Recenzovaný článek

Aktuální přístupy České republiky, EU a NATO k hybridním hrozbám

Current Approaches of the Czech Republic, the EU and NATO to Hybrid Threats

Martin Havlík

Abstrakt: Článek pojednává o aktuálním přístupu České republiky k fenoménu hybridních hrozeb a analyzuje zásadní nedostatky determinující efektivní čelení těmto hrozbám. V rámci komplexního přístupu je text doplněn o současný pohled Evropské unie a NATO k řešení problematiky hybridního působení nepřátelských aktérů. Shrnující komparace přístupů České republiky, Evropské unie a NATO poukazuje na nutnost vzájemné institucionální synergie mezi těmito subjekty. Jakkoliv jsou současné přístupy zmíněných subjektů poměrně dostatečně doktrinálně ukotveny, nadále přetrvává absence komplexního a zejména prakticky fungujícího aparátu a konkrétních operativních nástrojů, které by dokázaly čelit širokému spektru hybridních hrozeb.

Abstract: The article discusses the current approach of the Czech Republic to the phenomenon of hybrid threats and analyses the fundamental shortcomings that determine the effective management of these threats. As part of a comprehensive approach, the text is supplemented by the current view of the European Union and NATO on addressing the issue of hybrid action by hostile actors. A summary comparison of the approaches of the Czech Republic, the European Union and NATO points to the need for mutual institutional synergy among these entities. Although the current approaches of the mentioned subjects are relatively sufficiently doctrinally anchored, the absence of a complex and especially practically functioning apparatus and specific operational tools that would be able to face a wide range of hybrid threats persists.

Klíčová slova: hybrid; hrozba; aktér; komplexní přístup.

Key words: Hybrid; Threat; Actor; Comprehensive Approach.

ÚVOD

Problematika čelení hybridnímu působení a hybridním hrozbám či oblast hybridního válčení je velmi rozsáhlá. Často záleží na perspektivě a konkrétním postoji jednotlivých expertů, akademiků či politických autorit, jakým prizmatem na danou problematiku nahlížet. Signifikantní a určující roli hraje v této souvislosti volba a identifikace referenčního objektu a neopomenutelně taktéž určitá reflexe vlastní lokace.

Cílem článku je provedení základní analýzy přístupu České republiky k problematice hybridních hrozeb, neboť oblast čelení hybridnímu působení a souvisejícím hrozbám nabývá postupně na významu, a to nejen v rámci naší republiky, ale také na úrovni společenství typu Evropské unie a NATO. S ohledem na požadovanou synergii v přístupech bude obsah doplněn také o základní komparaci přístupů Evropské unie a NATO.

Tento článek reflektuje pohled autora, který určitým způsobem předpokládá znalost aktéra hybridního působení a snaží se pouze rozklíčovat, jaké budou tímto aktérem použity hybridní prostředky. Záměrně je upozaděn fundamentální problém hybridu determinující současné dění v bezpečnostním prostředí (často podprahového charakteru).

1 METODOLOGIE A VÝZKUMNÉ OTÁZKY

Metodologie zpracování

Při zpracování toho článku byl využit kvalitativní výzkum, který hledá vysvětlující a generalizující kauzální mechanismy a souvislosti, než by umožnily zobecnění souvisejících zákonitostí.[1] Z praktické perspektivy je tak tento zvolený typ výzkumu vhodnější, neboť umožňuje validnější analýzu bezpečnostních aspektů v rámci zvoleného tématu zapadajícího do oblasti mezinárodních vztahů. Kvantitativní přístup výzkumu zvoleného tématu není úplně vhodný, neboť ke zkoumanému problému nejsou dostupné relevantní strukturální indikátory či jiné ukazatele, statistiky a průzkumy veřejného mínění, které by umožnily validně posoudit aktuální stav, či provést objektivní kvantitativní porovnání. Důraz byl položen na analýzu nejvýznamnější literatury, strategických dokumentů a nalezení hodnotících kritérií, kdy klíčovou roli hraje analýza empirie, tedy zkušenost získaná cílevědomým pozorováním.

Argumentační rámec hodnotící současný stav přístupů České republiky, EU a NATO k řešení hybridních hrozeb byl analyzován a podložen výsledky vlastního pozorování a expertních konzultací provedených v minulosti s cílem abstrahovat nepodstatné a okrajové skutečnosti.

Konkrétní přístupy čelení hybridnímu působení a hybridním hrozbám je vhodné vždy vztahovat a posuzovat k vybranému referenčnímu objektu. Pro potřeby tohoto článku byla za stěžejní referenční objekt zvolena Česká republika se svými zájmy. Je potřeba

1 DRULÁK, Petr. *Jak zkoumat politiku: kvalitativní metodologie v politologii a mezinárodních vztazích.* Praha, Portál, 2008. ISBN 978-80-7367-385-7. 256 s.

reflektovat, že následující exkurz není vše-popisným vysvětlením založeným na zevrubné analytické a výzkumné činnosti.

Definice výzkumných otázek

- Jaké jsou hlavní nedostatky a mezery v přístupu České republiky k čelení hybridním hrozbám a hybridnímu působení ze strany státních i nestátních aktérů?
- Jaké jsou rozdíly mezi přístupem České republiky, Evropské unie a NATO k čelení hybridním hrozbám a hybridnímu působení ze strany státních i nestátních aktérů?

