Hybridní hrozby – fenomén v oblasti válek 21. století

Alžběta Kartusová
Západočeská univerzita v Plzni, Fakulta právnická

Anotace: Tento odborný článek popisuje novodobý druh bezpečnostních hrozeb, tzv. hybridní hrozby, a snaží se osvětlit nejen samotný pojem hybridní hrozba či hybridní válka, ale taktéž přiblížit i v minulosti několikrát využívané metody při jejich plánování a vedení. Dále pojednává o způsobech obrany proti případným hybridním útokům, a to jak na mezinárodní, tak také na národní úrovni.
Klíčová slova: hybridní hrozba, hybridní válka, bezpečnost

Abstract: This article describes a new kind of security threats – hybrid threats – and aims to clarify not only the terms hybrid threat and hybrid warfare, but also examine the methods that are being used in relation to planning and engagement in such warfares. Furthermore, it suggests methods of protection against possible hybrid attacks both on international and national level.
Keywords: hybrid threat, hybrid warfare, security

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

Úvod

Ohlédneme-li se zpět do minulého století a srovnáme-li ho se stoletím jednadvacátým, zjistíme, že byť se naše společnost nachází na vrcholu vyspělosti celosvětové úrovně a z historie se snad dokázala poučit, stále se potýkáme s celou řadou hrozeb a nejistot. Tyto hrozby mají ale novou tvář a zaměřují se na zcela odlišné cíle, které jsme si dosud jako společnost nedokázali zcela určitě představit. V této souvislosti se setkáváme s pojmem „hybridní hrozba" stále častěji, a to nejen z novinového, rozhlasového i televizního zpravodajství. Můžeme však toto, mohlo by se zdát, neurčité slovní spojení nějak blíže definovat?

1 Pojem

Pojem „hybridní válka" je obtížné přesně definovat. Každý stát, ať již přímo ten, který se s hybridními útoky potýká, či ten, který pouze přihlíží, či je o nich pouze informován prostřednictvím zpravodajských služeb, nebo je dokonce cílem takového útoku, si tento pojem může vykládat podle svého vlastního přesvědčení, získaných informací či například pomocí legislativních předpisů.

V 21. století můžeme *largo sensu* hybridní válku označit jako kombinaci civilních a vojenských způsobů a prostředků, které jsou používány sloučenými způsoby k dosažení cíle a ukotvení postavení útočícího subjektu, destabilizaci jiného subjektu nebo šíření dezinformací.[1] Pokud bychom chtěli tento pojem

[1] *Co jsou hybridní hrozby* [online]. [cit. 2019-06-16]. Dostupné z https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

představit v užším slova smyslu, pak by se mohlo jednat o do detailu promyšlenou formu vedení dílčích útoků, ať již na mezinárodní úrovni, kdy pozici útočníků a cílů hybridních válek zaujímají státy, či na dimenzi vnitrostátní, tedy na prolínání nestátního aktéra, který využívá konvenčních principů k narušení mírového fungování ve státě. Je nutno poznamenat, že pod hybridní hrozbu můžeme subsumovat útoky postavené na konvenčních vojenských silách, dále na nekonvenčních, ale také na těch, které celou problematiku posouvají od roviny taktické po rovinu politickou či ekonomickou.

Hybridním útokem lze tedy nazvat řadu dílčích kroků, kterými je vyvinut i nedestruktivní nátlak sledující poškození cíle útoku. Jde o dopodrobna promyšlené strategie, kterými se agresor pokouší narušit bezpečnostní, ekonomickou nebo politickou sféru, která je po desítky let budována, a donutí tak druhou stranu ke krokům, na základě kterých získá větší moc, výsadní postavení či jiný profit. K vysvětlení či upřesnění pojmu dochází neustále a existuje čím dále tím více názorů, co to vlastně hybridní hrozba je a jak ji definovat. Například podle Iva Zelinky (výkonný důstojník zástupce náčelníka Generálního štábu AČR) musí převažovat počet nevojenských prostředků nad těmi vojenskými. Nevojenským prostředkem jsou pak myšleny například kybernetické útoky, terorismus, využití polovojenských skupin či ekonomické nástroje jako sankce, embarga, kvóty.

Ať se přikloníme ke kterékoliv definici, která by mohla v pravém slova smyslu opravdu hybridní hrozbu definovat, měli bychom se možná zamyslet nad tím, proč je tato „moderní“ hrozba 21. století nazvaná právě jako „hybridní“. Znamená

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

právě toto slovo hrozbu či válku z ní plynoucí jako „hrozbu“ méně závažnou, či naopak podstatnou?

