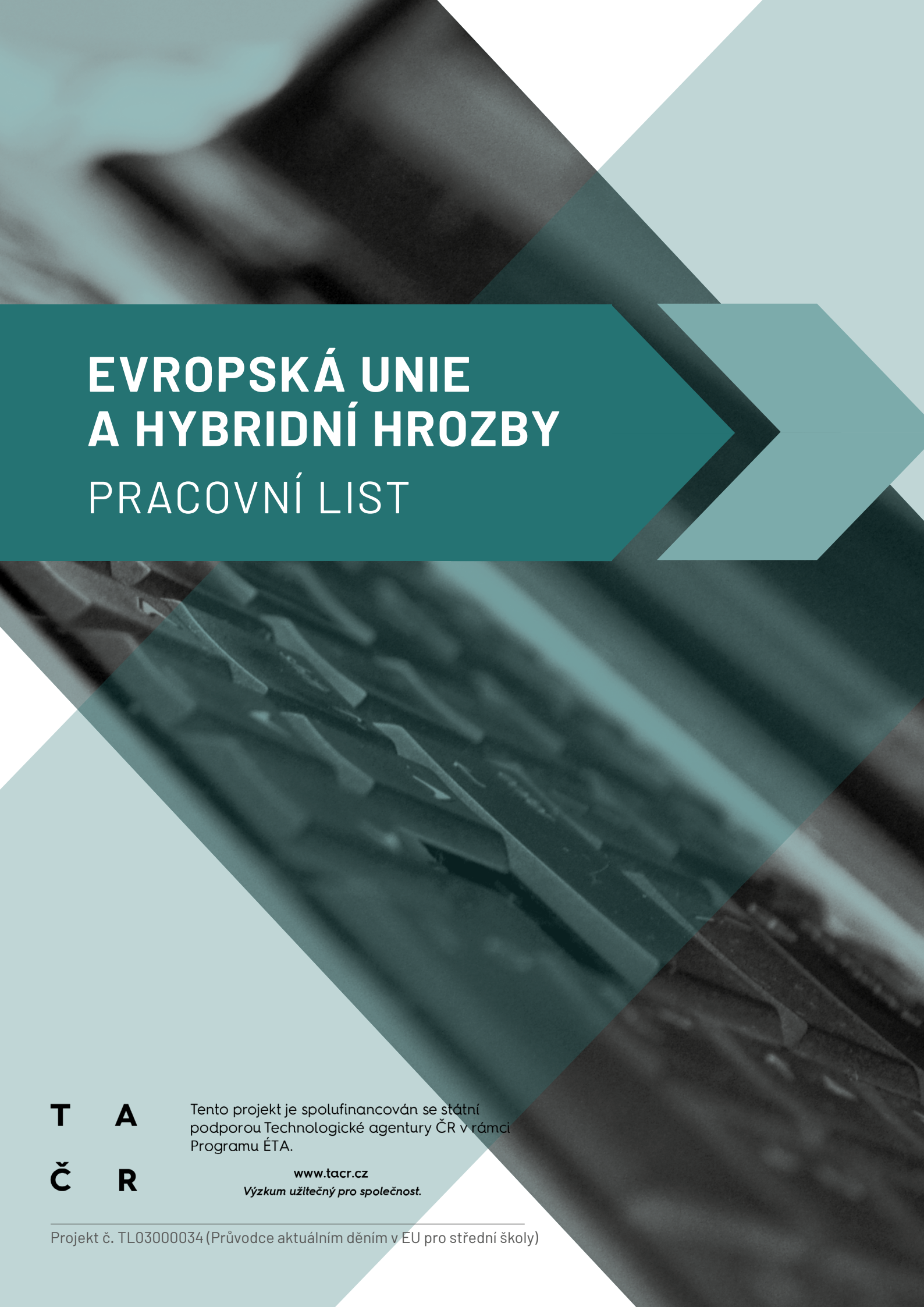


# EVROPSKÁ UNIE A HYBRIDNÍ HROZBY

## PRACOVNÍ LIST

T A
Č R

Tento projekt je spolufinancován se státní podporou Technologické agentury ČR v rámci Programu ÉTA.

www.tacr.cz
*Výzkum užitečný pro společnost.*

Projekt č. TL03000034 (Průvodce aktuálním děním v EU pro střední školy)

