EVROPSKÁ UNIE A HYBRIDNÍ HROZBY

METODIKA K PRACOVNÍMU LISTU

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)

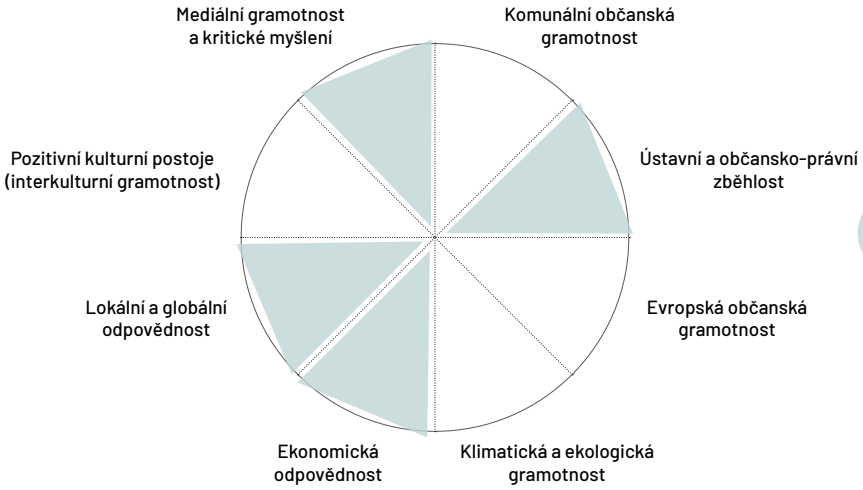
METODICKÝ LIST K PRACOVNÍMU LISTU EVROPSKÁ UNIE A HYBRIDNÍ HROZBY

Téma	Evropská unie a hybridní hrozby
RVP G	**Občanský a společenskovědní základ** MEZINÁRODNÍ VZTAHY, GLOBÁLNÍ SVĚT » uvede příklady činnosti některých významných mezinárodních organizací a vysvětlí, jaký vliv má jejich činnost na chod světového společenství, zhodnotí význam zapojení ČR ČLOVĚK VE SPOLEČNOSTI » objasní podstatu některých sociálních problémů současnosti a popíše možné dopady sociálně-patologického chování na jedince a společnost OBČAN VE STÁTĚ » uvede příklady, jak může občan ovlivňovat společenské dění v obci a ve státě a jakým způsobem může přispívat k řešení záležitostí týkajících se veřejného zájmu **Dějepis** MODERNÍ DOBA II – SOUDOBÉ DĚJINY » vymezí základní problémy soudobého světa a možnosti jeho dalšího vývoje **Člověk a svět práce** PRACOVNĚPRÁVNÍ VZTAHY » volí bezpečné pracovní postupy šetrné k životnímu prostředí, používá adekvátní pracovní pomůcky FINANCE » využívá moderní formy bankovních služeb, včetně moderních informačních a telekomunikačních technologií, ovládá způsoby bezhotovostního platebního styku **Informatika** DATA, INFORMACE A MODELOVÁNÍ » odhaluje chyby a manipulace v cizích interpretacích a závěrech DIGITÁLNÍ TECHNOLOGIE » chrání digitální zařízení, digitální obsah i osobní údaje před poškozením či zneužitím s vědomím změn v technologiích, které ovlivňují bezpečnost **Český jazyk a literatura** LITERÁRNÍ KOMUNIKACE » postihne smysl textu, vysvětlí důvody a důsledky různých interpretací téhož textu, porovná je a zhodnotí, odhalí eventuální dezinterpretace textu **Geografie** SOCIÁLNÍ PROSTŘEDÍ » lokalizuje na politické mapě světa hlavní aktuální geopolitické problémy a změny s přihlédnutím k historickému vývoji **Výchova ke zdraví** OCHRANA ČLOVĚKA ZA MIMOŘÁDNÝCH UDÁLOSTÍ » rozhodne, jak se odpovědně chovat při konkrétní mimořádné události

