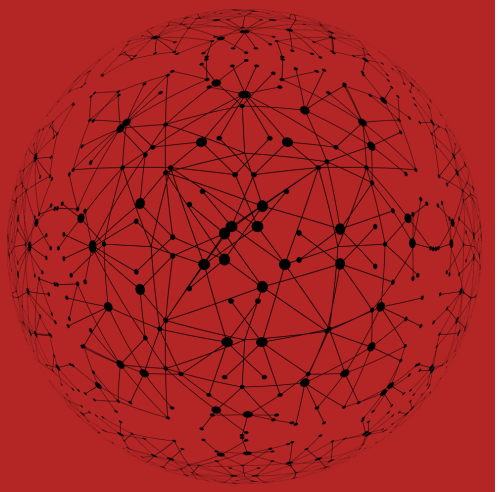
OZVĚNY INFORMAČNÍCH PONDĚLKŮ



01

INFORMACE - TECHNOLOGIE - TRENDY - DISKUSE

Sborník prezentuje vybrané seminární práce z předmětu Informační pondělky. Seminář s hosty proběhl v akademickém roce 2020/21.

EDITOŘI

Nina Wančová

Jana Hecová

Jaroslav Nedavaška

2021

ÚSTAV INFORMAČNÍCH STUDIÍ A KNIHOVNICTVÍ
Filozofická fakulta
Univerzita Karlova

https://uisk.ff.cuni.cz/

Obsah

1 Ozvěny informačních pondělků **1**
1.1 Úvodní slovo garantky . . . 1
1.2 Úvodní slovo studentů . . . 2

2 Vliv koronaviru na média **3**
2.1 Úvod . . . 3
2.2 Koronavirus – nová výzva pro novináře . . . 3
2.3 Koronavirus a jeho vliv na média . . . 4
2.4 Přehlcení médií a jejich vliv na psychické zdraví . . . 5
2.5 Sociální sítě v době koronaviru . . . 6
2.6 Dezinformace, hoaxy a fake news . . . 7
2.7 Závěr . . . 8
2.8 Zdroje . . . 9

3 Internet bezpečný seniorům **11**
3.1 Úvod . . . 11
3.2 Kdo je senior? . . . 12
3.3 Bezpečnost na internetu . . . 13
3.4 Možnosti vzdělávání . . . 16
3.5 Závěr . . . 17
3.6 Zdroje . . . 17

4 Nebezpečí sociálních sítí a komunikace **19**
4.1 Úvod . . . 19
4.2 Komunikace v kyberprostoru . . . 19
4.3 Nebezpečí sociálních sítí . . . 21
4.4 Prevence . . . 24
4.5 Závěr . . . 24
4.6 Zdroje . . . 25
4.7 Použité obrázky . . . 27

5 Kybernetické války **29**
5.1 Úvod . . . 29
5.2 Kybernetické války . . . 29
5.3 Historie kybernetických válek . . . 31
5.4 Příklady kybernetických válek . . . 33
5.5 Současné hrozby . . . 36
5.6 Budoucí hrozby . . . 39
5.7 Obrana proti kyberválkám . . . 40
5.8 Závěr . . . 41
5.9 Zdroje . . . 41

6 Jak digitální technologie mění lidské myšlení **45**
6.1 Úvod . . . 45
6.2 „Stavíme nový svět, všechno je možné“ . . . 46
6.3 „Používej to, nebo o to přijdeš“ . . . 48
6.4 Závěr . . . 49
6.5 Zdroje . . . 50

7 Podmořské optické sítě: kritická infrastruktura **51**
7.1 Úvod . . . 51
7.2 Obecná historie optických sítí . . . 51
7.3 Vývoj podmořských kabelů optických sítí . . . 52
7.4 Bezpečnostní hrozby pro optické sítě . . . 56
7.5 Závěr . . . 57
7.6 Zdroje . . . 58

8 Open Science a její implementace v knihovnách **61**
8.1 Úvod . . . 61
8.2 Implementace Open Science v knihovnách . . . 65
8.3 Příklad Open Access na Univerzitě Karlově . . . 66
8.4 Závěr . . . 67
8.5 Zdroje . . . 67
8.6 Použité obrázky . . . 68

9 Virtuální realita v knihovnách **69**
9.1 Úvod . . . 69
9.2 Virtuální realita . . . 69
9.3 Virtuální prohlídka . . . 70
9.4 Virtuální výstava . . . 72

9.5 Potenciální možnosti VR v knihovnách 73
9.6 VR jako nástroj pro vzdělávání 73
9.7 Negativní vlivy informačních a komunikačních technologií na uživatele 74
9.8 Závěr 75
9.9 Zdroje 75

10 Hry jako učební pomůcka **77**
10.1 Úvod 77
10.2 Hra jako učební pomůcka 78
10.3 Platformy zpřístupňující vzdělávací a naučné hry 79
10.4 Význam vzdělávacích her v současnosti 81
10.5 Závěr 82
10.6 Zdroje 82

1 Ozvěny informačních pondělků

1.1 Úvodní slovo garantky

Na Ústavu informačních studií a knihovnictví se v roli studentky a později doktorandky a vyučující pohybuji přes 10 let. Celou tu dobu, semestr za semestrem, se vyučují Informační pondělky a bylo tomu tak dříve, než jsem nastoupila. Tento klasický a etablovaný předmět, ve kterém se studenti potkávají s odborníky, přemosťuje a propojuje akademické prostředí vysoké školy s praxí. Toto propojení je nesmírně důležité, protože ze školní lavice se mohou některé věci zdát jiné, než je tomu potom v praxi. Právě Informační pondělky mohou být tím předmětem, kde se studenti a studentky zase o trochu více potkají s realitou, sundají si růžové brýle, porovnají teorii s reálnými zkušenostmi a nechají se inspirovat.

Informační pondělky získaly v posledním akademickém roce podtitulek *Informace - Technologie - Trendy - Diskuse*, který přibližuje hlavní cíle a rámec předmětu. Předmět si klade za cíl informovat o aktuálním dění, neopomenout silné propojení našeho oboru s technologickým aspektem informační vědy a v neposlední řadě podnítit diskusi. Diskuse není míněná pouze jako příležitost přímo na přednáškách komunikovat s odborníkem, ale diskutovat i v rámci seminární práce, která je podmínkou zápočtu.

Seminární práce neodmyslitelně patří k vysokoškolskému studiu a zvláště na humanitních oborech. Osobně je psaní mým koníčkem. Ráda vedu dialog s mými myšlenkami, vedu diskuse s jinými odborníky prostřednictvím psaného textu a tříbím si názory a argumenty. A už mi ani tak nevadí, když to nikdo nečte. Jenže psát bez zpětné vazby, bez čtenářů a do šuplíku bude myslím pro většinu lidí spíše frustrující než naplňující. Účastníci Informačních pondělků si přečtou jednu práci svého kolegy a aktivně pracují se zpětnou vazbou. Rozhodli jsme se jít ještě dál a vybrané práce uveřejnit ve sborníku a “vytáhnout je ze dna šuplíku”. Texty ve sborníku odrážejí zaujetí studentů a studentek, reflektují přednášky a dění v oboru. Zároveň mohou sloužit jako inspirace a jistá reflexe toho, jak seminární práce tohoto typu mohou vypadat a jak ještě lépe psát.

Upřímně doufám, že se sborník stane stejně tradiční jako Informační pondělky samy a pomůže zlepšit odbornost studentů a studentek v práci s akademickým textem, protože bez čtení se kvalitní psaní neobejde.

Závěrem bych ráda poděkovala České informační společnosti, z.s., která je spolupořadatelem předmětu a studentům Janě Hecové a Jaroslavovi Nedavaškovi za společnou práci na sborníku.

Hezké čtení a inspiraci přeje **Nina Wančová**

1.2 Úvodní slovo studentů

Práce, které se vzedmuly ze dna šuplíku i díky nám dvěma aktivním studentům, budou prezentovány na dalších stránkách tohoto sborníku. Bylo těžké vybrat z tolika prací pouze 9 nejzajímavějších témat v rámci tohoto různorodého předmětu *Informační pondělky,* který ještě oba jako zkušení studenti na ÚISKu pamatujeme pod názvem *Jinonické informační pondělky*. Předmět pod vedením doktorky Niny Wančové prošel značnou revolucí, co se týče propagace a dostupnosti přednášek a jejích záznamů i pro veřejnost.

Myšlenka realizace sborníku je dalším stupněm pokroku v prezentaci tohoto předmětu. V každém akademickém roce jsou prezentována jiná zajímavá témata od odborníků z praxe. Tento první sborník obsahuje jen malou ochutnávku prací ze zimního i letního semestru uplynulého akademického roku. Tento rok byl pro všechny netradiční svou online formou, což také ovlivnilo témata všech prací.

Sborník otevírá první práce s témamatem vlivu koronaviru na média a to jako připomínka toho, čím jsme všichni intenzivně žili. Dále se ve sborníku objevuje problematika pandemie v souvislosti s tématy, jako jsou sociální sítě, online nakupování a bankovnictví, digitální technologie či hry v rámci vzdělávání. I přes to, že většina studentů během roku měla hlavy plné myšlenek týkajících se koronaviru, tak se našli tací, kteří se věnovali ne-koronavirovým tématům. Proto najdete ve sborníku texty pojednávají o podmořských optických sítích, virtuální realitě v knihovnách, kybernetických válkách či open science.

Výsledný sborník chápejte jako prototyp - jistě v něm najdete mnoho chyb a nedokonalostí, za které se jako editoři omlouváme. Nicméně alespoň jsme nastavili základní proces a udělali si představu, jak náročná práce to je. Věříme, že příští roky se bude sborník zlepšovat. Doufáme, že i přes drobné nedokonalosti si čtení sborníku užijete a získáte nové poznatky.

Slovy Oscara Wildea:

> *„Dochvilností samy sebe připravujeme o čas“*

Proto tento úvod a poslední editace textů vznikly v den před vydáním a prezentací samotného sborníku, 3. 10. 2021.

Jaroslav Nedavaška & Jana Hecová

2 Vliv koronaviru na média

Autorka: Natálie Šnaiberková

2.1 Úvod

Aktuální situace s celosvětovou pandemií onemocnění COVID-19 zasáhla s nebývalou silou většinu odvětví lidské činnosti a zapříčinila řadu změn. Zasažena byla i oblast médií a žurnalistiky, jejíž fungování výrazně ovlivňuje i průběh a vnímání pandemie samotné, protože díky zpravodajství si veřejnost utváří na průběh pandemie názor a získává informace a podklad pro své jednání a chování. Práce zkoumá vliv koronaviru na média, a to jak na tradiční, tak na moderní a nová. Inspirací pro práci byla přednáška s názvem *Historie v televizi (Česká televize, redakce vědy)*, kde se přednášející Aneta Černá mimo jiné věnovala i tomu, jak probíhá práce v médiích během období pandemie.

V roce 2020 nás zavalilo velké množství zpráv, které se ne vždy zakládaly na pravdě. Na média byly kladeny velké nároky a média sama se musela rychle přizpůsobit dané situaci, která navíc nastala poměrně nečekaně. V textu se postupně zabývám celou řadou aspektů vlivu pandemie na média a to jak z pohledu médií, tak i z pohledu příjemců informací. Pravdivost zpráv se ukázala jako klíčová, neboť lidé se sami museli rozhodnout, zda se skutečně jedná o dezinformaci či ne. Pandemie zároveň může být vnímána jako příležitost ke změně uvnitř samotných médií, proto se v textu budu věnovat otázce, zda se média díky pandemii měla šanci vyvíjet, a to pozitivně nebo naopak negativně. Informovanost občanů o aktuální situaci byla a stále je klíčová, což se mohlo jevit jako nová výzva pro novináře. Přílišné nebo naopak nedostatečné informování mohlo mít vliv na psychické zdraví lidí. Důležitou roli kromě tradičních médií sehrály i sociální sítě. A za snad nejdůležitější téma považuji to, jestli bylo snadné rozeznat pravdu od hoaxu a zda se zvýšil počet dezinformací.

2.2 Koronavirus – nová výzva pro novináře

Není pochyb, že se koronavirus stal tématem a námětem číslo jedna, který sledoval celý svět. Trvalo však určitou dobu, než-li se povaha a rozsah katastrofy plně projevila a začala dominovat ve zpravodajské agendě. Když nastane takováto krizová situace, novináři čelí hned několika výzvám. Mezi ty nejhlavnější patří např.:

- informování prostřednictvím komplexního a přesného zpravodajství o vývoji krize;
- poskytování informací o rizicích pro veřejné zdraví tak, aby nedocházelo k vyvolání paniky;
- šíření vědeckých poznatků;
- překonávání nevědomosti;
- informování o nezbytných ochranných opatřeních a úpravách chování;
- neopomenout ostatní důležité skutečnosti a udržení si funkce "hlídacího psa" demokracie i v době krize (European Journalism Observatory, 2020).

To, jak se média s nynější výzvou – tedy psaní o koronavirové krizi, vypořádají se projeví v následujících letech. Žurnalistika může být vnímána jako něco díky čemuž se lidé vyznají ve velkém množství informací, které ať už chtějí nebo ne, musí přijímat každý den. Nyní je situace mnohem složitější, nejistější a zmatenější. Byl zaznamenán velký nárůst mylných informací, dezinformací a hoaxů. Společnost tak od sdělovacích prostředků očekává: říkat pravdu, poskytnout fakta a držet se zodpovědnosti.

Dochází také ke změně v redakčním procesu. Začalo se více pracovat z domova, je nedostatek zaměstnanců, zvýšilo se tempo a rozsah příběhů. Z reportérů se tak ze dne na den stali zdravotnický korespondenti. „*To znamená, že (téměř) všichni novináři informují o problému, na který oni nejsou specialisté*" (Beckett, 2020). Ještě k tomu navíc je těžší všechny informace, články, reportáže apod. upravovat, jelikož se ne vždy smí jít přímo do studia. To by ale nemělo znamenat, že se budou omlouvat chyby nebo zaujatost a „*je třeba říci, že jsme si nikdy nebyli více vědomi novinářských omezení*" (Beckett, 2020). Chyby jsou nyní rychleji odhaleny než kdykoliv předtím a médiím tak začíná pomalu ale jistě vládnout větší kontrola. „*Nám, veřejnosti, na tom všem velmi záleží a jsme vystrašení a naštvaní. Emoce, které k této nemoci a způsobu, jakým s ní politici jednají, pociťujeme právě prostřednictvím médií*"(Beckett, 2020).

2.3 Koronavirus a jeho vliv na média

Pandemie koronaviru neměla dopad pouze na naše životy ale také na sdělovací prostředky. „*Online zpravodajské weby i televizní zpravodajské programy zaznamenaly nárůst pozornosti publika, když se lidé snažili porozumět pandemii, co se s ní děje a co mohou sami dělat. Mnoho nezávislých sdělovacích prostředků, na které se lidé spoléhají, však bude během této krize i tak ohroženo*" (Digital News Report, 2020).

Jako negativní se vnímá, že se poslední měsíce snížila rozmanitost článků, které se produkují. Tato skutečnost může vést k poklesu příjmu z reklamy a pokles příjmu čtenářů u některých titulů, i když samozřejmě některé mohou postupem času zaznamenat i vzestup.

Naopak pozitivní je, že „*krize koronaviru podstatně zvýšila spotřebu zpráv pro mainstreamová média ve všech zemích*" (Digital News Report). Výrazný vzestup tak zaznamenaly především televizní zprávy a

online zdroje. Konkrétně televize byla u většiny lidí považována za hlavní zdroj informací. Stále zde ale přetrvávají obavy z dezinformací. Občané tak hledají zprávy, které se snaží být co nejvíce objektivní. Zajímavostí je i to, že předplatitelé nejen online služeb ale i tradičních sdělovacích prostředků věří v to, že získávají lepší informace na rozdíl od těch, který mají pouze přístup k těm informacím, které jsou poskytnuty zdarma.

„*Koronavirus mimo jiné připomíná lidem hodnotu tradičních zpravodajských zdrojů*“ (Digital News Report). Za posledních několik let se hlavní zdrojem staly online zprávy. Nyní díky pandemii ale posílily i televizní zprávy a noviny. Média byla vnímána jako že odvádějí dobrou práci v tom smyslu, že pomáhají obyčejným lidem pochopit rozsah krize a také objasňují, co mohou lidé udělat pro zmírnění dopadů osobně. Avšak velkou roli hrála i důvěra v média, která se během krize měnila. „*Když koronavirus zasáhl, pozorovali jsme celkovou úroveň důvěry ve zprávy na jejich nejnižším bodě. Jakákoli „důvěryhodnost“ pro média může být často pouze krátkodobá*“ (Digital News Report).

2.4 Přehlcení médií a jejich vliv na psychické zdraví

Podle průzkumu agentury Native PR, který proběhl v dubnu 2020, sledovalo zprávy ohledně aktuální situace koronaviru 87 % Čechů. „*Zájem o informace přitom stoupá s věkem, starší ročníky také zprávy sledují častěji. Každý druhý Čech informace o koronaviru sleduje denně, čtvrtina dokonce několikrát denně*“ (Man, 2020).

Článků je napsáno až několik tisíc denně což bylo pro 2/3 z dotazovaných až příliš. „*Z hlediska úplnosti informací je za dostatečné považuje 80 % respondentů, při 71 % jsou vyvážené i emočně*“ (Man, 2020). Výzkum ukázal i to, že na jejich počet jsou více citlivý muži nežli ženy.

Avšak číst každý den několik měsíců v kuse o světové pandemii a mít snahu udržet si podvědomí o narůstajících číslech nakažených a nových přibývajících opatřeních může být pro mnohé velmi vyčerpávající, a to hlavně psychicky. „*Vzhledem k závažnosti současné situace by se média měla kriticky podívat na to, jakým koronavirovým tématům se rozhodla věnovat a proč*“ (Man, 2020). Zaměřit se na zásadní informace, které nyní veřejnost potřebuje – jak můžeme nejlépe chránit sebe i ostatní, co vše už o nemoci ale i novém očkování víme a jak mohou získat pomoc ti, kteří jí v danou chvíli nejvíce potřebují.

Když se z České republiky přesuneme do USA, tak díky studii, které publikovalo Pew Research Center, se dozvíme, že sedm z deseti Američanů si musí dát pauzu od zpráv o koronaviru. „*Čtyři z deseti tvrdí, že se v důsledku sledování těchto zpráv emocionálně cítí hůř. V dobách krize lidé skutečně chápou potřebu řádné žurnalistiky … [ale] začíná to být zdrcující, protože v zásadě neexistuje nic jiného než příběhy o koronaviru*“ (Digital News Report, 2020).

Navzdory tomu, kolik článků už bylo napsáno v souvislosti s pandemií, tak zde stále přetrvává otázka

ohledně toho, jak dlouho budou opatření pokračovat, a hlavně jak budou vypadat naše životy v budoucnu.

Není tedy divu, že koronavirus a články o něm se podepisují na našem psychickém zdraví. Úzkosti se mohou dostavit např. u těch, kteří přišli díky krizi o práci. „*Ti si mohou přečíst článek, kde získají věcné informace o ekonomice, poté „jít dolů do králičí nory" a zaměřit se na nejhorší scénář pro jejich vlastní vyhlídky na příjem*" (DW, 2020). Nejen, že přijdou o příjem, ale díky tomu mohou přijít i o bydlení, zbývá málo peněz na jídlo apod. Jiní zas mohou trpět úzkostí i přestože jich samotných se přímo krize nedotkla. Představují si, jak se ostatní lidé mají špatně a jak hrozné a zneklidňující to pro ně musí být. Je tedy řešením „*vypnout zprávy*"? Bohužel to není až tak lehké. „*Úzkost pro lidi obecně spočívá v tom, že nás nutí kontrolovat [informace], snažit se úzkost zmírnit*" (DW, 2020).

Naopak u osob s depresí to bývá naopak. Pokud je na ně informací nejen o koronaviru příliš, tak se stávají apatickými, „*a místo toho se obracejí k alternativním a potenciálně nebezpečným zdrojům stimulace, jako je příliš mnoho alkoholu nebo jídla*" (BBC, 2020).

Jak zmírnit úzkosti ale zároveň zůstat informováni? Odborníci tvrdí, že pro většinu z nás by mělo stačit kontrolovat zprávy jednou denně. U osob, který trpí úzkostí by to mělo být sníženo na jedenkrát za týden. Důležité je vybrat si důvěryhodný sdělovací prostředek ať už se bude jednat o rádio, televizi či noviny. Upřednostňovat fakta před domněnkami, jelikož ne všechna žurnalistika je dobrá. Velmi významné je „*vyvinout úsilí, abyste „stanovili hranice" kolem toho, kolik informací sledujete nebo čtete, a vyčleňte si čas na odpočinek a relaxaci*" (BBC, 2020).

2.5 Sociální sítě v době koronaviru

Nesmíme zapomínat ani to, že velkou roli v informovanosti a sdělovaní informací hrály a stále hrají i sociální sítě. Vraťme se zpět ke studii, kterou publikovalo Pew Research Center v dubnu 2020. Podle ní *„téměř čtvrtina (24 %) dotazovaných použila WhatsApp k vyhledání, diskusi nebo sdílení zpráv o COVID-19"* (Digital News Report, 2020). Dále zhruba 18 % se připojilo na Facebook(u) do skupin, které se týkaly právě aktuální situace spojené s koronavirem a více jak polovina (51 %) se začala zúčastňovat skupinových hovorů např. na Zoom či MS Teams se svými kolegy, spolužáky apod. Pro mnohé z nich byla toto první zkušenost se setkáním na online platformách. Mladší generace využívala především platformy jako je Instagram či Snapchat pro získávání informací. V USA přistupovalo 11 % lidí ke zprávám přes TikTok.

Pojďme se zaměřit na jednotlivé sociální sítě. „*Například Facebook a Instagram založily „informační centrum COVID-19", které sdílelo informace o viru z vládních zdrojů a důvěryhodných médií. Toto středisko bylo propagováno společně se všemi druhy příspěvků týkajících se pandemie*" (Evropská kopise, 2020). Již ho využilo více jak 2 miliardy lidí po celém světě.

Podobný krok udělal i Twitter. „*Na informačních stránkách najdete nejnovější tweety řady důvěryhodných vládních orgánů, médií a organizací občanské společnosti, a to v místním jazyce*“ (Evropská komise, 2020).

YouTube začal propagovat videa, které se týkají pandemie, z oficiálních zdrojů jako je např. organizace WHO.

„*Microsoft uvádí, že pokud se do vyhledávače Bing zadá otázka ohledně očkovacích látek proti koronaviru, zobrazí se údaje a aktuality ze spolehlivých oficiálních zdrojů. Kromě toho Microsoft aktualizoval svou politiku týkající se zavádějícího obsahu a zakázal reklamu, která se na krizi COVID-19 přiživuje*“ (Evropská komise, 2020).

TikTok se zaměřil na videa, která obsahují slova či hashtagy týkající se koronaviru, a označil je „*covid-19 štítkem*“, který přesměruje uživatele na důvěryhodné zdroje informací, kde se mohou dozvědět více.

Co se týče Google, tak „*vedle výsledků vyhledávání a bannerových reklam na webových stránkách byly také umístěny zdroje odborných informací*“ (Evropská komise, 2020). Všechny sociální sítě se především snaží propagovat spolehlivé zdroje informací, a naopak zabránit šíření klamavého a zavádějícího obsahu.

2.6 Dezinformace, hoaxy a fake news

Spolu s přibývajícími případy spojených s nákazou COVIDEM – 19, začaly přibývat i články plné dezinformací, hoaxů a fake news, které se většinou týkaly toho, jakými způsoby předcházet nákaze či jak koronavirus vyléčit. Naneštěstí v několika případech lidi, který těmto nepravdivým informacím uvěřili, zaplatili svým životem.

Koncem března se poprvé objevila informace, že léky zvané hydroxychlorochin a chlorochin by měly pomáhat v léčbě koronaviru. Dokonce samotný (nyní už bývalý) prezident Spojených států Amerických - Donald Trump přidal tweet, kde se o hydroxychlorochinu a ještě o azithromycinu zmiňuje a doporučuje si je vzít protože není co ztratit. Předávkování těmito léky je velmi vzácné, avšak není nemožné. Např. v Hanoji byl přijat muž, který požil velké dávky chlorochinu a měl štěstí, že se dostal do nemocnice včas a začal se rychle léčit. Stejné štěstí bohužel neměl pár, který požil čistič, kde se kromě chlorochinu vyskytovali i jiné, jedovaté látky. Muž zemřel a žena, která byla hospitalizována později vypověděla, že přípravek se svým mužem vypili právě díky doporučení Donalda Trumpa.

Když se podíváme do další země, tak „*v Íránu stovky lidí zemřely na otravu alkoholem kvůli zvěstech o jeho léčivých účincích*“ (BBC, 2020). Na konci dubna 2020 bylo známo téměř 800 takových případů. Dezinformace o údajné léčbě se začala šířit především na aplikaci zvané Telegram.

Existují i hoaxy o léčbě, která vám sice nijak neuškodí ale zároveň nemají žádný vliv na nemoc jako je koronavirus. Mezi ně patří např.: jezení česneku, nošení teplých ponožek či potírání husího sádla na hruď.

Samozřejmě i u nás v České republice kolovalo mnoho dezinformací, a i z toho důvodů najdeme na webových stránkách Ministerstva vnitra a Ministerstva zdravotnictví souhrn těch nejčastějších dezinformačních tvrzení a pravdivá fakta, která je vyvracejí.

Přítomnost dezinformací si uvědomuje i Evropská unie, která se snaží na jejich přítomnost upozornit. „*Následkem dezinformací mohou v době koronavirové pandemie umírat lidé. Jsme povinni naše občany chránit a na nepravdivé informace je upozorňovat a musíme ukázat na subjekty, které se k těmto praktikám uchylují. V dnešním světě stojícím na technologiích, kdy se bitvy nesvádějí pomocí mečů, ale klávesnic, a kdy se státní i nestátní subjekty systematicky dopouštějí cíleného ovlivňování a dezinformačních kampaní, zintenzivňuje Evropská unie svou činnost a posiluje kapacity, aby těmto zbraním dokázala čelit*“ (Evropská komise, 2020). Významná je komunikace, a proto Evropská komise vytvořila webové stránky věnované informacím o koronaviru, kde je také část vyhrazená dezinformacím. Tyto sekce jsou dostupné ve všech jazycích Evropské unie. Dále zde máme spolupráci se svými partnery v rámci EU, kde se využívá systém včasného varování. „*V rámci systému byla vytvořena zvláštní sekce, v níž mohou členské státy a evropské orgány sdílet informační materiály týkající se koronavirové pandemie*“ (Evropská komise, 2020). Komise mimo jiné také sleduje činnost online platforem se zřetelem na kodex zásad boje proti dezinformacím.

Jak odlišit fakta od dezinformací? Občas je to velmi jednoduché a stačí kontrolovat čtyři základní věci: titulek, jméno autora, datum a použité zdroje. „*Dezinformační weby rády využívají VELKÁ PÍSMENA v titulku článku doplněná o zjevné fotomontáže*“ (Covid portál, 2020). Důležité je zkontrolovat si, zda je uveden autor článků, jelikož ten v případě dezinformačních webů často chybí. Nesmí se zapomínat i na datum zveřejnění článků, jelikož se často šíří články i několik let staré a nejvíce významné jsou uvedené zdroje ze kterých autor čerpal.

2.7 Závěr

Média během doby světové pandemie rozhodně prošly změnou. Na novináře byl, je a bude kladen velký důraz, aby přinášeli fakta z důvěryhodných zdrojů za co nejméně krátkou dobu, což se jeví jako velká výzva. I z důvodu, že mnoho žurnalistů musí nyní dělat práci doma, i když dříve jí směli vykonávat ze studia, a proto jsou jistým způsobem omezeni. Nesmím zapomenout ani na to, že informují o odborném tématu, na který většina odborníci nejsou. I média samy o sobě se změnila. Jako pozitivní je vnímán fakt, že se zvýšila pozornost skoro všech médií. Až od tradičních po ta moderní. Negativní je však velká míra dezinformací, kterých za poslední rok přibylo a pro lidi se některé mohly stát nebezpečné pro jejich život.

Vývojem prošly samozřejmě také sociální sítě, které se snažily co nejvíce propagovat taková fakta, která jsou věrohodná a pomohou lidem. Zprávy o koronaviru jsou všude, kam se podíváme, a proto není divu, že to ovlivnilo i psychické zdraví občanů. Je důležité zůstat informovaný ale zároveň i myslet na sebe a na to, jestli není vhodné omezit sledování zpráv. Při čtení a sledování médií je důležité myslet na jejich důvěryhodnost a vždy si ověřovat zdroje odkud se čerpalo, nezapomínat na svoje mentální zdraví a na to jak nás, tak velké množství informací ovlivňuje, a hlavně nevěřit každé zprávě, kterou vidíme či si přečteme, jelikož dezinformací, hoaxů a fake news jsou plná média.

