitostí, seznamy studentů vysokých škol – tedy informace, které jsou do těchto databází vkládány, aniž by k tomu byl nutný Váš souhlas. Ani výše uvedené nepředstavuje kompletní výčet možných zdrojů, kde se dá vyhledávat. K dispozici jsou dále např. zpravodajská média a jejich archivy, blogy, osobní stránky, různé kvazimediální servery, ale i třeba internetové archivační služby.

Útočník mnohdy zkusí i metody sociálního inženýrství a může Vám zavolat nebo poslat zprávu např. přes sociální sítě, e-mail anebo SMS. Útočník to má o to snazší, že minimálně část těchto informací je o Vás už z podstaty Vaší práce v sektoru vysokého školství veřejných.

Útočník může ale využít i odposlech Vašeho telefonu, kanceláře anebo domova.[85] Můžete být i sledováni s cílem zjistit více o Vašem životě, zvycích a kontaktech.[86] Odposlech telefonu, kanceláře či domova anebo sledování nejsou již dlouhou dobu jen doménou bezpečnostních složek. Existuje celá řada soukromých subjektů, které se těmto aktivitám věnují, a jejich práce se dá objednat jako služba.

Několik základních tipů pro zvýšení Vaší bezpečnosti online

Obecně

- Zkontrolujte si, jaké Vaše privátní informace se nacházejí na sociálních sítích. Ty zbytné odstraňte.
- Nastavte si bezpečnost Vašich účtů na sociálních sítích tak, aby byl jejich obsah viditelný jen okruhu přátel.
- Pracujete-li na nějakém citlivém projektu, pak tuto informaci nezveřejňujte.
- Snažte se o to, aby nebyla poznat Vaše ekonomická situace. Nesdělujte výši Vašeho platu (mzdy). Nezveřejňujte fotografie Vašeho domu, bytu atp.
- Předtím než budete cestovat do zahraničí, pro jistotu znovu ověřte, jaké osobní informace lze o Vás na sociálních sítích veřejně dohledat.

V zahraničí

- Nepřihlašujte se k soukromým ani pracovním e-mailům, k Vašemu Google (Microsoft/Apple) účtu, sociálním sítím nebo internetovému bankovnictví. Pokud tak musíte učinit, využijte připojení přes VPN.
- Nepřipojujte svá zařízení (mobil, notebook, tablet…) k Wi-Fi sítím na veřejných místech, nádražích, letištích, v hotelech anebo kavárnách.
- Nepoužívejte Vaše soukromé anebo pracovní mobilní telefony, notebooky a ani různé datové nosiče (USB, externí HDD…), a pokud je to jenom trochu možné, používejte předplacené SIM karty a mobilní telefony, které v budoucnu nehodláte znovu používat. Notebook využívejte ideálně zapůjčený a po návratu jej nechte přeinstalovat.
- Nepoužívejte datové nosiče anebo jakákoliv elektronická zařízení, které jste dostali darem anebo někde našli.[87, 88, 89]

6.4 Nebezpečné nabídky (pozvání na akce, dary, hrazená školení, hrazené cesty)

Různé společenské akce, konference, semináře či formální a neformální pracovní setkání mohou být místem, kde budete čelit nevědomému vytěžování či pokusům o zverbování Vaší osoby.[90] **Mnohé z těchto akcí jsou právě za tímto účelem organizovány**. Mohou být využity k seznámení se s Vámi a k provedení prvotního kontaktu, který může zprvu vypadat i velmi nevinně. Samotný program pobytu a aktivity na místě mohou být hostitelem účelově naddimenzovány tak, aby došlo ke snížení Vaší ostražitosti a následně i plné kontroly nad tím, jaké informace sdělujete.

Je to také příležitost rozdat přítomným různé drobné dárky.[91] **Zvláště dárky v podobě datových nosičů (zejména pak různá CD, DVD či USB) v sobě mohou ukrývat špionážní software**, který se aktivuje v momentě, kdy uživatel zapojí datový nosič do počítače.[92] Špionážní software je ve většině případů tak sofistikovaný, že jej ani antivirová kontrola není schopna odhalit. Infikovaný počítač umožní odesílání citlivých informací na počítače útočníka. Může ale napadnout i celou počítačovou síť Vaší instituce. I výhradní používání darovaného zařízení doma vystavuje obdarovaného a celou jeho rodinu riziku sběru využitelných osobních, kontaktních nebo i kompromitujících informací. Váš domácí počítač pak může útočník ovládnout a využít k útoku na počítačové sítě Vaší vysoké školy, ale i dalších subjektů, se kterými Vaše vysoká škola spolupracuje.[93]

Pozor na darované datové nosiče. Nevkládejte a ani nepřipojujte je k počítači v práci anebo doma. Neotvírejte nevyžádané e-maily.

Podobná rizika jako datové nosiče s sebou nesou i přílohy e-mailů a zpráv zasílaných přes komunikační aplikace jako WhatsApp, Viber, Signal a další. Je tomu tak zejména tehdy, pokud Vám taková příloha, dokument či odkaz na webovou stránku (tzv. link) přišly od neznámé osoby. Opatrní buďte i tehdy, když jde o zprávu třeba od kolegy či známého, hlavně pokud takovou zprávu neočekáváte. Pak je lepší osobně či telefonicky u dotyčného ověřit, zda Vám takovou zprávu s vloženým souborem či odkazem posílal. V případě jakéhokoliv podezření, že se na Váš počítač mohl dostat škodlivý software, kontaktujte Vaše IT oddělení (správce sítě) a počítač vypněte, aby nedocházelo k dalšímu šíření škodlivého softwaru.[94]

6.5
Rizika ovlivňování na zahraničních cestách

Na zahraniční cesty se pečlivě připravte a buďte obezřetní.

Cestování a kontakty se zahraničím k akademickému sektoru patří, ať už se jedná o studijní pobyt, stáž, cestu na mezinárodní konferenci, anebo účast v programu Erasmus.[95] Rizika ovlivňování pracovníků akademického sektoru, ale i studentů na zahraničních služebních i soukromých cestách jsou zcela reálná.[96, 97] Vaše pozornost je upřena k realizaci cíle Vaší cesty. Pro útočníka se ale otevírá prostor, kdy k Vám může přistoupit s vědomím toho, že pokud by se něco nepovedlo úplně podle jeho představ, existuje menší pravděpodobnost, že budete svoje podezření ihned někam hlásit či s někým probírat.

