

**UNIVERZITA KARLOVA**

**FAKULTA SOCIÁLNÍCH VĚD**

Institut politologických studií

Katedra politologie

**Bakalářská práce**

**2021**

**Michael Koula**

**UNIVERZITA KARLOVA**

**FAKULTA SOCIÁLNÍCH VĚD**

Institut politologických studií

Katedra politologie

**Koncept hybridní války jako zdroj bezpečnostní politiky**

Bakalářská práce

Autor práce: Michael Koula

Studijní program: Politologie a veřejná politika

Vedoucí práce: Mgr. Bohumil Doboš, Ph.D.

Rok obhajoby: 2021

## **Prohlášení**

1. Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne 27. 7. 2021

Michael Koula

## **Bibliografický záznam**

KOULA, Michael. *Koncept hybridní války jako zdroj bezpečnostní politiky*. Praha, 2021. 40 s. Bakalářská práce práce (Bc). Univerzita Karlova, Fakulta sociálních věd, Institut politologických studií, Katedra politologie. Vedoucí diplomové práce Mgr. Bohumil Doboš, Ph.D.

**Rozsah práce: 67 291**

## **Abstrakt**

Cílem práce je zjistit, jestli lze na základě konceptu hybridní války, zpracovaného ve strategických dokumentech ČR, vytvořit dostatečnou bezpečnostní politiku pro zvládnutí této hrozby. V práci popisují postupný vývoj konceptualizace hybridní války v českém prostředí. Klíčovými dokumenty pro tuto práci je *Audit národní bezpečnosti* a *Národní strategie pro čelení hybridnímu působení*, což jsou strategické dokumenty, které v rámci ČR pracují s konceptem hybridní války. Zároveň v práci využívám konceptualizaci hybridní války, které je obsažena v dokumentech mezinárodních organizací jako NATO, EU a také Evropského centra excelence pro čelení hybridním hrozbám. Na základě mezinárodních dokumentů v práci určuji ideální konceptualizaci na národní úrovni a snažím se ji porovnat s konceptualizací ve strategických dokumentech ČR. V závěru práce dojde ke zjištění, že vývoj konceptualizace v ČR začal v roce 2016 vydáním prvního dokumentu a pokračoval o pět let později v roce 2021 s tím, že se dokumenty v konceptualizace drobně odlišují na základě nových poznatků. Zároveň je v práci určeno, že na základě konceptu hybridní války ve strategických dokumentech ČR lze vytvořit dostatečnou bezpečnostní politiku.

## **Abstract**

The goal of this thesis is to find out if it is possible to create adequate security policies to counter hybrid warfare based on the concepts, which are included in strategic documents of the Czech republic. This thesis also tries to explain development of concept of hybrid warfare in czech environment. The key documents for this thesis are *Audit národní bezpečnosti* and *Národní strategie pro čelení hybridnímu působení*, which are the only strategic documents, that use concept of hybrid warfare inside the Czech republic. At the same, this thesis uses concept of hybrid warfare, which is used in key documents of international organizations, such as NATO, EU, and The European Center of Excellence for Countering Hybrid Threats. Based on these international documents, this thesis creates ideal concept for work on national level and tries to compare it with the concept used inside strategic documents of the Czech republic. In the summary of this thesis, I will explain, that the development of concept of hybrid warfare in strategic documents started in 2016 with the first document and continued five years later in 2021, with small changes

to the concept, based on new findings. At the same time, this thesis finds out, that it is indeed possible make adequate security policies based on concept of hybrid warfare inside czech strategic documents.

### **Klíčová slova**

Hybridní válka; bezpečnostní politika; mezinárodní organizace; státní aktér; koncept

### **Keywords**

Hybrid warfare, security policy, international organization, state actor, concept

### **Title/název práce**

Hybrid warfare concept as a source of security policies

## **Poděkování**

Na tomto místě bych rád poděkoval vedoucímu mé bakalářské práce Mgr. Bohumilovi Dobošovi, Ph.D., který mi při psaní velmi pomohl včasnými a věcnými připomínkami k mé práci. Zároveň bych chtěl poděkovat své rodině a kamarádům, kteří mě při tvorbě práce podporovali.

# Obsah

Úvod.....	2
1. Vymezení výzkumného problému .....	3
1.1 Cíl výzkumu .....	3
1.2 Výzkumné otázky .....	3
1.3 Metodologie.....	3
1.4 Rozdíl ve vymezení výzkumu oproti původnímu projektu.....	4
2. Konceptuální a teoretická východiska .....	4
2.1 Vývoj pojmu v bezpečnostní politice .....	4
2.2 Konceptualizace Auditu národní bezpečnosti.....	6
2.3 Konceptualizace Národní strategie pro čelení hybridnímu působení .....	13
3. Analytická část .....	16
3.1 Vývoj konceptualizace v dokumentech ČR.....	16
3.2 Ideální konceptualizace .....	19
3.3 Konceptualizace v českých dokumentech .....	22
Závěr.....	27
Summary.....	28
Použitá literatura .....	31



# Úvod

Ve své bakalářské práci se zaměřím na koncept hybridní války a budu zkoumat, zda lze na jeho základě možné v ČR vytvořit dostačující bezpečnostní politiku, která má popisovanou hrozbu potlačit. Hybridní válka je novodobý pojem, který je těžké přesněji ukotvit, jelikož na rozdíl od dalších druhů hrozeb nespadá pouze pod jednu dimenzi moci (ty zahrnují například diplomacii, informace, ozbrojené síly, ekonomiku, finančnictví, zpravodajství, veřejný pořádek). Samotná konceptualizace hybridní války je velmi složitá, pojem se neustále rozvíjí, u různých akademiků a autorů se liší jeho definice a pohled na jeho užitečnost. Proto považuji za vhodné přesně určit konceptuální základ, ze kterého budu v práci vycházet. V rámci ČR mi k tomu budou sloužit dva dokumenty. Prvním z nich je dokument, vypracovaný ministerstvem vnitra se jménem *Audit národní bezpečnosti*, kde je koncept popsán, definován a také jsou určeny instituce a nástroje, které by měly napomoci k eliminaci hybridní války v rámci České republiky. V dubnu roku 2021 schválila česká vláda také nový dokument s názvem *Národní strategie pro čelení hybridnímu působení*, což je první dokument, jež se v českém prostředí zabývá jenom a pouze hybridní válkou. Na základě této relevance a unikátnosti v českém prostředí byly tyto dokumenty vybrány pro mou bakalářskou práci.

Ze začátku této práce bych chtěl zamezit možnému zmatení a ujasnit, že v rámci této práce budu vnímat pojmy hybridní válčení, hybridní způsob vedení konfliktu, hybridní kampaň, hybridní hrozba nebo hybridní působení jako synonyma. Různé instituce a autoři preferují různá pojmenování pro tento koncept, nicméně není možné je vzájemně odlišit (Bahenský, 2018, str. 90). Toto řešení mi taktéž přijde vhodné, jelikož ho využívá jeden z hlavních konceptuálních dokumentů (Audit, 2016, str. 127). Aby byla má práce co nejlépe uspořádána, budu v ní používat především pojem “hybridní válka”, který mi přijde nejvhodnější, vzhledem k názvu mé práce. Nicméně v kapitolách, ve kterých budu popisovat konceptualizaci v konkrétních strategických dokumentech ČR se budu držet slovníku, který je v nich použit.

Rostoucí technologický vývoj s sebou přináší mnoho pozitiv, ale mimo jiné také vytvořil nové hrozby, se kterými se musíme vypořádat. Z tohoto důvodu je, dle mého názoru, toto téma velice aktuální a vzhledem k současnému vývoji a expandující povaze konceptu a technologií obecně, zůstane aktuální i v budoucnu. Fakt, že je koncept zmíněn i ve

strategických dokumentech České republiky navíc dokazuje, že má cenu se jím zabývat, jelikož se jedná o problém, který je řešen na národní, ale i mezinárodní úrovni v rámci Severoatlantické aliance (dále pouze “NATO”) a Evropské Unie (dále pouze “EU”) (*NATO’s response to hybrid threats, 2016 až 2019; Společný rámec pro boj proti hybridním hrozbám - Reakce Evropské Unie, 2016.*).

Tato práce je užitečná vzhledem k tomu, že může sloužit jako revize efektivity jednotlivých bezpečnostních institucí a nástrojů, které se mají zabývat hybridní válkou.

# 1. Vymezení výzkumného problému

## 1.1 Cíl výzkumu

Cílem mé práce je popsat, zda se dá na základě konceptu hybridní války, který je popsán ve strategických dokumentech ČR, vytvořit adekvátní bezpečnostní politika pro zvládnutí této hrozby.

## 1.2 Výzkumné otázky

Jak se postupně proměňovala konceptualizace hybridní války v rámci oficiálních dokumentů ČR?

Je možné na základě konceptu hybridní války, který je popsán ve strategických dokumentech ČR, vytvořit dostačující bezpečnostní politiku k zvládnutí této hrozby?

## 1.3 Metodologie

V mé bakalářské práci budu provádět kvalitativní výzkum (Hendl, 2005), konkrétně budu analyzovat vybrané dokumenty na základě jejich využití konceptualizace hybridní války.

V rámci této práce se budu opírat o konceptualizaci hybridní války, jak je pojatá v dokumentu ministerstva vnitra *Audit národní bezpečnosti* a dokumentu ministerstva obrany *Národní strategie pro čelení hybridnímu působení*.

Z výše určených dokumentů vypíšu konceptualizaci hybridní války tak, jak je v daných dokumentech popsána, včetně odpovědných institucí a orgánů, které jsou v nich uvedeny. Na základě dalších konceptualizací, uvedených v dokumentech relevantních mezinárodních organizací (EU, NATO, Evropské centrum excelence pro čelení hybridním

hrozbám) se pokusím přijít s vlastním řešením problému. Toto řešení budu poté aplikovat na konceptualizaci z relevantních dokumentů v ČR a pokusím se určit, zda je česká konceptualizace vhodná.

Na základě vypsání konceptualizace budu také ve snaze odpovědět na další výzkumnou otázku analyzovat rozdíl mezi jednotlivými konceptualizacemi v českých dokumentech, tedy *Auditů národní bezpečnosti a Národní strategii pro čelení hybridnímu působení*.

