HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 4. szám 113–129.
DOI: 10.32567/hm.2022.4.8

Bihaly Barbara[1]

A felhőalapú szolgáltatások alkalmazása az amerikai haderőben, különös tekintettel a U.S. Army stratégiájára

The Use of Cloud-Based Services in the U.S. Military, Particularly in the Strategy of the U.S. Army

A rohamos technológiai fejlődésnek hála a kormányzati és a védelmi szerveknek is ideje modernizálni rendszereit. Ennek egyik lépése a felhőalapú szolgáltatások lehetőségeinek kiaknázása a kormányzati és rendvédelmi szférában. A cikk célja bemutatni a U.S. Army által kiadott két stratégiát a felhőalapú szolgáltatások alkalmazásáról.

Kulcsszavak: **felhőalapú szolgáltatások, Egyesült Államok, U.S. Army**

Thanks to rapid technological development, it is time for both government and defence agencies to modernise their systems. One step in this is to take advantage of the potential of cloud-based services in government and law enforcement. The purpose of this article is to present two strategies issued by the U.S. Army on the use of cloud-based services.

Keywords: **cloud computing, United States, U.S. Army**

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: bihaly.barbara@hm.gov.hu

1. Bevezetés

Az elmúlt évtizedekben rohamos technológiai fejlődésnek lehettünk tanúi, amellyel egyidejűleg exponenciálisan megnőtt a társadalom függősége az infokommunikációs rendszerektől. Ezek az új technológiák felgyorsítják a folyamatokat, költséghatékonyak és egyre szélesebb körben elérhetőek. Ugyanakkor megnőtt a biztonság iránti igény is, ez pedig felveti az egyes technológiák biztonságosságának és alkalmazhatóságának kérdéseit

Napjaink egyik kiemelkedő technológiai trendje a felhőalapú rendszerek térnyerése a piacon. A Microsoft jelentései már 2016-ban és 2017-ben is, a negyedéves eredménybeszámolókban rendre a felhőszolgáltatást emelték ki mint meghatározó húzóágazatot.[2]

A fő kérdés a felhőalapú rendszerekkel kapcsolatban, hogy mennyire biztonságosak és mennyire ellenőrizhetők? Elsődleges, hogy a megfelelő biztonság garantálható legyen a felhasználónak. Másrészről a hatóságoknak és védelmi szerveknek meg kell győződniük arról, hogy az adott rendszer megfelelőséget mutat az egyes, meghatározott biztonsági követelményeknek, ugyanakkor tisztában kell lennünk a fennmaradó biztonsági kockázatokkal is.[3]

Abban az esetben, ha ilyen új típusú rendszereket szeretnénk integrálni a meglévő (hon)védelmi rendszerekbe, akkor felvetődik a törvényes ellenőrzés problematikája is. Az informatikai rendszerekkel kapcsolatos biztonsági követelmény legpontosabb megfogalmazása a CIA- (*confidentiality* – bizalmasság, *integrity* – sértetlenség, *availability* – rendelkezésre állás) alapelv.[4]

Viszont, a rendkívül gyors ütemű technológiai fejlődéssel együtt jár az is, hogy a védelmi szféra, a haderők sem kerülhetik el a felhőalapú szolgáltatások alkalmazását.

A 2000-es években a világ egyik vezető hadereje, az amerikai haderő is felfedezte a felhőalapú szolgáltatásokban rejlő lehetőségeket. Egy 2016-ban kezdődő pilotprogrammal – hibrid felhőkörnyezettel – kezdték meg a felhőalapú rendszerek integrálását a könnyebb információmegosztás érdekében. Ez a hibrid felhőkörnyezet magában foglalta a helyszíni Védelmi Minisztériumi (Department of Defence, DoD) felhőkörnyezetek kombinációját, például a DoD-létesítményben elhelyezett milCloudot, valamint a kereskedelmi felhőszolgáltatókat és a nem helyszíni szövetségi felhőkörnyezeteket, például azokat, amelyeket más szövetségi ügynökségek üzemeltetnek.[5]

Habár a felhőalapú rendszereknek sok előnye van, felmerül, hogy milyen keretekben használhatók katonai célokra, és mennyi kockázatot rejtenek magukban, illetve kielégítik-e a CIA-alapelvet?

E felvetések okán jelen cikk célja bemutatni, milyen tervei, törekvései és szabályzói vannak az amerikai haderőnek a felhőalapú szolgáltatások integrálására, vizsgálva a kormányzati felhőstratégiákat, a haderő szintű felhőstratégiákat és a U.S. Army speciális terveit.

[2] Clarke 2016; Clarke 2017.
[3] Kovács 2021.
[4] Lásd: www.itbiztonsag.siteset.hu/index.php?m=996
[5] Vergun 2016.

2. Felhőalapú szolgáltatások katonai alkalmazásának alapjai

Korunk egyik legvitatottabb és legdivatosabb technológiai fejlesztése a felhőrendszer. A felhőalapú rendszerek lényege, hogy nem a saját IT-infrastruktúránkon található adatokkal, szoftverekkel vagy platformokon dolgozunk, hanem „valahol az interneten",[6] ugyanis a konkrét infrastruktúra helye a felhasználó számára többnyire nem, vagy nem pontosan ismert. A konkrét infrastruktúra akár országhatáron kívül is eshet, ha például külföldi szolgáltatót veszünk igénybe. Ez az országhatáron kívüliség további biztonsági kérdéseket vet fel, ha azt szeretnénk elérni, hogy egy rendvédelmi vagy nemzetbiztonsági szerv munkáját ültethessük át (részlegesen) felhőalapú rendszerekbe.

2.1. Felhőalapú rendszerek, szolgáltatások fogalma, típusai

Felhőalapú szolgáltatás lehet tárhely (például iCloud), szoftver (például Microsoft Office 365) vagy platform/infrastruktúra is (például Oracle Cloud Infrastructure). A NIST (National Institute of Standards and Technology, Nemzeti Szabványügyi és Technológiai Intézet) Információtechnológiai Laboratóriuma (Information Technology Laboratory) a következőképp rendszerezte a felhőalapú szolgáltatásokat tulajdonságaik alapján:

- igény szerinti önkiszolgálás *(on-demand self service);*
- jó hálózati hozzáférés *(broad network access);*
- teljes rugalmasság *(rapid elasticity);*
- mért szolgáltatások *(measured service).*[7]

Hasonló keretrendszert használ a Német Szövetségi Információbiztonsági Hivatal (Bundesamtes für Sicherheit in der Informationstechnik, BSI) is.[8] De léteznek olyan további kérdéses tulajdonságok is, mint például a rendelkezésre állás, a kiszolgálás gyorsasága, a megbízhatóság, a skálázhatóság, a teljesítmény, a biztonság, a karbantartás, a költség stb. Ezek alapján a felhasználó a saját igényeire és prioritásaira szabott szolgáltatást tud választani. Kovács azonban munkájában felhívja a figyelmet arra is, hogy a felhőalapú rendszerek csoportosításához szükség van a szolgáltatási és telepítési kategóriák ismeretére is, előnyeikkel, hátrányaikkal együtt.[9]

A szolgáltatási modellek lehetnek: szoftver mint szolgáltatás (*software as a service,* SaaS), platform mint szolgáltatás (*platform as a service,* PaaS) és infrastruktúra mint szolgáltatás (*infrastructure as a service,* IaaS). Ezeket a modelleket már többféleképpen próbálták kiegészíteni, továbbá megjelentek már a *desktop as a service* (DaaS) és PRaaS *(process as a service)* megoldások is.[10]

[6] Kovács 2021. 15.
[7] Lepenye 2011.
[8] Security Recommendations for Cloud Computing Providers (Minimum information security requirements) White Paper. 2011.
[9] Kovács 2021. 19.
[10] Kusnetzky 2009.