Omezující podmínky

Při posuzování, oponování a kritice věcného obsahu i komplexního rámce je nutné reflektovat omezující podmínky a základní východiska, které reálně limitují míru detailu interpretovaných faktů, argumentačního rámce i zkoumaných údajů. Jedná se zejména o citlivost tématu a s ní související omezený zdrojový rámec, ze kterého jsou vyloučeny všechny citlivé a klasifikované utajované informace, a to podle Zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.[2]

2 PROBLEMATIKA PŘÍSTUPU PROTI HYBRIDNÍMU PŮSOBENÍ

Problematika čelení hybridnímu působení generuje několik základních variant možného přístupu. Za nejvhodnější lze považovat komplexní systémový přístup, označovaný v zahraniční literatuře jako tzv. *Comprehensive Approach*, který řeší všechny podstatné záležitosti související s problematikou čelení hybridnímu působení a hybridním hrozbám. Tento přístup popisuje společné využití veškerých dostupných nástrojů a politik z celého existujícího spektra moci, a to s cílem čelit hybridnímu působení, aktivitám a hrozbám nejrůznějších aktérů. Lze zmínit zejména nástroje diplomacie, bezpečnosti, obrany, ekonomiky apod.[3] Je zásadní chápat propojení veškeré oblasti fungování státu a společnosti, stejně jako nástroje hybridního působení. K zajištění bezpečnosti je z toho důvodu potřeba přistoupit z pohledu celé společnosti[4] a reflektovat toto vzájemné provázání. Komplexní přístup lze považovat za nejvhodnější, ačkoliv je poměrně zdrojově náročný a vyžaduje značnou fundovanost i záběr participantů. V případě bezpečnostních hrozeb a působení hybridního charakteru může komplexní přístup zahrnovat jak analýzu operačního prostředí, tak i analýzu protivníka, analýzu vlastní situace, analýzu možných variant činnosti protivníka i vlastní činnosti, analýzu řízení stěžejných relevantních rizik

2 Včetně Přílohy č. 5 k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.

3 BAUEROVÁ, Helena, HLAVÁČKOVÁ, Hana, VOŠTA, Milan. *Vnitřní a vnější dimenze bezpečnosti Evropské unie.* Nakladatelství Libri, Praha, 2018. ISBN 978-80-7277-576-7. Str. 31.

4 Takzvaný *Whole of Society Approach.*

a v neposlední řadě taktéž výběr optimální varianty vlastní činnosti zaměřené na eliminaci existující hybridní hrozby či hrozeb.[5]

Zásadními důvody pro implementaci komplexního přístup jsou především:

- častá přímá i nepřímá provázanost původně oddělených hrozeb;
- stírání rozdílů mezi vojenskými, nevojenskými, vnitřními a vnějšími hrozbami;
- působení hrozeb na referenční objekty překrývající hranici mikro a makro-okolí vnějšího prostředí či vnitřního prostředí organizace nebo aktéra;
- využívaní širšího spektra dostupných operačních domén (dimenzí)[6];
- využívaní širokého spektra nejrůznějších nástrojů moci;
- růst míry zapojení nestátních a proxy státních aktérů v bezpečnostních konfliktech;
- značný význam asymetrického způsobu boje a asymetrie při vedení konfliktů;
- existence sekundárních a terciálních hrozeb, migrace či mezietnického násilí atd.

Rostoucí význam komplexního přístupu zmiňuje také *Bezpečnostní strategie České republiky* z roku 2015, kde je tento přístup představen jako kombinace vojenských a civilních nástrojů, včetně diplomatických, právních a ekonomických prostředků k předcházení hrozeb a zmírnění jejich negativních vlivů. V kontextu posilujícího významu komplexního přístupu se zvyšují také nároky na připravenost včasně a efektivně reagovat na nenadálé hrozby.[7]

Mezi další významné přístupy patří především obranný pasivní přístup zahrnující systematické a nepřetržité monitorování, vyhodnocování hybridních aktivit protivníka a také posilování vlastní odolnosti (Resilience). Naproti tomu lze postavit přístup aktivní útočný reprezentovaný velmi často vedením vlastní propagandy, strategické komunikace, kybernetických a informačních operací, a celé řady dalších aktivit pro odstrašení (Deterrence), včetně demonstrace vojenské síly. Vzájemnou kombinací těchto přístupů lze logicky dosáhnout nejefektivnějšího přístupu v čelení hybridnímu působení a hrozbám.[8] Aktivní, pasivní a kombinované přístupy vždy korespondují se zájmy konkrétního aktéra bránit se cizím vlivům a snaze o prosazení cizích zájmů na svém teritoriu či v oblasti svého výlučného zájmu.[9]

---

5 HAVLÍK, Martin. *Fenomén hybridního působení státních i nestátních aktérů.* Rigorózní práce. Univerzita Karlova, Praha, 2021. Vedoucí práce prof. PhDr. RNDr. Nikola HYNEK, M.A., Ph.D. Str. 88.

6 Od roku 2016 nově v prostředí NATO akceptovaného kybernetického prostoru jako další operační domény a od konce roku 2019 také blízkého vesmíru jako aktuálně poslední operační domény.

7 Kolektiv autorů pod vedením Ministerstva zahraničních věcí. *Bezpečnostní strategie České republiky 2015.* Ministerstvo zahraničních věcí České republik, Praha. ISBN 978-80-7441-005-5. Str. 8. [online]. 2015 [cit. 2021-12-29]. Dostupné z: https://1url.cz/Ft2Hp

8 Viz Havlík, ref. 3, str. 89 – 90.

9 Ibidem, str. 90 - 91.

3 PŘÍSTUP ČESKÉ REPUBLIKY PROTI HYBRIDNÍMU PŮSOBENÍ

První explicitní zmínky o přístupu České republiky k čelení hybridním hrozbám (obecně hybridnímu působení) lze časově zasadit do období formulace obsahu strategického dokumentu *Audit národní bezpečnosti* z roku 2016, kde do širšího spektra nejvýznamnějších aktuálních hrozeb pro Českou republiku byly zakomponovány konkrétně i hybridní hrozby a jejich vliv na bezpečnost občanů České republiky.