## **1.4 Rozdíl ve vymezení výzkumu oproti původnímu projektu**

Vymezení mého výzkumu se liší oproti původním tezím mé bakalářské práce. Konkrétně jsem rozšířil analyzované dokumenty o *Národní strategii pro čelení hybridnímu působení*. Během zpracovávání původního projektu tento dokument neexistoval. Schválen byl až poté, co jsem měl práci zapsanou a začal jsem na ni pracovat. Vzhledem k povaze mého výzkumu (tj. zaměření se na konceptualizaci v rámci strategických dokumentů ČR) mi přišlo vhodné pracovat s tímto novým dokumentem, jelikož představuje další krok v konceptualizaci v ČR a zároveň určuje budoucí vývoj v českém prostředí v této tématice. Také jsem přidal jednu výzkumnou otázku, a to *Jak se postupně proměňovala konceptualizace hybridní války v rámci oficiálních dokumentů ČR?* Během výzkumu, který jsem provedl, abych odpověděl na původní otázku, jsem zpracoval shrnutí konceptualizace obou dokumentů. Jelikož jsem tedy měl zpracovanou velkou část k zodpovězení této nové otázky, rozhodl jsem se práci rozšířit tímto směrem.

## **2. Konceptuální a teoretická východiska**

### **2.1 Vývoj pojmu v bezpečnostní politice**

Ze začátku této kapitoly bych chtěl věnovat část své práce popisu vzniku a rozvoje samotného konceptu hybridní války. Vývoj tohoto konceptu byl již detailně popsán v jiných pracích (například diplomová práce Vojtěcha Bahenského, zpracována na FSV UK v roce 2016), proto bych se chtěl pouze stručně zmínit o nejdůležitějších událostech, který vývoj ovlivnily. Chtěl bych tím popsat kontext, který vedl k popularizaci konceptu při vytváření bezpečnostní politiky a také kontext ve kterém je s ním pracováno na národní nebo mezinárodní úrovni.

Pojem hybridní válka získal na popularitě ve 21. století i přesto, že jeho definici lze aplikovat na situace ze století minulého. Koncept hybridní války je rozporuplný, jelikož se v akademickém prostředí setkává s poměrně častou kritikou, ale přesto je používán v rámci tvorby bezpečnostní politiky, ať už na mezinárodním poli v rámci NATO a EU, tak na národní úrovni například právě v České republice.

Prvním významným akademickým dílem, které se pojmu věnuje je práce "*Conflict in 21st Century: The Rise of Hybrid Wars*" od amerického autora Franka Hoffmana. Podle tohoto autora je hybridní válkou způsob vedení války, ve kterém státní nebo nestátní aktér spojuje konvenční a nekonvenční strategie a přístupy, aby dosahoval svých cílů (Hoffman, 2007). Za zmínku stojí také fakt, že autor s pojmem pracoval v kontextu ozbrojených konfliktů v Iráku a Afghánistánu. V tu dobu probíhala diskuse mezi zastánci konvenčního přístupu k vedení války a zastánci zaměřením na protipovstalecké operace, přičemž Hoffman navrhuje hybridní válku jako kompromisní řešení. (Hoffman, 2009). Je nutno podotknout, že i když se jedná o jednoho z nejvýznamnějších a nejcitovanějších autorů v rámci tématu hybridní války, je tato konceptualizace kritizována dalšími významnými autory, jakým je například Colin Gray. Ani v tomto případě se tedy nelze vyhnout akademickému pragmatismu (Bahenský, 2018, str. 94).

Koncept hybridního válčení se poté objevuje jako reakce na okupaci Krymu Ruskou federací a následné ruské operace na východní Ukrajině v roce 2014. Úspěch ruských operací vyvolal touhu a nutnost přesně označit způsob vedení konfliktu, což nakonec vyhrál pojem hybridní válka. Pro lepší porozumění nových publikací na toto téma po roce 2014 je nutno dodat, že byl přijat pouze pojem "hybridní válka", nikoliv samotný koncept a konkrétní definice. Někteří autoři usoudili, že původní americká definice moc neodpovídá ruskému způsobu vedení konfliktu, proto si vytvořili vlastní na základě ruských operací (Bahenský, 2018, str. 95).

Právě situace na Krymu z roku 2014 zvýšila zájem o téma hybridní války i v mezinárodních organizacích jako je NATO a EU. Tento zájem se projevil vznikem nových dokumentů, kde je s konceptem pracováno (např. *Společný rámec pro čelení hybridním hrozbám ze 7. dubna 2016*). Popularizace konceptu na mezinárodní úrovni bezpečnostní politiky také později vedla ke vzniku další organizace s názvem *Evropské centrum excelence pro čelení hybridním hrozbám*, vzniklé v roce 2017 v Helsinkách za podpory EU a NATO. Tato organizace slouží jako platforma pro strategickou diskuzi ohledně hybridní

války (About us - Hybrid CoE, 2021).

Rozšíření konceptu i do oficiálních dokumentů mezinárodních organizací, jejímž členem je Česká republika, eventuálně vedlo i ke zpracování pojmu i v českém prostředí. Konkrétně se jednalo o dva dokumenty: *Audit národní bezpečnosti* z roku 2016 a *Národní strategie pro čelení hybridnímu působení* z roku 2021.

## 2.2 Konceptualizace Auditů národní bezpečnosti

Audit národní bezpečnosti (dále pouze "Audit") je dokument, který vytvořilo ministerstvo vnitra na základě zadání někdejšího předsedy vlády Bohuslava Sobotky ve spolupráci s expertní skupinou určující osnovu materiálu (Audit, 2016, str. 8). Tento dokument věnuje hybridnímu válčení jednu z celkových 10 kapitol, nicméně jak autoři sami zmiňují, jednotlivá témata se mohou a nemusí v rámci kapitol překrývat.

Autoři nazývají v auditu hybridní válku jako hybridní kampaň. Ta je v dokumentu definována takto: *"Úkolem hybridní kampaně je využít slabin protivníka; maskovat se sledováním legitimních cílů; znemožnit jasnou interpretaci událostí a odhalení jejich vzájemné souvislosti; komplikovat či přímo znemožnit identifikaci původce a zastřít jeho úmysly; komplikovat, destabilizovat či přímo paralyzovat rozhodovací proces, a tím znemožnit včasnou a účinnou reakci ze strany napadeného. Hybridní útočník osnuje a provádí aktivity poškozující životní, strategické či obecně bezpečnostní zájmy jiného aktéra a přitom usiluje o vytvoření prostředí, kdy mu za tyto aktivity nelze (přinejmenším formálně) jednoznačně přiřknout odpovědnost, nebo tak lze učinit pouze velmi obtížně a spekulativně. Hybridní útočník se bude snažit udržovat své aktivity pod prahem, jehož překročení by mezinárodní společenství považovalo za ozbrojenou agresi. Přímé vojenské konfrontaci se patrně bude snažit vyhnout, ovšem je nutné předpokládat, že do hybridní kampaně v nějaké podobě zakomponuje i použití vojenských prostředků."* (Audit, 2016, str. 127).

Audit také zmiňuje, že aktér, který se snaží vytvořit hybridní aktivitu, může využívat nástroje z dimenze moci - DIMEFIL (Audit, 2016, str. 128):

D) Diplomacy: snaha o narušení a ovlivnění oficiálních politických aktérů na různých úrovních;

I) Information: využití různorodých sdělovacích prostředků k šíření specifických

informací, za cílem propagandy nebo vytvoření dezinformační kampaně;

M) Military: využití vojenské síly útočníka buďto k zastrašování už pouhou existencí (např. přesunutím velké části armády k hranicím se sousedním státem) nebo přímé nasazení na území druhého státu v rámci malých skupin;

E) Economy: vytvoření formy nátlaku pomocí akcí, které ovlivňují ekonomiku státu (uvalení cla, embargo, odepření dodávek surovin či energie, destabilizace podniků a odvětví);

F) Financial: snaha destabilizovat měnu, bankovní sektor, trh s akciemi a dluhopisy;

I) Intelligence: nasazení špiónů na území jiného státu, snaha získat spolupracovníky na státních nebo politicky aktivních pozicích, kteří budou pomáhat vytvářet protistátní činnost;

L) Law Enforcement: snaha vytvářet na území státu rozvratné činnosti, jež mají oslabit hodnotové, právní a společenské aspekty běžného života. Konkrétními přístupy v této dimenzi může být například podněcování k nepokojům na základě etnických nebo náboženských dělících liniích společnosti nebo pomocí teroristických útoků a jiných kriminálních metod.

Tyto dimenze moci vychází z přístupu, který mají k hybridní kampani organizace NATO a EU. Ty přenášejí odpovědnost na samostatné státy a jejich vnitřní bezpečnostní infrastrukturu. Zároveň ale podotýkají, že je nepravděpodobné, že by tomuto konfliktu čelil pouze jeden stát, je tedy také zdůrazněna vzájemná podpora a spolupráce, kdy role samotných organizací je spíše podpůrná (NATO's response to hybrid threats, 2016 až 2019; Společný rámec pro boj proti hybridním hrozbám - Reakce Evropské Unie, 2016).

Je nutno podotknout, že jednotlivé aktivity nemusí být nutně protizákonné a vlastně ani nemusí samostatně představovat hrozbu pro bezpečnost státu. Situace se ale komplikuje, pokud dochází právě ke společnému propojení jednotlivých dimenzí v synchronizovaném útoku, který má společný cíl. Značným problémem je také fakt, že pro aktéra napadeného hybridní kampaní je těžké určit, že je vůbec napaden. To samotné zvyšuje efektivitu hybridní kampaně, proto je pro eliminaci nutné zaměřit se na efektivní získání informací. (Audit, 2016, str. 128)

S rostoucím technologickým rozvojem společnosti je také třeba zdůraznit roli kybernetického prostoru, který v tomto případě funguje jako prostředí, kde se jednotlivé

části dělení DIMEFIL prolínají. Konkrétně může sloužit k šíření dezinformací, pro špionáž, ohrožení finančního sektoru atd. (Audit, 2016, str. 128)

Audit také zmiňuje, že model hybridní kampaně využila Ruská federace v konfliktu s Ukrajinou v roce 2014 s vysokou mírou koordinace v delším časovém pásmu. Stejně tak je jmenována teroristická organizace tzv. Islámský stát, jakožto organizace, která využívá některé nástroje hybridní povahy. Konkrétně se dle autorů jedná například o propagandu za použití sociálních médií, manipulace s fakty a šíření dezinformací, využití kybernetických útoků, zastrasování ostatních aktérů hrozbou teroristických útoků a jiné. U obou případů je zdůrazněno, že hybridní kampaň je přizpůsobena svému cíli, tudíž nelze očekávat naprosto totožné nástroje a způsoby v případě napadení ČR. (Audit, 2016, str. 128).