Telepítési modellek lehetnek: magán számítási felhő *(private cloud)*, közösségi számítási felhő *(community cloud)*, nyilvános számítási felhő *(public cloud),* hibrid számítási felhő *(hybrid cloud)*.

A felhasználó e modellek mátrixa alapján tudja igényeinek megfelelően kiválasztani, hogy milyen szolgáltatásra lenne szüksége.

2.2. Kormányzati felhőrendszerek

Az általános, technikai modellek mellett célja szerint beszélhetünk kormányzati *(gov-cloud)* és katonai *(mil-cloud)* felhőalapú rendszerekről.

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) a *Good Practice Guide for Securely Deploying Governmental Clouds* (Jó gyakorlati útmutató a kormányzati felhők biztonságos telepítéséhez)[11] című, 2013-ban kiadott dokumentumban megkísérli definiálni a gov-cloud-ot. A szakértők alapul vették a NIST által meghatározottakat, és kiemeltek három megoldást a gov-cloud-ra, mégpedig: a nyilvános számítási felhő, a magán számítási felhő és a közösségi számítási felhő.

A gov-cloudra általános definíció még nincs, de több szempontot is figyelembe vevő meghatározások már az ENISA említett dokumentumában is léteznek:

- „A gov-Cloud egy olyan környezet, ahol a futó szolgáltatások megfelelnek a kormányzati és EU szabályozásoknak az információbiztonság és az ellenálló képesség terén (ez a mi kérdésre ad választ).
- A gov-Cloud a közintézmények, kormányzatok által működtetett szolgáltatások futtatásának (magán vagy nyilvános felhőben) egy biztonságos és megbízható módja (ez a hogyan kérdésre ad választ).
- A gov-Cloud egy telepítési modell, amelyet arra építettek, hogy szolgáltatásokat nyújtsanak állami szervek (belső szolgáltatások nyújtása), polgárok és vállalkozások (külső szolgáltatások nyújtása a társadalom) számára (ez a kinek kérdésre ad választ)."[12]

A Technopedia meghatározása szerint,[13] az Egyesült Államokbeli szabályozások alapján, a gov-cloud megnevezés az összes felhőalapú számítástechnikai és virtualizációs termékre és megoldásra vonatkozik, amelyeket kifejezetten kormányzati szervezetek és intézmények számára fejlesztettek ki. A Gov-Cloud föderális kezdeményezés olyan felhőmegoldások kezelésére és tervezésére, amelyek megfelelnek az IT-szükségleteknek, valamint a szövetségi kormány stratégiai, pénzügyi és működési céljainak.

A Gov-Cloud program az Egyesült Államokban megkönnyíti a felhőalapú számítástechnikai megoldások megvalósítását formális szabványok és eljárások szerint, kiemelt hangsúlyt fektetve a biztonságra és az interoperabilitásra. Számos iránymutatást tettek közzé e program keretében, mint például a Federal Cloud Computing

[11] *Good Practice Guide for Securely Deploying Governmental Clouds.* 2013.
[12] *Good Practice Guide for Securely Deploying Governmental Clouds.* 2013.
[13] Lásd: www.techopedia.com/definition/28218/govcloud

Strategy,[14] a Federal CIO 25-Point Roadmap[15] terve és a NIST Cloud Computing Technology Roadmap.[16] Mindezek mellett, a GovCloudot olyan privát felhőszolgáltató, mint például az Amazon AWS is, márkatermékként kínálja.

A 2010-es évekre felismerték, hogy a szövetségi kormány információs technológiai (IT-) környezetét az alacsony eszközkihasználás, az erőforrások iránti töredezett kereslet, a duplikált rendszerek, a nehezen kezelhető környezetek és a hosszú beszerzési határidők jellemzik. Ezek a hiányosságok negatívan befolyásolják a szövetségi kormány azon képességét, hogy kiszolgálja az amerikai közvéleményt. A felhőalapú számítástechnika jelentős szerepet játszhat e hiányosságok kezelésében és a kormányzati szolgáltatások javításában. A számítási felhő modell jelentősen segítheti azokat az ügynökségeket, amelyek erőforráshiánnyal küzdenek. Tehát, a szövetségi kormány számára a felhőalapú számítástechnika óriási lehetőségeket rejt magában azáltal, hogy növeli a működési hatékonyságot és gyorsabban reagál a szükségletekre.

A fentieket alátámasztják a Federal Cloud Computing Strategy-ben megfogalmazott alábbi célitűzések is:

- a felhőalapú számítástechnika előnyeinek, szempontjainak és kompromisszumainak megfogalmazása;
- adjon döntési keretet és esetpéldákat, hogy támogassa az ügynökségeket a felhőalapú számítástechnikára való átállásban;
- a számítási felhő megvalósítási erőforrásainak kiemelése;
- határozza meg a szövetségi kormány tevékenységeit, szerepköreit és felelősségeit a felhő bevezetésének katalizálásával kapcsolatban.[17]

Ez a stratégia megfogalmazza azt is, hogy a digitalizálódó világban a kormány felelőssége az, hogy élen járjon az innovatív szolgáltatások amerikai néphez való eljuttatásában. Tekintettel arra, hogy minden ügynökség egyedi küldetési szükségletekkel, biztonsági követelményekkel és informatikai környezettel rendelkezik, a stratégia felszólítja az ügynökségeket, hogy a stratégia alapján dolgozzanak ki saját cselekvési tervet és beszerzési stratégiát összhangban a Cloud First Irányelvvel *(Cloud First Policy)*.[18]

A CIO 25-Point Roadmap egy 2010-ben kidolgozott cselekvési terv, amely bár nem oldotta meg az összes szövetségi informatikai kihívást, a legsürgetőbb, állandó kihívások közül sokra nyújtott megoldást. A CIO 25-Point Roadmap inkább a végrehajtásra összpontosított.

A szintén 2011-es NIST Cloud Computing programhoz szorosan kapcsolódik az USG Cloud Computing Technology Roadmap és az Egyesült Államok kormányának USG Cloud Computing Technology Roadmap dokumentuma 500-293. sz. speciális kiadványának első kiadása két kötetből áll. A NIST Cloud Computing program stratégiájával összhangban az ütemterv a felhőalapú számítástechnikával kapcsolatos stratégiai és műveleti célokra összpontosít.