Ve zmiňovaném *Auditu národní bezpečnosti* byly související hybridní hrozby vůči České republice rozděleny do tří klíčových oblastí, které zahrnují: působení proti soudržnosti a ideově-hodnotovému zakotvení společnosti; působení proti fungující ekonomice; působení proti bezpečnosti státu a občanů.[10]

Existence pouhého dokumentu vymezujícího hybridní hrozby vůči České republice však nijak nezaručí disponibilitu schopnostmi čelit samotnému praktickému hybridnímu působení. Je nutná pravidelná aktualizace a evaluace veškerých souvisejících procesů na základě nepřetržitého monitorování všech zásadních faktorů. Praktické implementaci specifických přístupů v rámci České republiky, jak čelit hybridním hrozbám a hybridnímu působení, předchází odpovídající *Národní strategie pro čelení hybridnímu působení*[11], na kterou navazuje konkrétní akční plán determinující specifické úkoly a opatření. Komplexní národní systém čelení hybridním hrozbám by měl zahrnovat všechny národní zpravodajské služby, silová a další ministerstva i další relevantní subjekty, včetně soukromého sektoru či akademické obce. Nepopiratelnou úlohu v boji proti hybridním hrozbám hraje také vzájemná součinnost s dalšími subjekty, aktéry a partnery mimo Českou republiku. Zdůraznění zaslouží především členství České republiky v NATO a Evropské unii. Důležitá potřeba nadnárodní spolupráce a koordinace je umocněna charakteristikou hybridních hrozeb, které mají často nadnárodní rozměr a svým charakterem potvrzují vzájemné prolínání vnější i vnitřní dimenze bezpečnosti.[12]

V oblasti odpovědnosti je nutné zdůraznit, že v České republice je za oblast čelení hybridnímu působení odpovědná vláda, která by měla v ideálním případě přijímat odpovídající opatření reagující na konkrétní hybridní hrozby a projevy hybridního působení. Za čelení jednotlivým aktivitám a projevům hybridního působení jsou v rámci svých působností následně odpovědné jednotlivé rezorty (ministerstva). Gestorem tvorby odpovídající národní strategie pro oblast čelení hybridním hrozbám či obecně hybridnímu

---

10 Vláda České republiky. Audit národní bezpečnosti. [online]. 2016. [cit. 2022-01-10]. Dostupné z: https://1url.cz/4KVaU

11 Sekce obranné politiky a strategie Ministerstva obrany od roku 2020 intenzivně pracovala na nadresortní národní strategii, která determinuje národní přístupy, jak čelit hybridnímu působení. Tato národní strategie byla schválena v dubnu 2021 (více viz https://mocr.army.cz/informacni-servis/zpravodajstvi/vlada-schvalila-narodni-strategii-pro-celeni-hybridnimu-pusobeni-227120/). Tuto zastřešující strategii navíc doplňuje Strategie kybernetické obrany České republiky (2018 – 2022) v gesci Vojenského zpravodajství a dále Strategie kybernetické bezpečnosti z roku 2020 v gesci NÚKIB (Národní úřad pro kybernetickou bezpečnost).

12 Viz HAVLÍK, ref. 3. str. 91.

působení a navazujícího akčního plánu[13] byl stanoven rezort Ministerstva obrany České republiky. Aktuální národní strategie stanovuje v oblasti čelení hybridnímu působení tyto strategické cíle: odolná společnost, odolný stát, odolná kritická infrastruktura; systémový a celostní přístup v rámci ČR; schopnost adekvátní a včasné reakce.[14] Uvedené strategické cíle České republiky jsou dále členěny na odpovídající specifické cíle. Další rozpad determinující konkrétní úkoly a jednotlivá opatření ve vztahu k čelení hybridním hrozbám aktuálně jsou ukotveny v navazujícím akčním plánu.

Ačkoliv jsou velmi obecné postupy, jak čelit působení proti bezpečnosti státu a občanů, zakotveny ve výše zmiňovaném *Auditu národní bezpečnosti*, je nutné poukázat na to, že se v praktické rovině zásadního progresu doposud nedostalo. Přestože je explicitně jmenováno celé spektrum odpovědných subjektů, v České republice doposud neexistuje společný koordinační a integrační prvek, který by komplexně zastřešil předmětnou problematiku. Mezi institucemi odpovědnými za řešení této oblasti jsou zahrnuty primárně zpravodajské služby. Specifickou a průřezovou úlohu mají orgány kybernetické bezpečnosti, obrany a ochrany, kde klíčového aktéra představuje NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost), síť pracovišť typu CERT (Computer Emergency Response Team), NCKO (Národní centrum kybernetických operací) a také VeKySIO (Velitelství kybernetických sil a informačních operací).[15] K institucím, které mají hlavní výkonné pravomoci a nástroje, patří Ministerstvo vnitra (zejména pak Centrum boje proti terorismu a hybridním hrozbám[16]), orgány vnitřní bezpečnosti a ochrany obyvatelstva či ozbrojené síly České republiky. Zmiňované ozbrojené síly České republiky nejsou aktuálně koncipovány pro samostatnou robustní obranu České republiky, ale pouze pro poskytnutí proporcionálního příspěvku ke kolektivní obraně za účasti všech členů NATO. Role ozbrojených sil České republiky v kontextu čelení hybridním hrozbám spočívá především v přispění k odstrašení, posilování odolnosti, případně odražení útoku směřovaného na ČR či jiného člena Aliance nebo Unie.[17]

---

13 Bezpečnostní rada státu vzala na vědomí (na svém zasedání dne 19. října 2021) Akční plán k Národní strategii pro čelení hybridnímu působení a zřídila funkci koordinátora agendy čelení hybridnímu působení a Odbornou pracovní skupinu Bezpečnostní rady státu pro čelení hybridnímu působení.

