Převzato

Redakce Vojenských rozhledů vám představuje článek RNDr. Pavla Štalmacha, MBA bývalého prvního náměstka ministra obrany a předsedy Krizového štábu Ministerstva obrany, který v současné době působí jako pracovník Ministerstva obrany. Článek byl pod názvem „Hybridní hrozby – včera, dnes a zítra - pohled z Prahy" zveřejněn v časopise Czech Industry č. 3/2018.

Hybridní hrozby – včera, dnes a zítra – pohled z Prahy

RNDr. Pavel Štalmach, MBA

HYBRIDNÍ BEZPEČNOSTNÍ HROZBY

V rámci nejrůznějších diskusí o stavu a vývoji bezpečnostního prostředí v posledních letech se stále více vyskytují pojmy jako hybridní hrozby, hybridní působení nebo hybridní konflikty a války. O těchto pojmech se často mluví jako o nových fenoménech, které stále více poznamenávají charakter dnešního i budoucího bezpečnostního prostředí.

Slovo hybridní (mimochodem tento pojem se poprvé objevil v biologii) má zcela jasný věcný význam. **Hybridní znamená vzniklý smíšením nebo křížením nějakých entit podle toho, jestli výsledkem je entita složen**á z původních entit **a zachovávající jejich původní vlastnosti nebo zcela nová entita, jejíž vlastnosti mohou být od vlastnosti původních entit odlišné i zcela nové.** Proces hybridizace může probíhat a také reálně probíhá v nejrůznějších přírodních i společenských systémech jako jedna z důležitých procesních optimalizačních metod v rámci evolučního vývoje.

Bezpečnostní prostředí je takové prostředí, jehož vývoj určují bezpečnostní aktéři, kteří prostřednictvím vytváření a nasazení bezpečnostních hrozeb či bezpečnostních protiopatření negativně nebo pozitivně ovlivňují míru ohrožení (stability, fungování, existence) prvků v prostředí či dokonce celého prostředí a tím realizují své zájmy. I v rámci bezpečnostního prostředí mohou probíhat nejrůznější hybridizační procesy, jejichž obecným cílem je vytváření takových efektivních asymetrií, bez nichž nelze dosáhnout požadovaného stavu bezpečnostního prostředí.

V rámci bezpečnostního prostředí probíhají hybridizační procesy především na 2 základních úrovních (tab. č. 1):

- **na úrovni bezpečnostních aktérů a jejich zájmů, které realizují prostřednictvím změn stavu bezpečnostního prostředí;**
- **na úrovni bezpečnostního působení, které je vytvářeno prostřednictvím vytvářených bezpečnostních schopností a jejich nasazení (bezpečnostní činnosti).**

Tabulka č. 1: Hybridní struktury v rámci bezpečnostního prostředí

	1 forma bezpečnostního působení	**2 a více společně realizovaných forem bezpečnostního působení**
1 bezpečnostní aktér	Jednoduché (generické) hrozby	Hybridní působení bezpečnostního aktéra
2 a více bezpečnostních aktérů	Bezpečnostní působení hybridního aktéra	Hybridní hrozby

V rámci hybridního bezpečnostního působení se v bezpečnostním prostředí kombinují nejrůznější nástroje (formy) bezpečnostního působení schopné způsobit změnu stavu bezpečnostního prostředí, zejména pak:

- vojenské (bezpečnostní) nástroje;
- politické nástroje;
- ekonomické nástroje;
- civilní nástroje;
- informační (a dezinformační) nástroje.

Jejich vzájemné kombinování se provádí tak, aby díky optimální volbě vzájemné synchronizace a dynamické intenzity bylo dosaženo maximálního efektu bezpečnostního působení.

Hybridizace bezpečnostního prostředí není ničím novým, probíhá v něm odjakživa (např. společné působení vojenských jednotek a lidových milicí, hybridní působení zpravodajských služeb, fungování mezinárodních bezpečnostních resp. vojenských aliancí atd.)**. V průběhu historie se samozřejmě různě měnily formy, rozsah a dynamika hybridizace.**

Historicky se vyvíjející hybridizaci bezpečnostního prostředí významně ovlivnil jak obsah bezpečnostních střetů, tak i technologický vývoj a jeho implementace v prostředcích hybridního bezpečnostního působení.