V Auditě jsou také uvedeny tři základní pilíře státu, na které může být podle autorů zacílen případný hybridní útok. Uvedeny jsou jejich konkrétní nástroje a odpovědné instituce, které mají v daném pilíři zasahovat a představují důležitou roli. (Audit, 2016, str. 129):

#### **A) Soudržná společnost a její ztotožnění s ideově-hodnotovým zakotvením státu**

V rámci hybridní kampaně může vzniknout pokus agresivního aktéra ovlivnit politické struktury a celkový politický proces, soudy, policii a ozbrojené síly, sdělovací prostředky a obecné veřejné mínění. Tento pokus má za cíl destabilizovat daný stát a jeho společnost, zejména pak pomocí celkového rozdělení společnosti a také pomocí podlomení její důvěry v existující politické uspořádání, ať už na celostátní úrovni (právní stát, demokracie, základní lidská práva a svobody) tak co se týče mezinárodní politiky (zaměření ČR na spolupráci v rámci organizací jako je NATO, EU a dalších). Hlavním terčem hybridních aktivit by mohla být snaha o snížení vůle politické reprezentace a obyvatelstva pomoci jiným státům, zejména pak členům NATO a EU v případě jejich napadení. (Audit, 2016, str. 129.)

Autoři dokumentu uvádějí, že pravděpodobnost vzniku hybridního útoku tohoto typu je v porovnání s jinými typy relativně vysoká. Nicméně celkové riziko v této části hodnotí jako střední. (Audit, 2016, str. 129)

Na hybridní aktivity v tomto pilíři je třeba reakce od volené politické obce (zejména pak parlament) a celkově obyvatelstva. Z bezpečnostních institucí je pak nejvíce odpovědná vláda. Ta by měla podle autorů reagovat jak k agresorovi, tak k obyvatelstvu. U komunikace s obyvateli by je vláda měla ujistit o kompletní připravenosti k zajištění

bezpečnosti. Je potřeba posílit celkovou odolnost a jednotu v rámci společnosti, stejně tak by se měly odstraňovat vnitřní problémy. Nicméně se jedná o velice složitý a časově náročný proces, proto je zde těžké hledat a vytvářet specifické nástroje. (Audit, 2016, str. 131)

Při komunikaci s protivníkem je nutné, aby při strategické komunikaci vláda ukázala svou připravenost a schopnost bránit sebe sama, ale také své spojence, čímž může být agresivní aktér zastrašen a jeho útoky budou oslabeny. Tato komunikace vlády musí jít ruku v ruce s dalšími relevantními úřady. Konkrétně je uvedeno Ministerstvo zahraničních věcí, vnitra, obrany, průmyslu atd. Stejně tak je důležité zkoumat oblasti, ve kterých se objevují dezinformace a neustále je vyhodnocovat. (Audit, 2016, str. 131)

Do tohoto pilíře spadá také snaha ovlivnit politickou reprezentaci, průběh rozhodovacích procesů, soudů a obecně útok na běžné fungování státu. V této oblasti jsou odpovědné instituce vyšetřující závažnou trestnou činnost (zejména korupci) a zpravodajské služby. (Audit, 2016, str. 131)

## **B) Fungující ekonomika**

Dalším cílem hybridní kampaně může být snaha ovlivnit ekonomiku jiného státu. Konkrétními aktivitami může být například přerušení dodávek strategických surovin a energií nebo bojkot exportu. V případě České republiky je šance na setkání se s tímto druhem aktivit velká, jelikož je česká ekonomika otevřená, tudíž ji lze negativně ovlivňovat. Hlavními problémy může být například dodávka energií, jelikož vlastní české zdroje v této oblasti jsou značně omezené a jsme závislí na jejich dovozu. Tento dovoz navíc není dostatečně rozlišný. Nicméně obecně je riziko možných dopadů autory hodnoceno jako nízké, neboť je česká ekonomika propojená v rámci Evropské Unie a dá se očekávat rychlá pomoc, která by pomohla při zotavení. (Audit, 2016, str. 129-130)

V tomto pilíři je značná již zmíněná propojenost s dalšími kapitolami Auditů, které se nevěnují hybridní kampani. Konkrétně je to propojení s kapitolou „Energetická, surovinová a průmyslová bezpečnost“. Odpovědné instituce se tedy mění na základě povahy hybridní aktivity, nicméně lze předpokládat účast Ministerstva průmyslu a obchodu, Energetického regulačního úřadu, Státní energetické inspekce, Správy státních hmotných rezerv. (Audit, 2016, str. 112). Bezpečnostní systém ČR potom musí zjistit souvislost těchto ekonomických událostí s dalšími aktivitami, které jsou zaměřené proti zájmům ČR.



## **C) Bezpečnost a obrana**

V této oblasti může agresivní aktér využívat kriminální a zájmové skupiny (definované na základě národnosti, jazyku, náboženství nebo etnicity) k protistátní činnosti za účelem narušení pořádku. Ještě přesněji může vzniknout snaha oslabit přímo ozbrojené síly státu, stejně jako policii a další bezpečnostní služby pomocí šíření extremismu, čímž se sníží jejich efektivita a akceschopnost. Stejně tak může být ohrožena bezpečnost ozbrojených sil České republiky s cílem oslabit českou účast na zahraničních operacích a misích v rámci NATO a EU. V poslední řadě mohou být nasazeny speciální jednotky přímo na našem území za účelem špionáže. (Audit, 2016, str. 130)

Pravděpodobnost vojenského napadení na území ČR je vzhledem ke geografické poloze ve středu Evropy (a tedy i EU) velice nízká. Přesto je třeba počítat s tím, že někteří spojenci ČR mají toto riziko větší a vzniká tedy nutnost solidárního zapojení ČR na zajištění bezpečnosti. Riziko střední závažnosti vzniká v případě použití ozbrojených sil ČR v některých komplexních událostech jako například kolektivní odstrašení či obrana v rámci NATO proti konvenčnímu protivníkovi. Toto riziko se vztahuje zejména k personální a materiální naplněnosti a pohotovosti ozbrojených sil. (Audit, 2016, str. 130)

Nejdůležitější roli v tomto pilíři mají instituce, jejichž hlavním cílem je získávání informací, tedy zpravodajské služby. Konkrétně se jedná o Bezpečnostní informační službu; Úřad pro zahraniční styky a informace; Vojenské zpravodajství. Dále jsou odpovědné orgány kybernetické bezpečnosti, tedy: Národní bezpečnostní úřad; síť pracovišť typu Computer Emergency Response Team (CERT); Národní centrum kybernetických sil vytvořené u VZ. Hlavní pravomoci a nástroje potom spadají pod Ministerstvo vnitra; orgány vnitřní bezpečnosti a ochrany obyvatelstva a ozbrojené síly ČR. (Audit, 2016, str. 132)

K zisku informací mohou pomoci i jiné instituce, například ostatní ministerstva. Nicméně celkovou odpovědnost má vláda. Na základě Ústavy rozhoduje v nejdůležitějších momentech o obraně státu Parlament ČR.

### **Odpovědné instituce a jejich nástroje**

Než se pustím do této části, ve které popíšu jednotlivé instituce a orgány, které jsou v Auditě zmíněny jako zodpovědné pro čelení hybridní kampani, je třeba zmínit roli ministerstva obrany. Tento orgán nemá v rámci auditu v kapitole hybridních hrozeb

připsán žádnou specifickou roli, nicméně je i přesto důležitý. Ministerstvo obrany je totiž zodpovědné za plnění úkolů, které z Auditů vyplynuly.

### **Zpravodajské služby**

Jak již bylo zmíněno, hlavním cílem těchto institucí je neustálý sběr a vyhodnocování informací, které ohrožují zájmy a bezpečnost státu a obyvatelstva. Jejich činnost je vymezena zákonem č. 153/1994 Sb., o zpravodajských službách ČR, zákonem č. 154/1994 Sb., o bezpečnostní informační službě a zákonem č. 289/2005 Sb., o Vojenském zpravodajství. V případě zjištění zvětšené nepřátelské aktivity na našem území je možné jejich kapacity zpravodajských služeb posílit, za což je odpovědná vláda.

Činnost těchto institucí je čistě informativní, tj. není možné jejich aktivní zapojení do preventivních opatření pro zajištění bezpečnosti ČR. Do této oblasti spadají celkově 3 instituce: Bezpečnostní informační služby (BIS), Úřad pro zahraniční styky a informace (ÚŽSI) a Vojenské zpravodajství (VZ). (Audit, 2016, str. 133)

### **Orgány kybernetické bezpečnosti**

Na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, je hlavní koordinátorem kybernetické bezpečnosti na našem území Národní bezpečnostní úřad (dále pouze NBÚ). Jeho aktivita a pravomoci spočívají zejména v zajištění bezpečnosti a zlepšování odolnosti napříč celou českou kybernetickou infrastrukturou. Využívají také pracoviště typu Computer Emergency Response Team (CERT), které fungují i u jiných institucí.

NBÚ také vypomáhá zpravodajským službám a Policii České republiky při odhalování a vyšetřování kybernetických útoků a určením odpovědnosti za ně přesným aktérům. Nicméně vzhledem k nízkým personálním kapacitám je tato aktivita značně omezená a doporučuje se ji v budoucnu zlepšit. (Audit, 2016, str. 133)

### **Ministerstvo vnitra, orgány vnitřní bezpečnosti a ochrany obyvatelstva**

Pravomoci ministerstva vnitra vycházejí z kompetenčního zákona č. 2/1969 Sb. Na jeho základě je MV hlavním odpovědným aktérem při řešení nevojenských aktivit v rámci hybridní kampaně, zejména pak v oblasti veřejného pořádku, vnitřní bezpečnosti a ochrany obyvatelstva.

Důležitou roli hraje pak také Policie ČR, která se stává hlavním aktérem v případě ohrožení vnitřní bezpečnosti. V případě nedostatečné personální kapacity může být

doplněna částí ozbrojených sil a dalších bezpečnostních složek (Audit, 2016, str. 134).

### **Ozbrojené síly ČR**

Ozbrojené síly ČR a jejich pravomoci jsou stanoveny zákony: ústavním zákonem č. 110/1998 Sb., o bezpečnosti ČR; zákonem č. 222/1999 Sb., o zajišťování obrany ČR; zákonem č. 219/1999 Sb., o ozbrojených silách ČR; zákonem č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), poté Bezpečnostní strategií ČR a Obrannou strategií ČR. Role tohoto aktéra je zaměřena na vnější útoky a jejich odvrácení. Vzhledem k účasti ČR v organizacích jako NATO a EU je předpokládán útok na české území velice nepravděpodobný, zejména protože je ČR obklopena spojenci, nejedná se o hraniční stát organizací.