# EVROPSKÁ UNIE A HYBRIDNÍ HROZBY

S příchodem 21. století se významným způsobem změnila a rozšířila definice bezpečnosti a bezpečnostních hrozeb. Musíme stále více uvažovat i o jiných prostředcích a potenciálních hrozbách, než jsou zbraně či nasazení vojenských jednotek v otevřeném konfliktu. Různí státní, ale i nestátní aktéři (teroristické skupiny, aktéři organizovaného zločinu, soukromé armády apod.) využívají také nevojenských prostředků, jejichž účinnost se často prokáže být minimálně stejně velká. Dochází k využívání různých ekonomických a finančních nástrojů, ale i moderních informačních technologií apod. Cílem je zasáhnout existující slabiny a zranitelná místa protivníka. K takovým slabinám může patřit např. přílišná závislost na určitých energetických zdrojích či dodavatelích, ale také napětí a polarizace ve společnosti, které pomáhá posilovat například cílené šíření nepravdivých informací. Cílem takových útoků, které využívají nevojenské prostředky, bývá destabilizovat ekonomickou, politickou i sociální situaci a ve výsledku přispět ke zhroucení stávajícího systému.

**Úkol. Doplňte slova:**

*Ruské federace; „hybridní hrozby"; liberální; Krymského poloostrova; Ukrajině; psychologických; vojenský konflikt; virtuálním světě; kybernetické útoky*

Pod termínem ..... se toho skrývá hodně a pravdou je, že ani vědci jej nejsou v dnešní době schopni bez problémů definovat. Do širšího povědomí se dostal po anexi ukrajinského ..... ..... v roce 2014. Tehdy to bylo označení pro ruské působení, které má za cíl rozložit ..... a demokratické hodnoty západních společností a procesy (např. volby) a způsobit v nich rozkol. Cílem bylo vytvořit část společnosti sympatizující s ruským politickým režimem, podkopat celkovou důvěru v instituce a ztížit rozhodovací procesy (což je problém zejména v krizi, kdy je třeba jednat rychle). Nicméně prakticky se nejedná o nový fenomén, podobné snahy o všemožné pokoření protivníka můžeme sledovat v celé lidské historii a netýkaly se pouze působení ..... či předtím SSSR. Díky legislativním a jiným snahám se dnes tomuto působení EU, její členské státy i další demokratické státy snaží bránit. Hybridní hrozby jsou vnímány jako závažné riziko, mohou totiž přerůst i ve ....., jak to vidíme na ..... od roku 2014 a zejména od února 2022.

Konkrétně si můžeme pod pojmem hybridní hrozby představit nepřeberné množství jak vojenských, tak i nevojenských (....., ekonomických, politických a jiných) prvků. Patří mezi ně například i dezinformace, podněcování radikalizace (např. určitých skupin ve společnosti či jednotlivců), ..... ....., psychologické působení (operace), propaganda apod. Působit mohou tyto hrozby jak ve skutečném, tak i ve ..... V kyberprostoru je toto působení pro útočníka poměrně jednodušší, proto jej hojně využívá, a proto bude i v tomto pracovním listu použit jako hlavní pojící linka mezi jednotlivými typy hrozeb.

# SEKCE A – DEZINFORMACE A DALŠÍ OPERACE PODPOŘENÉ AKTIVITAMI V KYBERPROSTORU

Hybridní hrozby, či hrozby obecně související s kyberprostorem, si můžeme rozdělit do dvou skupin: „cyber--enabled" (tedy hrozby, které ke svému vzniku nutně kybernetické nástroje a prostor nepotřebují, ale jejich škodlivé dopady jsou jimi podpořené, umocněné) a „cyber-dependent" (hrozby, které by bez kybernetických nástrojů a on-line prostoru nemohly být realizovány nebo by byly velmi neúčinné). Pod první kategorií se skrývají tradičnější hrozby jako je propaganda a dezinformace, organizovaný zločin, vydírání apod., které díky on-line nástrojům, jako jsou sociální sítě, získávají na síle, ale nutně je nepotřebují. Druhou kategorii, tedy hrozby, které ke své realizaci kyberprostor potřebují (hackerské útoky apod.), si představíme v sekci B.