Na rozdíl od historických střetů o území, suroviny či obchodní příležitosti se hlavním cílem budoucích bezpečnostních střetů stane prostor životních příležitostí. **Hlavním cílem bezpečnostního působení bude stále méně ničení nějakých materiálních aktiv a stále více především účelové ovládnutí chování jejich vlastníků či uživatelů.**

Na rozdíl od silových letálně vedených bezpečnostních střetů se hlavní formou vedení bezpečnostních střetů stane vedení střetů v neletálním, často dokonce i jen virtuálním, prostředí. Časově omezené bezpečnostní především materiální střety se budou stále více měnit na permanentní nemateriální informačně-psychologické střety (válka vjemů).

Hlavními důvody pro měnící se úroveň hybridizace bezpečnostního prostředí byly a nadále především budou:

- **rostoucí cena materiálních bezpečnostních střetů;**
- **rostoucí počet obětí bezpečnostních střetů;**
- **rostoucí společenská neochota nést přímé následky bezpečnostních střetů.**

V historickém kontextu lze vysledovat i některé základní trendové změny ve vyvíjejícím se bezpečnostním prostředí generované jeho stále větší hybridizací – viz. následující tabulka (tab. č. 2).

Tabulka č. 2: Vývoj hybridizace bezpečnostního prostředí (hlavní trendy)

Minulost	Dnešek	Budoucnost
Propojování zájmů zejména nestátních bezpečnostních aktérů Účelová propojení bezpečnostních aktérů Přímé bezpečnostní působení (zničení) Převaha vojenských schopností a činností Převaha materiálních prostředků bezpečnostního působení	Propojování zájmů zejména státních bezpečnostních aktérů Operační aliance bezpečnostních aktérů Přímé bezpečnostní působení a bezpečnostní ovlivňování Rovnováha vojenských a nevojenských schopností činností Kombinace materiálních a nemateriálních prostředků bezpečnostního působení	Propojování zájmů státních a nestátních aktérů Strategické aliance bezpečnostních aktérů Bezpečnostní ovlivňování (rozklad) Převaha nevojenských schopností a činností Převaha nemateriálních prostředků bezpečnostního působení

ELIMINACE HYBRIDNÍCH BEZPEČNOSTNÍCH HROZEB

Eliminace hybridních bezpečnostních hrozeb (ale i pouze hybridního bezpečnostního působení) probíhá sice stejným procesem jako u jednoduchých bezpečnostních hrozeb, ale musí se vyrovnat se všemi specifiky vytváření a působení hybridních bezpečnostních hrozeb.

Eliminace každé bezpečnostní hrozby je založena na její identifikaci, na vytvoření adekvátních bezpečnostních schopností pro zajištění její eliminaci (pro ochranu a obranu) a na efektivním nasazení těchto schopností k zajištění její eliminace. Specifičnost hybridních bezpečnostních hrozeb a jejich působení (strukturální složitost) především vždy vyžaduje hybridní eliminaci – a to jak z pohledu vytvářených bezpečnostních systémů, tak i z pohledu tvorby relevantních bezpečnostních schopností a činností pro řešení mimořádných a krizových situací vyvolaných hybridními bezpečnostními hrozbami (tab. č. 3).

Tabulka č. 3: Eliminace hybridních bezpečnostních hrozeb

Úroveň působení bezpečnostních hrozeb	Eliminace jednoduchých bezpečnostních hrozeb	Eliminace hybridních bezpečnostních hrozeb
Mimořádné situace	**Standardní bezpečnostní systémy**	**Systémy pro eliminaci hybridních hrozeb**
Krizové situace	**Systémy pro eliminaci krizových situací**	**Systémy pro eliminaci hybridních hrozeb**

Dnešní bezpečnostní praxe ukazuje, že:

- v situacích, kdy hybridní bezpečnostní působení nedosáhne úrovně vzniku krizových situací, ale pouze úrovně vzniku mimořádných událostí, nejsou standardní bezpečnostní systémy schopny zajistit adekvátní eliminaci takového působení;
- v situacích, kdy hybridní bezpečnostní působení dosáhne úrovně krizových situací, není možné zajistit adekvátní eliminaci takového působení bez významného prohloubení míry integrity a integrability v rámci standardních bezpečnostních systémů, zejména pak v oblasti jejich řízení.