2.8 Zdroje

Beckett, C. Journalism and coronavirus: the challenge for the news media [Online]. Charlie Beckett. Retrieved from https://charliebeckett.medium.com/journalism-and-coronavirus-the-challenge-for-the-news-media-9c1a8551826d

Burack, C. Opinion: Why we need less coronavirus media coverage [Online]. Dw. Retrieved from https://www.dw.com/en/opinion-why-we-need-less-coronavirus-media-coverage/a-55294446

Meißner, F. Koronavirus a média: Výzvy pro novináře v době pandemie [Online]. European Journalism Observatory. Retrieved from https://cz.ejo-online.eu/6386/etika-a-kvalita-zurnalistiky/koronavirus-a-media-vyzvy-pro-novinare-v-dobe-pandemie

Newman, N. Executive Summary and Key Findings of the 2020 Report [Online]. Digital News Report. Retrieved from https://www.digitalnewsreport.org/survey/2020/overview-key-findings-2020/

Savage, M. Coronavirus: How much news is too much? [Online]. Bbc. Retrieved from https://www.bbc.com/worklife/article/20200505-coronavirus-how-much-news-is-too-much

Spring, M. Coronavirus: The human cost of virus misinformation [Online]. Bbc. Retrieved from https://www.bbc.com/news/stories-52731624

Média informují o covid-19 příliš, míní Češi. Klíčovým zdrojem jsou ČT a Novinky.cz [Online]. Mam. Retrieved from https://mam.cz/zpravy/2020-04/klicovym-zdrojem-jsou-ct-a-novinky-cz-media-informuji-o-koronaviru-prilis-mini-cesi/

EU stupňuje boj proti dezinformacím o koronaviru [Online]. Retrieved January 18, 2021, from https://ec.europa.eu/commission/presscorner/detail/cs/ip_20_1006

Jak odlišit fakta od dezinformací [Online]. Retrieved January 18, 2021, from https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_cs

3 Internet bezpečný seniorům

Autorka: Tereza Vacková

3.1 Úvod

Cílem této práce je určité ucelení tématu seniorů využívajících internet a zaměření se na vybrané nástrahy internetu, které ztěžují seniorům využívání internetu a jsou pro ně hrozbou, dále je na místě osvětlit i jednoduché kroky pro jejich prevenci.

Senioři jsou jednou z nejpočetnějších skupin naší populace a tato skupina se díky prodlužování průměrné délky života nadále zvětšuje. Světová zdravotnická organizace uvádí, že mezi lety 2015 a 2050 se zvýší procento populace starší 60 let z 12% na 22% (WHO, 2018). Ti senioři, kteří se pohybují na internetu a nejsou dostatečně digitálně a informačně gramotní, se nevystavují rizikům internetu samotní. Svým chováním vystavují rizikům internetu i další nezkušené uživatele. A tímto způsobem se dá například u dezinformací a hoaxů snadno a efektivně manipulovat a ovlivňovat opravdu početnou skupinou lidí. Proto je nesmírně důležité, aby byla v dnešní době digitálních technologií pro tuto skupinu zajištěna prevence proti léčkám, které jim na internetu hrozí a tím zaručena internetová bezpečnost, ale také pravdivost a věrohodnost informací nejen pro ně, ale po všechny uživatele internetu.

První část seminární práce definuje, kdo je senior a nastiňuje problematiku přesné definice tohoto termínu a pokračuje tématem volného času, který senioři na internetu tráví, a definuje velmi podstatné termíny související s celou touto problematikou - digitální propast a informační gramotnost. Následující část se jmenuje *Bezpečnost na internetu* a věnuje se třem vybraným hrozbám, které seniorům znepříjemňují pobyt na internetu - podvodům při nakupování, phishingu a fake news spolu s hoaxy. Spolu s jejich popisem obsahuje přehled postupů, jak tyto nekalé praktiky odhalit. Poslední část se krátce věnuje tématu vzdělávání a zdokonalování seniorských znalostí v oblasti digitálních technologií, neboť prevence může zabránit řadě problematických jevů.

3.2 Kdo je senior?

Důležité pro pochopení tématu je stanovení si definic. Bohužel při vyhledávání termínu „senior“ uvádí každý zdroj odlišné formulace a věkové vymezení. Pro potřeby této práce budeme věkovou hranici člověka - seniora chápat vzhledem k ukončení ekonomické aktivity, tedy odchodu do důchodu. Důchodový věk se počítá s pomocí demografických prognóz, a jelikož se průměrná délka života člověka prodlužuje, prodlužuje se i věk odchodu do penze. V České republice je aktuálně hranice důchodového věku dovršení 65 let (Hovorková, 2019). Jelikož věková kategorie 65 let a výše a i její další případné rozdělení vychází z data narození, jedná se o věk kalendářní, který však nenapovídá nic o fyzickém či psychickém zdraví člověka, které je v definici slova senior neméně podstatné. Mimo fyzickou a duševní kondici a věk, se senioři liší také rozdílnou ekonomickou situací, vzděláním, sociálním statutem, životním stylem, kreativitou, společenskou angažovaností, atd. (Houšková, 2017). Tyto poznatky dokládají, že samotné zařazení do věkové kategorie nestačí a rozhodně nejsou rozhodující. Podstatný je celkový obraz utvořený ze všech aspektů života seniora.

Ke všem různým aktivitám, které senioři ve svém volném čase vykonávají, se u stále většího počtu lidí právě nad 65 let přidává i využívání internetu. Počet seniorů, kteří internet využívá, se tedy každým rokem navyšuje, v roce 2015 využívalo internet 28,4 % seniorů, v roce 2020 to bylo již 40,3 % a tento trend bude jistě stále růst. Internet je seniory využíván k různým činnostem, především ale k vyhledávání informací o zdraví (31,3 %) a zpravodajství (35,5 %) nebo k zasílání e-mailů (33,8 %). Na vzestupu v počtu uživatelů starších 65 let je i využívání internetového bankovnictví, internetových nákupů či sociálních sítí (ČSÚ, 2020).

3.2.1 Digitální propast

Pojem digitální propast neboli „digital divide“ popisuje rozdělení v oblasti využívání digitálních technologií na jejich uživatele a na ty, kterým něco v jejich využívání brání. Digitální propast vzniká dle van Dijka a Hackera ze 4 důvodů, prvním z nich je nedostatek základních digitálních zkušeností, což je způsobeno nízkým zájmem, strachem či odmítáním technologií. Druhým důvodem je nedostatek materiálních prostředků pro pořízení digitálních technologií. Třetím důvodem je nedostatek digitálních dovedností. Tento problém je způsoben nedostatečnou sociální podporou a vstřícností k uživatelům nebo nedostatečným vzděláním v oblasti digitálních technologií. Posledním, čtvrtým důvodem je nevyužívání nebo nedostatek příležitostí pro využívání digitálních technologií (van Dijk a Hacker, 2003, s. 315-316).

Případ, kdy je rozdíl mezi těmi, kteří mají k digitálním technologiím přístup a těmi, kteří k nim přístup nemají, se nazývá primární digitální propast. Ta se týká především těch seniorů, kteří nemají dostatek financí pro samotné pořízení digitálních prostředků. Žádnou roli tudíž nehraje věk, nýbrž ekonomická situace seniora.

Sekundární digitální propast, která postupně nahradila tu primární, se vyznačuje problémem v samotném využívání technologií. Není to však chápáno ve smyslu základních počítačových dovedností, ale spíše jako schopnost orientace v široké nabídce a počítačové bezpečnosti, vyhledávání informací a ovládání základních online úkonů, mezi které patří např. internetové bankovnictví, nakupování přes internet, online vzdělávání, apod. „Sekundární digitální propast se tedy vytváří mezi skupinami lidí, kteří přístup k technologiím mají a vlastní je, nicméně jejich dovednosti využití jsou diametrálně odlišné." (Zadražilová, 2017, s. 104-105).

Další předpokládaná úroveň, tzv. terciální digitální propast, není ještě dostatečně prozkoumaná a chybí o ní dostatek relevantní literatury, avšak už teď je vnímaná z několika možných hledisek. Prvním příkladem je vnímání terciální digitální propasti z hlediska toho, jakým způsobem člověk dokáže aplikovat výhody internetu a technologií do svého offline života. Tuto studii provedli vědci Alexander Van Deursen a Ellen Hesper. Druhým příkladem je vnímání terciální digitální propasti ve spojitosti s omezením svobodného přístupu k informacím, cenzuře internetu, blokování přístupu k internetu, kterou ve své diplomové práci představila Jana Piskurová (Zadražilová, 2019, s. 19-20).

V České republice problém primární digitální propasti u seniorů již mizí. V roce 2020 využívá internet, jak je výše zmíněno, více než 40 % seniorů a již 39,9 % domácností osob starších 65 let vlastní počítač nebo tablet (ČSÚ, 2020). Dostupnost internetu přestává být tak závažným problémem i z toho důvodu, že je možné se k němu dostat například pomocí veřejně dostupného připojení.

Problémem tedy zůstává digitální propast sekundární, která nejvíce trápí právě ty seniory, kteří s moderními technologiemi a internetem mnohdy přišli do styku až v pozdním věku, na rozdíl od mladších ročníků. Proto je nanejvýš nutné cílit na tuto věkovou skupinu programy, které jim zajistí vzdělání v oblasti informační nebo digitální gramotnosti (Zadražilová, 2019, s. 21-22).

Digitální gramotnost je soubor určitých digitálních kompetencí, které uživatel potřebuje k využívání digitálních technologií. Digitálně gramotný člověk pak může tyto technologie kdykoliv bezpečně, sebejistě, kriticky a tvořivě využívat (NÚV, 2021). Informační gramotnost je podle TDKIV „schopnost jedince identifikovat informační potřebu, vyhledat informace, zhodnotit je, zpracovat a efektivně využít." (Švejda a Planková, 2003).

3.3 Bezpečnost na internetu

> „Internet jako takový je bezpečný, nebezpeční jsou na něm jen lidé"

(Kožíšek a Písecký, 2016, s. 36).

Vzhledem k tomu, že počet seniorů, kteří využívají internet, bude stále narůstat, je podstatné znát nástrahy, které na ně mohou na internetu číhat a to hlavně z toho důvodu, že patří v online prostředí

mezi jednu z nejohroženějších skupin uživatelů. „Důvodem může být neznalost či podcenění rizik při aktivitách na internetu, stejně jako přílišná důvěřivost v informace, získané od osob, kterým důvěřují a které si dále neprověřují.“ (Vojtěchovská, 2020, s. 19).

3.3.1 Podvody při nakupování

Nakupování přes internet se těší velikému rozmachu, čemuž přispěla i pandemie koronaviru. ČSÚ uvádí, že v roce 2019 nakoupilo na internetu 8,1 % seniorů nad 65 let, v rozmezí 3 měsíců, alespoň jednou. V roce 2020 to bylo již 14,9 % (ČSÚ, 2020). Vzhledem k takovému nárůstu uživatelů internetových nákupů z řad seniorů a k nedostatečném povědomí o bezpečném nakupování je toto téma opravdu důležité, jelikož prevence v tomto odvětví může pomoci zamezit páchání trestného činu podvodu. Podle definice trestního zákoníku spáchá trestný čin podvodu ten, „kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou“ (Zákon č. 40/2009 Sb., § 209). Díky rozmachu internetu došlo ke zvýšení výskytu podvodů, k čemu dopomáhá i pocit anonymity, které online prostředí navozuje, nebo také skoro neomezený počet uživatelů, kteří podvod včas neodhalí. V oblasti podvodů při nakupování jde především o podvodné e-shopy a podvody na inzertních nebo aukčních službách (Kožíšek a Písecký, 2016, s. 111). *Desatero bezpečného nakupování na internetu* uvedené v publikaci *Bezpečně n@ internetu* (Kožíšek a Písecký, 2016, s. 119-120) je výborným rádcem pro odhalování podvodů při online nakupování. Obsahuje následující rady:

1. Prověřte si internetového prodejce.
2. U neznámých obchodníků neplaťte za zboží předem a volte možnosti platby na dobírku.
3. Vyhledejte si všechny dostupné informace o výrobku.
4. Vyhledejte recenze na obchodníka.
5. Srovnejte si ceny zboží na internetu.
6. Můžete reklamovat do 30 dní.
7. Neexperimentujte.
8. Pokud je to možné, tak volte osobní předání zboží.
9. Sledujte www adresu obchodu.
10. Nezadávejte více údajů, než musíte.

3.3.2 Phishing

Jak vyplývá z výzkumu **Starci na netu**, senioři mnohem častěji než jiné věkové skupiny reagují na e-maily od své bankovní instituce, tudíž jsou velmi ohroženou skupinou, na kterou mohou být cíleny útoky vykazující znaky phishingu (Kopecký a kol., 2018, s. 18). Špatná zkušenost může způsobovat nechuť seniorů nadále se vzdělávat a seznamovat s digitálními technologiemi a tím prohlubovat

sekundární digitální propast. „Phishing je podvodné jednání s cílem vylákat vaše osobní data jako např. čísla kreditních karet, hesla a další důležité údaje. Dá se také popsat jako krádež identity nebo jako typ sociálního inženýrství.“ (Bezpečný internet, 2021). Phishing funguje na základě rozesílání podvodných zpráv, které přicházejí od zdánlivě věrohodně vypadajícího odesílatele, kterému většinou oběť phishingu důvěřuje. Jde například o banku poškozeného, nebo třeba sociální síť, kterou využívá. Toto podvodné jednání spoléhá na odkazy v daných zprávách, díky kterým se po otevření obvykle nainstaluje spyware nebo se snaží oběť zmást pro účely získání citlivých informací (Bezpečný internet, 2021).

Obrana proti phishingu je především ignorování doručených zpráv, na místě je opatrnost při přihlašování a registrování, pro které by měl uživatel využít oficiálních stránek. Dále je doporučeno využití zabezpečeného spojení, pravidelně aktualizovat operační systém, firewall a antivirový program. Některé nepovedené formy phishingu jsou rozpoznatelné na první pohled, nejsou věrohodné, obsahují chyby (Bezpečný internet, 2021).

3.3.3 Fake news a dezinformace, hoax

Vzhledem k tomu, že většina seniorů využívá internet z velké části k vyhledávání zpravodajství nebo ke komunikaci přes e-mail, je tato skupina uživatelů vystavena fake news a často jim také podlehnou. Jejich zvýšená náchylnost k fake news může být způsobena vícero faktory, jedním z nich je výše zmíněná nižší úroveň digitální gramotnosti, ale také gramotnosti mediální.Fake news je nejčastěji definován jako „úmyslně nepravdivé nebo zavádějící informace, které se objevují v médiích a na sociálních sítích“. Fake news je jen jiný název pro dezinformace. Problémem fake news je to, že její autor si dal za cíl ovlivnit či zmanipulovat příjemce zprávy, kterým může být kdokoliv. Někdo by si mohl dezinformace zaměnit s pojmem misinformace, česky fáma. V obou případech jde o nepravdivou či zavádějící zprávu, avšak v případě fámy je šířena bez vědomí toho, že jde o lež (Gregor a Vejvodová, 2018, s. 8).

Za hoax je označována poplašná zpráva s naléhavým sdělením, která se šíří řetězově pomocí sociálních sítí a e-mailu. Typickým znakem je pocit urgentnosti zprávy, odkazování na důvěryhodné zdroje, nebo naopak zjištění, která autority a média tají, v neposlední řadě nabádají příjemce k dalšímu šíření takové zprávy (Pajgrtová, 2020, s. 14).

K odhalení falešných zpráv by mohla pomoci příručka od vzdělávací organizace **Jeden svět na školách** (Gregor a Vejvodová, 2018, s. 126), která obsahuje těchto pět základních otázek, které by si měl každý položit při čtení mediálního obsahu:

- Kdo je autorem nebo tvůrcem sdělení?
- Co je obsahem sdělení?
- Které cílové skupině je sdělení určeno?

- Jak se sdělení snaží upoutat mou pozornost?
- Proč bylo sdělení vytvořeno?

3.4 Možnosti vzdělávání

Vojtěchovská vidí největší potenciál při vzdělávání seniorů v oblastech jako informační technologie, práce s výpočetní technikou a orientace v online prostředí v mezigeneračním učení. Dalším benefitem mezigeneračního učení je možnost zlepšení sociálních vazeb seniorů, což má příznivé účinky na jejich psychickou pohodu (Vojtěchovská, 2021).

Mezi další možnosti vzdělávání se řadí např.:

- Univerzity třetího věku (U3V)
- Virtuální Univerzita třetího věku (VU3V)
- Akademie třetího věku (A3V)
- přednáškové tematické cykly, jednorázové vzdělávací aktivity
- kurzy

Všechny výše zmíněné možnosti vzdělávání může v obci pro seniora zprostředkovávat knihovna, která již dávno není vnímána jen jako instituce podporující formální vzdělávání, ale také jako instituce napomáhající k neformálnímu vzdělávání obyvatel (Mazurová a Houšková, 2016, s. 37-40).

3.4.1 Elpida

Elpida je jednou z organizací která se pomoci seniorům v oblasti digitálních technologií věnuje. Uspořádává tzv. Akademie po seniory, mezi níž patří také **Počítačová akademie Elpida**. Pod touto počítačovou akademií se ukývá nespočet kurzů, které se zabývají tématy ze světa technologií a internetu. Senioři se zde mohou přihlásit na kurzy pro úplné začátečníky i pokročilé. Elpida nabízí jak několikahodinové kurzy, které obsáhnou celé téma, tak také jednorázové semináře, obojí se uskutečňuje buď on-line nebo osobně. Nabídka kurzů se obměňuje a ty právě aktuální lze vyhledat přímo na webových stánkách Elpidy. Vzhledem k internetové bezpečnosti by měl být vyzdvihnut kurz s názvem **Bezpečný internet on-line - www s přehledem a bez rizik**. Tento kurz seznamuje seniory obecně s tím, co je to internet, s hlavními druhy ohrožení na internetu a s tím, jak se jim bránit. Osvětluje také problematiku počítačových virů a představuje fungování antivirových programů. Nechybí ani zásady chování na internetu, pod což spadá také vytvoření bezpečného hesla a následné zacházení s ním. Cena kurzu je 150 Kč za 90 minut a pobíhá on-line (Elpida, 2021).

3.5 Závěr

Cílem této práce bylo ucelení tématu seniorů využívajících internet a zaměření se na vybrané hrozby, které ztěžují seniorům jeho využívání. Z práce vyplývá, že hrozby na internetu jsou stále aktuální a je potřeba proti nim bojovat. Je potřeba snažit se překlenout sekundární digitální propast pomocí edukace seniorů v oblasti digitální a informační gramotnosti. Tato edukace může seniorům pomoci hrozby rozpoznávat a eliminovat a díky tomu i využívat internet s větší jistotou a beze strachu.Závěrem práce je nutno dodat, že jistě nepokryla všechny hrozby, které na seniory na internetu číhají, ať už jde o jiné podoby fake news, se kterými přijdou senioři do styku, nebo například o určitou formu kyberšikany a nebo o jiné formy podvodů, které se snaží využít nejisté uživatele internetu z řad seniorů. Dále by bylo vhodné zaměřit svou pozornost na podrobné zmapování možností vzdělávání v oblasti informační a digitální gramotnosti.

3.6 Zdroje

Bezpečný internet. Bezpečný internet: Rady pro bezpečnost na internetu [Online]. Retrieved May 28, 2021, from http://www.bezpecnyinternet.cz/

Český statistický úřad. (2020). Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci [Online]. Praha: Český statistický úřad. Retrieved from https://www.czso.cz/documents/10180/122362692/06200420.pdf/d203b0fc-50c5-4763-ae5c-4ad5d2a8e2fd?version=1.3

Elpida. Akademie pro seniory [Online]. Retrieved from https://www.elpida.cz/aktivity-centra-elpida

Gregor, M., & Vejvodová, P. (2018). Nejlepší kniha o fake news, dezinformacích a manipulacích!!! [Online]. Brno: CPress.

Houšková, Z. (2017). Senioři a knihovny [Online]. Duha: Informace O Knihách A Knihovnách Z Moravy, 31(4). Retrieved from https://duha.mzk.cz/clanky/seniori-knihovny

Hovorková, K. Penze se mladým vzdaluje, krizi řeší celá EU. Česko však stárne rychleji než ostatní [Online]. Retrieved from https://zpravy.aktualne.cz/finance/v-petasedesati-i-pozdeji-v-kolik-letech-se-ve-svete-chodi-do/r~f1fb970cc5a411e98aa4ac1f6b220ee8/

Kopecký, K., Szotkowski, R., Kožíšek, M., & Kasáčková, J. (2018). Starci na netu: výzkumná zpráva [Online]. Olomouc. Retrieved from https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/102-starci-na-netu-2017-2018/file

Kožíšek, M., & Písecký, V. (2016). Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing.

Mazurová, H., & Houšková, Z. (Eds.). (2016). Rovný přístup: knihovna přátelská k seniorům : metodická příručka pro práci knihoven se seniory. Praha: Národní knihovna České republiky - Knihovnický institut.

Národní ústav pro vzdělávání. (2021, January 20). Stručné vymezení digitální gramotnosti a informatického myšlení [Online]. Retrieved from http://www.nuv.cz/t/strucne-vymezeni-digitalni-gramotnosti-a-informatickeho

Pajgrtová, A. (2020). Senioři v době fake news (Diplomová práce). Praha.

Švejda, J., & Planková, J. (2003-). Informační gramotnost [Online]. Retrieved from https://aleph.nkp.cz/F/DS4QBYJEN6P1M3XBUCQ6ICY8KPM141RMF9SYJQ8A8CG15KJ3BD-52405?func=full-set-set&set_number=207626&set_entry=000002&format=999#tail

van Dijk, J., & Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon [Online]. The Information Society, 19(4), 315-326. https://doi.org/10.1080/01972240309487

Vojtěchovská, P. (2020). Senioři a využívání plateb na internetu (bakalářská práce). Praha.

WHO. (2018). Ageing and health [Online]. Retrieved from https://www.who.int/news-room/fact-sheets/detail/ageing-and-health

Zadražilová, I. Potřeby seniorů při práci s internetem - výsledky kvalitativního šetření [Online]. Proinflow: Časopis Pro Informační Vědy, 2017(9), 103-119. Retrieved from https://www.phil.muni.cz/journals/index.php/proinflow/article/view/2017-2-6/1905

Zadražilová, I. (2019). Senioři a problematika digitální propasti (Dizertační práce). Praha.

Zákon č. 40/2009 Sb., trestní zákoník, 2009 Sbírka zákonů §. Retrieved from https://www.zakonyprolidi.cz/cs/2009-40/zneni-20210526

4 Nebezpečí sociálních sítí a komunikace

Autorka: Denisa Šourková

4.1 Úvod

Seminární práce Nebezpečí sociálních sítí a komunikace se zabývá hrozbami dorozumívání se i celkovou interakcí v kyberprostoru. Zahrnuje zejména služby dostupné na internetu určené především ke komunikaci mezi lidmi. Konkrétně vymezuje a zaměřuje se na pojem **sociální síť**, přičemž upozorňuje na její celospolečenský vliv a možná rizika.

S počátkem digitálního věku a rozvojem vyspělých komunikačních technologií vznikají nové možnosti a způsoby pro dorozumívání mezi lidmi. Velké popularitě se těší zejména sociální sítě. Každá sociální síť umožňuje sdílení informací, což může být rizikem pro mnoho aktivních jedinců na těchto platformách. Mnohdy dochází ke zneužívání osobních údajů pro potřeby inzerentů nebo samotných členů sítě, popřípadě hackerů provádějících útoky, pomocí nichž se snaží získat především citlivá data od uživatelů.

V tomto online prostředí dochází často také k sociální interakci, kdy se vytvářejí tzv. *virtuální vztahy*. Existují zde falešné identity vzhledem k možnosti využití anonymity, které mohou vést až k riskantním známostem či k různým sociálně-patologickým jevům. Cílem je zejména popsat tyto nebezpečné aspekty sociálních sítí a nastínit možná preventivní opatření. Práce navazuje na přednášku pana docenta Václava Jirovského o kybernetické společnosti, která se konala v předmětu Informační pondělky na UISK FF UK 8.3.2021.

4.2 Komunikace v kyberprostoru

Obecně se představuje **kyberprostor** jako prostředí, jehož základ tvoří počítačové sítě a zejména pak internetová infrastruktura. Dnes je existence tohoto virtuálního světa důležitou součástí každodenního života pro mnoho lidí, protože poskytuje různé užitečné funkce. Jednou z nich je i **zprostředkovávání komunikace**, která umožňuje vzájemnou interakci mezi jedinci nebo skupinou lidí a napomáhá k výměně informací (Čech, 2010).

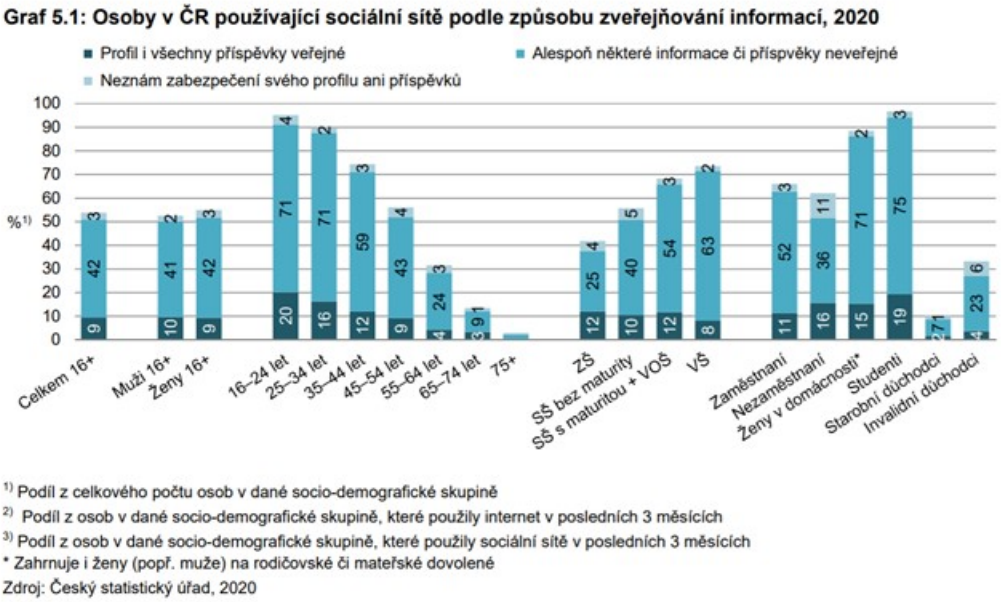
Komunikaci v kyberprostoru lze rozdělit na **synchronní** a **asynchronní.** Asynchronní sdělování informací není založeno na okamžité reakci, tudíž uživatelé odpovídají nezávisle na tom, kdy oznámení obdrželi. Příkladem mohou být e-maily nebo diskusní skupiny. Naopak synchronní komunikace probíhá v reálném čase, tzn., že dochází k výměně informací mezi jedinci či skupinami osob ve stejnou dobu. Pro tento druh spojení jsou nejčastěji vytvářeny chaty (Suler, 1996). V souvislosti s neustálým vylepšováním komunikačních zařízení, se však mnohdy synchronní i asynchronní interakce slučují (Čech, 2010). Tuto funkci umožňují zejména chytré telefony, kde je možné kombinovat oba druhy komunikace (Cz.NIC, 2021).

S počátkem digitálního věku a v důsledku vývoje internetu vznikají nové možnosti, které přispívají k objevu jiných způsobů komunikace a sebevyjadřování. Lidé najednou mohou sebe a své myšlenky sdílet se světem (Guo, 2008). Vytvářejí se platformy, aplikace apod., které umožňují rychlé posílání zpráv mezi lidmi po celé planetě. Pro komunikaci v kyberprostoru se stávají stále populárnější sociální sítě (Leong, Morando, 2015).

4.2.1 Sociální síť

Pojem **síť sociální** je v sociologické encyklopedii definována jako “soubor sociálních subjektů, které jsou navzájem provázány určitými vztahy”. Především tento termín označuje uspořádání společnosti, která své vazby rozšiřuje mimo ustálené skupiny, jako jsou např. rodiny, spolky, sdružení atd. Podle sociálních sítí se dá dobře zjistit zařazení ve společnosti daného jedince. Sociální sítí (ang. – Social Network) je také nazývána služba dostupná prostřednictvím internetu. Uživatelé si na základě této platformy vytvoří veřejný profil a následně si vyberou a kontaktují konkrétní členy sítě. Navazují tak různé virtuální vztahy, které jim umožňují komunikaci mezi sebou, sdílení informací, videí, fotografií nebo odkazů apod. Obsah sociálních sítí je tedy utvářen jejími uživateli (KTD, 2014).

