VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÉ A INFORMAČNÍ HROZBY PRO ČESKOU REPUBLIKU V KONTEXTU RUSKO-UKRAJINSKÉ VÁLKY

Autor práce: Kamil Hanek, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: doc. Ing. Jaroslav Slepecký, PhD.,

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Kamil Hanek, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Kybernetické a informační hrozby pro Českou republiku v kontextu rusko-ukrajinské války

Název bakalářské práce v anglickém jazyce: Cyber and information threats to the Czech Republic in the context of the Russian-Ukrainian war

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: doc. Ing. Jaroslav Slepecký, PhD.

Datum zadání bakalářské práce: prosinec 2025

Cíl bakalářské práce: Hlavním cílem této práce je navrhnout opatření pro zvýšení odolnosti obyvatel České republiky vůči kybernetickým a informačním hrozbám, zejména v oblasti šíření dezinformací, a doporučit postupy podporující rozvoj informační a kybernetické gramotnosti. Vedlejším cílem práce bude identifikovat společenské skupiny nejvíce ohrožené dezinformacemi a dalšími formami hybridního působení.

Student: Kamil Hanek, DiS.	5.12. 2025 *Datum*	
Vedoucí práce: doc. Ing. Jaroslav Slepecký, PhD.	5.12. 2025 *Datum*	

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.12. 2025 *Datum*	
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2025 *Datum*	
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.12.2025 *Datum*	

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce doc. Ing. Jaroslavu Slepeckému, PhD. za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

HANEK, K. Kybernetické a informační hrozby pro Českou republiku v kontextu rusko-ukrajinské války: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 73 s. Vedoucí bakalářské práce: doc. Ing. Jaroslav Slepecký, PhD.

Klíčová slova: kybernetické hrozby, informační hrozby, dezinformace, hybridní hrozby, informační gramotnost, bezpečnost České republiky, rusko-ukrajinský konflikt, kybernetická bezpečnost

Bakalářská práce se zabývá problematikou kybernetických a informačních hrozeb pro Českou republiku v souvislosti s rusko-ukrajinským konfliktem. Cílem práce je přiblížit, jak tento konflikt ovlivnil bezpečnostní prostředí státu, zejména v oblasti informačního prostoru, šíření dezinformací a kybernetických útoků. V teoretické části jsou vymezeny základní pojmy, historické a geopolitické souvislosti konfliktu a principy hybridního působení, které Rusko dlouhodobě využívá. Praktická část je založena na kvantitativním dotazníkovém šetření mezi obyvateli České republiky a zjišťuje jejich povědomí o současných hrozbách, úroveň informační gramotnosti a míru náchylnosti k dezinformacím. Na základě získaných dat práce hodnotí odolnost české společnosti vůči těmto hrozbám a navrhuje možná opatření vedoucí ke zvýšení její bezpečnosti a informovanosti.

ABSTRACT

HANEK, K. Cyber and information threats to the Czech Republic in the context of the Russian-Ukrainian war: Bachelor's thesis. České Budějovice: College of European and Regional Studies, 2026. 73 pages. Thesis Supervisor: doc. Ing. Jaroslav Slepecký, PhD.

Key words: cyber threats, information threats, disinformation, hybrid threats, information literacy, security of the Czech Republic, Russian-Ukrainian conflict, cybersecurity

This bachelor's thesis deals with cyber and information threats to the Czech Republic in the context of the Russian-Ukrainian conflict. The aim of the thesis is to describe how this conflict has affected the state's security environment, especially in the areas of the information space, the spread of disinformation, and cyber attacks. The theoretical part defines basic concepts, outlines the historical and geopolitical background of the conflict, and explains the principles of hybrid activities that Russia has long employed. The practical part is based on a quantitative questionnaire survey conducted among inhabitants of the Czech Republic and examines their awareness of current threats, their level of information literacy, and their susceptibility to disinformation. Based on the obtained data, the thesis evaluates the resilience of Czech society to these threats and proposes possible measures to increase its security and awareness.

Obsah

Úvod

Ozbrojený konflikt mezi Ruskou federací a Ukrajinou, který v roce 2022 přerostl v otevřenou válku, představuje zásadní zlom v bezpečnostním uspořádání Evropy. Přestože se boje odehrávají mimo území České republiky, jejich dopady významně ovlivňují bezpečnostní prostředí i vnitřní stabilitu států střední Evropy. Moderní konflikty se již neodehrávají výhradně na bojišti, ale stále častěji se přesouvají do kybernetického a informačního prostoru, kde jsou cílem nejen státní instituce, ale především samotná společnost. Kybernetické útoky, dezinformační kampaně a další formy hybridního působení se staly běžnou součástí současných mezinárodních konfliktů. Rusko dlouhodobě využívá informační válku jako nástroj k oslabování důvěry veřejnosti ve státní instituce, k polarizaci společnosti a k narušování demokratických procesů v cílových zemích.

Česká republika jako členský stát Evropské unie a Severoatlantické aliance patří mezi státy, které jsou těmto hrozbám vystaveny zvýšenou měrou. Zranitelnost společnosti v oblasti informační a kybernetické bezpečnosti tak představuje významný bezpečnostní problém. Téma kybernetických a informačních hrozeb je v současné době mimořádně aktuální, neboť se bezprostředně dotýká každodenního života obyvatel, jejich schopnosti orientovat se v informačním prostoru a odolávat manipulativnímu obsahu. Nízká úroveň informační gramotnosti, nedostatečné povědomí o fungování dezinformací a rostoucí závislost na digitálních technologiích mohou vést k oslabení společenské soudržnosti a bezpečnostní stability státu.

Cílem této bakalářské práce je analyzovat kybernetické a informační hrozby, které v kontextu rusko-ukrajinské války působí na Českou republiku, a zhodnotit jejich vliv na českou společnost. Práce se zaměřuje zejména na problematiku dezinformací, informační války a hybridních hrozeb. Na základě teoretické analýzy a empirického dotazníkového šetření mezi obyvateli České republiky budou identifikovány nejvíce ohrožené společenské skupiny a navržena opatření ke zvýšení odolnosti obyvatel vůči těmto hrozbám. Struktura práce je rozdělena do teoretické a praktické části, přičemž teoretická část se věnuje vymezení základních pojmů, historickým a příčinným souvislostem rusko-ukrajinského konfliktu a analýze hybridních hrozeb, zatímco praktická část je zaměřena na vyhodnocení získaných dat z dotazníkového šetření a jejich interpretaci ve vztahu k bezpečnosti české společnosti, přičemž závěrem práce jsou formulována doporučení,

která mohou přispět ke zvýšení informační a kybernetické odolnosti obyvatel České republiky.

1 Cíl a metodika bakalářské práce

Hlavním cílem této práce je navrhnout opatření pro zvýšení odolnosti obyvatel České republiky vůči kybernetickým a informačním hrozbám, zejména v oblasti šíření dezinformací a doporučit postupy podporující rozvoj informační a kybernetické gramotnosti. Vedlejším cílem práce bude identifikovat společenské skupiny nejvíce ohrožené dezinformacemi a dalšími formami hybridního působení.

Ambicí dotazníkového šetření bylo zjistit, jaké je povědomí veřejnosti o kybernetických a informačních hrozbách souvisejících s rusko-ukrajinským konfliktem, a zároveň posoudit úroveň informační gramotnosti respondentů. Dotazník se zaměřoval zejména na schopnost rozpoznat dezinformace, důvěru ve vybrané informační zdroje a chování respondentů v online prostředí. Získaná data měla sloužit k vyhodnocení míry odolnosti české společnosti vůči dezinformačnímu působení a k identifikaci skupin obyvatel, které mohou být těmito hrozbami nejvíce ovlivněny.

1.1 Výzkumná metoda

Pro zpracování praktické části bakalářské práce byla zvolena kvantitativní výzkumná strategie. Tento přístup pracuje s číselnými údaji, jejich měřením a následným statistickým vyhodnocením. Umožňuje ověřovat předem stanovené předpoklady a na základě získaných výsledků je potvrdit či vyvrátit. Hlavním cílem bylo získat objektivní a přehledná data o tom, jak obyvatelé České republiky vnímají kybernetické a informační hrozby související s rusko-ukrajinským konfliktem.

Ke sběru dat bylo využito strukturované dotazníkové šetření. Dotazník byl zaměřen na povědomí respondentů o aktuálních bezpečnostních hrozbách, jejich zkušenosti s dezinformacemi a také na jejich chování v online prostředí. Součástí šetření byly otázky týkající se důvěry v jednotlivé informační zdroje, schopnosti rozpoznat nepravdivé informace a základní orientace v problematice kybernetické bezpečnosti.

Dotazník byl distribuován elektronickou formou mezi obyvatele České republiky od 15 let věku, a to především prostřednictvím sociálních sítí a online komunikačních platforem. Respondenti jej mohli vyplnit kdykoliv a odkudkoliv s připojením k internetu. Elektronická forma byla zvolena z důvodu snadné dostupnosti, rychlé distribuce a

možnosti oslovit širší skupinu respondentů napříč věkovými kategoriemi a sociálními skupinami.

Dotazník obsahoval výhradně uzavřené otázky, které umožnily přehledné zpracování a následné statistické vyhodnocení výsledků. Získaná data byla následně analyzována a použita k posouzení míry odolnosti české společnosti vůči dezinformacím a dalším formám informačního a kybernetického působení.

1.2 Participanti výzkumu

Výzkumný soubor tvořili obyvatelé České republiky různého věku, pohlaví i dosaženého vzdělání. Dotazník vyplňovali respondenti napříč věkovými kategoriemi, přičemž minimální věk byl stanoven na 15 let. Vzhledem k tomu, že se téma týká celé společnosti, snažil jsem se oslovit co nejširší okruh lidí.

Dotazník byl šířen především pomocí odkazu, který jsem zasílal přímo známým a zároveň jej sdílel ve facebookových skupinách. Část respondentů byla oslovena i osobně. U starších osob, které nemají běžně přístup k internetu nebo si s moderní technikou příliš nerozumí, jsem umožnil vyplnění dotazníku na svém mobilním telefonu.

Pro tvorbu a sběr odpovědí byl využit online nástroj Google Forms. Dotazníkového šetření se celkem zúčastnilo 161 respondentů.

1.3 Výzkumné otázky

Tyto otázky sloužily k ověření jednotlivých hypotéz a zároveň pomohly získat podklady potřebné pro splnění výzkumných cílů práce.

1) Jaká je úroveň povědomí obyvatel České republiky o kybernetických a informačních hrozbách souvisejících s rusko-ukrajinským konfliktem?
2) Jaké informační zdroje obyvatelé České republiky považují za důvěryhodné při získávání informací o bezpečnostních událostech?
3) Do jaké míry jsou obyvatelé České republiky schopni rozpoznat dezinformační obsah v online prostředí?
4) Ovlivňují sociodemografické faktory (věk a vzdělání) schopnost rozpoznat dezinformace a orientovat se v informačním prostoru?

Hypotézy, které budou potvrzeny nebo vyvráceny:

H1**:** Mladší respondenti vykazují vyšší schopnost rozpoznat dezinformaci než starší respondenti.

H2**:** Respondenti s vyšším dosaženým vzděláním mají vyšší úroveň informační gramotnosti než respondenti s nižším vzděláním.

H3**:** Respondenti více důvěřují tradičním médiím (televize, tisk, zpravodajské portály) než informacím získaným ze sociálních sítí.

H4**:** Respondenti, kteří aktivně ověřují informace z více zdrojů, vykazují vyšší povědomí o kybernetických a informačních hrozbách.

2 Hybridní hrozby a jejich podoby v kybernetickém a informačním prostoru

Hybridní hrozby a jejich současná podoba vycházejí z využití metod a prostředků běžných, které zahrnují konvenční síly v podobě fyzické armády a jejího materiálního vybavení. Součástí těchto prostředků jsou ale rovněž i ty nekonvenční, kterým Česká republika čelila již v roce 2014 během teroristického útoku v muničním skladišti Vrbětice společnosti Imex Group.[1] Vedle teroristických útoků hovoříme i o dalších faktorech jako dezinformacích a cíleně řízenému organizovanému zločinu a území cizího státu. Hlavním úkolem těchto procesů je cílit na destabilizaci, vnitřní rozvrat a politický nesoulad, následným sekundárním faktorem je rovněž snížení míry politické schopnosti a rozhodnosti vlády daného státu.[2] Projevy hrozeb v České republice vypadají zpravidla tak, že jsou typické svým výskytem v kybernetickém a informačním prostoru, kde hovoříme o takzvané reflexivní kontrole. Ta spočívá v manipulaci a vnímání oběti tak aby sama učinila z vlastní vůle taková rozhodnutí, které bude výhodné pro útočníka.[3]

2.1 Informační hrozby České republiky

Dezinformace samotné ze své podstaty lze definovat specificky vzhledem oblasti kde přímo působí a nebo jinak negativně hrozí. Jejich souhrnná definice však pracuje s předmětem ovlivňování nebo zkreslování pro konkrétní subjekty a nebo skupiny. Základ dezinformace stojí zároveň na vědomí jejího původce, že se jedná o vědomě upravenou informaci s určitým cílem. Její odlišnost ve vícero definicích spočívá v interpretaci.[4] Dezinformace byla v tomto případě pro občana ČR často se vyskytujícím jevem ohledně války na Ukrajině, nebo kauze Vrbětic. V praxi se setkáváme s pravidelnou záměnou pojmů dezinformace, misinformace a malinformace. Misinformace označuje nepravdivou nebo nepřesnou informaci, která je šířena bez vědomého úmyslu příjemce manipulovat či cíleně ovlivnit. Malininformace je charakteristická svojí pravostí sdělení, není nijak zkreslena ani věcně upravena. Jsou distribuovány cíleně podobně jako

[1] IVANČÍK, Radoslav a NEČAS, Pavel. *Hybridné hrozby: bezpečnostná výzva pre demokratické spoločnosti*. Teoretik. Praha: Leges, 2025. ISBN 978-80-7502-823-5. s. 11–18

[2] Richard STOJAR. *Vývoj a proměna konceptu hybridní války*. Vojenské rozhledy. 2017, roč. 26, č. 2, DOI: 10.3849/2336-2995.26.2017.02.044-055. ISSN 1210-3292. s. 44–55.

[3] Jan ŠÍR a kolektiv. *Ruská agrese proti Ukrajině*. 1. vyd. Praha: Univerzita Karlova, Nakladatelství Karolinum, 2017. ISBN 978-80-246-3711-2. s.119-135

[4] IVANČÍK, Radoslav. *Dezinformácie: teoretické východiská ich skúmania*. Teoretik. Praha: Leges, 2025. ISBN 978-80-7502-769-6. s. 30-33

dezinformace, ve většině případů se jedná o interní informace, které svým šířením mohou negativně ovlivnit jednotlivce anebo větší aparáty.[5]

2.2 Související pojmy

V souvislosti, s již zmíněnými pojmy, kterým společnost a informační prostředí České republiky čelí, je vhodné vymezit také další související fenomény, jako jsou propaganda, falešné zprávy, hoaxy a konspirační teorie. Propaganda jako nástroj působení může být založena na polopravdách, nepravdách, ale i na pravdivých informacích vytržených z kontextu. Jejím typickým znakem je jednostranné zaměření a snaha přesvědčit či ovlivnit postoje jednotlivců, skupin obyvatelstva, nebo širší veřejnosti. Konspirační teorie se mnohdy mohou rovněž setkat se záměnou s pojmem dezinformací. Předmětem konspiračních teorií je často odmítání již prokazatelně doložených událostí nebo jevů a jejich nahrazování alternativním výkladem. Tyto teorie se rovněž objevují v situacích, kdy je určitý jev složitý nebo obtížně vysvětlitelný, což vytváří prostor pro zjednodušená a spekulativní vysvětlení.[6] Typickým prvkem konspiračních teorií je přesvědčení o existenci skrytého působení vlivných skupin nebo jednotlivců, kteří mají údajně zásadní vliv na chod státu, společnosti či dalších oblastí veřejného života. V praxi se obyvatelé České republiky s touto formou ze strany ruských služeb běžně nesetkávají, jejich preference spočívají v šíření konkrétních dezinformací.[7]

Fake news, neboli také falešné zprávy jsou dalším nezbytným pojmem. Jejich identifikace bývá mnohdy často náročnější, jejich obsah se odkazuje pravidelně na skupiny ověřitelných faktů, tato skutečnost zpravidla podpoří jejich validitu. Tyto vytvořené příběhové scénáře distribuované prostřednictvím internetu anebo i médií mají za cíl ovlivnění politických názoru anebo vnímání konkrétní politické situace. Jako poslední pojem toho úseku je hoax, v digitálním světě často označován jako správa, která má poplašný a nepravdivý charakter. Hoax je mnohdy rovněž vedle poplašné zprávy nebo určitého druhu podvodu například specifickým druhem zprávy s cílem pobavit anebo nějak zveličit určitou informaci v rámci pobavení konkrétních jedinců v souvislosti reakce okolí nebo společnosti na tuto zprávu. Tyto klamné zprávy, jež nesou tento název

[5] IVANČÍK, Radoslav. *Dezinformácie: teoretické východiská ich skúmania*. Teoretik. Praha: Leges, 2025. ISBN 978-80-7502-769-6. s. 33-35
[6] FRIDMAN, Ofer. *Russian "Hybrid Warfare": Resurgence and Politicisation*. London: Hurst & Company, 2018. ISBN 978-1-84904-909-2. s. 14-24
[7] IVANČÍK, Radoslav. *Dezinformácie: teoretické východiská ich skúmania*. Teoretik. Praha: Leges, 2025. ISBN 978-80-7502-769-6. s. 36-38

jsou nezaměnitelné tím, že jejich obsah častokrát zahrnuje i prosbu dalšího šíření k vícero subjektům.[8]

2.3 Informační prostor a dezinformační kampaně

Informační válka představuje významnou součást hybridního působení a jejím hlavním cílem je ovlivňování veřejného mínění a oslabování důvěry obyvatel v demokratické instituce. Nejde tedy o přímé ničení fyzických cílů, ale o systematické působení na myšlení společnosti. V prostředí České republiky nabývají tyto hrozby několika konkrétních podob.