Váš mobil, počítač, datový nosič, ale i poznámky Vám mohou při hraniční nebo jiné, i zinscenované, policejní kontrole okopírovat. Při těchto příležitostech Vám do něj může útočník nainstalovat také špionážní software. **Techniku a datové nosiče byste nikdy neměli nechávat bez dozoru** ani nikde jinde – na hotelovém pokoji, v recepci či v restauraci, ale ani při jednáních, na konferencích atp. Podobně nebezpečné situace nastávají, pokud využijete sdílené nabíječky mobilů, ale i veřejně přístupné Wi-Fi sítě.[98] Obojí bývá velmi často zneužíváno k instalaci škodlivého softwaru[99] do připojených zařízení anebo ke krádeži dat uložených na těchto zařízeních.[100] Stejně tak s sebou na zahraniční cesty rozhodně nevozte ani karty anebo čipy používané jako klíč pro různé systémy elektronické kontroly vstupu. I ty Vám mohou být odebrány, okopírovány a později využity k útoku na Vaše pracoviště. Totéž platí i o různých kartách, čipech a tokenech, které používáte pro autorizaci svého přihlášení do počítačové sítě, resp. jako svůj elektronický podpis.

Zvýšenou pozornost věnujte také situacím, kdy se během Vaší zahraniční cesty nebo pobytu objeví výjimečná příležitost[101] setkat se s někým velmi významným, ať už je to nějaký místní vedoucí pracovník, podnikatel, který se zajímá o Váš výzkum a nabízí, že by jeho výsledky dovedl dobře a pro Vás výhodně zpeněžit, či jiná významná osoba. Zejména pokud se jedná o osoby s vazbami na nedemokratické a neliberální státy a režimy či s vazbami na různé korporátní subjekty, ale i různé inovativní firmy či firmy pátrající po nových talentech a investičních příležitostech, tak existuje vážné riziko, že ve skutečnosti jde o pokus získat Vás ke spolupráci.

Dokumenty obsahující citlivé anebo jakkoliv zneužitelné informace mějte, stejně jako techniku, buď u sebe, anebo je s sebou do zahraničí vůbec neberte. Může jít o podkladový materiál, ale i zápisník s Vašimi myšlenkami, měřeními nebo i kontakty. Rozhodně takové dokumenty mějte vždy na očích nebo v příručním zavazadle, nenechávejte je na pokoji a při cestách letadlem je nedávejte do zavazadel, která budou uložena v zavazadlovém prostoru letadla.

Rizikové situace mohou přinášet i návštěvy zástupců cizí moci na Vašem pracovišti. Je možné, že součástí delegace je osoba pověřená úkolem získávat citlivé informace. Nemusí se jednat pouze o zahraniční návštěvy. Cizí moc se může pokusit vyzvídat citlivé informace také prostřednictvím osob, které se Vám představí jako studenti, novináři, zástupci akademické obce či neziskových organizací apod.

Možné znaky toho, že jste se stali cílem zájmu cizí moci při hraniční/policejní kontrole

- Ověřování Vámi předložených dokladů (a dalších dokumentů) trvá nestandardně dlouho.
- Jste eskortováni do výslechové místnosti či na policejní stanici, aniž by k tomu byl nějaký zjevný důvod.
- Aniž by se jakkoliv představil, objeví se důstojník v civilním oblečení a začne Vám klást řadu otázek nesouvisejících s důvodem původní kontroly; důstojník v civilním oblečení zpravidla nebude sám a je pravděpodobné, že v průběhu rozhovoru se objeví minimálně ještě jeden další důstojník v civilním oblečení, který bude více naslouchat a bude spíše jen klást doplňující dotazy.
- Zazní otázky na Vaše přesné pracovní zařazení, k detailům Vaší práce, ale i na Vaše kontakty; můžete být požádáni o to, abyste k Vašim kontaktům sdělili i jejich adresy a telefonní čísla, e-maily…, ale i to, zda cestují, jak často a do jakých zemí.
- Pokud odmítnete odpovídat na pokládané otázky, může Vám být naznačeno, že jste se dopustili porušení místních zákonů; někdy dokonce i včetně uvedení konkrétního protizákonného jednání (ať již existujícího, či smyšleného).
- Dostanete na výběr ze dvou možností. Buď akceptujete, že začnete spolupracovat s místními zpravodajskými službami, anebo Vám bude doživotně zakázán vstup do dané země a Vaše současná víza budou anulována. V případě odmítnutí spolupráce Vám může být vyhrožováno i uvězněním.
- Důstojník, který s Vámi vedl pohovor, Vám předá telefonní číslo, e-mail…, pomocí něhož jej můžete příště zkontaktovat (a nahlásit mu např. Vaši další cestu do země či do zahraničí).
- Budete informováni o tom, že se nemáte snažit zapírat nebo jakkoliv jinak sabotovat spolupráci, a budete upozorněni, že máte o proběhlém rozhovoru a vzájemné domluvě zachovat mlčenlivost[102]

6.6
Vydírání a nátlak

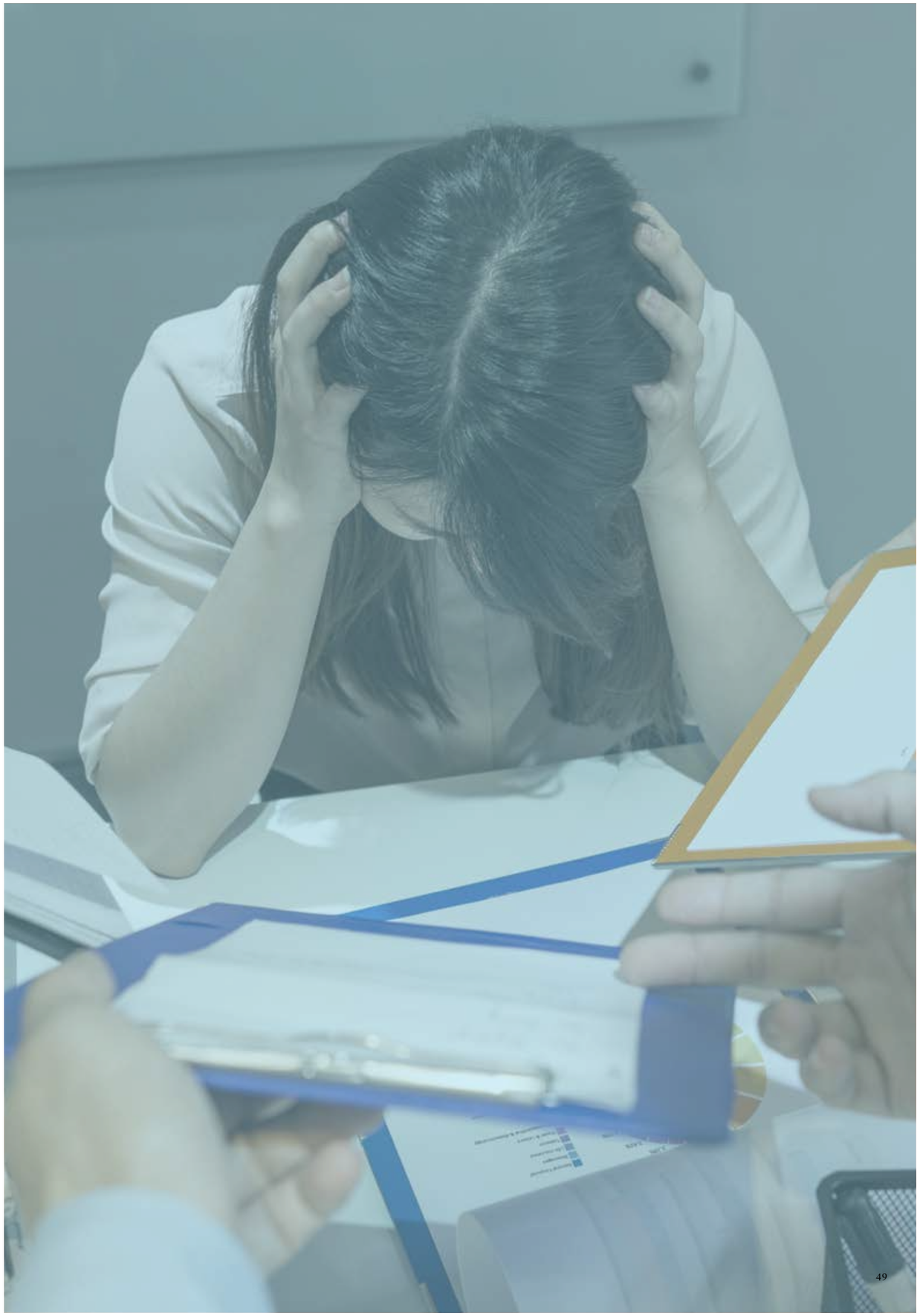
Vydírání neřešte sami, svěřte se.