## 1. Dezinformace, konspirace a psychologické operace

Konspirační teorie mohou vznikat buď samovolně (někdo je může vymyslet například z nedostatku jiné aktivity), nebo s konkrétním úmyslem. Výsledkem takové záměrné dezinformační aktivity pak může být např. neférové odrazení voličů nějaké strany nebo člověka. Důsledky ale mohou být i ještě závažnější, například když se člověk, který záměrně lživé informaci uvěřil, pokusí o násilný čin. Příkladem může být tzv. Pizzagate aféra, k níž došlo v USA, kde byly šířeny nepravdivé informace o tom, že v zemi vládne skupina lidí z Demokratické strany, která znásilňuje děti ve sklepích pizzerií. Jeden z občanů dokonce s útočnou puškou v ruce do jedné z pizzerií vtrhl a chtěl údajné oběti osvobodit. Falešný a zavádějící obsah ale může být šířen i bez nekalého úmyslu a nezáměrně, pak se jedná o tzv. misinformace. Jejich dopady jsou ale stejné.

**a) Někdy jsou falešné zprávy, které se nezakládají na pravdě (fake news), velmi těžko odlišitelné od skutečnosti. V následujícím úkolu jsou uvedeny 4 informace, z nichž 2 se zakládají na skutečnosti a 2 jsou tzv. fake news. Dokázali byste je rozeznat a přiřadit jim následující označení: VYMYŠLENO/SKUTEČNOST?**

A. Evropská lingvistická rada spadající pod EU jednohlasně rozhodla, že ruší písmeno Ř. Důvodem je skutečnost, že téměř nikdo toto písmeno v Evropě nepoužívá a pro každého, kdo neovládá češtinu, je jeho výslovnost extrémně obtížná. ☐ VYMYŠLENO ☐ SKUTEČNOST

B. Členem Evropské komise se může stát pouze „dobrý Evropan". Od vstupu v platnost tzv. Lisabonské smlouvy jsou členové Evropské komise vybíráni nejen podle způsobilosti vykonávat funkci eurokomisaře, ale také na základě jejich „evropanství". ☐ VYMYŠLENO ☐ SKUTEČNOST

C. Když 25. března 1957 státníci zastupující 6 zakládajících států Evropského hospodářského společenství podepisovali smlouvu o EHS, podepisovali namísto smlouvy pouze prázdné papíry. Vytištěný finální text tzv. Římské smlouvy totiž večer před ceremoniálem vyhodily uklízečky. ☐ VYMYŠLENO ☐ SKUTEČNOST

D. Hrozí zvýšení cen vepřového masa. To proto, že vejde v platnost nová směrnice EU, podle níž se pro chovatele prasat zavádí povinnost pořídit prasnicím hračky. Pokud se totiž prase nebude starat jen samo o sebe nebo o mláďata, bude tak mnohem klidnější, což následně povede k přibývání na váze a menší ztrátovosti selat. ☐ VYMYŠLENO ☐ SKUTEČNOST

V České republice se dezinformace objevují poměrně často. Například těsně před 2. kolem prezidentské volby 2023 se na sociálních sítích objevila lživá zpráva, že kandidát Petr Pavel zemřel. Tyto falešné zprávy pak velmi často podporují určité skupiny s cílem podpořit zvolení lidí, kteří by pak prosazovali pro ně výhodný typ politiky u nás i v EU. Unie se však tomuto snaží bránit za pomoci tzv. fact-checkingových kampaní (uvádění dezinformací na pravou míru), legislativních kroků (např. zakázání propagandistických médií) apod. Tím, že se tyto obranné snahy objevují na celounijní platformě, mají mnohem větší sílu a dopad, než kdyby je aplikovaly členské státy samostatně.

Dezinformace souvisejí velmi úzce také s psychologickými operacemi. Dobře to ukazuje fakt, že se v dnešní době čím dál více smazává rozdíl mezi civilním a vojenským světem. Psychologické operace jsou totiž jeden z prostředků vojenského působení na nepřítele a dezinformace pod tuto činnost spadají. Dezinformace ke svému vzniku on-line prostor nutně nepotřebuje, ale nástroje jako řetězové e-maily či tzv. trollí farmy (skupiny státem či jinými aktéry podporovaných internetových „trollů", kteří mají za úkol psát on-line komentáře či přispívat do internetových diskusí za účelem manipulace) významně pomáhají k jejich šíření a zesilují jejich účinek. Důležitým „pomocníkem" pro možné šíření dezinformací jsou i samotné sociální sítě a jejich fungování pomocí algoritmů, které uživateli de facto „vybírají" obsah podle předchozích preferencí.