Členové sociálních sítí jsou jako virtuální komunikační médium nebo online komunita. V takové skupině může existovat více typů vazeb s různou povahou. Některé kontakty vzniknou z již reálných vztahů, které jen reagují na omezení prostorových či časových možností. Často se však utvoří také úplně nové komunity, jež sdílejí společné zájmy a jež mohou vést až k osobním setkáním. Z toho je tedy patrné, že tradiční i online skupiny se vzájemně prolínají a doplňují (Veselá, Šmahel, 2009). V posledních letech zaznamenaly sociální sítě obrovský nárůst popularity, avšak nenadálé nadšení může opadnout při zjištění, že se dá tento nástroj také snadno zneužít a představit tak hrozbu pro celou společnost (Luo, Liu, Liu, Fan, 2009).



Osoby v ČR používající sociální sítě podle způsobu zveřejňování informací, 2020

4.3 Nebezpečí sociálních sítí

Obvykle sociální sítě požadují po svých uživatelích vytvoření profilu, který jim umožní sdílení informací s ostatními členy platformy. Tyto údaje zahrnují většinou pohlaví, věk, zájmy, vzdělání a zaměstnání, popřípadě rodinnou situaci. Uživatelé si také mohou pravidelně aktualizovat svůj stav. Dále pak členové prostřednictvím těchto platforem sdílejí fotografie, videa a jiné příspěvky. Sociální sítě jim také umožňují, označovat polohu, kterou následně sledují, aby mohly například doporučovat události konající se v jejich okolí apod. Uživatelé si však často neuvědomují, že poskytují tyto informace inzerentům nebo hackerům (Privacy Rights Clearinghouse, 2019). **Fire, Goldschmidt a Elovici uvádějí, že členové aktivní na sociálních sítích mohou vystavit sami sebe ztrátě soukromí nebo nebezpečí**. Hrozby rozdělují do 4 kategorií:

- Klasické hrozby
- Moderní hrozby
- Kmbinované hrozby
- Hrozby cílené na děti

4.3.1 Klasické hrozby

Tyto hrozby se objevily již s rozvojem internetu. Jsou to zejména **malware, spam, phishing** nebo jiné útoky, které se dále rozšířily mezi sociální sítě vzhledem k jejich povaze. Hackeři pomocí těchto

virů využívají hlavně informace dostupné na profilu daného uživatele a snaží se prostřednictvím nich napadnout jeho přátele na síti. **Cílí především na údaje jako čísla kreditních karet nebo hesla k bankovnímu účtu apod.** (Fire, Goldschmidt, Elovici, 2014).

K několika snahám o celkové napadení sociální sítě již došlo, a to konkrétně v roce 2005 na **MySpace**, kdy útočník známý pod pseudonymem Sammy chtěl získat osobní data uživatelů. I když se mu to nakonec nepodařilo, jeho vniknutí mělo nebezpečný dopad na tuto sociální síť. V roce 2009 zažil nepříjemný útok také **Twitter**, kde byly nahrazeny informace uživatelů za nepoužitelná data. **Facebook** se pak potýkal s napadením, při kterém však již byla ukradena hesla několika uživatelů (Rathore, Sharma, Loia, Jeong, Park, 2017).

4.3.2 Moderní hrozby

Útočníci se v tomto případě obvykle zaměřují rovnou jak na osobní informace daného uživatele, tak zároveň i jeho přátel. Pokud chtějí hackeři získat citlivé údaje, mohou si vytvořit falešný profil a odeslat žádost o přátelství konkrétním osobám. Když bude přijata, zpřístupní se jim informace i kontakty, podle nichž dokážou odvodit soukromá data (Fire, Goldschmidt, Elovici, 2014). Některé sociální sítě jako například Twitter sice neumožňují zveřejňovat soukromé údaje, ale na základě obsahu, který uživatel sdílí na svém profilu, je mohou hackeři snadno odvodit (Rathore, Sharma, Loia, Jeong, Park, 2017).

4.3.3 Kombinované hrozby

Obě předešlé uvedené hrozby je možné také zkombinovat. Pomocí **phishingu** útočník získá heslo a zveřejní na profilu konkrétního uživatele odkaz, na který mohou vstupovat jeho přátelé a tím nahrají do svých počítačů vir. Dále může dojít k **ukradení identity** a posílání důvěryhodných **spamových zpráv**, přičemž tak hackeři získají osobní údaje od přátel daného uživatele, kteří se mylně domnívají, že se jedná o jejich kamaráda (Fire, Goldschmidt, Elovici, 2014).

4.3.4 Hrozby cílené na děti

Mezi uživateli sociálních sítí jsou také děti, které se mohou setkat jak s již zmíněnými hrozbami, tak i s útoky, které jsou zaměřeny přímo na ně. Jedná se například o interakci s **online predátory**, riskantní chování, kdy začnou komunikovat s neznámým člověkem apod. (Fire, Goldschmidt, Elovici, 2014).

Obecně ohromné množství těchto osobních informací na jednom místě, představuje obrovské riziko pro uživatele online komunikačních platforem, protože hackeři mohou prostřednictvím nich snadno získat citlivá data. **Sociální sítě jsou stále více zneužívány různými útočníky pro získávání osobních údajů** (Rathore, Sharma, Loia, Jeong, Park, 2017).

4.3.5 Zneužívání informací

V podstatě všechny sociální sítě umožňují svým uživatelům zveřejňovat nějaké informace. Každý, kdo také využívá tuto platformu, je může vidět. Přestože existuje způsob, jak transparentnost těchto dat částečně omezit a konfigurovat je alespoň jako soukromé, nelze to tak učinit u všech. **Navíc sociální síť někdy mění zásady ochrany osobních údajů, čímž znovu obnoví jejich nastavení a také většinou nezaručí uživatelům úplnou bezpečnost dat.** Kontakty, jež má uživatel přidané, mají možnost kopírovat a přeposílat jeho příspěvky nebo informace. Dále je udělen přístup k soukromým datům také tzv. *třetím stranám* (Privacy Rights Clearinghouse, 2019). Inzerenti získávají informace z online aktivit daného uživatele a následně jsou mu zobrazovány reklamy na sociálních sítích, které by měly odpovídat jeho zájmům. Data dostupná na těchto platformách mohou být také hodnotná v mnoha případech pro právní orgány. Mnohdy můžou zabránit nelegálním aktivitám. Pro potřeby ověření konkrétního člověka, využívají informace na sociálních sítích také zaměstnavatelé, kteří se na základě toho rozhodují, zda je daný jedinec pro profesi vhodný (Privacy Rights Clearinghouse, 2019).

Uživatelé své profily často zakládají i upravují s vědomím, že mohou prostřednictvím jejich vizualizace a dostupných informací ovlivnit názory ostatních na svou osobu. I když sociální sítě vyžadují, aby uživatelé o sobě uváděli nezbytné pravdivé údaje, ne všichni jsou přesní. Zároveň i sdílený obsah s veřejností prezentují dalším členům sítě, jak uznají za vhodné. Zatímco by mohli nechat zobrazit příspěvky jen pro sebe a jejich přátele, mnozí přesto rádi zpřístupňují svůj obsah veřejně (Hamburger, Vinitzky, 2010).

4.3.6 Interakce na sociálních sítích

Kyberprostor je v současné době také místem, které umožňuje online interakci. Lidé se scházejí prostřednictvím sociálních sítí (Mustafa, Hamzav, 2011). Nedílnou součástí bytí člověka je potřeba kontaktu s ostatními lidmi. V moderní společnosti se někteří jedinci cítí osaměle a izolovaně. Navíc v důsledku současné situace pandemie Covid-19 většina zemí zavedla restriktivní opatření v podobě sociálního distancování, aby nedocházelo k šíření nákazy. Možnost využití internetu a digitální podpora může tyto stavy osamělosti snížit (Aleman, Sommer, 2020).

Mnoho lidí však vystupuje na internetu anonymně a skrývají svou pravou tvář. Jejich chování navíc nemusí odpovídat tomu, jací jsou ve skutečnosti. **Komunikace ve virtuálním prostředí probíhá bez rozdílu a neklade žádné podmínky na věk, pohlaví nebo společenskou roli**. Proto často dochází k interakci mezi dospělým a dítětem, k překonávání různých komunikačních bariér, změně sociálního statutu apod. Tyto aspekty mohou vést k různým konfliktům (E-bezpečí, 2009).

Vzhledem k tomu, že osobní údaje uvedené na sociálních sítích nelze nijak ověřit, mnoho lidí včas nerozpozná uživatele, který je pouze manipulátorem a vydává se za někoho jiného. Často proto dochází k různým sociálně-patologickým jevům jako jsou například kyberšikana, kybergrooming,

sexting nebo kyberstalking atd. V některých případech komunikace prostřednictvím internetu může vést až k osobnímu setkání. Webová stránka **E-bezpečí** uvádí, že 42,5 % dětí se setká s člověkem, kterého znají pouze ze sociálních sítí (E-bezpečí, 2009).

4.4 Prevence

Každý uživatel by měl individuálně dbát zodpovědnosti a dávat si pozor, jaké informace na svých sociálních sítích zveřejní (Macháčková, 2011). Přesto však existují různá doporučení, která mohou pomoci zajistit větší bezpečnost na těchto platformách.

Nejprve by si měl uživatel přečíst **zásady použití a ochrany osobních údajů** před registrací. Při vytváření profilu, si může daný jedinec vybrat místo vlastního jména pseudonym, který ochrání jeho identitu. Mezi své kontakty by měl přijímat pouze osoby, s nimiž se opravdu zná. Nutné je také dobře promyslet, co člen sítě sdílí za obsah. Své osobní údaje si může předělat v nastavení sociální sítě, a navíc svá citlivá data by neměl nikomu sdělovat. Není doporučeno ani označování polohy, zaměstnání nebo prozrazování nepřítomnosti v domácím prostředí. Důležité je také omezení reakcí na různé reklamy a ze sítě se vždy odhlásit. Zároveň pro přihlašování do uživatelského účtu nevyužívat pracovní e-mail (Macháčková, 2011). Zvolení silného hesla může pomoci před možnými útoky hackerů. Na sociálních sítích se také šíří spoustu dezinformací, a ne všemu by měl uživatel zcela věřit. Vulgární zprávy raději ignorovat a neposílat nikomu citlivé údaje (Vohanková, 2019).

Sociální sítě jsou velmi populární a mají velký vliv na společnost. Mnoho uživatelů na nich sdílí nespočet informací každý den. Na těchto platformách se také může stát člověk závislý, pokud je využívá nadměrně. Naopak jejich výhodou je, umožnění navazování nových vztahů a celková podpora interakce mezi lidmi. Otázkou však zůstává, zda čím dál častěji nedochází k omezování osobní komunikace či setkávání se tváří v tvář v důsledku stále rostoucího stráveného času na sociálních sítích (E-bezpečí, 2009). **Nové průzkumy ohledně interakce během pandemie Covid-19 však ukázaly, že komunikace prostřednictvím technologií jako náhrada za osobní kontakt nestačí** (Kovacs, Caplan, Grop, King, 2021).

4.5 Závěr

Seminární práce Nebezpečí sociálních sítí a komunikace se zabývala tématem dorozumívání se a interakcí v kyberprostoru. Zaměřila se především na problematiku sociálních sítí, které mají obrovský celospolečenský vliv a představují mnohá rizika.

Každá sociální síť umožňuje svým uživatelům sdílet obrovské množství informací, zakládat profily s osobními údaji a vytvářet tak obsah na těchto platformách. Tato citlivá data bývají často napadána

útočníky, kteří se k nim snaží dostat pomocí šíření různých virů v podobě malwaru, phishingu apod., vytvářením falešných identit, popřípadě využíváním dětské důvěřivosti. Dalším neadekvátním jevem bývá poskytování těchto informací tzv. třetím stranám, což jsou například inzerenti, kteří se snaží ovlivnit uživatele cílenými reklamami ke koupi jejich produktů apod.

Na sociálních sítích je také možné navazování tzv. virtuálních vztahů. Dochází k sociální interakci, při které uživatelé tvoří online komunitu. Mnozí však využívají možnosti anonymního prostředí a zakládají si falešné profily, pod nimiž se vydávají často za někoho jiného. Dochází k riskantním známostem, popřípadě mnohdy i k různým socio-patologickým jevům jako jsou například kyberstalking, kyberšikana atd. Až 42,5 % dětí je ochotných setkat se osobně s někým koho znají jen přes sociální sítě.

Důležité je, aby uživatelé dbali na ochranu svých osobních údajů při používání těchto sociálních sítí, uvědomovali si, že jsou tyto informace veřejně dostupné a můžou vést k ohrožení jejich soukromí nebo bezpečnosti. Navíc by měli přijímat mezi své kontakty pouze lidi, které opravdu znají.

Sociální sítě jsou velmi populární, ale otázkou je, zda přílišné trávení času na těchto platformách, nemůže narušit osobní komunikaci a setkávání se tváří v tvář. Nové průzkumy týkající se mezilidské interakce v období pandemie Covid-19 však prokazují, že komunikace a setkávání se prostřednictvím technologií není dostatečnou náhradou za osobní kontakt.

4.6 Zdroje

Aleman, A., & Sommer, I. (2020). The silent danger of social distancing. *Psychological Medicine*, 2 strany. https://doi.org/10.1017/S0033291720002597

Amichai-Hamburger, Y., & Vinitzky, G. (2010). Social network use and personality. *Computers in Human Behavior*, 26(1289–1295), 7 stran. https://www.sciencedirect.com/science/article/abs/pii/S0747563210000580

Čech, J. (2010). *Sociální interakce v prostředí kyberprostoru* [Bakalářská práce, Univerzita Karlova]. https://dspace.cuni.cz/bitstream/handle/20.500.11956/37575/BPTX_2007_1_11210_ASZK00306_130314_0_37409.pdf?sequence=1&isAllowed=y

Facebook: American Company. (2021). *Britannica*. Retrieved July 28, 2021, from https://www.britannica.com/topic/Facebook

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys & Tutorials*, 16(4), 18 stran. https://doi.org/10.1109/COMST.2014.2321628

Guo, R. M. (2008). Stranger Danger and the Online Social Network. *The Berkeley Technology Law Journal*, 23(1), 28 stran. https://www.btlj.org/data/articles2015/vol23/23_1_AR/23-berkeley-tech-l-j-

0617-0644.pdf

Havlová, J. (20014-). *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*. Retrieved May 25, 2021, from https://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD#tail

IT slovník.cz: Co je to chat?. (2021). Retrieved May 25, 2021, from https://it-slovnik.cz/pojem/chat

Jak na internet. (2021). Cz.NIC. Retrieved July 28, 2021, from https://www.jaknainternet.cz/page/1236/komunikace-pres-internet/

Kovacs, B., Caplan, N., Grop, S., & King, M. (2021). Social Networks and Loneliness During the COVID-19 Pandemic. *Sage Journals*, (7), 1 strana. https://doi.org/10.1177/2378023120985254

Leong, N., & Morando, J. (2015). Communication in Cyberspace. *North Carolina Law Review*, 94(1), 57 stran. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=4762&context=nclr

Luo, W., Liu, J., Liu, J., & Fan, C. (2009). An Analysis of Security in Social Networks. *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 5 stran. https://doi.org/10.1109/DASC.2009.100

Macháčková, P. (2011). *Bezpečnost na sociálních sítích s důrazem na ochranu osobních dat* [Diplomová práce, Masarykova univerzita v Brně]. https://is.muni.cz/th/gztfh/Machackova_DP.pdf

Mustafa, S. E., & Hamzah, A. (2011). Online Social Networking: A New Form of Social Interaction. *International Journal of Social Science and Humanity*, 1(2), 9 stran. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/9CFFBF2802D6A6042A0707CD6D8E1052/S0033291720002597a.pdf/div-class-title-the-silent-danger-of-social-distancing-div.pdf

Myspace: Web site. (2021). *Britannica*. Retrieved July 28, 2021, from https://www.britannica.com/topic/Myspace

Nešpor, Z. R. (Ed.). (2018). *Sociologická encyklopedie: Síť sociální*. Retrieved May 25, 2021, from https://encyklopedie.soc.cas.cz/w/S%C3%AD%C5%A5_soci%C3%A1ln%C3%AD

Online Community. (2021). Cambridge Dictionary. Retrieved July 28, 2021, from https://dictionary.cambridge.org/dictionary/english/online-community

Privacy Rights Clearinghouse: Social Networking Privacy: How to be Safe, Secure and Social. (1992). Privacy Rights Clearinghouse. Retrieved May 29, 2021, from https://privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. -S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421(43-69), 27 stran. https://doi.org/doi.org/10.1016/j.ins.2017.08.063

((c) 2008-2020). Sociální sítě jako prostředí pro nebezpečnou virtuální komunikaci. *E-bezpečí*. Retrieved May 29, 2021, from https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/147-222

Suler, J. (1996). *The Psychology of Cyberspace*. Retrieved May 25, 2021, from http://users.rider.edu/~suler/psycyber/psycyber.html

Twitter: microblogging service. (2021). Britannica. Retrieved July 28, 2021, from https://www.britannica.com/topic/Twitter

Veselá, M., & Šmahel, D. (2009). Online komunity v České republice: Analýza členů a jejich sociálního kontextu. *Sociální studia/Social Studies*, 6(2), 1-18. https://doi.org/10.5817/SOC2009-2-55

Vohanková, A. (1988 - 2021). Přinášíme 10 tipů, jak se chránit na sociálních sítích. *Avast blog*. Retrieved May 29, 2021, from https://blog.avast.com/cs/socialni-site-bezpecne

4.7 Použité obrázky

Graf 5.1: *Osoby v ČR používající sociální sítě podle způsobu zveřejňování informací*, 2020. (2020). Český statistický úřad. Retrieved May 26, 2021, from https://www.czso.cz/documents/10180/122362692/0620042051.pdf/a1a8dd54-2158-45bb-81ab-4953e1b2dd1e?version=1.1

5 Kybernetické války

Autor: Lukáš Kudláček

5.1 Úvod

Seminární práce se bude vzhledem k omezenému prostoru v takto komplexním tématu zabývat úzkým výsekem kyberprostoru, a to **kybernetickými válkami**. Respektive používáním kyberprostoru jako útočného nástroje s cílem poškození buď kyberprostoru protivníka, nebo i objektů ve fyzickém světě, jako je například kritická infrastruktura. Jak lze usoudit, tyto nástroje hromadného útoku jsou natolik komplexní a náročné, že je využívají zejména státy. Respektive jejich armádní celky či zpravodajské služby. Ať už jde o oficiální nebo neoficiální cesty. Tyto nástroje jsou také využívány sofistikovanými skupinami hackerů, kteří se těmito útoky snaží získat finanční prostředky, slávu, a nebo jsou zkrátka posedlí destruktivními myšlenkami. V mnoha případech jsou tyto skupiny podporovány konkrétními státy a pracují tzv. *na zakázku*. Vzhledem k nedávným útokům na základní infrastrukturu, ať už na zdroje pitné vody, ropovody, elektrické sítě, nebo zdravotní zařízení, je toto téma velmi aktuální dnes i do budoucna.

V rámci práce bude přiblížen krátký vývoj kybernetických válek a některé konkrétní případy. Tři případy jsou v rámci práce stěžejní. Prvním případem je vytvoření a rozšíření viru **Stuxnet** jako prvního útočného kybernástroje s cílem ničit infrastrukturu protivníka. Druhým je několikaměsíční napadení desetitisíců společností za účelem krádeže duševního vlastnictví v kauze **SolarWinds** a třetí případ se zabývá **šířením dezinformací a nástrojů propagandy v kyberprostoru**, které slouží ke zmatení a ovlivnění obyvatelstva protivníka. Jako celek by práce měla sloužit ke krátké ilustraci toho, čemu jako lidstvo dnes čelíme a co nás čeká v budoucnosti v kontextu kyberprostoru, ve kterém se většina z nás pohybuje.

5.2 Kybernetické války

Jak již bylo uvedeno, kybernetické války jsou promyšlené a velmi sofistikované útoky na zájmy, kritickou infrastrukturu (vodovody, plynovody, elektrická síť, optické kabely, servery, dodavatelský

řetězec a další), průmyslová tajemství, bankovní systémy apod. konkrétního státu, jiným státem, či organizací najatou tímto státem. Tyto útoky probíhají prakticky neustále. Co je na těchto typech konfliktů zásadní, je změna přístupu k takovému typu válečného konfliktu, který je **decentralizovaný, asymetrický, postrádá hierarchii a odehrává se v kyberprostoru**, tedy ve virtuálním světě. Teprve důsledky takových útoků se projevují v hmotném fyzickém světě a často bývají velmi destruktivní. Nesouhlasím pak s názory, které popisují kybernetickou válku klasickým způsobem jako konflikt dvou států, neboť akt kybernetického útoku je aktem jednoho státu vůči druhému, často ale ani první stát nerozpozná, že na něho někdo útočí, popřípadě útočníka zjišťuje se zpožděním a následně na něho reaguje. **Kybernetická válka je tedy souborem asymetrických nárazových kybernetických útoků, na úrovni států.** Je zde pak nepodstatné, zda útok provádí konkrétní stát přímo prostřednictvím svého kybernetického oddělení armády, nebo ho nahrazuje profesionální hackerská skupina, které jsou daným státem poskytnuty finanční zdroje a zázemí pro její práci. Z tohoto důvodu jsou brány útoky těchto skupin z území Ruska, Severní Koreje, Íránu či Číny jako akty těchto států. **Kybernetická válka je součástí naší reality již od roku 2010.**

V klasickém pojetí válečného konfliktu, kterou do hloubky popisuje například **Carl von Clausewitz (2020)**, - autor jednoho z nejznámějších děl válečné teorie **O Válce**, kde komplexně popisuje různé typy historické i současné strategie války - je válka násilným činem, jehož cílem je přimět protivníka k naplnění naší vůle. Autor knihu napsal po napoleonských válkách *(1. vydání je z roku 1832 - poznámka editora)*, ve kterých byl sám účasten. Jiný autor historického klasického díla o válečném umění Sun C‘ (2008) s názvem **Umění války**, zase popisuje jako hlavní cíl války získání celého území nepřítele bez velkých škod, neboť ničení a rozdělování nenese takový prospěch. Autor v krátké knize popisuje různé typy útoků a obrany, zejména se věnuje způsobu klamu a získávání vítězství bez boje.

Byť mnoho aspektů moderní kybernetické války obsahuje ponaučení z obou uvedených děl, v základním bodě se liší. Moderní kybernetické války mají jediný cíl, a tím je zničit nepřítele, jeho infrastrukturu, data či hmotný majetek bez ohledu na konečný výsledek konfliktu. V klasickém válečném střetu se jednotlivé strany snaží o získání co největšího vlivu za nejmenších škod, neboť se zde jedná o nasazení lidských životů – vojáků a hmotné výzbroje, což stojí velké množství peněz a času. V kyberprostoru je naopak snaha o maximalizaci škod, neboť napsat škodlivý kód a nasadit ho na nepřítele stojí sice mnoho hodin vývoje, ovšem útočník sám osobně do boje nevstupuje. Vše se odehrává ve virtuálním světě – kyberprostoru. Tím se také kybernetické války liší od kyberterorismu, jehož cílem je většinou převzít kontrolu a dosáhnout vlastního cíle, ať už se jedná o manifestaci názoru, či získání výkupného.

5.3 Historie kybernetických válek

Přesto, že kyberprostor a digitální infrastruktura existují již delší dobu, z pohledu historie se stále jedná o velmi krátký časový úsek. Tzv. *informační války*, ze kterých teprve nedávno vzešly kybernetické války, jsou tu s námi mnohem déle, než samotný kyberprostor. Dříve se projevovaly ve formě **špionáže** a **propagandy**. Tento typ válek se omezoval pouze na získávání informací. Většinou šlo o formu odposlechů, získávání dat fyzickými, nebo později kybernetickými krádežemi či propagací dezinformací a ovlivňováním názorů veřejnosti. V přesném slova smyslu tyto informační války, které probíhají dodnes, nic neničí, pouze využívají slabostí systému k získávání dat a výhod. Tak jak to bylo a je běžné v klasickém válečnictví.

Tyto informační války probíhají dodnes. Například díky zveřejněným informacím v souvislosti s Edwardem Snowdenem (2020) víme, že je masivně sledována celosvětová komunikace a data jsou ukládána a analyzována pomocí klíčových slov. Víme, že probíhají obrovské **dezinformační kampaně** z tzv. *trollích farem*, které popsala finská novinářka Jessikka Aro (2020). Celosvětové sledování toku informací státními celky, ať už na americkém, evropském či asijském kontinentě, ruské či čínské dezinformační kampaně, nebo přímé krádeže duševního vlastnictví ze stran států jsou dnes běžné a daly by se považovat za součást kybernetické války. Ovšem jsou pouze informační válkou, nemají destruktivní povahu.

Kybernetické války jako takové začaly po sérii malých testů. Jako byly například útoky na estonskou webovou infrastrukturu Ruskem, napadení počítačové sítě Pentagonu v roce 2007 pravděpodobně Čínou či naopak napadením čínské počítačové sítě ze strany Taiwanu a USA v témže roce. Oficiálně začaly v roce 2010 vypuštěním velmi pokročilého viru jménem **Stuxnet**, který pravděpodobně vyvinula americká tajná služba NSA (Americká národní bezpečnostní agentura) ve spolupráci s izraelskou tajnou službou, jak je uvedeno v dokumentu Zero Days (2016). Měl za cíl zničení íránského jaderného programu. Případová studie rozšíření viru Stuxnet je uvedena dále v textu.

V roce 2011 byly napadeny kanadské, americké a francouzské úřady cizí mocností. V roce 2013 byla napadena infrastruktura jihokorejské televizní sítě a bankovních účtů ze strany Severní Koreje. Dalším významným bodem v kybernetických válkách byl ruský **DDoS (Distributed denial of service)** (Mirkovic&Reiher, 2004). Útok proti Ukrajině v roce 2014. DDoS útok se vyznačuje zapojením velkého množství napadených počítačů, které ve stejném okamžiku svými tzv. dotazy, zahlcují provoz konkrétní webové stránky či konkrétní služby nebo serveru, na kterých běží napadaný obsah. Může se jednat o web státních úřadů, platební službu banky, nebo chod chlazení v elektrárně. Takto napadený objekt pod náporem selže a útočník nad ním může převzít kontrolu. Tento konkrétní DDoS útok byl zahájen ruskou armádou za účelem zahlcení a následném spadnutí ukrajinského internetu v okamžiku záboru poloostrova Krymu proruskými rebely. Útok byl součástí klasické vojenské operace, a tedy kybernetickým válečným aktem. Téhož roku zaútočilo Rusko proti Ukrajině znovu. Zahltilo a následně svrhlo ukrajinskou volební komisi, což mělo mít za následek chaos a vítězství

proruského kandidáta.

V roce 2015 zaútočilo Rusko proti Německu, respektive proti německému parlamentu, za účelem získání tajných informací o Německu, NATO a jejich spojencích. Ve stejném roce zaútočila Čína proti Spojeným státům, konkrétně proti kanceláři civilních zaměstnanců, kde odcizila 21,5 milionů záznamů civilních zaměstnanců amerických úřadů včetně nepřijatých kandidátů. Tento útok naštěstí neměl za následek smazání těchto dat. V roce 2016 zaútočilo opět Rusko proti Ukrajině, a to na její základní infrastrukturu, elektrickou rozvodnou síť. Elektrická síť spadla v pětině kyjevské oblasti a v západní Ukrajině odstřihla více jak 225 tisíc domácností od elektřiny. Tento útok byl připravován více jak 6 měsíců.

V roce 2017 byl vypuštěn **ransomware virus** - druh škodlivého programu - (Scaife et al., 2016) pojmenovaný **WannaCry** (Wikipedia, 2020), který ve více jak 150 zemích zasáhl přes 250 tisíc počítačů a požadoval výkupné za jejich znovuzprovoznění. Virus byl rozšířen neznámou skupinou, nejvíce na území Ruska, Ukrajině, Indii a Taiwanu. Jednotlivé části kódu mohou pocházet z NSA, což ovšem není ověřené. **Tento útok je považován za součást kybernetické války**, protože ochromil například zdravotní systém ve Velké Británii, způsobil výpadek telefonních služeb ve Španělsku, vypnul železniční počítače v Německu…apod. Následně v roce 2017 byl vypuštěn na Ukrajině malware (Biscontini, 2020) virus s názvem **NotPetya** (Wikipedia, 2018), který již ale ne vždy požadoval výkupné, také jen ničil soubory a uložená data v počítačích s operačním programem Windows. Tento malware během jediného dne zničil více než 10% všech počítačů v zemi. Prvotní zásah byl, kromě nefunkčnosti systémů a rozsáhlé vymazání dat na Ukrajině v kyjevské oblasti zahrnující nemocnice, pošty, vládní úřady, bankomaty, veřejnou dopravu, také nemocnice v USA, továrny farmaceutického giganta Merck a terminály kontejnerové dopravy společnosti Maersk. Autorství je přisuzováno **hackerské skupině Sandworm** (Greenberg, 2019), která je součástí ruské zpravodajské služby GRU (Orr, 2018) a jednou z nejaktivnějších hackerských skupin.