I v současnosti jde o velmi intenzivně využívanou techniku, i když se může zdát, že patří spíše do špionážních filmů. Zejména cizí moc, která se necítí být vázána principy právního státu a základními lidskými právy a svobodami, se nebude zdráhat vydírání a nátlak použít. Snažte se proto na maximální možnou míru omezit riziko, že se ocitnete v situaci, kvůli níž byste mohli být potenciálně vydíratelní.

Uvědomte si, že zejména Vaše zahraniční pobyty Vás mohou do takových situací dostat. Nemusí se jednat o Vaši chybu či selhání, ale o útočníkem předem pečlivě připravený scénář.[103] Zneužitelné však může být jakékoliv Vaše tajemství, pokud nějaké máte a skutečně stojíte o to, aby se nestalo veřejně známým. Takových věcí může být celá řada – alkoholem, sázkami či gamblerstvím počínaje a sexuálními dobrodružstvími a různými hříchy, včetně těch z minulosti, konče. Nakonec to ale může být skutečně cokoliv, co chcete před svým okolím utajit.[104]

Útočník k získání materiálu, pomocí něhož Vás bude vydírat, použije všechny dostupné síly a prostředky, které má k dispozici a které mu současný stav poznání nabízí. Na místech veřejnosti přístupných Vás zkusí sledovat a nafotit fotografie, natočit videa či zvukové záznamy kompromitujících situací, do kterých se dostanete ať již svojí vlastní vinou, anebo v rámci připraveného scénáře. Technická a komunikační zařízení, která využíváte doma nebo v práci, se pokusí dostat pod svoji kontrolu a opět pořídit záznam takové potenciálně kompromitující činnosti. Když ani to nebude stačit, pokusí se Vám doma nebo v práci nainstalovat špionážní zařízení (tzv. štěnici). Pokud se útočníkovi nebude dařit získat takový záznam přirozenou cestou, pokusí se Vás do nějaké potenciálně kompromitující situace vmanipulovat. Díky dnešní technické vyspělosti může použít i úpravu fotografií a videí (tzv. deep-fake video) a kompromitující materiál může zfalšovat. Může najít osobu, která Vás z něčeho obviní a podá na Vás trestní oznámení. Může proti Vám vést na internetu pomlouvačnou kampaň. To vše se děje s cílem donutit Vás spolupracovat anebo zdiskreditovat za to, že jste spolupráci odmítli.

Pokud zaznamenáte pokus o nátlak či o vydírání vůči Vaší osobě, **situaci rozhodně neřešte sami. Svěřte se** rodině a kontaktujte bezpečnostního manažera Vaší školy či fakulty. V zahraničí můžete oslovit i český zastupitelský úřad. I když se Vám v některých případech může zdát, že pomoc, kterou získáte touto cestou, není taková, jakou byste si představovali, získáváte několik důležitých věcí. Pohled nezúčastněné osoby, se kterou situaci proberete, Vám pomůže podívat se na věc trochu z nadhledu, dále se Vám podaří si takovou událost urovnat v hlavě, ale zejména máte k dispozici svědka, který Vám dosvědčí, že jste se situaci pokoušeli obratem řešit, což může být podstatné pro Vaši budoucí kredibilitu. V konečném důsledku, byť by se situace mohla zdát jakkoliv bezvýchodná, má podlehnutí vydírání a nátlaku vždy mnohonásobně horší důsledky než řešení situace otevřeně s odpovědnými osobami a orgány.



7

Co Vám hrozí?

Neriskujte svůj profesní a soukromý život.

Mezi ta nejzávažnější rizika hrozící Vám jako jednotlivci lze zařadit ztrátu profesní prestiže, ztrátu zaměstnání (výpověď z pracovního poměru pro porušení pracovních povinností dle zákoníku práce, vyloučení z výzkumného projektu či grantu) a následné rodinné a osobní potíže, které mohou nabývat definičně velmi různorodých podob. Může nastat i situace, kdy Vám v souvislosti s prací pro cizí moc bude hrozit trestní stíhání. Případů, kdy spolupráce s cizí mocí dopadla pro spolupracujícího špatně, můžete i Vy sami najít v otevřených zdrojích velké množství. **Neriskujte svůj profesní a soukromý život** pro krátkodobý zisk či úlevu, a to ani v situacích, které v daný okamžik vnímáte jako bezvýchodné. Podlehnutí nátlaku cizí moci skončí ve valné většině případů daleko hůř než řešení situace standardní cestou.