Jedním z nástrojů jsou dezinformační weby a alternativní mediální platformy, které dlouhodobě šíří obsah odpovídající zájmům cizí moci. Tyto zdroje často pracují s manipulativní interpretací událostí, vytrháváním informací z kontextu nebo záměrným šířením nepravdivých tvrzení. V českém prostředí je jako problematický opakovaně zmiňován například server AE News, celým názvem Aeronet, který byl podle výročních zpráv bezpečnostních složek označován za rizikový z hlediska šíření proruských narativů a obsahu oslabujícího důvěru ve státní instituce. Cílem působení těchto platforem je narušovat informační stabilitu státu a zvyšovat společenskou polarizaci.[9]

Další formou informačního působení je manipulace s historickou pamětí. Ruská státní či proruská média se opakovaně pokoušejí reinterpretovat historické události tak, aby podpořila vlastní geopolitické narativy. Typickým příkladem je snaha ospravedlňovat invazi vojsk Varšavské smlouvy do Československa v roce 1968 jako údajně nutný krok k zabránění politickému převratu. Tímto způsobem dochází ke zkreslování historických faktů a k postupnému oslabování společenského konsenzu o minulosti. Významnou roli hrají také sociální sítě a online diskusní prostředí. Prostřednictvím falešných účtů nebo organizovaných skupin diskutujících dochází k zahlcování informačního prostoru velkým množstvím zavádějících nebo polarizujících příspěvků.[10] Tento jev ztěžuje běžným uživatelům orientaci v aktuálním dění a přispívá k prohlubování společenských rozporů. Specifickým rysem dezinformačních kampaní je rovněž šíření strachu a relativizace pravdy. Cílem často není přesvědčit veřejnost o jediné konkrétní lži, ale vyvolat dojem, že objektivní pravda neexistuje nebo že „každá strana má svou pravdu“. Takové prostředí

[8] Tamtéž s. 39-42
[9] RID, Thomas. *Aktivní opatření: tajná historie dezinformací a politické války*. Přeložil Aleš VALENTA. Historie. Praha: Academia, 2025. ISBN 978-80-200-3523-3. s. 410-428
[10] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti 2026–2030*. Brno: NÚKIB, 2025. s. 30-37

nejistoty následně oslabuje schopnost společnosti jednotně reagovat na krizové situace a bezpečnostní hrozby.[11]

2.4 Kybernetický prostor jako nové bojiště

Vedle informačního prostoru se významným polem působení hybridních hrozeb stal také kybernetický prostor, který je dnes často označován za pátou doménu válčení. V tomto prostředí lze způsobit značné škody bez nutnosti formálního vyhlášení ozbrojeného konfliktu a bez přímého nasazení konvenčních vojenských sil. Jednou z nejzávažnějších hrozeb jsou útoky na kritickou infrastrukturu státu. Ty mohou být zaměřeny na energetiku, zdravotnictví, dopravu nebo informační systémy státní správy. Úspěšný kybernetický útok na tyto sektory by mohl vést k ochromení základních funkcí státu a vyvolat paniku mezi obyvatelstvem. Závažnost těchto rizik v České republice v posledních letech postupně narůstá v souvislosti s rostoucí digitalizací společnosti.

Další významnou oblast představuje šíření škodlivého softwaru, zejména ransomwaru, který po napadení systému zablokuje přístup k datům a požaduje výkupné. Globální kampaně, jako byly útoky WannaCry nebo Petya, zasáhly i subjekty na území České republiky a ukázaly, jak zranitelné mohou být systémy závislé na informačních a komunikačních technologiích. Specifickou kategorií je kybernetická špionáž, kterou provádějí státní nebo státem podporovaní aktéři. Jejím cílem je získávání citlivých dat, technologických informací nebo strategických dokumentů, které mohou být následně zneužity k politickému, ekonomickému nebo vojenskému tlaku.[12]

2.5 Obrana a strategický rámec České republiky

Česká republika na tyto hrozby reaguje postupným budováním legislativního a institucionálního rámce kybernetické a informační bezpečnosti. Základním právním předpisem v této oblasti je zákon o kybernetické bezpečnosti, který stanovuje povinnosti pro provozovatele kritické informační infrastruktury a významných informačních systémů.

Klíčovou roli zde sehrává Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním orgánem státní správy odpovědným za koordinaci ochrany kybernetického prostoru, vydávání bezpečnostních opatření a monitoring hrozeb. Významnou součástí

[11] Jan ŠÍR a kolektiv. *Ruská agrese proti Ukrajině*. 1. vyd. Praha: Univerzita Karlova, Nakladatelství Karolinum, 2017. ISBN 978-80-246-3711-2. s. 172-176

[12] KOLOUCH, Jan; BAŠTA, Pavel; KROPÁČOVÁ, Andrea; KUNC, Martin. *CyberSecurity.* 1. vyd. Praha: CZ.NIC, 2019. ISBN 978-80-88168-32-4. s. 22-30

systému jsou také národní a vládní týmy typu CERT a CSIRT, které poskytují metodickou podporu a pomoc při řešení kybernetických bezpečnostních incidentů.

Strategický rámec doplňuje Národní strategie kybernetické bezpečnosti, jež definuje dlouhodobé politické a technické priority směřující k posilování odolnosti České republiky vůči kybernetickým hrozbám. Obrana proti hybridním operacím však nespočívá pouze v technických opatřeních. Neméně důležité je zvyšování mediální a informační gramotnosti obyvatel, rozvoj kritického myšlení a schopnosti vyhodnocovat důvěryhodnost informačních zdrojů. Hybridní působení tak využívá otevřenosti demokratické společnosti a svobodného informačního prostředí k šíření nejistoty a chaosu. Úspěšná obrana proto vyžaduje kombinaci technologických, institucionálních i společenských nástrojů, které společně přispívají k celkové odolnosti státu.[13]

2.6 Ruská Propaganda jako nástroj informační války

Skutečnost poukazující na samotnou závažnost situace odráží fakt, že Kremelský režim do tohoto odvětví svého rozpočtu posílá ročně více jak 30 miliard českých korun. Přikládá rovněž velkou pozornost jeho výsledkům a dopadům. Pro běžného občana České republiky je zásadním několik kroků, jimiž se dokáže takovým vlivům vyvarovat. Lidské emoce a pocity jsou jedním z těchto napadnutelných faktorů, na jejich základě lze ovlivnit jedince mnoha způsoby. Jedním takovým je právě zavádějící název nebo titulek článku, který čtenář mnohdy nezobrazí celý a zanechá v něm cílenou emoci například v odporu proti Ukrajinské menšině na území Čr.[14]

2.7 Možnosti a techniky jimiž se lze bránit

V rámci zvyšování odolnosti společnosti vůči informačním manipulacím je zásadní rozvoj schopnosti kriticky vyhodnocovat zdroje a obsah sdělení. Jedním ze základních kroků je ověřování původu informací a důvěryhodnosti autora. Uživatelé by měli věnovat pozornost tomu, z jakého média nebo platformy informace pochází a zda je daný zdroj dlouhodobě považován za seriózní. V tomto směru lze využít i specializované projekty zaměřené na hodnocení kvality médií. Stejně důležité je posuzování profilů na sociálních sítích, odkud jsou informace šířeny. Podezřele nově založené účty, nepravidelná aktivita

[13] Tamtéž s. 31-35
[14] Ministerstvo zahraničních věcí České republiky. *Informační manipulace Kremlu: Jak je rozeznat a jak jim čelit.* Praha: Ministerstvo zahraničních věcí ČR, 2025. s. 2-4

nebo jednostranně zaměřený obsah mohou signalizovat neautentické profily či automatizované účty, jejichž cílem je uměle zesilovat určité narativy.

Pozornost by měla být věnována rovněž historii konkrétních informačních kanálů. Některé platformy jsou dlouhodobě spojovány se šířením manipulativního nebo nepravdivého obsahu, a proto je vhodné k informacím z těchto zdrojů přistupovat se zvýšenou mírou opatrnosti. Kritické hodnocení informací by mělo zahrnovat také porovnávání více nezávislých zdrojů. Pokud je určitá zpráva prezentována pouze na omezeném počtu ideologicky vyhraněných platforem a chybí její potvrzení v respektovaných médiích, může to být varovný signál.

Významným nástrojem ověřování je rovněž práce s otevřenými zdroji a databázemi zaměřenými na mapování dezinformací a manipulačních kampaní. Vyhledávání klíčových slov spojených s konkrétní informací může napovědět, zda již nebyla označena jako nepravdivá či zavádějící. Specifickou oblast představuje vizuální obsah, který je v současném digitálním prostředí snadno upravitelný. Fotografie a videa mohou být vytržena z původního kontextu nebo technologicky pozměněna. Reverzní vyhledávání obrázků proto umožňuje zjistit, zda daný materiál nebyl v minulosti použit v jiných, nesouvisejících nebo lživých souvislostech.

Odolnost vůči informačním manipulacím úzce souvisí také se schopností rozpoznat psychologické a komunikační taktiky, které jsou při šíření propagandy využívány. Jednou z nich je záměrné zahlcování informačního prostoru velkým množstvím protichůdných verzí téže události. Cílem takového postupu není přesvědčit příjemce o jediné „pravdě“, ale vyvolat pocit nejistoty a rezignace, kdy se zdá, že objektivní realitu nelze dohledat. Další častou metodou je práce s dílčí pravdou, která je vytržena z širšího kontextu a následně zveličena tak, aby podporovala zavádějící interpretaci. Významnou roli hrají i zastrašovací narativy, například vyvolávání obav z rozsáhlé eskalace konfliktu, jejichž cílem je oslabit veřejnou podporu určitých politických nebo bezpečnostních kroků.

Je třeba zdůraznit, že manipulativnímu obsahu může podlehnout kdokoliv, bez ohledu na věk či vzdělání. Rozvoj mediální a informační gramotnosti, schopnost pracovat s více zdroji a ochota ověřovat si informace však významně zvyšují individuální i společenskou

odolnost vůči informačním hrozbám. Tyto kompetence se tak stávají důležitou součástí širší bezpečnostní odolnosti demokratické společnosti.[15]

[15] Ministerstvo zahraničních věcí České republiky. *Informační manipulace Kremlu: Jak je rozeznat a jak jim čelit.* Praha: Ministerstvo zahraničních věcí ČR, 2025. s. 2-15

3 Kybernetické a informační hrozby z pohledu bezpečnostní strategie České republiky a národní strategie kybernetické bezpečnosti

Bezpečnostní strategie České republiky z roku 2023 představuje základní koncepční dokument bezpečnostní politiky státu. Slouží jako výchozí rámec pro tvorbu dalších navazujících strategií a koncepcí v oblasti bezpečnosti. Dokument vymezuje hlavní principy, priority a dlouhodobé směřování bezpečnostní politiky České republiky a je závazným podkladem pro činnost orgánů státní správy i dalších složek veřejné moci.[16]

3.1 Bezpečnostní prostředí České republiky

V kontextu strategických dokumentů státu je bezpečnostní prostředí chápáno jako celek vnitřních i vnějších okolností, vlivů a aktérů, které se podílejí na utváření bezpečnosti a stability České republiky. Aktuální strategie zároveň upozorňují, že toto prostředí prochází rychlými změnami, je silně propojené a jeho další vývoj je stále hůře předvídatelný v kontextu mezinárodní situace.[17]

3.2 Vývoj a proměny bezpečnostního Prostředí České Republiky

Bezpečnostní strategie také vymezuje hlavní státy, které mají zásadní vliv na aktuální bezpečnostní situaci. Ruská federace je označována jako největší přímá hrozba pro bezpečnost Evropy, a to jak v současnosti, tak i z dlouhodobého hlediska. Čínská lidová republika naopak nepůsobí jako bezprostřední vojenské ohrožení, ale představuje významnou systémovou výzvu. Oba aktéři jsou spojováni se snahou oslabovat a měnit stávající mezinárodní řád založený na pravidlech. Významnou změnu bezpečnostního prostředí přinesla ruská invaze na Ukrajinu, která znamenala návrat otevřeného ozbrojeného konfliktu do Evropy. Tím skončilo období relativní stability, které následovalo po studené válce, a znovu se ukázala důležitost vojenské síly při prosazování politických zájmů. Současné bezpečnostní prostředí je zároveň velmi komplexní a vzájemně propojené. Stále obtížněji lze rozlišovat mezi vnitřní a vnější bezpečností státu a současně se prolíná i fyzický a kybernetický prostor, protože bezpečnostní hrozby se objevují v obou těchto oblastech současně.[18]

[16] ČESKO. Vláda České republiky. *Bezpečnostní strategie České republiky 2023*. Praha: Úřad vlády České republiky, 2023. s. 5
[17] Tamtéž s. 11
[18] Tamtéž s. 12-13

4 Teroristický útok na muniční sklad ve Vrběticích

Každý stát, který disponuje uzemní celistvostí a individuální mírou bezpečnostního prostředí je specificky náchylný na narušení své bezpečnosti, ať už pomocí vlivu dezinformací a nebo jiných způsobů vedení moderní války. Česká Republika se dlouhodobě řadí mezi světovou elitou co se týče vnitřní bezpečnosti. Události ve Vrběticích v říjnu 2014 však velmi značně a razantně ovlivnily toto vnímání.[19]

Munice, jež vybuchla ve Vrběticích, byla v té době ve vlastnictví společnosti Imex Group. Útok na sklad ve Vrběticích byl proveden ruskými agenty z jednotky 29155. Tato jednotka spadala pod GRU. Jmenovitě byl útok proveden agenty Anatolijem Čepigou a Alexandrem Miškinem. Rozklíčování tohoto případu přišlo až po více než pěti letech, v roce 2020, kdy se objevily první náznaky skutečnosti, že sklad byl zničen právě těmito agenty. Pomyslným vodítkem bylo jejich zadržení na území Velké Británie. Důvodem jejich pobytu na území Velké Británie bylo provedení vraždy ruského agenta Skripala, který poskytoval mnoho informací západnímu světu a stal se tak pro Ruskou federaci nebezpečným. Při pokusu o jeho vraždu měla být použita látka Novičok. Spojitost agentů ohledně Vrbětic souvisela prvotně s tím, že se v době výbuchu zdržovali na území ČR. To bylo prvotním impulzem k hledání souvislostí. Ruští agenti pracovali samostatně, nelze však ani stanovit, nebo vyloučit, zda jim v průběhu pomáhal někdo z ruské ambasády, kdo by jim připravil zázemí operace. Je nutné dodat, že atentát byl proveden v období, kdy Ruská federace intervenovala na Ukrajině.[20]

4.1 Události před rokem 2014

BIS a NCOZ vyvodily závěr, že operace v roce 2014 byla již několikátá v pořadí. V roce 2011 došlo k obdobnému útoku, ale již za hranicemi ČR. Tento útok se týkal konkrétně bulharského Lovnidolu, kde bylo nástražné výbušné zařízení instalováno tak, aby explodovalo až na místě po exportu munice z ČR. Důležitou osobou ve věcech společnosti Imex Group je Nikolaj Šapošnikov. Tato osoba figurovala ve funkci konzultanta pro zahraniční obchod a mimo jiné zaštiťoval zakázku doručenou právě do Bulharska. Šapošnikov se na území ČR dostal již v letech rozpadu Sovětského svazu. V mládí sloužil jako voják tehdejší sovětské armády v Afghánistánu a jeho kariéru lemovala spousta úspěchů a pochval. Po předčasném opuštění armády a ukončení přímé vojenské

[19] SPURNÝ, Jaroslav. *Vrbětice: ruská operace, která změnila Česko: pozadí největšího teroristického útoku v moderních dějinách země*. Praha: Respekt Media, 2025. ISBN 978-80-909308-6-5. s. 35-43
[20] Tamtéž s. s. 43-46

služby se vydal žádat o azyl do České republiky. Spoustu skutečností o svém původu zatajil, včetně toho, že byl vyšším příslušníkem sovětské armády. V průběhu let jeho činnost na území ČR vykazovala diskutabilní transakce ohledně nemovitostí a skupování majetků v zahraničí za finanční částky, kterými by v rámci svého příjmu nemohl disponovat. Zahraniční operace tohoto typu původně vykonávala lokální FSB, ta měla fungovat pouze na území Ruské federace, ale neefektivita GRU na začátku tisíciletí donutila Vladimira Putina k tomuto razantnímu kroku. Velkým milníkem pro Českou republiku byla skutečnost že se Bezpečnostní informační službě podařilo na počátku první dekády nového tisíciletí detekovat vznikající systém s cílem špionáže. Na svědomí ho měli mít dva agenti GRU.[21]