**b) Prohlédněte si karikaturu a okomentujte ji. Víte, co jsou to řetězové e-maily? Dostali jste někdy takový e-mail?**


## 2. Důsledky dezinformací a dalších aktivit v kyberprostoru

Kromě lidí, kteří dezinformacím prostě uvěří (at' již v důsledku informační izolovanosti nebo toho, že si informace neověří z jiných zdrojů) se mohou dezinformacemi a konspiračními teoriemi radikalizovat i mnohem nebezpečnější jedinci a pak i celé segmenty společnosti. V prvním případě se může jednat o tzv. osamělé vlky – teroristy. Mohou k nim patřit islamisté, ale také rasisté či hnutí incel (termín „incel" je složeninou slov *involuntary celibate, tedy nedobrovolně v celibátu.* Jedná se často o frustrované mladé muže, nepřátelské vůči ženám, kteří mohou svou frustraci vybíjet i násilnými, dokonce teroristickými činy). K radikalizaci těchto lidí může dojít z nejrůznějších důvodů (např. jejich psychologických predispozic) pouhou konzumací dezinformačních, propagandistických či konspiračních obsahů na internetu.

Typickým výsledkem práce dezinformátorů je pak prohloubení rozkolu mezi velkými částmi společnosti. Např. při rasových protestech v USA z ruské strany přicházely podněty k založení jak skupin „Black Lives Matter", tak i „White Lives Matter", stejně jako snahy stavět je proti sobě, což vyústilo v masové nepokoje po celých Spojených státech. V ČR se tyto techniky také používají – stačí se podívat do diskuzních sekcí na sociálních sítích nebo zpravodajských webech. To vše pak přispívá k šíření strachu a nenávisti ve společnosti a nutně i k erozi demokratických hodnot a demokracie samotné. Strach a nenávist jsou totiž velmi silnými motivátory a lidé pod jejich vlivem mají tendenci uchylovat se pod „ochranu" politických subjektů slibujících například mír a bezpečí za použití jednoduchých řešení, která ale nemohou v moderní a komplexní společnosti fungovat. Politici nabízející jednoduchá řešení jsou často nazýváni populisty.

a) Přiřaďte termíny k jejich definicím

| | |
|---|---|
| **Cyber-dependent hrozby** | Velmi široký soubor nástrojů psychologického, ekonomického, politického, diplomatického aj. působení proti nepříteli, které se velmi často „přelévá" mezi on-line i off-line světem. |
| **Hybridní hrozby** | Hrozby, které ke svému vzniku nutně kybernetické nástroje a on-line prostor nepotřebují, ale tyto nástroje zesilují jejich škodlivý účinek. |
| **Dezinformace** | Hrozby, které by bez kybernetických nástrojů a on-line prostoru nemohly být realizovány nebo by byly velmi neúčinné. |
| **Cyber-enabled hrozby** | Škodlivý obsah šířený s nekalým úmyslem, který může být politicky i ekonomicky škodlivý pro společnost a narušit fungování politického systému, ekonomických struktur apod. |
| **Osamělí vlci** | Dezinformace, k jejichž šíření ale dochází bez nekalého úmyslu. |
| **Misinformace** | Jednotlivci radikalizovaní na internetu (buď sami, nebo na dálku teroristickou organizací) a plánující a/nebo uskutečňující teroristické útoky. |

