2. BLOK · STRATEGICKÁ SUVERENITA A ZPRAVODAJSTVÍ

Nechceme Palantir. Chceme vlastní digitální mozek české armády

Petr Mlejnek · bývalý ředitel ÚZSI

Zápis z přednášky na konferenci IIČR 2026

Informace, inteligence a čas na rozhodnutí · 19. 11. 2026 · CEVRO Univerzita, Praha
AFCEA Česká pobočka, pracovní skupina PS07 Intelligence · CRIK při CEVRO Univerzitě
Stav 20. 11. 2026 · https://iicr.afcea.cz/zaznelo/



2. BLOK · STRATEGICKÁ SUVERENITA A ZPRAVODAJSTVÍ

Petr Mlejnek

bývalý ředitel ÚZSI

Nechceme Palantir. Chceme vlastní digitální mozek české armády

Petr Mlejnek, bývalý ředitel ÚZSI, se ptal, jestli má česká armáda „digitální mozek“, tedy systém, který propojuje senzory, data, umělou inteligenci a rozhodování velitele, koupit od americké firmy Palantir, nebo si ho postavit sama. Podle něj Palantir není špatná technologie. Hlavním rizikem je strukturální závislost na jednom zahraničním dodavateli. Navrhl českou národní platformu po vzoru ukrajinského systému Delta, kterou bude možné na Palantir napojit.

Zkušenost výsadkáře a zpravodajce

Řečník začal tím, odkud přichází. Několik let sloužil v armádě u výsadkových jednotek, kde mu velel Aleš Opata. Potom ho vybrala zpravodajská služba a několik let v ní působil jako operativec. Na začátku absolvoval několikaměsíční zpravodajský institut. Podle jeho vzpomínky tam první den platila zásada nevěřit nikomu a sobě jen napůl. Ta mu prý mnohokrát pomohla. Z tohoto pohledu chtěl vysvětlit, proč Česko podle něj nepotřebuje Palantir, ale vlastní digitální mozek armády. Připomněl také, že i přes spojenectví se Spojenými státy má střední Evropa se závislostí na velmocích opakovaně špatné zkušenosti.

Válka na Ukrajině podle něj změnila představu o vedení vojenských operací. Nerozhoduje už jen počet tanků, děl, letadel a raket. Stále víc rozhoduje schopnost propojit senzory, data, umělou inteligenci a zbraně do jednoho funkčního systému. Klíčová je rychlost celého cyklu, od získání informace přes její vyhodnocení po rozhodnutí velitele. Volba mezi nákupem a vlastním vývojem proto už podle něj není jen technická nebo ekonomická otázka.

Palantir v Evropě: rozsah a ústup

Řečník uvedl, že novinářská pátrání ukázala, jak hluboko pronikla americká společnost Palantir do evropských bezpečnostních struktur. Evropské veřejné zakázky firmy podle něj dosahují zhruba 1,4 miliardy eur. Její software používají armády, zpravodajské služby, policie i civilní infrastruktura. Zdůraznil, že není odpůrcem amerických technologií a že Palantir patří ke špičce v integraci dat, vojenské analytice a podpoře rozhodování. Problém nastává podle něj ve chvíli, kdy se výkonný systém stane tak důležitou součástí státní infrastruktury, že ho stát už nedokáže vyměnit.

Představil hlavní platformy firmy. Gotham slouží zpravodajským službám a policejní analýze, tedy propojování databází a vazeb (linkové analýze). Foundry slouží k integraci dat, analytice a řízení procesů. Maven Smart System vytváří vojenský operační obraz a podporuje rozhodování pomocí AI. Nad nimi stojí vrstva AIP s generativní umělou inteligencí. Gotham podle něj používá policie v Dánsku, Finsku, Norsku, Nizozemsku a Švédsku, dále vybrané instituce v Německu a Velké Británii. Dánsko ho používá i pro zpravodajství včetně Grónska. Mezi riziky zmínil integraci citlivých databází a obtížnou migraci z platformy. Uvedl také objemy zakázek: Velká Británie kolem 992 milionů liber, Německo kolem 86 milionů liber, Litva 67 milionů eur, španělské ministerstvo obrany 16,5 milionu eur a Itálie 6,2 milionu eur.