4.2 Detaily a odlišnosti strategií

Fungování GRU dlouhodobě vykazovalo znaky operací spíše přímo v terénu, oproti například Číně, která se snažila progresivněji pojmout tento způsob prosazování svých zájmů. Čína se upírala primárně cestou kybernetiky. Zpravidla se dnes jedná o méně nákladnou a detekovatelnou metodu vedení boje, která častokrát dokáže ve výsledcích předčit kinetické operace přímo na území. Ruská GRU opět začala nabývat na významu díky nově jmenovanému generálovi do jejího čela, jednalo se o Igora Sorguna. GRU přešla k metodám diverzních akcí mimo území Ruské federace. Jednotky Specnatz podléhaly opět GRU, podobně jako v Československu v roce 1968 tak v roce 2014 velmi výrazně ovlivnily a dopomohly strategiím GRU.[22] Ruskou progresivní podobu dnešních nově vzniklých strategii spatřujeme i ve skutečnosti sestřelení malajského dopravního letounu nad Východní Ukrajinou právě v roce 2014. Letoun byl zasažen dle stanoviska soudu ruským systémem obsluhovaným několika příslušníky ruských tajných služeb. Náčelník ruského generálního štábu Valerij Gerasimov se veřejně sám pochlubil vývojem ruských strategií, paralelu v tomto současném schématu lze najít v již zmíněných čínských strategiích. Změna strategie, kterou Gerasimov veřejně odhalil je vymezena do několika bodů. V prvním bodě se soustředí na upuštění od přímé destrukce a ničení k jiným druhům působení nebo ovlivňování. Bod druhý opět obdobně stanovuje upuštění od destrukce a ničení k internímu rozložení. Ve třetím bodě se ruská strategie opírá o kulturní válku a nabourání vnitřního stavu společnosti. Následují část se zaměřuje na

[21] SPURNÝ, Jaroslav. *Vrbětice: ruská operace, která změnila Česko: pozadí největšího teroristického útoku v moderních dějinách země*. Praha: Respekt Media, 2025. ISBN 978-80-909308-6-5. s. 47-55

[22] LITVINENKO, Aleksandr Val'terovič; FEL'ŠTINSKIJ, Jurij Georgijevič a LEMEŠANI, Tomáš. *Rusko v plamenech: jak vznikl režim v Kremlu a jak funguje*. Universum. Praha: Euromedia Group, 2022. ISBN 978-80-242-8237-4. s. 269-275

využití menších speciálních oddílů na místo početnější konvenční armády. Zhruba v polovině seznamu hovoříme o přesunu z fyzického prostoru boje k boji spojenému s informacemi a psychologií. Šestý bod cílí na preferování bezkontaktního boje, opět na místo náročnějšího fyzického způsobu. V sedmém bodě se klade důraz na postup od lineární a lineárně členěné války k válce absolutní. Třetí bod od konce seznamu stanovuje preferenci války v kyberprostoru a lidském vědomí. Předposlední bod seznamu se věnuje přesunu od symetrické války k asymetrické, ta zahrnuje oblasti politiky, ekonomiky a technologií v podobě kampaní a programů. Poslední a nejvíce radikální bod stanovuje vnímání války jako dočasného stavu k pojetí dlouhodobého, trvalého konfliktu jako přirozeného rámce fungování národa. Tento souhrn novodobých ruských strategií velmi výrazně ohrožuje bezpečnostní prostředí České republiky, dokáže působit soustavně a trvale. Válka psychologická a informační je dnes prostředkem podmanění národa a jeho psychologického rozpoložení, které dokáže velmi výrazně usnadnit přístup k jeho strategickým materiálům v podobě zbrání a podobně. Vrbětické události lze definovat jako cizí mocností řízenou sabotážní operaci, která vykazovala znaky dlouhodobé přípravy a kombinovala zpravodajské aktivity, diverzní prvky a nepřímé formy nátlaku.[23]

4.3 Kybernetické a informační útoky na Českou republiku pro rok 2024

Podle úřadu pro národní a kybernetickou bezpečnost, Byly data pro rok 2024 následující. Česká republika čelila více jak 250, konkrétně 268 kybernetickým útokům. Nejvíce tuto oblast zahrnoval phishing,, sekundárním prvkem útoků byly v předloňském roce podvodné emaily. Četnost útoků v předloňském roce mírně zvýšila svoji četnost, ale zároveň snížila míru své závažnosti, co se týče konkrétních dopadů.[24] Veřejný sektor čelil ve značné míře DDoS útokům. Ty v roce 2022 byly směřovány více konkrétně. Speciální zaměření se týkala jednotlivých rozhodnutí našeho vládního aparátu, právě v souvislosti s Válkou na Ukrajině. Původ těchto útoků NUKÚB přisuzuje ruskojazyčným celkům nebo jednotlivcům.[25] Následujícím odvětvím, které rovněž čelilo četným útokům byl finanční sektor. Tato oblast čelila převážně již zmíněnému phishingu. Dalším využitým prvkem, se kterým se jednotlivé instituce finančního sektoru setkávaly bylo vnější skenování sítě doplněné o podvodné emailové zprávy.

[23] SPURNÝ, Jaroslav. *Vrbětice: ruská operace, která změnila Česko: pozadí největšího teroristického útoku v moderních dějinách země*. Praha: Respekt Media, 2025. ISBN 978-80-909308-6-5. s. 56-63
[24] Národní úřad pro kybernetickou a informační bezpečnost. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Brno: NÚKIB, 2024. s. 11
[25] Tamtéž s. 29

V pořadí již třetí prvek kritické infrastruktury, který byl kybernetickými zásahy dotčen se týká energetiky a průmyslu. Útoky jsou cíleně vedeny v této oblasti proti systémům operačních technologií. Dotčeny bývají rovněž systémy SCADA. Česká energetika čelila v tomto období jednomu takovémuto útoku, jeho výsledkem bylo ovlivnění technických funkcí systému a jejich běžných provozních hodnot. Následky těchto aktivit markantně ohrožují bezpečnost, ale i například právě majetek a zdraví ve spojitosti s jejich dopady.

Zdravotnictví vykazuje převážně cílené útoky na člověka samotného. Metoda zde využívaná velmi četně, je phishing. Specifikace toho sektoru se oproti třeba finančnímu liší ve větší náchylnosti pro samotné subjekty, které jsou součástí těchto zařízení. Osoby z oblasti zdravotnictví jsou na tyto útoky náchylnější z hlediska znalosti těchto útoků a práce s nimi, oproti například finančnímu sektoru.

Posledním zmíněným odvětvím je Vzdělávací sektor. Více jak tři čtvrtiny těchto zařízení byly nějak konfrontovány v podobě phishingu a podvodných emailů.[26]

Z hlediska konkrétních bezpečnostních incidentů byl rok 2024 významně ovlivněn činností ruských státem podporovaných kybernetických skupin, zejména APT28, napojované na GRU, dále APT29 a skupiny COLDRIVER. Tyto subjekty se dlouhodobě zaměřují na špionážní a vlivové operace v kyberprostoru.[27] Přetrvávající riziko představoval rovněž ransomware. V říjnu 2024 byl zaznamenán dosud nejvyšší měsíční počet útoků, konkrétně sedm případů. Tyto incidenty vedly k zašifrování dat napadených organizací a v některých situacích také k dočasnému omezení nebo přerušení poskytovaných služeb.

V oblasti informačního působení byly mezi českým publikem nejvíce rozšířené dezinformační narativy týkající se vývoje bojů na frontě, ekonomických dopadů sankční politiky a vojenské podpory poskytované Ukrajině. Výraznou odezvu měl zejména narativ, podle něhož tato pomoc oslabuje obranyschopnost České republiky.[28]

[26] Tamtéž s. 30-35
[27] Tamtéž s. 23-24
[28] VINŠ, Petr Jan. *Dezinformační narativy o válce na Ukrajině v ČR a ve střední a východní Evropě: Analýza za období červen–říjen 2022*. Praha: Prague Security Studies Institute, 2022, s. 7

5 Příčinné a historické souvislosti rusko-ukrajinského konfliktu

Počátky dnes již probíhajícího konfliktu mezi Ruskou federací a Ukrajinou, které značně zesílily hrozby informační války pro Českou republiku lze definovat v jejich společné minulosti, napříč jejich vztahy a nebo přímo spory o jednotlivá území. Ukrajina již dlouhodobě společně jako zbytek světa musí čelit ruské propagandě a dalším způsobům, jak ruská federace pracuje s informacemi. Za Jeden z mnoha výrazných a negativních vlivů považujeme spor o Kyjevskou Rus. Tady nastává samotný nesoulad mezi oběma stranami. Již v období existence sovětského svazu byla Kyjevský Rus vždy historiky definována jako původní ruské území, Naproti tomu se ruští historici potýkali s opačnými tezemi historiků z Ukrajiny. Tento jeden z prvních státních útvarů však ale těžko zařadíme na jednu nebo druhou stranu. V kontextu tehdejších poměrů je třeba si uvědomit, že v období Kyjevské Rusy nelze definovat existence určitých národností spojené s jednotlivým územím tak jak je známe dnes.[29] Spor o Kyjevskou Rus díky těmto skutečnostem považujeme za nepříliš validní a založený na reálných podkladech, je ale stále předmětem Ruské propagandy která si území přidružuje a považuje ho za ruské území, kde vznikly individuální zvyky a obyčeje až v průběhu 19. Století. Tyto zvyky a aspekty kultury podle ruských tvrzení definují Ukrajinu do dnešních dnů a zasadily základy jejímu vzniku.

Další velmi výrazný a pomyslný opěrný bod ruských propagandistických tvrzení se velmi urputně opírá o vznik slova Rus, jenž si s oblibou přivlastňují z hlediska původu a historických souvislostí. Samotné slovo má však původ vzniku v severských zemích a nazývali se jím Varjagové. Dalším zásadním milníkem pro ranou historii Ukrajiny bylo období kdy území padla pod správu zlaté hordy jenž svojí politikou omezila rozvoj v oblasti. Následně Ukrajina čelila podmanění Turky a následně až ruskou carevnou. Povstání v sedmnáctém století bylo dalším historickým markantem, opět se měnila uzemní uspořádání. Toto období stanovilo rozdělení na levobřežní a Pravobřežní Ukrajinu. Oba tyto celky se opět nevyhnuly svému rozpadu a tak Ukrajina v druhé polovině osmnáctého století zanikla.[30]

[29] SYRUČEK, Milan. *Rusko-ukrajinské vztahy: jak hluboké jsou kořeny současného konfliktu?* Aktualizované vydání. V Praze: Grada, 2023. ISBN 978-80-271-5221-6 s. 20-40.
[30] HOLÝ, Petr. *Válka na Ukrajině: kontext*. Pemmikan. Praha: Gnóm! - Jakub Němeček, 2022. ISBN 978-80-88299-21-9 s. 10-47

5.1 Novodobá historie Ukrajiny

V novodobé historii Ukrajiny narážíme velmi značně na nástroje ruské propagandy, které jednoznačně definují Ukrajinu jako celek, který vznikl až díky sovětskému svazu, jenž umožnil její vznik a byl jejím základním stavebním kamenem. Skutečnost je ale vzdálená této ruské tezi. V období kdy se rozpadla carská monarchie a na území Ruska probíhala občanská válka vznikla Ukrajina samostatně. Tento stav vydržel ale pouhé 4 roky.[31] Ukrajina opět padla do područí nově vzniklého Sovětského svazu. V tomto období Ukrajinci čelili označení Malorusové. Být součástí SSSR pro Ukrajinu znamenalo desítky let utlačování a rovněž hladomor který měl za cíl kompletně zničit a nechat zaniknout svobodné a individuální hospodářství. Oběti byly v řádu milionů lidských životů. Stalin tímto krokem v podstatě zredukoval ukrajinskou populaci o necelých sedmnáct procent.[32]

5.2 Krymské Spory

Typickým předmětem sporu mezi Ruskem a Ukrajinou, který se často skloňuje a funguje na ruské straně jako prostředek jakési obhajoby některých jednání a činů, je území Krymu. Krym byl Ukrajině darován v první polovině padesátých let dvacátého století, v době studené války se tak Nikita Chruščov tímto gestem zasadil o to, že dočasně narovnal a částečně podpořil vztahy uvnitř SSSR. Tato událost se velmi úzce propojila s budoucí problematikou tohoto území v souvislosti s rozpadem SSSR a sporu o něj. Je velmi obtížné stanovit oficiálnější postoj ke Krymu z dob sovětského svazu, každý jeho představitel měl na Krym značně odlišný názor, někdo mu nepřikládal váhu a důležitost a někdo naopak ano.[33]

[31] MOKRYK, Radomyr a PADEVĚT, Jiří. *Hovory o Ukrajině*. Praha: Academia, 2023. ISBN 9788020034366 s. 28-49
[32] Tamtéž s. 56-82
[33] FILIP, Scherf. *Ztracená země: Příběh moderního Ruska*. Host, 2024. ISBN 978-80-275-2342-9. s. 94-108

Banderovské hnutí v historickém kontextu

Ukrajina je na dezinformačních a proruských platformách často mylně označována za fašistický stát. Toto tvrzení bývá nejčastěji spojováno s historickým odkazem tzv. banderovců. Organizace, které jsou s tímto pojmem spojovány, lze skutečně označit za nacionalistické až fašizující, přičemž jejich ideologické sympatie směřovaly spíše k autoritářským fašistickým režimům než výhradně k nacistickému Německu. Počátky banderovského hnutí sahají do období před druhou světovou válkou, kdy působilo především na území tehdejšího Polska, konkrétně v oblasti západní Ukrajiny. Ve třicátých letech zde probíhaly ozbrojené střety s polskými bezpečnostními složkami, jejichž cílem bylo dosažení nezávislé ukrajinské státnosti. Významnou postavou tohoto hnutí byl Stepan Bandera, který byl polskými úřady odsouzen k doživotnímu trestu odnětí svobody. Po napadení Polska nacistickým Německem v roce 1939 byl Bandera z vězení propuštěn. V následujícím období došlo ke vzniku Organizace ukrajinských nacionalistů (OUN) a Ukrajinské povstalecké armády (UPA). V historické paměti jsou banderovci neoddělitelně spojeni s tzv. Volyňským masakrem, při němž jednotky UPA prováděly rozsáhlé násilí vůči polskému civilnímu obyvatelstvu, místy doplněné i útoky na židovské komunity.[34]

Samotné hnutí nebylo jednotné a postupně se rozdělilo na dvě hlavní frakce. Jedna část otevřeně spolupracovala s nacistickým Německem a za hlavního nepřítele považovala Sovětský svaz. Druhá frakce, spojená přímo se Stepanem Banderou, vedla ozbrojený boj nejen proti sovětskému režimu, ale v určitých obdobích i proti nacistickému Německu. Společným znakem obou proudů však byla silná protikomunistická orientace a snaha aktivně čelit sovětskému vlivu. V roce 1944 byl Stepan Bandera po několikaletém internování v koncentračním táboře Sachsenhausen nacistickými úřady propuštěn. Tento krok byl motivován snahou využít banderovské struktury ke zpomalení postupu Rudé armády. Přímé připisování válečných zločinů banderovců samotnému Banderovi je však problematické, neboť od roku 1941 neměl faktickou možnost ovlivňovat činnost organizace. Ozbrojené aktivity banderovců neskončily s koncem druhé světové války. Část jejich příslušníků se pokoušela ustoupit přes Maďarsko a Československo na Západ, zatímco jiní pokračovali v partyzánském boji v lesnatých a odlehlých oblastech. Tyto aktivity přetrvávaly až do počátku 50. let, kdy byly jednotky postupně zlikvidovány

[34] MOKRYK, Radomyr a PADEVĚT, Jiří. *Hovory o Ukrajině*. Praha: Academia, 2023. ISBN 9788020034366 s. 51-59.

sovětskými bezpečnostními složkami. V současnosti se k odkazu Stepana Bandery hlásí pouze okrajová část ukrajinské ultrapravicové scény. Vnímat jeho osobu a činy jako reprezentativní symbol ukrajinské společnosti, jak je tomu v ruské propagandě, je proto značně zkreslující. Přirovnání lze jen obtížně hledat, nicméně určitou analogii by bylo možné spatřovat v hypotetické situaci, kdy by byla postava Emanuela Moravce chápána jako klíčový symbol české národní identity.[35]

Etnická a lingvistická struktura obyvatelstva Ukrajiny

Klíčovým determinantem v diskurzu o nezávislosti a národní identitě Ukrajiny je demografické složení obyvatelstva, zejména z hlediska mateřského jazyka a národního sebeuvědomění. Lingvistická mapa země vykazuje značnou regionální diferenciaci: v západní části Ukrajiny tvoří rodilí mluvčí ruštiny méně než 5 % populace. Směrem k východu tento podíl postupně graduje; v centrálních a přilehlých východních regionech se pohybuje v rozmezí 5 % až 24 %, zatímco v nejvýchodnějších oblastech dosahuje zastoupení ruskojazyčného obyvatelstva 24 % až 74 %. Za dominantně ruskojazyčné oblasti lze označit Krym a část Donbasu, což je přímým důsledkem dlouhodobých rusifikačních procesů. Ačkoliv oficiální ruská rétorika, reprezentovaná Vladimirem Putinem, často operuje s tvrzením o převážně ruskojazyčném charakteru celého ukrajinského státu, statistická data tuto interpretaci vyvracejí.[36] Zásadním zjištěním je, že jazyková příslušnost nekoreluje přímo s identitou národní; i v regionech s nejsilnějším zastoupením ruštiny (s výjimkou Krymu) se více než 55 % obyvatel identifikuje jako Ukrajinci, nikoliv jako Rusové. V ostatních částech země se podíl obyvatel s proukrajinským smýšlením pohybuje nad hranicí 70 %, zatímco Krym vykazuje specifické složení, kde se k ruské identitě hlásí přibližně 75 % rezidentů. Historickou legitimitu ukrajinské státnosti a jednoty potvrzují výsledky referenda o nezávislosti z roku 1991, v němž se pro samostatnost vyslovilo přes 80 % voličů i v nejvýchodnějších regionech, přičemž na Krymu byla tato hranice rovněž překročena (více než 50 %). Je však nutné zdůraznit, že v důsledku probíhajícího válečného konfliktu lze v současné době očekávat významné posuny v těchto demografických ukazatelích.[37]