Hlavní zásadou, kterou je potřeba si zapamatovat, je **„Pokud něco vidíte (vnímáte), pak něco řekněte“**.[105] V žádném případě nejde o to, budovat v sektoru vysokého školství „udavačskou“ kulturu. Je však nutné reflektovat, že každý jednotlivý zaměstnanec sektoru vysokého školství je součástí skládačky, která ve výsledku pomáhá udržovat akademické prostředí svobodné, demokratické a kreativní, a tím pádem brání vysoké školy proti nežádoucímu vlivovému působení cizí moci. Transparentnost i předběžná opatrnost jsou v těchto případech zcela zásadní. **Je vždy lepší, pokud Váš bezpečnostní manažer nebo nadřízený vyhodnotí Vaše hlášení jako neopodstatněné se závěrem, že k vlivovému působení cizí moci nedochází, než situaci zlehčovat, tvářit se, že se nic neděje, a pak čelit mnohonásobně horším následkům.**

Přestože i po zavedení systému identifikace a řízení rizika vlivového působení cizí moci může dojít k selhání jednoho či více jednotlivců na Vaší vysoké škole – protože tam, **kde jsou lidé, jsou i lidské slabosti – připravenost všech zúčastněných je v této oblasti klíčová.**

Vaše vysoká škola se díky Vašemu odpovědnému přístupu stane resistentnější a bude umět na situace s přítomným rizikem na vlivové působení cizí moci lépe reagovat, což povede i ke snížení případných následků plynoucích z takové situace.

8

Závěrečné shrnutí k vlivovému působení cizí moci na jednotlivce

Stali jste se cílem zájmu cizí moci? Mezi možné varovné signály lze zahrnout:

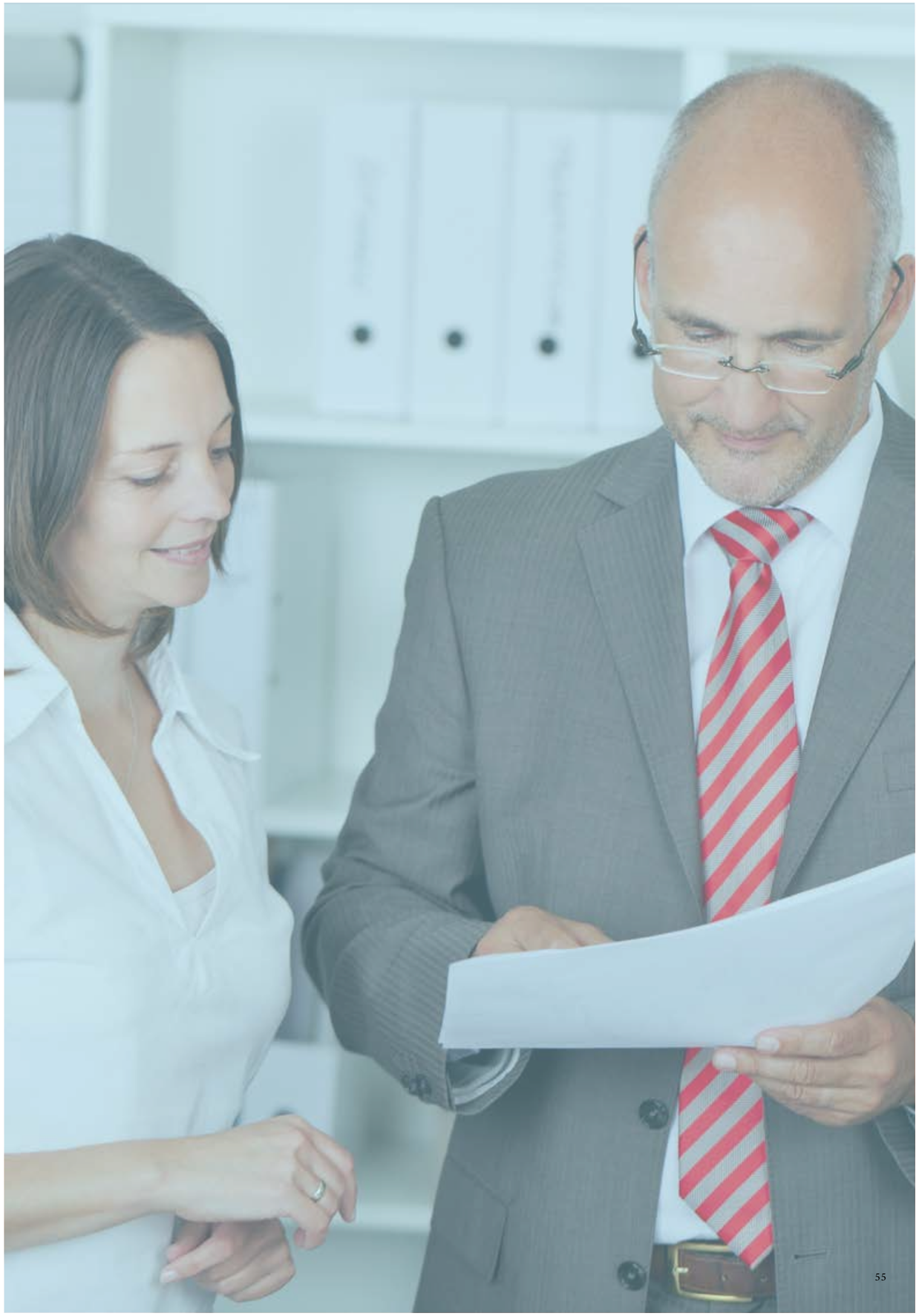
- Objeví se nový zvídavý známý, ptá se v míře větší než obvyklé na Vaši práci, koníčky a život, vykazuje nestandardní znalosti o Vaší práci či životě. Pozor na to, že informace pro cizí moc takto může zjišťovat i někdo z Vašich dlouhodobých známých anebo kamarádů, pokud začali spolupracovat s cizí mocí.
- Získáte nečekané výhodné nabídky zaměstnání od zahraniční instituce či firmy.
- Dostávají se k Vám žádosti o poskytnutí dokumentů, které jsou dostupné i jinak.
- Na cestách zjistíte známky manipulace s Vašimi osobními věcmi, zavazadly, elektronikou atp.
- Setkáte se se snahou nenadále Vás odloučit od Vašich věcí, telefonu, notebooku atp.
- Přijde nenadálá nabídka přijetí u vysoce postavené či jinak velmi vážené osoby.
- Nečekaný kontakt s bývalým kolegou, který začal pracovat v zahraničí.
- Možným příznakem, že informace z Vašeho pracoviště získává cizí moc, je i to, když Váš pracovní partner vykazuje větší znalosti o předmětu jednání, než by měl mít.