V roce 2020 zaútočilo Rusko proti Spojeným státům, respektive **skupina APT29** napojená na ruskou tajnou službu GRU proti společnosti **SolarWinds**, jejíž produkty spojené s informačními systémy správců sítí používalo více jak 33 tisíc společností, jejichž data byla napadena. Oficiální počet napadených společností je 18 tisíc. Případová studie tohoto útoku je popsána dále (Temple-Raston, 2021).

V roce 2021 zaútočila dle nejnovějších odhalení ze strany amerických a britských úřadů Čína (Tucker, 2021) na USA v rozsáhlém **kybernetickém útoku na poštovní servery služby Exchange** americké společnosti Microsoft (Osborne, 2021). Tento útok se odehrál již na začátku roku, nicméně trvalo pět měsíců určení viníka, to potvrzuje, že kybernetická válka běží ve formě jednostranných aktů. Útok měl v sobě integrované 4 tzv. *zero days* (nulté dny). Škodlivý kód uměl napadnout a ovládnout poštovní server včetně kalendáře, který používá mnoho společností, úřadů, univerzit i jednotlivců, dostat se skrze něho do počítače, ukrást data, či rozesílat nepravé informace. Společnost Microsoft vy-

dala zabezpečovací upgrade až v březnu. Do té doby se útok týkal již miliónů serverů, mezi nimiž byl například Evropský bankovní úřad. Podrobnosti kódu se také objevili na různých fórech a jsou dodnes zneužívány dalšími hackery. Hlavním cílem jsou krádeže dat a těžba kryptoměn. V témže roce 2021 také proběhl masivní **útok na ropovody společnosti** Colonial Pipelines ze strany Ruska za účelem získání výkupného ve výši 4,4 milionů amerických dolarů. Vedlejším produktem bylo zjištění slabých míst v základní infrastruktuře. O tomto útoku je pojednáno dále v kapitole kritické infrastruktury.

Dalším výrazným útokem byl útok opět z Ruska hackerskou skupinou **REvil**, která je přímo napojena na ruský stát. Útok byl mířený na největší americkou společnost zpacování masa JBS (CNBC, 2021). Dopadem útoku byla blokace a přístup k datům, ovládání celého provozu a nakonec výpadek dodávek masných produktů do obchodních řetězců. Společnost zaplatila výkupné 11 milionů amerických dolarů za obnovení dat. Vedlejším efektem bylo opět nalezení slabých míst ve zpracovatelském řetězci.

Posledním zásadním útokem byl opět útok společnosti **REvil** za pomocí nulového dne v **největším dosud evidovaném ransomware útoku** na konkrétní společnosti, kterých bylo po celém světě napadeno více jak 1500. U každé chtěli výkupné za obnovu přístupu k datům celkem v hodnotě 70 milionů amerických dolarů. Útok byl proveden prostřednictvím společnosti **Kaseya**, která poskytuje spíše menším klientům softwarové nástroje na vzdálenou správu dat (Satter, 2021). Nejvíce zasaženou společností byl švédský potravinový řetězec **COOP**, který musel zavřít většinu obchodů ve Švédsku z důvodu nefunkčních pokladen. Zasažen byl také švédský řetězec lékáren, síť čerpacích stanic, státní železnice a veřejnoprávní televize STV. Na Novém Zélandu byly vyřazeny školy a školky. V Nizozemí a Německu byly zasaženy zejména malé podniky jako zubní ordinace, architektonická studia, centra plastické chirurgie, knihovny a podobně. Skupině REvil poskytuje útočiště přímo ruský stát.

5.4 Příklady kybernetických válek

5.4.1 STUXNET

Jak je uvedeno výše, virus Stuxnet byl použit při prvním skutečném kybernetickém útoku v rámci zničení kritické infrastruktury jiného státu. V dokumentu **Zero Days**, který popisuje vznik viru v průběhu první dekády 21. století a následný samotný průběh útoku na iránská jaderná zařízení, je zmíněna výpověď jednoho z hackerů, kteří virus stvořili. Údajně pracovali pro americkou Národní bezpečnostní agenturu NSA (2021). Ta se ve výrobě viru, který měl za cíl zpomalit militantní íránský jaderný program, spojila s tajnou službou **Mossad** (2021), národní zpravodajskou službou státu Izrael, který cítí bezprostřední ohrožení likvidací svého území ze strany Íránu. **Zde tedy máme první vážný kybernětický útok suverénního státu vůči jinému.** Nebere se zde v potaz útok z roku 2007, kdy Rusko zaútočilo na internetovou infrastrukturu Estonska. V té době byly offline prakticky všechny

webové stránky v daném státu a jednalo se o test bez fyzické destrukce.

Virus skutečně po dobu jednoho roku tiše útočil na jádrovou infrastrukturu závodu na obohacování uranu v Natanzu. Přeskočil tzv. *offline mezeru*, kde je samotný systém zařízení nepropojen s okolní infrastrukturou, čehož lze dosáhnout dvěma způsoby. Buďto fyzickou infiltrací přes USB disky či tzv. *přeskočením kódu ze zařízení do zařízení*. Tímto způsobem bez vědomí obsluhy několikrát zvýšil neúměrně rotaci centrifug na obohacování uranu, kterou následně rapidně snížil. Přeskočení kódu mělo za následek jejich destrukci. Výsledkem bylo zničení více jak pětiny centrifug a zpomalení programu o více jak rok. Dalším následkem byla frustrace íránských vědců, kteří nevěděli, co se děje a upadali v nemilost íránského režimu. **Tento virus byl od prvního útoku několikrát upravován a vylepšován a dodnes ničí íránskou infrastrukturu** (iRozhlas, 2020; The New York Times, 2021).

Snahou neustále stupňovat útoky na íránskou infrastrukturu ze strany Mossadu, ovšem virus unikl a v roce 2010 byl zaznamenán malou běloruskou antivirovou společností, která o něm podala zprávu bezpečnostní komunitě po celém světě (Zetter, 2014). Po celém světě se začal virus šířit a také zkoumat, nikdo nevěděl, kde se vzal a k čemu slouží. Po mnoha týdnech se podařilo zjistit, že virus byl napsán tak, aby útočil na klíčové ovládací zařízení společnosti Siemens, tzv. PLC (programmable logic controller), který řídí a kontroluje činnost čerpadel, ventilů, elektromotorů napříč celou infrastrukturou od vodovodů a plynovodů, přes čerpadla v elektrárnách po centrifugy a výrobní linky ve většině továrnách. Konkrétní čísla modelů a specifikací tohoto zařízení, včetně zpětné snahy o trackování viru se dala vystopovat do jaderného zařízení v Natanzu. Kód byl napsán tak čistě a přesně, včetně autodestrukčního řádku, že to poukazovalo na státní komplexní vývoj, který se na rozdíl od hackerských skupin či východních států zabýval i otázkami právního přesahu takového útoku. Ten byl následně přisouzen USA a Izraeli, kteří to nikdy oficiálně nepřiznaly.

Ovšem toto rozšíření viru do celého světa způsobilo napadení řady systémů, včetně systémů v samotných Spojených státech, evropských zemí, v Asii a Středním východě. To ukázalo všem, že je tu stát, který pomocí viru útočí na jiné státy, skrývá to a nenese přímou odpovědnost za útok, který se svou destruktivností rovnal konvenčnímu vojenskému zásahu. Rovnalo se otevření Pandořiny skříňky. To následně způsobilo rozvoj kybernetických zbraní nejen v samotném Íránu, který investoval velké množství prostředků na vývoj kybernetické armády (tedy hackerů ve službách státu), ale i v zemích jako Rusko, Čína či Severní Korea, kteří zjistili, že toto je způsob, jak útočit na citlivou infrastrukturu nepřítele, aniž by je někdo vedl ke zodpovědnosti. **To přineslo rozvoj kybernetických obranných sil v zemích NATO**, včetně České republiky. V celkovém rozsahu se vystupňoval rapidní rozvoj dnešních kybernetických útoků. Na závěr dokumentu **Zero days** uvádí bývalý hacker z NSA, že jsou připraveni Írán vypnout jako celek. Mají již mnohem pokročilejší zbraně, ktrými mohou zasáhnout infrastrukturu. Tedy Stuxnet byl základem toho, jak dnes pojmem kybernetické války chápeme.

Vypuštění a rozšíření viru Stuxnet mělo za následek také změnu ve vztazích jednotlivých států, zejména mezi USA a Íránem. Írán oficiálně obvinil USA z tohoto útoku a jako reakce byla silná protiam-

erická nálada v zemi, která ovlivnila většinu obyvatelstva. Írán v reakci na tento útok oficiálně založil kybernetickou odnož své armády a začal školit hackery, kteří jsou dnes za řadou vážných kybernetických útoků. Další narušení vztahu byla mezi arabskými zeměmi jako celek a Izraelem, kdy arabské země obvinily Izrael z tohoto útoku na Íran a uvědomili si, že stejně může zaútočit i na ně. Další přesah útoku bylo vyprovokování armády Severní Koreje, která oficiálně založila kybernetickou odnož armády a dnes stojí zejména za mnoha krádežemi kryptoměn, kterými posilují vlastní rozpočet. Stejně tak Čína mnohonásobně rozšířila svoji kybernetickou armádu a dnes patří k jedné z nejsilnějších na světě v této oblasti. Přesah narušení vztahů byl ale mnohem hlubší, zejména mezi USA a Evropskými zeměmi, které se necítili ohroženi, ovšem nesouhlasili s takto jednostranným aktem člena NATO.

5.4.2 SolarWinds

V roce 2020 zaútočila ruská skupina **APT29** (Cozy Bears) napojená na ruskou tajnou službu GRU proti Spojeným státům, konkrétně proti společnosti SolarWinds, jejíž produkty spojené s informačními systémy správců sítí používalo více jak 33 tisíc společností, jejichž data byla napadena. Oficiální počet napadených společností je 18 tisíc. Mezi těmito společnostmi bylo mnoho federálních úřadů v USA, například Agentura pro kyberbezpečnost a bezpečnost infrastruktury, Ministerstvo vnitřní bezpečnosti, zahraničí, financí, energetiky či Pentagon a komunikace na nejvyšší úrovni. Ovšem úřady byly napadeny napříč mnoha zeměmi, Českou republiku nevyjímaje. Tento útok probíhal po dobu devíti měsíců, než byl odhalen, a překonal digitální obranu USA. Mezi velkými korporacemi, které byly napadeny, byly například **Microsoft, Intel či FireEye** (společnost zaměřena na kyberbezpečnost). Útok měl výzvědnou povahu, monitoroval aktivitu dotčených subjektů, respektive veškerá jejich data. Naštěstí nemohl do informací zasáhnout, či je smazat. Technicky sice mohl, ale v rámci co nejdelší doby utajení to neudělal.

Prezident společnosti Microsoft uvedl, že se pravděpodobně jedná o **největší a nejsofistikovanější útok jaký zatím svět viděl.** Jako důvod uvedl rozsáhlost útoku. Skupina použila **malware Sunburst**, kterým infikovala populární software **Orion** od společnosti SolarWinds. Malware byl ukryt a nerozpoznán nastavenými bezpečnostními mechanismy společnosti a ve formě aktualizace softwaru byl rozšířen mezi jejích 18 tisíc zákazníků. Tím se malware rozšířil. SolarWinds Orion je jedním z nejrozšířenějších softwarových produktů, skládající se z miliónu řádků počítačového kódu. Z těchto řádků jich bylo 4032 tajně přepsáno a distribuováno rutinní aktualizací, čímž se otevřela zadní vrátka do 18 tisíc počítačových sítí. Sama společnost Microsoft na útok vyčlenila 500 svých inženýrů (Whitaker, 2021).

Právě rozšíření se infikace i do společnosti FireEye zabývající se kyberbezpečností, která také používala software Orion, se na útok přišlo, když si jeden z pracovníků společnosti všiml nesrovnalostí v kódu. Tou nesrovnalostí bylo, že jeden zaměstnanec měl přihlášené dva telefony, byť si přihlásil jen jeden. Po zkoumání se přišlo na to, že malware vydávající se za zaměstnance společnosti slídí

v jejich síti a krade patentované nástroje sloužící k obraně před takovými útoky. Hackeři nenechali žádné stopy. Po prozkoumání všech nástrojů, které společnost používala nakonec prošli těch několik miliónů řádků a objevili chybu. Tu pak oznámili světu.

Během té doby ovšem hackeři dokázali napáchat značné škody. Například měsíce sledovali e-mailový provoz ministerstva spravedlnosti v USA, stejně jako energetiky, financí, obchodu a dokonce i agentury, která chrání a přepravuje jaderný arzenál. Tyto cíle jednoznačně ukazují na zahraniční státní špionáž. Hlavním podezřelým se nakonec stala **ruská špionážní agentura SVR.** Je pravděpodobné, že se malware v tichosti rozšířil do dalších zařízení a infikoval mnohem více objektů a dodnes sbírá informace. Podobný přístup zvolila ruská agentura GRU v případě viru NotPetya na Ukrajině v roce 2017, ktrý byl zmíněn již dříve v textu. Jediným rodílem bylo to, že v případě Ukrajiny se infikované počítače zlikvidovaly. Pokud by se to stalo v případě SolarWinds, pak by následky byly katastrofické.

V těchto dvou útocích je jasně viditelný rozdíl mezi informační a kybernetickou válkou, a také jak tenká hranice mezi nimi panuje.

5.5 Současné hrozby

Současné hrozby kybernetické války jsou všudypřítomné. Hrozby vypnutí internetového připojení, zablokování telekomunikací, bankovních systémů, elektrické rozvodné sítě, ropovodů, či zásah do armádních systémů. To vše je na denním pořádku. Možný rozsah kybernetické války dobře ukazuje film **Smrtonosná past 4** (20th Century Fox, 2007) který je z roku 2007.

Po případech jako Stuxnet a SolarWinds víme, že to vše je reálné a jsme mnohem dál. Moderní přístroje - od mobilních telefonů až po chytré domácnosti - stupňují rozsah a možnou destrukci takové kybernetické války. Například útok na elektrickou rozvodnou síť dobře popisuje románová kniha **Blackout** (Elsberg, 2017), kde po dlouho připravovaném hackerském útoku na vodní elektrárnu v Maďarsku, chytré elektroměry v Itálii a páteřní trafostanice na několika místech v Evropě, dojde k přetížení celoevropské elektrické rozvodné sítě, která je navzájem pevně propojená. Následkem je několikatýdenní blackout a tím celkové ochromení obyvatelstva. Autor knihy čtyři roky sbíral materiál skutečného fungování evropské rozvodné elektrické sítě a možných reálných dopadů přetížení, kniha tak poskytuje náhled na možný černý scénář, který by reálně mohl nastat po takovém kybernetickém útoku.

To je pouze jeden z mnoha příkladů. Vezměme si útoky již zmíněné: ropovod, zpracovatelský průmysl, serverové softwary, elektrické sítě, pošty, řetězce, přístavy. Citlivým cílem je rovněž finanční sektor, jehož destabilizace by mohla značně zasáhnout každého z nás a zdravotnická zařízení, která jsou v dnešní pandemické době pod neustálými útoky. Školní vzdělávací systém, veřejná doprava, letecké terminály, prakticky vše, na co si dnes vzpomeneme, lze napadnout ve formě kybernetického útoku.

5.5.1 Dezinformace a propaganda

Je otázkou, zda zařadit šíření dezinformací a propagandy do kybernetické války, nebo je ponechat spíše v informační. Informační války historicky známe až od té doby kdy se začaly ve velkém rozšiřovat propagandistické letáky. Brigádní generál Řehka, současný ředitel Národního úřadu pro kybernetickou a informační společnost (NÚKIB, 2021) uvádí ve své knize **Informační bezpečnost** (Řehka, 2017), že "kybernetická válka je neoddělitelnou součástí válek informačních, neboť se jedná o válku v informačním prostředí a kybernetický prostor je neoddělitelnou součástí informačního prostředí".

V dnešní době se mluví zejména o ruských **dezinformačních kampaních**, které mají za cíl měnit názory a postoje v západní společnosti, což je také uvedeno v již zmíněné knize Putinovy trollové. Jedná se o taktiku vytváření celospolečenského narativu, který má vyobrazit Rusko jako oběť západního světa. Nepochopené, bez nároku na svou politiku a odlišný postoj ke standardu západních hodnot. Tyto dezinformační kampaně připravují půdu pro nárůst proruských nálad, vzedmutí odporu proti západním zemím v čele s USA a NATO, a následný podklad pro reálnou politickou či dokonce vojenskou intervenci. V roce 2007 vedlo Rusko silnou dezinformační kampaň v Estonsku, kterou po připravení půdy následně využilo pro napadení v kyberprostoru spolu s oficiální politickou intervencí za ruskou menšinu v Estonsku a za svůj vliv na pobaltské země, o který přišlo. Podobným krokem dezinformačních kampaní připravilo půdu pro reálnou vojenskou intervenci v roce 2008 do Gruzie, kde se následně odštěpila separatistická republika Abcházie. Následovala Ukrajina v mnoha podobách. V dnešní době útočí Rusko dezinformačními kampaněmi na USA a Evropské země zcela běžně. U nás v České republice je jasně patrné, nakolik se dezinformační kampaně podepisují na proruských a protiamerických náladách ve společnosti. Jedná se tedy také o nedílnou součást kybernetické války, řekněme že se jedná o její první stupeň. Dezinformační kampaně za cílem zmatení protivníka či ovlivnění a rozkladu protivníkova obyvatelstva provádí mnoho států na světě, včetně západních.

Další úroveň dezinformační kampaně je **propaganda**. Propaganda je účelné matení nepřítele a donucení ho přijmout náš pohled na svět. Propaganda je využívána mnoho staletí a od dezinformačních kampaní se odlišuje zejména tím, že propaganda nepracuje pouze s nepravdivými informacemi, ale i s pravdivými a přesnými informacemi. Jde o informace, které protivník nechce zveřejňovat svému obyvatelstvu. Propaganda má dlouhou historii, kterou popisuje kniha od Phillipa Taylora (2003) "Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era," kde autor shrnuje historický vývoj propagandy a její různé podoby, včetně konkrétních příkladů, protože Čína, která používá propagandu jako nedílnou součást masivní informační války, a to s přesahem do reálných kybernetických útoků. Čína se snaží v prvé řadě získat sympatie a pozornost na svou stranu, obhájit své komunistické myšlenky jejich srovnáním se západními myšlenkami a následně postavit roli západu, zejména Spojených států, do postavení její podřízenosti. **Čínská propaganda** je postavena na několika úrovních. První úrovní je fyzická infiltrace, pomocí peněz, a to do mezinárodních institucí,

univerzit, rozvojových zemí, kde propaguje svůj světonázor a postavení největší světové mocnosti. Druhá úroveň představuje infiltraci názorů do médií, jak televizí, tak novin, opět prostřednictvím peně. Platí si obsah ve velkých seriózních médiích jako je CNN či New York Times, které publikují její propagandu. Na třetí úrovni její propagandy jsou sociální sítě. Zde se již dostáváme do úrovně kybernetické války, neboť za Čínu vystupuje armáda státem placených hackerů, kteří vstupují na sociální sítě, kde se infiltrují, mění obsah příspěvků a v komentářích hlásají svou propagandu. Tyto aktivity potom přerůstají do infiltrací počítačových sítí a krádeže duševního vlastnictví. Čtvrtou a poslední úrovní propagandy je destabilizace a ničení infrastruktury protivníků, kde jsou využíváni nejlepší státem placení hackeři, kteří koordinují předchozí úrovně. Bavíme se tu o statisících až milionech lidí, kteří se tomuto věnují a snaží se ovlivnit celosvětovou veřejnost. Zároveň se snaží ukrást co nejvíce informací aby předehnala svět ve výzkumu a vývoji.

Dezinformační kampaně a propaganda jsou nástroje kybernetických válek. Jak je vidět, oba zmíněné státy používají odlišnou techniku. Rusko na jedné straně používá asymetrický informační nátlakový systém způsobený malými, zdánlivě samostatnými skupinami hackerů. Čína naproti tomu postupuje velmi symetricky, systematicky a v mnohem větším a hlubším rozsahu za pomoci oficiální armády. Proč obě země zmiňuji, je fakt, že obě mají za cíl destabilizovat západní společnost, tedy naši společnost. Mnoho dalších zemí používá stejné nástroje, jsou většinově ovšem lokální, jako například blízký východ, nebo úzce vymezené. Tyto dvě země je používají v celosvětovém měřítku.

5.5.2 Útoky na kritickou infrastrukturu

Nejčastější cíle koordinovaných kybernetických útoků jsou na **základní infrastrukturu**. Zejména na datovou infrastrukturu, tedy koncová zařízení, servery, routery, optické kabely apod. Zde se potkávají snahy státních celků se snahami velkých i malých skupin hackerů, či jednotlivců. Máme zde etické hackery, tedy ty, co se snaží upozornit na chyby v systému, máme tu černé hackery, kteří chtějí proniknout do systémů a použít je, a máme crackery, kteří chtějí proniknout do systému a napáchat v něm co největší škody. O tomto tu však hovořit nebudeme. Nejznámější takový útok byl na společnost SolarWinds, který byl popsán v předchozí kapitole. Tento útok byl ze strany ruského státu, který po dobu devíti měsíců stahoval data ze společností. Reálný přesah kybernetické války do fyzické infrastruktury, tedy do elektrické sítě, zdrojů pitné vody, ropovodů, nádraží, letišť, telefonních sítí apod. je to, co započalo virem Stuxnet. Stuxnet napadl fyzickou infrastrukturu jaderného zařízení v Natanzu a od té doby dále ničí základní infrastrukturu Íránu, včetně petrochemických závodů, elektráren, plynovodů a vodovodů, je dnes standardem.

Posledním takovým útokem byl letošní útok hackerské skupiny DarkSide na společnost Colonial pipeline (ZDNet, 2021), která operuje třetinu toku ropy v USA, ropovody, rafinérie, zásobníky. Společnost měla zablokovanou celou počítačovou infrastrukturu podmíněnou výkupným, které nakonec zaplatila. Následkem bylo vyprázdění mnoha benzínových pump a nedostatek paliva.

Taková situace byla v USA nevídaná od ropné krize v osmdesátých letech minulého století. Pro mnoho obyvatel to byl naprostý šok. Chvilku se zamysleme nad tím, že by šlo o cílený útok, který by měl za následek odstavení nepřítele od základní suroviny - paliva. Ruská skupina Darkside (FireEye, 2021) používá tzv. Zero days, tedy nástroj, kdy dochází k infiltraci, ale virus nic neudělá, dokud nepřijde nultý den. Poprvé byl použit v rámci viru Stuxnet, který byl podrobně popsán v případové studii. Zda má skupina vazby na ruský stát je zatím neznámé. Je ovšem zcela logické, že pokud by stát chtěl použít podobný útok, uspěl by také.

Jiný letošní útok měl za cíl zásobárnu pitné vody ve městě Oldsmar na Floridě, který infiltroval počítačový systém rozvodny a zvýšil úroveň hydroxidu sodného ze 100 jednotek na 11 tisíc jednotek na milion. Tedy tak, že je to zdraví velmi nebezpečné. Útok se podařilo odhalit a zvýšení dávky zastavit. Podobný útok se stal v jiném americkém městě v roce 2015 a 2016, podobný útok cílil také na zásobárny pitné vody, vodní čerpadla a závlahové systémy v Izraeli na jaře a v létě roku 2020. Ten označil za útočníka Íránské ozbrojené síly (ZDNet, 2021).

Případů ohrožení kritické infrastruktury je velmi mnoho. U nás byla napadena **zdravotní zařízení** - nemocnice v Benešově na konci roku 2019 (Seznam, 2019) a v Brně v roce 2020. To jsou jen nejviditelnější případy. Případů útoku na nemocnice jsou za poslední roky jen u nás tisíce a milióny jich pak jsou celosvětově. Hackerský útok na české nemocnice se podařilo vypátrat do Ruska (Seznam, 2020). Zda mají útoky vazbu na ruský stát jako takový a jsou součástí kybernetické války vedené proti našemu státu je otázkou. To, že mají státy tyto schopnosti je ovšem fakt a je potřeba se připravit na podobné scénáře i v budoucnosti.

5.6 Budoucí hrozby

Vzhledem k rozsahu zmíněných útoků, jejich sofistikovanosti a dlouhodobé přípravě, a také vzhledem k přijímání obranných opatření na úrovni armádních celků je jasně patrné, že kybernetické války budou pokračovat i nadále. Zde se ovšem dostáváme do bodu, kdy je potřeba zmínit co nás čeká. Dnešní moderní svět je již na pokročilých technologiích závislý, neobejde se bez nich ani v obstarání základních surovin a potravin. A svou závislost dále rozvíjí a zesiluje. Mezi další nastupující body napadnutelné kritické infrastruktury v následujících letech bude všudypřítomný internet věcí spojený s pokročilými sítěmi 5G nové generace. To v překladu znamená, že se připojí na internet i věci jako ledničky, pračky, kotle, ale i například kávovary, nemluvě o rozvoji chytrých domácností zahrnujících osvětlení, klimatizaci, rolety a mnoho dalšího. Dokážeme si představit možný rozsah škod pokud by byl takto propojený systém napadnut a ničen.

Další podstatným bodem je **rozvoj elektromobility a autonomního řízení**. V dnešní době je napříč světem protěžována elektromobilita, bez ohledu na vzrůstající požadavky na elektrickou rozvodnou síť. Ta bude významně přetěžována a stejně tak jako nové zdroje elektřiny ji nedokážeme do roku 2030

nijak významně navýšit. Tedy je ohrožena síť jako celek, ta síť, která již dnes je v Evropě téměř každý den na okraji blackoutu z důvodu masivního zapojování obnovitelných zdrojů, které mají nestabilní dodávky elektřiny (O Energetice, 2021). To je ovšem jen jeden možný následek napadnutí elektromobility. Druhý a stejně závažný následek by byl, pokud by byly v rámci kybernetického útoku napadeny řídící systémy vozidel, konkrétně jejich systém vidění okolního světa, ať již pomocí kamerového systému či moderního radaru LIDAR. Nebo autopilot, to by mohlo mít za cíl naprostý chaos ve veřejné dopravě.

Zásadními rozvíjejícími se oblastmi kritické infrastruktury, které mohou být napadnutelné z pohledu kybernetických válek jsou také **databáze databází a přesun osobních, podnikových a vládních dat na cloudové řešení**. Tyto cloudy na jedné straně pomáhají překlenout útok na fyzickou infrastrukturu jako v případě útoku na ropovody společnosti Colonial. Na druhé straně přinášejí závislost na přihlášení k virtuálnímu místu, kde jsou uložená veškerá data. Což je velmi zranitelná cesta. Podobný útok jako v případě SolarWinds by mohl touto obrannou cloudu proniknout a poté jsou ohrožena veškerá korporátní tajemství.

A poslední důležitou oblastí jsou jistě **big data a decentralizace**. Big data jsou budoucností mnoha sektorů ekonomiky, od průmyslu po oděvní společnosti, kde se snaží všichni kolektovat obrovské množství dat ze svých procesů a optimalizovat je tak aby šetřili náklady a maximalizovali zisk. V dnešní době je mnoho společností jako je například **Palantir**, které procesují milióny vstupů dat v reálném čase a vyhodnocují je za pomocí algoritmů a pokročilého strojového učení. Jejich databáze jsou velkým lákadlem pro kybernetické útoky. Společnosti typu Palantir jsou ovšem na tyto útoky dobře připraveny, je tu však velké množství společností, které si tato data snaží zpracovávat sami a úroveň zabezpečení je nízká. Pak tu máme společnosti jako **C3.ai**, které nabízejí určitou formu umělé inteligence pro správu a optimalizaci datových toků, kde například tato společnost vytváří stínové procesní řízení elektrárenské sítě v několika oblastech v USA či optimalizuje chod těžebních ropných plošin. Útok na takový typ společnosti by mohl mít katastrofální následky. Nehledě na to, že většinu společností jako je Palantir používají celky, které nás mají před kybernetickou válkou chránit, tedy armáda a zpravodajské služby. Jisté je, že jednotlivých cílů kritické infrastruktury bude přibývat.

5.7 Obrana proti kyberválkám

Na začátku zmíněný autor knihy Umění války, Sun C' řekl, že *„…získat sto vítězství ve stovce bitev není znakem vynikajícího vojevůdce. Pravým znakem vynikajícího vojevůdce je podrobení nepřátel bez boje.“* Přesně tak se dnes buduje obrana proti kybernetické válce. Dnes již více jak sto států světa buduje **kybernetickou obranu**, ať již na rovině **civilní**, tak na úrovni **vojenské**. Jedná se tedy o stavění mohutné obranné síly, která by odstrašila jednotlivé pokusy o kybernetické útoky a která by byla připravena na možnost kybernetické války. U nás v České republice máme dvě roviny obrany proti kybernet-

ickým útokům. První je civilní obrana, kterou zastupuje *Národní úřad pro kybernetickou a informační bezpečnost*. Druhou rovinou je **vojenské zpravodajství**, které převzalo úkol kybernetické obrany na úrovni armády České republiky (Ministerstvo Obrany, 2021).