[35] SCHULZE WESSEL, Martin. *Prokletí impéria: Ukrajina, Polsko a scestí ruských dějin*. V českém jazyce vydání první. Přeložil Petr DVOŘÁČEK. Praha: Maraton, 2024. ISBN 978-80-88411-31-4. s. 171-186

[36] SYRUČEK, Milan. *Rusko-ukrajinské vztahy: jak hluboké jsou kořeny současného konfliktu?* Aktualizované vydání. V Praze: Grada, 2023. ISBN 978-80-271-5221-6 s.76-85

5.3 Denuklearizace Ukrajiny

Zánik Sovětského svazu postavil mezinárodní společenství před zásadní bezpečnostní výzvu spojenou s rozmístěním jaderného arzenálu na území nově vzniklých postsovětských republik. V důsledku dislokace sovětských strategických zbraní se Ukrajina, společně s Běloruskem a Kazachstánem, stala faktickým držitelem nukleárního potenciálu včetně odpalovacích stanic a výrobní infrastruktury. V té době by Ukrajina svou vojenskou silou zaujímala pozici třetí nejmocnější jaderné velmoci světa, hned po Spojených státech a Ruské federaci.[38]

Mezinárodní obavy vyvolávala zejména absence kontroly nad těmito zbraněmi a skutečnost, že tyto státy nebyly signatáři smluv o nešíření jaderných zbraní. K technickým komplikacím se přidávala také končící životnost většiny hlavic, jejíž limitní horizont byl odhadován na rok 2008. Zatímco Bělorusko a Kazachstán přistoupily na podmínky odzbrojení relativně brzy, ukrajinská politická reprezentace byla v otázce denuklearizace nejednotná. Část vedení prosazovala zachování jaderného statusu, což vnímala jako nástroj k získání prestiže a případného křesla v Radě bezpečnosti OSN. Prodloužená jednání a neochota ratifikovat příslušné smlouvy vedly k eskalaci napětí mezi Ukrajinou a mocnostmi. Zásadním argumentem pro odzbrojení se nakonec stala extrémní finanční náročnost údržby arzenálu a silný diplomatický tlak USA a Ruska. Existovala reálná hrozba, že bez odevzdání jaderných zbraní nebude ukrajinská nezávislost mezinárodně uznána, což by zablokovalo její vstup do globálních struktur. Klíčové milníky procesu denuklearizace Ukrajiny zahrnovaly podpis trilaterální dohody v Moskvě dne 14. ledna 1994 o transportu veškerého jaderného arzenálu z ukrajinského území a následné přistoupení Ukrajiny ke Smlouvě o nešíření jaderných zbraní v listopadu téhož roku. Proces byl završen dne 5. prosince 1994 oficiálním podpisem Budapešťského memoranda, které Ukrajině garantovalo bezpečnostní záruky a respektování její územní celistvosti. Hlavním pilířem memoranda byl závazek signatářských mocností garantovat Ukrajině územní celistvost a nedotknutelnost hranic výměnou za její úplné jaderné odzbrojení. V rámci implementace dohody převzalo Rusko zbývající hlavice, zatímco Spojené státy finančně participovaly na likvidaci nosičů, strategických bombardérů a raketových sil, včetně transformace základny v Pervomajsku na muzeum. Ukrajině byla jako součást vyrovnání předána námořní základna na Krymu. Tento proces byl klíčovým

[38] HOLÝ, Petr. *Válka na Ukrajině: kontext*. Pemmikan. Praha: Gnóm! - Jakub Němeček, 2022. ISBN 978-80-88299-21-9 s. 20-42

momentem pro stabilizaci postsovětského prostoru, byť jeho dlouhodobá účinnost byla pozdějšími událostmi zpochybněna.[39]

5.4 Moderní dějiny Ukrajiny

Události označované jako oranžová revoluce představují zásadní zlom v moderních dějinách Ukrajiny a jsou bezprostředně spjaty s koncem prezidentského mandátu Leonida Kučmy a následnými volbami v roce 2004. V tomto volebním klání se proti sobě postavili dva kandidáti s diametrálně odlišnými vizemi budoucího směřování země: Viktor Janukovyč, prosazující orientaci na Ruskou federaci a východní politické struktury, a Viktor Juščenko, který reprezentoval prozápadní aspirace a snahu o užší ekonomickou integraci s Evropou. Veřejnost tuto volbu vnímala jako rozhodující moment pro budoucí geopolitickou identitu státu.

Průběh voleb byl charakterizován značným napětím, přičemž Viktor Juščenko byl na základě předběžných průzkumů i po prvotním sčítání hlasů favorizovaným kandidátem. Oficiální výsledky však po druhém kole přinesly nečekaný zvrat ve prospěch Viktora Janukovyče, který měl zvítězit o 3 %. Tento výsledek vyvolal okamžitá podezření z rozsáhlých volebních manipulací a falšování dat. Mezi nejčastěji uváděné praktiky patřilo zneužívání volných volebních lístků, které stoupencům Janukovyče umožňovaly vícenásobné hlasování v různých okrscích, což v některých případech vedlo k situaci, kdy počet odevzdaných hlasů převyšoval počet registrovaných voličů. Reakcí na nerespektování demokratických principů byla masivní mobilizace občanské společnosti, která vyústila v oranžovou revoluci, symbolizovanou právě touto barvou. Protesty na kyjevském náměstí Nezávislosti (Majdan) se nesly v pokojném duchu a vyvinuly značný tlak na státní instituce. V důsledku těchto událostí přistoupil ukrajinský parlament 27. listopadu 2004 k anulování výsledků druhého kola voleb. Kontext voleb byl navíc zatížen pokusem o vraždu Viktora Juščenka, který byl před zahájením hlasování otráven dioxiny, což následně potvrdili experti na klinice v Rakousku. Ačkoliv neexistují oficiální prameny jednoznačně identifikující viníka, v politickém diskurzu se často spekulovalo o zapojení ruské Federální služby bezpečnosti (FSB) s cílem eliminovat prozápadního kandidáta ve prospěch Janukovyče. Politická krize byla nakonec vyřešena opakováním

[39] HOLÝ, Petr. *Válka na Ukrajině: kontext*. Pemmikan. Praha: Gnóm! - Jakub Němeček, 2022. ISBN 978-80-88299-21-9 s. 35-48.

druhého kola voleb, v němž Viktor Juščenko zvítězil s náskokem 8 % hlasů a stal se legitimním prezidentem Ukrajiny.[40]

5.5 Prezidentské volby na Ukrajině v roce 2010

Prezidentské volby konané na počátku roku 2010 představovaly pro Ukrajinu zásadní politický mezník, který reflektoval postupné vyčerpání ideálů oranžové revoluce a rostoucí skepsi veřejnosti k tehdejšímu vedení státu. Ačkoliv vítězství prozápadních sil v roce 2005 vzbuzovalo očekávání v podobě ekonomické stabilizace a emancipace z ruského vlivu, realita funkčního období Viktora Juščenka byla poznamenána jeho klesající popularitou.[41] Juščenko čelil kritice ze strany svých spolupracovníků pro administrativní neefektivitu a neschopnost schvalovat klíčové dokumenty v řádných termínech, což vedlo k jeho transformaci v očích veřejnosti z progresivního reformátora v politika motivovaného primárně udržením moci. V této atmosféře politické deziluze se jako hlavní protikandidát Viktora Janukovyče profilovala Julia Tymošenková, která si i po odeznění revolučních událostí udržela značný veřejný vliv. Její kandidatura však byla zatížena kontroverzemi a obviněními, která často iniciovala Ruská federace. Tymošenková byla obviňována z korupčního jednání vůči ruským státním činitelům a z uzavření ekonomicky nevýhodných kontraktů na dodávky zemního plynu. Tyto útoky byly v médiích umocňovány poukazem na její dřívější podnikatelské aktivity v energetickém sektoru, které realizovala společně se svým manželem.[42]

5.6 Geopolitické důsledky volebního výsledku

Volební souboj v roce 2010 do značné míry kopíroval mocenské rozložení z roku 2004, zejména co se týče diametrálně odlišné geopolitické orientace obou finalistů. Zatímco Julia Tymošenková reprezentovala kontinuitu prozápadního směřování, Viktor Janukovyč byl exponentem ruských zájmů a podporovatelem vize Vladimira Putina o těsném přidružení Ukrajiny k Ruské federaci. V konečném sčítání hlasů zvítězil Viktor Janukovyč s těsným náskokem přibližně 3 %. Julia Tymošenková sice vyjádřila pochybnosti o regulérnosti volebního procesu, nicméně k zásadním krokům k jejich zpochybnění již nepřistoupila. Nástup Janukovyče k moci předznamenal období politické perzekuce, které vyvrcholilo v roce 2011 odsouzením Julie Tymošenkové k sedmiletému

[40] KŘÍŽ, Zdeněk. *Cesta z Ruska: ruská agrese proti Ukrajině a její důsledky*. Brno: Munipress, 2023. ISBN 8028002609. s. 15-25

[41] SYRUČEK, Milan. *Rusko-ukrajinské vztahy: jak hluboké jsou kořeny současného konfliktu?* Aktualizované vydání. V Praze: Grada, 2023. ISBN 978-80-271-5221-6 s. 151-164

[42] MOKRYK, Radomyr a PADEVĚT, Jiří. *Hovory o Ukrajině*. Praha: Academia, 2023. ISBN 9788020034366 s. 100-110.

trestu odnětí svobody. Její věznění bylo provázeno opakovanými hladovkami a skončilo až v souvislosti s převratnými událostmi na počátku roku 2014, kdy byla ze zdravotních důvodů propuštěna. Přestože se Tymošenková následně pokoušela o návrat na politické výsluní, její aktivní role ve vrcholné politice byla po těchto událostech již výrazně oslabena.[43]

5.7 Asociační proces Ukrajiny s Evropskou únií

Klíčovým momentem pro další politický vývoj Ukrajiny byla očekávaná asociační dohoda s Evropskou unií, jejímž předmětem mělo být posílení hospodářské a kulturní kooperace. Je nezbytné zdůraznit, že tato smlouva nepředstavovala přímý příslib vstupu do EU, nýbrž rámec pro hlubší integraci a spolupráci. Před plánovaným podpisem dokumentu však došlo k zásadnímu geopolitickému obratu, do něhož aktivně vstoupil ruský prezident Vladimir Putin. Ruská federace využila vlivu na tehdejšího proruského prezidenta Viktora Janukovyče a nabídla ukrajinské straně ekonomicky atraktivní alternativu v podobě rozsáhlých finančních půjček, redukce cen zemního plynu i ropy a navýšení podílu na tranzitu surovin. Podlehnutí tomuto tlaku a následné odstoupení od podpisu dohody s Evropskou unií vyvolalo okamžitou a masivní reakci ukrajinské společnosti, která se odmítla smířit s opětovným posilováním ruského vlivu na úkor proevropského směřování.

Následná vlna protestů, známá jako Majdan, kulminovala v centru Kyjeva za účasti přibližně 200 000 demonstrantů, které v jejich úsilí podpořila i politická opozice. Významnou roli v protestním hnutí sehrála studentská obec, neboť dle dostupných dat se až 75 % studentů identifikovalo s vizí spolupráce s EU. Tato demografická skupina iniciovala rozsáhlé stávky na vysokých školách, které se následně rozšířily i do dalších měst, například do Charkova. Eskalace napětí vedla k nasazení pořádkových sil, které k potlačení demonstrací využívaly donucovací prostředky včetně slzného plynu a obušků. Poté, co bylo zřejmé, že k podpisu asociační dohody definitivně nedojde, se k protestům připojily také radikálnější skupiny, což vedlo k dalšímu zintenzivnění policejní agrese vůči davu. Politickým vyústěním této krize byl pád režimu Viktora Janukovyče, který byl následně obžalován z velezrady a uprchl z území Ukrajiny. Tato etapa dějin tak jasně

[43] SYRUČEK, Milan. *Rusko-ukrajinské vztahy: jak hluboké jsou kořeny současného konfliktu?* Aktualizované vydání. V Praze: Grada, 2023. ISBN 978-80-271-5221-6 s. 170-178

demonstrovala hluboký rozpor mezi aspiracemi většinové populace a politickou orientací tehdejších vládních špiček.[44]

5.8 Eskalace Politické krize

Leden roku 2014 představoval v kontextu probíhajících demonstrací zásadní zlom, neboť se stal obdobím první tragické eskalace s oběťmi na životech. Přestože ani s odstupem času není zcela objasněno, která ze zúčastněných stran iniciovala první výstřel, je prokazatelné, že se bezpečnostní složky udržující pořádek staly terčem palby z ručních zbraní. Tento incident měl za následek bezprostřední ztráty na životech a vysoký počet zraněných na obou stranách barikády.

V reakci na rozvíjející se ozbrojený střet byly státní složky následně vybaveny ostrou municí, což vedlo k dalšímu stupňování násilí. K nejintenzivnějším a nejtragičtějším bojům v centru Kyjeva došlo v následujícím měsíci, konkrétně v období mezi 18. a 21. únorem 2014. Tato vlna násilí si vyžádala celkem 75 obětí a téměř 600 osob bylo vážně zraněno. V mediálním prostoru, zejména v tom ovlivněném ruskou interpretací událostí, byli za hlavní viníky těchto krvavých střetů označováni stoupenci tzv. banderovců, kteří byli v tomto narativu často paušálně identifikováni jako fašistické živly. Tato etapa protestů tak definitivně transformovala původně poklidné demonstrace v otevřený vnitropolitický konflikt s mezinárodním přesahem.[45]

5.9 Využití Ukrajinské Krize Ruskou federací

Transformační procesy spojené s ukrajinskou revolucí byly charakterizovány značnou nestabilitou a střetem mocenských zájmů několika klíčových subjektů. Tato nepřehledná vnitropolitická situace vytvořila specifické prostředí, které Ruská federace dokázala strategicky využít ve svůj prospěch. Významným faktorem v této dynamice bylo působení tehdejšího proruského prezidenta Viktora Janukovyče. Jeho politické kroky a reakce na eskalaci napětí na Majdanu přispěly k prohloubení krize, čímž vznikl legitimizační rámec pro represivní opatření a tvrdý postup vůči vládní opozici. Tato vnitřní polarizace ukrajinské společnosti a oslabení státních institucí následně usnadnily vnější zásahy. Z geopolitického hlediska představoval tento chaos rozhodující příležitost pro Vladimira Putina. Pro ruské vedení se otevřela faktická cesta k realizaci strategických

[44] HLOUŠKOVÁ, Kateřina a MIKŠ, František (ed.). *Prokletí impéria a ruská lež: Rusko a Ukrajina v kontextu a Kontextech*. Brno: Books & Pipes, 2023. ISBN 978-80-7485-267-1. s.16-22
[45] GALEOTTI, Mark. *Putinovy války: od Čečenska po Ukrajinu*. Přeložil Alena BYRNE. V Praze: Bourdon, 2023. ISBN 978-80-7611-074-8. s. 165-173

cílů na ukrajinském území, přičemž destabilizace sousedního státu posloužila jako katalyzátor pro následnou ruskou intervenci a posílení vlivu v regionu. Ruská federace tak dokázala operativně reagovat na vnitrostátní rozvrat Ukrajiny a transformovat jej v nástroj pro prosazování vlastních zahraničněpolitických zájmů.[46]

5.10 Zásah Ruské federace na Ukrajině a hybridní konflikt v oblasti Donbasu

Vojenská operace Ruské federace na Krymu, která vyvrcholila anexí poloostrova 21. března 2014, vykazovala zásadní rozdíly oproti pozdější plnohodnotné invazi z roku 2022. Úspěch ruského postupu byl v roce 2014 usnadněn kritickým stavem ukrajinských ozbrojených sil, které se po revolučních událostech potýkaly s výraznou názorovou nejednotností, nedostatečným technickým vybavením a nízkou morálkou. Tato destabilizace, spolu se separatistickými tendencemi v jižních a východních částech země, vytvořila příznivé podmínky pro ruskou intervenci.

Strategickým prvkem operace bylo nasazení neoznačených příslušníků ozbrojených sil, v mediálním prostoru známých jako „zelení mužíčci“. Absence insignií na uniformách vyvolala v počáteční fázi zmatek a paralyzovala schopnost ukrajinské armády efektivně reagovat, dokud nebyla identita ruských vojáků potvrzena. Následný politický proces zahrnoval urychlené referendum o připojení k Rusku, které proběhlo pod přímým dohledem ruských sil, a bleskové uznání Krymu jako subjektu Ruské federace. Ukrajinské jednotky na poloostrově byly často vystaveny nátlaku k dezerci, přičemž významná část jich pod pohrůžkou násilí kapitulovala nebo přešla na stranu Ruska. Ačkoliv byla operace z vojenského hlediska pro Kreml překvapivě snadná, vyvolala mezinárodní sankce, které v kombinaci s poklesem cen ropy uvrhly Rusko do finanční krize. Bezprostředně po anexi Krymu se těžiště konfliktu přesunulo do oblasti Donbasu. Tento střet lze charakterizovat jako kombinaci vnitřního ozbrojeného konfliktu a zástupné ruské intervence. Ruská podpora separatistických struktur měla především finanční a personální charakter, přičemž klíčové velitelské posty byly obsazovány příslušníky ruské armády. Primárním strategickým cílem Moskvy nebylo přímé dobytí území, ale snaha o mocenské vymezení a udržení Ukrajiny v ruské sféře vlivu, což však ukrajinská strana odmítla akceptovat. Ruská propaganda v této fázi systematicky podněcovala nejistotu u ruskojazyčného obyvatelstva a delegitimizovala novou ukrajinskou vládu jejím

[46] BOREK, David; ČERNOHORSKÝ, Václav; JONÁŠ, Martin; KUBAL, Michal; MIŘEJOVSKÝ, David et al., SZÁNTÓ, Jakub (ed.). *Putinova válka: ukrajinská kronika zpravodajů ČT*. Edice ČT. Praha: Argo, 2023. ISBN 978-80-257-4046-0. s. 47-72

označováním za „fašistickou“. Eskalace násilí na obou stranách vedla k vysokému počtu obětí, a to i v řadách civilistů, čehož tragickým příkladem bylo sestřelení civilního dopravního letadla jednotkami pod velením ruského důstojníka Strelkova. Přímé zapojení ruských obrněných brigád do bojů proti ukrajinské armádě definitivně odhalilo roli Ruska jako aktivního účastníka konfliktu. Po období intenzivních bojů přešel konflikt do fáze opotřebovací války s nárazovými střety, která trvala až do února 2022, kdy Ruská federace zahájila otevřenou masivní invazi[47]

[47] MOKRYK, Radomyr a PADEVĚT, Jiří. *Hovory o Ukrajině*. Praha: Academia, 2023. ISBN 9788020034366 s. 120-135.