[14] Kundra 2011.
[15] Kundra 2010.
[16] Hogan et al. 2011.
[17] Kundra 2011. 2.
[18] Kundra 2011. 33.

Az I. kötet, *Az USG felhőalapú számítástechnika további bevezetésének kiemelt követelményei,* keretet ad a vitának, és bemutatja az ütemtervet azon összefoglaló stratégiai követelmények tekintetében, amelyeknek az USG ügynökségei számára teljesíteniük kell a felhőalapú számítástechnika további bevezetéséhez. Az ütemterv stratégiai elemei „kiemelt prioritású műszaki területként" jellemezhetők, amelyek rövid és hosszú távon egyaránt lehetővé teszik a számítási felhőt.

A II. kötet tájékoztatást nyújt azoknak, akik aktívan dolgoznak a stratégiai és műveleti számítási felhőkezdeményezéseken, beleértve, de nem kizárólagosan, a kormányzati-felhő-használókat. Ez a kötet összefoglalja a 2010 novembere és 2011 szeptembere között a NIST Cloud Computing program és az USG Cloud Computing Technology ütemtervének kidolgozására irányuló közös erőfeszítések révén végzett munkát.[19]

A NIST-program megfogalmaz továbbá bizonyos standardokat az interoperabilitás, a mobilitás és a biztonság területein is a felhőalapú rendszerekkel kapcsolatban. A felhőalapú számítástechnika megvalósításának fő biztonsági céljai a NIST-program alapján a következők:

- Védje az ügyfelek adatait a jogosulatlan hozzáféréstől, nyilvánosságra hozataltól, módosítástól vagy megfigyeléstől. Ez magában foglalja az identitáskezelés támogatását, hogy az ügyfél képes legyen identitás- és hozzáférés-szabályozási irányelveket érvényesíteni a felhőszolgáltatásokhoz hozzáférő jogosult felhasználókon.
- Véd az ellátási láncot érő lehetséges fenyegetésektől. Ez jelenti a szolgáltató megbízhatóságát, valamint a használt hardver és szoftver megbízhatóságának biztosítását.
- Akadályozza az illetéktelen hozzáférést a felhőalapú számítástechnikai infrastruktúra erőforrásaihoz. Tehát a biztonsági tartományok megvalósítása a cél, amely révén a logikai elemek elválasztásával rendelkeznek a számítási erőforrások fölött, ezáltal biztosítva az alapértelmezett konfigurációk használatát.
- Felhőben telepített webalkalmazások tervezése egy internetes fenyegetésmodellhez, és a biztonság beágyazása a szoftverfejlesztési folyamatba.
- Végfelhasználói biztonsági rések csökkentése az internetre csatlakoztatott személyi számítástechnikai eszközök védelmét szolgáló intézkedések megtétele, biztonsági szoftverek, személyi tűzfalak és javítások, karbantartás révén.
- Állapítson meg bizalmi határokat a szolgáltató(k) és a fogyasztók között azért, hogy a biztonságért való felelősség egyértelmű legyen.
- Támogatja a hordozhatóságot, hogy az ügyfél szükség esetén a rendelkezésre állási, bizalmassági és integritási követelmények teljesítése érdekében intézkedhessen a felhőszolgáltatók megváltoztatásáról. Ez magában foglalja a fiók bezárásának lehetőségét egy adott napon és időpontban, valamint az adatok átmásolását egyik szolgáltatótól a másikhoz.[20]

A már említett Cloud First Irányelv célja volt felgyorsítani a tempót, amellyel a szövetségi kormány felismerte a felhőalapú rendszerek használhatóságának értékét azáltal,

[19] Hogan et al. 2011. 11–13.
[20] Hogan et al. 2011.

hogy megkövetelte az ügynökségektől, hogy értékeljék a biztonságos felhőalapú számítástechnikai lehetőségeket, mielőtt bármilyen új befektetést eszközölnének.[21]

Magyarországtól eltérően, az Egyesült Államok Szövetségi Kormánya tradicionálisan szerződésben áll magánszolgáltatókkal, akik megfelelnek a sajátos követelményrendszereknek és kiszolgálják a különböző ügynökségeket. A felhőszolgáltatások szempontjából a fő központi szolgáltató az Amazon Web Services (AWS).

Az AWS GovCloud (USA) elszigetelt AWS-régiókból áll, amelyek lehetővé teszik az egyesült államokbeli kormányzati szervek és ügyfelek érzékeny adatainak áthelyezését a felhőbe azáltal, hogy megfelelnek sajátos szabályozási és megfelelőségi követelményeiknek, ideértve a Szövetségi Kockázat- és Engedélykezelési Programot (FedRAMP), a Védelmi Minisztérium biztonsági követelményeinek útmutatóját (DoD SRG) és a Criminal Justice Information Services (CJIS) követelményeit.[22] A szolgáltatás specifikusan az Egyesült Államok szövetségi, állami és helyi szintű kormányzati szervei, valamint a vállalkozók, az oktatási intézmények és más egyesült államokbeli ügyfelek igényeire lett fejlesztve. Például, 2013 óta a CIA is használja az AWS szolgáltatásait (több egyéb multinacionális entitás szolgáltatásai mellett).[23]

3. Az amerikai haderő tervei és elképzelései a felhőalapú szolgáltatások alkalmazására

A kormányzat mellett a haderő szereplői is felismerték, hogy a felhőalapú rendszerek hatékonyabbá tehetnek bizonyos munkafolyamatokat.

A 2012 júliusában kiadott U.S. DoD Cloud Computing Strategy[24] olyan megközelítést vezet be, amellyel a minisztérium a duplikált, nehézkes és költséges alkalmazássilók jelenlegi állapotából egy agilis, biztonságos és költséghatékony végállapotba kerül, egy hatékony szolgáltatási környezet által, amely gyorsan reagál a változó küldetési igényekre. A DoD-szintű központosított felhőre való átállásának megközelítése a következő négy lépésből áll a stratégia szerint:

1. a felhőalapú szolgáltatások katonai célokra való alkalmazásának előmozdítása;
2. az adatközpontok konszolidációjának optimalizálása;
3. a DoD Enterprise Cloud Infrastructure létrehozása és
4. Deliver Cloud Services – kereskedelmi szolgáltatók igénybevétele és a DoD felhőszolgáltatások fejlesztésének és megvalósításának folytatása.

A DoD Cloud Computing Strategy külön megvalósításokat és adatcseréket határoz meg a kevésbé biztonságosnak tekintett Internet Protokoll Router Network (NIPRNet), a Secure Internet Protocol Router Network (SIPRNet) és a Top Secret Sensitive Compartmented Information (TS SCI) biztonsági tartományokhoz.[25]

[21] Lohrmann 2010.
[22] *What is AWS GovCloud (US)?* é. n.
[23] Fedscoop 2020.
[24] Az Amerikai Egyesült Államok Védelmi Minisztériumának Felhőstratégiája. 2018.
[25] Magar 2014. 16.