## 3. Co EU dělá proti dezinformacím?

EU považuje boj proti dezinformacím a hybridním hrozbám obecně za jednu ze svých bezpečnostních priorit. Spolupracuje v tomto ohledu se soukromým sektorem, zejména s platformami sociálních sítí na označování a v krajním případě i odstraňování dezinformačního a misinformačního obsahu. EU také podporuje fact-checkingové organizace a rozvoj občanské společnosti a vzdělávání v této oblasti. Významným aktérem pro boj s dezinformacemi v rámci EU je její „ministerstvo zahraničí" – Evropská služba pro vnější činnost (ESVČ, ang. ESVA). Její projekt EUvsDisinfo v 15 jazycích analyzuje ruské dezinformační snahy na půdě EU a za pomoci článků a reportů se je snaží odhalovat a zneškodňovat. Zde je ale třeba podotknout, že problematickým aktérem v této oblasti není pouze Rusko, ale i např. Čína a Írán. V rámci ESVA je vyčleněna pracovní skupina East Stratcom, která má za cíl posilování evropských hodnot v zemích východní Evropy, které jsou k ruským narativům náchylnější. Dále ESVA spravuje v rámci Akčního plánu proti dezinformacím i systém včasného varování, který propojuje instituce členských zemí, univerzity, mezinárodní partnery a další organizace za účelem včasného zachycení dezinformačních narativů a rychlé společné akce k jejich potlačení. Dalším významným strategickým dokumentem EU je Kodex zásad boje proti dezinformacím z roku 2022.

a) **Evropská unie čelí trendu konspiračních teorií např. i tím, že spolu s UNESCO vyvinula webovou stránku, která veřejnosti pomáhá rozlišit dezinformační přístup jednotlivců, skupin i médií. Vyhledejte tuto stránku Evropské komise (do vyhledávače na internetu vepište „Jak rozpoznat konspirační teorii?"; https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_cs). Na základě informací z těchto stránek a textu v Sekci A pracovního listu doplňte tabulku.**

| Jak poznat konspirační teorii? | Jak se proti konspiracím bránit? | Jak bojuje proti dezinformacím EU? | Proč to EU dělá? Jaký má boj proti dezinformacím význam? |
|---|---|---|---|
| | | | |

b) **S pomocí zmíněné stránky „Jak rozpoznat konspirační teorii?" vyberte správné odpovědi o konspiračních teoriích a dezinformacích (může být více správných odpovědí).**

Autor konspirace:

A. Svou „pravdu" prezentuje jako jedinou platnou a okořeňuje ji emotivními historkami a obrázky.
B. Vyjmenovává ověřitelná fakta a důkazy z vědeckého nebo akademického výzkumu.
C. Má příslušné vzdělání v oboru a je na toto téma uznávanou kapacitou.
D. Se prohlašuje za odborníka, ale není spojen s žádnou uznávanou organizací nebo institucí.
E. Démonizuje toho, kdo podle něj za údajným tajným spiknutím stojí.

Zdroj konspirace:

A. Byl citován v několika renomovaných médiích.
B. Není jasný, transparentní.
C. Správnost zdroje a příslušných tvrzení dokládají nezávislé internetové stránky, které se zabývají ověřováním faktů.
D. Uváděné informace potvrzuje mnoho vědců nebo akademických pracovníků.

Při střetu s konspirační teorií a jejími přívrženci:

A. Když narazím na sociální síti na konspiraci, šířím ji dál, aby byla legrace.
B. Když mluvím s přívržencem konspirace, je vhodné vést otevřenou diskusi, kde je možné se na cokoli zeptat.
C. Když mluvím s přívržencem konspirace, nebudu ho zesměšňovat, ale budu se snažit pochopit, proč daná osoba věří tomu, čemu věří (možná je i vystrašená, nebo je v obtížích).
D. Při komunikaci s přívrženci konspirace je vhodné (nekonfrontačně) poukázat na to, že se jedná o chybné informace.
E. Při komunikaci s přívržencem konspirace je vhodné naléhat, aby se šířením nesmyslů přestal.
F. Je pravděpodobné, že přívrženec věří více než jedné konspirační teorii.

# SEKCE B – KYBERNETICKÉ ÚTOKY A KYBERBEZPEČNOST

## 1. Co jsou to kybernetické útoky a proč jsou nebezpečné?

a) Doplňte slova:

*politický a diplomatický nátlak; botnet; počítačů; tzv. DDoS útoky; zkolabuje; kritickou infrastrukturu; ekonomiku; člověk; plynovody*

V této sekci se podíváme blíže na tzv. cyber-dependent hrozby – tedy ty, které by bez kyberprostoru a ..... nemohly existovat. Existuje jich nepřeberné množství a jednotlivé techniky se dají nekonečně kombinovat mezi sebou a také s dalšími hybridními hrozbami. Například ..... lze kombinovat s tzv. DDoS útoky na kritickou infrastrukturu apod.