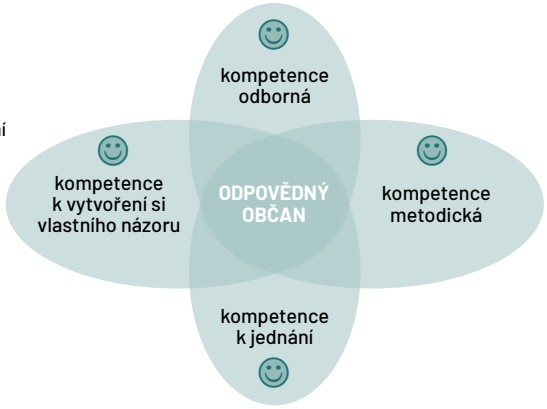
	Průřezová témata **Výchova k myšlení v evropských a globálních souvislostech** PL pomáhá žákům: » uvažovat a nacházet řešení problémů a konfliktů s ohledem na historickou zkušenost Evropy a jiných částí světa » orientovat se v neznámém prostředí a mezinárodních situacích » vnímat a hodnotit lokální a regionální jevy a problémy v širších evropských a globálních souvislostech » vytvořit si na základě osvojených informací vlastní názor, umět ho vyjádřit a obhajovat ho **Mediální výchova** V oblasti postojů a hodnot má průřezové téma žákovi pomoci: » rozvíjet kritický odstup od podnětů přicházejících z mediálních produktů (tedy rozvíjet schopnost přijímat a zpracovávat mediální produkty s vědomím toho, jak jsou konstruovány a s jakým komunikačním záměrem jsou nabízeny na trhu)
RVP SOV	**Občanský vzdělávací základ / Společenskovědní vzdělávání** ČESKÁ REPUBLIKA A SVĚT » charakterizuje soudobé cíle EU a posoudí její politiku SOUDOBÝ SVĚT A ČESKÁ SPOLEČNOST NA PRAHU 21. STOLETÍ » analyzuje vybraný problém české společnosti z hlediska médií a jiných zdrojů » charakterizuje konflikty a místa napětí v současném světě **Průřezové téma** **Člověk/občan v demokratické společnosti** Žáci jsou vedeni k tomu, aby: » hledali kompromisy mezi osobní svobodou a sociální odpovědností a byli kriticky tolerantní » byli schopni odolávat myšlenkové manipulaci **Obsah tématu** » masová média a rozvíjení mediální gramotnosti žáků
Klíčová slova	Konspirace, dezinformace, kybernetické hrozby, hybridní hrozby
Cíl vyučovací jednotky	Adekvátně reagovat na hybridní hrozby současnosti
Pracovní materiály, pomůcky	Pracovní list, internet
Způsob práce	Čtení textů, obrázků, karikatur s porozuměním, diskuse, práce s internetem
Organizační forma práce	Individuální, frontální, skupinová
Časová dotace	2–3 h

Zdroj: Doslovně převzato (a částečně upraveno) z: Rámcové vzdělávací programy pro gymnázia (https://www.edu.cz/rvp-ramcove-vzdelavaci-programy/ramcove-vzdelavaci-programy-pro-gymnazia-rvp-g/) a Rámcové vzdělávací programy středního odborného vzdělávání (https://www.edu.cz/rvp-ramcove-vzdelavaci-programy/ramcove-vzdelavaci-programy-stredniho-odborneho-vzdelavani-rvp-sov/).

Které občanské kompetence lekce rozvíjí?



Zdroj: LESŇÁK, Slavomír, a kol. *Rozvíjení personální, sociální a občanské kompetence učitelů, studentů a žáků.* Brno: Masarykova univerzita, 2020, s. 46.



Zdroj: ŠTĚRBA, Radim, a kol. *Kompetence pro odpovědné občanství. Příspěvek do diskuze o revizi rámcových vzdělávacích programů.* Praha: Nakladatelství Jalna, 2018, s. 7. Diagram autoři převzali od rakouských autorů: KRAMMER, Reinhard, a kol. *Kompetenzorientierte Politische Bildung*. Innsbruck, Bozen, Wien: Studien-Verl., 2008, s. 6.