3.1. Haderőszintű tervek, elképzelések

Haderőszinten két fontos terv született a felhőrendszereket illetően. Az első a Joint Enterprise Defense Infrastructure (JEDI), a második a JEDI-t váltó, Joint Warfighter Cloud Capability (JWCC) program volt.

Mivel a számítógép-hálózatok kritikus szerepet játszanak a modern harctéren, továbbá tekintettel kell lennünk arra, hogy az Egyesült Államok jelenlegi katonai doktrínája a jövőben több domainben is (azaz szárazföldön, tengeren, levegőben, kibertérben vagy az űrben) vívandó háborúkra is felkészül, ezek a hálózatok még fontosabbá válnak. Lehetővé teszik az egységek számára a kommunikációt, az adatok feldolgozását, az információk megosztását és az erőfeszítések szinkronizálását ezekben a műveleti tartományokban. Az elmúlt, nagyjából két évtizedben a hagyományosabb számítógépes hálózatok helyét átvették a felhőalapú rendszerek. Ennek megfelelően az Egyesült Államok Védelmi Minisztériuma (DoD) 2019-ben szerződést kötött a Microsofttal a JEDI fejlesztésére, hogy ezeket a felhőképességeket eljuttassa a harcosokhoz.

A JEDI-nek az volt a célja, hogy a DoD komplex, darabokra bontott hálózatait egyetlen egységes felhőalapú vállalatra cserélje, hogy ezzel nagyobb megbízhatóságot és jobb információáramlást tegyen lehetővé a különböző rendszerek között. A felhőalapú szolgáltatás lehetővé tenné a DoD számára azt is, hogy számos új képességet hozzon be. A modern csatatéren elért siker attól függ, hogy a megfelelő információkat a megfelelő személyhez, a megfelelő időben eljuttathassuk. Bár számos egyéb technológia kötődik ehhez – mesterséges intelligencia, gépi tanulás, big data analitika –, a védelmi vállalat hatalmas mérete miatt szükség van a számítási felhőre.[26] Tehát a JEDI-t a meglévő, kereskedelmi forgalomban lévő technológia katonai megfeleltetésére szánták, miközben a méretgazdaságosságot is figyelembe veszi.

A programot 2021 júliusában törölték, arra hivatkozva, hogy a DoD-nak más típusú szükségletei lettek időközben, amelyekre a Joint All Domain Command and Control (JADC2) és a Artificial Intelligence and Data Acceleration (ADA) iniciatívák vetettek fényt. [27]

A JEDI-ről a JWCC-re való áttérés biztonságosabb és sokoldalúbb hálózatot biztosít a DoD számára. Tekintettel a számítógépes hálózatok fontosságára a modern harcokban, ez a lépés véleményem szerint szükséges volt.

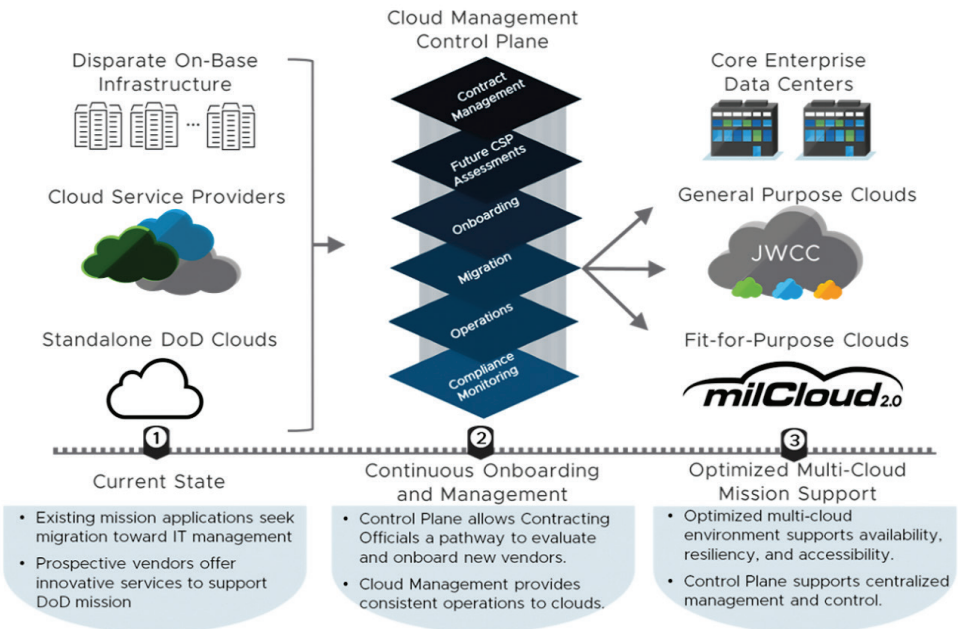
Végrehajtva a JWCC-ben megfogalmazottakat, egy többszállítós szervezeti felhő jön létre, amely a DoD-t minden biztonsági szinten lefedi. A JWCC lehetővé teszi a DoD számára, hogy megteremtse azokat a multicloud[28] előnyöket, amelyeket a multicloudot alapstratégiaként alkalmazó vállalati szervezetek nagy többsége realizált

[26] Mittal 2021.

[27] U.S. Department of Defense 2021.

[28] A multicloud, magyarul többfelhős környezet, amely több (kapcsolt) nyilvános felhőt jelent. Többfelhős telepítést használó vállalatok több nyilvános felhőt is használnak több felhőszolgáltatótól. Ahelyett, hogy egy vállalkozás egyetlen „szállítót" használna a felhőalapú tárhelyszolgáltatáshoz, tároláshoz és a teljes alkalmazásveremhez, a többfelhős konfigurációban többet használnak. A többfelhős környezetnek számos felhasználási módja van. A többfelhős telepítés több IaaS *(infrastructure-as-a-service)* szállítót is igénybe vehet, vagy használhat másik szállítót az IaaS-, PaaS- és SaaS-szolgáltatásokhoz. A többfelhő pusztán redundancia és rendszermentés célját szolgálhatja, vagy magában foglalhat különböző felhőszolgáltatókat a különböző szolgáltatásokhoz.

már.[29] A multicloud jobban illeszkedik a küldetésekhez az architektúrákon belül, szélesebb körű innovációkat kínál a jövőbeli küldetésekhez, jobb ellenálló képességet biztosít az egyetlen forrásból származó hibákkal szemben, és gazdasági előnyöket kínál versenyképes lehetőségekkel. A multicloud használatának masszív növekedése miatt az ipari szabványok és megoldások lehetővé teszik a multicloud környezetek egyszerű integrációját, hordozhatóságát, virtuális hálózatkezelését és irányítását



1. ábra: A többfelhős környezet előnyeinek maximalizálása
Forrás: https://blogs.vmware.com/industry-solutions/2021/10/19/how-jwcc-benefits-from-multi-cloud-adoption/

3.2. Haderőnemi szintű tervek, elképzelések

A hadsereg megváltoztatta az ICT-infrastruktúra korszerűsítésével kapcsolatos megközelítését a felhőalapú rendszerekre való átállással. Ez a megközelítés az IT-hardver-beszerzések és a fenntartás csökkentését helyezi előtérbe annak érdekében, hogy ezeket a képességeket szolgáltatásként a felhőszolgáltatóktól szerezzék be.