14 Ministerstvo obrany ČR. Národní strategie pro čelení hybridnímu působení. [online]. 2021. [cit. 2022-01-10]. Dostupné z: https://1url.cz/rK5Bq

15 Roli NÚKIB a prvků CERT v problematice řešení hybridních hrozeb na území ČR lze spatřovat především v zajišťování kybernetické bezpečnosti a navyšování odolnosti kritické infrastruktury proti kybernetickým útokům. Roli NCKO a VeKySIO lze spatřovat do budoucna jak v oblasti posilování odolnosti, tak rovněž i v oblasti vedení reaktivních útoků v informačním prostředí a kybernetickém prostoru. Okrajově se hybridním konfliktům věnuje také *Strategie kybernetické bezpečnosti rezortu Ministerstva obrany na období let 2017 až 2020,* kde se uvádí, že kybernetické útoky jsou v současnosti nedílnou součástí hybridních konfliktů.

16 Centrum boje proti terorismu a hybridním hrozbám bylo prvním institucializovaným subjektem, který se v rámci České republiky začal věnovat problematice hybridních hrozeb. S ohledem na dostupné zdroje a omezenou působnost pouze v rámci působnosti Ministerstva vnitra však aktivity tohoto centra neplní širší úlohu v oblasti integrace, jakkoliv prvotní ambice byly více průřezové. Logicky proto centrum nedisponuje informacemi, které jsou v gesci zpravodajských subjektů a také dalších ministerstev či relevantních subjektů. (více viz https://www.mvcr.cz/cthh/)

17 Vláda České republiky. Audit národní bezpečnosti. [online]. 2016. [cit. 2022-01-10]. Dostupné z: https://1url.cz/4KVaU

4 PŘÍSTUP EU PROTI HYBRIDNÍMU PŮSOBENÍ

Bezpečnost Evropské unie začíná podle EU Global Strategy[18] na národní domácí úrovni a umožňuje občanům požívat nebývalé bezpečnosti, demokracie a prosperity. V současné době jsou nicméně obyvatelé i samotné teritorium Evropské unie ohroženi hybridním působením, pandemií, terorismem, ekonomickou volatilitou, změnou klimatu a energetickou nejistotou. Evropská unie postupně stále intenzivněji prohlubuje své partnerství s NATO, a to prostřednictvím rozvoje koordinované obranné schopnosti, souběžných a synchronizovaných cvičení a vzájemně se posilujících akcí zaměřených na budování kapacit v boji proti hybridním a kybernetickým hrozbám. Hybridní a kybernetické hrozby, tak jako například terorismus neznají z hlediska bezpečnosti hranice. To vyžaduje těsnější institucionální sepětí a propojenější úsilí samotných členských států v oblasti posilující spolupráce.[19]

Je velmi nepravděpodobné, že by Česká republika čelila rozvinutému hybridnímu působení osamoceně. Podobně tuto hrozbu vnímají EU a NATO, a rozvíjejí proto své schopnosti. Oba nadnárodní subjekty jako řídící princip uznávají primární odpovědnost členských států a svou roli vidí jako podpůrnou. Přístup Evropské unie byl primárně determinován *Společným rámcem pro boj proti hybridním hrozbám*.[20] Přístup, úloha a schopnosti Evropské unie a NATO jsou do značné míry komplementární, proto je žádoucí jejich úsilí provázat a zvýšit tak jejich efektivitu.

V oblasti čelení existujícím hrozbám uvnitř Evropské unie je nutné vnímat současné vymezení zdůrazňující potírání rozdílu a hranice mezi vnější a vnitřní bezpečností. Vnější a vnitřní dimenze bezpečnosti se v rámci Evropské unie a zahraničně-bezpečnostních politik členských států velmi přibližují a částečně prolínají, a to především od přijetí *Lisabonské smlouvy*. Vlivem migrační krize linoucí se s určitými výkyvy od roku 2015, přetrvávající hrozby teroristických útoků uvnitř Evropské unie nebo pandemie koronaviru transformuje unijní společenství bezpečnostní a zahraniční politiku tak, aby plně odpovídala potřebám směřujícím k zajištění evropské vnitřní bezpečnosti.[21],[22]

Pro účinný boj proti hybridním hrozbám je třeba řešit potenciální slabá místa nejdůležitějších infrastruktur, dodavatelských řetězců a celé společnosti. Hlavním nástrojem zvýšení odolnosti vůči hybridním hrozbám je získání informací o situaci, a to prostřednictvím sledování a posuzování zranitelností referenčních objektů. Kontinuálně je nutné rozvíjet metody pro hodnocení bezpečnostních rizik, které mají poskytovat informace subjektům

18 After the EU Global Strategy – Consulting the experts – Security and Defence. EU Institute for Security Studies, 2016. Published by the EU Institute for Security Studies and printed in France by Jouve. Graphic design by Metropolis, Lisbon. ISBN 978-92-9198-503-6.