Uvědomte si základní principy obrany proti vlivovému působení cizí moci:

- Každý může být pro cizí moc zajímavý – i Vy.
- Každá informace může být pro cizí moc zajímavá. I ta z Vašeho pohledu zdánlivě nejbanálnější informace může být zneužita.
- Kdokoliv, s kým se seznámíte mimo okruhy svých ověřených přátel a kolegů, může pracovat v zájmu cizí moci. To nelze nikdy spolehlivě vyloučit ani u lidí, které znáte delší dobu, neboť pro cizí moc začali pracovat např. až v průběhu doby, kdy se vzájemně znáte. V tomto případě zaměřte svoji pozornost zejména na nápadnou změnu chování a probíraných témat.
- Ubezpečte se, že informace, které jsou o vás dostupné online, ale i jinde, odpovídají výše definovaným okruhům, a držte se tohoto pravidla i v komunikaci (e-mail, telefon, dopisy apod.).
- Pokud máte dojem, že jste se dostali do nestandardní situace, nebo v případě, že jste se stali cílem pokusu o zverbování, nepropadejte panice a informujte příslušné kontaktní osoby. Čím déle spolupracujete s cizí mocí, tím hůře to může dopadnout.

Obecná doporučení na závěr:

- Všímejte si podezřelé aktivity vůči své osobě i situací, kdy se domníváte, že můžete být cílem vyzvídání (vytěžování) či verbování, nebo když zažijete neobvyklý zájem o vlastní osobu.
- Pokud máte pocit, že se něco děje, nesnažte se situaci řešit sami, pište záznamy a zprávy a ty sdílejte s bezpečnostním manažerem na Vaší vysoké škole. Nebojte se zeptat na radu. Obrátit se můžete přímo na svého nadřízeného, bezpečnostního manažera ve vedení Vaší školy či fakulty nebo v odůvodněných případech přímo na Bezpečnostní informační službu.
- V případě nabídek na zahraniční služební cesty či pozvánek na stáže a konference, zejména pokud nejsou pro výkon Vaší práce nezbytné, Vám doporučujeme zvýšenou obezřetnost. Zvláště opatrní buďte tehdy, když Vám pořadatel nabízí v neobvyklé míře úhradu výdajů a kapesné.
- Na pracovních cestách do zahraničí se nenechte vmanipulovat do kompromitující situace (alkohol, společnost v hotelu apod.). Dokumenty, notebook, mobil či USB s Vašimi informacemi mějte pořád u sebe, nenechávejte je ani zavřené v trezoru v hotelovém pokoji (hotelový management má master-code pro případy, že by hosté zapomněli přístupové kódy a nemohli se dostat do trezoru pro své cennosti). Při cestě na zahraniční cestu a zpět z ní nenechávejte tyto věci ani v zavazadle, které nemáte pořád na očích.
- Jestliže provázíte zahraniční návštěvu na svém pracovišti, mějte přehled o tom, kde se účastníci pohybují, neumožňujte jim volný pohyb po budově a nenechávejte je samotné ve Vaší kanceláři ani v kanceláři kolegů.
- Před cestou do zahraničí zvažte, zda je nutné mít s sebou vlastní techniku jako notebook a telefon. Jejich zanechání v práci či doma snižuje riziko ztráty Vašich informací nebo nakažení Vaší techniky nebezpečným softwarem.
- Pokud se potřebujete připojit k internetu, berte na vědomí, že Vaše komunikace může být na různých místech monitorována (kavárna, hotel, letiště apod.). Internetový provider, přes kterého se připojujete, má vždy přehled o tom, co na síti děláte. Využívejte VPN.
- Bude-li to možné, vyhněte se využívání veřejných Wi-Fi sítí, hotelových počítačů a internetových kaváren, které všeobecně nebývají příliš bezpečné.
- Na sociálních sítích a v e-mailech sdílejte jen nezbytně nutné informace a nastavte si maximální možné soukromí. Toto nastavení průběžně a opakovaně kontrolujte.
- S maximální opatrností přistupujte k různým zdvořilostním darům v podobě flash disků, paměťových karet apod., protože mohou být nakaženy nebezpečným softwarem. Nakazit svůj počítač ale můžete i návštěvou různých webových stránek, proto vždy zvažujte, zda jde o stránky důvěryhodné. Vždy si aktualizujte operační systém a všechny bezpečnostní aplikace (antivirový software, firewall…).



9

Kontakty

Metodické dotazy

Centrum proti terorismu a hybridním hrozbám
Odbor bezpečnostní politiky
Ministerstvo vnitra ČR

E-mail: cthh@mvcr.cz
Web: www.mvcr.cz/cthh/

Hlášení incidentů

Bezpečnostní informační služba
Tel: +420 257 142 211 a +420 235 521 400
E-mail: prevence@bis.cz a info@bis.cz
Web: www.bis.cz

Policie ČR

Web: www.policie.cz/imapa.aspx

10

Odkazy

1 https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf

2 https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788

3 http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/644207/EPRS_ATA(2019)644207_EN.pdf

4 https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1564018 & t=e & l=en

5 https://www.cdse.edu/index.html

6 https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/10902.htm

7 https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx

8 https://www.hrk.de/positionen/beschluss/detail/leitfragen-zur-hochschulkooperation-mit-der-volksrepublik-china/

9 https://docs.education.gov.au/system/files/doc/other/ed19-0222_-_int_-_ufit_guidelines_acc.pdf

10 https://www.research.uky.edu/office-sponsored-projects-administration/guidance-regarding-foreign-influence-university-research

11 https://www.ucop.edu/ethics-compliance-audit-services/compliance/research-compliance/foreign-influence.html

12 https://researchservices.cornell.edu/policies/guidelines-on-undue-foreign-influence

13 https://research.unl.edu/researchcompliance/foreign-influence-international-activities/

14 Někdy bývá označováno také jako tzv. soft power.

15 Australský think-tank Lowy Institute se stal nejméně dvakrát terčem hackerského útoku, jehož cílem bylo ukrást zejména databázi kontaktů osob, se kterými tento think-tank spolupracuje a které docházejí na jím organizované události. Podobným hackerským útokům ale čelily i další australské a americké think-tanky (https://www.smh.com.au/national/watering-hole-attacks-how-china-s--hackers-went-after-think-tanks-and-universities-20181203-p50jxj.html).

16 Aston University z Birminghamu ve Velké Británii vyšetřovala stížnosti studentů z Hong Kongu, že byli obtěžováni svými spolužáky z Číny. Jeden ze studentů podporujících demokratický proces v Hong Kongu byl obestoupen studenty z pevninské Číny tak, že nemohl odejít, zatímco čínští studenti stojící okolo něj drželi čínskou vlajku a zpívali národní hymnu. Další z hongkongských studentů mají obavu, že je spolužáci z pevninské Číny monitorují a odesílají jejich fotografie a identifikaci jejich účtů na sociálních sítích do Číny (https://www.telegraph.co.uk/news/2019/10/12/police-called-hong-kong-china-tensions-spread-uk-universities/).