Druhou linií obrany musí ovšem být lepší **fyzické zabezpečení kritické infrastruktury** nezbytné pro chod státu a života obyvatelstva. Například zabezpečení přístupu ke zdrojům pitné vody, ochranná pásma okolo elektráren, výstavba zálohových trafostanic, posílení serverových uzlů, budování silnějších firewallů, upgradování informačních systémů apod. Třetí linií obrany by nakonec mělo být i lepší **vzdělávání obyvatel** v rámci informační bezpečnosti a podnícení je k zodpovědnějšímu chování vůči možným kybernetickým hrozbám.

5.8 Závěr

Na závěr bych rád podotknul, že kybernetické války s rozvojem kybernetické společnosti jsou budoucností ozbrojených konfliktů mezi státy i v rámci asymetrického boje různých zájmových skupin. Tyto potenciální útoky na kritickou infrastrukturu mohou výrazně ovlivnit lidskou společnost tak, jak ji známe. Čím více se bude lidstvo stávat závislejší na pokročilých technologií, tím náchylnější společnost bude. Hrozba blackoutu, hrozba otravy pitné vody, hrozba nefunkčního cloudu či bankomatu je více než reálná a pravděpodobnost skutečně černého scénáře je čím dál vyšší.

5.9 Zdroje

20th Century Fox. Smrtonosná past 4.0 (Live Free or Die Hard) [film]. Režie Len Wiseman. USA: 20th Century Fox, 2007.

ARO, Jessikka. Putinovi trollové. Praha: N Media, 2020. ISBN 978-80-907922-1-0.

BISCONTINI, Tyler. Malware: Computer Security. Salem Press Encyclopedia of Science [online]. 2019 [cit. 2021-7-26].

CLAUSEWITZ, Carl von. O Válce. Praha: LEDA, 2020. ISBN 978-80-7335-672-9.

CNBC. JBS, world's largest meat producer, getting back online after cyberattack. CNBC [online]. USA: CNBC, 2021 [cit. 2021-7-25]. Dostupné z:https://www.cnbc.com/2021/06/02/jbs-worlds-largest-meat-producer-getting-back-online-after-cyberattack.html

ELSBERG, Marc. Blackout: Zítra bude pozdě. Praha: Dobrovský, 2017. ISBN 978-80-7390-188-2.

FireEye. Shining a Light on DARKSIDE Ransomware Operations. FireEye [online]. USA: FireEye, 2021 [cit. 2021-5-29]. Dostupné z: https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html

GREENBERG, Andy. Snadworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Anchor Books, 2019. ISBN 978-0-525-56463-8.

iRozhlas. Osmá exploze během tří týdnů. V Íránu vybuchl průmyslový komplex na úpravu zemního plynu. IRozhlas [online]. Praha: Český rozhlas, 2020 [cit. 2021-5-29]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/iran-vybuch-pozar-prumysl-tovarny-izrael_2007141651_aur

Ministerstvo Obrany. KYBERNETICKÁ OBRANA. Vojenské zpravodajství [online]. Praha: Ministerstvo obrany, 2021 [cit. 2021-5-29]. Dostupné z: https://www.vzcr.cz/kyberneticka-obrana-46

MIRKOVIC, Jelena a Peter REIHER. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communications Review [online]. 2004, 2004, 2004(34), 39-53 [cit. 2021-5-29]. ISSN 01464833. Dostupné z: doi:10.1145/997150.997156

Mossad. About Us. Mossad: Israeli secret inteligence service [online]. Izrael: Mossad, 2021 [cit. 2021-5-29]. Dostupné z: https://www.mossad.gov.il/eng/about/Pages/default.aspx

NSA. Mission & Values. NSA/CSS [online]. USA: NSA, 2021 [cit. 2021-5-29]. Dostupné z: https://www.nsa.gov/about/mission-values/

NÚKIB. NÚKIB [online]. Brno: NÚKIB, 2021 [cit. 2021-5-29]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

Nulté dny (Zero Days) [film]. Režie Alex Gibney. USA, 2016.

O Energetice. Evropská přenosová soustava zažila v pátek nejzávažnější incident za posledních 14 let. O Energetice [online]. Třebíč: OM Solutions, 2021 [cit. 2021-5-29]. Dostupné z: https://oenergetice.cz/prenos-elektriny/evropska-soustava-patek-tesne-unikla-blackoutu-jednalo-se-nejzavaznejsi-incident-za-poslednich-14-let

ORR, Trystan. A Brief History Of Cyberwarfare. GRA Quantum [online]. USA: GRA Quantum, 2018 [cit. 2021-5-29]. Dostupné z: https://graquantum.com/a-brief-history-of-cyberwarfare/

OSBORNE, Charlie. Everything you need to know about the Microsoft Exchange Server hack. ZDNet [online]. USA: ZDNet, 2021 [cit. 2021-7-25]. Dostupné z: https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

ŘEHKA, Karel. Informační válka. Praha: Nakladatelství Academia, 2017. ISBN 978-80-200-2770-2.

RID, Thomas. Cyber War Will Not Take Place. Journal of Strategic Studies. 2012, (35), 5-32. ISSN 1743937X. Dostupné z: doi:10.1080/01402390.2011.608939

SATTER, Raphael. Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says. Reuters [online]. USA: Reuters, 2021 [cit. 2021-7-25]. Dostupné z: https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

Seznam. Nemocnici v Benešově ochromil počítačový virus. Problémy mohou trvat týdny. Seznam zprávy [online]. Praha: Seznam, 2019 [cit. 2021-5-29]. Dostupné z: https://www.seznamzpravy.cz/clanek/nemocnici-v-benesove-ochromil-pocitacovy-virus-rusi-se-operace-84575

Seznam. Místo kyberútoků na české nemocnice odhaleno. Stopy vedou na sever Moskvy. Seznam zprávy [online]. Praha: Seznam, 2020 [cit. 2021-5-29]. Dostupné z: https://www.seznamzpravy.cz/clanek/misto-kyberutoku-na-ceske-nemocnice-odhaleno-stopy-vedou-na-sever-moskvy-106710

SCAIFE, Nolen, Henry CARTER, Patrick TRAYNOR a Kevin R.B. BUTLER. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In: Proceedings - International Conference on Distributed Computing Systems. Japonsko: Institute of Electrical and Electronics Engineers, 2016, s. 303-312. ISBN 978-150901482-8. Dostupné z: doi:10.1109/ICDCS.2016.46

SNOWDEN, Edward. Nesmazatelné záznamy. Frýdek-Místek: Alpress, 2020. ISBN 978-80-7633-216-4.

SUN, C'. Umění války. Brno: B4U Publishing, 2008. ISBN 978-80-903850-6-1.

TAYLOR, Philip M. Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era. Second edition. USA: Manchaster University Press, 2003. ISBN 0-7190-6767-7.

TEMPLE-RASTON, Dina. A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR [online]. USA: NPR, 2021 [cit. 2021-5-29]. Dostupné z: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1622254904545

The New York Times. Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. The New York Times [online]. USA: The New York Times, 2021 [cit. 2021-5-29]. Dostupné z: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html

TUCKER, Eric. Microsoft Exchange hack caused by China, US and allies say. Associated Press: AP News [online]. USA: Associated Press, 2021 [cit. 2021-7-25]. Dostupné z: https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35

Wikipedia. WannaCry. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2021-5-29]. Dostupné z: https://cs.wikipedia.org/wiki/WannaCry

Wikipedia. Petya (malware). Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2018 [cit. 2021-5-29]. Dostupné z: https://en.wikipedia.org/wiki/Petya_(malware)

WHITAKER, Bill. SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments. CBS News [online]. USA: CBS News, 2021 [cit. 2021-7-25]. Dostupné z: https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/

ZDNet. Colonial Pipeline attack: Everything you need to know. ZDNet [online]. USA: ZDNet, 2021 [cit. 2021-5-29]. Dostupné z: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-

everything-you-need-to-know/

ZDNet. Hacker modified drinking water chemical levels in a US city. ZDNet [online]. USA: ZDNet, 2021 [cit. 2021-5-29]. Dostupné z: https://www.zdnet.com/article/hacker-modified-drinking-water-chemical-levels-in-a-us-city/

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the Worlds First Digital Weapon. USA: Broadway Books, 2014. ISBN 978-0-7704-3619-3.

6 Jak digitální technologie mění lidské myšlení

Jana Bednářová

6.1 Úvod

Obsah textu se v krátkém přehledu zaměřuje na moderní technologie a na člověka z hlediska vzájemného působení reálného světa a kyberprostoru. Nepředkládá možná řešení technických a technologických faktů, ale zabývá se otázkou, jak se mění lidské myšlení vlivem digitálních technologií, zároveň nastiňuje možné přínosy i negativa těchto jevů. Tématu se v současné době věnují specialisté z různých vědních oborů, zejména z psychologie, sociologie, neurovědy, informační vědy a jiné (Gardner, 2018; Greenfield, 2016; Prensky, 2012; Spitzer, 2014). Za jednu z hlavních oblastí, v níž se k sobě výzkumné problémy interdisciplinárně přibližují, lze považovat zejména spojení několika dimenzí myšlení a využití znalostí a dovedností na základě určitých metod podporujících lidskou mysl (vzájemné ovlivňování a působení vlastních zkušeností v souvislosti s využíváním digitálních technologií).

Moderní technologie během let nepochybně změnily způsob, jakým žijeme, jak myslíme a jak přistupujeme k řešení problémů. Informační technologie se stále více ukotvují v našem každodenním životě, následkem čehož se hranice mezi lidmi a kyberprostorem tenčí a lidská bytost lapená do sítě virtuálního světa se pomalu přetváří na „*kyberorganismus*“ (v přeneseném smyslu „*kyberneticky řízený organismus*“, ať již ve smyslu rozumového či fyzického ovlivnění). Stejně jako všechny ostatní přeměny civilizace se i tato transformace zatím jeví jako nevratná. Přináší s sebou ztráty i zisky. Digitální technologie představují novou etapu v historii lidského myšlení a je příhodné se zamyslet nad tím, jaký vliv mají na lidský mozek – uvažování, paměť, učení a jednání. Odhalení možných negativních dopadů tohoto jevu a nalezení potenciálu jejich každodenního využívání může být dáno do souvislosti s dalším utvářením lidské budoucnosti. Ať je to fakt či idea, všichni se nakonec nějak musí vypořádat s inteligentními, vzájemně propojenými všudypřítomnými prostředími podporovanými kybernetickým světem. Nezáleží na tom, zda se již do světa protkaného digitálním prostorem narodili, či se s ním setkali v průběhu svého života.

6.2 „Stavíme nový svět, všechno je možné“

(Mitchell, c2004)

Dopad moderních technologií vykresluje odlišný způsob myšlení a učení dnešních dětí a mladých lidí oproti předchozím generacím. Americký spisovatel a lektor Marc Prensky ve své práci použil pro rozlišení těchto dvou protipólů dnes již běžně používané termíny „*digitální domorodec*“ a „*digitální přistěhovalec*“ (Prensky, 2001). Digitálního domorodce Prensky vysvětluje jako někoho, kdo se do digitálního světa narodil, bezděčně vnímá a jako houba nasává schopnosti a dovednosti moderních technologií ze svého okolí a automaticky je uplatňuje v běžném životě. Digitální přistěhovalec si naproti tomu musí dovednosti nejprve praktickými cvičeními či memorováním osvojit, aby je mohl využívat. Někteří digitální přistěhovalci se adaptují rychleji, jiným zůstává jistý „*přízvuk*“, kterého se nikdy nezbaví. Zajímavostí je, že každý z nich používá jinou část mozku na stejnou činnost, jak tvrdí Prensky. Velkou roli hraje způsob používání primární paměti (co člověk zná a dokáže na to ihned odpovědět) a sekundární paměti (o čem člověk ví, jak to najít, a odpoví po nalezení odpovědi), které ve své prezentaci o kybernetické společnosti zmiňoval docent Jirovský (Jirovský, 2021). Jak bylo poznamenáno, primární paměť se stále zmenšuje, zato se zvyšuje objem dat v kyberprostoru, který lze využívat pomocí paměti sekundární. Informační záplava tak způsobila rozkol v původním užívání primární a sekundární paměti. Lidský mozek v digitální době více selektuje, které informace je potřeba uložit a které si pamatovat nepotřebuje. Namísto toho si spíše uchovává povědomí o tom, jak se k potřebné informaci rychle dostane. Příkladem může být situace, kdy v mysli pátráme po telefonním čísle na přítele – víme, kde máme kontakt uložen, ale na číslo si nevzpomeneme.

Digitální technologie mění život člověka v různých aspektech a jistě by bylo naivní si myslet, že nemění i způsob fungování jeho mozku. Lidé se v podstatě lépe než většina jiných druhů dokáží již po staletí adaptovat na měnící se svět. Když se rozvinuly informační technologie, jako by se objevil svět paralelní. Lidé jsou kyberprostorem od jeho vzniku přitahováni, stává se postupně životním stylem a rozšířením některých funkcí jejich mozku. Ten na jednu stranu tlumí některé dovednosti, na druhou stranu rozvíjí další – přechází od zapamatování po hledání. Způsob, jak moderní technologie používáme, pozměnil modus lidského myšlení. Internet je zábavou, slouží k přehrávání hudby, ke čtení, k hraní her, ale zahrnuje i společenský život, nákupy, práci a učení, uspokojuje touhu po vědění a sociálním (virtuálním) kontaktu. Svět virtuální částečně vytlačuje a nahrazuje skutečný život (Greenfield, 2016 s.33-40).

Lidský mozek prochází nepřetržitou fyzickou změnou a přetváří se v reakci na vnější podněty, prostředí a zkušenosti (Greenfield, 2016 s.76-78). Když se ohlédneme dále do minulosti, do doby orální kultury v místě, kdy se střetla s vynálezem hláskové abecedy a písma a od orality se posunula ke gramotnosti, najdeme zde určité paralely s přeměnou současného světa stále více využívajícího všudypřítomné technologie – jde mj. o souvislosti s neurofyziologickými změnami v lidské mysli. V orální kultuře se slova omezovala pouze na zvuk a neovlivňovala jen způsob vyjadřování, ale i

myšlenkové procesy. Lidé více využívali své vzpomínky, protože neměli přístup k informacím tak snadno jako dnes. Na zapamatování se používaly různé techniky memorování a až s rozvojem písma vznikaly podpůrné seznamy a rejstříky a s nimi i změna uvažování (Ong, 2006 s.36-43).

Pokud se na lidskou paměť zaměříme z obecného hlediska, lze pozorovat, že po nástupu moderních technologií začala v některých oblastech mírně ztrácet na významnosti. Důvodem se stala informační exploze přinášející ohromný objem cirkulujících dat a informací. Neexistuje lidská paměť, která by všechny informace dokázala pojmout a využít bez další informační opory. Paměť neměla jinou možnost, než se začít opět měnit. Jak je řečeno výše, určila si, která data si zapamatovat, a zároveň se naučila novou dovednost – rychlé vyhledání dat, jejich zpracování a vyhodnocení (Greenfield, 2016 s.41-51).

V odborné literatuře se lze dočíst, že psychologické a sociální aspekty má i používání mobilních telefonů a sociálních sítí. V obou případech užívání těchto technologií jde o exponenciální růst. Mobilní telefon je zrovna jedním z přístrojů, který se stal součástí lidských těl, je malou kanceláří, rádcem, komunikačním prostředkem, spojením s celým světem. Mozek dokonce změnil způsob, jakým řídí ruku lidí, kteří mobilní telefony používají – v reakci na nový způsob používání prstů se oblast mozku řídící palce významně rozšířila (Gindrat et al, 2015).

Kolem sociálních sítí existuje stále řada otazníků. To, jak lidé komunikují a jsou navzájem v sociální interakci, se spontánně mění. Způsobů, jakým sociální sítě ovlivňují myšlení a chování lidí, může být několik. Určitá anonymita v kybersvětě odbourává zábrany, strach, nejistotu a plachost a lidské myšlení se mění v přímém přenosu. Lidé jsou schopni o sobě prozradit velké množství osobních informací a vůbec nepřemýšlí o možném nebezpečí. Mění se způsob chování vůči ostatním, většinou spíše v negativní. Navíc při nepřímé osobní interakci běžně nedochází k základní neverbální komunikaci – k očnímu kontaktu, modulaci hlasu a nemůže být dostatečně vnímána řeč těla. Každodenní užívání internetu, čtení a psaní krátkých zpráv způsobilo, že je zvláště pro digitální domorodce obtížnější se soustředit na čtení delších textů, porozumět jim a absorbovat je. Všechny tyto případy vyžadují modifikaci některých funkcí mozku (Greenfield, 2016 s.52-62). K tomu více ve druhé části článku.

Neurovědecké výzkumy ukazují, že rozsáhlé používání internetu a časté vstupy do kyberprostoru mohou lidské mozky změnit i fyzicky. Lidská mysl je každý den konfrontována s novými myšlenkami a plány. Mozek se mění a s každým novým úkolem se otevřou „*nové nervové dráhy, které dávají pokyn lidským tělům*“. Schopnost mozku měnit se učením se objevuje v jakémkoli věku. Nervové dráhy se vytvářejí v případě, že se člověk naučil něco nového. Stejná spojení ale mohou být i zničena – selhání paměti člověka se může projevit například zapomenutím jména jiné osoby. Studie ukazují, že čím více času lidé tráví na internetu, tím více si zvykají na rychlé zpracování zjednodušených úryvků informací a mají problém vrátit se k delším tištěným textům (Michelon, 2008). Jak se krok za krokem vrátit k hluboké a soustředěné četbě tištěných knih, řeší například americká neuroložka Maryanne Wolfová ve své knize Čtenáři, vrať se, v níž „*shrnuje dosavadní vědecké poznání o vlivu digitálních médií na pro-*

ces čtení a lidský mozek“ (Wolf, 2020).

6.3 „Používej to, nebo o to přijdeš“

(Wolf, 2020 s.72)

Pro pochopení toho, jak mohou digitální technologie zanechat fyzické stopy na lidském mozku a posunout jeho myšlení, je potřeba pochopit, jak mozek funguje. Zjednodušenou definici tohoto procesu lze převzít od Greenfieldové, která popisuje mozek jako komplexní organizaci, „*kde vznikající hierarchii stále složitějších vrstev sítí neuronů nakonec tvoří zvláštní makrostrukturu mozku. Všechny oblasti mozku se nakonec vzájemně propojí, a to i na velké vzdálenosti, prostřednictvím nervových drah, které fungují podobně jako telefonní linky a umožňují nepřetržitý dialog po celém mozku*“ (Greenfield, 2016 s.67). Žádná oblast mozku nemá samostatnou úlohu, ale funguje na principu „*společné práce*“, která vede k celkové finální funkci všech částí. Tyto procesy v mozku nesou informaci o lidském vnímání světa. Bryan Kolb, odborník na problematiku vývoje mozku, téma shrnul takto: „*Cokoliv, co mění náš mozek, mění i to, kým budeme. Náš mozek neformují pouze naše geny; je utvářen celoživotními zkušenostmi. Zkušenosti mění mozkovou činnost, což zapříčiní změnu exprese genu. Jakékoliv změny v chování, které vidíme, odrážejí změny v mozku*“ (Kolb & Gibb, 2011).

Jaká jsou pozitiva a jaký negativní dopad má používání digitálních technologií na funkci mozku a lidské myšlení, není příliš zřejmé, jelikož mezi oběma póly je velmi tenká hranice. Navíc jinak je situace vnímána u digitálních domorodců a jinak u digitálních přistěhovalců. Greenfieldová ve své práci zmiňuje výsledky průzkumu Ofcomu (pozn. britskou vládou schválený regulační a soutěžní úřad pro vysílání, telekomunikaci a poštu (Ofcom, 2021)), který se zabýval vztahy a sociální interakcí mezi přáteli a rodinou. Výzkum, který Ofcom provedl a publikoval v červenci 2012, zmiňuje úpadek verbální komunikace po telefonu nebo při osobnímu setkání, kdy jen 63 % lidí je denně v osobní interakci se svými přáteli nebo rodinou. Digitální domorodci preferují komunikaci pomocí rychlých zpráv (v roce 2012 bylo uváděno, že takto komunikuje 96 % mladých lidí) (Greenfield, 2016 s.138). Bylo zjištěno, že prostřednictvím této komunikace nedochází k dostatečné emocionální podpoře – namísto řeči těla, modality hlasu a fyzického kontaktu jsou prostředkem vyjádření slova bez emocí. Vyvstává tak otázka, zda paralelní kyberprostor může být schopný zničit skutečnou neverbální komunikaci, v níž pak lidé nebudou mít dostatečně osvojeny dovednosti lidské interakce. Digitální domorodci, kteří v tomto světě uvíznou, mohou mít problém komunikovat tváří v tvář a nepřekonatelnou překážkou se pro ně může stát i pohled do očí druhé osoby. Realita se postupně mění ve svět, kde již dnes někteří vnímají propojení s vnějším světem jako nepříjemný pocit z přímého osobního střetnutí a kde je osobní identita stále více definována uznáním ze strany virtuálního publika sociálních sítí (Greenfield, 2016 s.139,256).

Na druhou stranu kyberprostor nabízí i místo pro rozvoj kognitivních funkcí mozku – moderní

technologie lze použít ke vzdělávacím účelům a zvyšování lidské gramotnosti. Kromě obecnějších aktivit pro efektivní získávání, třídění a zpracovávání informací dochází pomocí různých technik v souvislosti s digitálními technologiemi k možnému využívání různých produktů a médií pro trénink mozku. Lze jejich pomocí „*zlepšit uvažování, paměť, plánování, vizuálně-prostorové dovednosti a pozornost*“ (Greenfield, 2016 s.225). K těmto procvičováním mohou sloužit např. videohry, které vedle procvičování mozku poskytují i zážitek, ale i osvojení si schopnosti digitálního čtení, které formováním dvojjazyčného mozku (digitální média a tištěný text) dokáže přepínat mezi různými kódy. Zejména digitální domorodci, u nichž je dvojjazyčný mozek dostatečně podporován, v tomto směru dokáží pro konkrétní příležitost ke čtení a myšlení aplikovat patřičný režim (např. rychlý a lehký režim pro čtení e-mailu a hluboké čtení pro tištěný text) (Wolf, 2020 s.192).

6.4 Závěr

Moderní technologie nabízejí neuvěřitelné možnosti pro práci, zábavu i sociální interakci. Známe ale dobře jejich cenu? Stojíme za hranicí nové éry s kořeny pevně zahloubenými do virtuálního prostoru, který přináší neustálé změny do našeho světa. Automatizace, umělá inteligence a robotika – to vše mění naše životy. Digitální narušení však může jít mnohem dále, než si dokážeme uvědomit. Technologie umožňují lidem z celého světa být virtuálně na jakémkoliv místě a v podstatě ihned se spojit s osobou, na niž pomyslíme. A přesto zůstáváme nohama na zemi a v prázdných místnostech. Změna, kterou sami na sobě příliš nevnímáme a jíž povětšinou nevěnujeme pozornost, probíhá v našem mozku, ovlivňuje naše myšlení a kreativitu.

Jako krajní příklad bych na závěr ráda citovala pasáž z knihy Susan Greenfieldové (Greenfield, 2016 s. 257-258):

> *„Tak to jsme my, protloukáme se davy, ale ty nás vůbec nevnímají. Alespoň v jedné ruce držíme něco k snědku a do ucha se nám line neutuchající proud nejspíše hudby, případně nahraných verbálních textových zpráv či možná informací o tom, kde si můžeme koupit nejnovější zboží, které, jak ukázala naše dosavadní historie brouzdání, je pro nás přesně to pravé. Kyberprostor se již neomezuje na dvojrozměrnou obrazovku, ale roztahuje se do třech dimenzí, čímž transformuje realitu. Náš svět připomíná spíše bublinu. Venku kolem nás chodí jiní lidé, ale chrání nás před nimi průhledný štít zahrnující náš virtuální prostor, naši novou dimenzi. Můžeme se dotýkat různých věcí a přivonět k nim, můžeme je slyšet i vidět je, ale nikdy nejsme sami, nikdy nejsme nezávislí. Vždy máme onen hlas v uchu, našeho nejlepšího přítele, který působí jako prostředník, a proto nás paradoxně zároveň ode všech a všeho ostatního vzdaluje v momentě, kdy nás spojí. Nebudeme příliš tušit, kdo jsme, nebudeme mít představu o minulosti ani budoucnosti, jen o jednolitých atomizovaných okamžicích. […] Jakomalé děti budeme ochotni poslouchat na slovo a přizpůsobovat se,*

> *neboť se adaptujeme na svět, kde očekáváme neustálé uznání od ostatních. […] K tomuto stírání hranice mezi vlastním já a vnějším světem přibude ještě stírání mezi skutečností a fantazií. Protože již nebudeme používat své smysly, ale ve všem nám bude pomáhat a asistovat náš nejlepší kyberpřítel, bude hranice reality díky pokroku v biotechnologii čím dál rozmazanější, stejně jako náš ambivalentní generační status.“*

Samozřejmě jde o poněkud extrémní scénář a „*za vlasy přitažené*“ vyjádření vidiny budoucnosti lidstva. Zamysleme se ovšem nad tím, jak je právě dnes hranice mezi lidskou bytostí a „*kyberorganismem*“ tenká a jakou cestu dokáže ujít do zítřka.

6.5 Zdroje

Gindrat, A. -D., Chytiris, M., Balerna, M., Rouiller, E. M., & Ghosh, A. (2015). Use-Dependent Cortical Processing from Fingertips in Touchscreen Phone Users [Online]. Current Biology, 25(1), 109-116. https://doi.org/10.1016/j.cub.2014.11.026

Greenfield, S. (2016). Změna myšlení: jak se mění naše mozky pod vlivem digitálních technologií. V Brně: BizBooks.

JIROVSKÝ, V. (2021, March 9). Kybernetická společnost (8. 3. 2021) [Online]. Retrieved July 28, 2021, from https://www.youtube.com/watch?v=3kkLYmIV3sg&list=PLdzensQPEAPOkMAVMoJuhbV43UNizW7G2&index=2

KOLB, B., & GIBB, R. (2011). Brain plasticity and behaviour in the developing brain [Online]. Journal Of The Canadian Academy Of Child And Adolescent Psychiatry, 20(4), 256-267. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222570/

MICHELON, P. (2008). Brain plasticity: how learning changes your brain [Online]. Retrieved from https://sharpbrains.com/blog/2008/02/26/brain-plasticity-how-learning-changes-your-brain/

Mitchell, W. J. (c2004). E-topia: život ve městě trochu jinak. Praha: Zlatý řez.

Ong, W. J. (2006). Technologizace slova: mluvená a psaná řeč. Praha: Karolinum.

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1 [Online]. On The Horizon, 9(5), 1-6. https://doi.org/10.1108/10748120110424816

Wolf, M. (2020). Čtenáři, vrať se: mozek a čtení v digitálním světě. Brno: Host.

Ofcom [Online]. (2001-). Retrieved from https://en.wikipedia.org/wiki/Ofcom

7 Podmořské optické sítě: kritická infrastruktura

Autor: Lukáš Kudláček

7.1 Úvod

Práce se věnuje, vzhledem k omezenému prostoru při tak komplexním tématu, optickým sítěm z pohledu jejich důležitosti pro světový tok informací, a také z pohledu jejich bezpečnosti, neboť jakýkoliv útok na tuto kritickou infrastrukturu, přes kterou probíhá jak celosvětová komunikace, tak i mezinárodní obchod, burzy, činnost států, činnost armád, a podobně, by znamenal buď biliónové škody, či potenciál k rozpadu společnosti tak jak ji známe dnes. A tato důležitost dnes výrazně vzrostla, kdy většina věcí z důvodu pandemie probíhá on-line, a do budoucna se bude tento způsob komunikace rozvíjet stále víc. I takto specifikované téma by bylo příliš objemné na tak krátkou práci, tak se specificky zaměřím pouze na část podmořských kabelů optické sítě, které tvoří většinovou část datového propojení.

7.2 Obecná historie optických sítí

Dějiny optických sítí, které jsou v současnosti strategickou a kritickou infrastrukturou lidstva, se začali psát ve 20. letech minulého století, kdy skotský vynálezce televize John Logie Bard (Calder&Ovassapian, 2000), zkoušel přenášet obraz po kabelu, který byl spleten z několika stovek skleněných vláken. To se mu však nezdařilo. Další vývoj začal až po druhé světové válce, kde ovšem také nebyl zaznamenám výrazný pokrok. Až roku 1960, kdy americký vynálezce laseru Theodore Maiman (Benson, 2010) zkusil pustit do skleněných vláken paprsky laseru a navýšil tak kapacitu přenosu desetitisíci násobně. Nicméně i tak měl signál ztrátu přes 90 % na dvaceti metrech (Webster, 2021).