Potom popsal, proč evropské státy spolupráci přehodnocují. Švýcarská armáda nabídky opakovaně odmítla. Kromě etických výhrad šlo o obavy z technické závislosti a z možného přístupu americké strany k citlivým vojenským datům. Francie oznámila, že její vnitřní zpravodajská služba po skončení současné smlouvy už ji neobnoví, aby se vyhnula strategické závislosti. Dánsko zastavilo pokročilá jednání o systému Maven kvůli Grónsku, protože podle řečníka přestalo Američanům věřit. V Německu Palantir používají některé policejní instituce, ale představitelé vojenského velení mají zásadní výhrady k jeho nasazení v Bundeswehru.

Jako zvlášť zajímavý uvedl příklad Izraele, který je jedním z nejbližších technologických a bezpečnostních partnerů USA. Podle izraelských médií jednotka vojenského zpravodajství 8200 a bezpečnostní služba Šin Bet po testování některých řešení nepřistoupily na navrhované partnerství s Palantirem. Řečník upozornil, že to neznamená úplné přerušení spolupráce. Ukazuje to ale, že Izrael má vlastní schopnosti, a proto si může vybírat, které zahraniční technologie přijme. V tom viděl podstatu diverzifikace bezpečnosti.

Největším rizikem je závislost, ne únik dat

Přístup americké firmy k citlivým evropským datům označil řečník za legitimní bezpečnostní otázku. Zmínil přístup některých zaměstnanců Palantiru k utajovaným informacím v nizozemském obranném prostředí. Nizozemské ministerstvo podle něj poté omezilo zahraniční pracovníky a oznámilo, že hledá evropskou alternativu. Zároveň upozornil, že technické oprávnění dodavatele k přístupu není totéž co prokázané neoprávněné předání utajovaných informací.

I kdyby však byla všechna data bezpečně chráněna, hlavní problém by podle něj nezmizel. Tím je strukturální závislost. Pokud stát postaví na jedné zahraniční platformě operační obraz, analytické procesy, propojení dat, umělou inteligenci a část velení a řízení, stane se na ní postupně závislým. Změna dodavatele pak neznamená jen nákup nového softwaru. Vyžaduje přestavbu datových modelů, rozhraní, bezpečnostních pravidel, pracovních postupů a výcviku. Řečník si nedokázal představit Palantir například v systému mobilizace, protože by Američané dostali data o českých občanech nebo přístup k rozmístění protivzdušné obrany na českém území. Chápe, že vrchní velitel spojeneckých sil v Evropě (SACEUR) chce jeden operační systém typu Maven. Pro jednotky vyslané v rámci aliance s tím počítal. Na území České republiky ale podle něj musí běžet vlastní systém velení a řízení.

Umělá inteligence jako asistent velitele

Umělá inteligence podle řečníka zásadně zrychluje zpracování zpravodajských informací, rozpoznávání objektů, analýzu obrazu, hledání souvislostí a podporu rozhodování. Moderní velitelské stanoviště přijímá data z tolika senzorů, že je člověk nestihne průběžně vyhodnocovat. AI tak může sloužit jako analytický asistent: upozornit na změny v rozmístění protivníka, propojit zdroje, najít nesrovnalosti a navrhnout varianty postupu. Může ale také pracovat s neúplnými nebo chybnými daty, dojít k přesvědčivým, a přesto mylným závěrům a protivník se může pokusit data zmanipulovat. Když se rozhoduje o použití síly, musí být podle něj ověřitelný původ informací i spolehlivost výstupu a jasná odpovědnost za rozhodnutí. AI má být nástrojem velitele, ne neprůhlednou autoritou.

Připomněl, že AI mají k dispozici i protivníci. Podle zprávy společnosti Anthropic se někteří aktéři v Jemenu pokoušeli využít model Claude při práci na softwaru pro navádění raket. Hútíové používají íránské rakety a AI jim může pomoci se simulacemi a s diagnostikou existujících problémů. Řečník dodal, že neexistuje důkaz, že by takto vyrobili novou použitelnou raketu. Offline nástroje však mohou fungovat i po zablokování přístupu k modelu.