17 V únoru 2020 čelila německá Trier University vlně kritiky za to, že její akademik, filozof Andreas Lammer, akceptoval ocenění „World Award for Book of the Year of the Islamic Republic of Iran". To mu udělil íránský prezident H. Rouhani za jeho práci o islámském učenci Ibn Sínovi, který zemřel v Hamedánu (dnešní Írán) v roce 1037. Kritika se týkala zejména porušování lidských práv a podpory terorismu ze strany Íránu, což by mělo být dostatečné zdůvodnění pro nepřevzetí či odmítnutí udělené ceny (https://www.jpost.com/Diaspora/Antisemitism/German-university-under-fire-for-accepting-award-from-Irans-regime-617996).

18 V lednu 2020 došlo k odhalení spolupráce profesora Gu Jiana, působícího na čínské Hainan University a věnujícího se informační bezpečnosti, s čínským Ministerstvem státní bezpečnosti (MSS). Ten svoji pozici využíval k získávání mladých odborníků na IT s cílem najmout je ve prospěch hackerské skupiny APT40 ovládané hainanskou centrálou MSS. Postupně se podařilo odhalit 13 firem, které velmi pravděpodobně působí jako krycí firmy pro APT40 a kterým profesor Gu Jian umožňoval zveřejňovat pracovní inzeráty na webu Hainan University (https://intrusiontruth.wordpress.com/2020/01/14/who-is-mr-ding/, https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/, https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu/, https://intrusiontruth.wordpress.com/2020/01/13/who-else-works-for-this-cover-company-network/).

19 K akademickým svobodám viz § 4 zákona č. 111/1998 Sb., o vysokých školách.

20 Čtyři akademici působící na britské London School of Economics (LSE) protestovali v červnu 2019 u rektora LSE proti „zvyšujícímu se riziku pro dobrou pověst školy pro její intenzivní spolupráci s Čínou" a dožadovali se „pečlivého přezkoumání etických dopadů toho, že na LSE existují sdílené výukové a vědecké programy s institucemi, na kterých jsou omezovány akademické svobody ze strany Komunistické strany Číny" (https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all-1573-rdf).

21 Vysoké školy v USA i jinde ve světě si začaly uvědomovat kontroverznost Konfuciových institutů. Tyto instituty byly zakládány s cílem podpořit studium čínštiny a čínské kultury, ale hodně akademiků je aktuálně vnímá jako zástěrku pro působení čínských zpravodajských služeb (https://www.voanews.com/student-union/chinese-college-students-being-forced-spy-us).

22 V roce 2019 byla britská London School of Economics nucena pozastavit plánovaný program spolupráce se šanghajským podnikatelem panem Li, který sliboval štědré financování výzkumu a podíl na financování výuky v magisterských a doktorských programech týkajících se čínské ekonomiky, politiky a společnosti, přičemž nad správností obsahu výuky měla dohlížet skupina význačných osobností z Číny (https://www.ft.com/content/2dd5ed50-f538-11e9-a79c-bc9acae3b654).

23 https://www.dailymail.co.uk/news/article-8535623/How-Britain-teaches-China-conquer-West-UKs-universities-share-research-China.html

24 V dubnu 2019 varoval úřadující ředitel americké FBI, Christopher Wray, že čínské zpravodajské služby tlačí ve velkém na čínské studenty studující v USA a na jejich rodiny v Číně, aby „dovezli" domů nějaké cenné duševní vlastnictví, jinak se rodinám povede zle (https://www.voanews.com/student-union/chinese-college-students-being-forced-spy-us).

25 Britská London School of Economics (LSE) čelila v únoru 2020 rozsáhlé veřejné kritice za to, že zvažovala uzavření tříleté poradenské smlouvy s čínskou firmou Huawei, přičemž se měla věnovat výzkumu „vedoucí role firmy ve vývoji technologií 5G" (https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all-1573-rdf).

26 https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/kontrola_exportu_zbrani/mezinarodni_spoluprace/mezinarodni_kontrolni_rezimy_obecna.html

27 https://www.mpo.cz/cz/zahranicni-obchod/licencni-sprava/

28 https://www.financnianalytickyurad.cz/

29 https://occrp.org/en

30 www.hsgac.senate.gov/imo/media/doc/PSI%20Report%20China%27s%20Impact%20on%20the%20US%20Education%20System.pdf?utm_content=&utm_medium=email & utm_name=&utm_source=govdelivery & utm_term=

31 https://www.aspi.org.au/report/party-speaks-you

32 https://unitracker.aspi.org.au/

33 https://www.aspi.org.au/report/picking-flowers-making-honey

34 V říjnu 2019 podepsal rektor pražské Karlovy univerzity smlouvu o partnerství s firmou Home Credit. Tento krok vyvolal ostrou reakci části akademické sféry, studentů, ale i veřejnosti. V rozsahu několika dnů v reakci na extenzivní veřejnou debatu kritizující takové partnerství firma Home Credit od smlouvy odstoupila (https://www.seznamzpravy.cz/clanek/konec-kritiky-na-akademicke-pude-odbornici-jsou-proti-partnerstvi-univerzity-karlovy-s-home-creditem-80303, https://www.seznamzpravy.cz/clanek/home-credit-po-vlne-kritiky-vypovedel-smlouvu-s-karlovou-univerzitou-80463, https://www.respekt.cz/tydenik/2019/42/univerzita-kellnerova).

35 V roce 2011 propukl na britské London School of Economics (LSE) skandál s přijetím finančních prostředků od nadace vedené Saifem Al-Islámem, synem tehdejšího lybijského diktátora Muammara Kaddáfího, přičemž panovalo silné podezření, že se mohlo jednat o finanční prostředky pocházející z úplatků. Aféra nakonec skončila až rezignací rektora LSE. Jedna z dceřiných firem LSE také získala kontrakt na vzdělávání libyjských státních úředníků, což také vzbudilo vlnu nevole a kritiky (https://www.theguardian.com/education/2011/nov/30/gaddafi-donation-lse-bribes-inquiry, https://www.ft.com/content/2dd5ed50-f538-11e9-a79c-bc9acae3b654, https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all-1573-rdf).

36 Koncem roku 2018 začalo v USA vyšetřování některých amerických vysokých škol kvůli jejich financování ze strany Kataru, ale i jiných blízkovýchodních států. Poskytováním štědrých finančních příspěvků Katar sledoval primárně svoje zahraničněpolitické cíle, a tudíž docházelo ke zneužívání amerických vysokých škol. Velká část těchto finančních toků navíc postrádala transparentnost a americké vysoké školy jejich část tajily před americkými úřady (http://english.alarabiya.net/en/features/2018/12/20/How-Qatar-is-paying-1-3-billion-to-US-institutions-to-gain-dubious-influence.html, https://clarionproject.org/exclusive-foreign-funding-billion-dollar-black-hole/, https://www.novinky.cz/zahranicni/amerika/clanek/bernak-jde-i-po-harvardu-a-yale-40313470?seq-no=5 & dop-ab-variant=&source=article-detail).

