Polgári Szemle, 18. évf. 4–6. szám, 2022, 325–337., DOI: 10.24307/psz.2022.1223

Dobos Oszkár

A kiberhadviselés projektszempontú értelmezése elméleti és gyakorlati síkon

Understanding Cyber Warfare from a Project Perspective in Theory and in Practice

Összefoglalás

Napjaink fontos, talán legfontosabb területe az információs műveletek. Azért a legfontosabb, mert alkotó elemei, maga az információ, valamint a környezet, amiben az információ keletkezik, tárolódik és felhasználódik. A kibertérbe minden terület becsatlakozik, mi több joggal mondhatjuk, hogy napjainkra az alapja és mozgatórugója ezeknek. Ezért nevezzük a jelenkor társadalmát információs társadalomnak. Az ipar, a gazdaság és a politika, valamint természetesen a hadviselés is információs alapokon működik, mindegy milyen szakterületről beszélünk, az adat, az információ a digitalizáció biztosan szerves részét képezi. Napjainkban teljes mértékben az információ alapján működik a világ, ezért a fejlesztések iránya megfordul, nem a lakosság veszi át a hadsereg fejlesztéseit, hanem a hadsereg indul ki a civil fejlesztésekből. Eszerint az informatika szektor, pontosabban az infokommunikációs (továbbiakban IKT) szektor adja az alapot a fejlesztéseknek, amelyek utána az információs műveletekben is felhasználásra kerülnek. Napjainkban az IKT ipar és fejlesztéseik (ez minden iparágra vonatkozik) teljesen projekt alapon működnek, mind módszertant, mind pedig gazdasági, üzleti modellt tekintve. Ezen projektek, több aspektusból is kiemelkedően komplexek. A projektek mindig ideiglenes szerveződések, ezért sérülékenyebbek. Ezért tartom fontosnak a projektmenedzsment és az információs műveletek vizsgálatát, ami jelen publikáció témája.

Journal of Economic Literature (JEL) kódok: O22, D89, H56

Kulcsszavak: projektmenedzsment, információs műveletek, kiberhadviselés, kibervédelem

Summary

Information operations may be the most important area of our time. It can be considered the most important because it is made up of the information itself and the environment in which it is created, stored and used. Cyberspace integrates all domains and, moreover, it is fair to say that cyberspace has become the foundation and driving force of all these fields; hence the term information society. Industry, economy and politics, and of course warfare, are all based on information: no matter what discipline we are talking about, data, information and digitalisation are certainly an integral part of it. Today, the world operates entirely based on information, and therefore the direction of development is reversed: it is not the population that adopts the development of the military, but it is the mi-

Dobos Oszkár, tanársegéd, Óbudai Egyetem, Keleti Károly Gazdasági Kar, (dobos.oszkar@kgk.uni-obuda.hu).

litary that takes off from civilian development. Accordingly, the information sector, or more precisely the infocommunications (ICT) sector, provides the basis for developments which are then used in information operations. Today, the ICT industry and its developments are entirely project-based, both in terms of methodology, and economic and business models. These projects are very complex from different aspects. The information technology is so interdisciplinary in this times, many autonomous organizations belong to a project organisation with different IT security policies. The projects have temporary organizations, that is why they have higher vulnerability. This is why I consider it important to study project management and information operations, which is the subject of this publication.

Journal of Economic Literature (JEL) codes: O22, D89, H56
Keywords: Project management, information operations, cyberwarfare, cyber defence

Bevezetés

Több, a köznyelvben szállóigévé vált mondás bizonyítja az információ fontosságát. „Az információ hatalom" kifejezés jól rámutat: akinek a birtokában van, az a másik fölé tud kerekedni, versenyelőnybe kerül. „Az információ a jelenkor olaja", ami mutatja a gazdasági jelentőségét, jól alátámasztja a nagy tech óriások működését, hiszen mára már ez a legfőbb „termék", amivel kereskednek. Egyes kimutatások szerint az adatlopások motivációi közt is előkelő helyen szerepel a gazdasági haszon, vagyis pénzügyi értéket képvisel. Egy másik területen keresztül, de az információ fontosságára hívja fel a figyelmet a következő két mondás: „Az információ szabadság" és az „információ a demokrácia valutája". Szabadság, sajtó, politika területén is előkelő helyen szerepel a fontossági rangsorban az információ. Ezekben a közhelyekben az információ mellett az a közös, hogy nem cáfolja senki. Nem érdemes, ugyanis ez a legfőbb ismérve az információs társadalomnak, amiben élünk, az információ az alap építőkő és a legfőbb működtető elem.