19 Globální strategie zahraniční a bezpečnostní politiky Evropské unie – Sdílená vize, společný postup: silnější Evropa. 2016. Str. 7, 14, 27, 36. [online]. 2016. [cit. 2022-01-10]. Dostupné z: https://1url.cz/Dzbq5

20 Joint Communication to the European Parliament and the Council "Joint Framework on countering hybrid threats: a European Union response". [online]. 2016. [cit. 2022-01-10]. Dostupné z: https://1url.cz/ozbEd

21 BAUEROVÁ, Helena, HLAVÁČKOVÁ, Hana, VOŠTA, Milan. *Vnitřní a vnější dimenze bezpečnosti Evropské unie.* Nakladatelství Libri, Praha, 2018. ISBN 978-80-7277-576-7. Str. 15.

22 Viz HAVLÍK, ref. 3. str. 92.

s rozhodovací pravomocí a podporovat vytváření odpovídajících bezpečnostních politik. Hlavními subjekty v rámci Evropské unie, které se věnují problematice hybridních hrozeb, jsou EU INTCEN (European Union Intelligence and Situation Centre), HFC (Hybrid Fusion Cell), STRATCOM (Strategic Communication Taskforces) a RAS-DIS (Rapid Alert System--Disinformation).[23] Za aktuálně nejvýznamnější subjekt z výše uvedených lze považovat středisko EU INTCEN, které má shromažďovat, analyzovat a sdílet utajované informace a informace z otevřených zdrojů, které se konkrétně týkají ukazatelů a varování v souvislosti s hybridními hrozbami, od různých zúčastněných stran.[24] Zpravodajské a situační středisko EU INTCEN je zpravodajský orgán služby pro vnější činnost (EEAS - European External Action Service) Evropské unie pod vedením vysokého představitele EU. EU INTCEN má kořeny v evropské bezpečnostní a obranné politice (CSDP - Common Security and Defence Policy), které se původně nazývalo Joint Situation Centre (Společné situační středisko). Od roku 2007 je EU INTCEN součástí jednotky Single Intelligence Analysis Capacity (SIAC), která integruje civilní zpravodajství (EU INTCEN) a vojenské zpravodajství (EUMS Intelligence Directorate). V rámci SIAC se k vypracování všech zpravodajských hodnocení ze všech zdrojů používají civilní i vojenské příspěvky.[25] Evropská unie definovala následující dílčí oblasti ke zvýšení odolnosti proti hybridním hrozbám: ochrana kritické infrastruktury (energetické sítě, bezpečnost dopravy a dodavatelských řetězců, vesmír); posílení obranné schopnosti; ochrana veřejného zdraví a potravinového zabezpečení; kybernetická bezpečnost (průmysl, energetika, zajištění zdravých finančních systémů, doprava); boj proti financování hybridních hrozeb a další; posilování odolnosti proti radikalizaci a násilnému extremismu; posílení spolupráce s třetími zeměmi. [26]

V evropském kontextu je vhodné zdůraznit, že pro Unii a především její soudržnost je možno za nejnebezpečnějších ve vztahu k hybridním hrozbám považovat státní nekinetické aktéry. Tato kategorie zahrnuje primárně výzkumné a mediální subjekty pocházející z Ruské federace a Čínské lidové republiky. Zásadním milníkem v oblasti hybridních hrozeb byl za poslední dekádu především rok 2016, kdy byla prezentována nová globální bezpečnostní strategie obsahující jako jednu z priorit rozvoje *Společné bezpečnostní a obranné politiky* rovněž i prohloubení spolupráce Evropské unie a NATO. Toto sblížení by mělo být zacíleno na segment obrany proti hybridním hrozbám, dále pak na kybernetickou bezpečnost, obranný výzkum a obranné kapacity, a také na společný výcvik.[27] Předmětná problematika spojená s potřebou zajistit bezpečnost v rámci Evropské unie

23 FIOTT, Daniel, PARKES, Roderick. Protecting Europe - The EU's response to hybrid threats. European Union Institute for Security Studies (EUIS). ISBN 978-92-9198-832-7. [online]. 2019. [cit. 2022-01-10]. Dostupné z: https://1url.cz/mK5BH

24 Ministerstvo zdravotnictví České republiky. Hybridní hrozby. [online]. 2016 [cit. 2021-12-29]. Dostupné z: https://www.mzcr.cz/hybridni-hrozby/

25 Evropský parlament. Answer to Question. [online]. 2012 [cit. 2021-12-29]. Dostupné z: https://1url.cz/mK5Bo

26 Senát Parlamentu České republiky. Společné sdělení Evropskému parlamentu a Radě, Společný rámec pro boj proti hybridním hrozbám, reakce Evropské Unie. [online]. 2016 [cit. 2021-12-29]. Dostupné z: https://1url.cz/ZzbEL

27 Euroskop.cz – Věcně o Evropě. Bezpečnostní a obranná politika. [online]. 2018 [cit. 2021-12-29]. Dostupné z: https://1url.cz/rK5Bi

svým způsobem iniciovala rovněž i vytvoření nového centra excelence CoE (Centre of Excellence)[28]. Toto centrum však neintegruje výhradně členské státy Evropské unie, ale také další aktéry (například Spojené státy americké, Norsko či Kanadu). V rámci tohoto centra excelence (nebo i dalších institucializovaných subjektů Evropské unie) je kontinuálně kladen důraz na koordinované a sdílené úsilí v boji proti hybridním hrozbám a hybridnímu působení[29], které však musí být vždy doplňováno a rozšiřováno odpovídajícími národními aktivitami jednotlivých členských států.[30]