Haderőnemi szinten felhőalapú rendszereken dolgozik már az Egyesült Államok haderejének szárazföldi komponense (U.S. Army), az Amerikai Légierő és a Haditengerészet is.

Haderőnemi szinten a U.S. Army két fontos stratégiai dokumentumot készített a felhőalapú rendszerek implementálásáról a haderőben: Army Cloud Computing

[29] *What is JWCC?* é. n.

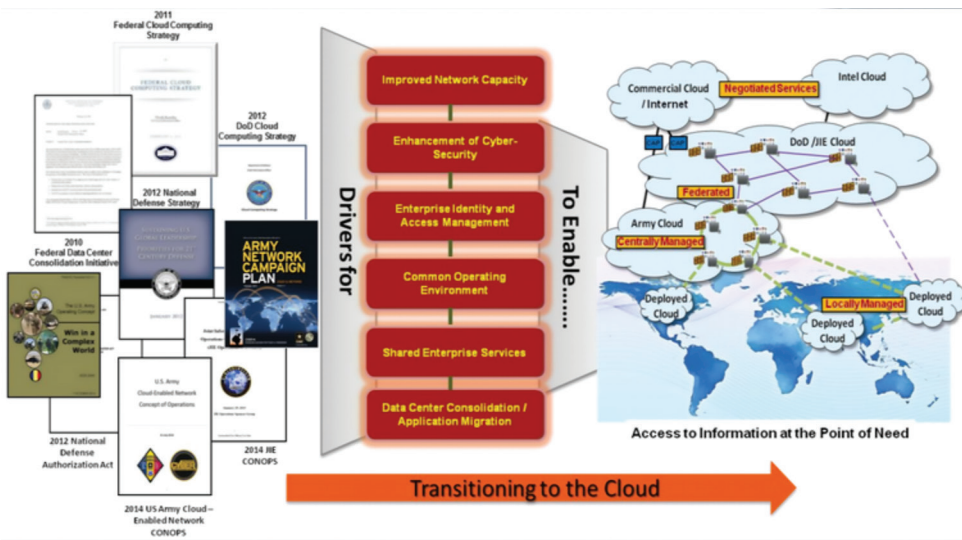
Strategy (a szárazföldi komponens stratégiája, 2015); Army Cloud Plan (a szárazföldi komponens stratégiája, 2020).

De a légierő (Air Cloud One) és a haditengerészet is használ felhőplatformokat (Navy Cloud, amelyet a 2021-es Navy Cloud Computing Policy szabályoz).

Az alábbiakban a fő fókuszt a U.S. Army két stratégiájára helyezi a cikk, mivel az ő példájukon keresztül lehet a legjobban bemutatni a stratégiai környezet fejlődését.

3.3. U.S. Army

Az Army Cloud Computing Strategy-t (ACCS)[30] 2015-ben adta ki a U.S. Army. Az Army Cloud Computing Strategy leírja a hadsereg vízióját és stratégiáját a felhőalapú hálózati képességek biztosítására, a küldetés és a hatékonyság javítása, az operatív információs technológia (IT) hatékonyságának növelése, valamint a hadsereg adatainak és infrastruktúrájának védelme érdekében. Az Army Cloud Computing Strategy kiterjeszti a különböző szövetségi, biztonsági és katonai irányelvekben és dokumentumokban meghatározott alapvonalat és koncepciókat, és beágyazódik a hadsereg hálózati kampánytervébe.



2. ábra: Felhőszámítási stratégiák kontextusa
Forrás: Army Cloud Computing Strategy 2015.

A 2. ábra a különböző megfelelő stratégiákat és dokumentumokat mutatja be, amelyek a hadsereg hadműveleti koncepcióját támogató felhőalapú képességek létrehozását segítik elő. Amint ezek a tevékenységek és kezdeményezések megvalósulnak, megvalósul a hadsereg hibridfelhő-képessége.

[30] U.S. Army (2015): *The Army Cloud Computing Strategy* (2015. március 26.).

Ennek érdekében a vezérkari főnökök és a DoD informatikai igazgatója egyesítették a szolgáltatás összetevőit és a DISA-t (Deployment of the Defense Information Systems Agency)[31] a JIE (DoD Joint Information Environment) létrehozásához és kezeléséhez. A JIE célja az egységes, biztonságos információs környezet létrehozása, amely lehetővé teszi a parancsnokok számára, hogy kapcsolódjanak, hozzáférjenek és megosszák a hatékony működéshez szükséges információkat. Ugyanis a felhőalapú képességek kulcsfontosságúak a JIE sikerében; lehetővé teszik az alkalmazások és az alapvető képességek konszolidálását biztonságos környezetben, valamint az egyetemes hozzáférhetőséget a DoD és a hadsereg között.[32]

A DoD CIO (Chief Information Officer)[33] és a DISA folyamatos együttműködését munkacsoportok biztosítják azért, hogy a DoD felhőstratégia és a kapcsolódó megvalósítási tervek és architektúrák összhangban legyenek a JIE-ben. A hadseregnek javítania kell a hatékonyságot és csökkentenie kell a költségeket, miközben meg kell őriznie az adatbiztonságot a jelenleg és az előrejelzések szerint használatban lévő nagyszámú szoftveralkalmazás és rendszer tárolásával és támogatásával kapcsolatban.

Ezért a speciális adatkommunikációs vezérlési eljárások (Advanced Data Communication Control Procedures, ADCCP) részeként a hadseregnek a hadsereg adatközpontjainak százait kell egységesítenie szabványosított adatközpontokká, telepítési feldolgozási csomópontokká és/vagy nem DoD felhőszolgáltató létesítményekké. A hadsereg parancsnokságának, a személyzetnek, a küldetési területeknek és a tartománymenedzsereknek kell eldönteniük, hogy fenntartsák vagy modernizálják alkalmazásaikat. A tartós alkalmazásoknak ezután át kell állniuk egy jóváhagyott tárhelykörnyezetbe.

A hadseregnek gondoskodnia kell arról is, hogy a meglévő missziós parancsnoki rendszerek, például a taktikai információs hálózat (Warfighter Information Network-Tactical, WIN-T), a széttagoltan települt szárazföldi csapatok (Distributed Common Ground System Army, DCGS-A), a jövőbeli parancsnokságok (Command Post of the Future, CPOF) és a modern tábori rendszerek (Advanced Field) képességei biztosítottak legyenek.[34]

A U.S. Army célja ezzel a stratégiával az volt, hogy megváltoztatja az ICT-infrastruktúra korszerűsítésével kapcsolatos megközelítését a felhőalapú megközelítésre való átállással. Ez a megközelítés az IT-hardver-beszerzések csökkentését és a fenntartást helyezi előtérbe annak érdekében, hogy ezeket a képességeket szolgáltatásként a felhőszolgáltatóktól szerezzék be.