Kvůli tomu je u českých ozbrojených sil předpoklad poskytnutí podpory ke kolektivní obraně ostatních členských států NATO. Míra této podpory se odvíjí od intenzity jednotlivého konfliktu, je tedy proměnlivá. Jak již bylo zmíněno výše, ozbrojené síly lze nasadit v případě vnitrostátního nebezpečí jako podpůrnou jednotku k Policii ČR. Speciální roli hraje také Vojenská policie, která se snaží odhalit snahu o ovlivnění vojáků (např. podněcováním extremismu). (Audit, 2016, str. 134-135)

### **Vláda ČR**

Pravomoci vlády jsou vymezeny ústavním zákonem č. 1/1999 Sb., Ústava ČR; ústavním zákonem č. 110/1998 Sb., o bezpečnosti ČR; zákonem č. 222/1999 Sb., o zajišťování obrany ČR; zákonem č. 219/1999 Sb., o ozbrojených silách ČR. Klíčovou úlohou vlády je přijímat konkrétní rozhodnutí. Jelikož má k dispozici celý bezpečnostní systém, nese vláda veškerou odpovědnost za bezpečnost a obranu státu v případě hybridní kampaně. Má za úkol vydávat rozhodnutí a řešit krizové situace, k čemuž ji slouží výše zmíněné zpravodajské služby a další komunikační kanály s jinými státy v případě napadení spojeneckého státu (např. v rámci NATO).

Obecně je v rámci hybridní kampaně u vlády nutno splnit tři podmínky, které dopomohou ke správnému chodu: vláda musí být usnášeníschopná, musí mít zabezpečené pracoviště a zabezpečené spojení s ostatními prvky bezpečnostního systému. Získávání a vyhodnocování informací je důležitým prvkem pro odhalení a potlačení hybridní kampaně. Sdílení informací by také mělo probíhat na jednom místě, což je zdůrazněno jako důležitý prvek bezpečnostního systému pro vládu ČR. (Audit, 2016, str. 135)

## **Prezident ČR**

Pravomoci prezidenta jsou upraveny ústavním zákonem č. 1/1999 Sb., Ústava ČR; zákonem č. 219/1999 Sb., o ozbrojených silách ČR a zákonem č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon).

Prezident je vrchní velitel ozbrojených sil, nicméně aby jím vydaná rozhodnutí vešla v platnost, potřebují podpis předsedy vlády nebo jiného pověřeného člena vlády. Pokud nějaké rozhodnutí vyžaduje takovýto podpis, přebírá za toto rozhodnutí odpovědnost vláda, proto je prezidentská role v rámci hybridní kampaně malá. (Audit, 2016, str. 135)

## **Parlament ČR**

Pravomoci jsou upraveny ústavním zákonem č. 1/1999 Sb., Ústavou ČR a v ústavním zákonem č. 110/1998 Sb., o bezpečnosti ČR.

Parlament rozhoduje o vyhlášení válečného stavu nebo stavu ohrožení. V případě napadení spojence rozhoduje také o vyslání ozbrojených sil ČR na území jiného státu, stejně tak o pobytu ozbrojených sil jiného státu na území ČR. Stejně jako v případě vlády je i u Parlamentu ČR nutnost zajistit nepřetržitou usnášenišchopnost za jakýchkoliv podmínek. V případě rozpuštění Parlamentu ČR se tyto odpovědnosti přenášejí na Senát Parlamentu ČR. (Audit, 2016, str. 136)

## **2.3 Konceptualizace Národní strategie pro čelení hybridnímu působení**

V dubnu 2019 schválila vláda České republiky Národní strategii pro čelení hybridnímu působení (dále pouze "Strategie"). Tento dokument byl vytvořený vzájemnou spoluprací Ministerstva obrany, Úřadu vlády, Ministerstva zahraničních věcí, Ministerstva vnitra, zpravodajských služeb, Armády ČR a Národního úřadu pro kybernetickou a informační bezpečnost. (Ministerstvo obrany ČR, 2021). Jedná se o první dokument v rámci ČR, který se věnuje pouze této tématice. Jeho vytvoření bylo zadáno samotným auditem a slouží k doplnění dalších bezpečnostních dokumentů pomocí formulace komplexní a celospolečenské politiky k čelení hybridnímu působení (Strategie, 2016, str. 1). Nicméně se nejedná o poslední dokument, který je v ČR na tuto tematiku připravován. V budoucnu bude ještě upravován a také na něj má navázat akční plán, který by měl přinést konkrétní opatření. (Strategie, 2016, str. 10).

Samotná definice hybridní války (ve Strategii je používán termín “hybridní působení”) se poté liší od Auditu. Konkrétně zní takto: *Hybridní působení je skrytá i zjevná činnost státních či nestátních aktérů (původců hybridního působení) namířená proti zranitelným prvkům demokratického státu a společnosti. Původci hybridního působení využívají politické, diplomatické, informační, vojenské, ekonomické, finanční, zpravodajské a další nástroje s cílem narušit chod demokratických institucí, procesy právního státu a vnitřní bezpečnost. Hybridní působení využívá i legálních a legitimně se jevících nástrojů k dosažení nepřátelských cílů a působí proti zájmům ČR. Rychlost, rozsah a intenzita hybridního působení se zvyšuje, a to i v důsledku rozvoje nových technologií* (Strategie, 2021, str. 3-4).

Podle Strategie dochází v bezpečnostním prostředí ČR k velkým změnám, které snižují jeho předvídatelnost. Šance, že bude ČR terčem přímého vojenského útoku na svém území je sice nízká, nicméně v rámci euroatlantického prostoru může země čelit činnosti využívající nástrojů hybridního působení.

Je uvedeno, že původcem hybridního působení mohou být státní i nestátní aktéři. Jejich útok nemusí být namířen pouze proti bezpečnostním složkám nebo orgánům veřejné správy, ale může být mířen do komerčního, mediální, vzdělávacího a neziskového sektoru. Také je podotknuto, že státními aktéry, kteří ovlivňují ČR dlouhodobě a systematicky v oblasti hybridního působení jsou zejména autoritářské a revizionistické velmoci (Strategie, 2021, str. 5).

Cílem hybridního působení je rozostření hranic mezi mírem, krizí a konfliktem. Útočník se snaží skrýt svou činnost a ztížit možnost určení původce. Využívá existující slabiny a společenské rozpory, které se snaží rozšiřovat. Cílem může být zejména ochromení politického rozhodovacího procesu, oslabení důvěry občanů v ústavněprávní uspořádání a demokracii, narušení ekonomických procesů, získání vlivu v informačním prostředí a oslabení funkce kritické infrastruktury. (Strategie, 2021, str. 5). Kritickou infrastrukturou se chápe energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systém, finanční trh a měna, nouzové služby a veřejná správa (Nařízení vlády č. 432/2010 Sb.)

Některé nástroje hybridního působení byly využívány i v minulosti, nicméně vývoj nových a rozšíření starých technologií umožnil také nárůst rozsahu a komplexity těchto nástrojů. Využívání moderních technologií v kyberprostoru, konkrétně například sociálních sítí a

internetových aplikací, vytváří nové zranitelnosti, které je třeba omezit (Strategie, 2021, str. 6).

Strategie říká, že hlavní odpovědnost při čelení hybridnímu působení má vláda ČR, která má také vydávat daná opatření. Nicméně při čelení individuálním aktivitám je odpovědnost přiřazena příslušným resortům na základě jejich pole působnosti. Zároveň je ale uvedeno, že existují platformy, které mají pomáhat při sdílení informací napříč těmito resorty za cílem lepší efektivity, zejména pak v rámci Bezpečnostní rady státu.

Dokument stanovuje tři oblasti, které mohou sloužit jako hlavní cíl pro vystavení hybridnímu působení. Jedná se o totožné oblasti, které jsou uvedeny ve třech pilířích v konceptualizaci Auditů, tj.:

- a. ideově-hodnotové zakotvení společnosti a ústavněprávní uspořádání státu,
- b. ekonomika
- c. bezpečnost a obrana

Dokument také zmiňuje tři strategické cíle, které určuje vláda ČR v rámci jejího boje s hybridním působením. Těmto cílům je věnována samostatná kapitola, kde jsou přesně definovány a je obecně určeno, jak mají být splněny. Konkrétně jsou to tyto cíle:

### **Odolná společnost, odolný stát, odolná kritická infrastruktura**

V rámci tohoto cíle je nutno chápat odolnost jako schopnost společnosti a státu vyhnout se v případě dlouhodobého hybridního působení škodám, případně je rychle a efektivně napravit. Konkrétní zmíněné cíle, na něž se má ČR v budoucnu zaměřit zahrnují: posílení možnosti včasné detekce hybridního působení a přesné určení původce (což je politické rozhodnutí vlády); zlepšení odolnosti státu za cílem snížení zranitelnosti; zlepšení odolnosti a funkčnosti kritické infrastruktury; kontrola zahraničních finančních investic do kritických sektorů ekonomiky ČR; snížení závislosti na zemích s odlišnou ideově-hodnotovou orientací; zvýšení znalosti o hybridním působení napříč společenskými sektory; provádění testů a cvičení, které předstírají hybridní působení ve veřejné správě a kritické infrastruktuře; (Strategie, 2021, str. 7-8).

### **Systémový a celostní přístup v rámci České republiky**

Cílem opatření je zajistit zlepšení meziresortní spolupráce a koordinace. Prioritou je zefektivnit komunikaci mezi všemi relevantními domácími aktéry, kteří zasahují do

oblastí, jež se mohou stát terčem hybridního působení. Z těchto důvodů budou vylepšeny platformy pro výměnu informací, které už existují v rámci Bezpečnostní rady státu. Důležitá bude také nově vzniklá funkce koordinátora agendy čelení hybridnímu působení. Celkově bude pravidelně prověřován bezpečnostní systém pomocí cvičení, které budou probíhat jak na národní, tak mezinárodní úrovni. Všechny nové informace v této oblasti budou pravidelně diskutovány v expertní skupině (Strategie, 2021, str. 8).