Teprve v roce 1966 odhalili George Hockham (In Memoriam, 2013) a Charles Kao (Chan, 2018) v přelomové studii, že samotná technologie je v pořádku, ovšem problém je ve znečištění skla tzv. ionty přechodových kovů, které rozptylují signál (Hockham&Kao, 1966). Také zjistili, že nejlepším materiálem pro optická vlákna bude křemík. Charles Kao na základě tohoto objevu získal v roce 2009 Nobelovu

cenu za fyziku. Zde se tedy začíná psát moderní historie optických vysokorychlostních sítí na kterých je postavena dnešní internetová síť. Tento objev vedl k vývoji nových typů skleněných vláken, již bez nečistot, které snížily útlum z 1000 dB na 5 dB na kilometru kabelu. Útlum optického kabelu je změna síly signálu na obou koncích optického kabelu (Crisp, 2005). Vyšší útlum znamená pomalejší přenos a horší kvalitu přenosu. Ta je, zejména u přenosu živé hudby, naprosto zásadní, aby jednotlivý účastníci hráli v souladu a každý umělec nebyl slyšet jinak.

Poprvé byl přes optická vlákna přenášen obraz ze zimních olympijských her v Lake Placid v USA, které se odehrávali v roce 1980. Typ vlákna byl tzv. vicevidový (Crisp, 2005) s velikostí mezi 10 až 100µm, a útlum se začal pohybovat okolo 0,5 dB na kilometru vlákna. Další zásadní vývoj probíhal až na přelomu tisíciletí, kdy došlo k zavedení tzv. vlnového multiplexu (Kavický, 2008), který umožnil na jednom optickém vláknu pouštět více optických signálů, což vede k mnohonásobnému navýšení kapacity optických kabelů. Tato technologie se používá dodnes. Také se zvýšila výrazně rychlost přenosu ke 100 Gb/s, což je již standardní rozsah v domácích ethernetových sítích. Od té doby rychlost neustále roste, ne již v Gb, ale Tb za sekundu.

7.3 Vývoj podmořských kabelů optických sítí

Podmořské kabely optických sítí hrají zásadní roli při přenosu informací na internetu napříč světem, obsluhují více jak 98 % datového toku (Newsweek, 2015). Jedná se jen o jednu z částí celého procesu, jsou zde pozemní optické kabely, směrovače, opakovače, přepínače a pochopitelně samotná koncová zařízení. Podmořské kabely jsou ale nejdelší částí tohoto řetězce. První podmořský kabel byl položen mezi Velkou Británií a Evropou v roce 1850, jednalo se o telegrafní kabel. První podmořský oceánský kabel byl položen roku 1858 mezi Irskem a Kanadou, také ve formě telegrafního spojení. Rychlost byla 25 slov za minutu.

Skutečný datový optický podmořský kabel byl položen až roku 1984 mezi Velkou Británií a Belgií. První transatlantický optický podmořský kabel s názvem TAT-8 byl položen roku 1988 a měl kapacitu 280 Mb/s, což byl ekvivalent 40tis telefonních kanálů najednou. Spojoval Spojené státy, Velkou Británii a Francii (Abbott, 2008). Jednalo se o zásadní milník v datovém spojení mezi kontinenty, které umožnilo globální rozvoj internetu. Pokládání podmořských optických datových kabelů je velmi nákladné, nejen finančně, ale i časově. Vzhledem k velkým vzdálenostem v řádu tisíců až desetitisíců kilometrů trvá položení takového kabelu klidně i měsíce až roky. Aby se snížil útlum signálu je každých 50-100 km integrován tzv. opakovač signálu, který známe i ze satelitní, mobilní či bezdrátové komunikace.

Poslední atlantický kabel s označením TAT, TAT-14 byl položen v roce 2001 s kapacitou 640 Gb/s, což je ekvivalent 9,7 miliónu telefonních kanálů najednou. Byl složen ze čtyř optických vláken, z nichž měl každý 16 vlnových délek, každá o 10 G signálu. Posledním položeným atlantickým kabelem byl v roce 2015 tzv. GTT Express, který má kapacitu 100 vlnových délek o kapacitě 100 Gb/s, celkem tedy

53 Tb/S (Burns, 2020). Kapacita výrazně vzrostla, nicméně ani to dnešnímu světu nestačí, a proto je mnoho společností, zejména velkých světových mobilních operátorů, kteří pokládají další a další kabely. Zároveň se přidaly velké technologické společnosti, které pokládají vlastní kabely na zajištění propojení serverů po světě, aby byly schopné uspokojit enormní nárůst uživatelů

7.3.1 Současný stav

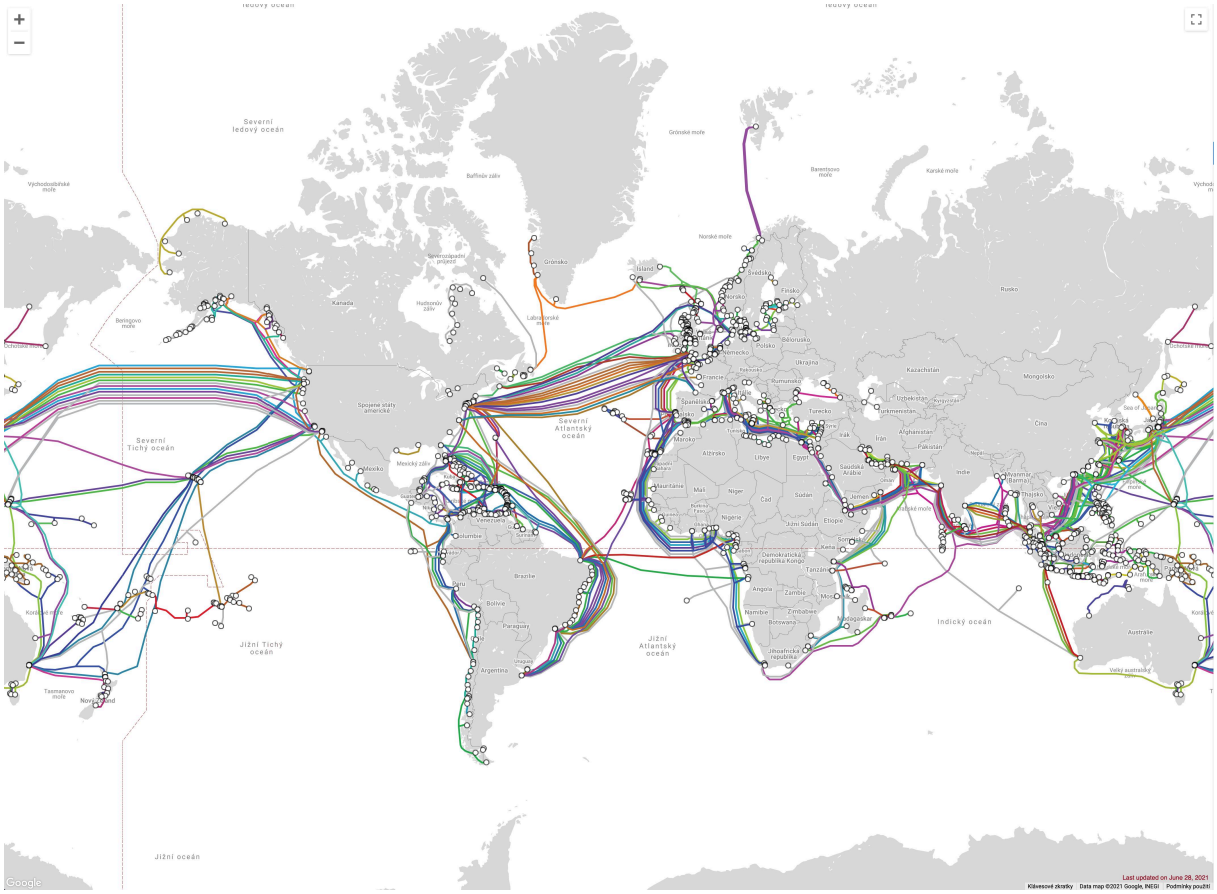
V poslední době je rychlost a objem přenosu dat novým zlatem, o to více v dnešním turbulentním epidemiologickém období, kdy je většina oborů, od školství po průmysl, odkázáno na on-line provoz, zejména pak v oblasti přenosu audio-vizuálních dat, tedy konferencí a přednášek, a to s mnoha účastníky najednou. Člověk by si řekl, že pokud se jedná například o vysokoškolskou přednášku, kde jsou připojeni uživatelé jen z jedné země, tak že data cestují pouze po lokální síti a nemají s podmořskými datovými kabely nic společného. Tak tomu ale není, neboť ve většině případů cestují data přes servery daných služeb. Tyto servery se mohou nacházet v odlišných zemích, než kde komunikace probíhá. Například aplikace Zoom, kde probíhá většina distanční výuky, by měla data přenosu posílat mezi účastníky přes servery společnosti Zoom, které má pro střední a východní Evropu v Německu, přesto ale proudily a proudí přes servery v Číně, za což si zasloužily velkou kritiku, neboť je zde oprávněné podezření z monitorování obsahu (Business Insider, 2020). V takovém případě se bavíme o desítkách tisíc kilometrů optických kabelů, přes které taková přednáška proudí, z nichž i v tomto případě hrají největší podíl pomořské kabely. Dokážeme si tak představit jejich vytíženost.

Samotná distanční výuka je ovšem jen jednou ze služeb, které byly donuceny se přestěhovat do virtuálního prostoru. Rychle se rozvíjí sektor telemedicíny, kdy pacient komunikuje se svým lékařem online o svém zdravotním stavu, který je jedním z nejdůležitějších osobních údajů člověka. Dále se rozvíjí poradenství a právnické služby, kdy společnosti mají miliony klientů, kteří za pomocí vzdáleného přístupu řeší zakládání společností a soudní spory. Nakonec tu máme velké množství obchodů, které byly donuceny nabídnout své zboží ve virtuálním prostoru. Jen v těchto případech hovoříme o obrovském zatížení internetové komunikace.

Dalším a jedním z největších nárůstů objemů dat v podmořských kabelech optických sítí je rozvoj cloudového ukládání dat. Zde nehovoříme o konkrétním uživateli, který si zálohuje osobní data na cloudovém úložišti, hovoříme o velkých korporacích, které přechází na cloudové řešení, aby jejich zaměstnanci mohli pracovat kdekoli a mít přístup k datům společnosti. Kapacita těchto dat astronomicky roste. Vzhledem k rozsáhlým internetovým útokům na velké korporace, které mají přesah do fyzického světa, například v dodávkách paliva či potravin, se i tyto korporace přesouvají do cloudového prostoru. V něm nemůže útočník blokovat data a žádat výkupné, neboť tyto úložiště, od společností jako Amazon či Microsoft mají velmi dobrou ochranu. Na základě nedávných útoků vydal dokonce americký prezident Biden příkaz, ve které vybízí společnosti ke přesunu do cloudového řešení, a vládním to určuje (The White House, 2021). Podle odhadů pracuje z cloudového prostředí

cca 40% společností a do roku 2025 se očekává růst na 70% (Aycock, 2021). A to v USA, kde je technologie velmi rozvinutá. Jak se více a více společností bude kompletně přesouvat na cloud, exponenciálně poroste potřeba datové kapacity, jejíž základní součástí jsou podmořské optické kabely. Jak je patrné, již dnes jsme na hraně kapacity a proces výstavby optických sítí je velmi pomalý.

V současné době je síť optických kabelů sice velmi široká, jak je znázorněno na mapě níže, a stále přibývají nové kabely, které pokládají soukromé společnosti, zejména technologické jako Google, Facebook, či Amazon, které mají samy o sobě enormní datovou zátěž mezi svými uživateli, ale ani tak to nestačí. Celkově je dnes položených 420 optických podmořských kabelů s celkovou délkou 1,1 milionů kilometrů a stále se pokládají nové s lepší technologií a větší propustností dat (Routley, 2017).



PriMetrica. Submarine Cable Map [online]. Carlsbad, USA: PriMetrica, 2021. Dostupné z: https://www.submarinecablemap.com

Například, společnost Google oznámila v polovině roku 2020 začátek pokládání nového optického atlantického kabelu s názvem Grace Hooper (CNBC, 2020), který by měl být hotový v roce 2022, a který bude měl směřovat z New Yorku do Bude ve Velké Británii a Bilbao ve Španělsku. Tento nový optický kabel, který je 6,300 km dlouhý, citelně posílí datové spojení mezi Spojenými státy a Velkou Británií,

neboť se jedná o první kabel mezi těmito zeměmi od roku 2003. V zásadě bude poskytovat svou kapacitu celému internetu, posílí také služby společnosti Google, zejména jejich mailovou a cloudovou službu. Kapacita kabelu je 32 optických vláken, což spolu s novou architekturou směrovačů, bude dle společnosti Google výrazný krok vpřed (Google, 2020).

Samotný Google má v provozu již tři vlastní podmořské kabely, Curie ze Spojených států do Jižní Ameriky, pak Dunant od Spojených států k Francii a Equiano, který vede okolo západního pobřeží Afriky od Portugalska po Jihoafrickou republiku (E15, 2020). Spolupracoval a spolupracuje však na výstavbě dalších 15 podmořských kabelů. Jedním z nich je například kabel Firmina, který spojí východní pobřeží USA s Brazílií, Uruguay a Argentinou. Jen za období let 2016 až 2018 investovala společnost Google do této infrastruktury 47 miliard amerických dolarů (Qiu, 2019).

Dalším výrazným investorem, krom společnosti Amazon a mobilních operátorů, nemluvě o armádních projektech, je společnost Facebook, která obsluhuje více jak 2 miliardy uživatelů po celém světě a má velmi náročnou službu na přenos dat. Společnost Facebook pokládá v konsorciu dalších společností jako je China Mobile, MTM, Vodafone a Orange, více jak 37 tisíc kilometrů dlouhý podmořský kabel okolo celého afrického kontinentu. Projekt s názvem 2Africa má za cíl zlepšit dostupnost internetového připojení a tím i služeb společnosti Facebook více jak 1,3 miliardě lidí, kteří na kontinentu žijí (Fryedlewicz, 2020). Dle vyjádření společnosti Facebook, poskytne tento podmořský kabel třikrát větší síťovou kapacitu než všechny ostatní kabely připojené ke kontinentu dohromady. Společnost Facebook spoluvlastní dalších 10 podmořských datových kabelů. Sám operátor Orange staví podmořský kabel Amitié, který propojí USA a Francii. Kabel má 16 optických vláken, každé o kapacitě 23 Tbps, tedy 23tis giga za sekundu. Kapacita by měla být stejná jako většina kabelů pod Atlantikem dohromady. Dokončení se očekává v roce 2022. Společnost Orange navíc předpokládá, že se kapacita dat mezi USA a Francií každé dva roky zdvojnásobí (O'Halloran, 2021). Společnost Amazon spoluvlastní dva podmořské kabely, jinak si kapacitu kupuje, a plánuje samostatnou výstavbu také. Společnost Microsoft spoluvlastní tři podmořské kabely.

7.3.2 Budoucnost

Kromě výše uvedených služeb, jako jsou distanční výuka, telemedicína, online právní služby, cloudové řízení společností, bude datová kapacita v budoucnosti výrazně narůstat i se zavedením 5G sítí nové generace a díky tomu, masivního rozvoje tzv. internetu věcí (Al-Fuaqaha et al., 2015). Do budoucna tedy bude nutné kapacitu podmořských datových kabelů neustále rozšiřovat, a to i s ohledem na stárnutí a snižování kapacity již položených kabelů, a také jak si uvedeme v další kapitole, s vyšším rizikem útoků na tyto datové superdálnice.

Internet věcí, který zahrnuje od propojování automobilové dopravy v rámci samořiditelných vozů, přes komunikaci ledničky s oblíbeným obchodním řetězcem, po RFID čipy v knihách a správu on-line

výpůjček v knihovně, bude pracovat s extrémním datovým tokem. Tyto toky musí někudy proudit a nejrychlejší a nejefektivnějším způsobem jsou optické sítě, z nichž převážná většina jsou podmořské datové kabely. Pokud do toho zapojíme zvýšení datového toku skrze sítě páté generace, kdy se odhaduje že datová spotřeba mobilních telefonů vzroste pětinásobně a čím dále více konzumace audiovizuálního obsahu, ať již na osobních počítačích či přes streamovací služby na televizích, tak je jasné, že datový přenos může vzrůst desetinásobně i více v horizontu několika let. Například společnost Wejo, leader v oblasti shromažďování dat v automobilovém provozu, která slouží pro vývoj autonomního řízení automobilů, zaznamená z více jak 11 miliónů propojených aut téměř 15 miliard dat každý den (Wejo, 2021). Všechna tato data proudí přes optické kabely.

Vzhledem k pomalé výstavbě nových podmořských kabelů, jejich náchylnosti na poškození, jak si uvedeme dále, a opotřebení těch starých, se můžeme dostat do situace, že bude datový přenos záměrně zpomalován, či prioritizován tomu, kdo zaplatí více.

7.4 Bezpečnostní hrozby pro optické sítě

Jak jsme si uvedli výše, podmořské optické kabely obsluhují drtivou většinu datového toku na zemi. Jejich kapacita je omezená a jejich položení vyžaduje výrazné finanční a časové zdroje. Riziko jejich poškození je tedy velké a muže být eliminováno pouze většími náklady na výstavbu, kdy se vybírají bezpečnější trasy, nebo aktivní ochranou, například dronovými ponorkami.

Hrozby jsou v zásadě hlavní tři, jedny z pohledu klasického poškození, například při zemětřesení a vulkanické podmořské činnosti, druhé z pohledu záměrného poškození při teroristickém či státním útoku, a třetí bez fyzického poškození, ovšem s krádeží přenášených dat v případě špionáže. V každém případě se jedná o kritickou infrastrukturu, bez které se moderní lidstvo neobejde, která je navíc relativně volně přístupná, neboť známe body, kde kabely vystupují z moře na pevninu, a máme podrobné mapy jejich tras, a která není snadno a rychle nahraditelná. V případě poškození jednoho kabelu se datový tok automaticky přesměruje na jiný kabel, pokud by se však jednalo o koordinovaný útok na více kabelů zároveň, pak by skutečně mohl způsobit globální omezení datového toku, internetu, obchodních a burzovních dat, a mnoho dalšího.

Jako příklad můžeme uvést zemětřesení u Taiwanu, které přerušilo osm optických podmořských kabelů vedoucích do Číny, kde spadla většina provozu internetu a datových sítí obecně. Oprava trvala 49 dní a pracovalo na ní intenzivně 11 opravářských lodí (Newsweek, 2015). V roce 2008 došlo k sérii otřesů u egyptského pobřeží, které poškodily podmořské optické kabely a zasáhly 60 miliónů uživatelů v Indii, 12 miliónů v Pákistánu, 6 miliónů v Egyptě a 4,7 miliónů v Saudské Arábii. Zde se pracuje i se scénářem, že byly tyto otřesy způsobeny záměrně výbušninami, aby se přerušil datový transfer informací a zastavil se chod internetu v daných zemí. Tyto a mnoho dalších incidentů, včetně historie a důležitosti této infrastruktury, jsou popsány v knize T***he undersea network*** od Nicole Starosielski

(2015). Ta nicméně v knize upozorňuje, že útok na jeden či několik kabelů by neměl zásadní dopad. Muselo by se jednat o koordinovaný útok na několik desítek kabelů správným způsobem a musel by to být někdo kdo ví, jak tyto kabely fungují. Také ovšem v knize zmiňuje situaci, že kdyby došlo například k přerušení podmořských kabelů u Egypta, tak by mohla vypadnout až třetina světového internetu.

To, že by se mohlo jednat i o koordinovaný útok na úrovni státu, zmiňují již několik let představitelé amerického námořnictva, kteří sledují aktivitu ruských ponorek v blízkosti podmořských kabelů v Atlantiku. Takový koordinovaný útok by podle nich měl katastrofální dopady pro ekonomiku. I z tohoto důvodu obnovuje NATO velitelská stanoviště z dob studené války, aby ruské aktivity monitorovalo (Matsakis, 2018). Jak jsem již zmínil, obecná ochrana této kritické infrastruktury není nastavena, jako v případě plynovodů či ropovodů. Na druhé straně ale například Čínští představitelé považují kontrolu podmořské infrastruktury za součást širší strategické soutěže o data a oficiálně říkají, že pokládání podmořských kabelů je sice obchod, ale také bojiště, kde lze získat informace. Podmořský odposlech dat v kabelech je obtížný, ovšem při výrobě lze nainstalovat součásti, které poskytnou zadní vrátka pro sběr informací (Schadlow&Helwig, 2020). Přibližně čtvrtinu všech podmořských kabelů postavila či opravovala čínská společnost Huawei, která je napojena na ústřední komunistickou stranu Číny, a která je mnoha západními státy a jejich bezpečnostními experty považována za zásadní bezpečnostní hrozbu nejen pro krádež dat, ale i pro jejich případné vypnutí. Nakonec, vzhledem k tomu, že jsou podmořské optické kabely z větší části vedeny po mořském dně, které nepatří žádnému suverénnímu státu, je jejich právní ochrana velmi těžko vymahatelná. Již se ale začalo pracovat na nápravě tohoto stavu. Podle současné stavu tak není útok na podmořský kabel kvalifikován jako ozbrojený útok dle článku 51 Charty OSN, který umožňuje státům použití síly v případě sebeobrany.

7.5 Závěr

Dle výše uvedených informací je jasně patrné, že se jako moderní lidstvo bez podmořských optických kabelů neobejdeme, ba jsme na nich zcela závislí. Jedná se o klíčovou, strategickou a kritickou infrastrukturu, kterou je pomalé a drahé postavit, ale naopak je snadné ji narušit či zničit. O této infrastruktuře máme podrobné mapy, víme, kde jdou kabely do moře a oceánů, a jaké jsou jejich přesné trasy. Do budoucna budeme na tyto datové superdálnice spoléhat více a více a naše závislost se bude výrazně prohlubovat s tím, jak bude datový tok ovlivňovat naše životy od nákupu po řízení auta, stále více. Tyto podmořské kabely mají dlouhou historii plnou výzkumu a vynálezů, ustálený současný stav vývoje a nepříliš možné další extrémní zlepšení dané technologie, způsobuje prohlubující se ohrožení.

Přesto je tato kritická infrastruktura málo chráněná, prakticky neviděná běžným světem, který ji bere jako samozřejmost a neuvědomuje si její důležitost, a takřka bezbranná proti zásahu zvenčí. Plynovody, elektrická rozvodná síť, ropovody, jsou všechny branné jako strategické a klíčové, ovšem da-

tové infrastruktury si všímá málokdo. Předpokládám, že si to ale jednotlivé země uvědomují, neboť pokud by chtěl někdo zaútočit na celosvětový obchod, způsobit paniku na burze, přerušit tok zpravodajských informací, či prostě jen poslat na pár týdnů lidstvo do off-line režimu, pak mu stačí se zaměřit právě jen na tyto podmořské dálnice.

7.6 Zdroje

Abbott, S. (2008). Review of 20 years of undersea optical fiber transmission system development and deployment since TAT-8 [Online]. 34Th European Conference On Optical Communication, 1-4. https://doi.org/10.1109/ECOC.2008.4729162

Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., & Ayyash M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications [Online]. Ieee Communications Surveys And Tutorials, 2015(14), 2347 - 2376. https://doi.org/10.1109/COMST.2015.2444095

Aycock, J. (2021). Biden's cybersecurity order means new boon for enterprise cloud stocks - Wedbush [Online]. Retrieved July 24, 2021, from https://seekingalpha.com/news/3696415-bidens-cybersecurity-order-means-new-boon-for-enterprise-cloud-stocks-wedbush

Benson, A. K. (2010). Great Lives from History: Inventors and Inventions (Vol. 3).

History of the Atlantic Cable & Undersea Communications: from the first submarine cable of 1850 to the worldwide fiber optic network [Online]. (2021). Retrieved January 17, 2021, from https://atlantic-cable.com/Cables/speed.htm

Zoom is giving paid users more control over where their calls are routed, after it got slammed for 'mistakenly' using data centers in China [Online]. (2021). Retrieved from https://www.businessinsider.com/zoom-data-routing-control-china-servers-2020-4

I, C., A, O., & N, C. (2000). John Logie Baird-fibreoptic pioneer [Online]. Journal Of The Royal Society Of Medicine, 93(8), 438-439.

Google is building a huge undersea fiber-optic cable to connect the U.S. to Britain and Spain [Online]. (2021). Retrieved January 17, 2021, from https://www.cnbc.com/2020/07/28/google-undersea-cable-grace-hopper.html

Crisp, J. (2005). Introduction to Fiber Optics (2005 ed.). Amsterdam: Newnes.

Google rozšíří vlastní internetové kabely pod mořem. Propojí USA, Velkou Británii a Španělsko [Online]. (2021). Retrieved January 17, 2021, from https://www.e15.cz/byznys/technologie-a-media/google-rozsiri-vlastni-internetove-kabely-pod-morem-propoji-usa-velkou-britanii-a-spanelsko-1371937

Frydlewicz, J. (2021, January 20). Facebook pokládá obří podvodní kabel kolem celé Afriky, má přinést internet miliardě lidí [Online]. Retrieved January 17, 2021, from https://www.e15.cz/zahranicni/facebook-poklada-obri-podvodni-kabel-kolem-cele-afriky-ma-prinest-internet-miliarde-lidi-1369712

Announcing the Grace Hopper subsea cable, linking the U.S., U.K. and Spain [Online]. (2021). Retrieved January 17, 2021, from https://cloud.google.com/blog/products/infrastructure/announcing-googles-grace-hopper-subsea-cable-system

Hockhman, G., & Kao, C. (1966). Dielectric-fibre surface waveguides for optical frequencies. Proceedings Of The Institution Of Electrical Engineers, 1966(113), 8. Retrieved from https://digital-library.theiet.org/docserver/fulltext/piee/113/7/19660189.pdf?expires=1610838428&id=id&accname=guest&checksum=4BD04C7F9A0315FEDBCE85993E16A630D

Chan, V. W. S. (2018). In Memory of Charles Kao Kuen, the Father of Optical Fiber [Online]. Eee Communications Magazine, 56(10), 14-14. https://doi.org/10.1109/MCOM.2018.8493109

In Memoriam: George Hockham [Online]. (2013). Eee Antennas And Propagation Magazine, 55(5), 177-177. https://doi.org/10.1109/MAP.2013.6735504

Kavický, M. (2008). Optický vlnový multiplex (Bakalářská práce) [Online]. Brno. Retrieved from http://hdl.handle.net/11012/17680

Matsakis, L. (2018). What Would Really Happen If Russia Attacked Undersea Internet Cables [Online]. Retrieved July 24, 2021, from https://www.wired.com/story/russia-undersea-internet-cables/

Undersea Cables Transport 99 Percent of International Data [Online]. (2021). Retrieved January 17, 2021, from https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072

O'Halloran, J. Orange announces submarine cable linking US East Coast to France [Online]. Retrieved from https://www.computerweekly.com/news/252495050/Orange-announces-submarine-cable-linking-US-East-Coast-to-France

Complete List of Google's Subsea Cable Investments [Online]. (2021). Retrieved January 17, 2021, from https://www.submarinenetworks.com/en/insights/complete-list-of-google-s-subsea-cable-investments

Routley, N. (2021). Map: The World's Network of Submarine Cables [Online]. Retrieved January 17, 2021, from https://www.visualcapitalist.com/submarine-cables/

Schadlow, N., & Helwig, B. (2020). Protecting undersea cables must be made a national security priority [Online]. Retrieved July 24, 2021, from https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/

Starosielski, N. (2015). The Undersea Network. Durham, USA: Duke University.

Executive Order on Improving the Nation's Cybersecurity [Online]. (2021). Retrieved July 24, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Ubik, S. (2020). Distanční spolupráce v živé kultuře [Online prezentace]. Retrieved January 17, 2021, from https://www.slideshare.net/UISKFFUK

Webster. (2021). Historie optických sítí [Online]. Retrieved January 16, 2021, from https://phgame.cz/PHGame_serialy/serialy/opticka-vlakna-technologie-prenosu-dat-a-vyhody-optiky/historie-optickych-siti/

Project Yellowstone - Investor Presentation [Online]. (2021). Retrieved July 24, 2021, from https://assets.website-files.com/5911c9453963fd7f6719341a/60b63e1ace5b9d8734b9cb1f_Wejo%20PIPE%20Presentation%20FINAL%20May%202021.pdf

8 Open Science a její implementace v knihovnách

Autorka: Denisa Šourková

8.1 Úvod

Seminární práce Open Science (OS) a její implementace v knihovnách se zaměřuje na **otevřený přístup k vědeckým informacím**. Konkrétně se zabývá hnutím **Open science** *(otevřená věda)*, které dostupnost aktuálního výzkumu umožňuje a usnadňuje.

V současné době se objevují různé pokusy o podporu a propagaci otevřené vědy, a to prostřednictvím šíření povědomí a jejím zaváděním do praxe. Z toho důvodu dochází často k implementaci otevřené vědy v organizacích, jež se zabývají výzkumem.