Odborná kompetence: které výstupy odborné kompetence PL umožňuje a rozvíjí? Žák:
rozliší každodenní jazyk od jazyka odborného
zná a dokáže nakládat s kategoriemi a koncepcemi, které souvisí a jsou nutné pro politiku

Metodická kompetence: které výstupy metodické kompetence PL umožňuje a rozvíjí? Žák:
rozpozná závislost výsledku na způsobu získávání dat
rozpozná a staví se kriticky k analýzám dat daných problémů a k použitým kritériím vyhodnocování

Kompetence k vytvoření si vlastního názoru: které výstupy kompetence k vytvoření si vlastního názoru PL umožňuje a rozvíjí? Žák:
prověřuje předložené politické názory s kompatibilitou lidských práv
dotazuje se na závislost kontroverzních postojů při hledání politického rozhodnutí na předurčených ekonomických, sociálních, náboženských a kulturních zájmech
rozlišuje podložené politické názory od názorů, které nejsou podloženy a jsou emočně zabarvené, a od politických předsudků
prověřuje předložené politické názory s kompatibilitou lidských práv
ověřuje informace, na nichž zakládá vlastní názory, jestli jsou kvalitativně a kvantitativně dostačující a relevantní

Kompetence k jednání: které výstupy kompetence jednání PL umožňuje a rozvíjí? Žák:
používá demokratické prostředky k prosazování vlastních žádostí
podílí se na politických procesech a přejímá politickou odpovědnost v různých rovinách

Zdroj: Doslovně převzato z: ŠTĚRBA, Radim, a kol., 2018, s. 8–10.

Doporučený průběh lekce:

PL je rozdělený na **úvod** a specifické tematické **sekce**:

Sekce A – Dezinformace a další operace podpořené aktivitami v kyberprostoru
Sekce B – Kybernetické útoky a kyberbezpečnost
Sekce C – Umělá inteligence a hybridní hrozby

Pracovní list doporučujeme rozdělit do **2 vyučovacích hodin**:

1. hodina: úvod + sekce A;
2. hodina: sekce B + sekce C;

v případě větší časové dotace do **3 vyučovacích hodin**:

1. hodina: úvod + sekce A;
2. hodina: sekce B;
3. hodina: sekce C.

V případě časové nouze je možné kombinovat jednotlivé aktivity z částí PL, např. tímto způsobem: (**1 vyučovací hodina**)

Úvod PL: práce s textem (doplňování slov) (5 min);
Sekce A 1a) – Práce s fake news o EU (5 min);
Sekce A 2a) – Přiřazování technických termínů k definicím (domácí práce jako příprava na hodinu);
Sekce A 3a) nebo A 3b) – Práce s webem EK o rozpoznávání dezinformací a konspirací (3–10 min);
Sekce B 1a) – Práce s výukovým textem o kyberzločinu (domácí práce jako příprava na hodinu);
Sekce B 2a) – Práce s karikaturou – diskuze o kyberzločinu (10–15 min);
Sekce C 1b) – Diskuse o boji EU s deep fake (5–15 min).

Část v PL	Čas (odhad) v min	Forma výuky / metoda	Fáze výuky	Scénář	Učební pomůcky
Úvod	3–5	Frontální výuka / samostatná práce s textem	Evokace / uvědomění	Pracovní list začíná úkolem práce s textem – požádáme žáky o samostatné doplnění chybějících slov a následně ověříme porozumění textu otázkami: Co jsou to hybridní hrozby? (2. část textu) Požádáme žáky, aby uvedli alespoň dva příklady těchto hrozeb.	PL
A	18–39			**Dezinformace a další operace podpořené aktivitami v kyberprostoru** *1. Dezinformace, konspirace a psychologické operace*	PL, internet
	2	Frontální výuka	Evokace / uvědomění	Úvodní výukový text informuje o používání dezinformací a konspirací v politickém boji v USA v posledních letech např. tzv. Pizzagate aféra. Příběh se dá využít k evokaci studentů např. otázkou: Proč v USA vtrhl muž s puškou do pizzerie? Následně můžeme rozvíjet diskuzi o nebezpečí dezinformací a misinformací.	PL
	5–8	Samostatná práce / práce ve dvojicích / frontální výuka / práce s textem / internetem	Uvědomění / reflexe	a) Žáky vyzveme, aby si individuálně přečetli jednotlivé výroky o EU a následně se ve dvojicích pokusili označit ty, které se jim jeví jako pravdivé/nepravdivé. Následně s třídou uskutečníme hlasování o ne/pravdivosti výroků a vysvětlení, proč se jim informace jeví jako ne/pravdivé. Požádáme je, aby zkusili pravdivost informací ověřit na internetu. Na závěr srovnáme počet studentů, kteří dokázali identifikovat pravdivé a nepravdivé výroky a vyzveme je k reflexi: jak se vyhnout podlehnutí dezinformacím a konspiracím? Jaké pocity a názory bychom měli, kdybychom uvěřili dezinformacím o EU z úkolu? Proč není vhodné dané informace dál šířit? Jaký cíl sledují autoři dezinformací? Jak se cítí „uživatel" dezinformací poté, co odhalí, že uvěřil nepravdám?	PL, internet