Bez vytvoření nových adekvátních „hybridních bezpečnostních struktur" není reálné zajistit efektivní eliminaci hybridních bezpečnostních hrozeb resp. eliminaci hybridního bezpečnostního působení.

Výše uvedené tvrzení je možné dokumentovat i již nabytými zkušenostmi z dosavadní realizace opatření v oblasti identifikace hybridních bezpečnostních hrozeb. Identifikace hybridních bezpečnostních hrozeb (tj. identifikace konkrétních hybridních struktur a jejich vlastností) je vždy primárním a neopominutelným krokem z pohledu jejich následné eliminace. Identifikace a evaluace běžných jednoduchých bezpečnostních hrozeb se provádí prostřednictvím standardních zpravodajských činností realizovaných relevantními zpravodajskými či dalšími bezpečnostními institucemi.

Identifikace a evaluace hybridních bezpečnostních hrozeb vyžaduje provádění adekvátních zpravodajských činností v podstatně širším prostoru pro hledání koincidence mezi různými ději v různých relevantních prostředích (strategické, operační, bezpečnostní).

Dnes jsou tyto zpravodajské činnosti realizovány převážně v sektorové formě. Shromažďování a adekvátní koincidenční a kontextová analýza informací nezbytná pro identifikaci a evaluaci hybridních bezpečnostních hrozeb se dnes ukazuje jako největší procesní problém v oblasti eliminace hybridních bezpečnostních hrozeb. Ukazuje se i fakt, že jednoduchá koordinace resp. integrace existujících zpravodajských či dalších bezpečnostních institucí v národním nebo mezinárodním měřítku je často procesně velmi složitá (bezpečnost informací, mocenské či politické problémy) a efektivnost takového postupu je velmi malá. Bez vytvoření dostatečně „hybridních" nových identifikačních a evaluačních struktur v rámci existujících bezpečnostních systémů tento stav ale zjevně nezměníme (tab. č. 4)..

Tabulka č. 4: Model procesní „hybridní" struktury pro identifikaci a evaluaci hybridních bezpečnostních hrozeb

Hybridní struktura	Sektorová struktura – FUSION CELL	Datová struktura
Identifikace koincidencí (hybridních struktur)	Identifikace bezpečnostních událostí	Shromažďování a anonymizace dat (ochrana zdrojů)

HYBRIDNÍ BEZPEČNOSTNÍ HROZBY A ČESKÁ REPUBLIKA

Česká republika (jako novodobý nástupce československého státu vzniklého v roce 1918) se po svém vzniku v roce 1993 stala novým samostatným prvkem globálního bezpečnostního prostředí, a tím také objektem i subjektem jeho probíhající hybridizace.

Vzhledem ke geografickému, ekonomickému i politickému zakotvení Česká republika **je a jistě i dále bude předmětem nejenom různého konkrétního hybridního bezpečnostního působení různých bezpečnostních aktérů, ale i předmětem konkrétního bezpečnostního působení velmi komplexních hybridních aktérů.** V rámci strategických dokumentů České republiky i mezinárodních institucí, jejichž je Česká republika členem, lze nalézt řadu explicitních vyjádření o nutnosti zajištění efektivní eliminace hybridních

bezpečnostních hrozeb. Lze také sledovat různé pokusy o implementaci různých konkrétních aktivit zaměřených na tvorbu schopností využitelných v rámci procesu eliminaci hybridního bezpečnostního působení resp. hybridních bezpečnostních hrozeb.

Asi nejvýznamnější tlak na implementaci řešení problematiky hybridních bezpečnostních hrozeb působících na Českou republiku vytvořil Audit národní bezpečnosti, provedený v roce 2016 a na něj navazující akční plán další optimalizace bezpečnostního systému České republiky. V akčním plánu je problematice hybridních bezpečnostních hrozeb věnována celá jedna samostatná kapitola, v níž je specifikováno 13 konkrétních kroků (cílů) zaměřených především na zajištění adekvátních bezpečnostních schopností pro efektivní eliminaci hybridních bezpečnostních hrozeb.