6 Praktická část bakalářské práce

Praktická část bakalářské práce navazuje na teoretická východiska uvedená v předchozích kapitolách a je zaměřena na empirické ověření poznatků prostřednictvím vlastního výzkumného šetření. Hlavním cílem praktické části bylo zjistit úroveň povědomí obyvatel České republiky o kybernetických a informačních hrozbách v souvislosti s rusko-ukrajinským konfliktem, posoudit jejich schopnost rozpoznat dezinformační obsah a analyzovat důvěru v jednotlivé informační zdroje. Současně bylo cílem identifikovat skupiny obyvatel, které mohou být dezinformačním působením ovlivněny ve větší míře, a na základě získaných výsledků formulovat návrhy opatření vedoucích ke zvýšení informační a kybernetické gramotnosti.

Za účelem získání relevantních dat bylo provedeno dotazníkové šetření mezi obyvateli České republiky. Výzkum byl realizován formou kvantitativního výzkumu, který umožňuje pracovat s číselně vyjádřitelnými údaji a jejich následným statistickým vyhodnocením. Získaná data sloužila k posouzení míry odolnosti české společnosti vůči dezinformačnímu působení a k identifikaci faktorů, které tuto odolnost ovlivňují. Praktická část práce se dále věnuje charakteristice respondentů, vyhodnocení jednotlivých otázek dotazníku, ověření stanovených hypotéz a interpretaci výsledků ve vztahu k bezpečnosti společnosti.

6.1 Metodika výzkumu

Pro zpracování praktické části bakalářské práce byla zvolena kvantitativní výzkumná strategie. Tento typ výzkumu umožňuje získat přehledná a statisticky zpracovatelná data a na jejich základě ověřit předem stanovené hypotézy. Cílem výzkumu bylo zjistit, jak obyvatelé České republiky vnímají kybernetické a informační hrozby související s rusko-ukrajinským konfliktem, jaká je jejich schopnost rozpoznat dezinformace, kterým informačním zdrojům důvěřují a jakým způsobem si informace ověřují.

Ke sběru dat bylo využito strukturované dotazníkové šetření. Dotazník obsahoval výhradně uzavřené otázky, které umožňují jednoznačné vyhodnocení a statistické zpracování výsledků. Otázky byly zaměřeny především na povědomí respondentů o aktuálních bezpečnostních hrozbách, jejich zkušenosti s dezinformacemi, důvěru v jednotlivé informační zdroje a jejich chování v online prostředí.

Dotazník byl vytvořen v online prostředí nástroje Google Forms a distribuován elektronickou formou. Odkaz na dotazník byl šířen především prostřednictvím sociálních sítí a přímého oslovení respondentů. V některých případech bylo respondentům umožněno vyplnění dotazníku s asistencí na mobilním zařízení, zejména u starších osob. Elektronická forma šetření byla zvolena z důvodu rychlé distribuce a možnosti oslovit širší skupinu respondentů napříč věkovými kategoriemi.

Dotazníkové šetření probíhalo v období od prosince 2025 do února 2026. Výzkumný soubor tvořili obyvatelé České republiky starší 15 let bez dalšího omezení. Celkem se výzkumu zúčastnilo 161 respondentů různého věku, pohlaví a dosaženého vzdělání.

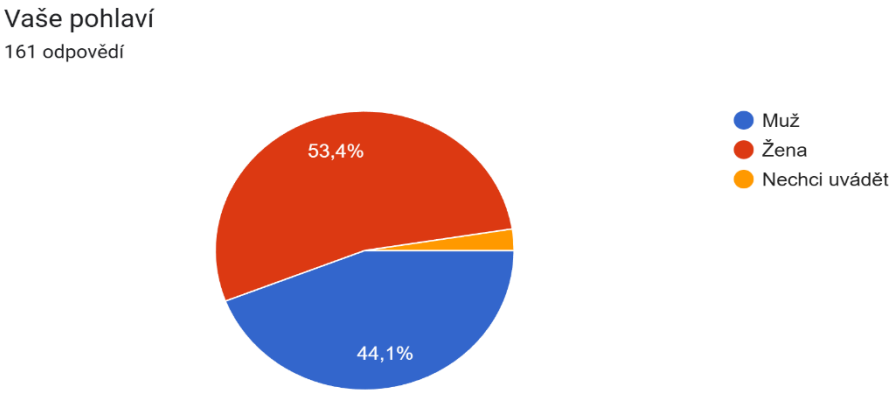
Získaná data byla následně exportována do tabulkového procesoru a vyhodnocena pomocí deskriptivní statistiky. Výsledky byly prezentovány prostřednictvím grafů a tabulek. Pro ověření stanovených hypotéz byly využity také křížové tabulky, které umožnily porovnat sociodemografické charakteristiky respondentů (zejména věk a vzdělání) s jejich schopností rozpoznat dezinformace, důvěrou v informační zdroje a chováním při ověřování informací.

6.2 Charakteristika respondentů

V této podkapitole je charakterizován výzkumný soubor respondentů, kteří se zúčastnili dotazníkového šetření. Struktura respondentů je analyzována podle pohlaví, věku a dosaženého vzdělání. Tyto údaje jsou důležité pro následnou interpretaci výsledků a umožňují identifikovat skupiny obyvatel, které mohou být více náchylné k dezinformačnímu působení.

1.Pohlaví respondentů

Výzkumného šetření se celkem zúčastnilo 161 respondentů. Z hlediska pohlaví převažovaly ženy, které tvořily 53,4 % (86 respondentů). Muži představovali 44,1 % (71 respondentů) a 2,5 % respondentů (4 osoby) nechtělo své pohlaví uvést.



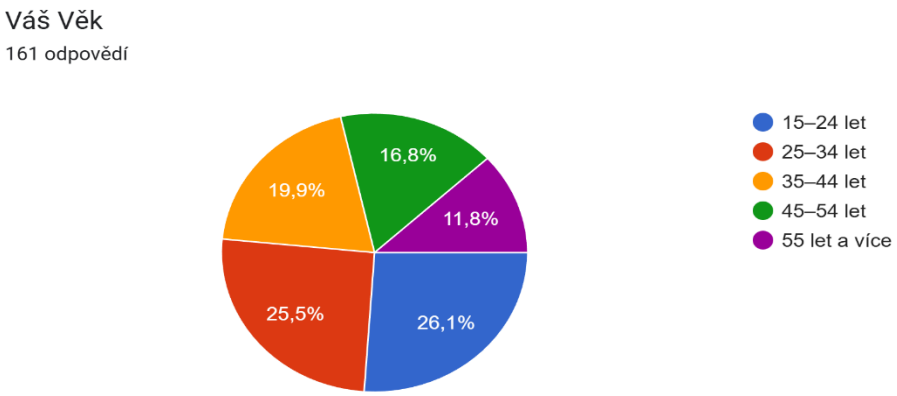
Graf 1: Struktura respondentů podle pohlaví[48]

Z výsledků vyplývá, že ve výzkumném souboru mírně převažují ženy. Rozdíl mezi zastoupením mužů a žen však není výrazný, a proto lze výzkumný soubor považovat za relativně vyvážený. Získaná data tak umožňují interpretovat výsledky dotazníku bez zásadního zkreslení z hlediska pohlaví respondentů.

[48] Vlastní zpracování

2.Věk respondentů

Největší zastoupení měli respondenti ve věku 15–24 let, kteří tvořili 26,1 % (42 respondentů). Podobně početná byla i skupina ve věku 25–34 let s podílem 25,5 % (41 respondentů). Ve věkové kategorii 35–44 let se nacházelo 19,9 % (32 respondentů), ve věku 45–54 let 16,8 % (27 respondentů) a respondenti ve věku 55 let a více tvořili 11,8 % (19 respondentů).



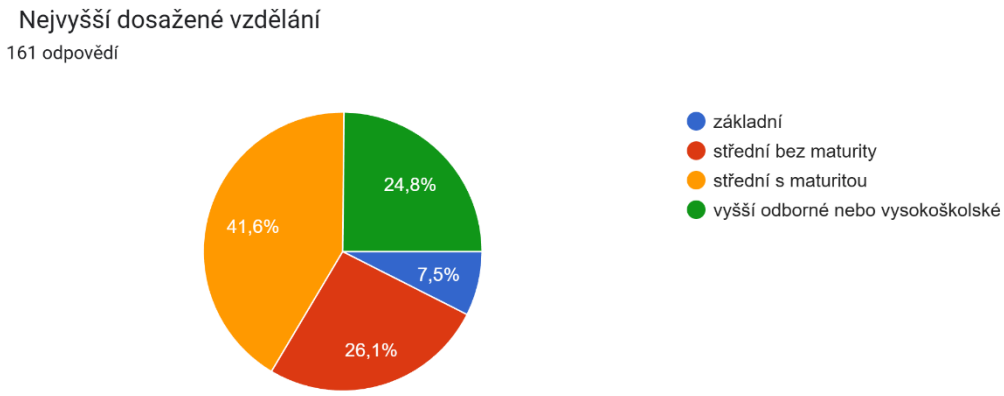
Graf 2: Struktura respondentů podle věku[49]

Z věkové struktury respondentů vyplývá, že nejvíce zastoupeni jsou mladší a střední věkové skupiny obyvatel. Nižší zastoupení starších respondentů je pravděpodobně ovlivněno elektronickou formou distribuce dotazníku, která je bližší především mladším uživatelům internetu. Přesto jsou ve výzkumném souboru zastoupeny všechny věkové kategorie, což umožňuje porovnávat jejich přístup k informacím a schopnost orientace v informačním prostoru.

[49] Vlastní zpracování

3.Nejvyšší dosažené vzdělání respondentů

Největší část respondentů tvořili lidé se středoškolským vzděláním s maturitou, a to 41,6 % (67 respondentů). Středoškolské vzdělání bez maturity uvedlo 26,1 % (42 respondentů). Vyšší odborné nebo vysokoškolské vzdělání mělo 24,8 % respondentů (40 osob) a základní vzdělání uvedlo 7,5 % (12 respondentů).



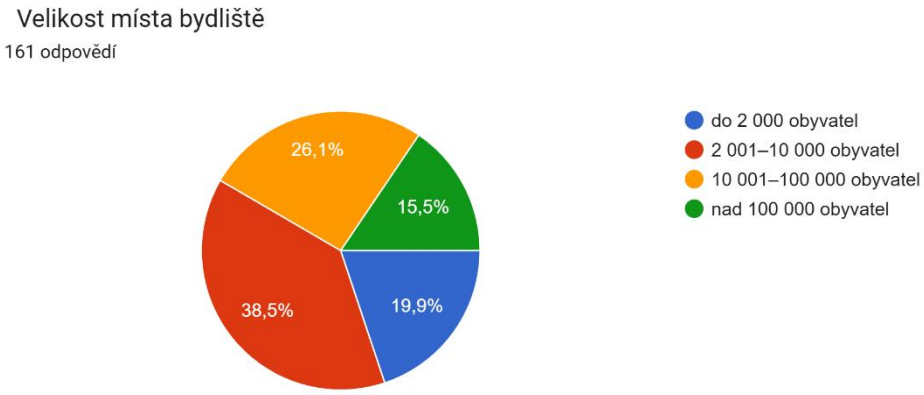
Graf 3: Struktura respondentů podle vzdělání[50]

Struktura vzdělání respondentů ukazuje, že většina dotazovaných dosáhla alespoň středoškolského vzdělání. Významné zastoupení osob s vyšším odborným nebo vysokoškolským vzděláním umožňuje posuzovat vztah mezi vzděláním a informační gramotností. Současně je ve výzkumném souboru zastoupena i skupina respondentů s nižším vzděláním, což je důležité pro následné ověření hypotézy o vlivu vzdělání na schopnost rozpoznat dezinformace.

[50] Vlastní zpracování

6.3 Vyhodnocení dotazníkového šetření

4.Velikost místa bydliště respondentů

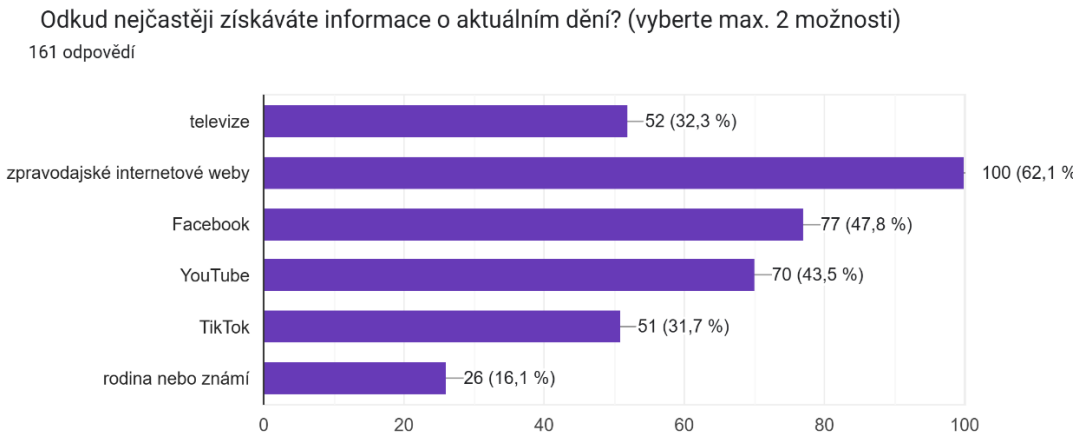


Graf 4: Struktura respondentů podle velikosti místa bydliště[51]

Z výsledků vyplývá, že respondenti pocházejí jak z menších obcí, tak i z větších měst, přičemž největší zastoupení tvoří obyvatelé od 2 001 do 10 000 obyvatel. Tato skutečnost je významná pro následnou interpretaci výsledků, protože informační prostředí se v závislosti na velikosti sídla výrazně liší. Obyvatelé větších měst mají obvykle širší přístup k různým mediálním zdrojům a vyšší dostupnost ověřených informací, zatímco v menších obcích může docházet k většímu šíření informací prostřednictvím sociálních sítí a neformálních komunikačních kanálů. Výsledky této otázky tak budou dále zohledněny při posuzování schopnosti respondentů rozpoznat dezinformační obsah a jejich důvěry v informační zdroje.

[51] Vlastní zpracování

5. Zdroje, ze kterých respondenti nejčastěji získávají informace o aktuálním dění



Graf 5: Zdroje informací o aktuálním dění[52]

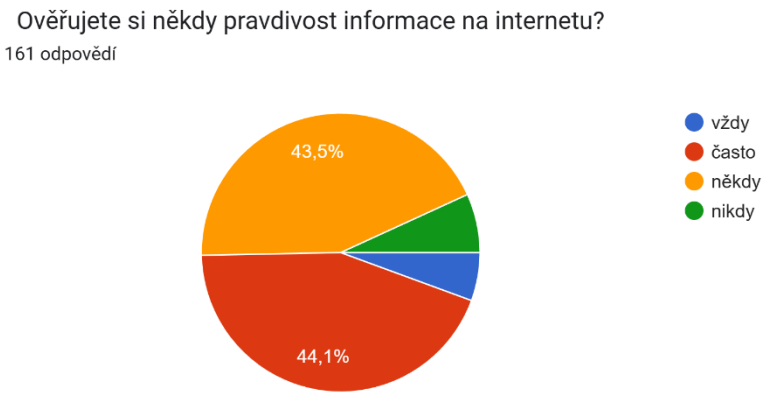
Z výsledků dotazníkového šetření vychází, že nejčastějším zdrojem informací respondentů jsou zpravodajské internetové weby, které uvedlo 62,1 % dotázaných. Významné zastoupení mají také sociální sítě, zejména Facebook (47,8 %) a YouTube (43,5 %), přičemž část respondentů využívá i platformu TikTok (31,7 %). Televizi jako zdroj informací označilo 32,3 % respondentů a informace od rodiny nebo známých uvedlo 16,1 % dotázaných.

Výsledky ukazují výrazný posun od tradičních médií k online prostředí. Zatímco klasická média, zejména televize, stále představují významný zdroj informací, převládající část respondentů získává informace prostřednictvím internetu a sociálních sítí. Právě sociální sítě však často neprocházejí redakční kontrolou a uživatelé jsou zde vystaveni většímu množství neověřených či manipulačních informací.

Tato skutečnost je důležitá pro posouzení náchylnosti respondentů k dezinformačnímu působení. Sociální sítě fungují na principu personalizovaného obsahu, který může vytvářet tzv. informační bubliny a posilovat jednostranné vnímání reality. Vysoký podíl respondentů využívajících tyto platformy proto může zvyšovat riziko šíření dezinformací a představuje významný faktor ovlivňující informační bezpečnost společnosti.

