Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

# Digitalizace obrany: Ochrana Evropy ve věku kvantových počítačů a cloudu

(Digitalising defence: Protecting Europe in the age of quantum computing and the cloud)

**Zdroj:** https://www.iss.europa.eu/content/digitalising-defence

**Autor**: Ústav Evropské unie pro studium bezpečnosti (Daniel Fiott)

Dokument pojednává o dopadech nových technologií na obranu. Jedná se například o internet věcí, kvantové počítače, umělou inteligenci, 5G sítě nebo cloud computing. Ačkoliv tyto technologie představují velkou příležitost, mohou také vytvořit nové zranitelnosti a v případě použití těchto technologií nepřítelem i nové hrozby. Evropa v současnosti nemá úplný přehled jak digitalizace ovlivní moderní konflikty a tudíž by měla tuto problematiku promítnout do současných nástrojů EU.

## Technologie

Dokument pojednává o dopadech nových technologií na obranu. Tyto technologie jsou například internet věcí, kvantové počítače, umělá inteligence, 5G sítě nebo cloud computing. Dokument zkoumá nové příležitosti, hrozby a zranitelnosti využívání těchto technologií v obraně.

V rámci NATO se jeho členové zavázali v roce 2016 k podpoře kapacit kybernetické obrany a EU má čtyři projekty ve spolupráci PESCO přímo zaměřené na kybernetickou obranu. V rámci Evropského programu rozvoje obranného průmyslu Evropská komise bude poskytovat 17,7 milionů Euro na činnost v kybernetické obraně. Pouze čas ukáže, jak tyto aktivity pomohou digitalizovat evropské armády.

Digitalizace v ozbrojených silách má za sebou již dlouhou historii. Od prvních primitivních počítačů k počítání balistiky artilerie, až po digitalizace komunikačních systémů současnosti.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

V roce 1990 Válka v Zálivu ukázala, jak technicky vyspělá vojenská síla (koalice v čele s USA) může v boji dominovat méně vyspělé konvenční síle (Irák), zejména díky použití GPS, digitální komunikaci, elektronickému boji a technologiím stealth. Americká invaze do Afghánistánu v roce 2001 však ukázala, že moderní technologie mají svoje limity, zejména v nekonvenčních konfliktech.

Na digitalizaci obrany se nedá pohlížet pouze ze směru nových příležitostí. Musí se také zohlednit nové potencionální hrozby a použití těchto technologií u protivníků. Například použití rozsáhlých informačních systémů otevírá dveře novým kybernetickým hrozbám. Většina Evropských armád si tyto nové hrozby uvědomuje a provádí opatření.

## Příklady technologií

Čím více budou evropské armády závislé na digitálních technologiích, tím více budou vznikat nové zranitelnosti, které bude potřeba ošetřit. Následují příklady technologií, které mají pro ozbrojené síly velký potenciál, ale zároveň vytvoří nové zranitelnosti/hrozby:

- Potenciál kvantových počítačů spočívá v tom, že jsou mnohonásobně rychlejší než ty klasické. Tím by mohly armády vytvořit mnohem účinnější kybernetickou ochranu díky lepšímu šifrování. Problém spočívá v tom, že infrastruktura kvantových počítačů je vysoce energeticky náročná a samotná technologie je velice citlivá na změny teplot. Ačkoliv by armády vyřešily problémy v oblasti kybernetické ochrany, vzniknou nové zranitelnosti v oblasti ochrany kritické infrastruktury.
- Dalším příkladem podobné technologie je využívání cloud computing (vzdálená počítačová infrastruktura poskytuje uživateli výpočetní výkon a ten nemusí mít k této infrastruktuře přístup). U těchto technologií je velkou zranitelností fakt, že 70 % tohoto trhu mají americké firmy, zatímco 7 % mají firmy čínské. V extrémních případech by tedy mohlo dojít k tomu, že by ozbrojené síly neměly přístup k vlastním informacím.
- Posledním příkladem je 3D tisk a nanotechnologie, při jejichž spojení už v současnosti existují sledovací zařízení o velikosti zrnka písku, které mohou při nasazení poskytnout

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

analýzu zeměpisné oblasti. Evropské armády nemají žádnou odpověď na takové technologie, ať k jejich detekci nebo ke zneškodnění.

## Závěr

Ačkoliv EU a členské země si uvědomují potenciál těchto technologií, v současnosti je jasné, že nejsou evropskými armádami zcela pochopené. Proto je potřeba, aby si zástupci EU a ozbrojených sil uvědomili nutnost vytvořit standardy, strategie a plány, které přesněji odhalí jak příležitosti, tak i zranitelnosti, které moderní digitální technologie mohou přinést. K tomu by mohlo pomoci zohlednění této problematiky do již existujících nástrojů, jako je spolupráce PESCO nebo Každoročního přezkumu v oblasti obrany CARD.