Az információs környezet, vagyis a kibertér fontos szereplői és fejlesztői a magán vállalkozások, szervezetek és szakemberek. Ennek analógiájára feltételezem, hogy ezen stakeholderek a kiberhadviselésnek is aktív szereplői. Ebben az esetben a projektmenedzsereknek, mint szakembereknek is van szerepe a kiberhadviselésben. Rajtuk keresztül szeretném vizsgálni a publikáció fő kérdését: *létezik-e bármiféle kapcsolat a projektmenedzsment és a kiberhadviselés között?*

Az írás célja bemutatni a projektmenedzsment fontosságát a kiberhadviselésben. Megmutatni a jelenlegi kapcsolódási pontokat, elemezni és kategorizálni azokat, majd további lehetőségeket keresni ezek bővítésére. Be fogom mutatni a kiberhadviselés elválaszthatatlan viszonyát az infokommunikációs szektorral és civil szakemberekkel. Továbbá fontos szempont, hogy rávilágítsak arra, hogy a gyakorló projektmenedzserek aktív szereplői a kiberhadviselésnek, fontos kompetenciákat birtokolnak a reguláris erő számára. Jelen publikáció szempontjából, kiemelten fontos az információ, az információs környezet és az infokommunikációs iparág (továbbiakban: IKT), mert, ahogy a következőkben bemutatom, ez köti össze a kiberhadviselést és a projektmenedzsmentet.

A kiberhadviseléssel kapcsolatban a kiberműveletek is fókuszba kerülnek, az információval való közeli kötődésük és a kibertérhez való szoros viszonyuk miatt. A következő részben röviden kitérek mindkettő értelmezésére, összefüggésükre, de továbbra is egymás helyettesítőjeként fogom alkalmazni mindkettőt e munka keretein belül.

Tanulmányomban elsőként kitérek az általam használt fogalmak definíciójára, értelmezésére, úgymint a *kiberhadviselés, a kiberműveletek*, kiemelt fogalom lesz a *kibertér*, valamint ezek egymáshoz való kapcsolata is elemzésre kerül. Bemutatom az IKT szektort és kötődését egyik oldalról a kibertérhez, másik oldalról pedig a projektmenedzsmenthez. Megvizsgálom a projektmenedzsment szerepét az IKT szektorban és elhelyezem kiberhadviselésben. A felsoroltak világosan rámutatnak majd a kiberhadviselés és projektmenedzsment kapcsolatára, összefüggé-

sére. Majd az összegzés keretében, a lényeges pontok kiemelése mellett, további bizonyítandó következtetéseket, lehetséges kutatási irányokat mutatok be.

Jelen tanulmány módszertanát tekintve egy alapozó szekunder kutatás, mely szakirodalmi áttekintést jelent egy későbbi primer kutatáshoz. A tanulmány a témában meghatározó hazai és nemzetközi szakirodalmak áttekintésére készült. Ezen elemzést követően a primer kutatáshoz kerül majd hipotézis kidolgozásra.

A kibertér fogalma, szerepe napjainkban

A kibertér egyrészt a kiberhadviselést és az információs műveleteket körül ölelő környezet, másrészt pedig az IKT szektornak és projekteknek helyet adó tér. Ezen közös tulajdonság és kapcsolódás okán kezdem ennek értelmezésével a tanulmány szakmai részét. A számos létező és megalapozott definíció között a saját értelmezésemben a kibertér legfontosabb aspektusa az információ és annak tartózkodása, elérhetősége. Ezért a kibertér bemutatásánál Haig (2018:226) leírásából indulok ki: „a kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot" Magyarázatában a szerző is az információt emeli ki, mint kibertér magját és mozgatóját. Rávilágít a technológiai és logikai kapcsolatra gép-gép, ember-ember és ember-gép között. Továbbá rámutat az információáramlásra a szereplőkön és azok kapcsolatain keresztül, vagyis a virtuális dimenzióra. Ebből egyenesen következik a hálózatosodás, mely a mai tudás és információ alapú társadalom előfeltétele.

Haig gondolatait kiegészítve és alátámasztva, Kovács (2018) maximálisan tükrözi a modern IKT kor nézőpontját. Kovács szerint a kibertér egy olyan komplex halmaz, mely uniója minden elemnek és kisebb halmaznak, mely az információval érintkezik, vagyis a folyamatok, azok szereplői, technikai és szoftver eszközei, az érintett rendszerek és mindezek direkt módon vagy indirekt kapcsolattal, de egymással hálózatba vannak kötve.

A két meghatározást összegezve a kibertér meglátásom szerint egy olyan tartomány, melyben eszközök, folyamatok, rendszerek, tevékenységek és szereplők vannak kapcsolatban egymással, vagyis hálózatba vannak kötve. Direkt vagy indirekt módon kapcsolódnak az adat vagy az információ előállításához, feldolgozásához, átalakításához, szállításához, tárolásához vagy éppen a felhasználásához.

Kiberhadviselés és kiber műveletek

A kiberhadviselés az előbbiekben bemutatott, NATO által elismert hadszíntéren, a kibertérben zajló tudatos cselekmény. A hadviselés alapvetően szereplőket tekintve reguláris erők tevékenysége reguláris erők ellen, vagyis egy nemzet hivatásos állománya próbál valamilyen műveletet végrehajtani egy másik ellen. Az idejét tekintve határozottan elkülönül a béke és háborús időszak. Ezek mellett fizikailag vagy földrajzilag is behatárolható a műveleti terület. Ezekkel szemben a kibertérben mind a három aspektus határai elmosódnak.