1.1 Příklady z historie a současnosti

Pojem hybridní hrozba začal být v dnešním slova smyslu využíván až zhruba od roku 2014, tedy po událostech, se kterými jsou tyto hrozby spojovány a hojně medializovány.[2] Takovými mezníky, kde se hybridní hrozba a útoky skloňují snad ve všech pádech, může být například tzv. anexe Krymu či válka na východní Ukrajině.

Je možné dnes tedy hovořit o hybridní válce jako aktuálním problému, kterým si jako vyspělá civilizace procházíme? Definici hybridní hrozby, která je nastiňována, bychom rozhodně mohli doložit na několika historických událostech, jejichž průběh byl taktéž ovlivňován poskytováním neucelených, nepravdivých a někdy i nulových informací. V posledních letech je poukazováno převážně na konflikty, ve kterých hlavní postavení zaujímá Rusko a USA. Strategie Ruska je hojně definována právě jako taková, která nástroje hybridních kampaní využívá. Takové chování však může vyplývat i z historického postavení Ruska, které se již od svých počátků připojilo ke strategii expanze, neboť čelilo neustálým útokům a ohrožení svého území. To, co je v nynějším postavení nové, vychází ze zkušenosti Ruska, přesněji z konfrontace s NATO, které sehrává nejen v problematice hybridních hrozeb klíčovou roli

[2] KUBEŠA, Milan – SPIŠÁK, Ján. *Hybridní hrozby a vývoj nové operační koncepce NATO* [online]. 2011 [cit. 2019-07-03]. Dostupné z: https://www.obranaastrategie.cz/cs/aktualni-cislo-2-2011/clanky/hybridni-hrozby-a-vyvoj-nove-operacni-koncepce-nato.html

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

(viz níže). Proč se Rusko vydalo cestou skryté války, můžeme pouze polemizovat. Možná právě NATO, které samo o sobě má i své odpůrce a kritiky, představuje pomyslnou silovou hranici, přes kterou se Rusko neodhodlá vykročit, a je tedy nuceno dosahovat svých cílů pod prahem agrese, přesně tak, aby jeho snahy nebyly odkryty členskými státy NATO. Rusko na základě nesdílení stejných názorů s NATO považuje tuto alianci za nepřátelsky laděnou, přestože je to právě Ruská federace, která je aktivní v kybernetické informační oblasti a má účinky v ovlivňování nálad domácího i zahraničního obyvatelstva, týkajících se politiky či ekonomiky.

Aniž by byl pojem hybridní válka nebo hrozba jako způsob vedení války té nejmladší generace definován, byl poprvé masově použit v případě Ruska a anexe ukrajinského Krymu. Podle Ruska se však nejednalo o násilné ovládnutí ukrajinského území, ale mělo jít o převzetí mírové, které bylo iniciováno zespodu od obyvatel Krymu, nikoliv na základě vnějšího tlaku Ruska, přičemž tento postoj byl jako jediný intenzivně předkládán veřejnosti. Proč tedy byla využita ozbrojená intervence, kterou nezpochybnitelně zachytila světová média? S názorem, že v žádném případě nešlo o mírové převzetí území, se ztotožnil mj. i Mezinárodní trestní soud v Haagu, který potvrdil, že vztah mezi Ruskem a ukrajinským Krymem byl mezinárodním ozbrojeným konfliktem.[3] V této publikaci bychom dohledali názor a možná se v něm i utvrdili, že

[3] Report on Preliminary Examination Activities 2018. *The Office of the Prosecutor, International Criminal Court, odstavec 68* [online]. [cit. 2019-07-16]. Dostupné z: https://www.icc-cpi.int/itemsDocuments/181205-rep-otp-PE-ENG.pdf. Působení Ruska je dle publikace HOFFMAN, Frank G., 2007a. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 72 s., novodobým typem vedení války.

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

hybridní válka je velmi promyšleným postupem, který se skládá z několika klíčových fází od té první, která probíhá ve formě publikování dezinformací či využití diplomatických kroků, až po tu, ve které jsou využity samotné válečné zbraně. Tato poslední fáze představuje nejtěžší formu využití nástrojů využívaných jak při mezinárodních, tak také vnitrostátních konfliktech.