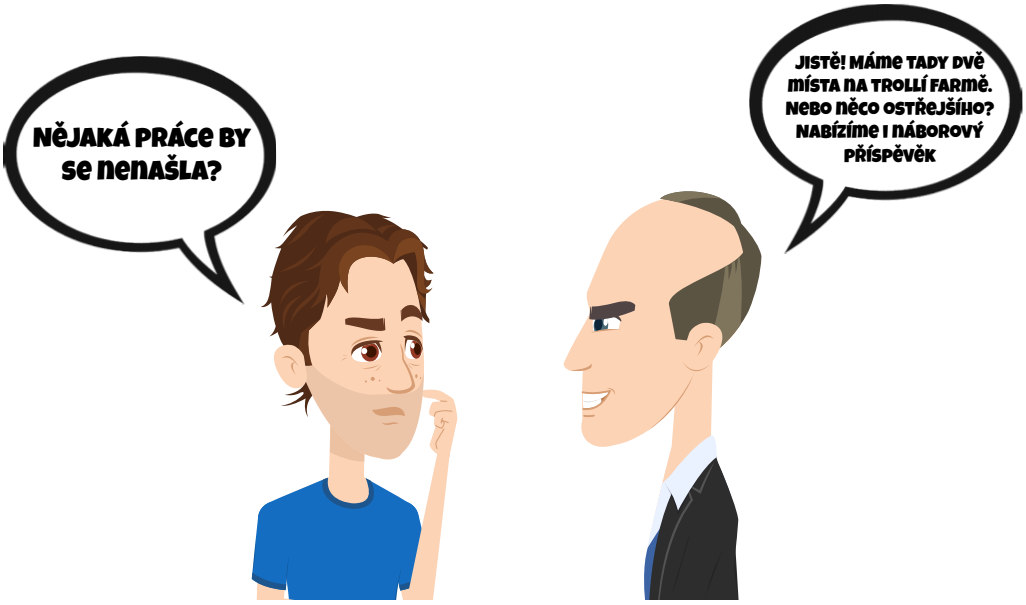
Nejslabším článkem v oblasti kybernetické bezpečnosti je ..... Největší útoky, úniky dat apod. velmi často začínají tím, že kompromitují nějakého zaměstnance např. tzv. phishingovým mailem obsahujícím odkaz, který se tváří jako legitimní požadavek na přihlášení do systému. Ve skutečnosti je to ale podvrh (někdy velice přesvědčivý) a přihlašovací údaje putují po zadání přímo útočníkovi. Ten tak s kompromitovaným systémem může dělat, co se mu zlíbí, např. z něj vyvést citlivá data nebo si z vícero takovýchto zařízení postaví „armádu" – tzv. ....., se kterým pak může provádět ..... .

Princip DDoS (Distributed Denial of Service) je velmi jednoduchý – obrovským množstvím dotazů se zahltí server a ten pod takovým náporem ..... i pro legitimní uživatele a ti pak nemohou využít např. stránky internetového bankovnictví. V dostatečné intenzitě a trvání to může poškodit i ..... celého státu (např. v roce 2007 vlivem takových útoků přišlo Estonsko odhadem až o 1–2 % svého HDP). Tyto útoky pak mohou být vedeny třeba i na ..... státu (elektrárny, čističky odpadních vod, ....., ropovody apod.). Takto například ruští hackeři vyřadili v roce 2015 (rok po anexi Krymu) z provozu elektrárnu zásobující statisíce lidí, a to v zimě, kdy jsou domácnosti na dodávkách energií často i životně závislé.