### **Schopnost adekvátní a včasné reakce**

Klíčovým prvkem pro obranu a včasnou reakci před hybridním působením je pro ČR členství v NATO a EU, zejména díky solidaritě a propojenosti napříč bezpečnostními sektory v rámci boje proti hybridnímu působení. Hlavním cílem ČR je tedy tuto propojenost prohlubovat a také se aktivně účastnit snahy o zlepšení schopností těchto organizací. V rámci zlepšení této mezinárodní spolupráce se bude ČR také snažit přispět v jiných iniciativách, jako například Evropské centrum excelence pro čelení hybridním hrozbám v Helsinkách. Další zmíněná opatření v této části je například identifikace typových reakcí na hybridní působení a jejich následné procvičení; využití systému strategické komunikace a následné zaměření tohoto systému na domácí i zahraniční publikum; zlepšení systému reakčních opatření, jak domácích, tak zahraničních v rámci mezinárodních organizací, včetně schopnosti vyhodnotit účinnost daných opatření. (Strategie, 2021, str. 8-9)

## **3. Analytická část**

### **3.1 Vývoj konceptualizace v dokumentech ČR**

Jak již bylo řečeno v předchozích kapitolách, v ČR se na konceptualizaci hybridní války zaměřují dva dokumenty. Konkrétně se jedná o *Audit národní bezpečnosti* a *Národní strategii pro čelení hybridnímu působení*, proto se na ně v této kapitole zaměřím z hlediska časového vývoje, ve snaze odpovědět na první výzkumnou otázku.

V první řadě je třeba zdůraznit, že konceptualizace nejsou v žádném případě protichůdné a žádným způsobem se nevyklučují. Samostatný vznik Strategie vychází z úkolů, které byly určeny v Auditě. Audit určuje, že je potřeba definovat strategický přístup ČR pro čelení hybridní válce, která může být vedena proti ní nebo jinému státu v rámci NATO a EU, přičemž má být tato definice buďto součástí Bezpečnostní strategie ČR nebo samostatný

dokument. Strategie tuto skutečnost sama zmiňuje a dodává, že se jedná pouze o doplnění současných bezpečnostních dokumentů.

Tuto návaznost lze také pozorovat u jednotlivých cílů, které Strategie zmiňuje. Kupříkladu Audit určuje, že vláda potřebuje pro efektivní odhalení hybridní války sdílet informace napříč resorty na jednom místě. V relevantní kapitole ve Strategii jsou poté uvedeny cíle jako vybudování systému strategické komunikace, vylepšení stávající infrastruktury pro sdílení informací, stejně jako vznik funkce koordinátory agendy pro čelení hybridnímu působení.

Mezi dokumenty je rozdíl v rámci kontextu, ve kterém vznikly. Audit v roce 2016 vypracovalo ministerstvo vnitra ve spolupráci s expertní skupinou. Oproti tomu byla Strategie schválena v dubnu 2021, na jejím vytvoření se podílelo několik ministerstev (obranu, vnitra, zahraničních věcí), Úřad vlády, zpravodajské služby, Armáda ČR a Národní úřad pro kybernetickou a informační bezpečnost. Tento posun k více meziresortní spolupráci při vytváření dostatečné bezpečnostní politiky pro čelení hybridní válce je určitě pozitivní změna. Jak se ostatně zmiňují oba dokumenty, téma hybridní války je komplexní a jeho původce se snaží zasahovat obránce ve více dimenzích, proto je propojenost a spolupráce jednotlivých oblastí zcela klíčová pro čelení.

Autoři Auditů v něm vymezili celkem deset okruhů hrozeb, které mohou ohrozit bezpečnost státu. Hybridní válka je v dokumentu obsažena v samostatném okruhu, přestože autoři sami zmiňují možnou propojenost v rámci ostatních kapitol (např. v rámci kapitol jako terorismus, hrozby v kyberprostoru atd.). Oproti tomu Strategie je prvním samostatným dokumentem v ČR, který se věnuje této tématice. Jedná se samozřejmě o logický sled událostí. Audit byl první dokument, který hybridní válku zmínil v českém prostředí, čímž ji zařadil mezi významné bezpečnostní hrozby. Vznik samostatného dokumentu pouze na téma hybridní války byl tedy logický krok.

Dokumenty se odlišují z hlediska svých cílů, což samozřejmě vede také ke změně v konceptualizaci. Ta je v Auditě více popisně zaměřená. Snaží se přesněji vymezit hrozbu, určit rizikové oblasti a odpovědné instituce společně s jejich nástroji. V textu jsou také zmíněny slabé a silné stránky, stejně jako budoucí doporučení. Konceptualizace je ve Strategii vůči samotné definici hybridní války daleko stručnější, například se nesnaží do tak velké míry identifikovat odpovědné instituce. Tento krok je samozřejmě logický a vyplývá z výše zmíněné návaznosti dokumentů. Strategie identifikuje strategické cíle, které



by se měla ČR snažit v budoucnu naplnit a také explicitně určuje možné způsoby jejich naplnění.

Z hlediska samotného chápání tématu hybridní války jsou oba dokumenty v některých směrech podobné. Jak již bylo zmíněno v předchozí kapitole, jak Audit, tak Strategie uvádějí tři pilíře, které se mohou stát terčem působení hybridní moci (ideově-hodnotové zakotvení společnosti a ústavněprávní uspořádání státu; ekonomika; bezpečnost a obrana). Stejně tak se celková definice příliš neodlišuje. Jedná se o zjevnou či skrytou činnost státního nebo nestátního aktéra, která se snaží ohrozit fungování právního státu a vnitřní bezpečnost, za použití širokého spektra nástrojů. Přesto se ale v hlubších definicích konceptualizace v některých směrech odlišují.

Rozdíl v dokumentech je v rámci určení aktérů, kteří jsou určeni jako původci hybridní války. Audit i Strategie oba určují, že původce může být jak státní, tak nestátní aktér, nicméně v konkrétních detailech se už liší. Audit je převážně psán z pozice preventivní, kdy hybridní válka je v dokumentu určena jako nový druh hrozby, který u nás může v budoucnu působit. Jako příklad státních aktérů je využita Ruská federace a její operace v roce 2014 na východní Ukrajině a Krymu. Stejně tak jsou zmíněny metody teroristické organizace Islámský stát, jelikož využívá hybridních nástrojů. Strategie tímto způsobem konkrétní aktéry neuvádí, nicméně určuje, že na ČR dlouhodobě a systematicky působí především autoritářské a revizionistické velmoci s regionálními či globálními mocenskými aspiracemi, pomocí nástrojů hybridní války.

V obou dokumentech je také zmíněno, že původce hybridní války může využívat nástroje ze sfér vlivu, tj. dimenzí moci DIMEFIL. V Auditě je tento název přesně zmíněn a u jednotlivých dimenzí jsou jmenovány konkrétní nástroje. Strategie vůbec název DIMEFIL nepoužívá, přesto jsou jednotlivé dimenze, které tato typologie zahrnuje v dokumentu jmenovány, spolu s dalšími nástroji. Tyto dimenze jsou pouze jmenovány, nejsou nijak konkrétně rozvedeny jako v Auditě, což může mít spíše souvislost s celkovou charakteristikou dokumentu, jelikož se více zaměřuje na strategické cíle, než na popis hrozby.

Jak již bylo zmíněno, v budoucnu vznikne v českém prostředí ještě akční plán, který bude na současnou konceptualizaci navazovat konkrétními opatřeními. Tento plán bude každoročně hodnocen a upravován.

## 3.2 Ideální konceptualizace

V rámci vytvoření vlastního řešení problému jsem vycházel z dokumentů významných mezinárodních organizací, kterých je ČR členem. Jednou z těchto organizací je Evropská Unie. V jejím případě se jednalo například o dokumenty *Závěry Rady EU o dalším úsilí za účelem posílení odolnosti a boji proti hybridním hrozbám z 10. prosince 2019* a *Společný rámec pro čelení hybridním hrozbám ze 7. dubna 2016*.

Druhou důležitou organizací pro ČR je NATO. V tomto případě jsem pracoval například s dokumenty jako *Komuniké z Varšavského summitu NATO 2016 z 9. července 2016* a *Odpověď NATO na hybridní hrozby z roku 2019*.

Mezi významné mezinárodní aktéry patří také Evropské centrum excelence pro čelení hybridním hrozbám, což je nezávislá organizace, která vznikla za podpory EU a NATO. Jejím hlavním cílem je zlepšit výkon členských států při prevenci a případnému boji s hybridní válkou. Toho je docíleno sdílením nejlepších praktik, testováním nových nápadů a přístupu a také vytvářením pomocných kurzů a cvičení, kterých se mohou členové zúčastnit. (What is Hybrid CoE, 2021). Česká republika se stala členem této organizace 21. května 2018 (Dates of accession for the Hybrid CoE Participating States, 2020). Mezi důležité dokumenty patří například *Klíčová témata a přístupy hybridního centra excelence pro čelení hybridním hrozbám v roce 2021* a *Zastrašování: návrh více strategického přístupu k čelení hybridních hrozeb*.

Jak již bylo zmíněno, role těchto organizací je víceméně podpůrná, a to jak v rámci prevence, tak případné obrany. V případě prevence slouží organizace jako platformy pro komunikaci mezi členskými státy, pro sdílení zkušeností při boji proti hybridní válce a také jako partneři pro pořádání kurzů a cvičení. V případě obrany je možné očekávat po napadení pomoc od ostatních členů organizací na různých úrovních, v závislosti na stylu útoku, a to včetně nasazení proti hybridním týmům NATO. Takové týmy už zasahovaly například v listopadu roku 2019 v Černé hoře (*Secretary General's Annual Report, 2019, s.29*).

Přesto je ale v rámci organizací kladena odpovědnost za vlastní obranu samotnému napadenému státu. Mimo jiné je i z tohoto důvodu doporučeno napříč organizacemi, aby každý stát pracoval s konceptem hybridní války sám, na své vlastní úrovni působnosti. Hybridní hrozby totiž využívají velkou škálu nástrojů a často jsou “šité na míru” pro daný

cíl. Vzhledem k různorodosti v infrastruktuře a geografii jednotlivých členských států by proto vypracování společné konceptualizace pro všechny bylo značně neefektivní řešení. (Hagelstam; Narinen, 2018). Proto by na národní úrovni měly existovat dokumenty, které zařazují téma hybridní války do bezpečnostních hrozeb pro ČR.

Vzhledem k tomu, že nástroje, které může využívat hybridní útočník jsou proměnlivé a dokážou se přizpůsobit napadenému cíli, je vhodné je definovat na národní úrovni. Konceptualizace by měla na základě systému a infrastruktury ČR přesně určit jaká hrozba státu hrozí, jaké sféry může ovlivnit a které instituce jsou při čelení hybridní válce zodpovědné. Stejně tak by měl být určen způsob, jakým bude s problémem vypořádáno.