V Radě Evropské unie byla pro boj proti hybridním hrozbám zřízena horizontální pracovní skupina označovaná jako HWP ERCHT (Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats), jejímž cílem je zlepšení odolnosti Evropské unie a jejích členských států vůči hybridním hrozbám a podpořena opatření na posílení odolnosti společností vůči krizi.[31] Komise a Evropská služba pro vnější činnost tyto snahy podporují na základě Společného rámce pro boj proti hybridním hrozbám z roku 2016 a společného sdělení z roku 2018 o zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb. Kromě toho Společné výzkumné středisko rozpracovalo rámec „koncepčního modelu", který má charakterizovat hybridní hrozby, s cílem pomoci členským státům a jejich příslušným orgánům určit typ hybridního útoku, jemuž by mohly čelit. Model se zabývá způsobem, jakým určitý aktér (státní nebo nestátní) využívá v různých oblastech (hospodářské, vojenské, sociální a politické) řadu nástrojů (od dezinformací po špionáž nebo fyzické operace) k ovlivnění svého terče tak, aby dosáhl řady cílů.[32]

Hybridní hrozby představují problém nejen pro EU, ale i pro ostatní důležité partnerské organizace, včetně Organizace spojených národů, Organizace pro bezpečnost a spolupráci v Evropě, a zejména NATO. Účinná reakce vyžaduje dialog a koordinaci mezi těmito organizacemi na politické i operační úrovni. Užší spolupráce by EU a NATO umožnila lépe se připravit a účinně reagovat na hybridní hrozby, vzájemně se doplňovat a podporovat na základě zásady začlenění a zároveň respektovat nezávislost obou subjektů při rozhodování.[33]

---

28 Konkrétně se jedná o The European Centre of Excellence for Countering Hybrid Threats se sídlem ve finských Helsinkách.

29 Zde jsou důležité především vybrané projekty strukturované spolupráce typu PESCO – Permanent Structured Cooperation.

30 Viz HAVLÍK, ref. 3. str. 92.

31 Evropská rada Evropské unie. Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats, [online]. 2019 [cit. 2021-12-29]. Dostupné z: https://1url.cz/sK5Be

32 Evropská komise. Sdělení komise Evropskému parlamentu, Evropské radě a Radě. Dvacátá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii. [online]. 2019 [cit. 2021-12-29]. Dostupné z: https://1url.cz/9K5Lp

33 Ministerstvo zdravotnictví České republiky. Hybridní hrozby. [online]. 2016 [cit. 2021-12-29]. Dostupné z: https://www.mzcr.cz/hybridni-hrozby/

5 PŘÍSTUP NATO PROTI HYBRIDNÍMU PŮSOBENÍ

Strategická koncepce NATO (*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*)[34] promítá operační a dynamické aspekty současné doby a zabývá se konkrétní geopolitickou situací, tedy hrozbami a způsoby, jak lze na tyto hrozby vojensky reagovat. Strategická koncepce uvádí tři základní úkoly: kolektivní obrana založená především na principu odstrašení; krizové řízení, které se zabývá politickými a vojenskými nástroji; společná bezpečnost (Cooperative Security).[35] Všechny základní úkoly mají neoddiskutovatelný přesah na nepřátelské hybridní působení.

Hybridní a kybernetické působení a útoky jsou často zaměřeny na nejslabší článek nebo spojenecké národy se specifickou zranitelností. V posledních letech NATO učinilo určité kroky pro boj proti těmto hrozbám. V roce 2010 byl iniciován vznik významného koncepčního dokumentu pod názvem *Military Contribution to Countering Hybrid Threats (MCCHT)*. Odpovědným orgánem tvorby tohoto dokumentu bylo ACT (Allied Command Transformation), které provedlo podrobnou analýzu bezpečnostního prostředí, vytvořilo a v srpnu 2010 publikovalo první návrh koncepce zabývající se řadou problémů a bezpečnostních výzev, které mohou ovlivnit existenci NATO i širšího mezinárodního společenství v průběhu nastávajících dvou desetiletí. Představitelé NATO očekávali, že nová operační koncepce *Military Contribution to Countering Hybrid Threats* bude znamenat výrazný posun a přínos v boji proti hybridním hrozbám, což se však v podstatě a v praktické rovině nestalo.[36] Na tuto významnou koncepci dále navazoval v roce 2010 dokument *New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*[37] a dále dokument *NATO Information Operations Reference Book*[38].

Dalším důležitým milníkem v přístupu Aliance k problematice hybridních hrozeb byl rok 2018, kdy došlo k vytvoření specifických týmů Counter Hybrid Support Teams (CHST), které spojencům poskytují pomoc v míru. Následně v listopadu 2019 schválilo NATO zprávu o posílení reakce NATO na hybridní hrozby (blíže rozebráno například v odborném článku NATO's Response to Hybrid Threats[39]), která nastiňuje priority a program

---

34 Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010. NATO Public Diplomacy Division, Brussels – Belgium.

35 PETRÁŠ, Zdeněk. *Strategický přístup a zásady vedení společných operací NATO a EU*. Prezentace pro kurz GŠT z 23.11.2020. UO Brno – CBVSS. Str. 12.

36 KUBEŠA, Milan, SPIŠÁK, Ján. *Hybridní hrozby a vývoj nové operační koncepce NATO.* Obrana a strategie (Defence & Strategy). ISSN 1214-6463 (print) and ISSN 1802-7199 (on-line). Volume 11, Number 2 (December 2011).