Část v PL	Čas (odhad) v min	Forma výuky / metoda	Fáze výuky	Scénář	Učební pomůcky
A	3–7	Frontální / ve dvojicích / práce s karikaturou / diskuze	Uvědomění / reflexe	b) Požádáme žáky, aby si ve dvojicích prohlédli karikaturu a následně sdíleli své zkušenosti s řetězovými e-maily. Jako podnět k další diskuzi můžou posloužit otázky: Jakým způsobem naléhají odesílatelé, aby byl e-mail dál šířen? Jaké motivy mohou mít tvůrci a šiřitelé těchto e-mailů?	PL
				2. Důsledky dezinformací a dalších aktivit v kyberprostoru	
	3–5	Samostatná práce / frontální výuka / práce s textem	Uvědomění / reflexe	a) Jedním z důsledků dezinformací ve společnosti je její rozdělení a vzájemné znepřátelení. Průvodní text před úkolem a) poukazuje na příklady rozdělení, znepřátelení či radikalizaci jednotlivců i celých skupin. Jaké nástroje jsou k dosažení těchto vlivů užívány? Vyzveme žáky, aby individuálně přiřadili názvy hrozeb k jejich definicím a následně je ve třídě zkontrolujeme, příp. zodpovíme otázky žáků.	PL
				3. Co EU dělá proti dezinformacím?	
	5–10	Práce ve skupinách / práce s textem / internetem	Uvědomění	a) Žáky rozdělíme do skupin (po 3–4) a následně je vyzveme, aby pomocí klíčové věty vložené do vyhledávače („jak rozpoznat konspirační teorii") našli webovou stránku vytvořenou EK a UNESCO. Požádáme žáky, aby na základě informací na webu vypracovali krátký „recept" nebo přehled jako odpovědi na otázky z tabulky úkolu. Každá skupina vytvoří odpověď na jinou otázku tabulky, kterou po skupinové práci následně prezentuje ostatním žákům. Pokud skupiny vypracovávaly odpověď na stejnou otázku, vzájemně se při prezentaci doplní. Na tabuli můžou zapsat klíčová slova svého zjištění/receptu.	PL, internet
	3–7	Práce ve skupině / práce s textem / internetem	Uvědomění / reflexe	b) Žáky požádáme, aby se ve skupinách pokusili určit pravdivé výroky o dezinformacích a konspiracích a následně si je ověřili na webové stránce EK (stejný web jako v úkolu a). Vyzveme žáky, aby sdíleli a reflektovali své zkušenosti střetu s přívržencem konspirační teorie (jak působí na diskutéra korektní/slušná a naopak posměšná či útočná komunikace?).	PL, internet
B	28–40			**Kybernetické útoky a kyberbezpečnost**	PL, internet
				1. Co jsou to kybernetické útoky a proč jsou nebezpečné?	
	3–5	Samostatná práce / práce s textem	Evokace / uvědomění	a) Požádáme žáky, aby samostatně (např. doma) doplnili do textu chybějící slova z rámečku. Co je překvapilo/šokovalo? Jaké nové pojmy se naučili?	PL
				2. (Organizovaný) kyberzločin	
	10–15	Práce ve skupinách / práce s karikaturou / diskuze	Uvědomění	a) Požádáme žáky, aby si prohlédli karikaturu a pokusili se o její interpretaci a vysvětlení. Pomoci jim můžou následující otázky: Jak vypadají postavy karikatury? Jaké mají oblečení? Jaký na vás dělají dojem? Jakou myšlenku chtěl autor karikatury vyjádřit? Jaké otázky vás ke karikatuře napadají? Jak si u obou postav máme vyložit výraz „něco ostřejšího"?	PL