Zřejmě tím nejaktuálnějším příkladem, kdy Rusko bylo označeno jako strana využívající hybridní nástroje, je spojitost s posledními prezidentskými volbami v USA, kdy Rusko prostřednictvím mnoha falešných účtů a identit publikovalo množství informací, které měly za cíl rozdělit a popudit americkou společnost, a tím ovlivnit výsledky prezidentských voleb. Oficiální vyjádření Ruska vměšování se do vnitrostátních voleb USA důrazně odmítala, což překvapivě nakonec tvrdila také americká vláda, když prohlásila, že k ovlivnění nedošlo a ani nebyly zaznamenány žádné útoky. Zda se ze strany Ruska jedná o úmyslné nepravdivé vyjádření a USA učinilo jen taktický krok, je jen těžko zjistitelné.

2 Nástroje a způsoby využívané v hybridních válkách

Nástroje, které mohou být využity při vedení hybridní války, můžeme spatřit již v mezinárodních konfliktech uskutečňovaných po celé století. Pokud se agresor rozhodne započít hybridní válku, respektive tzv. hybridní kampaň proti cíli svého útoku, využívá škálu nástrojů. Spektrum nástrojů, které jsou využívány a tvoří tak součást hybridní kampaně, nazýváme

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

jako tzv. DIMEFIL (Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement), díky kterým může mít agresorovo „válečné tažení" mnoho podob.[4] V rámci této problematiky je nutné pohlížet na hybridní válku jako na široký rozsah nástrojů, které jsou využívány pro získání benefitů daného agresora. Mezi takové nástroje řadíme na prvním místě šíření (dez)informací nebo tzv. „fake news", ať již pomocí sociálních sítí, nebo tradičních masmédií, které zapůsobí na značnou škálu obyvatel a s nimiž se setkáváme dennodenně. Právě tímto způsobem lze relativně snadno docílit značného vlivu na mínění velkého počtu jedinců, například občanů konkrétního státu nebo členů organizace. Aktuálně primární informační kanály představují nejpopulárnější globální sociální sítě jako Twitter, Facebook či jiné lokálního rázu, ze kterých čerpáme nejrůznější zpravodajství. Cílovou skupinou jsou zde uživatelé těchto moderních sítí, kteří by si měli být vědomi faktu, že internet bude přinášet čím dál tím více informací, které však ne vždy budou podány pravdivě. Je tedy nejen na státním prvku uchránit své občany před dezinformacemi, ale taktéž na každém občanovi dokázat přijímané informaci porozumět, porovnat ji a až posléze vytvořit svůj vlastní pohled na danou problematiku, neboť může docházet k pokusu o zmatení daného jedince a utváření jeho neopodstatněného mínění.

Další oblastí, která je v rámci vedení hybridní kampaně ovlivňována a má neméně závažné důsledky, je samotná politika. Niccolo Machiavelli tvrdil: „V politice, kde není odvolacího soudu, soudí člověk podle výsledku." Ať dáme tomuto citátu

[4] *Co jsou hybridní hrozby: O hybridních hrozbách* [online]. [cit. 2019-07-03]. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx.

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

za pravdu, či nikoliv, je právě politické dění jedním z nástrojů, který agresor využívá k ovlivňování celé společensko-politické nálady a vědomí občanů daného státu, ale i ke změně jejich politického přesvědčení a názoru na konkrétní problematiku.

Třetí oblastí, která je často cílem napadení hybridními útoky, je ekonomika. Na základě změn ekonomických prvků, kterými může být například zvýšení cla, zákaz dovozu či vývozu zboží, je daný cílový stát kontrolován a bezesporu je s ním jednáno tak, aby agresor tento státní celek koordinoval směrem dle svého uvážení a získal tím i právě „pouhou" ekonomickou prosperitu, neboť i ekonomický růst či ovlivnění ekonomického trhu na celosvětové i lokální úrovni může být bodem, kterého chce být dosaženo. [5]

K tomu, aby mohly být tyto kampaně efektivně využívány, jsou zapotřebí perfektní znalosti fungování a mezinárodního postavení daného cíle. V rámci rozvinuté hybridní války by tedy měly být využívány do detailu promyšlené kroky, které jsou vystavěny na dostatečném poznání úrovně zranitelnosti druhé strany, předvídání různorodých situací a výsledků (ať již z oblasti politiky, či taktéž zmíněné ekonomiky) a schopnosti flexibilně reagovat na aktuální bezpečnostní otázky například v kybernetickém prostoru, který se stále více rozrůstá a zrychluje tok informací do všech koutů světa.