A műveleti képességek átadásához és a kritikus működési funkciók támogatásához négy stratégiai követelmény és a hozzájuk kapcsolódó célkitűzések szükségesek:

[31] DISA: Védelmi Információs Rendszer Ügynökség, egy katonai, szövetségi civil és szerződő partnereikből álló Harci Támogatási Ügynökség. A DISA biztosítja a hálózatot, a számítástechnikai infrastruktúrát és a vállalati szolgáltatásokat az információmegosztás és a döntéshozatal támogatására a DoD-n és a szövetségi ügynökségeken belül.

[32] U.S. Army 2015. 5.

[33] DoD CIO: a Védelmi Minisztérium információs főtisztje, aki a védelmi miniszter fő vezérkari asszisztense és vezető informatikai tanácsadója. Ez a szerepkör számos nemzetbiztonsági és védelmi rendszer felügyeletét, információs erőforrások kezelését és a hatékonyság feltárását foglalja magában. Felelős az osztály információs vállalkozásával kapcsolatos minden ügyért. A cikk írásakor a pozíciót Dr. Kelly Fletcher töltötte be.

[34] U.S. Army 2015. 5.

- felhőirányítási és -kezelési gyakorlatok elfogadása;
- felhőalapú számítástechnikai képességek kategorizálása a hadsereg hálózatán belül;
- alkalmazások, rendszerek és adatok modernizálásának és migrációjának irányítása;
- felhőműveletek biztonságossá tétele és kezelése.[35]

Az ACCS-ban megfogalmazottak szerint a felhőalapú számítástechnika alkalmazásának másik kulcsfontosságú motivációja a felhőalapú számítástechnika bizonyított sikere a magánszektoron belül. Ez a siker olyan innovációknak és kulcsfontosságú technológiai áttöréseknek köszönhető, amelyek megkönnyítik:

- megfizethető, nagy sebességű sávszélesség széles körű elérhetővé tételét;
- kisebb, erősebb és olcsóbb számítógépes processzorok és végfelhasználói eszközök beszerzését;
- párhuzamos feldolgozási módszertanok kialakítását;
- gyors szoftvertelepítési ciklusok kialakítását;
- az adattárolási és -feldolgozási képességek továbbfejlesztett virtualizációját; így lehetővé téve több alkalmazás egyidejű futtatását megosztott fizikai erőforrásokon;
- továbbfejlesztett adatközpont automatizálását, amely jelentősen csökkenti a rendszeradminisztrációs munkaigényt;
- szinte univerzális szoftver-együttműködési szabványok megalkotását;
- új online piacterek létrehozását, ahol a szoftverplatform-szolgáltatók, eszközgyártók, alkalmazásfejlesztők és fogyasztók kapcsolatba léphetnek egymással.[36]

E fejlesztések elfogadása megteremtette a feltételeket az ADCCP számára, hogy az információk, adatok és alkalmazások gyűjtését, elérését, feldolgozását és terjesztését egyéni asztali számítógépekről, laptopokról vagy helyi szerverszobákról központilag kezelt távoli adatközpontokba helyezze át. Ugyanis úgy látták, hogy ha az adatközpont-konszolidációt felhőalapú számítástechnikával, az IT-képességek és -szolgáltatások vásárlására és eladására szolgáló segédprogram-alapú modellel kombinálják, az igény szerinti, fizetős szolgáltatások aggregálása és eljuttatása az ügyfelek számára vonzó és rendkívül versenyképes üzleti lehetőséggé válik. Ugyanakkor be kellett vezetni egy olyan módszeres folyamatot, amely figyelembe veszi a változó biztonsági és üzemeltetési aggályokat, és kockázati alapon végzett értékeléseken alapul. Mindezek a tényezők hozzájárulnak ahhoz, hogy a számítási felhő olyan opció legyen, amely jelentős költségmegtakarítást, IT-hatékonyságot és jobb képesség-szolgáltatást biztosít.

Tehát a U.S. Army Cloud Computing Strategy meghatározza a stratégiai irányt és útmutatást ad a U.S. Army számára a biztonságos működési környezet fenntartására, miközben átalakítja a hadsereg információtechnológiai infrastruktúráját, rendszereit, szoftvereit és alkalmazási platformjait, adatvagyonát, valamint a kapcsolódó műveleti

[35] U.S. Army 2015. 16.
[36] U.S. Army 2015. 6.

szintű folyamatokat és gyakorlatokat. Más néven a felhőalapú megoldásokra való átállás a U.S. Army-nak átfogó terve volt 2015-ben.

2020-ban a U.S. Army új stratégiát adott ki, az Army Cloud Plan-t, amely a 2018-as Nemzeti Védelmi Stratégia (National Defense Strategy, NDS) alá illeszkedik.

Az Army Cloud Plan stratégiai megközelítést kínál a változó digitális helyzetképhez, és támogatja az Army Data Plant (ADP) egy olyan „globálisan hozzáférhető, szabványokon alapuló környezet létrehozásához, ahol az adatok és információk láthatóak, hozzáférhetőek, érthetőek, megbízhatóak, interoperábilisak és biztonságosak a teljes életciklusukon keresztül".[37]

A 2018-as NDS-ben felismerték az új típusú biztonsági fenyegetéseket, ennek nyomán a U.S. Army új felhőstratégiája is igazodott ahhoz, hogy a U.S. Army folyamatai agilisabbá és hatékonyabbá válhassanak az információs hadviselésben.

Ennek értelmében az Army Cloud Plan stratégiai céljai a következők:

- az adatközpontú döntés felgyorsítása;
- a szoftver használati idejének csökkentése;
- optimalizálja a biztonsági akkreditációs folyamatot;
- alapvető kompetenciaként határozza meg a felhőtervezést, a szoftverfejlesztést és az adattervezést;
- szoftver tervezése a dinamikusan változó biztonsági környezethez való alkalmazkodáshoz (utalás történt tehát a gépi tanulás és a mesterséges intelligencia használatára);
- biztosítsa az IT-eszközök/-költségek átláthatóságát és elszámoltathatóságát.[38]

Látható, hogy az Army Cloud Plan a 2015-ös Army Cloud Computing Strategy-hez képest sokkal konkrétabb, kézzelfoghatóbb célkitűzéseket határozott meg, figyelembe véve a kialakult dinamikusan változó biztonsági környezetet.

Az alapvető elképzelés egy multicloud létrehozása a U.S. Army számára: egy minősített, egy nem minősített és egy nyilvános hálózatból.