[52] Vlastní zpracování

6. Způsob ověřování pravdivosti informací na internetu mezi respondenty



Graf 6: Ověřování pravdivosti informací na internetu[53]

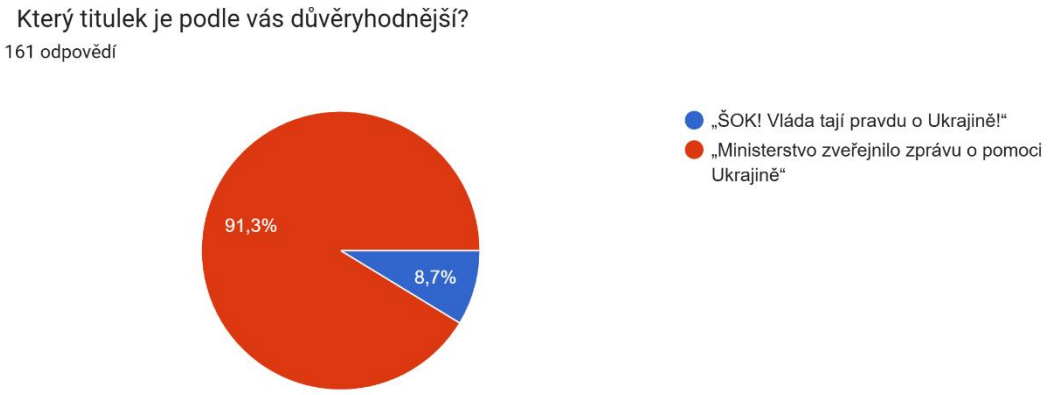
Z výsledků dotazníkového šetření vyplývá, že respondenti pravdivost informací na internetu ověřují v různé míře. Největší skupinu tvoří respondenti, kteří informace ověřují často (44,1 %), následovaní respondenty, kteří tak činí někdy (43,5 %). Informace vždy ověřuje pouze 5,6 % dotázaných, zatímco 6,8 % respondentů uvedlo, že pravdivost informací neověřují nikdy.

Výsledky ukazují, že ačkoli si většina respondentů uvědomuje potřebu ověřování informací, pravidelné a systematické ověřování není běžné. Pouze velmi malá část respondentů si informace ověřuje vždy, což naznačuje, že kritické hodnocení obsahu není u většiny uživatelů internetu samozřejmostí. Velká část respondentů kontroluje informace pouze příležitostně, což může vést k nekritickému přebírání neověřeného obsahu.

Nedostatečné ověřování informací představuje významný faktor zvyšující zranitelnost vůči dezinformacím, zejména v online prostředí. Dezinformační obsah je často šířen rychle a spoléhá na to, že uživatelé informace nepodrobí kontrole. Zjištěné výsledky tak naznačují, že úroveň informační gramotnosti respondentů není zcela dostatečná a část populace může být náchylná k manipulativnímu nebo nepravdivému obsahu.

[53] Vlastní zpracování

7. Schopnost respondentů posoudit důvěryhodnost mediálních sdělení byla testována prostřednictvím výběru z dvojice titulků



Graf 7: Posouzení důvěryhodnosti mediálních titulků[54]

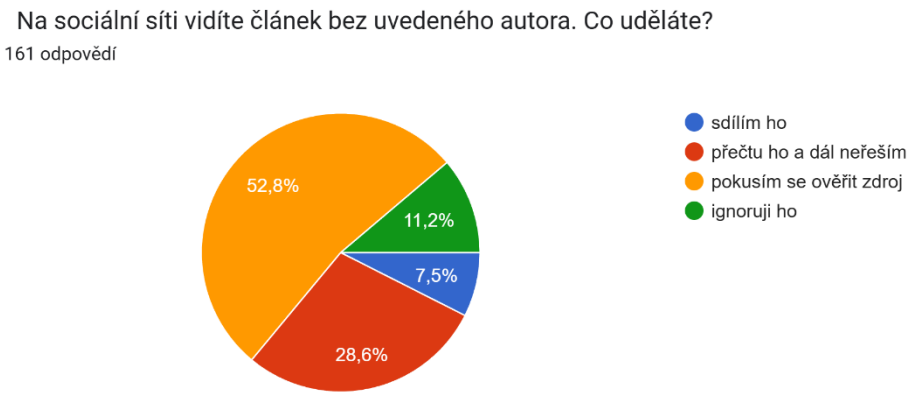
Respondenti měli vybrat titulek, který považují za důvěryhodnější. Většina respondentů (91,3 %) označila jako důvěryhodnější titulek „Ministerstvo zveřejnilo zprávu o pomoci Ukrajině“, zatímco pouze 8,7 % dotázaných považovalo za důvěryhodnější titulek „ŠOK! Vláda tají pravdu o Ukrajině!“.

Výsledky ukazují, že převážná část respondentů je schopna rozpoznat znaky manipulativního sdělení. Dezinformační titulky často využívají emotivní jazyk, výrazné formulace a snahu vyvolat negativní emoce nebo pobouření, zatímco důvěryhodné zpravodajství je charakteristické spíše věcným a neutrálním stylem sdělení.

Přestože většina respondentů zvolila správnou možnost, existence skupiny respondentů, která označila manipulativní titulek za důvěryhodnější, představuje bezpečnostní riziko. Tito jedinci mohou být náchylnější k dezinformačnímu působení a šíření nepravdivého obsahu v online prostředí. Výsledky tak potvrzují, že část společnosti zůstává vůči informačním manipulacím zranitelná.

[54] Vlastní zpracování

8. Reakce respondentů na článek bez uvedeného autora zveřejněný na sociální síti



Graf 8: Reakce na článek bez uvedeného autora na sociální síti[55]

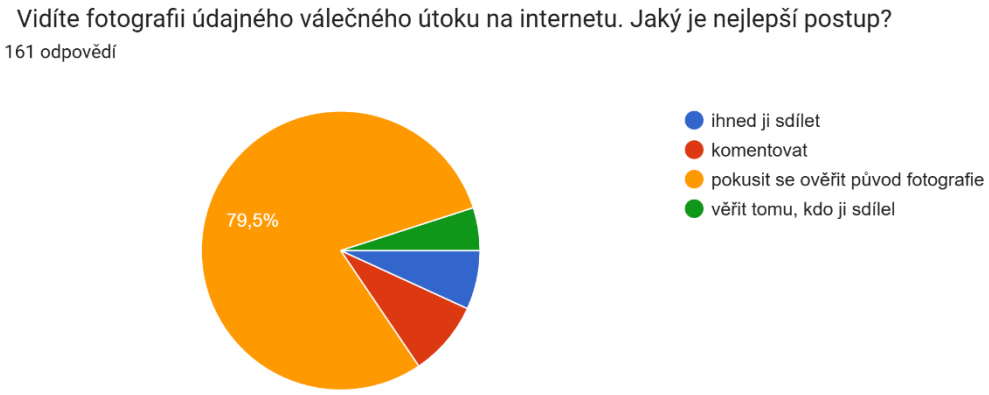
Respondenti byli dotázáni, jak by reagovali na článek zveřejněný na sociální síti bez uvedeného autora. Více než polovina respondentů (52,8 %) uvedla, že by se pokusila ověřit zdroj informace. Dalších 28,6 % respondentů by si článek pouze přečetlo a dále jej neřešilo. Menší část dotázaných by článek ignorovala (11,2 %) a 7,5 % respondentů by jej dokonce sdílelo.

Výsledky ukazují, že značná část respondentů si uvědomuje možná rizika nedůvěryhodného obsahu a snaží se informace ověřit. Na druhou stranu téměř třetina respondentů by se obsahem dále nezabývala a část by jej dokonce sdílela, aniž by znala jeho původ. Takové jednání může významně přispívat k dalšímu šíření dezinformací v online prostředí.

Absence uvedeného autora je přitom jedním z typických znaků nedůvěryhodného nebo manipulativního obsahu. Zjištěné výsledky proto naznačují, že přestože část respondentů vykazuje kritický přístup k informacím, významná skupina uživatelů internetu stále nepřistupuje k online obsahu dostatečně obezřetně, což zvyšuje zranitelnost společnosti vůči dezinformačním kampaním.

[55] Vlastní zpracování

9. Postup respondentů při setkání s fotografií údajného válečného útoku na internetu



Graf 9: Reakce na fotografii údajného válečného útoku na internetu[56]

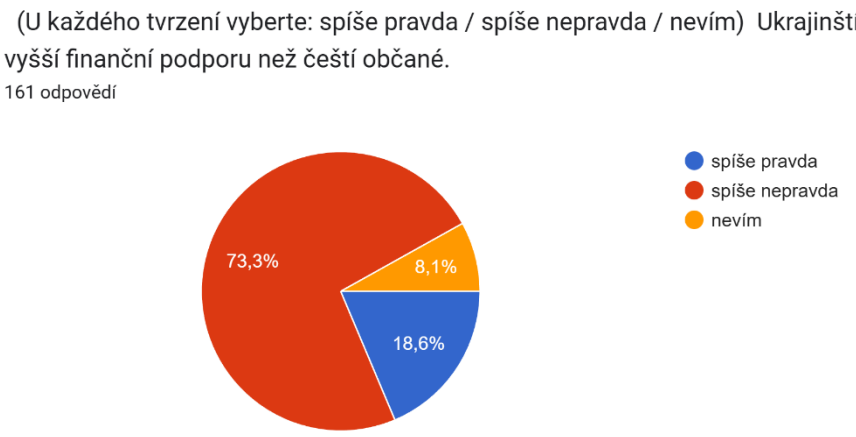
Respondenti byli dotázáni, jaký postup by zvolili v případě, že by na internetu viděli fotografii údajného válečného útoku. Největší část respondentů (79,5 %) uvedla, že by se pokusila ověřit původ fotografie. Naproti tomu 8,7 % respondentů by fotografii komentovalo, 6,8 % dotázaných by ji ihned sdílelo a 5 % respondentů by věřilo osobě, která fotografii zveřejnila.

Výsledky naznačují relativně dobrou míru kritického přístupu k obrazovému obsahu, jelikož většina respondentů deklaruje snahu o ověření pravosti fotografie. Přesto však zůstává část respondentů, která by obsah dále šířila nebo mu bez ověření důvěřovala. Takové jednání může významně přispívat k rychlému šíření manipulativního nebo nepravdivého obsahu.

Obrazový materiál přitom patří mezi nejúčinnější nástroje informační manipulace, protože působí emotivněji než text a uživatelé jej často považují za důkaz skutečné události. Zneužití starých nebo upravených fotografií je častou součástí dezinformačních kampaní souvisejících s ozbrojenými konflikty. Zjištěné výsledky proto ukazují, že přestože většina respondentů vykazuje kritické uvažování, část populace zůstává vůči vizuálním dezinformacím zranitelná.

[56] Vlastní zpracování

10. Názor respondentů na tvrzení týkající se finanční podpory ukrajinských uprchlíků



Graf 10: Posouzení tvrzení o finanční podpoře ukrajinských uprchlíků[57]

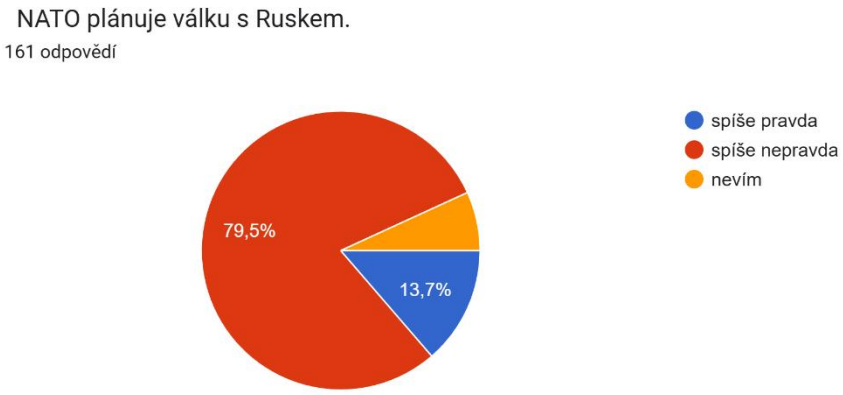
Respondenti hodnotili pravdivost tvrzení, že ukrajinští uprchlíci dostávají vyšší finanční podporu než čeští občané. Většina respondentů (73,3 %) označila toto tvrzení jako spíše nepravdivé. Naopak 18,6 % dotázaných jej považovalo za spíše pravdivé a 8,1 % respondentů uvedlo, že nedokáže posoudit jeho pravdivost.

Výsledky ukazují, že převážná část respondentů dokáže rozpoznat nepravdivé nebo manipulativní tvrzení. Přesto však téměř pětina respondentů tomuto sdělení věří, což představuje významný prostor pro působení dezinformačních kampaní. Podobná tvrzení jsou často využívána k vyvolávání negativních emocí, zejména pocitu nespravedlnosti a sociálního napětí ve společnosti.

Skutečnost, že část respondentů nedokáže pravdivost tvrzení posoudit, zároveň naznačuje nedostatek informací nebo nejistotu při orientaci v problematice. Výsledky tak potvrzují, že i přes relativně dobrou informovanost části populace zůstává určité procento obyvatel vůči dezinformačním narativům zranitelné.

[57] Vlastní zpracování

11. Názor respondentů na tvrzení týkající se role NATO v rusko-ukrajinském konfliktu



Graf 11: Posouzení tvrzení „NATO plánuje válku s Ruskem"[58]

Respondenti hodnotili pravdivost tvrzení, že NATO plánuje válku s Ruskem. Většina respondentů (79,5 %) označila toto tvrzení jako spíše nepravdivé. Naopak 13,7 % dotázaných jej považovalo za spíše pravdivé a zbývající část respondentů uvedla, že nedokáže pravdivost tvrzení posoudit.

Výsledky naznačují, že převážná část respondentů je schopna identifikovat nepravdivý nebo manipulativní obsah. Přesto však více než desetina respondentů tomuto tvrzení věří, což představuje významný bezpečnostní aspekt. Podobná sdělení jsou typickým prvkem dezinformačních kampaní, jejichž cílem je vyvolat nedůvěru k mezinárodním institucím a zpochybnit bezpečnostní spolupráci států.

Skutečnost, že část respondentů není schopna pravdivost tvrzení posoudit, zároveň poukazuje na nejistotu v oblasti bezpečnostní problematiky. Výsledky proto ukazují, že i přes relativně dobrou orientaci většiny populace zůstává určitá část společnosti náchylná k dezinformačnímu působení, což může mít dopad na vnímání bezpečnosti státu i jeho zahraničně-politické orientace.

[58] Vlastní zpracování

12. Názor respondentů na tvrzení o záměrném utajování informací o válce

Graf 12: Posouzení tvrzení „Většina informací o válce je veřejnosti záměrně tajena"[59]

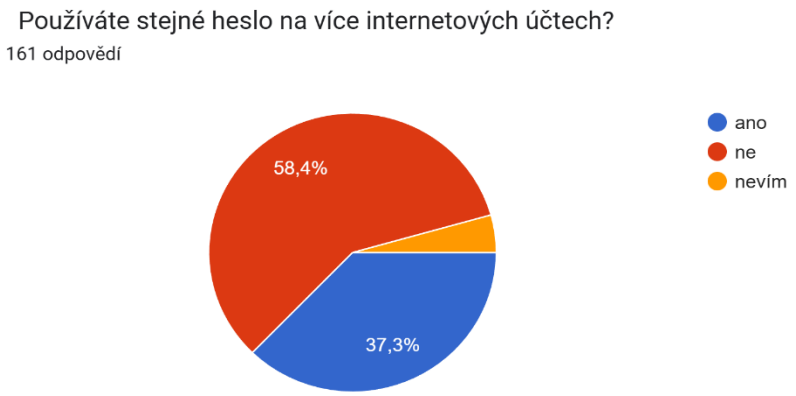
Respondenti hodnotili pravdivost tvrzení, že většina informací o válce je veřejnosti záměrně tajena. Většina respondentů (68,9 %) označila toto tvrzení jako spíše nepravdivé. Naopak 19,3 % dotázaných jej považovalo za spíše pravdivé a 11,8 % respondentů uvedlo, že nedokáže pravdivost tvrzení posoudit.

Výsledky ukazují, že přestože převládá nedůvěra k tomuto tvrzení, přibližně pětina respondentů věří, že jsou informace o konfliktu veřejnosti záměrně zatajovány. Takový postoj je charakteristický pro konspirační narativy, které zpochybňují důvěryhodnost médií, státních institucí a oficiálních zdrojů informací.

Víra v podobná tvrzení může snižovat důvěru ve veřejné instituce a zároveň zvyšovat náchylnost k přijímání alternativních či neověřených zdrojů informací. Zjištěné výsledky proto naznačují, že část společnosti je ovlivnitelná konspiračními interpretacemi událostí, což představuje významný faktor v oblasti informační bezpečnosti státu.

[59] Vlastní zpracování

13. Způsob nakládání respondentů s hesly k internetovým účtům



Graf 13: Používání stejného hesla na více internetových účtech[60]

Respondenti byli dotázáni, zda používají stejné heslo na více internetových účtech. Více než polovina respondentů (58,4 %) uvedla, že stejné heslo nepoužívá. Naopak 37,3 % dotázaných přiznalo, že stejné heslo používá a 4,3 % respondentů nedokázalo na otázku odpovědět.

Výsledky ukazují, že přestože si část respondentů uvědomuje základní zásady kybernetické bezpečnosti, stále významná skupina uživatelů používá stejné heslo pro více služeb. Takové jednání představuje bezpečnostní riziko, protože v případě prolomení jednoho účtu může dojít ke kompromitaci dalších účtů, včetně sociálních sítí nebo e-mailu.