37 NATO - *New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.* Supreme Allied Commander, Europe, SHAPE, Belgium. [online]. 2010 [cit. 2021-12-29]. Dostupné z: https://1url.cz/HzbGb

38 NATO - *NATO Information Operations Reference Book.* Supreme Allied Commander, Europe, SHAPE, Belgium. [online]. 2010 [cit. 2021-12-29]. Dostupné z: https://1url.cz/AzbG9

39 RUHLE, Michael. NATO's Response to Hybrid Threats. Information Series. National Institute For Public Policy. [online]. 2019 [cit. 2021-12-29]. Dostupné z: https://www.nipp.org/wp-content/uploads/2019/11/IS-448.pdf

boje proti hybridním hrozbám. Důraz byl zároveň položen také ve vztahu k vlastní kybernetické hygieně. I přes uvedené pokroky však NATO potřebuje společný politický rámec pro to, jak by mělo konkrétně hodnotit a reagovat na hybridní a kybernetické incidenty v krizi. Zdlouhavé politické diskuse o atribuci a o tom, jak a zda by mělo NATO jednat, brání alianci včas reagovat na skryté bezpečnostní výzvy, což zvyšuje riziko nezamýšlené eskalace potenciálních protivníků.[40]

Jak bylo zmíněno v předešlé kapitole, je samotný přístup NATO při čelení hybridním hrozbám a hybridnímu působení propojen s přístupem Evropské unie (mimo jiné platformy také v rámci zmiňovaného helsinského centra excelence). Přestože je v rámci NATO položen důraz na společné a koordinované úsilí, i v tomto případě by měly být všechny související procesy vždy doplňovány a rozšiřovány odpovídajícími národními aktivitami a schopnostmi jednotlivých členských států. V posledních letech jsou hybridní aktivity nepřátelských aktérů NATO směřovány na polarizaci poměrně soudržné západní společnosti s cílem destabilizovat samotnou institucionální soudržnost, a tímto krokem logicky oslabit schopnosti NATO. Proto je v posledních letech také zřejmá transformace strukturálního členění a využívání jednotlivých nástrojů moci, a to konkrétně od využívání nástrojů charakteru *hard power*, přes *soft power* až po *smart power* a *sharp power*.[41]

Důležitá součinnost uvnitř NATO mezi jednotlivými členskými státy a případnými uskupeními (zahrnující jak elementy a schopnosti pozemních sil, vzdušných sil, námořních sil, speciálních sil, kybernetických sil atd.) v rámci vedení hybridní obrany, ale i ofenzivních hybridních operací závisí na přístupu všech partikulárních jednotek. Je přínosné zdůraznit význam interoperability v rámci společných operací zahrnující oblast doktrín, administrativy, komunikací, letecké podpory pozemních sil, palebné podpory, prostředků protivzdušné obrany, shromažďování a distribuci zpravodajských informací (včetně sdílení informační i klíčových poznatků), organizaci personálu, elektronického boje, volbu cílů, využití technických a taktických přesil či výhod, jazykových znalostí, kulturních znalostí, výcviku, zajištění munice a pohonných hmot (celkově logistické zabezpečení) apod.[42] V rámci NATO byly ke vzájemné součinnosti v oblasti hybridního působení implementovány konkrétní projekty spadající do specifické kategorie označované jako *Smart Defence.* V této spojitosti lze za nejvýznamnější projekt považovat *MCDC Project: Countering Hybrid Warfare 3 (CHW3)*. Přístup NATO k čelení hybridním hrozbám a působení by měl principiálně zahrnovat široké zpravodajské a informační aktivity, dnes velmi důležitou strategickou komunikaci, odpovídající expertní podporu a poradenství napříč členskými státy aliance, komplexní zvyšování odolnosti, kybernetickou obranu, civilně-vojenskou interakci, související výcvik, cvičení a vzdělávání a také vzájemnou spolupráci

40 NATO 2030: United for New Era – Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General. 25 November 2020. Str. 45 – 46.

41 Viz HAVLÍK, ref. 3. str. 93.

42 SCHRÖFL, Josef, RAJAEE, Bahram M., MUHR, Dieter (eds.). *Hybrid and Cyber War as Consequences of the Asymmetry – A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace.* 2011, Peter Lang GmbH, Internationaler Verlag der Wissenschaften, Frankfurt am Main. ISBN 978-3-631-60285-0. Str. 260.

mezi jednotlivými partnery uvnitř aliance a také mezi jednotlivými členskými státy a aliančním centrálou.

Nedávný výzkum NATO navíc ukazuje tři společné názory na komplexní přístup, které zahrnují tato témata: důsledné uplatňování vnitrostátních nástrojů moci; komplexní interakci s ostatními aktéry a komplexní opatření ve všech oblastech a prvcích krizí. Aliance dále pracuje na následujících čtyřech oblastech komplexního přístupu: plánování a provádění operací; školení, vzdělávání, cvičení; posílení spolupráce s externími aktéry; veřejné správy.

Přístup NATO vůči hybridním hrozbám a působení by měl obecně zahrnovat zpravodajství a informace; možnosti civilně-vojenské interakce; strategickou komunikaci; podporu spojencům; odolnost; kybernetickou obranu; výcvik a vzdělávání či také spolupráci s partnery a EU.

6 KOMPARACE PŘÍSTUPŮ ČESKÉ REPUBLIKY, EU A NATO

Jak Evropská unie, tak i NATO mají ambice realizovat krizová opatření ve vztahu k hybridním hrozbám (obecně hybridnímu působení), jakkoliv jsou jejich aktuální možnosti a schopnosti velmi omezené a lze dokonce tvrdit, že velmi závislé na konkrétním přístupu jednotlivých členských států. Procesy plánování, přípravy a vedení operací reagujících na hybridní hrozby z pozice Evropské unie a NATO se liší, a to v reakci na odlišné soustavy politicko-vojenských ambicí. Zde je nutné reflektovat i to, že se liší také dílčí ambice jednotlivých členských států Evropské unie a NATO. Boj s hybridními hrozbami představuje jednu ze sedmi základních oblastí společného projektu Evropské unie a NATO (EU-NATO Joint Declaration: Implementation). Mimo uvedenou spolupráci je patrné provázání Evropské unie a NATO také v rámci sdílení schopností zastřešovaných evropským CoE (Centre of Excellence).