A virtuális világ egyik fontos ismérve a földrajzi határtalanság, ami egyszer a világhálóra lett kötve, az elérhető a világ bármely pontjáról minimális késleltetési idővel, ezért a távolság, mint fizikai tényező megszűnik.

A későbbiekben bemutatott technológiák bizonyítják, hogy a virtuális világ szereplői nagyobb részt civil állampolgárok, akik a legtöbb esetben csak elszenvedői a kiberhadviselésnek, de ha szofisztikáltabb elemzést készítünk, akkor is maximum védekező szerepben tűnnek fel. Azonban ezen elemzés eredménye rámutat más szereplői körökre is, akik támadásokban is részt vesznek, akár tudatosan nemzet-nemzet elleni küzdelemben, akár önálló aktivistaként vagy anyagi haszon reményében (Gémes, 2018). Az időtényezőben is fontos változás

követhető nyomon: ezen tevékenységnek nincsen pontos eleje és vége . A legkönnyebben úgy lehet ezt bizonyítani, ha végig gondoljuk a jelenleg ismert tevékenységeket és technológiákat, amelyek akár támadásra, akár védekezésre szolgálnak a kibertérben. A védekezésre kifejlesztett technológiák, szoftverek és hardverek nem csak háborús készültségben, hanem minden percben, magas rendelkezésre állással működnek. Ez indokolt is, ugyanis a mindennapjainkban fellelhető adatgyűjtő szoftver robotok, zsaroló vírusok, automata adathalász e-mailek ellen folyamatos védekezés szükséges. Ezek a példaként említett eszközök, technológiák mindössze csak töredéke az interneten megtalálható folyamatosan működő kiberveszélyeknek és emellett számtalan kifejezetten tudatos, összehangolt támadás is történik olyan célpontok ellen, amelyek sérülése az állampolgárokon keresztül egy nemzet biztonságát veszélyeztetik. Ebben az esetben azt gondolom a támadás motivációja sem lényeges, ha az eredmény egy létfontosságú egység sérülése, leállása, mint például egy kritikus infrastruktúra elem.

A kiberhadviselést és kibertéri műveleteket a kibertér köti össze, ezért a kibertér leírt tulajdonságai, mindkettőre vonatkoznak. A kiberműveletek értelmezése Haig szerint: „A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire." (Haig, 2018:237).

A definíció rámutat a használt infokommunikációs technológiákra, valamint a kibertéren keresztül elérhető célközönségre, mely a később leírtak alapján meghatározóan az IKT szektorban tevékenykedő, vagy annak szolgáltatásait használó civil állampolgárok és szervezetek.

Kibertér technológiái, fejlődése

A kibertérben jelenleg vagy a jövőben alkalmazott technológiák közül jelen munkám fizikai keretei miatt nem térek ki teljes körűen. Azokat elemzem elsősorban, amelyek a kibertér bővüléséhez és a civilek kibertérbe való csatornázásához a leginkább hozzájárulnak, valamint bizonyítják az IKT szektor és a kibertér elválaszthatatlanságát.

Az első, ami mindenkinek eszébe jut, sőt tévesen sokak ezzel azonosítják magát a kiberteret, az az internet. Alapvetően a kibertérnek egy téves szűkítése, ha az internettel azonosítjuk, mégsem állunk tőle nagyon messze, ugyanis, ha hálózatra kötés alatt a globális hálózatot értjük, nagy valószínűséggel valahol összekapcsolódunk az internettel. Ez lehet direkt kapcsolat vagy egy eszköz, ami az interneten is elérhető. Ezután pedig már az internet részeivé váltunk, és elérhetőek leszünk. Ez az alapja a később bemutatásra kerülő *Internet of Things* technológiának (IoT) is.

Az internet lehetővé teszi és egyben ösztönzi a digitális ökoszisztéma kialakulását, melyben az állami és piaci szolgáltatások és adatok egyaránt elérhetőek szélessávú kapcsolaton keresztül. Ezen ökoszisztéma fejlődése és az internet fejlődése kölcsönösen ösztönzik egymást, így a folyamatos lefedettség és sávszélesség növekedéssel folyamatosan bővül a szolgáltatások köre és emelkedik a minősége.