Zároveň je vyžadována velká pružnost konceptualizace a možnost případné úpravy. Vzhledem k tomu, že je téma hybridní války úzce spjato s vývojem technologií, dá se očekávat, že bude v budoucnu potřeba přihlídnout k použití těchto nových nástrojů. Jedním z takových pokroků je například umělá inteligence (Rühle; Roberts, 2021). Je také třeba podotknout, že nové technologie mohou být novým nástrojem jak pro obránce, tak pro útočníka. V rámci jednotlivých mezinárodních organizací také neustále probíhají další výzkumy a analýzy, které mohou přinést nový pohled na tematiku hybridní války obecně. Z těchto dvou důvodů si myslím, že je vhodné, aby ideální konceptualizace nebyla pevně ukotvena, ale naopak by měla dovolovat v budoucnu implementovat změny, které ji lépe dovolí reagovat na nové nástroje hybridní války.

Dostatečná konceptualizace by měla určit konkrétní spojence, se kterými může ČR spolupracovat. Nejsilnější zbraní při obraně proti hybridním hrozbám je totiž znalost cílů a nástrojů hybridního útočníka. Individuální státy si kladou v tématu hybridní války podobné cíle, přičemž kolektivně jsou finanční a personální zásoby daleko větší, než samostatně. Proto je možnost sdílení nových poznatků a zkušeností klíčovým faktorem při cestě k úspěšné obraně.

Stejně tak by měl být určen potenciální nepřítel. Jmenovité určení těchto aktérů je samozřejmě nereálné, přesto ale může jejich typologický popis pomoci při identifikaci potenciálních nástrojů hybridní války, kterým může ČR čelit. Stejně tak může tato informace být nápomocná při určení politického zaměření ČR na mezinárodním poli.

U aktéra, snažícího se využívat nástrojů hybridní války lze předpokládat, že se bude snažit své opravdové, škodlivé cíle, skrýt za legitimními, a hlavně legálními cíli. Pro dosažení těchto cílů bude kombinovat nástroje z několika sfér a bude se snažit zmást napadený stát,

což je samotná podstata hybridní války. Stejně tak lze očekávat, že hybridní útočník může cílit právě na komunikační systém v rámci daného státu za cílem zefektivnit své aktivity na daném území. Pro potlačení efektů, které takové chování hybridního útočníka může mít, je nutné určit meziresortní komunikaci jako jeden z klíčových faktorů, při boji proti hybridní válce. V rámci komunikace je také důležité, aby v případě detekce hybridní války na svém území, byla ČR schopna efektivně komunikovat se spojenci, čímž by byla schopná využít jejich zásoby a infrastrukturu pro potlačení vlastních problémů.

Konceptualizace hybridní války ve strategických dokumentech by také měla zastrašovat a odradit potenciálního útočníka. Toho lze docílit různými způsoby. V první řadě je třeba uvést, že samotná existence bezpečnostní infrastruktury, věnující se tématu hybridní války, může tento požadavek naplnit. Útočníka může taková infrastruktura odradit, například tím, že mu zvýší náklady, které musí vynaložit na úspěšný útok. To může agresivního aktéra přimět nevykonat útok, jelikož jeho cena by převyšovala potenciální zisk z úspěšného provedení. Pro zastrašení hybridního útočníka je také nutné určit odpovědného aktéra nebo instituci, která v případě napadení dokáže vydat rozhodnutí o jeho potrestání. Také je třeba určit, jaké konkrétní tresty mohou být vykonány. Ve stejném duchu je třeba tento požadavek v některých případech naplňovat i v rámci solidarity v mezinárodním prostředí při napadení spojence.

Původce hybridní války může cílit mimo jiné i na samotnou společnost a občany státu pomocí různých nástrojů (například šíření dezinformací, propagandy, zastrašování pomocí teroristických útoků atd.). Takovým útokům lze předcházet, nicméně nelze předpokládat jejich naprostá eliminace, zejména díky neustálému vývoji nástrojů hybridní války. Proto je důležité, aby konceptualizace identifikovala snahu zlepšit odolnost společnosti jako jeden z důležitých faktorů při čelení hybridní válce. Společnost musí věřit, že je hybridní válka reálné téma, které může zasáhnout stát, ale které je zároveň řešeno příslušnými institucemi. Přesto je třeba adekvátně uvolňovat taktické informace. Ty mohou totiž sloužit i pro útočníka jako návod, kterého se může v rámci svého šíření hybridní války držet. Proto je třeba najít vyváženost v rámci uvolňování informací pro veřejnost.

Vzhledem k tomu, že hybridní válka může využívat nové nástroje, spojené s technologickým vývojem, je třeba na tuto skutečnost v konceptualizaci přihlídnout. Stejně tak je třeba vyvinout snahu o analýzu nových trendů v technologiích, například výše zmíněné umělé inteligence, ale také sociálních sítí a dalších. V rámci této analýzy by měly

být určeny potenciální hrozby, stejně jako slabé a silné stránky bezpečnostního systému v této oblasti. Nově vzniklé poznatky by měly být využity při přípravě dostatečné bezpečnostní politiky a v rámci mezinárodní spolupráce také sdíleny v příslušných platformách.

Ve výše uvedeném textu určuji, jak má dle mého názoru vypadat ideální konceptualizace hybridní války ve strategických dokumentech ČR. Tato ideální konceptualizace vychází z dokumentů, článků, závěrů a studií mezinárodních organizací (konkrétně jsou uvedeny na začátku kapitoly). Tyto dokumenty jsem analyzoval a vytvořil z nich daná kritéria. Pro lepší přehlednost a jednodušší práci v další kapitole jsem celkové požadavky shrnul do 8 bodů:

**Bod č. 1:** Konceptualizace musí existovat na národní úrovni;

**Bod č. 2:** Konceptualizace musí na základě struktury daného státu definovat hybridní hrozbu, odpovědné instituce a cíle, které je třeba naplnit;

**Bod č. 3:** Konceptualizace musí být flexibilní a dovolovat případné úpravy;

**Bod č. 4:** Konceptualizace musí identifikovat spojence a potenciální nepřátele;

**Bod č. 5:** Konceptualizace musí identifikovat meziresortní komunikaci jako klíčový faktor pro čelení hybridní válce;

**Bod č. 6:** Konceptualizace musí zastrášovat hybridní útočníky;

**Bod č. 7:** Konceptualizace musí identifikovat odolnou společnost jako jeden z důležitých prvků pro čelení hybridní válce;

**Bod č. 8:** Konceptualizace musí identifikovat nové technologie jako hybridní nástroj.

### **3.3 Konceptualizace v českých dokumentech**

V této kapitole se pokusím analyzovat, zda je konceptualizace hybridní války v českých dokumentech vhodná pro vznik dostatečné bezpečnostní politiky. Toho docílím porovnáním výše uvedených bodů ideální konceptualizace s konceptualizacemi, které jsou uvedeny v Auditě a Strategii. Kromě porovnání také u jednotlivých bodů zmiňuji, jaké cíle si v dané oblasti strategické dokumenty kladou do budoucna. Cílem této informace je ukázat, jak konkrétně bude s jednotlivými body pracováno v budoucnu a do určité míry vyhodnotit, zda je toto zaměření v souladu s mezinárodními organizacemi.

### **Bod č. 1: Konceptualizace musí existovat na národní úrovni**

V současnosti existují v ČR dva strategické dokumenty, které se věnují tématu hybridní války. V budoucnu má ještě vzniknout akční plán, který bude přinášet do tematiky konkrétní opatření. U tohoto bodu není třeba žádně vést dlouhou diskusi, v rámci strategických dokumentů ČR je splněn.

### **Bod č. 2: Konceptualizace musí na základě struktury daného státu definovat hybridní hrozbu, odpovědné instituce a cíle, které je třeba naplnit**

Oba strategické dokumenty ČR vytvářejí snahu v různé míře tento bod naplnit. Jak již bylo zmíněno v kapitole “Vývoj konceptualizace v dokumentech ČR”, Audit je více zaměřený na přesný popis hrozby a určení odpovědných institucí, zatímco Strategie spíše zmiňuje konkrétní cíle, které by měly být naplněny. Rozdílnost dokumentů samozřejmě není negativní bod, vzhledem k tomu, že na sebe navazují a Strategie sama vznikla na základě jednoho z cílů, které Audit určil. Ve výsledku je ale bod tento vzhledem k povaze dokumentů splněn v plné míře.

### **Bod č. 3: Konceptualizace musí být flexibilní a dovolovat případné úpravy**

Strategie tento požadavek splňuje, jelikož předpokládá, že bude třeba implementovat úpravy, proto bude dokument často aktualizován v závislosti na mezinárodním i národním vývoji z hlediska bezpečnostní politiky. Jak již bylo zmíněno, na strategii bude navazovat připravovaný akční plán, který bude každoročně hodnocen a upravován na základě potřeby.

### **Bod č. 4: Konceptualizace musí identifikovat spojence a potenciální nepřátele**

Ve strategických dokumentech ČR jsou zmíněny mezinárodní organizace EU a NATO jako spojenci při čelení hybridní válce. Je zdůrazněno, že pro budoucnost v oblasti bezpečnostní politiky je třeba roli ČR v těchto organizacích prohlubovat, ať už přispíváním ke kolektivní obranné schopnosti, tak ke sběru informací. Stejně tak je uvedeno, že ČR je připravena v rámci solidarity a jednoty napříč EU a NATO podpořit jakýkoliv spojenecký stát v případě napadení hybridní válkou, což může útočníka odradit.

Oba dokumenty zmiňují, že ČR může čelit hybridní válce od státních či nestátních aktérů. Audit se konkrétním určením těchto aktérů nevěnuje, pouze dává při popisu hrozby příklady státních aktérů, kteří používali nástroje hybridní války v minulosti. Oproti tomu Strategie určuje, že ČR čelí hybridní válce dlouhodobě od autoritářských a

revizionistických velmocí. V rámci určení konkrétních cílů dodává, že by ČR měla snižovat svou závislost na státech s odlišnou ideově-hodnotovou orientací. Tento bod je tedy v dokumentech splněn.