[5] HOFFMAN, Frank G. Op. cit. sub. 4, str. 22.

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

3 Způsoby obrany proti hybridním útokům

Již v minulosti se odehrálo několik klíčových mezníků, kdy si státy uvědomily nutnost mírových, mezinárodních, obchodních dohod, smluv a taktéž i organizací, které i nadále udržují mezinárodní vztahy na přátelské bázi a soudržnosti. V posledních deseti letech klíčovou roli sehrává Severoatlantická aliance založená roku 1949, známá spíše pod zkratkou NATO, která v boji proti hybridním útokům zastává zásadní postavení, i když má i své kritiky, odpůrce a je dokonce zpochybňována její činnost. Nelze ovšem přehlédnout, že to bylo právě NATO, které zařadilo pojem hybridní hrozba do širšího povědomí a dalo mu novodobý význam (byť ne přesnou definici). NATO a zástupci členských aliančních zemí, kteří se navzájem spojují a budují nové politické vztahy, reagují na případné hybridní útoky a navzájem kooperují – předávají si nové informace a zkušenosti s novým typem útoku.

Další širokou platformu spolupráce zaštiťuje Evropská unie, která si zakládá na spolupráci svých členů a tvoří tak nejdůležitější prvek, na kterém je založena obrana proti hybridním útokům na země starého kontinentu. V tomto roce Evropská rada přijala strategickou agendu pro rok 2019–2024, ve které se mj. zaměří i na problematiku dezinformací jako jednu z prioritních oblastí zasluhující si zvýšenou pozornost. Strategická agenda také předurčuje vyšší sankce, které by hrozily při využití kybernetického útoku třetího státu vůči členovi Unie. V roce 2016 byla přijata Globální strategie zahraniční a bezpečnostní politiky EU, která se na hybridní hrozby jako novodobý problém také zaměřuje. Píše se v ní kupříkladu: „EU bude nadále prohlubovat partnerství s NATO prostřednictvím koordinovaného

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

rozvoje obranných schopností, paralelních a synchronních cvičení a vzájemně se posilujících opatření k budování kapacit našich partnerů, proti hybridním a kybernetickým hrozbám…“ Dále pak, že „… z bezpečnostního hlediska terorismus, hybridní hrozby a organizovaná kriminalita naznají hranice. To vyžaduje užší institucionální vazby mezi naší vnější akcí a vnitřním prostorem svobody, bezpečnosti a práva“.

Jak bylo výše uvedeno, hybridní útoky zahrnují i šíření dezinformací, ale i zcela nepravdivých skutečností, proto je nutné naučit každého jedince kritickému myšlení a schopnosti přijímané informace filtrovat a ověřovat důvěryhodnost těchto informací a jejich relevanci.

4 Česká republika a hybridní hrozby

Základní právní rámec obrany České republiky a zajištění její komplexní bezpečnosti poskytuje zejména ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, zákon č. 222/1999 Sb., o zajišťování obrany České republiky, zákon č. 240/2000 Sb., tzv. krizový zákon, zákon č. 219/1999 Sb., o ozbrojených silách České republiky, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a dále pak zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), a zák. č. 153/1994 Sb., o zpravodajských službách.

Na národní úrovni došlo k vytvoření odborné složky specializující se na hybridní hrozby vůči České republice, a to Centrum proti terorismu a hybridním hrozbám (CTHH), které

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

zahájilo svou činnost v lednu roku 2017.[6] V rámci své činnosti se CTHH aktivně zapojuje do zajímavých projektů na mezinárodní úrovni, některé dokonce pořádá ze své vlastní iniciativy. Činnost CTHH můžeme sledovat samozřejmě online, na jeho twitterovém účtu, kde bychom nalezli aktuality o jeho fungování a mnoha aktivitách. V tomto roce například Centrum pořádalo Festival bezpečného internetu či se zapojilo do mezinárodní hry volně přístupné na internetu, která dle britského výzkumu po několika málo minutách aktivního hraní zlepšuje kritické myšlení a schopnost vytřídit tzv. „dezinfo" až o 25 %. CTHH poskytuje informace o aktuálně šířených dezinformacích, které hojně kolují internetem, a pomáhá tak občanům v jejich rozlišování.