Az internetre épülő technológiák közül a hálózatosodás egy következő szintjét a felhő technológia adja. A sávszélesség növekedésével lehetőség nyílt egy új megközelítésre. Nem a hálózatra kapcsolt eszközökön kell az adatokat tárolni és feldolgozni, hanem egy központi helyen a hálózaton. Ez egy fontos szemlélet váltás, mert alapjaiban változtatja meg a digitális működést, lehetővé teszi a komplex adatfeldolgozást, egymástól független rendszerek összekapcsolását. További előnye a felhasználók számára, a skálázhatóság, mindig annyi erőforrást használ, amennyire szüksége van, így a használt eszköznek nem szükséges szélsőségesen magas kapacitás a ritkán esedékes teljesítmény csúcsok kielégítésére. Az információk és szolgáltatások

több eszközről is elérhetőek, nem szükséges eszközönként többszörösíteni. Azért felhő technológiának nevezték el, mert a legtöbb esetben nem ismert az adatok holléte. Hatalmas szerverközpontokban kerül tárolásra és feldolgozásra az információ, de a performancia optimalizálás és terhelés megosztás miatt az is előfordulhat, hogy akár két külön földrészen is jelen van fizikailag a megjelenített tartalom. A vezeték nélküli kommunikáció térnyerése miatt, olyan, mintha egyszerűen a „felhőbe" küldenénk az adatokat. A felhő technológia fejlesztésével, ma már a virtuális infrastruktúra szolgáltatástól (IaaS), a platform szolgáltatáson át (PaaS) egészen a teljes szoftveres környezetig (SaaS) lehet stabilan és biztonságosan használni a szolgáltatásokat (IBM Cloud Education, 2021). Egy szemléltető példa a Google Chrome Book elnevezésű notebook, aminek nincs natív operációs rendszere. Egy Chrome böngésző fut a készüléken és minden más alkalmazást SaaS megoldással felhőből lehet online futtatni.

A tech cégek az IKT szektorban folyamatosan K+F+I projektekkel fejlesztik a meglévőkre épülő új technológiákat. A felhő alapú számítástechnika és az egyre fejlődő mobilkommunikáció, szemben az eddigi okos eszközök hálózatával, lehetővé teszi szinte minden elektronikai eszköz hálózatba kapcsolását, majd távolról való felügyeletét, vagy akár irányítását. Eszerint megfordul a feltétel iránya és a hálózatra kapcsolás alakít át okos eszközzé bármit. Ezt hívjuk Internet of Things-nek (IoT). Az IoT-nél sok esetben tényleg minden a felhőben történik az információval. A hálózatra kapcsolt eszközben mindössze egy szenzor és egy hálózati kapcsolatot lehetővé tevő mikrocsip található. Ez a kibertér vonatkozásában fontos mérföldkövet jelent, a valós fizikai világ nagy része a szenzorokon keresztül adatokká alakítható így a kibertérbe kerül. Az IoT technológia képezi az alapját a teljes okos ökoszisztémának, például az okosvárosoknak, okosotthonoknak, okosautóknak és azok tovább fejlesztésének az összekapcsolt járműveknek (connected vehicle), valamint az így létrejövő önvezető jármű technológiának (Farhan et al., 2018).

Ez hatalmas mennyiségű adatot jelent, amely az infokommunikációs technológiák térhódításával exponenciálisan növekszik. A Cisco 2018-2023-as előrejelzése szerint az internetfelhasználók száma 3,9 milliárdról 5,3 milliárdra fog növekedni és ennél is több hálózatra kapcsolt eszköz lesz elérhető 18,4 milliárdról 29,3 milliárdra fog növekedni a számuk (Cisco, 2018). Ez természetesen magával hozza az adatmennyiség növekedését is az egy évvel korábbi előrejelzés alapján, 2017-től 2021-ig a személyes adatforgalom 13 Gbyte-ról 35 Gbyte-ra fog emelkedni (Cisco, 2020). Az alkalmazott klaszszikus adatfeldolgozási módszerek, strukturált adatbázisok nem alkalmasak ilyen mennyiségű és ami még fontosabb, ilyen komplexitású adathalmazok feldolgozására, ezért egy újabb technológiai fejlődés van folyamatban, melyet *bigdata*-nak nevezünk. A *bigdata* az eddigi adatműveletektől eltérően működik, a hálózatra kapcsolt eszközön, szenzoron nincs adatfeldolgozás, ez a felhőben történik, ahol hatalmas mennyiségű adat gyűjtése és összekapcsolása megy végbe. Majd az ugyancsak hatalmas erőforrású szervereknek van megfelelő kapacitása a végpontokon kiadott műveletek végrehajtására. Ez a felhő alapú számítástechnika előnyei mellett lehetőséget ad egymástól teljesen független adatok összekapcsolására, ezáltal az információ eddig nem használt vagy nem is ismert módon való felhasználására, vizualizációjára.