**Bod č. 5: Konceptualizace musí identifikovat meziresortní komunikaci jako klíčový faktor pro čelení hybridní válce**

Strategické dokumenty ČR obecně tento požadavek identifikují a určují, že je třeba se s ním zabývat, aby bylo pokryto celé spektrum nástrojů hybridní války. Zlepšení odolnosti vůči případnému napadení je také určeno jako jeden z důležitých faktorů, pro posílení bezpečnostního systému ČR. Za cílem lepšího čelení hybridní válce budou v ČR vylepšeny současné způsoby pro sdílení informací napříč resorty, zejména v rámci Bezpečnostní rady státu. Se stejným cílem vznikne z Úřadu vlády funkce koordinátory agendy pro čelení hybridnímu působení. Dá se očekávat, že zlepšení efektivity těchto úřadů zlepší taktéž možnost komunikace a koordinace s NATO a EU v případě napadení, přesto se ale nejedná o explicitně stanovený cíl těchto kroků. Zlepšení komunikace s těmito organizacemi není přesně určeno jako jeden z klíčových faktorů pro čelení hybridní válce. Je zmíněno, že je třeba roli ČR v nich prohlubovat, ale snaha posílit odolnost komunikace s nimi už ne. To je rozhodně škoda, zejména díky kapacitám a nástrojům, které tyto organizace nabízejí a které by mohly pomoci v případě napadení ČR (například již zmíněné proti hybridní týmy NATO).

**Bod č. 6: Konceptualizace musí zastrašovat hybridní útočníky**

Jak již bylo uvedeno výše, samotná existence strategických dokumentů může být chápána jako jeden ze způsobů, jak zastrašit hybridního útočníka ukázkou připravenosti pro jeho detekci a potrestání. V rámci tohoto bodu je v dokumentech určena Vláda ČR jako orgán, který má veřejně určit hybridního útočníka, což je bráno jako politické rozhodnutí, za které tento orgán taktéž přebírá zodpovědnost. Identifikovány jsou potenciální tresty pro tohoto aktéra. Tyto tresty mohou zahrnovat sankce, ale také vyhoštění diplomatů. Také je uvedeno, že ČR je připravena tyto akce vykonat v případě napadení spojence v rámci solidarity. Strategické dokumenty tedy tento požadavek identifikují a snaží se ho naplnit.

**Bod č. 7: Konceptualizace musí identifikovat odolnou společnost jako jeden z důležitých prvků pro čelení hybridní válce.**

Identifikace společnosti jako oblasti, která může být zasažena hybridními útoky a jejíž

odolnost je třeba posilovat, je provedeno v obou dokumentech. Nicméně je uvedeno, že její posílení je dlouhodobý proces, který nezahrnuje pouze bezpečnostní aktéry ČR, ale také například celý vzdělávací systém ČR (Audit, 2016, str. 132). Samotný vznik obou dokumentů lze pak do určité míry chápat jako snahu informovat společnost (přičemž informovanost může sama posílit odolnost) o existenci a detailnějším popisu hybridní války, což je ostatně i uvedeno jako jeden z cílů dokumentu (Audit, 2016, str. 8). Nicméně nelze předpokládat, že si občané ČR budou číst strategické dokumenty ČR nebo vůbec vědět o jejich přesném zaměření, proto je potřeba cílit spíše do mediálního a veřejného prostoru. I z tohoto důvodu vznikne v ČR systém strategické komunikace, jehož cílem bude konkrétně, efektivně a včasné informovat veřejnost a další typy cílového publika na téma hybridní války. Ve stejném duchu budou probíhat akce a vzdělávací programy, které se budou snažit systematicky zvýšit znalosti o tématické ve společnosti. (Strategie, 2021, str. 8). Posoudit, zda konceptualizace poskytuje vhodné informace, které nebudou sloužit jako návod pro hybridního útočníka je bohužel nemožné, jelikož je velká část informací klasifikovaných. Nicméně lze přihlídnout k faktu, že Audit sám zmiňuje nutnost vyváženosti v této oblasti (Audit, 2016, str. 8), což je pozitivní trend.

Jeden z nástrojů, který je v rámci dokumentů v mezinárodních organizacích zmiňován, je šíření dezinformací (*Společný rámec pro boj proti hybridním hrozbám - Reakce Evropské Unie, 2016; Závěry Rady EU o dalším úsilí za účelem posílení odolnosti a boji proti hybridním hrozbám, 2019*). Dezinformační kampaně jsou ve strategických dokumentech ČR uvedeny jako potenciální nástroj hybridní války, přesto ale nevzniká jednoznačná snaha pro jejich potlačení na území ČR. Kupříkladu NATO zřídilo vlastní stránku (*Setting the record straight*), ve které se snaží reagovat na dezinformace ohledně jejího vztahu k Ruské federaci pravdivými fakty, které vyvracejí dezinformace. Tato stránka je dostupná ve více jazycích, ke kterým bohužel čeština nepatří. Proto si myslím, že obdobná stránka, snažící se vyvracet dezinformace spojené s hybridní válkou v českém prostředí, by mohla v naplnění tohoto požadavku pomoci. Takzvané fact-checking weby už na našem území existují, ale převážně se jedná o nezávislé projekty, které nespádají pod bezpečnostní infrastrukturu.

Obecně panuje v akademickém prostředí pragmatismus vůči pojmu hybridní válka. Tento pragmatismus vychází z trendu, kdy byl koncept užíván s postranními úmysly, které nejsou spojeny s analytickým účelem konceptu. Kupříkladu v ČR může být pojem hybridní válka



používán jako synonymum pro informační válku nebo jako slogan pro členění putinovskému Rusku (Daniel; Eberle, 2018). Zároveň není obsah konceptu přesně vymezen a různí autoři se v definicích liší, což samo pragmatismu nahrává. (Bahenský, 2018, str. 96). Tento trend může negativně ovlivnit vnímání pojmu v české společnosti. Samozřejmě je nepřijatelné, aby probíhala jakákoliv cenzura proti akademikům v tématu hybridní války, přesto ale lze předpokládat, že vystupování pragmatiků vůči hybridní válce v médiích může podkopávat snahu o zlepšení povědomí o tématice. Proto si myslím, že by konceptualizace měla snahu o zlepšení informovanosti společnosti rámovat tak, aby nebyl tento akademický pragmatismus skrýván nebo zatajován. Naopak by ho konceptualizace mohla zdůraznit, ale zároveň podotknout, že i přes široký rozsah akademických definicí a diskusí je tento problém pevně ukotven v bezpečnostních dokumentech a systém je na ně připraven reagovat.

Obecně je tedy tento bod ve strategických dokumentech naplněn, ale v rámci své práce bych chtěl pouze zmínit, že zatímco předchozí body jsou naplněny (tj. prvky hybridní války jsou identifikovány), jejich rozšíření a práce s nimi v budoucnu ve strategických cílech je taktéž v souladu s přístupem v mezinárodních organizacích. Tento trend se do takové míry neprojevuje v tomto bodu, zejména pak co se týče identifikace dezinformací jako nástrojů hybridní války.

#### **Bod č. 8: Konceptualizace musí identifikovat nové technologie jako hybridní nástroj**

Strategické dokumenty ČR uvádějí, že vývoj moderních technologií vytváří pro bezpečnostní systém nové zranitelnosti a hrozby, které je třeba omezit). Přesto není v těchto konceptuálních dokumentech uveden žádný cíl, který by zadával nutnost studie těchto nových technologií. V této oblasti se dá předpokládat zisk nových informací v rámci mezinárodních organizací, nicméně ČR nemůže pouze spoléhat na studie ze zahraničí, musí vyvinout snahu o vlastní analýzy a studie, mimo jiné i díky bodům 2 a 4 (tj. zisk informací o vlastní zranitelnosti a přispívání do kolektivní informační spolupráce na mezinárodním poli). Proto si myslím, že by konceptualizace měla zahrnovat i snahu o zisk nových informací v tomto poli, například financováním nových studií na toto téma nebo vznikem vlastních expertních týmů, zaměřujících se na tuto tematiku. Bod je tedy splněn, tj. nové technologie jsou identifikovány jako hybridní nástroje, ale stejně jako v případě 7. bodu není přesně s tematikou pracováno ve výhledu do budoucna.

# Závěr

V mé bakalářské práci jsem se zabýval konceptualizací hybridní války na území ČR, kdy jsem popsal její zpracování ve strategických dokumentech. Studium a popisem těchto dokumentů jsem chtěl získat odpověď na dvě výzkumné otázky, které jsem zadal na začátku práce. První z nich zkoumá, jak se vyvíjela konceptualizace na území ČR. Druhá se poté zajímá o to, jestli lze na základě této konceptualizace vytvořit dostatečnou bezpečnostní politiku, pro potlačení hybridní války.

Celkový vývoj konceptualizace hybridní války v oficiálních dokumentech ČR začal *Auditem národní bezpečnosti* v roce 2016 a pokračoval *Národní strategií pro čelení hybridnímu působení* v roce 2021. Dokumenty na sebe navazují a jsou propojeny, přesto v jejich konceptualizaci existují změny v rámci chápání tématu hybridní války. Tento trend je možné spojit s celkovým vývojem tématu v mezinárodním prostředí, tj. nové dokumenty v rámci NATO, EU a Evropského centra excelence pro čelení hybridním hrozbám. Nové poznatky a doporučení v tématu hybridní války, které se zrodily v pětiletém mezeře mezi vznikem obou českých dokumentů, jsou tedy pouze reflektovány ve Strategii. Stejně tak je vhodné zmínit, že se konceptualizace v určitých oblastech nepřekrývají. Konceptualizace Auditů je více zaměřená na popis odpovědných institucí při čelení hybridní válce a popisu jejich nástrojů, zatímco konceptualizace Strategie odpovědné instituce takřka nezmiňuje, jelikož je více zaměřená na určení strategických cílů pro budoucí vývoj bezpečnostní politiky ČR. To je určitě pozitivní vlastnost konceptualizací, jelikož mají fungovat propojeně, tudíž není třeba, aby se v každém z nich objevovaly stejné informace. V budoucnu bude vývoj konceptualizace hybridní války v českém prostředí určitě pokračovat. Strategie sama počítá s možnou aktualizací na základě vývoje v národním a mezinárodním prostředí. Stejně tak je počítáno s akčním plánem, který bude na Strategii navazovat konkrétními opatřeními a kroky.

Pro odpověď na druhou otázku jsem vytvořil na základě konceptualizací v mezinárodních organizacích (NATO, EU, Evropské centrum excelence) vhodné vlastnosti národní konceptualizace a snažil se je aplikovat na strategické dokumenty ČR. Tyto vlastnosti jsou v Auditě a Strategii ve velké míře naplněny. Konceptualizace ve strategických dokumentech identifikuje stejné oblasti, které jsem vytvořil na základě dokumentů mezinárodních organizací a je s nimi v souladu. Ve výsledku jsem tedy zjistil, že na

základě konceptualizace ve strategických dokumentech ČR lze vytvořit dostatečnou bezpečnostní politiku pro potlačení hybridní hrozby.