Část v PL	Čas (odhad) v min	Forma výuky / metoda	Fáze výuky	Scénář	Učební pomůcky
B				O karikatuře diskutují žáci ve skupinách, po několika minutách je požádáme, aby své vysvětlení prezentovali ostatním skupinám. Interpretace a vysvětlení by měly směřovat k vytváření pozitivních postojů – odpovědnému užívání sociálních sítí a technologií, kritickému pohledu vůči neověřeným zprávám a názorům, odmítání nenávistné komunikace a šikany na internetu, k užívání techniky způsobem, který neumožňuje její zneužití ke zločinům proti lidem a demokratickému zřízení.	
				3. Ochrana osobních údajů a co EU dělá pro její posílení	
	10–15	Samostatná práce / práce ve dvojicích / skupinová práce / práce s textem	Uvědomění / reflexe	a) Požádáme žáky, aby na základě samostatné četby částí textu 2. a 3. v sekci B shrnuli opatření EU ke kyberbezpečnosti, následně aby ve dvojicích zhodnotili pozitiva a negativa těchto opatření. Úkol ukončí tím, že si své shrnutí a reflexi srovnají s další dvojicí a své odpovědi vysvětlí.	PL
	5	Práce ve dvojicích / práce s textem	Uvědomění	b) Požádáme žáky, aby se na základě své práce s textem celé sekce B v předešlém úkolu pokusili ve dvojicích přiřadit technické termíny k jejich definicím. (Tip: smysl dává i prohození úkolů a) a b).)	PL
C	15–35			**Umělá inteligence a hybridní hrozby**	
		Samostatná práce / frontální výuka/práce s textem		*1. Umělá inteligence (AI) a kvantové počítače*	
	5		Uvědomění	a) Vyzveme žáky k samostatnému doplnění chybějících slov ve výkladovém textu. Po krátkém čase doplnění společně srovnáme a nejasnosti vysvětlíme.	PL
	5–15	Skupinová práce / práce s videem / diskuze	Evokace / uvědomění / reflexe	b) Žáky rozdělíme do skupin, následně jim pustíme výukové video. Požádáme je, aby si ve skupině společně shrnuli, co se ve videu dozvěděli a následně diskutovali o nebezpečí využívání AI v mediální sféře a o tom, jak by mohla EU a jednotlivé členské státy pomoct ochránit své občany před podvody. Své nápady si zapíší (brainstorming) a následně je seřadí dle efektivity a náročnosti. 3 nejefektivnější nápady prezentují a vysvětlí spolužákům. Úkol je vhodný i pro samostatnou práci jako přípravu na vyučování. Alternativa: začneme videem, následně úkolem a) a skupinovou aktivitou v úkolu b).	PL, internet
	5–15	Samostatná práce / spolupráce s umělou inteligencí / diskuze	Uvědomění / reflexe	c) Požádáme žáky, aby si otevřeli na počítači nebo mobilním zařízení webovou stránku s umělou inteligencí a dali jí 3 otázky (např. o celospolečenském problému, z vlastního osobního života, rizik AI, budoucnosti apod). Následně požádáme žáky, aby sdíleli své zkušenosti z komunikace a získané odpovědi. Diskutujeme o ne/odpovědném užívání AI: V čem se liší současné jednání lidí od představ K. Čapka v R.U.R.?	PL, internet

Správné odpovědi:

Klíč k pracovnímu listu

Úvod

Úkol. Doplňte slova:

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

Pod termínem **„hybridní hrozby"** 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 **Krymského poloostrova** v roce 2014. Tehdy to bylo označení pro ruské působení, které má za cíl rozložit **liberální** 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 **Ruské federace** 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 **vojenský konflikt**, jak to vidíme na **Ukrajině** od roku 2014 a zejména od února 2022.

Konkrétně si můžeme pod pojmem hybridní hrozby představit nepřeberné množství jak vojenských, tak i nevojenských (**psychologických**, ekonomických, politických a jiných) prvků. Patří mezi ně například i dezinformace, podněcování radikalizace (např. určitých skupin ve společnosti či jednotlivců), **kybernetické útoky**, psychologické působení (operace), propaganda apod. Působit mohou tyto hrozby jak ve skutečném, tak i ve **virtuálním světě**. 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

Úkol 1a) 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**

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". **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. **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**

KOMENTÁŘ: Tento úkol má ilustrovat, jak je někdy těžké rozeznat pravdivou a nepravdivou informaci. Následující odkazy na mediální články a primární právo EU dokládají, zda se daná událost stala, či nikoliv.