A bemutatott, jelenleg is használt és széles körben elfogadott technológiák mellett, természetesen a jövő is az ezek és ehhez hasonló műszaki megoldások fejlesztéséről szól. Bár Raymond Kurzweil (2013) által definiált technológiai szingularitás szerint, a jövő technológiáit nem tudjuk megmondani, mert eljutunk egy olyan pontra a fejlődésben, ahol a gyors ütem következtében nem tudjuk felfogni a holnap működését. Mégis vannak becslések, a különböző kutatóintézetek próbálnak trendeket meghatározni, amelyek mutatják a jövőt néhány éves távlatban. A Gartner kutatóintézet folyamatosan elemzi, és egy hype görbe segítségével határozza meg a trendeket. A legfrissebb előrejelzés (2019-es) öt területet azonosít:

- Szenzorok és mobilitás: ez a trend olyan technológiákat tömörít, amelyek egyre inkább lehetővé teszik a mobilitást és a hozzátartozó eszközök kezelését, beleértve a 3D érzékelő kamerákat és a fejlettebb autonóm vezetést. A szenzorok és a mesterséges intelligencia (MI) fejlődésével az autonóm robotok tudatosabban működnek az őket körülvevő környezetben. Például az olyan új technológiák, mint a könnyű szállító drónok (mind repülő, mind guruló) fejlettebben fognak navigálni és figyelembe venni a tárgyakat. Ezt a technológiát jelenleg akadályozza a jogi környezet, de a műszaki fejlesztés tovább folytatódik. Az ide tartozó technológiák: felhő alapú kiterjesztett valóság (AR), önvezetés negyedik és ötödik szintje, valamint a repülő önvezető járművek.
- Emberi robottechnológiák: a trend az ember fizikai és pszichológiai képességeit hivatott fejleszteni biochippekkel és érzelmi mesterséges intelligenciával. Egy robot kar az emberi erőnél lényegesen nagyobb erőt képes kifejteni, de egyéb a valóságosnál hatékonyabb, ellenállóbb szerv beültetése is lehetséges. Ezekkel az eszközökkel, az ember egészségét, erejét és intelligenciáját is lehet fejleszteni. A trendbe tartozó technológiák: megszemélyesítés, kiterjesztett intelligencia és biotechnológia.
- Poszt klasszikus számítás és kommunikáció: klasszikus vagy bináris számítástechnika, amely bináris biteket használ, a meglévő, hagyományos architektúrák megváltoztatásával fejlődik. Ezek a változások gyorsabb CPU-kat, fejlettebb memóriát és növekvő teljesítményt eredményeznek. Ez magában foglalja az 5G-t, a következő generációs cellás szabványokat, ugyanakkor ide tartoznak a következő generációs chippek és 3D nyomtatás
- Digitális ökoszisztémák, melyek a kibertér szereplőit összekötő megosztó platformok. Ezek az ökoszisztémák, a digitalizáció következtében fejlődtek ki, átalakították a hagyományos értékláncokat, lehetővé téve, dinamikus kapcsolatok kialakítását a különféle szereplőkkel és szervezetekkel a földrajzi és iparági határokon túlmutatva. A jövőben ezek automatikusan emberi beavatkozás nélkül működő decentralizált szervezetek lesznek. Ide tartoznak, a különböző elosztott, decentralizált technológiák, és az adattudományok.
- Magas szintű mesterséges intelligencia és elemzések. A következő generációs elemzés az adatok vagy a tartalom autonóm vagy félig autonóm vizsgálata, kifinomult eszközök használatával, a hagyományos üzleti szempontokon túl. A gépi tanulási modellekre épülő technológiák lehetővé teszik az AI és azon keresztül az adatelemzések továbbfejlesztését. Ebbe a trendbe tartoznak az adaptív gépi tanulás, az AI, a grafikon elemzések. (Gartner, 2019).

Az előzőekben ismertetett új technológiák, fejlesztések az előnyök mellett fokozott kockázatot jelentenek, ugyanis biztosítják a teljes társadalom, és gazdaság bekapcsolását a kibertérbe. Emiatt mosódnak el a kiberhadviselés fizikai határai és jellemezhetjük aszimmetrikus hadviselésként, ahol nem reguláris erők is tevékenykednek.

IKT és a kiberműveletek

Az eddigieket összefoglalva, bemutattam az erős logikai kapcsolatot a kibertér és kibertérben használt eszközök, valamint IKT szektor között. A következőkben a kiberhadviselés, és kiberműveletek IKT-vel való kapcsolódási pontjainak áttekintése látható. A kibertéri műveletek információs képességén keresztül jól szemléltethető a kapcsolat. Azokra az információs képességekre fogok kitérni, amelyek kifejezetten a civil IKT-beli technológiákat használnak. Ezáltal mutatva az IKT szereplők fontosságát a kiberműveletekben.

A *számítógép hálózati műveletek* a kibertéri műveletek meghatározó és magához a kibertérhez legjobban illeszkedő információs képessége. A hálózatokon keresztül történő, támadás, védekezés és felderítés tartozik ide. Ezen tevékenységek hatásukat tekintve történhetnek a fizikai

vagy logikai rétegben egyaránt. Alapvetően logikai tevékenység a hálózat logikai részeit célozza, szoftvereket, adatbázisokat, operációs rendszereket vagy akár magát a hálózatot.

A *megtévesztés* információs képesség alatt értjük, amikor jellemzően nem valós információval hatunk a másik fél döntéshozatalára. Félrevezetjük annak érdekében, hogy reakciójával saját célunk elérését segítse. Ez a kibertérben, az IKT technológiákra koncentrálva hamis információkat, álhíreket jelent, de jelenthet manipulált hálózati vagy szenzor adatokat is.

