Nechceme Palantir. Chceme vlastní digitální mozek české armády

Palantir jako alianční nástroj ANO.

Jako nenahraditelné národní jádro NE.

Petr Mlejnek

VÝCHOZÍ TEZE

Moderní válka je soutěží rozhodovacích cyklů

- Senzory → data → analýza → rozhodnutí → efekt
- AI urychluje vyhodnocování a podporuje velitele
- Kontrola operačního softwaru se stává strategickou schopností

Co ukázala evropská investigace

- Palantir má evropské veřejné kontrakty v hodnotě přibližně 1,4 mld. EUR
- Působí v obraně, zpravodajství, policii i civilní infrastruktuře
- Část států spolupráci přehodnocuje; jiné ji dále rozvíjejí
- Částky zahrnují různé druhy smluv a plateb, nikoli pouze již uhrazené prostředky

Tři klíčové platformy

- GOTHAM — zpravodajské a policejní analýzy; propojení databází a vztahů
- FOUNDRY — datová integrace, analytika a řízení procesů
- MAVEN SMART SYSTEM — vojenský operační obraz a podpora rozhodování pomocí AI
- AIP — další vrstva pro využívání generativní AI

KDE SE POUŽÍVÁ

Gotham: bezpečnostní analýza

- Policie: Dánsko, Finsko, Norsko, Nizozemsko, Švédsko
- Další policejní nasazení: vybrané instituce Německa a Británie
- Dánsko: Pol-Intel, včetně Grónska
- Riziko: integrace citlivých databází a složitá migrace k jiné platformě

KDE SE POUŽÍVÁ

Foundry: datové jádro institucí

- Velká Británie: zdravotnictví NHS a další instituce
- Nizozemsko: využití také v obranném prostředí
- Silná stránka: sjednocení dat a pracovních postupů
- Riziko: postupné přenesení klíčových procesů na proprietární platformu

Maven: nejcitlivější vojenská vrstva

- Americké ozbrojené síly; NATO pořídilo Maven v březnu 2025
- Integrace informací ze satelitů, dronů, radarů a dalších senzorů
- AI podporuje identifikaci, situační povědomí a plánování
- Nesmí se zaměňovat podpora rozhodnutí s autonomním povolením úderu

PŘIBLIŽNÉ HODNOTY

Evropské kontrakty: zveřejněné částky

- Británie: 992 mil. GBP | Německo: 47–86 mil. EUR
- Litva: přes 67 mil. EUR | Norsko: cca 52 mil. EUR
- Dánsko: cca 28 mil. EUR | Španělsko: 16,5 mil. EUR
- Itálie: 6,2 mil. EUR | Europol: přes 4 mil. EUR
- Údaje mají různá období a metodiky; nejde o jednotný součet plateb

Kdo a proč přehodnocuje spolupráci

- Švýcarsko: obavy ze závislosti a ochrany vojenských dat
- Francie: snaha o strategickou autonomii zpravodajských služeb
- Dánsko: zastavení jednání o Maven v kontextu napětí kolem Grónska
- Belgie: odmítání nové spolupráce; Německo: výhrady v Bundeswehru
- Norsko: také právní překážky propojení policejních databází

Izrael: spolupráce i selektivní odmítnutí

- Palantir spolupracuje s izraelskými obrannými strukturami
- Podle investigace některé izraelské služby po testech nepřijaly navržené partnerství
- Odmítnutí konkrétního řešení neznamená konec veškeré spolupráce
- Vlastní technologický ekosystém umožňuje volbu a nezávislé posouzení

Čtyři strategická rizika

- DATOVÉ — přístupy, klíče, umístění a zpracování citlivých informací
- TECHNOLOGICKÉ — proprietární architektura a náklady na migraci
- OPERAČNÍ — schopnost rychle měnit systém během konfliktu
- POLITICKÉ — odlišné priority dodavatele a jeho domovského státu

AI: urychlení i nová zranitelnost

- Chybná nebo zastaralá data mohou vést k chybným analytickým závěrům
- Protivník se může pokoušet manipulovat senzorové a vstupní informace
- Nutnost ověřitelnosti výstupů a odpovědnosti velitele
- AI musí podporovat lidské rozhodování, nikoliv jej neprůhledně nahrazovat

AI také posiluje protivníka

- Podle Anthropic se aktéři v Jemenu pokoušeli využít Claude při práci na naváděcím softwaru
- AI může pomoci s programováním, simulacemi a diagnostikou existujících systémů