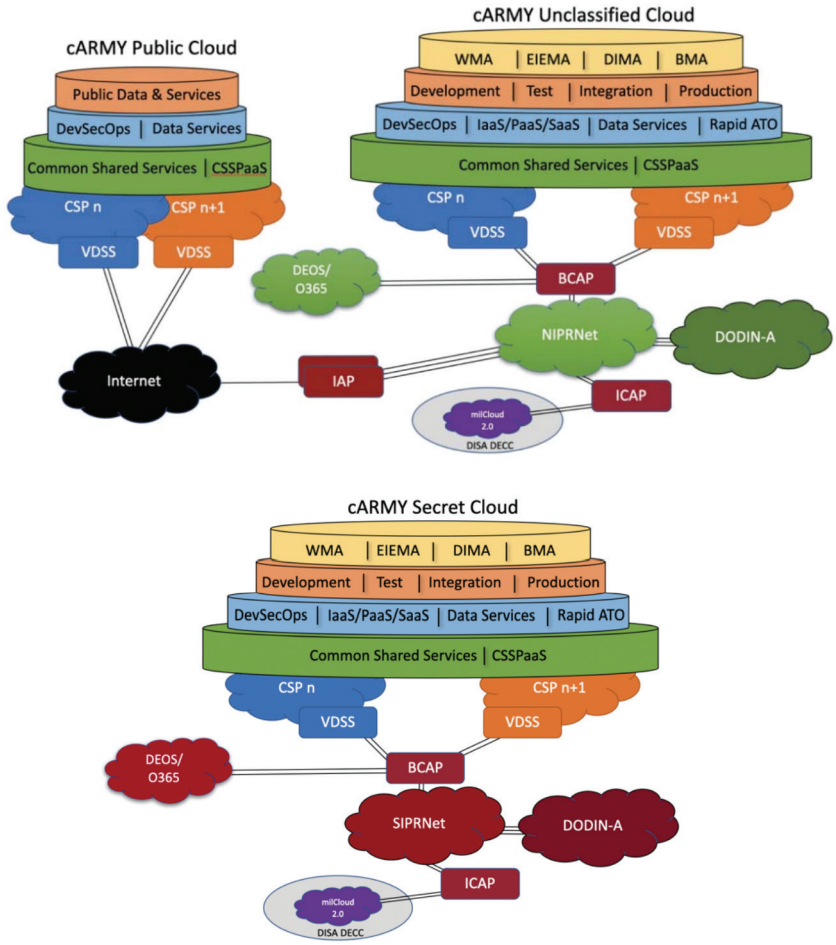
A terv felvázolja azokat a stratégiai célokat és ütemtervet, amelyek megvalósítják a U.S. Army felhőrendszerekről alkotott jövőképét. E terv értelmében a hadsereg többfelhős, több szállítós stratégiát valósít meg, kihasználva a legújabb kereskedelmi felhőszolgáltatásokat, beépített biztonsággal.

A U.S. Army honlapján található további információk szerint a jövőben folyamatosan fejleszti és frissíti a hadsereg felhőtervét, ahogy tapasztalatokat szerez a felhő használatával kapcsolatban. A felhőterv további lépései a következők:

- Közös megosztott szolgáltatások nyújtása, beleértve a kiberbiztonsági szolgáltatásokat is, hogy a hadsereg ügyfelei a cARMY[39]-felhőkörnyezetben működhessenek, operacionalizálhassák adataikat, és teljes mértékben kihasználhassák a felhőalapú számítástechnika előnyeit.

[37] U.S. Army 2020.
[38] U.S. Army 2020. 6.
[39] A cARMY közös megosztott szolgáltatás, amely lehetővé teszi az alkalmazások működését a tárhelykörnyezetben, és központilag az ECMA kezeli őket. A központosított közös megosztott szolgáltatások biztosítása csökkenti a költségeket és csökkenti a felhőbe való átvétel akadályait azáltal, hogy a környezetet minden alkalmazáshoz előkészíti.

- Tehetségkezelési terv kidolgozása és végrehajtása annak biztosítására, hogy a munkaerő rendelkezzen a szükséges adattudományi, szoftverfejlesztési és felhőtervezési készségekkel.[40]



3. ábra: Army Title 10 Enterprise Cloud Ecosystem
Forrás: https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf

2021-ben adták ki az *Army Enterprise Application/System Modernization and Migration to Commercial Cloud Statement of Objectives* (SOO)[41] című dokumentumot. Az Army Enterprise Cloud Management Agency (ECMA), egy helyszíni üzemeltető ügynökség adta ki, amely felügyeli a hadsereg összes felhőfolyamatát és tevékenységét.

[40] U.S. Army 2020.
[41] ECMA 2021.

A dokumentum leírja a hadsereg céljait és követelményeit, hogy vállalati szintű szerződést vagy megállapodást biztosítson a hadsereg alkalmazásai/rendszerei és adatok kereskedelmi felhőkörnyezetekbe történő modernizálására és migrálására.

Az Army Cloud Plan-nel összhangban, a hadsereg azon képessége, hogy hatékonyan használja a felhőalapú technológiákat, kritikus tényező az adatok operacionalizálására való törekvésben. Mint ilyen, a hadseregnek vállalati szintű képességre van szüksége az alkalmazások és adatok kereskedelmi felhőbe történő migrálásához.[42]

Ennek értelmében a hadsereg alkalmazásainak túlnyomó része a cARMY-ba, a hadsereg vállalati felhőkörnyezetébe költözik, amelyet az ECMA kezel. A cARMY jelenleg engedélyezett és működő közös megosztott szolgáltatásokat kínál az Amazon Web Servicesben (AWS) és a Microsoft Azure-ban, a közös, megosztott szolgáltatások fejlesztésére vonatkozó szerződésekkel/tervekkel.

A hadsereg a fentiek mellett figyelembe veszi a cARMY-ba való migráció alóli kivételeket, ha erre komoly üzleti indokok állnak fenn, például olyan szoftver mint szolgáltatás (SaaS) használata, amely nem elérhető a cARMY-ban, ugyanis a cARMY-ba vagy bármely kereskedelmi felhőbe való migráció előtt az akalmazásokat a Cloud Native Design[43] elvek alapján modernizálni kell, hogy kihasználhassák a kereskedelmi felhő előnyeit.[44]

4. Összegzés, következtetések

Az Egyesült Államok haderejében, és specifikusan a szárazföldi haderőben (U.S. Army) nem teljesen új keletű ötlet a felhőalapú szolgáltatások igénybevétele, illetve saját rendszerek építése erre a célra. A folyamatosan újuló stratégiák és tervek remekül körvonalazzák azt a szándékot, hogy a hadsereg lépést tudjon tartani a digitális korral.