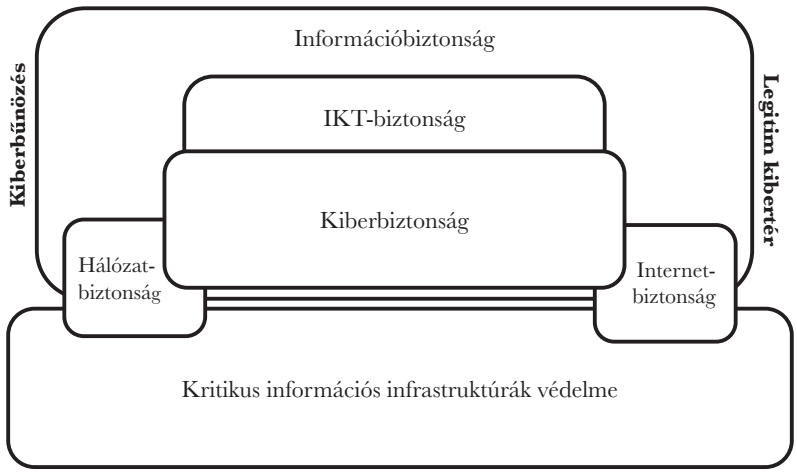
A *pszichológiai műveletek* képesség, egy speciális kommunikációs képesség, ahol az információ tartalmával kifejezetten az emberek kerülnek célpontba. A manipulálás, döntéseikre való hatásgyakorlás a cél. Ez lehet negatív is, akkor nagyon hasonló a megtévesztésnél alkalmazott dezinformáláshoz, vagy akár social engineering technikákhoz. Lehet pozitív is, valaminek az elfogadtatása, támogatása.

A tömegtájékoztatás lényeges információs képesség főleg a kibertérben, mert nagyon hatékonyan lehet nagy közösségekhez elérni, a weboldalakon, fórumokon és hírportálokon keresztül. Fontos ide sorolni a közösségi médiát, ami teljesen behálózza az információs társadalmat (Rózsa, 2019). Jelenleg már nem nagyon van offline média, tv vagy rádió, ami fel tudja venni a versenyt a tájékoztatás gyorsaságában, mennyiségében (Haig, 2018).

A számítógép hálózati műveletek egyértelműen civilek által is használt és üzemeltetett területek az IKT szektorban. A világhálón elérhető minden szervezet, szolgáltatás, szereplő lehet célpontja ezen tevékenységnek. Az infokommunikációs cégektől elkezdve, minden az ország szempontjából kritikus vagy létfontosságú rendszer, úgy, mint az állampolgárok tömegesen (Sridhar, 2019). A megtévesztés, pszichológiai műveletek és tömegtájékoztatás, ismét az IKT szektor termékeit és szolgáltatásait használva fejtik ki hatásukat, és az IKT által üzemeltetett hálózatokon találhatóak célcsoportjaik.

Az említett magas digitális szolgáltatás elterjedés következménye, a digitálisbiztonság iránti igény kialakulása, vagyis a kiberhadviselés védelmi képességének a kibervédelem megteremtésének szükségessége (Kelemen, 2020). Ezt tovább gondolva, a kibertér nélkülözhetetlen szereplői az IKT szervezetek és szakemberek, ezért fontos részét kell, hogy képezzék a kibervédelemnek. Alexander Klimburg véleménye szerint is az IKT szereplők szerves részét képezik az információ biztonságnak. A IKT

1. ábra: Az IKT biztonság elhelyezkedése a kiberbiztonságban



Forrás: Klimburg (2012) – szerző szerkesztése

cégek elfogadott és globálisan elterjedt termékei és szolgáltatásai egyúttal sérülékenységet is jelentenek. A világszerte használt termékek és szolgáltatások miatt egyetlen ország sem képes saját erőből, számára megbízható és kontrollálható forrásokból biztosítani a teljes IKT ellátási láncot. Azok a területek alapvetően kiemelt kockázatot jelentenek, ahol több beszállító termékét kell összeintegrálni, ezt még tovább növelik azok az esetek, ahol a szervezetek, vagy akár az adott ország számára megbízhatatlan, vagy kontrollálhatatlan termékek is beépülnek. A lenti ábra jól mutatja az IKT biztonság szerepét az kiberbiztonságban (Klimburg, 2012).

Tehát a legjobban kimutatható kapcsolata a kiberhadviselésnek és az IKT szektor szereplőinek a kibervédelemben, a kiberbiztonság megteremtésében van. Az IKT szektor szolgáltatásainak és eszközeinek a penetrációja olyan széleskörű és olyan mély a polgárok körében, mind a szervezeteket, mind pedig a magánembereket tekintve, hogy teljességgel lehetetlen leválasztani a kiberbiztonságról. Az úgynevezett puha támadások, ahol nem sérülnek adatok, rendszerek, jelenleg is léteznek. Ilyenek, a propaganda kampányok, álhír gyárak, de akár a bármilyen központi intézmény rendszerben meglevő polgári vagy akár piaci bizalom megrendítésére tett bejelentések is, ha megfelelő mértékben elterjednek a digitális világban (Csutak, 2018).