V České republice, stejně jako u řady dalších států, je základním problémem zajištění odolnosti vůči působení hybridních bezpečnostních hrozeb realizace takových konkrétních kroků, které by tuto odolnost dokázaly reálně ovlivnit a přiměřeně zvýšit. Přitom **je nutné si uvědomit, že tyto kroky musí učinit aktuálně právě především státy, nikoliv mezinárodní instituce, a to proto, že:**

- **předmětem hybridního působení jsou dnes především státy a jejich aktiva;**
- **většina potřebných schopností k eliminaci hybridních hrozeb stejně musí vzniknout na úrovni států (v rámci mezinárodních institucí může pak dojít k jejich koordinaci resp. integraci).**

V České republice je v současné době klíčovým a zlomovým krokem v oblasti řešení problému eliminace hybridních bezpečnostních hrozeb vytvoření adekvátního procesního mechanismu schopného reálně identifikovat a evaluovat konkrétní hybridní bezpečnostní hrozby působící na Českou republiku – což je mimochodem i první úkol v kapitole akčního plánu k Auditu národní bezpečnosti, která se zabývá problematikou hybridních bezpečnostních hrozeb. Tento proces, vycházející ze sběru širokého spektra relevantních dat i informací, musí zajistit takové zpravodajské informace, které především umožní racionální a efektivní rozhodování (a následné plánování) o konkrétním způsobu eliminace identifikované hybridní bezpečnostní hrozby. Teprve, až takový proces bude popsán, je totiž smysluplné a prakticky možné přemýšlet o jeho zdrojovém, institucionálním a právním rámci. Zde je i stále více zjevné, že pokud se co nejdříve nepodaří těmto krokům dát potřebný projektový charakter, bude Česká republika z hlediska vytváření své odolnosti proti hybridním bezpečnostním hrozbám stále v bodě nula.

Pokud již bude možné identifikovat konkrétní hybridní bezpečnostní hrozby působící na Českou republiku, bude možné i přistoupit k jejich eliminaci. Pak bude velmi důležité, jaká bude úroveň konkrétního hybridního bezpečnostního působení na Českou republiku.

V případě, že hybridní bezpečnostní působení bude pouze na úrovni vzniku mimořádných událostí, bude muset jeho eliminaci zajistit standardní bezpečnostní systém České republiky.

V případě, že hybridní bezpečnostní působení povede až ke vzniku krizových situací, bude muset jeho eliminaci zajistit specifický systém krizového řízení vytvořený nad standardním bezpečnostním systémem České republiky.

V obou dvou případech bude ale nutné:

- adekvátně optimalizovat existující schopnosti využitelné k eliminaci hybridního bezpečnostního působení, které jsou k dispozici v rámci bezpečnostního systému České republiky;
- doplnit bezpečnostní systém České republiky o nové schopnosti využitelné k eliminaci hybridního bezpečnostního působení, které zatím nejsou k dispozici v rámci bezpečnostního systému České republiky;
- doplnit systém řízení bezpečnostního systému České republiky o adekvátní složky operačního řízení, které zajistí při všech stavech bezpečnostního prostředí nezbytnou úroveň koordinace a integrace činností v rámci procesu eliminace hybridního bezpečnostního působení (adekvátní hybridnost bezpečnostních protiopatření).

K naplnění takových výše uvedených kroků bude jistě vhodné využít i již existující rámec aktuálně probíhající optimalizace procesu zajišťování obrany České republiky v rámci implementace Ústředního plánu obrany státu nebo plánované optimalizace zpravodajského systému České republiky atd.

Bylo by ale i skvělé, kdyby se ve veřejném prostoru v České republice brzo objevil i nějaký „PAN HYBRID“ (např. v roli „národního bezpečnostního poradce“, jak předpokládá v souvislosti s aktivitami v boji proti hybridním hrozbám generální tajemník NATO), schopný všechny další kroky adekvátně prezentovat a prosazovat.