37 https://gacr.cz

38 https://tacr.cz

39 Viz zákon č. 2/1969 Sb., kompetenční zákon (https://www.zakonyprolidi.cz/cs/1969-2).

40 V říjnu 2019 byly publikovány informace naznačující, že Středisko bezpečnostní politiky Fakulty sociálních věd Univerzity Karlovy vedené PhDr. Balabánem provádělo některé ne zcela standardní kroky, které nebylo schopné jednoznačně a transparentně vysvětlit (existovala např. stejnojmenná soukromá firma, do které plynuly některé finanční prostředky, které měly mířit na účty Karlovy univerzity; část z těchto peněz přicházela i od ambasády Čínské lidové republiky; PhDr. Balabán také vedl na FSV UK předmět o Číně, který byl financován čínskou ambasádou atd.). V reakci na tento stav byla ukončena pracovní smlouva PhDr. Balabána a jeho dalších dvou spolupracovníků ze Střediska bezpečnostní politiky s FSV UK. UK odhaduje výši jen finančních škod kolem pěti milionů korun (https://zpravy.aktualne.cz/domaci/univerzita-karlova-vazby-milos-balaban/r~5dc6cc54017811eab259ac1f6b220ee8/, https://www.respekt.cz/politika/za-odmenu-s-karlovou-univerzitou-zdarma-do-ciny, https://echo24.cz/a/Sifk9/horka-puda-na-univerzite-konflikt-mezi-akademiky-miri-k-eticke-komisi, https://archiv.ihned.cz/c1-66722060-policie-vysetruje-milionovou-skodu-na-karlove-univerzite?utm_source=mediafed & utm_medium=rss & utm_campaign=mediafed).

41 Americký Massachusetts Institute of Technology (MIT) akceptoval opakovaně částky v milionech USD od vlády Saúdské Arábie i přes protesty části akademické obce kvůli nevhodnosti dárce. Protestujícím vadilo zejména porušování lidských práv ze strany vlády Saúdské Arábie. V říjnu 2018, poté co došlo k vraždě novináře a oponenta saúdské vlády, Džamála Chásakdžího, byl MIT nucen pod tlakem veřejnosti neutracené peníze vrátit a čelil rozsáhlé veřejné kritice za akceptování finančních darů od takto problematických dárců (https://www.nytimes.com/2019/07/03/magazine/saudi-arabia-american-universities.html).

42 V srpnu 2018 byly publikovány informace o tom, že íránská hackerská skupina Cobalt Dickens zaútočila na 76 vysokých škol ve 14 různých státech, přičemž cílem tohoto útoku bylo porušit ochranu duševního vlastnictví a toto ukrást (https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html).

43 https://www.zakonyprolidi.cz/cs/2004-594

44 Šetřením bezpečnostních složek Velké Británie došlo ke zjištění, že na britských vysokých školách studovalo jen za posledních deset let přibližně 500 čínských vědců podílejících se aktuálně na čínském vojenském výzkumu, a to včetně oblastí, jako jsou technologie využitelné při stavbě stíhacích letounů, superpočítačů a balistických raket (https://www.thetimes.co.uk/article/security-services-fear-the-march-on-universities-of-beijings-spies-gv9pk3hzr).

45 Americký student čínského původu Si Jüe-Wang z Princetonské univerzity byl v červenci 2017 odsouzen během svého studijního pobytu v Íránu k deseti letům vězení za špionáž ve prospěch USA. Si Jüe-Wang se specializoval v rámci svého doktorského studia na období konce 19. a začátku 20. století a do Íránu jel kvůli výzkumu období královské dynastie Kádžár. Nejpravděpodobnějším důvodem k uvěznění studenta tak byla snaha Íránu získat rukojmí, které by mohl vyměnit za svoje občany vězněné v USA. O dva roky později, v prosinci 2019, si nakonec USA a Írán svoje vězně vyměnily a Si Jüe-Wang se dostal na svobodu (https://domaci.ihned.cz/c1-65801730-v-iranu-odsoudili-na-deset-let-americkeho-studenta-za-udajnou-spionaz-maskoval-ji-pry-vedeckou-praci, https://ct24.ceskatelevize.cz/svet/2998580-vedce-za-studenta-americane-a-iranci-si-ve-svycarsku-vymenili-vezne).

46 Např. cestovní doporučení Princetonské univerzity (https://informationsecurity.princeton.edu/intltravel).

47 Lotyšsko, VDD, Annual Report 2019 (str. 23, https://vdd.gov.lv/en/?rt=documents & ac=download & id=55).

48 Na podzim 2019 propukly na univerzitě v britském Sheffieldu nepokoje mezi studenty z Hong Kongu a Tchaj-wanu na straně jedné a studenty z pevninské Číny na straně druhé. Volená zástupkyně zahraničních studentů pocházející z Číny měla vyzvat další čínské studenty, aby hlásili čínským bezpečnostním složkám o hongkongských a tchaj-wanských studentech (https://thetab.com/uk/sheffield/2020/02/12/sheffield-university-hong-kong-chinese-students-sissi-li-42125).

49 Např. švédská příručka pro komunikátory přístupná v české i anglické verzi na stránkách CTHH (https://www.mvcr.cz/cthh/clanek/boj-proti-informacnim-vlivovym-aktivitam-prirucka-pro-komunikatory.aspx).

50 Podrobněji např. část Komunikace (str. 29–32) Metodiky koordinace měkkého cíle pro fázi po bezpečnostním incidentu (https://www.mvcr.cz/cthh/soubor/metodika-koordinace-mekkeho-cile-pro-fazi-po-bezpecnostnim-incidentu-aneb-jak-se-vyrovnat-s-nastalou-situaci-g-ben-david.aspx).

51 https://www.policie.cz/imapa.aspx

52 https://www.bis.cz/kontakty/

53 V březnu 2018 obvinilo americké ministerstvo spravedlnosti devět Íránců z rozsáhlé krádeže dat. Za krádeží stála mj. íránská firma Mabna Institute spolupracující s íránskými revolučními gardami (IRGC). Od roku 2013 útočníci opakovaně napadali IT systémy 144 amerických vysokých škol a 176 dalších vysokých škol ve 21 státech; celkem bylo odcizeno kolem 31 terabytů dat (https://www.timesofisrael.com/israeli-university-accounts-compromised-in-iran-hacking-scheme/).

54 Australian National University (ANU) oznámila v roce 2019, že se stala terčem hackerského útoku, při němž byly zcizeny informace obsahující osobní a bankovní údaje současných a minulých studentů a zaměstnanců za posledních 19 let, přičemž se odhadem může jednat o údaje až 200 000 osob (https://www.smh.com.au/politics/federal/anu-says-sophisticated-operator-stole-data-in-cyber-breach-20190604-p51ua9.html).