Zneužití účtů na sociálních sítích přitom může vést nejen k finančním škodám, ale také k šíření dezinformací nebo podvodných zpráv jménem napadeného uživatele. Výsledky proto ukazují, že kybernetická bezpečnost uživatelů úzce souvisí s informační bezpečností a může ovlivňovat šíření manipulativního obsahu v online prostředí.

[60] Vlastní zpracování

14. Zkušenost respondentů s podezřelými e-maily nebo odkazy

Graf 14: Kliknutí na podezřelý e-mail nebo odkaz[61]

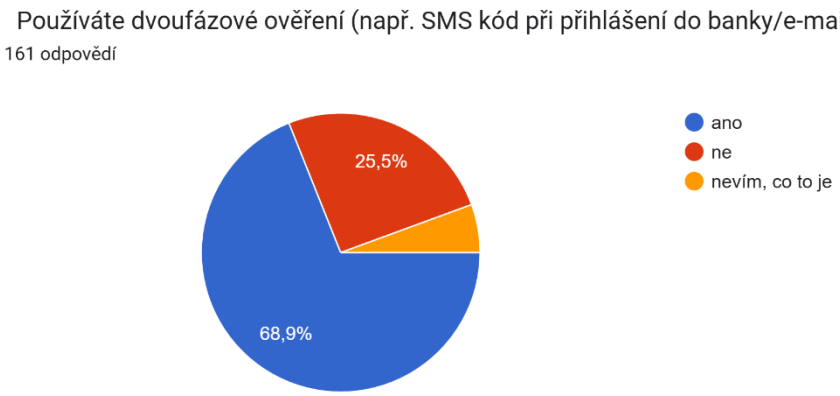
Respondenti byli dotázáni, zda někdy klikli na podezřelý e-mail nebo odkaz. Více než třetina respondentů (35,4 %) uvedla, že takovou zkušenost má. Naopak 47,8 % dotázaných odpovědělo, že na podezřelý odkaz nikdy nekliklo, a 16,8 % respondentů si nebylo jistých.

Výsledky ukazují, že významná část uživatelů internetu se již setkala s phishingovým útokem nebo na něj reagovala. Skutečnost, že více než třetina respondentů na podezřelý odkaz klikla, představuje významné bezpečnostní riziko. Phishingové útoky jsou přitom jednou z nejčastějších forem kybernetické kriminality a často slouží k získání přístupových údajů nebo k napadení uživatelských účtů.

Kompromitace účtů může následně vést nejen k finančním škodám, ale také k šíření podvodných zpráv a dezinformací jménem napadeného uživatele. Výsledky proto potvrzují, že nízká úroveň kybernetické opatrnosti části uživatelů může nepřímo přispívat k šíření manipulativního obsahu v online prostředí.

[61] Vlastní zpracování

15. Využívání dvoufázového ověření při přihlašování k internetovým službám



Graf 15: Používání dvoufázového ověření[62]

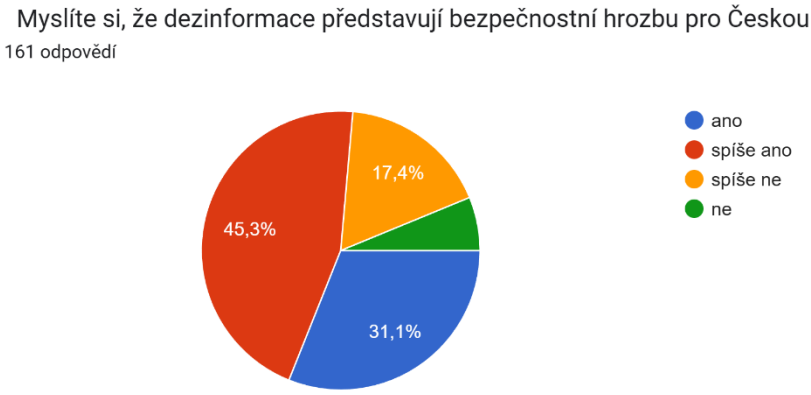
Respondenti byli dotázáni, zda používají dvoufázové ověření při přihlašování k internetovým účtům. Většina respondentů (68,9 %) uvedla, že tuto formu zabezpečení používá. Naopak 25,5 % dotázaných dvoufázové ověření nepoužívá a 5,6 % respondentů uvedlo, že neví, co tento pojem znamená.

Výsledky ukazují, že značná část uživatelů si uvědomuje význam zabezpečení svých účtů a využívá pokročilejší ochranné prvky. Přesto však přibližně čtvrtina respondentů tuto možnost nevyužívá a část populace nemá o této metodě zabezpečení dostatečné povědomí.

Dvoufázové ověření přitom významně snižuje riziko neoprávněného přístupu k účtům i v případě, že dojde k úniku nebo odcizení hesla. Jeho nevyužívání proto představuje bezpečnostní slabinu, která může vést k napadení účtů a následnému zneužití identity uživatele, například k šíření podvodných zpráv nebo dezinformací. Výsledky tak potvrzují, že úroveň kybernetické ochrany uživatelů není jednotná a část populace zůstává vůči kybernetickým hrozbám zranitelná.

[62] Vlastní zpracování

16. Názor respondentů na to, zda dezinformace představují bezpečnostní hrozbu pro Českou republiku



Graf 16: Vnímání dezinformací jako bezpečnostní hrozby[63]

Respondenti byli dotázáni, zda podle jejich názoru představují dezinformace bezpečnostní hrozbu pro Českou republiku. Více než tři čtvrtiny respondentů uvedly kladnou odpověď, přičemž 31,1 % zvolilo možnost „ano“ a 45,3 % možnost „spíše ano“. Naopak 17,4 % respondentů se přiklonilo k odpovědi „spíše ne“ a 6,2 % dotázaných uvedlo, že dezinformace za bezpečnostní hrozbu nepovažuje.

Výsledky ukazují, že většina respondentů si uvědomuje existenci informačních hrozeb a jejich možný dopad na bezpečnost státu. Přesto však část populace nepovažuje dezinformace za významný problém, což může vést k podceňování jejich dopadů a k nižší opatrnosti při práci s informacemi.

Uvědomění si hrozby je přitom důležitým předpokladem pro obranyschopnost společnosti vůči informačním operacím. Pokud část veřejnosti nepovažuje dezinformace za riziko, může být náchylnější k manipulativnímu obsahu a jeho dalšímu šíření. Zjištěné výsledky tak potvrzují, že problematika dezinformací je veřejností vnímána, avšak míra uvědomění není jednotná.

[63] Vlastní zpracování

6.4 Ověření hypotéz

Hypotéza H1

H1: Mladší respondenti vykazují vyšší schopnost rozpoznat dezinformaci než starší respondenti.

Schopnost rozpoznat dezinformační obsah byla posuzována především na základě otázky zaměřené na výběr důvěryhodnějšího mediálního titulku a hodnocení pravdivosti vybraných tvrzení souvisejících s rusko-ukrajinským konfliktem. Výsledky ukázaly, že většina respondentů dokázala identifikovat manipulativní sdělení a označila neutrálně formulovaný titulek za důvěryhodnější.

Dotazníkové šetření však neprokázalo výrazné rozdíly mezi věkovými kategoriemi respondentů, jelikož správné odpovědi se objevovaly napříč všemi věkovými skupinami. Na základě dostupných dat tedy nelze jednoznačně potvrdit, že by mladší respondenti vykazovali významně vyšší schopnost rozpoznat dezinformace než respondenti starší.

Hypotéza H1 nebyla jednoznačně potvrzena.

Hypotéza H2

H2: Respondenti s vyšším dosaženým vzděláním mají vyšší úroveň informační gramotnosti než respondenti s nižším vzděláním.

Úroveň informační gramotnosti byla posuzována zejména podle ověřování informací, schopnosti rozpoznat manipulativní titulky a reakce na nedůvěryhodný obsah na sociálních sítích. Výsledky ukázaly, že většina respondentů se snaží informace ověřovat a rozpoznat manipulativní sdělení, přičemž část respondentů naopak vykazovala nejistotu nebo věřila nepravdivým tvrzením.

Vzhledem k tomu, že dotazník neprokázal zásadní rozdíly v odpovědích mezi jednotlivými vzdělanostními skupinami a správné i nesprávné odpovědi se vyskytovaly napříč vzděláním respondentů, nelze s jistotou tvrdit, že vyšší vzdělání automaticky znamená vyšší informační gramotnost.

Hypotéza H2 nebyla potvrzena.

Hypotéza H3

H3: Respondenti více důvěřují tradičním médiím (televize, tisk, zpravodajské portály) než informacím získaným ze sociálních sítí.

Z otázky zaměřené na zdroje informací vyplynulo, že nejčastějším zdrojem informací respondentů jsou zpravodajské internetové portály a televize. Přesto významná část respondentů využívá sociální sítě, zejména Facebook a YouTube, jako jeden z hlavních zdrojů informací o aktuálním dění.

Výsledky ukazují, že tradiční média stále představují důležitý zdroj informací, avšak sociální sítě jsou využívány téměř stejně často a mají významný vliv na informační prostředí respondentů.

Hypotéza H3 byla potvrzena pouze částečně.

Hypotéza H4

H4: Respondenti, kteří aktivně ověřují informace z více zdrojů, vykazují vyšší povědomí o kybernetických a informačních hrozbách.

Výsledky ukázaly, že respondenti, kteří uváděli časté ověřování informací, zároveň ve větší míře považovali dezinformace za bezpečnostní hrozbu a častěji volili správné postupy při setkání s nedůvěryhodným obsahem (ověření zdroje, nešíření neověřených informací).

Naopak respondenti, kteří informace neověřovali nebo si jejich pravdivost kontrolovali jen výjimečně, častěji vykazovali nejistotu v posuzování tvrzení nebo byli náchylnější k jejich přijetí.

Hypotéza H4 byla potvrzena.

6.5 Diskuze výsledků

Cílem výzkumného šetření bylo zjistit úroveň povědomí obyvatel České republiky o kybernetických a informačních hrozbách v souvislosti s rusko-ukrajinským konfliktem a posoudit jejich schopnost orientace v informačním prostoru. Na základě získaných výsledků lze konstatovat, že respondenti vykazují relativně dobrou schopnost rozpoznat zjevně manipulativní sdělení, avšak jejich odolnost vůči dezinformacím není jednotná.

Výsledky ukázaly, že část respondentů stále věří některým nepravdivým tvrzením nebo není schopna jejich pravdivost posoudit. To potvrzuje, že dezinformace nepůsobí pouze na osoby s nízkou informovaností, ale mohou ovlivňovat široké spektrum populace. Zvláště významným faktorem se ukázala míra aktivního ověřování informací. Respondenti, kteří si informace pravidelně ověřují, vykazovali vyšší schopnost rozpoznat manipulativní obsah a častěji považovali dezinformace za bezpečnostní hrozbu.

Vliv sociálních sítí

Významnou roli sehrávají sociální sítě, které patří mezi hlavní zdroje informací respondentů. Přestože tradiční média zůstávají důležitým informačním kanálem, velká část respondentů získává informace prostřednictvím Facebooku, YouTube nebo TikToku. Sociální sítě přitom umožňují rychlé šíření neověřeného obsahu a vytvářejí tzv. informační bubliny, kdy je uživateli zobrazován převážně obsah odpovídající jeho názorům. Tím může docházet k posilování jednostranného vnímání reality a ke snížení schopnosti kritického hodnocení informací.

Mediální a informační gramotnost

Výzkum rovněž ukázal, že mediální gramotnost společnosti není jednotná. Přestože většina respondentů deklarovala snahu ověřovat informace, pravidelné a systematické ověřování provádí pouze menší část z nich. Část respondentů také přiznala sdílení neověřeného obsahu nebo kliknutí na podezřelý odkaz. To naznačuje, že teoretické povědomí o rizicích neodpovídá vždy skutečnému chování uživatelů v online prostředí.

Významným zjištěním je rovněž skutečnost, že kybernetická bezpečnost a informační bezpečnost spolu úzce souvisejí. Například používání stejného hesla nebo kliknutí na phishingový odkaz může vést k napadení účtu a jeho následnému zneužití k šíření dezinformací.

Vztah k válce na Ukrajině

V otázkách souvisejících s rusko-ukrajinským konfliktem většina respondentů správně identifikovala nepravdivá tvrzení. Přesto však přibližně pětina respondentů některým dezinformačním narativům věřila nebo si nebyla jistá jejich pravdivostí. Tyto výsledky ukazují, že informační operace zaměřené na vyvolání nedůvěry vůči institucím nebo spojencům mohou mít na část společnosti reálný dopad.

Zároveň většina respondentů považuje dezinformace za bezpečnostní hrozbu pro Českou republiku, což ukazuje na rostoucí povědomí veřejnosti o problematice informační války. Skutečnost, že část populace tuto hrozbu nepovažuje za významnou, však může snižovat celkovou odolnost společnosti.

6.6 Návrh opatření

Informační materiály distribuované domácnostem

Dalším vhodným opatřením je rozšíření osvětové činnosti prostřednictvím tištěných informačních materiálů distribuovaných přímo do domácností. Národní úřad pro kybernetickou a informační bezpečnost by mohl v pravidelných intervalech rozesílat stručné informační příručky nebo letáky zaměřené na základní pravidla bezpečného chování na internetu.

Tyto materiály by měly obsahovat především praktické rady, například jak rozpoznat phishingový e-mail, jak vytvářet bezpečná hesla, jak ověřovat informace na sociálních sítích nebo jak postupovat v případě kybernetického incidentu. Forma materiálu by měla být přehledná, stručná a srozumitelná i pro uživatele s nižší digitální gramotností.

Výhodou tohoto opatření je jeho dostupnost pro všechny věkové skupiny obyvatel, včetně osob, které aktivně nevyužívají internet. Současně se jedná o relativně nenákladný způsob prevence, který může přispět ke zvýšení povědomí o kybernetických a informačních hrozbách a ke snížení počtu úspěšných podvodných útoků.

Využití televizního vysílání pro informování starší populace

Pro starší věkové skupiny obyvatel, které internet nevyužívají pravidelně nebo jej využívají omezeně, může být nejdostupnějším zdrojem informací televizní vysílání. Vhodným opatřením by proto bylo zařazení pravidelného edukativního pořadu zaměřeného na kybernetickou bezpečnost a dezinformace do vysílání veřejnoprávní televize, například Česká televize.

Takový pořad by měl srozumitelnou formou vysvětlovat principy dezinformačních kampaní, upozorňovat na typické internetové podvody (např. phishing) a poskytovat praktické rady pro bezpečné používání digitálních technologií. Pravidelná informovanost by mohla přispět ke snížení zranitelnosti starší populace, která bývá častým cílem manipulativních sdělení a podvodných praktik.

Mediální a informační vzdělávání na středních odborných školách

Výsledky výzkumu ukázaly, že úroveň mediální a informační gramotnosti není u respondentů jednotná a část z nich má potíže s rozpoznáním manipulativního obsahu. Zvláštní pozornost je proto vhodné věnovat studentům středních odborných škol, které často neobsahují systematickou výuku mediální gramotnosti nebo ji zahrnují pouze okrajově.

Doporučit lze zavedení pravidelných kurzů zaměřených na kybernetickou a informační bezpečnost, a to například formou samostatného předmětu, semináře nebo blokové výuky. Obsah výuky by měl zahrnovat především rozpoznávání dezinformací, práci s informačními zdroji, zásady bezpečného chování na internetu a základní ochranu osobních údajů. Cílem těchto opatření je rozvoj kritického myšlení studentů a zvýšení jejich odolnosti vůči manipulativním sdělením v online prostředí.

Centrální státní portál pro ověřování informací

Jedním z problémů identifikovaných ve výzkumu je skutečnost, že respondenti často nevědí, kde si mohou pravdivost informace rychle ověřit. Vhodným opatřením by proto bylo vytvoření centrálního státního informačního portálu, který by sloužil jako oficiální zdroj pro ověřování aktuálně šířených dezinformací.

Tento portál by měl jednoduchou a přehlednou strukturu a obsahoval by zejména stručná vysvětlení aktuálních virálních tvrzení, krátké grafiky a srozumitelné shrnutí ověřených informací. Obsah by měl být formulován tak, aby byl pochopitelný i pro uživatele bez odborných znalostí. Významným prvkem by byla možnost snadného sdílení informací na sociálních sítích, čímž by bylo možné rychle reagovat na šíření nepravdivého obsahu.

Takové opatření by mohlo snížit nejistotu uživatelů a zároveň omezit prostor pro šíření manipulativních sdělení v krizových situacích.

Mezigenerační vzdělávání v oblasti informační bezpečnosti

Jedním z možných preventivních opatření je využití mezigeneračního přenosu informací v oblasti kybernetické a informační gramotnosti. Školy by mohly do výuky zařazovat praktické úkoly, v jejichž rámci by žáci seznamovali své rodiče nebo prarodiče se základními principy bezpečného chování na internetu. Konkrétně by mohlo jít například

o vysvětlení, jak rozpoznat dezinformační sdělení, manipulativní titulek, podvodný e-mail nebo phishingovou zprávu.

Toto opatření vychází z předpokladu, že starší generace často přijímá informace od státních institucí s určitou nedůvěrou, zatímco informace získané od rodinných příslušníků vnímá jako důvěryhodnější. Rodinné prostředí je založeno na vzájemné důvěře a přirozené komunikaci, což může významně zvýšit ochotu starších osob přijmout doporučené postupy bezpečného chování.