## 2. (Organizovaný) kyberzločin

Kromě státních aktérů a soukromého sektoru využívají kyberprostor samozřejmě i zločinci, od jednotlivců až po organizované skupiny. Vyplatí se to totiž. Orgány činné v trestním řízení dopadnou a usvědčí pouze jednotky procent pachatelů, zatímco na druhou stranu jsou zde možnosti výdělku velkého množství peněz. Většinovým způsobem této trestné činnosti je ransomware, tedy vyděračský malware. Ten po kompromitaci (průniku) systém či zařízení uzamkne a zašifruje a za odemčení požaduje výkupné (nejčastěji v kryptoměnách). Častým cílem jsou nemocnice, kde jsou počítače životně důležité a jejich uzamčení může celé zařízení i na dny ochromit. Dalším typem pak může být spyware, tedy špionážní software, který je tak možno považovat v širším smyslu i za nástroj hybridního působení proti jiným státům. Dalším příkladem jsou státem organizované zločinecké aktivity, od pašování drog a lidí po kybernetické útoky, které mají v Severní Koreji za úkol přivést do této uzavřené země valuty a devízy pro financování programu jaderných zbraní a dalších režimních aktivit. V oblasti kyberzločinu bohužel západní policejní a justiční složky zaostávají a řešení tohoto problému je velmi obtížné.

a) Prohlédněte si virtuální příběh a diskutujte o nebezpečí takového podnikání.




## 3. Ochrana osobních údajů a co EU dělá pro její posílení

Kybernetických útoků a jejich kategorií je obrovské množství, proto zde zmíníme spíše už jen zajímavosti a relativně nové oblasti opatření, která mohou přinést jak užitek, tak ale i zranitelnost. První je tzv. kapitalismus dohledu *(surveillance capitalism),* což je odborný termín pro ekonomický model Big Tech společností jako je Facebook, Amazon, Google apod., které stojí na tzv. extrakčním imperativu dat. Jejich tržní hodnota se totiž z velké části odvíjí od toho, kolik dat jsou schopni ze svých uživatelů získat a jak je přetaví v zisk. To vede jak k neetickému požadování citlivých údajů od lidí, tak i ke společenským hrozbám. Současně to znamená, že informace, které se k uživateli dostávají, jsou součástí algoritmem předvybrané sestavy, ale nikoliv odrazem reálného světa. Příkladem zneužití sítí může být nelegální přístup k datům poskytnutým třetím stranám, konkrétně firmě Cambridge Analytica, která tato data zkombinovala s poznatky z vojenské oblasti psychologických operací. Na tomto základu pak vytvořila personalizované reklamy (tzv. microtargeting) s cílem ovlivnit volby a referenda po celém světě. Je těžké jednoznačně změřit reálný vliv, který Cambridge Analytica na volby v nejrůznějších zemích měla (např. zda by bez jejího přičinění vyhrál prezidentské volby v USA v roce 2016 Donald Trump). Nicméně její případ dokazuje, že poměrně velké masy lidí jsou ovlivnitelné za využití informací, které o sobě jednotlivci zveřejňují např. na sociálních sítích.

Postup EU je v případě ochrany dat unijních občanů jedním z nejúspěšnějších na světě (viz pracovní list Moc a vliv). Za pomoci poměrně striktní legislativy, zejména pak nařízení o ochraně osobních údajů (GDPR), omezuje mocenskou převahu Big Tech společností ve prospěch jednotlivců (vzpomeňme např. tzv. právo být zapomenut v internetovém prostředí, tedy právo nebýt na standardní dotaz vyhledán internetovým vyhledávačem). Obecně pak proti kybernetickým hrozbám funguje na celounijní úrovni úřad ENISA, který se zabývá vážnými kybernetickými incidenty, pomáhá členským státům s digitalizací veřejné správy a v neposlední řadě koordinuje národní úřady ve společném boji proti kyberkriminalitě a útokům (u nás tuto funkci plní NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost). EU úzce spolupracuje i s NATO, kde problematiku hybridních a kybernetických hrozeb řeší hlavně centra excelence ve Finsku a v Estonsku.

a) Na základě četby částí 2 a 3 a vlastní zkušenosti doplňte následující tabulku a diskutujte.

| Jaká opatření EU podniká pro posílení kyberbezpečnosti a proti kyberzločinu? | Jaká jsou pozitiva a negativa těchto opatření? | Setkali jste se sami ve svém životě s příklady ohrožení vaší kyberbezpečnosti (např. snahami o vylákání osobních údajů přes internet, výhrůžkami apod.)? |
|---|---|---|
| | | |

b) Na základě předchozí četby v celé sekci B přiřaďte termíny k jejich definicím.