Problematikou hybridních hrozeb se zabývá v souladu s dodržováním Bezpečnostní strategie ČR z roku 2017, obsahující část týkající se hybridních hrozeb, jež v tomto dokumentu rozhodně nezastávají poslední místo k diskusi. Na tom je vidět, že i ČR jako stát stojící mimo okruh nejvýznamnějších globálních aktérů posiluje a nadále musí posilovat svou bezpečnost a odolnost vůči hybridním hrozbám a schopnost na ně dostatečně flexibilně reagovat, protože se mohou odehrávat i v řádu hodin a napáchat škody za miliardy. V současné době se ČR řadí mezi prvních deset nejbezpečnějších zemí z celého světa, o což musí nadále aktivně usilovat mj. proto, aby dokázala ochránit sdílené zpravodajské informace ze srovnatelně, nebo dokonce více zabezpečených zemí a nadále si tuto výměnu informací jako jeden z prostředků upevňování globální pozice udržet.

[6] *Centrum proti terorismu a hybridním hrozbám* [online]. [cit. 2019-07-03]. Dostupné z: https://www.mvcr.cz/cthh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

CTHH funguje pod záštitou Ministerstva vnitra ČR a jeho primárním úkolem je monitoring případných bezpečnostních hrozeb, jejich řešení, rozpoznávání dezinformací, jejich uvádění na pravou míru a vyjadřování se k legislativě vztahující se k bezpečnosti našeho státu. O aktuálním bezpečnostním stavu České republiky pojednává Audit národní bezpečnosti ČR vydaný Ministerstvem vnitra ČR v roce 2016.[7] Tento Audit se zabývá aktuální pružností legislativy zajišťující bezpečnost našeho státu, možnou reakcí bezpečnostních složek na různorodou formu útoků, ale právě též na novodobé hrozby, kterým by Česká republika mohla čelit. Jedním z jeho závěrů je, aby Česká republika započala lepší koordinaci nejen uvnitř státu, ale posílila komunikační schopnost i vně. Je nutné si uvědomit, že byť je Česká republika relativně silným samostatným státem, je nutné spolupracovat na evropském poli, spolupracovat a třeba se i solidárně označit za stát dotčený hybridním útokem primárně vedeným proti jinému našemu spojenci z řad EU nebo NATO anebo alespoň vyjádřit nesouhlasný postoj s takovým aktem vůči kterémukoli jinému státu, případně poskytnout přiměřenou pomoc.

Závěr

Bez ohledu na definici pojmu je nutné, aby každý stát mohl dostatečně flexibilně reagovat na hybridní útoky ze strany jiných států a proti svým občanům.

[7] *Audit národní bezpečnosti*. 2016. Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality.

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

Legislativa je nutným základem, ovšem měla by pomoci zajistit, aby bezpečnostní složky mohly reagovat v co nejkratším, ideálně reálném čase, kdy je obrana nejefektivnější a zároveň fakticky jedinou možnou, která je způsobilá útoku zabránit, odvrátit nebo alespoň minimalizovat škody, ať už na národní úrovni, nebo v rámci mezinárodní spolupráce.

Velmi účinnou a levnou zbraní proti hybridním hrozbám je vzdělaná, sebevědomá a uvědomělá demokratická společnost, která je ochotna bránit demokratické hodnoty i svou národní identitu. Tato ochota zahrnuje mimo jiné splňování daňové povinnosti a zajištění dostatečného rozpočtu na obranu státu.

POUŽITÉ PRAMENY

Audit národní bezpečnosti. 2016. Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality.

Co jsou hybridní hrozby [online]. Dostupné z: https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx

Centrum proti terorismu a hybridním hrozbám [online]. [cit. 2019-07-03]. Dostupné z: https://www.mvcr.cz/cthh/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx.

HOFFMAN, Frank G. Op. cit. sub. 4, str. 22.

KUBEŠA, Milan – SPIŠÁK, Ján. *Hybridní hrozby a vývoj nové operační koncepce NATO* [online]. 2011 [cit. 2019-07-03]. Dostupné z: https://www.obranaastrategie.cz/cs/aktualni-cislo-2-2011/clanky/hybridni-hrozby-a-vyvoj-nove-operacni-koncepce-nato.html

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102

Report on Preliminary Examination Activities 2018 [online]. The Office of the Prosecutor, International Criminal Court, odstavec 68. [cit. 2019-07-16]. Dostupné z: https://www.icc-cpi.int/itemsDocuments/181205-rep-otp-PE-ENG.pdf. Působení Ruska je dle publikace HOFFMAN, Frank G. 2007a. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 72 s., novodobým typem vedení.

DOI https://doi.org/10.24132/ZCU.2021.09228.89-102