Evropská unie i NATO pravidelně aktualizují definování svého přístupu, jak čelit hybridnímu působení vedenému proti nim (nebo proti jejich členským státům), a zároveň intenzivně pracují na nastavení mechanismů, jak v situaci hybridního útoku vzájemně spolupracovat a asistovat svým členským státům. Česká republika se do těchto procesů začíná postupně aktivně zapojovat ve snaze využít získané zkušenosti pro adaptaci vlastního bezpečnostního systému.

V rámci vzájemné komparace přístupů České republiky, Evropské unie a NATO je vhodné zdůraznit, že ve své podstatě žádný rozdíl mezi přístupy není a procesně lze hovořit o vzájemné a provázané synergii. Pro komparaci přístupů státních aktérů by bylo vhodné celý analytický rámec doplnit v dalším výzkumu například o přístup států s obdobnou velikostí a obdobnými demokratickými i bezpečnostními hodnotami.

ZÁVĚR

Argumentační rámec v přístupu České republiky v oblasti čelení vůči hybridním hrozbám potvrzuje zcela chybějící komplexní prakticky fungující aparát a konkrétní operativní nástroje, jak účinně čelit hybridnímu působení nepřátelských aktérů, a to ve všech klíčových oblastech (odolnost, detekce i reakce). Přestože je analyzovaná problematika v rámci doktrinálního ukotvení ve strategických dokumentech z pozice České republiky, Evropské unie i NATO relativně dobře ukotvena, stále chybí efektivní soubor komplexních schopností, který by mohl prakticky účinně čelit hybridnímu působení nepřátelských aktérů. Pouhé zanesení fenoménu hybridních hrozeb a hybridního působení jako důležitých bezpečnostních výzev do strategických dokumentů, nemůže být chápáno jako uspokojující komplexní opatření umožňující naší republice, Evropské unii či NATO účinně čelit takto významným hrozbám.

Je nutné, aby se celý bezpečnostní aparát České republiky a přeneseně také Evropské unie a NATO intenzivněji věnoval praktické aplikaci široké škály optimálních doporučení a tímto postupem pak zacelit existující bezpečnostní mezery v obranných a bezpečnostních systémech. Je zřejmé, že tyto procesy budou nejen zdrojově náročné, ale budou vyžadovat také širokou komunikaci a přijetí mnoha konsenzů, neboť z hlediska strukturální povahy je nutné k této problematice přistupovat velmi komplexně. Akcent v této souvislosti zaslouží tzv. Comprehensive Approach, a to napříč všemi zainteresovanými bezpečnostními aktéry, akademickou sférou, komerčním sektorem a také celou společností. Jakkoliv je takto navrhovaný přístup logicky komplikovaný, je nutné mu věnovat o to větší společné úsilí s hledáním reálného řešení. Už jen snaha bezpečnostních expertů a celé bezpečnostní komunity analyzovat problém hybridních hrozeb a stále šířeji o něm diskutovat, dává určité předpoklady budoucího úspěchu, jakkoliv v krátkodobém horizontu nemůžeme očekávat zásadní změny.

Pozitivním krokem v rámci České republiky je nedávno schválená *Národní strategie čelení hybridnímu působení*, na kterou na konci roku 2021 bezprostředně navázal související akční plán, který determinuje počáteční konkrétní úkoly a opatření k následné praktické realizaci. Za zmínku stojí také fakt, že přístup České republiky v čelení hybridnímu působení bude vždy korespondovat s aktuální politickou reprezentací, kdy samotná vláda je odpovědná za bezpečnost a v ideálním případě by měla přijímat odpovídající opatření reagující na konkrétní hybridní hrozby a projevy hybridního působení.

Bezpečnost České republiky je založena na členství v NATO a Evropské unii. Její odolnost vůči hybridním hrozbám je úzce spjata s odolností těchto dvou subjektů. Ačkoliv jsou přístupy České republiky, Evropské unie a NATO v oblasti čelení hybridním hrozbám ve svém koncepčním pojetí poměrně synergické, všem třem zmíněným subjektům i nadále chybí komplexní a navzájem komplementární efektivní systémy schopné praktické působit. Pouhé doktrinální ukotvení významu hybridních hrozeb není pro praktické čelení dostačující a je potřeba realizovat celou řadu důležitých navazujících opatření.

Autor: ***Plk. gšt. PhDr. Ing. Martin Havlík, Ph.D., MBA, MSc., LL.M.*** *Pracovník Ministerstva obrany České republiky. Specializuje se na zpravodajskou problematiku, zejména pak na oblast technických zpravodajských disciplín, informačních a kybernetických operací jakožto nedílné součásti hybridního působení státních i nestátních aktérů. Mimo uvedené se dlouhodobě zaměřuje na analýzy bezpečnostních hrozeb a rizik v oblastech konfliktů (především v Asii) s dopadem na obranu a bezpečnost České republiky.*

Jak citovat: HAVLÍK, Martin. Aktuální přístupy České republiky, EU a NATO k hybridním hrozbám. *Vojenské rozhledy.* 2022, 31 (2), 003-016. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.