*Kapitalismus dohledu; Phishing; Spyware; DDoS útok*

| | |
|---|---|
| | Kybernetický útok zahlcující server nebo zařízení velkým množstvím požadavků s cílem dočasně omezit jeho fungování. |
| | Manipulativní snaha (prostřednictvím e-mailu, sms = tzv. smishing, hovoru = tzv. vishing) vylákat z oběti přístupové údaje k nějaké službě či zařízení. |
| Botnet | Doslova síť robotů, tedy napadených zařízení, které útočník zcela nebo zčásti ovládá a používá je zpravidla k dalším útokům (např. DDoS). |
| | Společensky škodlivý byznysový model, ve kterém jsou uživatelé de facto ponížení na objekty, které jsou monetizovány (slouží ke generaci zisku) např. prodejem cílených reklam. |
| Ransomware | Typ malwaru (škodlivého softwaru), který má za cíl uzamknout zařízení či systém a pro odemčení vydírat oběť k zaplacení výkupného. |
| | Typ malwaru (škodlivého softwaru), který má za cíl (ideálně nepozorovaně) ukrást a vyvést z cílového systému citlivá data nebo know-how. |

# SEKCE C – UMĚLÁ INTELIGENCE A HYBRIDNÍ HROZBY

## 1. Umělá inteligence (AI) a kvantové počítače

**a) Doplňte slova:**

*tzv. deep fakes; kvantové počítače; chatboty; umělá inteligence; informatiky*

Zcela nové možnosti v oblasti hybridních hrozeb přináší také ..... Jedná se o obor ..... zaměřený na tvorbu takových systémů, které jsou schopné samostatně řešit i velmi komplexní úlohy, jako je zpracování obrazu, psaného textu, či dokonce mluveného jazyka, jsou schopné samostatného plánování a řízení a zpracovávají přitom velké objemy dat. Pro výše popsané hrozby není umělá inteligence nezbytně nutná, nicméně může jejich působení značně zesílit. Příkladem jsou ....., tedy dezinformační prostředek v podobě upravených videí, obrázků, zvukových stop apod., které jsou ale díky AI na takové úrovni, že není téměř možné rozpoznat rozdíl od skutečnosti. K dispozici jsou také např. ....., tedy nástroje na autonomní generování obsahu a textů (jako je ChatGPT3, který dokáže porozumět psanému textu a přesně odpovídat na dotazy, či pokročilejší GPT4).

Stále jsme ale poměrně daleko od tzv. obecné umělé inteligence, tedy skutečně autonomní entity. ..... ..... by se svou mnohonásobně vyšší výkonností v budoucnu mohly tohoto dosáhnout, ale těžko říci, kdy tato chvíle nastane.

**b) Podívejte se na deep fake video a diskutujte o něm:** https://www.youtube.com/watch?v=oxXpB9pSETo&ab_channel=DiepNep (video můžete najít také po zadání pojmu „This is not Morgan Freeman" na YouTube).
**Co byste poradili EU, jak by mohla čelit deep fakes a zneužívání umělé inteligence?**

**c) Úkoly k zamyšlení:**

Popovídejte si s jedním z nejpokročilejších AI modelů současnosti nebo si nechte napsat vědeckou práci (budeme moci věřit jejím závěrům?): https://chat.openai.com/ (web můžete najít prostřednictvím vyhledávače za pomocí pojmu „ChatGPT").

Jak vidíte svoji budoucnost ve světě, v němž budeme mít možnost využívat schopnosti umělé inteligence? Jaká bude úloha člověka v takovém světě? Můžete se inspirovat mimo jiné následujícím citátem Karla Čapka:

> *Jak budou jednou Roboti silnější než lidstvo, nastane tohleto, musí to nastat, víme? ... a my jsme se postarali, aby to bylo co nejdřív ... Celý svět chtěl mít své Roboty ... my jsme se jen vezli na té lavině poptávky, a přitom jsme žvanili – o technice, o sociální otázce, o pokroku, o moc zajímavých věcech. Jako by ty řečičky nějak řídily, kudy se to má valit. Zatím to všechno běželo vlastní tíhou, rychleji, rychleji, pořád rychleji...*
>
> *Karel Čapek: R.U.R. (1920)*

https://doi.org/10.5817/CZ.MUNI.O280-0333-2023-2