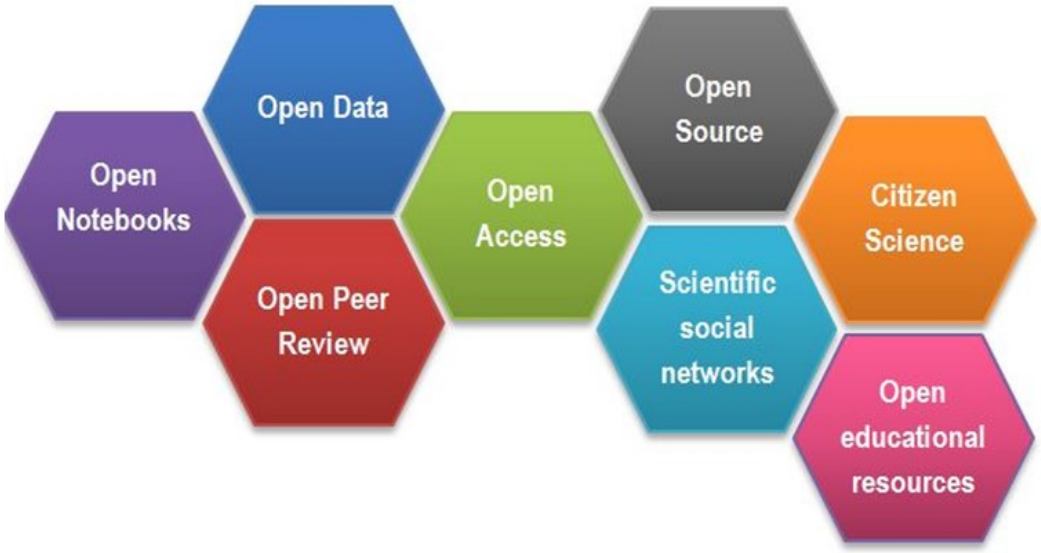
Mezi tyto instituce jsou řazeny mimo jiné i knihovny, které se obvykle snaží o rozvoj a zvyšování povědomí o Open Science. Aby však mohly poskytovat otevřený přístup k vědeckým informacím široké veřejnosti, musí splňovat některé podmínky.

Cílem je zejména představit hnutí Open Science a zaměřit se na současné zavádění otevřeného přístupu k vědeckým informacím v českých knihovnách. Vše je nakonec uvedeno na příkladu Univerzity Karlovy, která zřizuje *Centrum pro podporu Open Science ve spolupráci s Ústřední knihovnou UK*.

Práce volně navazuje na přednášku Terezy Simandlové o Open Science v prostředí akademických knihoven, nová výzva a také příležitosti, která se konala v předmětu Informační pondělky na FF UK 7.12. 2020. ## Specifikace Open Science

Open science v českém jazyce znamená otevřená věda nebo přístup k vědeckým informacím. Někdy se však mohou objevit i jiné názvy jako **Open Scholarship** nebo **Open Research**, ale jejich význam zůstává stejný. V této práci bude především využíván termín Open Science, popřípadě jeho zkratka *OS*. Pojem se dá vyjádřit mnoha různými definicemi, ale zjednodušeně ho lze vysvětlit například jako proces umožňující široké veřejnosti snadnější dostupnost k odborným poznatkům. Mezi uživatele může patřit kdokoli, ať jsou to neprofesionálové nebo odborníci, kterým sdílení výsledků napomáhá především k lepší komunikaci, výzkumu a hodnocení. Tento moderní postup získávání znalostí je zajištěn prostřednictvím online nástrojů, popřípadě digitálních technologií. Uživatel se pak může dostat zejména k *publikacím (Open Access), datům (Open Data), metodikám (Open Methods), zdrojovým kódům*

(Open Source), recenzním řízením (Open Peer Review), vzdělávacím materiálům (Open Education), alternativním metrikám hodnocení (Alternative Metrics) a jiným primárním nebo sekundárním zdrojům. Největším přínosem OS je **dostupnost** vědeckých informací, jejich **udržitelnost**, **transparentnost**, **reprodukovatelnost**, jež zajišťuje více odborných výsledků, rozvíjející se spolupráce a efektivnější šíření vědeckých výstupů. Otevřený přístup se v nedávné době také urychlil i posunul zejména v důsledku coronavirové pandemie, kdy mnoho dokumentů bylo alespoň na chvíli zveřejněno pro studijní a jiné účely (Hnátková, 2020).



Open Science fasety, zdroj: https://www.fosteropenscience.eu/content/what-open-science-introduction

Obecně platí, že výzkumná data a další výzkumné procesy by měly být volně dostupné. Zároveň je důležité, aby splňovaly podmínky jako opětovné využití, reprodukci, redistribuci nebo *fair-use*. Důraz se klade i na neustálé vylepšování jejich úrovně. (Open Science Training Handbook, 2018).

OS je založena na množství zásad, některé z nich byly definovány v různých koncepcích, jako například v *Berlínské deklaraci, Budapešťské iniciativě nebo prohlášení z Bethesdy*. Zmínka o **Budapešťské iniciativě otevřeného přístupu** poprvé zazněla v roce 2002 na budapešťském setkání. Jejím hlavním cílem zejména bylo zajištění finančních prostředků na přeměnu ekonomického modelu již stávajících, ale také i zcela nových časopisů.

Další a zároveň jednou z prvních iniciativ vztahující se k otevřenému přístupu v USA bylo **Prohlášení o otevřeném přístupu k publikování z Bethesedy**. Vzniklo v roce 2003 při setkání odborníků na zveřejňování vědeckých i odborných informací. Prohlášení se zabývalo vytvořením nejefektivnějšího

možného postupu pro šíření zásad o rychlém a otevřeném přístupu k primární vědecké literatuře.

V evropském kontextu je důležitá především **Berlínská deklarace o otevřeném přístupu ke znalostem v přírodních a humanitních vědách**, která byla představena v roce 2003 na vědecké konferenci. Hlavním bodem se zde stal internet, označený v podstatě jako přelomový nástroj pro šíření výzkumných poznatků (Planková, 2007). Jedním z příkladů, jak Open Science podrobněji konkretizovat a lépe jí porozumět shrnuje tzv. **5 myšlenkových škol**.

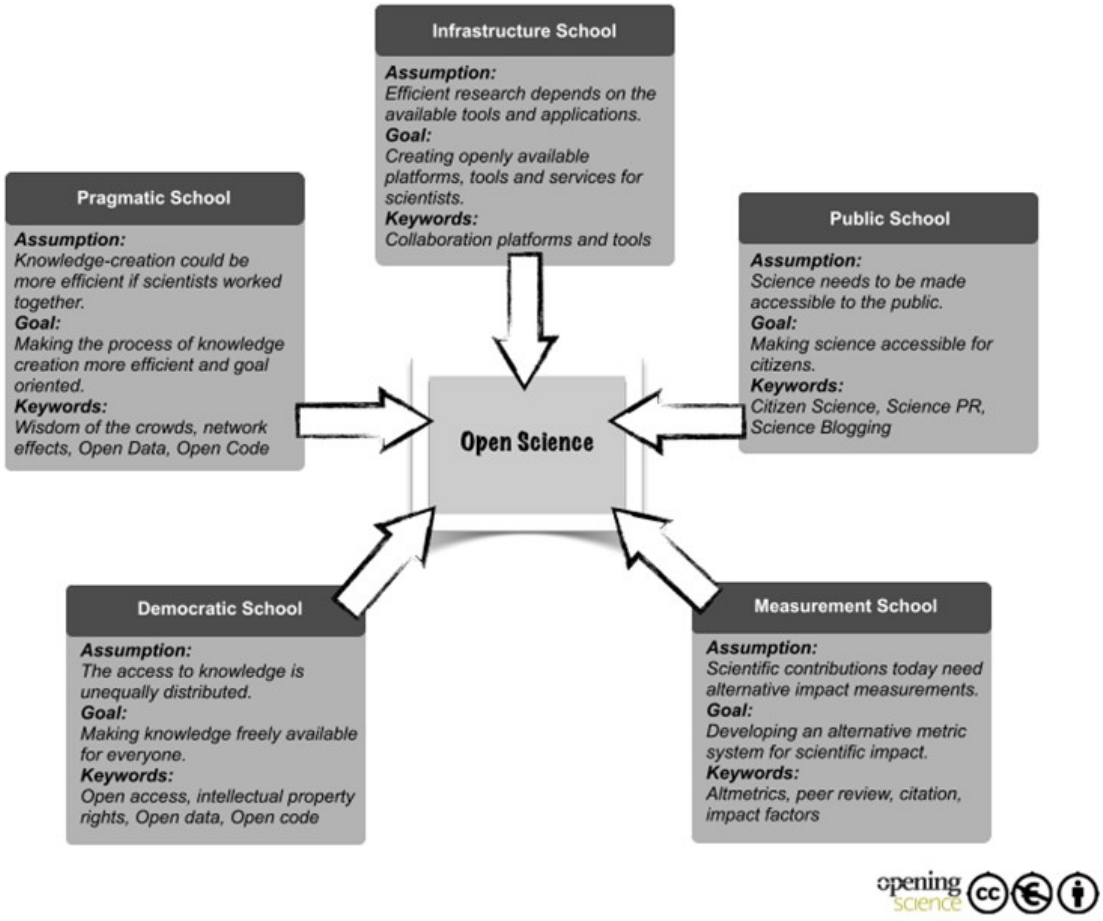
8.1.1 Rozdělení Open Science do „myšlenkových škol“

Bartling a Friesike se domnívají, že OS je definována příliš jednoduše, a tak rozlišili 5 myšlenkových škol, aby lépe vysvětlili a pokryli význam otevřené vědy. Jednotlivé školy jsou tvořeny z (Simandlová, 2014):

- **Demokratická škola:** hlavním cílem této školy je zpřístupnit vzdělání bez bariér pro každého (Bartling, Frienske, 2014). Ke znalostem se stále nedostanou úplně všichni, a proto se tato škola snaží zajistit dostupnost vědeckých výsledků pro většinu lidí bez větších rozdílů. (Open Science Training Handbook, 2018).
- **Pragmatická škola:** vytváření znalostí by mohlo být více efektivní, kdyby vědci pracovali spolu (Bartling, Frienske, 2014). Tato škola navazuje na zásadu, že při tvorbě vědeckých znalostí dochází k zefektivnění, pokud vědci navazují spolupráci a vzájemně dokážou hodnotit a vznést určitou kritiku ke své práci. Škola se také snaží o to, aby různé vědecké metody byly více transparentní a o vybudování tzv. sítě, která by vědce mohla více spojit (Open Science Training Handbook, 2018).
- **Škola infrastruktury:** efektivnost výzkumu záleží na dostupných nástrojích a aplikacích. Cílem této školy je vytvořit snadno dostupné platformy, nástroje i služby pro vědce a ostatní uživatele Open Science (Bartling, Frienske, 2014).
- **Veřejná škola:** věda se musí stát přístupnější pro veřejnost (Bartling, Frienske, 2014). Obecně by měla mít na společnost nějaký dopad. Je zapotřebí zapojovat veřejnost do výzkumu a vytvářet srozumitelné vědecké výsledky i pro *„laiky“*. Tímto způsobem se věda snaží přimět veřejnost ke spolupráci (Open Science Training Handbook, 2018).
- **Škola měření:** zkoumá, jaké mají vědecké výsledky dopad (Bartling, Frienske, 2014). Tradiční měření se ukázalo jako problematické, a to z toho důvodu, že zahrnovalo například pouze časopisy. Začaly se tedy hledat další alternativní metody, které mohou využívat možnosti digitálních nástrojů a měřit tak dopad vědeckých informací podrobněji (Open Science Training Handbook, 2018).

Myšlenkové školy jsou jedny z možných aspektů popisující OS a vystihující detailněji její význam. O Obecné politice otevřené vědy pak dále pojednává také tzv. ***Evropská komise***, která mimo jiné do-

poručuje ve svých cílech propagaci a podporu otevřené vědy.



Pět Open Science myšlenkových škol, zdroj: https://www.fosteropenscience.eu/content/what-open-science-introduction

8.1.2 Zavádění Open Science

Politiku Open Science upravuje Evropská komise v rámci programu, který zahrnuje financování výzkumu a inovací. Pokud vědci co nejdříve zveřejní své znalosti a data, dochází k rychlému šíření nejnovějších poznatků. Zároveň, když tento proces podpoří akademické obce, průmysl, veřejné orgány či občanské skupiny, zvyšuje se kreativita a důvěra ve vědu. Šířit vědecké výsledky umožňuje odborníkům napříč zeměmi tzv. platforma **European Open Science Cloud**, která měla vstoupit do fáze vývoje v roce 2021. Jedním z cílů Evropské komise je prosazovat přijetí OS a zapojovat občany, organizace občanské společnosti i koncové uživatele do jejího procesu (European Commission, 2021).

Nově se na rok 2021-2027 připravuje rámcový program **Horizon Europe pro podporu Open Science**. Další evropskou iniciativou je tzv. *Plán S*, která se opět zaměřuje na Open Science zejména na Open Access (Hnátková, 2020).

Obecně stále dochází k velkým rozdílům mezi jednotlivými zeměmi v oblasti zavádění otevřené vědy do praxe. V některých oblastech je povědomí o OS poměrně vysoké, přičemž stále jsou tu místa, kde se vývoj nachází stále v přípravné fázi. Iniciativy v západní a severní Evropě jsou pokročilejší než v jižní a východní Evropě (Grant, 2018).

Open science je založena na spolupráci, udržitelnosti i jistém vlivu. V podstatě by měla pozitivně působit na společnost, a to s cílem rozšiřování a sdílení vzdělanosti. To může vést k inovacím a řešením globálních problémů jako jsou klimatické změny nebo nemoci. Z toho důvodu je důležité stále podporovat navyšování implementace open science v různých organizacích, které se zabývají výzkumem (Grant, 2018).

8.2 Implementace Open Science v knihovnách

K rozvoji Open science je potřeba sdílet směrnice, zvyšovat o ní povědomí, a zavádět jí do praxe. Aby tyto všechny aspekty mohly být realizovány, musí se vyhledat vhodní kandidáti. Aktivními přispěvateli pro tento proces se staly právě knihovny. Mají spoustu možností, jak podporovat OS, ale jedna z hlavních činností je spolupráce. Tu mohou uskutečnit v rámci vlastní instituce nebo na regionální úrovni, a to vytvořením programů napomáhajících šíření osvědčených postupů a zdrojů, popřípadě se zapojit do mezinárodních projektů či rozvoje politiky. Bohužel ne každá knihovna má vysoký finanční rozpočet na to, aby mohla rozvíjet OS, tak jak by chtěla. Nicméně podstatné je, aby se knihovna alespoň nějak podílela na propagaci otevřené vědy bez ohledu na to, jestli se jedná o větší či menší instituci. Zároveň je to důležité jak pro knihovnu samotnou, tak pro její uživatele i celkovou společnost, aby stále mohlo docházet k novým objevům a inovacím. V **LIBER Open Science Roadmap** jsou definovány **tři základní klíčové principy OS v knihovnách** (Grant, 2018):

- **Transparentnost:** pro Open Science je transparentnost velmi důležitá, proto i knihovny by ji měly podporovat, a to například sdílením informací, které jsou dostupné na základě licencí, udržet povědomí o OS pro příští generace, seznámit s Open Access (OA), poradit výzkumným pracovníkům, jak publikovat přes OA (Grant, 2018).
- **Udržitelnost:** Jak již bylo napsáno v kapitole Specifikace Open Science, odborné výsledky by měly být opětovně využitelné. Knihovny se mohou starat o to, aby poskytovaly udržitelné metadatové služby a dlouhodobě je chránily (Grant, 2018).
- **Spolupráce:** Knihovny mohou v rámci spolupráce sdílet své osvědčené postupy, studie a zároveň se podílet na vývoji společných standardů a služeb (Grant, 2018).

8.2.1 Open Access v českých knihovnách

V České republice se mohou knihovny také zapojit do projektu Open Access. Musí však zajistit informační podporu pro své uživatele, což jsou akademičtí pracovníci, studenti nebo veřejnost. Informační podpora zahrnuje vytvoření webových stránek, které budou návštěvníky informovat o otevřeném přístupu a odkazovat na prameny, jež definují základní principy OA. Příkladem vhodného zdroje je **Open Access ÚK UK**, který bude podrobněji představen níže, **Open Access VUT v Brně**, **Open Access ÚK ČVUT** a další. Autorka doporučuje zejména také webové stránky **Národní technické knihovny v Praze**, která prostřednictvím nich přehledně zpracovává informace o Open Access. Stručně, ale jasně uvádí službu OA, a to také prostřednictvím krátkého propagačního videa. Zároveň poskytuje informace, jak publikovat přes tuto knihovnu, jaké jsou cesty publikování OA, vyhledávání OA podle různých typů dokumentů a odkazuje i na další webové stránky nebo průvodce jiných institucí poskytující OA. Každá knihovna, která se chce podílet na rozvíjení OA by měla vybudovat repozitář. Ten slouží k následnému ukládání a volnému zpřístupňování vědeckých publikací. Takové repozitáře vlastní **Akademie věd ČR, Vysoké učení technické v Brně, Univerzita Tomáše Bati ve Zlíně** a jiní. Repozitář je nutné vybudovat na základě standardů a postupů, jež umožňují podporovat následnou spolupráci, která napomáhá jednotnému formátování metadat ukládaného obsahu. Povědomí o OA mezi akademickými pracovníky a studenty rozšiřuje akce **Open Access Week**, jež se koná od roku 2010 (Asociace knihoven vysokých škol ČR, 2021).

8.3 Příklad Open Access na Univerzitě Karlově

Na Univerzitě Karlově lze publikovat zelenou cestou, umožňující zveřejňování dokumentů pomocí vědeckých časopisů. Plné texty pak autor ukládá či zpřístupňuje v **digitálním repozitáři**, jež je zde v současné době připravován. Dále lze publikovat zlatou cestou, a to prostřednictvím recenzovaných otevřených vědeckých časopisů. Publikace je následně přístupná přes vydavatele. V rámci UK mohou autoři využít slev na vybrané vydavatele. Otevřené publikování zde nabízí také **Nakladatelství Karolinum**. Pro dotazy je tu vytvořeno **Centrum pro podporu Open Science**, jež je součástí **Ústřední knihovny UK**. Oborově specifické rady mají na starosti fakultní koordinátoři (Ústřední knihovna UK, 2019). Univerzita Karlova vlastní své repozitáře a digitální knihovnu **Kramerius UK**, které slouží pro uložení a zpřístupnění digitálních či digitalizovaných dokumentů. Tyto práce obvykle vytvořili studenti, akademičtí pracovníci, vědci a zaměstnanci na UK. Repozitáře, které UK zprostředkovává jsou: *Digitální repozitář UK, Digitální univerzitní repozitář nebo Digitální knihovna Kramerius*. Dále se Univerzita Karlova připojila k akci **Open Access Week** v roce 2015 (Centrum pro podporu Open Science, 2021).

8.4 Závěr

Seminární práce Open Science a její implementace v knihovnách se zaměřila na otevřený přístup k vědeckým informacím. Konkrétně se zabývala hnutím Open Science, které umožňuje a usnadňuje dostupnost nejnovějších výzkumných poznatků.

V současné době dochází k různým pokusům, jak rozšířit povědomí o OS a její zavádění do praxe. Mnohdy se tento proces řídí určitou politikou, kterou upravuje Evropská komise v rámci programu, jež zahrnuje financování výzkumu a inovací. Často se na rozvoji OS podílejí také knihovny, jakožto jedny z výzkumných institucí. Dokážou zprostředkovávat otevřený přístup k vědeckým informacím široké veřejnosti a rozšiřovat tak povědomí o OS, avšak musí splňovat určité podmínky. K těm patří například vybudování vlastního repozitáře pro ukládání a zpřístupňování vědeckých publikací nebo webových stránek, kde bude veřejnost informována o OS.

Otevřená věda v praxi byla nakonec představena také na příkladu Univerzity Karlovy, která má zřízené Centrum pro podporu open science ve spolupráci s Ústřední knihovnou UK. Zmíněny byly také repozitáře, které univerzita spravuje.

Open Science by měla mít pozitivní vliv na společnost a jejím z hlavních cílů je rozšiřování vzdělanosti. Proces zpřístupňování vědeckých informací může podpořit inovace, popřípadě řešení globálních problémů apod. Proto je velmi důležitá implementace otevřené vědy v různých organizacích, které se podílejí na výzkumu, aby tak neustále docházelo k rozšiřování povědomí o OS.

8.5 Zdroje

Bartling, S., & Friesike, S. (2014). *Opening Science: The Evolving Guide on How the Internet is Changing Research, Collaboration and Scholarly Publishing*. SpringerOpen.

Grant, F. (2018). *Liber Open Science Roadmap*. https://zenodo.org/record/1303002#.YQJfOY4zY2z

Hnátková, E. (© 2016 - 2020). Open Science - zbožné přání nebo reálná budoucnost vědy? *Vědavýzkum.cz: Portál Vědavýzkum.cz - Nezávislé informace o vědě a výzkumu*, 1 strana. https://vedavyzkum.cz/nazory-a-komentare/nazory-a-komentare/eva-hnatkova-open-science-zbozne-prani-nebo-realna-budoucnost-vedy

Open access. (2021). Univerzita Karlova: Centrum pro podporu open science. Retrieved July 29, 2021, from https://openscience.cuni.cz/OSCI-8.html

Open access.cz: Jak být open access. (2021). Open access.cz. Retrieved July 29, 2021, from https://openaccess.cz/jak-byt-oa/#collapsable-item-0-1

Open Science Training Handbook. (2018) (Gitbook). https://open-science-training-handbook.gitbook.io/book/

Open Science: An approach to the scientific process that focuses on spreading knowledge as soon as it is available using digital and collaborative technology. Expert groups, publications, news and events. (2021). European Commission. Retrieved July 29, 2021, from https://ec.europa.eu/info/research and innovation/strategy/goals-research-and-innovation-policy/open-science_en

Plánková, J. (2007). Klíčové iniciativy Open Access – „3B". *Ikaros: elektronický časopis o informační společnosti*, 11(12), 1 strana. https://ikaros.cz/klicove iniciativy open access %E2%80%93 %E2%80%9E3b%E2%80%9C

Repozitáře. (© 2015 - 2019). Univerzita Karlova: Ústřední knihovna. Retrieved July 29, 2021, from https://knihovna.cuni.cz/rozcestnik/repozitare/

Simandlová, T. (2014). *Otevřená věda - vědecká (r)evoluce* [Diplomová práce, Filozofická fakulta Univerzity Karlovy v Praze]. https://dspace.cuni.cz/bitstream/handle/20.500.11956/63092/120166749.pdf?sequence=1&isAllowed=y

8.6 Použité obrázky

Five Open Science schools of thought. (2020). Foster. Retrieved July 29, 2021, from https://www.fosteropenscience.eu/content/what-open-science-introduction

Open Science facets as a beehive. (2020). Foster. Retrieved July 29, 2021, from https://www.fosteropenscience.eu/content/what-open-science-introduction

9 Virtuální realita v knihovnách

Autorka: Nikola Doleželová

9.1 Úvod

V této seminární práci, ke které mě inspirovala přednáška pana Jana Hrdličky o 3Dsense tvorbě a videomappingu, bych se chtěla zaměřit na virtuální realitu (VR) a její potenciál v oblasti knihovnictví. Nejprve se pokusím o vysvětlení virtuální reality jako takové, uvedu stručně její historii a vývoj. Poté se zaměřím na virtuální prohlídky a virtuální výstavy. Nakonec shrnu potenciální možnosti, které by mohla přinášet virtuální realita v budoucnu v knihovnách různým skupinám uživatelů.

9.2 Virtuální realita

Jak napsal Tomáš Pipota ve svém článku o virtuální realitě v knihovně, virtuální realita je spojení hardwaru a softwaru, které se v dnešní době těší poměrně velké oblibě a máme díky němu pocit, jako kdybychom se nacházeli v reálném prostředí. *„Hardwarové komponenty čítají pc nebo ps4 (v následujících měsících i xbox), virtuálně realitní brýle, dva a více snímačů pohybu a ovladače. Systémy pro virtuální realitu jsou dnes HTC Vive, Oculus Rift a PS VR. Co se softwaru týče, tady začíná prakticky nekonečná řada možností. Pořizovací cena těchto systémů se pohybuje od deseti až po sto tisíc“* (Pipota, 2019).

9.2.1 Historie

Virtuální realita začala vznikat v šedesátých až sedmdesátých letech minulého století, a to díky vývoji počítačové grafiky a muži jménem Ivan Sutherland, který vytvořil první přilbový displej. Zařízení umělo snímat polohu a směr a tvořily ho dvě obrazovky a brýle, do kterých se z obrazovek přenášel obraz (Škrob, 2020).

Dalším důležitý milníkem ve vývoji virtuální reality byla možnost ovlivňovat generovaný děj, o který se zasloužil Myron Krueger na konci šedesátých let (Zemánek, 2018).

Dnešní virtuální realita funguje v podstatě na podobných principech, díky jejímu rozšíření je ale mnohem dostupnější a skýtá mnoho možností.

9.2.2 Typy VR

Virtuální realita by se dala rozdělit podle určení. Existuje virtuální realita určená většímu množství diváků. Příkladem pro tento typ může být virtuální realita typu CAVE. Virtuální realita, pro kterou používáme náhlavní soupravu je naopak určena jen pro jednu osobu (Zemánek, 2018).

9.3 Virtuální prohlídka

> *„Virtuální prohlídku lze obecně charakterizovat jako interaktivní prezentaci prostoru, která vznikla reálně nasnímanými místnostmi nebo prostředím exteriéru.“*
>
> (Hlavičková, 2016)

Virtuální prohlídka muzea, galerie, knihovny nebo jiné instituce či stavby, je způsob, jak zprostředkovat zážitek z místa, aniž by se návštěvník musel nacházet přímo v dané instituci nebo zemi. Jak uvádí Barbora Šedivá ve své bakalářské práci o virtuálních prohlídkách v galeriích a muzeích, výhodu tohoto přístupu je menší poškození a opotřebení památek. Dalšími výhodou je podle ní neomezený čas prohlídky (Hlavičková, 2018).

9.3.1 Příklady virtuálních prohlídek knihoven v ČR

Možnost prohlédnout si prostor instituce, jako je knihovna, muzeum, galerie, nebo jiné kulturní památky je dnes poměrně rozšířená. Virtuální prohlídku můžeme často najít na webových stránkách instituce.

Národní knihovna České republiky

Příkladem virtuální prohlídky knihovny může být prohlídka na webových stránkách Národní knihovny. Díky ní si uživatel může prohlédnout architekturu Barokní knihovny, Studovny hudebního oddělení nebo třeba Zrcadlové kaple. Při prohlídce je možné pohybovat se mezi patry nebo měřit pomocí funkce metru cokoliv, co si zvolíme.

Krajská vědecká knihovna v Liberci

Knihovna zpřístupňuje prohlídku vnitřních prostor knihovny pomocí „Google maps“. Opět je zde možnost zvolení si libovolného patra budovy.

Městská knihovna Rožnov pod Radhoštěm

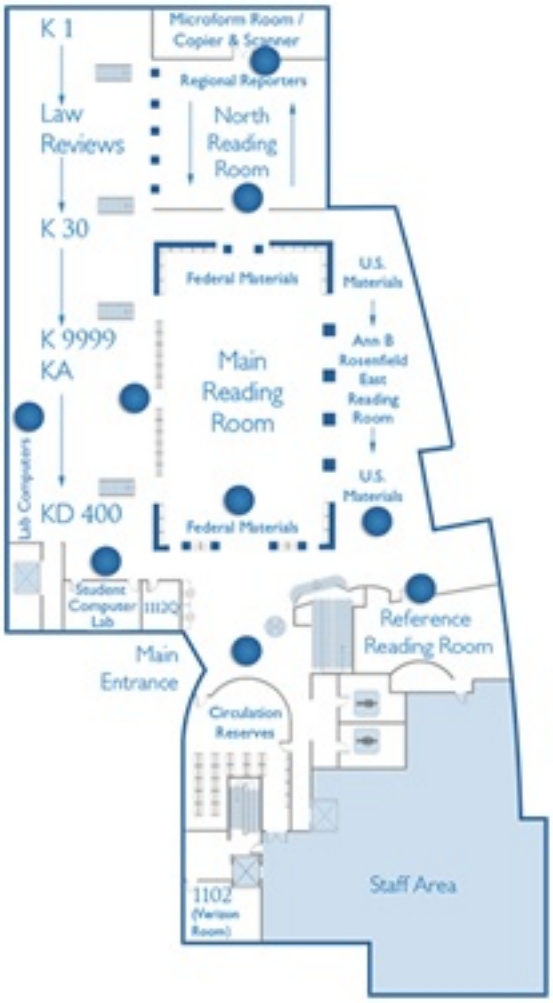
Virtuální prohlídka Městské knihovny v Rožnově pod Radhoštěm sice neumožňuje pohyb kliknutím na šipky, jako to umožňují předchozí knihovny. Naproti tomu ale nabízí volbu sekce knihovny, ve které se pak může uživatel rozhlédnout. Prohlídka také zahrnuje popisy fondu, které čtenáři mohou velmi usnadnit potenciální fyzickou návštěvu knihovny.