Přesto v práci identifikuji oblasti, které se dají zlepšit. Konkrétně nejsou v rámci posílení odolnosti společnosti vůči hybridní válce určeny konkrétní způsoby a cíle, kterými bude ČR reagovat na dezinformační kampaně. Stejně tak není ve strategických cílech určeno, jak (či vůbec) bude probíhat studium a analýza nových technologií jako nástrojů hybridní války. Tyto oblasti jsou sice v konceptualizaci identifikovány jako klíčové pro čelení hybridní válce, ale nenavazují na ně konkrétní kroky. Úprava konceptualizace v těchto oblastech může mít, dle mého názoru, pozitivní přínos pro bezpečnost ČR a celkovou akceschopnost při čelení hybridní válce.

Závěrem bych chtěl podotknout, že je třeba neusnout na vavřínech. Vzhledem k povaze hybridní války lze očekávat vývoj a vznik nových hrozeb, kterým bude ČR čelit. Jejich kompletní eliminace je nepravděpodobná, proto je třeba kontinuálně posilovat bezpečnostní systém v rámci zlepšení odolnosti, ale i včasné reakce. Naštěstí s tímto faktem konceptualizace počítá a já doufám, že tomu tak zůstane i v budoucnu.

Téma hybridní války je v různých kontextech poměrně diskutované v rámci ČR. Proto jsem se na něj chtěl ve své bakalářské práci zaměřit na národní úrovni. Věřím, že po přečtení této práce by mohl být způsob zpracování konceptualizace ve strategických dokumentech ČR jasnější a přehlednější.

## Summary

In my bachelor thesis, I studied conceptualization of hybrid warfare in czech environment, where I described it's details in strategic documents. By studying and describing these documents, I wanted to get answers to two research questions, which I specified at the start of this work. First of which examines how the conceptualization in czech environment evolved. The second one examines if it is possible to create adequate security policy based on this concept of hybrid warfare.

Evolvment of conceptualization of hybrid warfare in official documents of Czechia started with *Audit národní bezpečnosti* in 2016 and continued with *Národní strategií pro čelení hybridnímu působení* in 2021. Documents are continuous works and are intertwined, despite this, there are differences in their conceptualization of hybrid warfare. This trend is

connected to the overall evolution of the hybrid warfare theme in the international field, as in new documents, created on the level of NATO, EU and The European Centre of Excellence for Countering Hybrid Threats. New findings and recommendations in this field, which were created in the space of five years, are just reflected in the Strategy. At the same time, it is worth mentioning that conceptualizations are not always the same. Conceptualization in Audit is more focused on describing responsible institutions in facing hybrid warfare, as well as describing their tools, whereas conceptualization of Strategy almost doesn't describe responsible institutions. It is more focused on establishing strategic goals, which are important for the future of Czechia. That is definitely a positive quality of these conceptualizations, as they are supposed to work coherently, so it is not necessary for them to include the same information. In the future, the development of the conceptualization of hybrid warfare in Czech environment will definitely continue. Strategy itself is expecting new updates, based on development in the international field. It is also accounting for akční plán, which will create specific steps to follow.

To find the answer to the second research question, I specified appropriate qualities that conceptualization of hybrid warfare should have on state level, based on conceptualization that is used in international organizations. I then tried to apply it to the strategic documents. These qualities are met in Audit and Strategy. Conceptualization in strategic documents identifies the same areas that I created based on documents of international organizations and is working on them. In the end I found out that it is indeed possible to create adequate security policy for facing hybrid threats, based on conceptualization, which is used in strategic documents of Czechia.

At the same time, this thesis identifies areas, which could be improved. More specifically, in improving the endurance and toughness of society in facing the hybrid threats, there are no specific goals set in reaction to disinformation campaigns. In the same way, there are no strategic goals set for studying and analyzing new technologies as tools of hybrid warfare. These areas are identified as key for facing hybrid warfare, but are not followed with more specific steps. Improving conceptualization in these areas could, in my opinion, have a positive effect for improving the security of Czechia.

In the end, I would like to mention that it is important not to rest on one's laurels. Based on the concept of hybrid warfare, we can expect the creation of new threats that the Czechia will need to face. It is unlikely that they will be completely eliminated, which is why it is

necessary to improve czech security system. Thankfully, conceptualization accounts for this, and I only hope that it will continue to do so in the future.

The theme of hybrid warfare is discussed in different contexts in Czechia. Which is why I wanted to focus on it on a national level in this thesis. I believe that after reading this thesis, the understanding of conceptualization in strategic documents of Czechia becomes clearer and better for the reader.

# Použitá literatura

1. *Audit národní bezpečnosti*. In.: Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality, 2016. Dostupné také z: <https://www.vlada.cz/cz/media-centrum/aktualne/audit-narodni-bezpecnosti151410/>
2. BAHENSKÝ, Vojtěch. *Hybrid Warfare, Wars, and Threats: A Conceptual Analysis*. Praha, 2016. Diplomová práce. Univerzita Karlova, Fakulta sociálních věd. Vedoucí práce Jan Kofroň.
3. BAHENSKÝ, Vojtěch. PARADOX HYBRIDNÍ VÁLKY: O příčinách a následcích pragmatismu v debatě. *Obrana a Strategie* [online]. University of Defence, 2018, (2), 089-100 [cit. 2021-7-25].doi:10.3849/1802-7199.18.2018.02.089-100 Dostupné z: <https://www.obranaastrategie.cz/en/archive/volume-2018/2-2018/articles/paradox-of-hybrid-war.html>
4. ČESKÁ REPUBLIKA *Nářízení vlády č. 432/2010 Sb.: o kriteriích pro určení prvku kritické infrastruktury*. 2010.
5. *Další úsilí za účelem posílení odolnosti a boje proti hybridním hrozbám – závěry Rady* [online]. In.: Brusel, 10. prosince 2019. [cit. 2021-7-25]. Dostupné také z: <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/cs/pdf>
6. DANIEL, Jan – Jakub, EBERLE. *Hybrid Warriors: Transforming Czech Security through the ‘Russian Hybrid Warfare’ Assemblage*. Sociologický časopis. Přijato k publikaci.
7. FAJNOR, Jakub. *Vláda schválila Národní strategii pro čelení hybridnímu působení*. Ministerstvo obrany ČR [online]. 19. dubna 2021 [cit. 2021-5-25]. Dostupné z: <https://www.mocr.army.cz/informacni-servis/zpravodajstvi/vlada-schvalila-narodni-strategii-pro-celeni-hybridnimu-pusobeni-227120/>
8. GRAY, Colin S. *Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional*. Strategic Studies Institute, U.S. Army War College, Carlisle. 2012. ISBN 1-58487-520-8.
9. HAGELSTAM, Axel a Kirsti NARINEN. *Cooperating to counter hybrid threats* [online]. In: . NATO Review, 23. 11. 2018. [cit. 2021-7-25]. Dostupné z: <https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter->

- [hybrid-threats/index.html](#)
10. HENDL, Jan. Kvalitativní výzkum: základní metody a aplikace. Praha: Portál, 2005, 408 s. ISBN 80-7367-040-2-303.
  11. HOFFMAN, Frank. G, Conflict in the 21st Century: The Rise of Hybrid Wars [online]. Arlington, Virginia: Potomac Institute for Policy Studies, 2007 [cit. 2021-7-25]. Dostupné z: [https://www.potomacinstitute.org/images/stories/publications/potomac\\_hybridwar\\_0108.pdf](https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf)
  12. HOFFMAN, Frank G. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. Strategic Forum. 2009. No. 240
  13. Hybrid CoE: Dates of accession for the Hybrid CoE Participating States [online]. Helsinki: The European Center of Excellence for Countering Hybrid Threats. [cit. 2021-7-25]. Dostupné také z: <https://www.hybridcoe.fi/wp-content/uploads/2020/09/Dates-of-accession-for-the-Hybrid-CoE-Participating-States-03082020.pdf>
  14. *Hybrid CoE: Hybrid threats as a concept* [online]. Helsinki: The European Center of Excellence for Countering Hybrid Threats. [cit. 2021-7-25]. Dostupné také z: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>
  15. *Hybrid CoE's key themes and approaches to countering hybrid threats in 2021*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2021. [cit. 2021-7-25]. Dostupné z: [https://www.hybridcoe.fi/wp-content/uploads/2021/04/Workplan2021\\_summary\\_rgb.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/04/Workplan2021_summary_rgb.pdf)
  16. *Hybrid CoE: What is Hybrid CoE* [online]. Helsinki: The European Center of Excellence for Countering Hybrid Threats. [cit. 2021-7-25]. Dostupné také z: <https://www.hybridcoe.fi/who-what-and-how/>
  17. KERŠANKAS, Vytautas. *DETERRENCE: Proposing a more strategic approach to countering hybrid threats: Hybrid CoE* [online]. , 23. [cit. 2021-7-25]. Dostupné z: [https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence\\_public.pdf](https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf)
  18. NATO Summit Warsaw 2016: Warsaw Summit Communiqué. *NATO* [online]. Varšava, 2016. [cit. 2021-7-25]. Dostupné z: [https://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en)
  19. *NATO's response to hybrid threats* [online]. nato.int, 2019 . [cit. 2021-7-25]. Dostupné z: [https://www.nato.int/cps/en/natohq/topics\\_156338.htm](https://www.nato.int/cps/en/natohq/topics_156338.htm)

20. *Národní strategie pro čelení hybridnímu působení* [online]. Praha: Ministerstvo obrany, 2021. [cit. 2021-7-25]. Dostupné z: <https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf>
21. *Secretary General's Annual Report 2019* [online]. In: . Brusel: NATO, s. 128. [cit. 2021-7-25]. Dostupné z: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/3/pdf\\_publications/sgar19-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf)
22. *Setting the record straight: NATO - Russia* [online]. [cit. 2021-7-26]. Dostupné z: <https://www.nato.int/cps/en/natohq/115204.htm>
23. SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ Společný rámec pro boj proti hybridním hrozbám Reakce Evropské unie [online]. eur-lex.europa.eu, 6.4.2016 [cit. 2021-7-25]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52016JC0018&from=en>
24. RÜHLE, Michael a Clare ROBERTS. *Enlarging NATO's toolbox to counter hybrid threats* [online]. In: . NATO Review, 19. 3. 2021 [cit. 2021-7-1]. Dostupné z: <https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>