Az IKT és védelmi szektor kapcsolata a projektmenedzsmenttel

Az előzőekben bemutatott, kibertérhez szorosan kapcsolódó technológiák kivétel nélkül az IKT szektorban, vagy a szektor szereplőinek bevonásával kerülnek fejlesztésre, szolgáltatásra. A kiberműveletek projektmenedzsmenttel legjobban kimutatható kapcsolódása az infokommunikációs iparon, illetve annak fejlődésén keresztül látható. Ezért tartom fontosnak a szektor és a formális projektmenedzsment kapcsolatának vizsgálatát.

A világon legelterjedtebb és legtöbb nagy szervezet által használt formális projekt módszertanokat létrehozó és folyamatosan fejlesztő szervezetek a 20. század közepén jöttek létre. Az International Project Management Associoation (IPMA)-t 1965-ben (IPMA, 2015) a Project Management Institute (PMI)-t pedig 1969-ben (PMI) a brit kormány a projects in controlled environment (PRINCE) nevű módszertanát pedig 1989-ben (Prince2, 2017) alapították. Azóta folyamatosan fejlesztve, többször átdolgozva, mindig az adott környezetnek és technológiai eszközöknek megfelelően a projektek hatékony menedzsmentjét szem előtt tartva terjesztették a modelljeiket. Fontos megemlíteni, hogy ezek csak a formális módszertanok, a projektszerű működést és menedzsmentet, a század elejére tehetjük, Frederick Taylor definiálta művében a menedzsment tudományos elveit (Frederick, 1911) illetve, ami egy fokkal szorosabban kötődik a projektmenedzsmenthez, az pedig Henry Gantt által megalkotott Gantt diagram (Clark et al., 1922), amit a mai napig az egyik alapvető projektmenedzsment eszközként tartunk számon. A projektmenedzsment története szorosan összekapcsolódik hadviseléssel a védelmi iparon keresztül és az informatikával is. Az említett formális szervezetek előtt szűkebb körben használt már projektmenedzsmentet az Amerikai Védelmi Hivatal 1958-tól (Malcolm et al., 1959) több kutatás fejlesztési és prototípus fejlesztési területen is. Az informatikai kötődés direkt módon a PRINCE2 módszertannál, és a 2001-ben megalkotott agile manifesto-nál mutatható ki. Ez utóbbi, akkor még inkább volt szemlélet, mint konkrét modell, viszont kifejezetten informatikai, szoftverfejlesztési projektek menedzselése okán került kialakításra (Agile, 2001). A projektmenedzsment fejlődés története is bizonyítja a folyamatos kötődést a hadviseléshez és védelemhez, valamint az IKT iparban levő fejlesztésekhez is.

Jelenleg a Project Management Institute 2018-as felmérése szerint, a vállalatok 93%-a használ valamilyen standard projektmenedzsmentet (PMI, 2018). A Price Water-

house Coopers korábbi 2007-es felmérése is hasonlóan magas arányt mutatott ki, 77%-ban használnak a cégek, valamilyen dokumentált, egész vállalatra kiterjedő projektmenedzsment módszert (PWC, 2007).

A mai szervezetek szervezeti struktúrája az IKT szektorban, általában kétféle. Az egyik a projekt szervezet, ahol kifejezetten projekt alapú működés van, vagyis projekten kívül a kollégák csak tréningeken, oktatásokon, illetve belső hatékonyság javítási projekten vesznek részt. Jellemzően itt projekt után a munkavállalók bekerülnek egy úgynevezett erőforrás medencébe, ahonnan szabadon be lehet őket vonni egy induló, vagy futó projektbe. A másik szervezeti forma a mátrix szervezet, ahol, ha egy mátrixot képzelünk el, az oszlopok a funkcionális egységek a sorok pedig a projektek. Mind a funkcionális egységnek, mind pedig a projektnek van egy vezetője. A mátrix szervezetnél a funkcionális szervezeti egységben vannak alapfeladatok, amelyeket el kell látni. Az agilis módszertan elterjedésével, előtérbe kerül egy harmadik szervezeti struktúra, ami a projekt szervezetre hasonlít jobban, viszont itt nem esik szét a projekt csapat egy feladat elvégzése után, hanem egyben marad és csapatként dedikálják a következő feladatra. Ez kifejezetten agilis, rugalmas környezetben lehetséges csak, ezért még kevesebb szervezet választja és azok is tisztán szoftverfejlesztő cégek. (Saáry et al., 2021)

Mindkét fő szervezeti struktúra fókuszában a hatékony projektmenedzsment áll, működésük, munkájuk túlnyomó többsége projekt alapon zajlik. Látható, a projektmenedzsment kialakulását és fejlődését az informatika és a hadipar indukálta első sorban. Ez a kapcsolat átalakult egyfajta kölcsönhatássá, a projektmenedzsment és az IKT szereplők egymás fejlődését generálva alkotnak szimbiózist. A szervezetek működése és a szervezeti struktúrák átalakultak projekt fókusszal a hatékony projektmenedzsment érdekében. A projekt alapú működés pedig, a mindennapi munkánál, és ami nagyon fontos a K+F+I tevékenységnél is alapvető módszertan lett.