Zpráva A: Lidovky.cz (2017): Zruší Evropská unie písmeno Ř? Senátor Doubrava šířil vtip jako poplašnou zprávu; https://www.lidovky.cz/domov/senator-doubrava-hoax-pismeno-r.A170313_141102_ln_domov_rsa

Zpráva B: Článek 17 odst. 3 Smlouvy o EU říká: „Členové Komise jsou vybíráni podle celkové způsobilosti a evropanství z osob, které poskytují veškeré záruky nezávislosti.“; https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:12016M/TXT&from=EN

Zpráva C: Hospodářské noviny (2017): Zmizelý vagon, rázné uklízečky. Zakládací smlouva EU se podepisovala na prázdný papír; https://zahranicni.hn.cz/c1-62188560-zmizely-vagon-razne-uklizecky-zakladaci-smlouva-eu-se-podepisovala-na-prazdny-papir, EurActiv (2014): EU secret revealed: Rome Treaty was signed on blank sheet; https://www.euractiv.com/section/public-affairs/news/eu-secret-revealed-rome-treaty-was-signed-on-blank-sheet/

Zpráva D: EurActiv (2017): EUROMÝTUS: Farmář musí prasatům pořídit hračky; https://euractiv.cz/section/cr-v-evropske-unii/news/euromytus-farmar-musi-prasatum-poridit-hracky/

Úkol 1b) Prohlédněte si karikaturu a okomentujte ji. Víte, co jsou to řetězové e-maily? Dostali jste někdy takový e-mail?

KOMENTÁŘ: Neexistuje správná odpověď, jde o sdílení zkušeností a rozvíjení diskuze směřující k formování pozitivních postojů.

Úkol 2a) Přiřaďte termíny k jejich definicím

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

Úkol 3a) 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?
Předpokládá, že existuje tajný plán – spiknutí Za plánem stojí podle této teorie skupina vlivných lidí, která „ovládá svět“, rozhodovací procesy, něco běžným lidem záměrně tají apod.	Upozorňovat na existenci lživé zprávy, varovat před jejím šířením Podporovat racionální myšlení a ověřování faktů z různých zdrojů	Snaží se spolupracovat se soukromým sektorem, zejména s platformami sociálních sítí (jako je Facebook, Twitter apod.) na označování a v krajním případě i odstraňování dezinformačního a misinformačního obsahu	Protože výsledkem šíření dezinformací může být radikalizace skupin lidí či jednotlivců, kteří se mohou uchýlit i k násilnému činu

Zpráva předkládá „důkazy" na podporu teorie, ale zpravidla je nejde nijak ověřit z různých na sobě nezávislých zdrojů Zpráva tvrdí, že se nic neděje náhodou, že nic není tak, jak se jeví, vše spolu souvisí, „všichni lžou" apod. Zpráva nabízí černobílé vidění světa – rozděluje ho na dobro a zlo, svaluje vinu na určité lidi či skupiny osob, které např. vulgárně označuje a dehonestuje apod.	Upozorňovat na zdroje těchto zpráv (nejsou oficiální, patří ke zdrojům, které už v minulosti šířily lživé zprávy, přebírají stejnou, lživou, informaci jeden od druhého, někdy např. z jednoho zahraničního zdroje – v minulosti např. z ruských serverů Sputnik apod.) Zaměřovat se na fakta, ne na mýty, a poskytovat vysvětlení založené na faktech a různých zdrojích Vést otevřenou, věcnou a klidnou diskusi Nezesměšňovat, nenalého hat, nezapojovat negativní emoce, urážky apod.	Podporuje fact-checkingové organizace a platformy, které se snaží odhalovat a vyvracet lživé informace na síti; podporuje vzdělávání v této oblasti Evropská služba pro vnější činnost a její projekt EUvsDisinfo Pracovní skupina East Stratcom Akční plán proti dezinformacím Systém včasného varování, který propojuje instituce členských zemí, univerzity, mezinárodní partnery a další organizace za účelem včasného zachycení dezinformačních narativů Kodex zásad boje proti dezinformacím z roku 2022	Šíření dezinformací má za cíl destabilizovat společnost, narušit rozhodovací procesy, politické, ekonomické a společenské struktury, narušit akceschopnost státu v okamžicích krizí V krajním případě může šíření dezinformací vést až k násilným akcím, občanské válce Pomocí dezinformací se může snažit určitá skupina lidí např. ovlivnit volby, uchopit politickou moc ve státě, dosadit sympatizující osoby do vysokých funkcí tak, aby prováděly politiku v souladu s jejich zájmy apod.