Ukrajinská Delta jako vzor

Řečník byl v poslední době několikrát na Ukrajině a ukrajinský přístup hodnotil velmi pozitivně. Ukrajina Palantir používá, ale od roku 2016 vyvíjí vlastní vojenský digitální ekosystém Delta. Ten propojuje situační obraz, bezpilotní prostředky, senzory a operační informace. Delta Monitor vytváří operační obraz, systém Vezha zpracovává obrazová data z dronů a Target Hub a Mission Control koordinují informace z bezpilotních jednotek. Celek je propojen i s Palantirem. Ukrajinci podle něj pochopili, že nestačí koupit nejlepší zahraniční software. Je potřeba mít vlastní vývojové týmy, vlastní data, vlastní integrační architekturu a umět systém neustále upravovat podle zkušeností z bojiště. Dodal, že Ukrajina nabízí svá data a Česko by tak mohlo pracovat s reálnými daty z bojiště.

Návrh české národní platformy

Armáda podle řečníka zvažuje investici kolem 50 milionů dolarů do systému Palantir. Částku je podle něj potřeba ověřit proti rozsahu případné zakázky. Než ale padne rozhodnutí, je třeba se zeptat, jestli by za tyto peníze nebylo lepší vybudovat vlastní národní schopnost. České firmy mají zkušenosti se systémy velení a řízení, geografickými informačními systémy, komunikacemi, kybernetickou bezpečností, datovou analytikou i umělou inteligencí. Nemusí se proto začínat od nuly. Chybí hlavně společná architektura, která tyto schopnosti propojí.

Architekturu popsal v modulech:

Společná operační mapa je jednotný geoinformační obraz v reálném nebo téměř reálném čase. Ukazuje vlastní jednotky, potvrzené a předpokládané pozice protivníka, senzory, drony, komunikační uzly, logistiku, klíčovou infrastrukturu a geografická data. Kdo co vidí, určuje oprávnění, stupeň utajení a princip need-to-know.

Otevřená integrace a fúze dat stojí na dokumentovaných rozhraních pro radary, drony, družice, elektrooptiku a logistické systémy. Nový senzor se připojí přes rozhraní a jádro systému zůstane beze změny. Hlášení o stejném objektu z družice, dronu nebo od vojáka se spojí do jednoho záznamu a ověří z více zdrojů. Velitel vidí zdroje, míru jejich důvěryhodnosti a nejistotu výsledku. Samostatné moduly umožní vyměnit dodavatele AI modulu i rozhraní.

AI a simulace pod odpovědností velitele: AI shrnuje situaci, porovnává ji s historií a upozorňuje na změny a anomálie. Simulace porovnává varianty podle terénu, sil, logistiky a pokrytí senzory. Ke každému závěru musí jít dohledat podklady. Rozhodovat musí člověk a celý proces musí být auditovatelný, aby se dalo zpětně ověřit, z jakých informací velitel vycházel.

Video a Mission Control: po vzoru systému Vezha systém přijímá souběžné přenosy z více senzorů a označuje objekty, změny v terénu a anomálie. Zabezpečený archiv slouží k následné analýze a k přípravě trénovacích dat. Mission Control eviduje stav, dostupnost a operátory dronů od různých výrobců, plánované úkoly, historii a telemetrii.

Česká trénovací data a vojenská AI: vlastní data mají vznikat od prvního dne při cvičeních, testech a simulacích a doplňovat je data z provozu dronů. Jako vzor zabezpečeného vývojového prostředí uvedl ukrajinské Brave1 Data Room a Avengers Lab. České firmy a výzkumné týmy v nich pracují s prověřenými a očištěnými (sanitizovanými) daty, oddělenými od operačních systémů armády. Podle řečníka platí, že i u Palantiru provozovaného na vlastních serverech bude mít vždy někdo přístup, a to považoval za velké bezpečnostní riziko.

Odolnost a bezpečnost: centrální, regionální a taktické uzly nesmějí mít jediný kritický bod. Základní velení a řízení musí fungovat i při výpadku internetu nebo cloudu. Jako příklad uvedl odpojování služeb Starlink a Starshield na Ukrajině pod tlakem Spojených států. Systém má stát na principu Zero Trust, tedy ověřovat identitu a oprávnění každého uživatele, zařízení i služby, a auditovat přístupy k datům, jejich změny i předávání informací. Bránou má být české jádro propojené se spojenci, včetně napojení na Palantir, který používá SACEUR.