55 https://www.nukib.cz/download/vzdelavani/doporuceni/Admin%204.0%20brozura.pdf

56 https://www.govcert.cz/cs/informacni-servis/doporuceni/

57 https://nukib.cz/download/vzdelavani/rozcestniky/rozcestnik_metodici.pdf

58 https://www.nukib.cz/download/vzdelavani/doporuceni/NUKIB_doporuceni_uzivatele_a4_barva.pdf

59 https://www.govcert.cz/cs/informacni-servis/hrozby/

60 https://www.institutpraha.cz/kurzy/kyberneticka-bezpecnost/

61 V roce 2014 zaútočila íránská hackerská skupina známá jako Ajax Security Team na izraelské univerzity, přičemž cílila primárně na ty akademické pracovníky, kteří se věnují blízkovýchodním studiím a Íránu (https://www.ynetnews.com/articles/0,7340,L-4668686,00.html).

62 https://www.dni.gov/files/NCSC/documents/campaign/Recruitment.pdf

63 Lotyšsko, VDD, Annual Report 2019 (str. 10–11, https://vdd.gov.lv/en/?rt=documents & ac=download & id=55).

64 https://www.dni.gov/files/NCSC/documents/campaign/Espionage.pdf

65 https://securityawareness.usalearning.gov/itawareness/content/Block10/Introduction/page_0008.html

66 https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (str. 8)

67 https://kam.lt/download/53705/aotd%20gresmes%202016-en-el.pdf (str. 23–24, 26)

68 Pákistánský metalurgický inženýr Wasim Akram pracoval na programu pákistánských balistických raket. Pravidelně také létal do USA, kde se na University of New Mexico snažil získávat informace od lidí z amerických národních laboratoří Sandia a Los Alamos, které by mohl ve své práci využít. Wasim Akram začal ale být závislý na hazardu a dopustil se v USA blíže neurčeného drobného zločinu, který mu zpravodajská služba CIA výměnou za spolupráci pomohla zahladit. Od CIA dostal za poskytnuté informace několik stovek tisíc USD. Koncem roku 2019 byl Wasim Akram v Pákistánu popraven za špionáž ve prospěch CIA. (https://theprint.in/opinion/pakistans-spy-arrests-brigadier-kids-studied-in-us-doctor-bought-home-in--his-own-name/326871/).

69 ODNI, Human Targeting (https://www.youtube.com/watch?v=0eUVNV7ETyg & feature=youtu.be).

70 ODNI, Social Engineering (https://www.youtube.com/watch?v=FwbWOP-kZIw & feature=youtu.be).

71 Litva, National Threat Assessment – 2020 (str. 28, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf), dále např. ODNI, Know the Risk – Raise Your Shield: Human Targeting (https://www.youtube.com/watch?v=XpqOEniQK9U & feature=youtu.be).

72 https://www.hanford.gov/files.cfm/citravel.pdf

73 Litva, National Threat Assessment – 2020 (str. 33, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf), dále např. ODNI, Know the Risk – Raise Your Shield: Social Media Deception (https://www.youtube.com/watch?v=B9byyrX-_Rc).

74 https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020

75 https://www.dni.gov/files/NCSC/documents/campaign/Elicitation.pdf

76 https://securityawareness.usalearning.gov/itawareness/content/Block10/Introduction/page_0008.html

77 https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (str. 31–36)

78 Mezi takové informace může patřit např. rodinný stav a počet dětí, ale už ne to, kde pracuje Váš choť nebo kam chodí Vaše děti do školy. Z hlediska informování o Vaší práci je vhodné si např. vyhodnotit, které informace byste byli ochotni sdělit veřejně (např. do médií).

79 https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (str. 31–36)

80 ODNI, Human Targeting (https://www.youtube.com/watch?v=0eUVNV7ETyg & feature=youtu.be).

81 ODNI, Know the Risk – Raise Your Shield: Social Media Deception (https://www.youtube.com/watch?v=B9byyrX-_Rc).

82 https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Digitalfootprint.pdf.

83 https://cs-cz.facebook.com/about/privacy/update, https://help.twitter.com/en/safety-and-security/data-through-partnerships, https://policies.google.com/privacy#infocollect

84 https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/facebook-sel-s-pravdou-ven-az-do-vcerejska-byla-data-uzivatelu-jako-ve-vyloze-8922.

85 Uvědomte si, že útočník bude operovat mimo české zákony a pro takové úkony nebude potřebovat povolení soudu.

86 CSIS Physical Surveillance Unit – Recruiting Video (https://www.youtube.com/watch?v=DES9mJe1pM8).

87 https://vdd.gov.lv/en/useful/annual-reports/.

88 National Cybersecurity Alliance, Online Safety Basics (https://staysafeonline.org/stay-safe-online/online-safety-basics/, https://staysafeonline.org/resource/security-awareness-episodes/).

89 https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf.

90 ODNI, Know the Risk – Raise Your Shield: Human Targeting (https://www.youtube.com/watch?v=XpqOEniQK9U & feature=youtu.be).

91 https://www.eccouncil.org/ethical-hacking/

92 https://www.vaadata.com/blog/understanding-usb-attacks%EF%BB%BF/

93 https://hackinglethani.com/physical-hacking-with-usb/

94 ODNI, Know the Risk – Raise Your Shield: Spear Phishing(https://www.youtube.com/watch?v=X5P-VYxPNrk & feature=youtu.be).

95 https://informationsecurity.princeton.edu/intltravel

96 https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf.

97 FBI (https://www.fbi.gov/video-repository/newss-game-of-pawns/view, https://www.youtube.com/watch?v=Fw8ZorTB7_o).

98 ODNI, Threats to Public Wi-Fi Users (https://www.youtube.com/watch?v=pqX733zk04s & feature=youtu.be).

99 ODNI, Hotel Business Center (https://www.youtube.com/watch?v=fdqiPW4DrcM & feature=youtu.be).

100 ODNI, Know the Risk – Raise Your Shield: Travel Awarness (https://www.youtube.com/watch?v=6ZXYEdWPBYA & feature=youtu.be).

101 FBI (https://www.fbi.gov/video-repository/newss-game-of-pawns/view, https://www.youtube.com/watch?v=Fw8ZorTB7_o).

102 https://kam.lt/download/53705/aotd%20gresmes%202016-en-el.pdf (str. 31)

103 Litva, National Threat Assessment – 2020 (str. 33, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf).

104 https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (str. 18–23)

105 „If you see something, say something“ – mimo jiné stejnou zásadu uplatňují např. v USA a Velké Británii jako součást kampaně občanské bdělosti v boji proti terorismu.