Univerzitní knihovna Univerzity Pardubice

Prohlídka funguje na podobném principu jako prohlídka knihovny v Rožnově. Uživatel sice může k pohybu použít šipky, ale obraz se pohybuje o mnohem větší vzdálenost než například u prohlídky Národní knihovny České republiky, tím pádem skýtá i menší pocit skutečného procházení knihovnou. Na druhou stranu ale nabízí ikonu v podobě VR brýlí a možnost použít k prohlídce i headset.

Další způsoby virtuálních prohlídek

Kromě prohlídek, které zachycují 360° obraz volí některé knihovny jiné alternativní metody. Může to být video, ve kterém návštěvníky někdo provádí. Další zajímavou alternativu zvolila školní knihovna s názvem „Hugh & Hazel Darling Law Library“ v Los Angeles. Potenciální návštěvníky s prostorem knihovny seznamuje pomocí fotografie části knihovny, jejího popisu a popisu jejího umístění a nákres patra knihovny shora se slovním označením jednotlivých místností a sekcí.



První patro Hugh and Hazel Darling Law Library: https://www.law.ucla.edu/library

9.4 Virtuální výstava

Výstava jsou vybrané muzejní předměty, které jsou nějak vystavené, uspořádané tak, aby návštěvníka zaujaly a přinesly mu něco nového. Pokud výstava zahrnuje fyzickou přítomnost v instituci, může se návštěvník pohybovat od předmětu k předmětu, zažívat atmosféru a vlastně i spoluvytvářet prostředí výstavy. Naproti tomu u virtuální výstavy takovou možnost nemá. Jakub Jareš ale ve své glose Jak se pozná (dobrá) online výstava vytýká některým výstavám to, že se podobají spíše prohlídce. To znamená například to, že některé exponáty nebo popisy exponátů nejsou dostatečně vidět (Jareš, 2020). Národní galerie Praha nabízí v podstatě spojení virtuální výstavy a virtuální prohlídky. Návštěvník se virtuálně pohybuje přímo v místě výstavy a k vybraným uměleckým dílům je přiřazena detailní fotografie díla a jeho popis.

9.5 Potenciální možnosti VR v knihovnách

Virtuální realita se v poslední době těší velké oblibě a má mnoho vlastností, které by mohly knihovnám pomoci jak v propagaci a přilákání zákazníků, tak v jejím poslání vzdělávání, snižování digitální propasti a dalších činnostech.

Kromě poměrně slibných kladných vlastností má potenciální zabudování VR do služeb knihovny jisté „nepříjemnosti". Jedná se o velmi odlišný způsob přijímání informací od tradičního čtení tištěných knih a vlastně i e-knih. Dále jsou samozřejmě potřeba určité znalosti, které by se museli pracovníci knihovny naučit, aby mohli zařízení v knihovně poskytovat (Pipota, 2017).

9.6 VR jako nástroj pro vzdělávání

Knihovna by měla být místem vzdělávání, zároveň by ale měla, jako každá podobná kulturní instituce, zaujmout své návštěvníky a nabízet jim nové podněty a obecně se přizpůsobit době a způsobu učení. Jak zmiňuje ve své diplomové práci Zdeněk Foral: *„Virtuální realita představuje další vývojový stupeň a revoluci ve vizualizaci informace"* (Foral, 2017).

Virtuální realita má potenciál například u dětí a mladistvých. Zábavná forma by je mohla mnohem více motivovat k učení a vzhledem k čím dál tím větší dostupnosti těchto zařízení, se zdá být tato metoda výuky čím dál tím reálnější. Možnost vyzkoušet si virtuální realitu by také mohla do knihovny přitáhnout nové uživatele a dát jim možnost seznámit se s dalšími formami přijímání informací, které by třeba ani jinak nevyzkoušeli.

9.6.1 VR jako zábava a způsob aktivizace seniorů

Potenciál by mohla VR najít i u seniorů. Jedním z poslání knihovny je seniory aktivizovat, začleňovat do společnosti a celkově jim poskytovat možnosti pro pochopení moderních technologií. Virtuální realita by mohla seniorům tedy kromě možnosti trávení volného času, poskytnout možnost nových sociálních kontaktů jak mezi svou generací, tak mezi mladšími uživateli.

V České republice už virtuální realita pro seniory také není úplnou novinkou. V několika domovech pro seniory si mohlo pár jedinců VR vyzkoušet a například v domově seniorů v Prachaticích měla tato forma aktivizace velký úspěch. Prachatický domov seniorů se rozhodl VR pořídit natrvalo, i když začínají jen formou lehčích virtuálních her (Rabenhauptová, 2020).

9.6.2 VR pro uživatele s postižením

Lidé s postižením jsou stejně jako senioři skupinou, která je ohrožena vyčleněním ze společnosti. Knihovna se snaží plnit roli instituce, která dává těmto skupinám možnost vzdělávání, začleňování, a především rovného přístupu a bezbariérovosti.

> *„Lidé s poruchou autistického spektra (ASS) mají nepřetržité problémy při sociální komunikaci a interakci. Nedostatek sociálních kompetencí jim ztěžuje orientaci v normálních situacích a také jim působí problémy při hledání pracovního místa. V důsledku toho jsou tedy velmi často ohroženi sociální vykořeněností.“*

(Krtičková, 2020)

Virtuální realita v knihovně by mohla lidem s poruchou autistického spektra poskytnout možnost rozvoje a podporu sociálních dovedností nebo dokonce i pomoc se získáním pracovního místa. Tímto tématem už se zabývá několik projektů, například společnost organizace Pistes, která už provedla výzkumnou část projektu a připravuje se na ověření výzkumu v praxi. (Krtičková, 2020).

9.6.3 VR pro uživatele se zrakovým znevýhodněním

Aneta Drmotová ve své bakalářské práci na téma „Virtuální realita pro uživatele se zrakovým znevýhodněním“ uvádí výsledky své experimentální studie, ve které zkoumala, jak budou nevidomí schopni pracovat s VR. Jedinci si mohli nejprve vyzkoušet 2D tvary, následně si mohli zkusit vyjadřování barev pomocí kreslení ve VR. Studentka se také rozhodla vytvořit různé obrazy ve VR, které byly zobrazeny tak, jak je vidí lidé s různými druhy zrakového postižení (Drmotová, 2018).

V knihovně by mohl mít tento přístup přínos jak pro uživatele se zrakovým znevýhodněním, kteří by se mohli kreativně projevovat, tak pro běžné uživatele, kteří by se mohli díky simulaci zrakových vad více seznámit s problematikou a vcítit se do těl uživatelů se zrakovým znevýhodněním.

9.7 Negativní vlivy informačních a komunikačních technologií na uživatele

Informační a komunikační technologie, do kterých patří i VR, nám přinášejí spoustu výhod. K jejich užívání ale patří i určitá rizika. Jedním z možných rizik je závislost na těchto technologiích a tím i zanedbávání povinností, a dokonce i zdravotní a psychické potíže. Dalším možným problémem je tzv. digitální demence, která postupně poškozuje mozek uživatele. Rizika se objevují především při nevhodném či příliš častém používání. Dalším negativním atributem může být vliv na vzdělávání. I

když se VR často používá přímo ke vzdělávání, může uživatele odvádět od studia, díky široké nabídce her a dalších aplikací (Foral, 2017).

9.8 Závěr

Touto seminární prací jsem chtěla dokázat, že virtuální realita má v knihovně své místo. Snažila jsem se stručně definovat, co to vlastně virtuální realita je a jaké jsou potenciální možnosti jejího využití. Do seminární práce jsem se rozhodla zařadit i virtuální prohlídky a výstavy, protože mohou být prezentovány jak prostřednictvím obrazovky počítače, tak pomocí headsetu. Virtuální výstavy jsem se rozhodla zmínit z toho důvodu, že by dle mého názoru skvěle doplňovaly prohlídky knihoven. Tyto prohlídky by se pak posunuly na úplně novou úroveň a možnost listovat virtuálně v knize, kterou jsme si právě vytáhli z regálu by byl dle mého názoru velmi zajímavý zážitek, hlavně pokud bych třeba ve své obecní knihovně mohla virtuálně procházet nějakou významnou zahraniční knihovnou, a dokonce si knihy i zblízka prohlížet a listovat jimi. U virtuálních prohlídek jsem se snažila hlavně uvádět praktické příklady prezentace jednotlivými knihovnami. Nakonec jsem promluvila o výhodách využití VR pro různé skupiny uživatelů, včetně skupin ohrožených sociální izolací. Nemohla jsem nezmínit také možná rizika, která jsou s používáním VR spojená a se kterými by měli být uživatelé také seznámeni a varováni před nimi. Celkově myslím, že jsem cíl seminární práce splnila a že virtuální realita má v knihovně opravdu své místo, zvláště v dnešní době.

9.9 Zdroje

Drmotová, A. (2018). Virtuální realita pro uživatele se zrakovým znevýhodněním (Bakalářská práce). Brno.

Foral, Z. (2017). Vliv a role smartphonu na vzdělávání současnosti a budoucnosti – virtuální realita ve vzdělávání. (Diplomová práce). Brno.

Hlavičková, M. (2016). Virtuální prohlídky v galeriích a muzeích v České republice.(Bakalářská práce).Brno.

Jareš, J. Glosa: Jak se pozná (dobrá) online výstava [Online]. 8.5.2020 Retrieved January 17, 2021, from https://art.ceskatelevize.cz/inside/glosa-jak-se-pozna-dobra-online-vystava-Sqibg

Krtičková, D. Virtuální realita a autismus: Může virtuální realita pomoct lidem s autismem [online]. 7.8.2020 Retrieved January 19, 2021, from https://epale.ec.europa.eu/cs/blog/autism-vr-la-realite-virtuelle-peut-elle-aider-les-personnes-autistes

Pipota, T. Virtuální realita v knihovně. Duha: Informace o knihách a knihovnách z Moravy [online]. 2019, 33(4). ISSN 1804-4255. Retrieved January 17, 2021, from http://duha.mzk.cz/clanky/virtualni-realita-v-knihovne

Rabenhauptová, H. Virtuální realita pro prachatické seniory. [online]. 29.8.2020 Retrieved January 19, 2021, from https://www.sensen.cz/clanky/users/virtualni-realita-pro-prachaticke-seniory

Škrob, P. Vznik, rozvoj a perspektivy virtuální reality. [online]. 2020 Retrieved January 17, 2021, from https://www.fi.muni.cz/usr/jkucera/pv109/2000/skrob.html

Zemánek, J. (2018). Virtuální realita jako objekt a subjekt výstavní praxe.(Magisterská diplomová práce). Brno.

10 Hry jako učební pomůcka

Autorka: Eliška Goldschmídová

10.1 Úvod

Ve své práci bych chtěla navázat na téma přednášky Bc. Anny Hejlkové, která se zabývala její bakalářskou prací s názvem „*Reprezentace historie ve videohrách: Případová studie hry „Kingdom Come: Deliverence*“ ta se věnovala otázce „*jakým způsobem hráči vnímají a přistupují k historii prezentované skrze toto médium*“ konkrétně na hře Kingdom Come: Deliverence. Začala jsem přemýšlet o hrách jako o učebních pomůckách. Při hledání jsem narazila na odborníka, který se zabývá využitím historických her při výuce historie Jeremiahu McCalla. Ten v jednom článku hovoří o nejtradičnějších formách popsání historie, často tvořené akademiky, tedy knihy a učebnice. A o tom, že bychom se neměli nechat zmást dominancí těchto forem, protože nepatří mezi jediná legitimní média, která dokážou vyobrazit minulost (McCall, 2012b).

Mimo akademickou půdu, skoro všichni v nějaké formě dělají historii např. když vyprávějí, co se jim přes den událo, nebo nakreslí obrázek o své dovolené. Dále říká, že např. filmy, obrazy, divadlo, hudba i sociální sítě mohou a často vyobrazují části minulosti a když tak dělají stávají se historií (S tím, že je velký rozdíl mezi historií a přesnou historií a dílo, které je považováno za historii může být její špatnou interpretací ať jde o knihu, film, přednášku nebo jiné). Historické videohry se rozhodně dají považovat za médium, které může provádět historií a ukazovat aspekty minulosti (McCall, 2019). Jak říká McCall o vyobrazení historie, můžeme hry obecně využít v různých odvětvích vzdělávání jak dětí, dospívajících tak i dospělých a toto bude tématem mé seminární práce.

Konkrétně se zaměřím na hry, které jsou pro vzdělávání přímo určené. Zjistím, jaké jsou možnosti na trhu s naučnými hrami a kde je můžeme nalézt. Dále je rozdělím do kategorií podle možnosti jejich využití. Popíšu vliv her na jejich uživatele, a také to, jak velký význam mohou mít hry jako učební pomůcka a zaměřím se na výhody a nevýhody této metody. V dnešní době, kdy je velká většina vzdělávání přesunuta do digitálního prostředí z důvodu pandemie, může se využití her jako učebních pomůcek stát relevantnějším. Podle výsledků dotazníku ze stránky Participace 21, kde odpovídalo 205 učitelů povětšinou základních škol, v nižších procentech poté např. učitelé na střeních školách,

či víceletých gymnáziích. Ohledně otázky na to jak, a podle jakých materiálů učitelé učí se většina respondentů nespoléhá na klasické učebnice, vytváří vlastní výukové materiály, využívají on-line materiálů, webových rozhraní, internetové výukové programy apod. V otevřených odpovědích např. někdo využívá portály s online cvičeními, někdo dokonce přemýšlí na využitím webu k tvorbě didaktických her (Participence 21, 2021).

10.2 Hra jako učební pomůcka

Hra je jakákoli samostatná nebo skupinová činnost sloužící k zábavě, či odpočinku.

> *„Výsledkem vývoje počítačové hry je virtuální svět nebo prostředí, do kterého může hráč pomocí komponentů připojených k počítači (myš, klávesnice, joystick, gamepad a další) vstoupit a jeho dění ovlivňovat. K interakci dochází na základě zásahu hráče do spuštěného programu, který byl pro takový zásah vyvíjen. Obvykle se jedná o určitý úkol, který musí hráč splnit za daných podmínek nebo v časovém limitu, zvítězit v simulaci sportu či boje, případně dosáhnout jiného cíle odvislého od námětu a žánru hry i záměru vývojářů.“*

(Počítačová hra, 2001)

Hry jako učební pomůcky si představuji úplně stejně, jde o jakýsi interaktivní program, pomocí kterého uživatel plní úkoly, které nějakým způsobem rozvíjí jeho vědomosti v daném odvětví, ale zároveň se baví, může to přejít v to, že nemá primárně pocit toho, že se učí. Naučné hry v tuto chvíli považuji jako ozvláštnění, zábavné cvičení v rámci výuky, ne jako její úplnou náhradu, ale její doplnění. Příkladem může být výklad teorie učitelem a následná praxe s pomocí hry. „*Termín škola hrou popisuje Komenského systém výuky, který nemá nic společného s hraním, jak je často chápáno. Jde o hraní na divadle, kdy si látku děti předříkávaly jako v divadle*.“(Kučera, 2019) Možná to není zrovna škola hrou, kterou myslel učitel národů, ale rozhodně nám skrze metodu využití her ve výuce pomůže k procvičení učiva. Mimo školní lavice se vzdělávací hry dají využít několika způsoby např. sebevzdělávání, profesní využití, volná zábava, trénování paměti. Příkladem mohou být hry obsahující rébusy, nebo simulátory (např. starání se o virtuální zvířátko), obecně dále „deskové“ hry, které se přesunuly do digitálního prostředí např. šachy, dáma, pexeso, sudoku a tak dále.

V případě digitálních her záleží samozřejmě o jaký typ hry jde, jestli je náročnější na potřebnou výbavu, nebo ne. Mezi základní výbavu patří počítač, nebo jiné zařízení jako např. telefon, nebo tablet. Mezi komponenty, které připojíme k počítači patří již zmíněná – klávesnice, myš, ovladače a další. Mezi speciální výbavu patří např. VR headsety – brýle na virtuální realitu, senzory, nebo prostory – celé místnosti, které jsou využívané jako simulátory.

Jsou různé způsoby využití her jako učebních pomůcek pro nejrůznější typy studia. Hry mohou být využity již při předškolní vzdělávání, kde se může jednat o procvičování, rozvíjení osobnosti

atd. Kupříkladu pro předškolní děti můžeme obecně najít hry na procvičení logického myšlení a kategorického myšlení, poznávací hry – barvy, zvířátka, rostliny, tvary apod., pexeso, počítání, učení se mluvit, hledání rozdílů. Možnosti využití v předmětech na základní škole i při sebevzdělávání – počítání ve hře, jazyky, poznávací – vlajky, státy, hádání hlavních měst, států.Dále mohou být zakomponovány do výuky na předmětech ve škole, v tuto chvíli v distanční formě. Všem mohou také ve volném čase sloužit jako pomůcka pro sebevzdělávání, pomoct uživateli rozšířit vědomosti v daném obzoru, trénovat paměť nebo ho zapojit do sportovní aktivity. Hry nebo simulátory se dále využívají pro profesionální nebo jiná speciální využití.

10.3 Platformy zpřístupňující vzdělávací a naučné hry

Online zdarma v rámci internetových stránek jako příklad jsem našla několik, které zpřístupňují vzdělávací hry – stránky se buď konkrétně věnují hrám pro danou věkovou kategorii např. děti, nebo se nevymezují na žádnou věkovou kategorii.

Stažení aplikace/programu do zařízení prostřednictvím distributora buď zadarmo, nebo cenu určenou u produktu. Mezi platformy, na kterých jsem naučné hry hledala patří App store pro zařízení Apple nebo Google play store pro zařízení se systémem Android, distribuční platforma Steam, která je předně využívaná na stažení her do počítačů a v poslední řadě specializované platformy na vyučování mezi ně patří např. Dream box learning, Classcraft a další.

10.3.1 Internetové stránky věnující se vzdělávacím hrám

Na stránkách, které se věnují hrám pro nejmenší můžeme vidět již zmíněné poznávací, logické hry apod. Mezi tyto patří například MENSA ČR: PRO NADANÉ DĚTI, stránka, která mimo hry a cvičení zpřístupňuje i další vzdělávání. Dále stránka Strašidýlka, která zpřístupňuje a vytváří hry pro nejmenší. Mezi internetové stránky, které slouží pro sebevzdělávání a jsou určené všem bez rozdílu věku patří například portál MENTEM, který je projektem neziskové organizace, která lidem každého věku pomáhá trénovat sebe sama skrze zábavně stylizovaná cvičení. „*Psychologická cvičení a principy, které jsme vhodně umístili do zábavných her vám pomáhají zlepšovat vaše kognitivní funkce mozku – paměť, pozornost, nebo řešení běžných úkolů*“(Mentem, 2021). Služba je placená, ale nabízí slevu díky partnerstvím s různými organizacemi jako např. ISIC, zdravotní pojišťovny – OZP, VZP,atd. Mentem například využívají v ostravské a brněnské fakultní nemocnici při rekonvalescenci jako trénování mozku po zranění.

Na stránce Trénink paměti můžeme najít klasické hry, jako rozdíly mezi obrázky, tetris, sudoku nebo např. trénink na krátkodobou paměť. Nevýhodou hraní her na internetu může být, že internetové hry jsou často podporovány standard plug-inem do prohlížeče Adobe Flash Player, jehož funkci Adobe

letos ukončilo, ne všechny hry, ale závisí na Adobe Flash Player. Výhodou je, že často pokud jde o samostatné hry, nebývají placené.

10.3.2 Vzdělávací hry na App Store/Google Play

V rámci platformy App Store můžeme nalézt velký počet vzdělávacích her pokrývající předměty jako matematika – sbírky příkladů, zeměpis, chemie, dějepis, geografie, jazyky, českou gramatiku, pravopis, dále obecné procvičování, jakými jsou otázky a odpovědi z různých odvětví a spousta her pro úplně nejmenší.

Např. aplikace NaLékařskou uživatelům umožňuje se zábavnou formou připravit na přijímačky nejen na medicínské obory – tím, že obsahuje tisíce testových otázek z chemie, biologie a fyziky.

Výhodou je možnost stažení do zařízení, které máte většinou stále u sebe, můžete tedy trénovat např. při cestě MHD, když čekáte v čekárně u doktora, prostě ve chvíli, kdy zrovna máte čas. Často jsou aplikace zadarmo, ale zároveň z toho důvodu, se v nich často objevují reklamy. Na jednom místě je zde nejvíce her pro různé věkové kategorie.

10.3.3 Vzdělávací hry na platformě Steam

V rámci platformy Steam můžeme najít převážně simulátory, které při využití speciálních ovladačů mohou sloužit k vyzkoušení/natrénování si dané dovednosti nanečisto před jejím vyzkoušením „*doopravdy*“. Příkladem může být simulátor létání – např. pro ty, co se chtějí naučit létat s letadlem ovládaným vysílačkou, k takovému simulátoru staženému v počítači je možné připojit stejnou vysílačku a trénovat. Mezi další příklady patří – PC building simulator, car mechanic simulator apod. Dále je možné využití VR technologie posadit se a ovládat virtuální kokpit letadla, nebo například vařit. Nalézají se zde i hry zadarmo, ale ve většině případů jde o placené produkty. Výhodou může být stažení přímo v počítači, velice reálné zobrazení, umožnění trénování dané dovednosti. Nevýhodou může být cena produktu.

10.3.4 Vzdělávací hry sloužící pro speciální/profesní využití

Mezi ně patří speciální simulátory pro pracovní využití, to na platformách přímo nenajdeme, ale protože jeho význam ve společnosti jako učební pomůcky se stále zvyšuje, chtěla jsem ho do této sekce zařadit, i když k nim přímo nemáme jako uživatelé přístup. Cílem simulátoru je být co nejpřesnějším vyobrazením dané reality. Simulátory se využívají např. při cvičení armády, v leteckém průmyslu apod.

Česká armáda v minulém roce vyzkoušela nově zakoupený soubojový simulátor:

> *„Systém funguje jako soustava senzorů, která snímá laserové signály iniciované vystřelením cvičné munice. Vyhodnocuje se přesnost a efektivita zásahu a na základě toho je pak zasažený voják z další akce vyřazen, případně je označen jako zraněný a jeho stav vyžaduje ošetření a následnou evakuaci.“*

(Němec, 2020)

Tímto způsobem je vojákům umožněno procvičit vše, na co by narazili v reálném souboji a tím, že se jejich pohyb zaznamenává můžou např. projít své chyby v rámci akce.

10.4 Význam vzdělávacích her v současnosti

Jak jsem se již zmínila výše, hry mohou pomoci člověku rozvíjet logické myšlení, pomáhají mu procvičovat již naučené v nějaké zábavné formě. V rámci výuky ve školách se toho v souvislosti s pandemií koronaviru změnilo hodně, většina výuky musela přejít na distanční formu do digitálních prostor. To pro mnohé znamenalo velké komplikace, obzvlášť pro učitele a žáky nižších ročníků 1. a 2. stupňů základních škol, kteří mohou mít větší problém se soustředit. Zároveň se vše ztížilo i pro rodiče žáků. Distanční výuka by mohla být usnadněna využitím vzdělávacích her, děti by se v průběhu mohly více soustředit, kdyby byla výuka prokládána cvičeními. Zároveň zadávání, zpracovávání a oprava úkolů na další hodinu by v rámci platformy s hrami mohla být pro obě strany jednodušší. Např. systém Classcraft využívá her k vyučování studentů a umožňuje v rámci hraní a procvičování za získané body např. vylepšovat svou virtuální postavu, získat virtuálního mazlíčka apod. Tento systém se rozhodla využít učitelka základní školy Dag Hammarskjold ve Wallingford, Connecticut Gianna Gurg.

> *„Associated Press řekla, že dlouho hledala nové způsoby, kterými by ze svých studentů dostala to nejlepší, proto se rozhodla zkusit třídní herní systém Classcraft. Říká, že viděla zlepšení výsledků studentů od té doby, co začala nástroj v roce 2017 používat. Její výsledky dokonce vedly ostatní učitele k používání herního systému ve výuce.“*

(Lynn. 2019)

Mezi další takovéto programy patří např. Dreambox learning, věnující se výuce matematiky a na trhu se objevují další podobné systémy, které by mohly pomáhat dětem se více zajímat o předměty a zjednodušit distanční výuku. Mimo školní výuku může uživatel z jakékoli věkové kategorie trénovat kognitivní funkce mozku zábavnou formou.

Jak jsem již několikrát zmínila mezi hlavní výhody vzdělávacích her je zábavná forma učení, vhodná k rozvoji logického myšlení, tréninku paměti, a ostatních kognitivních funkcí mozku. U dětí pomáhá

s rychlejším vývojem mozku. V jakémkoli věku nám může pomoct se rychleji rozhodovat a lépe zvládat každodenní úkoly. Cvičením úkolů pracujeme na své koncentraci, předcházíme problémům s pamětí, která trénink potřebuje. Hraní vzdělávacích her, i „normálních“ her nám může pomoci umět lépe pracovat s technologiemi a orientací v nich.

Mezi nevýhody obecně při práci a využívání moderních technologií je dlouhé, nepřetržité hledění do obrazovky/displeje zařízení, což velice namáhá oči. Dalším problémem je sezení u zařízení stále ve stejné poloze, což může vést ke zmenšení zájmu o chození ven, sport apod. protože se zrovna bavíme u hry. Což byl obecně problém v souvislosti s pandemií koronaviru, z důvodu omezení pohybu a přechodu na distanční výuku, jsme všichni většinu času nuceni držet se u obrazovky, nejen z důvodu zábavy, ale i věcí, které by se normálně odehrávaly mimo jejich prostředí. Jako jiné věci může přehnané užívání technologií přejít v závislost. Nebezpečné může být nadměrné vystavování dětí technologiím ve velmi brzkém věku, může značně ovlivnit vývoj jejich mozku, z toho důvodu by se měl každý rodič zamyslet nad tím v jakém věku a jak často využívat digitální technologie jako učební pomůcku a ve volném čase.

10.5 Závěr

V rámci práce jsem nejdříve definovala hru jako takovou a poté výbavu potřebnou k jejich hraní. Představila jsem jaké typy vzdělávacích her můžeme najít a na jakých platformách. Dále jsem zmínila možné výhody a nevýhody platforem. Hry jsem se poté pokusila rozdělit podle jejich možnosti využití jako učebních pomůcek, a zmínit jaký vliv mohou mít na jeho uživatele. Zároveň z různých zdrojů se potvrdilo, že hry/simulátory mohou sloužit jako dobrá učební pomůcka ve škole, práci i při sebevzdělávání. Význam vzdělávacích her se postupně zvyšuje a v souvislosti s pandemií by mohl zjednodušit některé procesy ve vzdělávání. Jako poslední jsem zformulovala odstavec výhod a nevýhod her jako učebních pomůcek. Hry jako učební pomůcky nám mohou v mnohém pomoci, ale v rámci výuky malých dětí, i u nás samých bychom měli přemýšlet, jak moc využíváme technologie a zda si dáváme důležité pauzy, protože technologie a hry, jsou, jak se říká dobrý sluha, ale zlý pán.

10.6 Zdroje

Hejlková, A. (2020). Reprezentace historie ve videohrách: Případová studie hry “Kingdom Come: Deliverance” (Bakalářská práce). Praha.

Kučera, J. Komenský jako oběť propagandy. Co vlastně znamená jeho škola hrou? [Online]. Čtidoma. Retrieved from https://www.ctidoma.cz/zpravodajstvi/komensky-jako-obet-propagandy-co-vlastne-znamna-jeho-skola-hrou-54543

Lynn, B. Video Games Used as Learning Tools in Schools [Online]. Retrieved from https://learningenglish.voanews.com/a/video-games-used-as-learning-tools-in-schools/4754113.html

McCall, J. Playing with the past: history and video games (and why it might matter) [Online]. Retrieved February 10, 2021, from https://jgeekstudies.org/2019/04/22/playing-with-the-past-history-and-video-games-and-why-it-might-matter/

Němec, F. Nové simulátory vyzkoušeli vojáci ze Žatce při výcviku v terénu i v posádce [Online]. Retrieved from https://www.acr.army.cz/informacni-servis/zpravodajstvi/nove-simulatory-vyzkouseli-vojaci-z-zatce-pri-vycviku-v-terenu-i-v-posadce-219167/

Počítačová hra [Online]. (2001-). Retrieved from https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_hra

Jak učitelé hodnotí přechod na online výuku z důvodu pandemie COVID-19 [Online]. Retrieved from https://www.participace21.cz/data/folders/7.pdf

Internetové platformy zaměřené na učení skrze hry ve škole • https://www.dreambox.com/why-dreambox • https://www.classcraft.com/

Platformy distribuující hry/aplikace • https://store.steampowered.com/ • https://www.apple.com/app-store/