A (kereskedelmi) felhőalapú megoldásra való áttérés a DoD digitális és szoftver-modernizációs törekvéseinek egyik pillére. Nem annyira a felhőről van szó, hanem arról, hogy a felhő mire képes. A vállalati kereskedelmi felhő ugródeszka olyan kritikus kezdeményezésekhez, mint a Joint All-Domain Command, Control Framework (JADC2).[45]

A felhőalapú számítási modellek alapvető jelentősége azonban a DoD számára a legkorszerűbb kapacitások támogatásában oda vezetett, hogy a Pentagon újraértékelte megközelítését, amivel a tervezés négy évvel korábban elkezdődött. Ez magában foglalta a felhőalapú szerződések és a kapcsolódó technológiai felvásárlások újraértékelését a JEDI-szerződéstől való elállás nyomán, és létrejött a JWCC, mert a DoD

[42] ECMA 2021. 3

[43] Cloud Native Desgin: a felhőalapú natív architektúra fokozza az IT Ops csapatok hatékonyságát, termelékenységét és együttműködési erőfeszítéseit azáltal, hogy a számítási felhő és a különböző felhőszolgáltatások kombinációját alkalmazza, hogy testreszabható moduláris infrastruktúrát hozzon létre nagyobb méretezhetőség mellett.

[44] ECMA 2021. 3.

[45] A JADC2 az Egyesült Államok Védelmi Minisztériumának (DoD) mozaikszava, a Joint All Domain Command and Control rövidítése, egy stratégiai háborús koncepció, amely összeköti az összes amerikai katonai szolgálat – hadsereg, haditengerészet, légierő, tengerészgyalogság – adatérzékelőit, lövészeket és kapcsolódó kommunikációs eszközöket és az űrerőt, és végül szövetséges partnereit egyetlen integrált „hálózati hálózatba". A stratégia 2022. január 3-án jelent meg.

szerint fontos lépést tartani a gyors technológiai változásokkal. Ezért az új szerződési feltételek biztosítják, hogy a DoD folyamatosan megkapja a kereskedelmi felhőpiac által kínált legjobb technológiai megoldásokat – mindhárom besorolási szinten.

Ezen elvek mentén a U.S. Army Cloud Computing Strategy meghatározza a stratégiai irányt és útmutatást ad a U.S. Army számára a biztonságos működési környezet fenntartására, miközben átalakítja a hadsereg információtechnológiai (IT-) infrastruktúráját, rendszereit, szoftvereit és alkalmazási platformjait, adatvagyonát, valamint a kapcsolódó műveleti szintű folyamatokat és gyakorlatokat. Ennek továbbfejlesztése az Army Cloud Plan, amely felvázolja a hadsereg vízióját arra vonatkozóan, hogy miként kívánja használni a felhőt annak biztosítására, hogy a hadsereg harci erői erősebbek, jobban felfegyverzettek és képzettebbek legyenek ellenfeleiknél az információs technológia használatában az információs harctéren.

Elmondható, hogy a stratégiai környezet a cArmy teljes körű használatára elég erős lábakon áll, amivel, ha a technikai kivitelezés sikeres, és sikerül operacionalizálni az adatokat és megfelelő beruházásokat tenni egy rugalmas információs ökoszisztémába, az amerikai haderő komoly előnyt szerezhet az információs térben.

A U.S. Army azon képessége, hogy elsajátítsa a számítási felhőt, fontos tényező abban, hogy a mesterséges intelligenciát és a gépi tanulást kiaknázzák a kibertéri hadviselésben. A hadseregnek kiemelten kell kezelnie pénzügyi és személyi erőforrásait, hogy céltudatosan folytathassa a fent felvázolt modernizációs erőfeszítéseket, illetve, hogy létrehozza, fenntartsa a digitális fölényt az ellenérdekelt felekkel szemben.

Felhasznált irodalom

Clarke, Steve (2016): *Fourth Quarter Results Highlight Microsoft Cloud Strength.* Online: https://news.microsoft.com/2016/07/19/microsoft-cloud-strength-highlights-fourth-quarter-results/

Clarke, Steve (2017): *Fourth Quarter Results Highlight Microsoft Cloud Strength.* Online: https://news.microsoft.com/2017/07/20/microsoft-cloud-strength-highlights-fourth-quarter-results-3/

ECMA (2021): *Army Enterprise Cloud Management Agency. Army Enterprise Application/System Modernization and Migration to Commercial Cloud Statement of Objectives (SOO)*. (2021. április). Online: https://bit.ly/3u0ZWoh

ENISA (2013): *Good Practice Guide for Securely Deploying Governmental Clouds*. Online: https://doi.org/10.2824/25181

Fedscoop (2020): *CIA Quietly Awards c2e Cloud Contract Possibly Worth Billions*. 2020. november 20. Online: www.fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/

Hogan, Michael – Liu, Fang – Sokol, Annie – Tong, Jin (2011): *Nist Cloud Computing Standards Roadmap*. NIST Special Publication, 35. 6–42. Online: https://csrc.nist.rip/library/NIST%20SP%20500-291%20Cloud%20Computing%20Standards%20Roadmap,%202011-07-05.pdf

Kovács Zoltán (2021) *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest, Ludovika Egyetemi Kiadó. Online: http://real.mtak.hu/128878/1/722_

az_infokommunkicios_rendszerek.pdfjsessionid513BA7B61ED404292AF714063F446241sequence1
Kundra, Vivek (2010): *25 Point Implementation Plan to Reform Federal Information Technology Management.* Online: https://apps.dtic.mil/sti/pdfs/ADA543512.pdf
Kundra, Vivek (2011): *Federal Cloud Computing Strategy*. 10–46. Online: https://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf
Kusnetzky, Dan (2009): Fourth Type of Cloud Computing. *ZD Net,* 2009. október 5. Online: www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346
Lepenye Tamás (2011): *Számítási felhő – egyszerűen.* Online: http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/
Lohrmann, Daniel (2010): Cloud First Policy. What Does It Really Mean? *Government Technology,* 2010. december 19. Online: www.govtech.com/blogs/lohrmann-on-cybersecurity/cloud-first-policy—121910.html
Magar, Alan (2014): *Assessing the Use of Tactical Clouds to Enhance Warfighter Effectiveness*. Defence Research and Development Canada. Online: https://apps.dtic.mil/sti/pdfs/AD1016956.pdf
Mittal, Vikram (2021): The Next JEDI: The Joint Warfighter Cloud Capability. Forbes, 2021. július 10. Online: www.forbes.com/sites/vikrammittal/2021/07/10/the-next-jedi-the-joint-warfighter-cloud-capability/?sh=543463a88550
Security Recommendations for Cloud Computing Providers (Minimum information security requirements) White Paper. Federal Office for Information Security, 2011. június 22. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2
U.S. Army (2015): *The Army Cloud Computing Strategy* (2015. március 26.). Online: www.army.mil/standto/archive/2015/03/26/
U.S. Army (2020): *The Army Cloud Plan* (2020. október 9.). Online: www.army.mil/standto/archive/2020/10/09/
U.S. Department of Defense (2021): *Future of the Joint Enterprise Defense Infrastructure Cloud Contract.* (2021. július 6.). Online: www.defense.gov/News/Releases/release/article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/
Vergun, David (2016): *The Army Aims for the Cloud.* U.S. Army, 2016. július 17. Online: www.army.mil/article/171548/the_army_aims_for_the_cloud
What is AWS GovCloud (US)? (é. n.). Online: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html
What is JWCC? (é. n.). Online: www.oracle.com/industries/government/federal/jwcc/