- Neexistuje důkaz, že by tím sami vyrobili novou operačně použitelnou raketu

- Offline nástroje mohou přetrvat i po zablokování přístupu k modelu

Ukrajina: národní ekosystém Delta

- Delta Monitor — společný operační obraz
- Vezha — práce s obrazovými daty z dronů
- Target Hub a Mission Control — koordinace informací a bezpilotních jednotek
- Ukrajina používá zahraniční technologie, ale rozvíjí vlastní digitální kompetenci

Jak má vypadat české řešení

- České národní jádro: data, pravidla, rozhraní, bezpečnost a vývoj
- Modulární integrace senzorů, dronů, geografických dat a AI
- Distribuovaný provoz a odolnost v degradovaném prostředí
- NATO Gateway: řízená interoperabilita s Maven a dalšími systémy
- Možnost vyměnit dodavatele bez ztráty národní operační schopnosti

Společná operační mapa

- Jednotný geoinformační obraz v reálném či téměř reálném čase
- Vlastní jednotky, potvrzené i předpokládané pozice protivníka, senzory a drony
- Komunikační uzly, logistika, klíčová infrastruktura a geografická data
- Rozsah zobrazení určuje oprávnění, stupeň utajení a princip need-to-know

Otevřená integrace a fúze dat

- Dokumentovaná rozhraní pro radary, drony, družice, elektrooptiku, elektronický průzkum a logistické systémy
- Nový senzor se připojí přes rozhraní, jádro zůstává beze změny
- Hlášení o stejném objektu se spojí do jednoho záznamu
- Velitel vidí zdroje, míru jejich důvěryhodnosti a nejistotu výsledku
- Samostatné moduly umožní vyměnit dodavatele, AI model i rozhraní

PODPORA ROZHODOVÁNÍ

AI, simulace a odpovědnost velitele

- AI shrnuje situaci, porovnává historii a upozorňuje na změny a anomálie
- Simulace porovnává varianty podle terénu, sil, logistiky a pokrytí senzory
- Ke každému závěru AI lze dohledat použité podklady
- Oprávněný člověk rozhoduje o krocích s významnými operačními nebo právními důsledky
- Audit zachytí dostupné podklady, doporučení AI a rozhodnutí člověka

Video a Mission Control

- Video podle vzoru Vezha přijímá souběžné přenosy z více senzorů
- AI označuje objekty, změny v terénu a další anomálie
- Bezpečný archiv slouží k následné analýze a přípravě trénovacích dat
- Mission Control eviduje stav, dostupnost a operátory dronů různých výrobců
- Přehled zahrnuje plánované úkoly, historii misí a telemetrii

Česká trénovací data a vojenský AI Dataroom

- Vlastní datasety vznikají od prvního dne při cvičeních, testech a simulacích
- Data z provozu dronů doplňují databázi zkušeností pro další vývoj
- Vzorem pro zabezpečené vývojové prostředí jsou Brave1 Dataroom a Avengers Labs
- České firmy a výzkumné týmy pracují s prověřenými a sanitizovanými daty v prostředí odděleném od operačních systémů AČR

Velení i při ztrátě spojení

- Centrální, regionální i taktické uzly fungují bez jediného kritického bodu
- Při výpadku internetu či cloudu zůstává dostupné základní velení a řízení
- Vybrané analytické a AI funkce běží lokálně. Po návratu spojení se změny bezpečně synchronizují.
- Zero trust ověřuje identitu a oprávnění každého uživatele, zařízení i služby
- Audit zaznamenává přístupy k datům, změny i předání dat

NATO Gateway propojí české jádro se spojenci

- Samostatná brána obousměrně převádí český datový model do standardů NATO
- Pravidla pro sdílení určují, která data mohou opustit české prostředí
- Palantir, Maven a další spojenecké systémy lze integrovat přes bránu
- Při změně aliančního standardu se upraví integrační vrstva

Česká Delta jako základ pro AČR

- Národní platforma může stavět na existujících českých technologiích
- Při uvažované investici kolem 50 mil. USD bych dal přednost českému jádru
- Investice rozvíjí domácí datovou infrastrukturu, know-how a vojenskou AI
- Palantir může přispět zkušenostmi a interoperabilitou se spojenci
- AČR musí mít možnost měnit software i v krizi podle vlastních potřeb

Co rozhodnout před případným nákupem

- Co přesně získáme: licence, provoz, integrace, zdrojové úpravy?
- Kdo kontroluje data, přístupy, kryptografické klíče a aktualizace?
- Jaké jsou náklady na celý životní cyklus a plán odchodu?
- Jak se zahraniční řešení srovnává s investicí do české platformy?
- Úvahy o 50 mil. USD nejsou ověřenou cenou konkrétní české zakázky

ZÁVĚREČNÉ SDĚLENÍ

Digitální suverenita je obranná schopnost

Palantir připojit k českému systému.

Ne český systém podřídit Palantiru.