Úkol 3b) 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

Úkol 1a) 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 **počítačů** nemohly existovat. Existuje jich nepřeberné množství a jednotlivé techniky se dají nekonečně kombinovat mezi sebou a také s dalšími hybridními hrozbami. Například **politický a diplomatický nátlak** lze kombinovat s tzv. DDoS útoky na kritickou infrastrukturu apod.

Nejslabším článkem v oblasti kybernetické bezpečnosti je **člověk**. 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. **botnet**, se kterým pak může provádět **tzv. DDoS útoky**.

Princip DDoS (Distributed Denial of Service) je velmi jednoduchý – obrovským množstvím dotazů se zahltí server a ten pod takovým náporem **zkolabuje** i pro legitimní uživatele a ti pak nemohou využít např. stránky internetového bankovnictví. V dostatečné intenzitě a trvání to může poškodit i **ekonomiku** 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 **kritickou infrastrukturu** státu (elektrárny, čističky odpadních vod, **plynovody**, 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.

Úkol 2a) Prohlédněte si virtuální příběh a diskutujte o nebezpečí takového podnikání.

KOMENTÁŘ: Neexistuje jedna správná interpretace a vysvětlení karikatury. Jde ale samozřejmě o „podnikání" – organizovaný zločin, který je propojen s některými zločineckými státy nebo zločineckými soukromými zdroji. Trolling např. za určitým účelem ovlivňuje obsah a průběh internetových diskusí (psaní komentářů, ovlivňování diskuze na sociálních sítích např. hromadným přidělováním emotikonů "like" a "dislike" určitým příspěvkům, vytváření nátlaků a virtuálního násilí apod.). „Něco ostřejšího" u postavy vpravo by mohlo být návrhem „práce" i mimo počítače, např. zločin v naší realitě.

Úkol 3a) 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.)?
Nařízení o ochraně osobních údajů (GDPR) – např. tzv. právo být zapomenut v internetovém prostředí 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 NÚKIB Spolupráce s NATO Centra excelence ve Finsku a v Estonsku, která řeší problematiku hybridních a kybernetických hrozeb	Pozitiva – snaha ochránit občana, spotřebitele a ve výsledku i stát před hrozbami jednotlivcům i celé společnosti Snaha bránit kybernetické kriminalitě a útokům, které mohou mít vážné následky Negativa – kritikové hovoří o nadměrné regulaci (např. GDPR), omezování „svobody slova" např. blokováním serverů šířících dezinformace, posilování „dohledu" nad společností apod. Kritika zasahování do činnosti soukromých společností, jako je Facebook, Google apod.	Toto musí studenti vyplnit sami, podle vlastní zkušenosti sebe nebo svých blízkých

Úkol 3b) Na základě předchozí četby v celé sekci B přiřaďte termíny k jejich definicím.

DDoS útok	Kybernetický útok zahlcující server nebo zařízení velkým množstvím požadavků s cílem dočasně omezit jeho fungování.
Phishing	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).
Kapitalismus dohledu	Společensky škodlivý byznysový model, ve kterém jsou uživatelé de facto poníženi 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.
Spyware	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

Úkol 1a) Doplňte slova.

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

Zcela nové možnosti v oblasti hybridních hrozeb přináší také **umělá inteligence**. Jedná se o obor **informatiky** 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 **tzv. deep fakes**, tedy dezinformační prostředky 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. **chatboty**, 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. **Kvantové počítače** by se svou mnohonásobně vyšší výkonností v budoucnu mohly tohoto dosáhnout, ale těžko říci, kdy tato chvíle nastane.

Úkoly 1b–c)

KOMENTÁŘ: Neexistuje správná odpověď, jde o generování nápadů a diskusi směřující k vytváření odpovědného a kritického postoje vůči mediální realitě kolem nás, k technologiím a umělé inteligenci.

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