Výhodou tohoto opatření je zároveň jeho nízká finanční náročnost. Škola plní vzdělávací roli vůči žákům a ti následně přenášejí získané poznatky do rodinného prostředí. Dochází tak k nepřímému vzdělávání širší populace, aniž by bylo nutné organizovat rozsáhlé veřejné kampaně. Mezigenerační výuka může přispět ke zvýšení odolnosti společnosti vůči dezinformacím i kybernetickým podvodům a současně posiluje obecné povědomí o bezpečném využívání digitálních technologií.

Bezpečnostní upozornění v internetovém bankovnictví

Výzkum ukázal, že část respondentů klikla na podezřelý odkaz nebo e-mail, což ukazuje na zranitelnost uživatelů vůči phishingovým útokům. Vhodným preventivním opatřením by proto byla spolupráce státu a bankovních institucí.

Internetové bankovnictví patří mezi digitální služby, kterým uživatelé důvěřují a pravidelně je využívají. Bankovní aplikace by mohly zobrazovat krátká bezpečnostní upozornění upozorňující na aktuální podvody, například falešné zprávy o balíkových zásilkách, vydávání se za banku nebo podvodné investiční nabídky. Informace by byly stručné, srozumitelné a zaměřené na praktické rady.

Tímto způsobem by bylo možné oslovit široké spektrum uživatelů, včetně starší populace, která běžně nereaguje na informační kampaně vedené pouze prostřednictvím internetu.

6.7 Shrnutí praktické části

Praktická část bakalářské práce byla zaměřena na zjištění úrovně povědomí obyvatel České republiky o kybernetických a informačních hrozbách v souvislosti s rusko-ukrajinským konfliktem. Výzkum byl realizován formou kvantitativního dotazníkového šetření, kterého se zúčastnilo 161 respondentů. Dotazník se zaměřoval zejména na zdroje informací respondentů, jejich schopnost rozpoznat dezinformační obsah, přístup k ověřování informací a úroveň kybernetické bezpečnosti při používání internetu.

Výsledky ukázaly, že většina respondentů dokáže rozpoznat zjevně manipulativní sdělení, například emotivně formulované titulky nebo nepravdivá tvrzení. Přesto však část respondentů některým dezinformačním narativům věří nebo si jejich pravdivostí není jistá. To naznačuje, že schopnost rozpoznat dezinformace není u populace jednotná a že i relativně informovaní uživatelé mohou být manipulativním obsahem ovlivněni.

Za jeden z nejdůležitějších faktorů se ukázal přístup k ověřování informací. Respondenti, kteří uváděli pravidelné ověřování informací z více zdrojů, vykazovali vyšší schopnost identifikovat manipulativní obsah a častěji považovali dezinformace za bezpečnostní hrozbu. Naopak osoby, které informace ověřují pouze příležitostně nebo vůbec, vykazovaly větší nejistotu při posuzování pravdivosti tvrzení.

Významnou roli v informačním prostředí respondentů hrají sociální sítě. Ačkoliv tradiční média, zejména zpravodajské portály a televize, zůstávají důležitým zdrojem informací, velká část respondentů získává informace také prostřednictvím sociálních sítí, jako jsou Facebook, YouTube nebo TikTok. Tyto platformy umožňují rychlé šíření neověřeného obsahu a mohou přispívat k vytváření informačních bublin, ve kterých uživatelé přicházejí do kontaktu především s názory odpovídajícími jejich přesvědčení.

Výzkum dále ukázal, že část respondentů reaguje na nedůvěryhodný obsah pasivně nebo jej dokonce sdílí bez ověření zdroje. Přestože většina respondentů deklarovala snahu informace ověřit, menší skupina by obsah bez uvedeného autora komentovala nebo sdílela. Takové jednání může přispívat k dalšímu šíření dezinformací v online prostředí.

V oblasti kybernetické bezpečnosti bylo zjištěno, že respondenti si jsou základních rizik vědomi, avšak jejich skutečné chování není vždy dostatečně opatrné. Část respondentů používá stejné heslo pro více účtů nebo již klikla na podezřelý odkaz. Přestože většina respondentů využívá dvoufázové ověření, významná skupina uživatelů jej nepoužívá

nebo nezná jeho význam. Tato zjištění naznačují, že kybernetická hygiena uživatelů není na jednotné úrovni.

Za nejvíce ohroženou skupinu lze považovat osoby, které informace neověřují a spoléhají především na obsah ze sociálních sítí. Tito respondenti častěji nedokázali posoudit pravdivost tvrzení a byli náchylnější k manipulativním sdělením. Rizikovým faktorem se neukázal pouze věk nebo vzdělání, ale především pasivní přístup k informacím a nízká míra kritického hodnocení obsahu.

Výsledky také ukázaly, že většina respondentů považuje dezinformace za bezpečnostní hrozbu pro Českou republiku. Přesto však část populace jejich význam podceňuje, což může snižovat celkovou odolnost společnosti vůči informačním operacím. Lze tedy konstatovat, že česká společnost si existenci dezinformací uvědomuje, avšak úroveň odolnosti vůči nim není jednotná.

Na základě praktické části lze shrnout, že společnost jako celek není vůči dezinformačnímu působení bezbranná, avšak její odolnost závisí především na individuálním přístupu jednotlivců k informacím. Klíčovým faktorem se ukazuje kritické myšlení, schopnost ověřovat informace a dodržování základních zásad bezpečného chování v online prostředí.

Závěr

Bakalářská práce se zabývala problematikou kybernetických a informačních hrozeb pro Českou republiku v kontextu rusko-ukrajinské války. Hlavním cílem práce bylo analyzovat působení těchto hrozeb na českou společnost, zhodnotit úroveň povědomí obyvatel o dezinformacích a kybernetické bezpečnosti a navrhnout opatření vedoucí ke zvýšení odolnosti obyvatel vůči manipulativnímu působení v informačním prostoru. Teoretická část práce ukázala, že moderní konflikty se již neodehrávají pouze ve fyzickém prostoru, ale významnou roli hraje také prostor kybernetický a informační. Informační operace, propaganda a dezinformační kampaně představují nástroje hybridního působení, jejichž cílem je především ovlivňování veřejného mínění, oslabování důvěry ve státní instituce a vyvolávání společenské polarizace. Česká republika jako členský stát Evropské unie a NATO je těmto aktivitám vystavena, přestože se ozbrojený konflikt odehrává mimo její území.

Praktická část práce byla založena na kvantitativním dotazníkovém šetření mezi obyvateli České republiky. Výsledky ukázaly, že většina respondentů má základní povědomí o existenci dezinformací a dokáže rozpoznat zjevně manipulativní sdělení. Zároveň však část respondentů některým nepravdivým tvrzením věří nebo si není jejich pravdivostí jistá. Zjištěno bylo také, že značná část respondentů získává informace ze sociálních sítí, které představují prostředí s vysokým výskytem neověřeného nebo manipulativního obsahu.

Za klíčový faktor odolnosti se ukázalo aktivní ověřování informací. Respondenti, kteří si informace pravidelně ověřují z více zdrojů, vykazovali vyšší schopnost rozpoznat dezinformační obsah a častěji považovali dezinformace za bezpečnostní hrozbu. Naopak osoby, které informace neověřují, byly náchylnější k manipulativním sdělením a častěji vykazovaly nejistotu při posuzování pravdivosti informací.

Výzkum dále ukázal, že zranitelnost vůči dezinformacím není určena pouze věkem nebo vzděláním, ale především přístupem jednotlivce k informacím. Nejohroženější skupinu tak nepředstavuje konkrétní věková nebo vzdělanostní kategorie, ale osoby s pasivním přístupem k informacím, které nekriticky přebírají obsah ze sociálních sítí a neověřují jeho původ.

Z hlediska kybernetické bezpečnosti bylo zjištěno, že respondenti mají základní povědomí o rizicích, avšak jejich chování není vždy bezpečné. Část respondentů používá slabá nebo opakovaná hesla, klikla na podezřelý odkaz nebo nevyužívá pokročilé ochranné prvky, například dvoufázové ověření. To potvrzuje, že informovanost o rizicích neznamená automaticky bezpečné chování v online prostředí.

Na základě získaných poznatků byla navržena opatření zaměřená především na zvyšování mediální a informační gramotnosti obyvatel. Důležitou roli by měla hrát škola, stát i jednotlivé instituce, zejména v oblasti vzdělávání, prevence a informování veřejnosti. Klíčové je zejména vedení obyvatel k ověřování informací, rozvoj kritického myšlení a posilování bezpečného chování na internetu.

Lze konstatovat, že česká společnost si existenci dezinformačních kampaní uvědomuje, avšak její odolnost není jednotná. Dezinformace nepředstavují pouze mediální problém, ale také bezpečnostní riziko, které může ovlivňovat stabilitu státu, veřejné mínění i schopnost společnosti reagovat na krizové situace. Zvyšování informační a kybernetické gramotnosti obyvatel proto představuje důležitou součást bezpečnosti České republiky.

Cíl práce byl splněn, neboť na základě teoretické analýzy a empirického výzkumu byly identifikovány hlavní rizikové faktory ovlivňující náchylnost obyvatel k dezinformacím a byla formulována konkrétní doporučení vedoucí ke zvýšení odolnosti společnosti vůči kybernetickým a informačním hrozbám

Seznam použitých zdrojů

Literární zdroje

1) BOREK, David; ČERNOHORSKÝ, Václav; JONÁŠ, Martin; KUBAL, Michal; MIŘEJOVSKÝ, David et al. SZÁNTÓ, Jakub (ed.). Putinova válka: ukrajinská kronika zpravodajů ČT. Praha: Argo, 2023. s.331. ISBN 978-80-257-4046-0.
2) FRIDMAN, Ofer. Russian "Hybrid Warfare": Resurgence and Politicisation. London: Hurst & Company, 2018. s.288. ISBN 978-1-84904-909-2.
3) GALEOTTI, Mark. Putinovy války: od Čečenska po Ukrajinu. Přeložila Alena BYRNE. V Praze: Bourdon, 2023. s.439. ISBN 978-80-7611-074-8.
4) HLOUŠKOVÁ, Kateřina; MIKŠ, František (eds.). Prokletí impéria a ruská lež: Rusko a Ukrajina v kontextu a Kontextech. Brno: Books & Pipes, 2023. s.357. ISBN 978-80-7485-267-1.
5) HOLÝ, Petr. Válka na Ukrajině: kontext. Pemmikan. Praha: Gnóm! – Jakub Němeček, 2022. s.145. ISBN 978-80-88299-21-9.
6) IVANČÍK, Radoslav. Dezinformácie: teoretické východiská ich skúmania. Teoretik. Praha: Leges, 2025. s.188. ISBN 978-80-7502-769-6.
7) IVANČÍK, Radoslav; NEČAS, Pavel. Hybridné hrozby: bezpečnostná výzva pre demokratické spoločnosti. Teoretik. Praha: Leges, 2025. s.226. ISBN 978-80-7502-823-5.
8) KOLOUCH, Jan; BAŠTA, Pavel; KROPÁČOVÁ, Andrea; KUNC, Martin. CyberSecurity. 1. vyd. Praha: CZ.NIC, 2019. s.542. ISBN 978-80-88168-32-4.
9) KŘÍŽ, Zdeněk. Cesta z Ruska: ruská agrese proti Ukrajině a její důsledky. Brno: Munipress, 2023. s.168. ISBN 978-80-280-0260-9.
10) LITVINENKO, Aleksandr Val'terovič; FEL'ŠTINSKIJ, Jurij Georgijevič; LEMEŠANI, Tomáš. Rusko v plamenech: jak vznikl režim v Kremlu a jak funguje. Praha: Euromedia Group, 2022. s.294. ISBN 978-80-242-8237-4.
11) MOKRYK, Radomyr; PADEVĚT, Jiří. Hovory o Ukrajině. Praha: Academia, 2023. s.190. ISBN 978-80-200-3436-6.
12) RID, Thomas. Aktivní opatření: tajná historie dezinformací a politické války. Přeložil Aleš VALENTA. Praha: Academia, 2025. s.558. ISBN 978-80-200-3523-3.
13) SCHERF, Filip. Ztracená země: Příběh moderního Ruska. Brno: Host, 2024. s.383. ISBN 978-80-275-2342-9.

14) SCHULZE WESSEL, Martin. Prokletí impéria: Ukrajina, Polsko a scestí ruských dějin. V českém jazyce vydání první. Přeložil Petr DVOŘÁČEK. Praha: Maraton, 2024. s.213. ISBN 978-80-88411-31-4.
15) SPURNÝ, Jaroslav. Vrbětice: ruská operace, která změnila Česko: pozadí největšího teroristického útoku v moderních dějinách země. Praha: Respekt Media, 2025. s.203. ISBN 978-80-909308-6-5.
16) SYRUČEK, Milan. Rusko-ukrajinské vztahy: jak hluboké jsou kořeny současného konfliktu? Aktualizované vydání. V Praze: Grada, 2023. s.271. ISBN 978-80-271-5221-6.

Elektronické zdroje

1) MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Informační manipulace Kremlu: Jak je rozeznat a jak jim čelit.* Praha: Ministerstvo zahraničních věcí ČR, 2025. 16 s.
2) NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti 2026–2030.* Brno: NÚKIB, 2025. 41 s.

narodni_strategie_kb_2026-2030

3) STOJAR, Richard. Vývoj a proměna konceptu hybridní války. *Vojenské rozhledy.* 2017, roč. 26, č. 2, s. 44–55. DOI 10.3849/2336-2995.26.2017.02.044-055. ISSN 1210-3292.
4) ŠÍR, Jan et al. *Ruská agrese proti Ukrajině.* 1. vyd. Praha: Univerzita Karlova, Nakladatelství Karolinum, 2017. 199 s. ISBN 978-80-246-3711-2.
5) VINŠ, Petr Jan. *Dezinformační narativy o válce na Ukrajině v ČR a ve střední a východní Evropě: Analýza za období červen–říjen 2022.* Praha: Prague Security Studies Institute, 2022. 15 s.

Legislativní dokumenty

ČESKO. VLÁDA ČESKÉ REPUBLIKY. *Bezpečnostní strategie České republiky 2023.* Praha: Úřad vlády České republiky, 2023. 39 s.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti 2026–2030.* Brno: NÚKIB, 2025. 41 **s.**

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024.* Brno: NÚKIB, 2024. 56 s.

Seznam zkratek

CSIRT – tým řešení bezpečnostních incidentů v informačních systémech

DDoS – útok zahlcením služby vedoucí k nedostupnosti systému

EU – Evropská unie

FSB – Federální služba bezpečnosti Ruské federace

GRU – Hlavní správa rozvědky Generálního štábu Ozbrojených sil Ruské federace

NATO – Severoatlantická aliance

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OUN – Organizace ukrajinských nacionalistů

UPA – Ukrajinská povstalecká armáda

Seznam tabulek a grafů

Seznam příloh

Příloha č. 1 - Dotazníkové šetření Kybernetických a informačních hrozeb pro Českou republiku v kontextu rusko-ukrajinské války

Příloha č. 1 - Kybernetické a informační hrozby pro Českou republiku v kontextu rusko-ukrajinské války

Použité otázky dotazníkového šetření:

1. Věková kategorie
☐ 15-24 let
☐ 25-34 let
☐ 35-44 let
☐ 45-54 let
☐ 55 let a více

2. Pohlaví
☐ Muž
☐ Žena
☐ Nechci uvádět

3. Nejvyšší dosažené vzdělání
☐ základní
☐ střední bez maturity
☐ střední s maturitou
☐ vyšší odborné nebo vysokoškolské

4. Velikost místa bydliště
☐ do 2 000 obyvatel
☐ 2 001-10 000 obyvatel
☐ 10 001-100 000 obyvatel
☐ nad 100 000 obyvatel

5. Odkud nejčastěji získáváte informace o aktuálním dění? (max. 2 odpovědi)
☐ televize
☐ zpravodajské internetové weby
☐ Facebook
☐ YouTube
☐ TikTok
☐ rodina nebo známí

6. Ověřujete si někdy pravdivost informace na internetu?
☐ vždy
☐ často
☐ někdy
☐ nikdy

7. Který titulek je podle vás důvěryhodnější?
☐ „ŠOK! Vláda tají pravdu o Ukrajině!“
☐ „Ministerstvo zveřejnilo zprávu o pomoci Ukrajině“

8. Na sociální síti vidíte článek bez uvedeného autora. Co uděláte?
☐ sdílím ho
☐ přečtu ho a dál neřeším
☐ pokusím se ověřit zdroj
☐ ignoruji ho

9. Vidíte fotografii údajného válečného útoku na internetu. Jaký je nejlepší postup?
☐ ihned ji sdílet
☐ komentovat
☐ pokusit se ověřit původ fotografie
☐ věřit tomu, kdo ji sdílel

10. Ukrajinští uprchlíci dostávají vyšší finanční podporu než čeští občané.
☐ spíše pravda
☐ spíše nepravda
☐ nevím

11. NATO plánuje válku s Ruskem.
☐ spíše pravda
☐ spíše nepravda
☐ nevím

12. Většina informací o válce je veřejnosti záměrně tajena.
☐ spíše pravda
☐ spíše nepravda
☐ nevím

13. Používáte stejné heslo na více internetových účtech?
☐ ano
☐ ne
☐ nevím

14. Klikli jste někdy na podezřelý e-mail nebo odkaz?
☐ ano
☐ ne
☐ nejsem si jistý

15. Používáte dvoufázové ověření (např. SMS kód při přihlášení do banky/e-mailu)?

☐ ano

☐ ne

☐ nevím, co to je

16. Myslíte si, že dezinformace představují bezpečnostní hrozbu pro Českou republiku?

☐ ano

☐ spíše ano

☐ spíše ne

☐ ne