Na závěr shrnul svůj návrh. Při investici kolem 50 milionů dolarů by dal přednost českému jádru, tedy jakési české Deltě pro Armádu České republiky. Taková investice rozvíjí domácí datovou infrastrukturu, know-how a vojenskou AI. Palantir může přispět zkušenostmi a propojitelností se spojenci. Armáda však musí být schopna měnit software i v krizi podle svých potřeb. Digitální suverenitu označil za obrannou schopnost. Palantir se má připojit k českému systému, ne český systém vzniknout jako nákup od Palantiru.

Dotazy a diskuse

V čem je český softwarový ekosystém pro armádu nejsilnější a jaké výhody by vlastní systém přinesl?

> Pokud vlastní systém dodají české firmy, má stát podle řečníka vůči dodavatelům mnohem větší vliv a celé řešení je efektivnější. Uvedl příklad: kdyby za války protivník nasadil jiný typ raket a bylo nutné rychle upravit aplikaci protivzdušné obrany, na zahraničního dodavatele by se mohlo čekat měsíce, kdežto česká firma úpravu naprogramuje hned. Druhou výhodou je ochrana dat o českých občanech, území a geografii.

Co dnes brání tomu, aby se věci vyvíjely žádoucím směrem, a jaký je nejdůležitější další krok?

> Řečník doporučil zpracovat případové studie a analýzu rizik, které ukážou, která varianta je lepší a která horší. Za cestu do pekel označil rozhodování podle toho, co někdo uvidí na zahraniční služební cestě, bez posouzení jiných možností. Moderátor jeho přání podpořil, ale řekl, že je vzhledem k současné situaci mírně skeptický.

Co z přednášky plyne pro stát

- Před rozhodnutím o investici kolem 50 milionů dolarů do systému Palantir zpracovat případové studie a analýzu rizik, které porovnají zahraniční platformu s vybudováním vlastní národní schopnosti.
- Systém velení a řízení na území ČR, mobilizaci a data o občanech a rozmístění protivzdušné obrany provozovat na vlastní platformě. Spojeneckou platformu (Palantir, Maven) používat pro jednotky nasazené v rámci aliance a napojit ji na české jádro přes bránu.
- Postavit modulární národní architekturu (společná operační mapa, otevřená rozhraní a fúze dat, auditovatelná AI pod odpovědností velitele, video a Mission Control, odolnost bez jediného kritického bodu, Zero Trust) z existujících schopností českých firem, s vyměnitelnými dodavateli modulů.
- Od prvního dne sbírat vlastní trénovací data z cvičení, testů, simulací a provozu dronů a zřídit zabezpečené vývojové prostředí, kde české firmy a výzkumné týmy pracují s očištěnými daty oddělenými od operačních systémů, podle vzoru Brave1 Data Room. Využít nabídku dat z ukrajinského bojiště.

- Zajistit, aby armáda mohla měnit software i v krizi podle vlastních potřeb a aby základní velení a řízení fungovalo i bez internetu, cloudu nebo satelitního spojení cizího poskytovatele.

Co řekl sál

Na čem má stát stavět svou technologickou sílu? n = 34



Otázky ze sálu poslané přes aplikaci

- Jak moc vnímáte to, že hlavním nebezpečím Palantiru je jeho majitel/zakladatel Petr Thiel?

Zápis pořadatelů ze strojového přepisu, ne autorizovaný text řečníka. Citace zveřejníme až po schválení řečníkem. Opravy: ps07@afcea.cz.

Čtení pořadatelů, ne společné stanovisko řečníků. Zápisy vycházejí ze strojového přepisu konference, ankety vyjadřují názor sálu, ne reprezentativní průzkum. Citace řečníků zveřejníme až po jejich schválení. Opravy a dotazy: ps07@afcea.cz. Volně k použití s uvedením zdroje „IICR 2026, AFCEA Česká pobočka“. Více na https://iicr.afcea.cz/zaznelo/