IKT projektek és a kiberműveletek

Az infokommunikációs projektek a kibertér kiterjedése, mindent áthatósága miatt, rendkívül összetettek, szinte soha nem csak informatikai területet érintenek, biztosan egy olyan program vagy rendszer részei, ahova más típusú domain tudás is szükséges. Éppen ezért jellegzetességei (Pather et al., 2022):

- A sok szereplő, akik java részt szervezeten belülről, de a legtöbb esetben szervezeten kívülről is érkeznek. Mivel, minden projekt egy ideiglenes szervezetet alkot ezek folyamatosan változnak az időben, még az aktuális projekten belül is.
- A különböző ismeret területek és sok szereplő összekapcsolása okán, több teljesen egymástól független szakismeret integrálása szükséges, ez bonyolulttá és nagy kockázatúvá teszi ezen projekteket.
- Az informatika terület egy nagyon dinamikus tudomány, a sok érintett miatt folyamatosan változó és nagyon bonyolult projektcélok jönnek létre.
- A fentiek és a teljesen egyedi projekttermékek miatt magas kockázatot hordoznak az ICT projektek.

Az informatikai projektek típusát, ha megvizsgálva láthatjuk, hogy minden terület erős összeköttetésben van a kibertérrel, abban kerül kivitelezésre, valamint felhasználásra később.

- Szoftver fejlesztési projekt
- Hardver fejlesztési projektek
- Alkalmazásfejlesztési projekt
- Rendszerintegrációs projekt
- Implementációs projekt
- Infrastruktúra fejlesztési projekt
- Költözés/migrációs projekt
- Tesztelési projekt

Fontos megjegyezni, a projektek komplexitása itt is jelen van, ezen projektek ugyan külön-külön is értelmezhetőek, a globális projektek, amelyeket az kibertéri műveletekben is értelmezünk ezek valamilyen arányú keveréke (Gaál-Szabó, 2003).

A projekt típusokkal leírhatóak a kibertéri műveletek információs képességeinek tevé-

kenységei, illetve az azokhoz használt eszközök és szolgáltatások fejlesztése. Ezen eszközök műszakilag lehetővé teszik az offenzív tevékenységet, ahogy erre létezik példa a világban civil-katonai együttműködés formájában (Dely, 2017). Jelen munkában leginkább a védelemre tudok koncentrálni az előzőekben említett jogi okok miatt. A védelem megtervezése, fejlesztése implementálása, valamint működése közbeni, fejlesztés, költözés tesztelési projektek, de pl. ide tartoznak egy incidens utáni a reagáló projekt is.

Kibervédelem mint, kiberhadviselési tevékenység és a projektmenedzsment

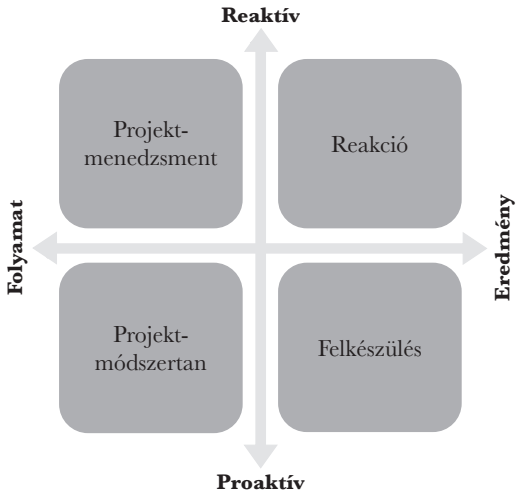
A kibervédelemnek az ICT szektorban határozottan elkülönülő tevékenységek típusait lehet megkülönböztetni. Az egyik típus, a védekezésre való felkészülés. Ide tartoznak a módszerek, modellek kidolgozása, technológiai fejlesztések a szoftver és hardver, valamint fizikai eszközök területén. Ezek után a védelmi rendszer megtervezése, kiépítése, tesztelése, majd üzembe helyezése és átadása az üzemeltetésnek következik. A másik terület, ennél dinamikusabb, egy esetleges támadás alatt és után felmerülő, olyan komplex feladatok, amelyek nincsenek benne a vészhelyzeti tervekben vagy a végrehajtásuk tervezést és jóváhagyást igényel. Ilyenek lehetnek a kárelhárítás során, egy költözés, migráció, új technológia bevezetése, a meglévő infrastruktúra átalakítása, rendszerek átparaméterezése, új szoftver verziók kiadása, távolról való beavatkozás a felhasználók által használt eszközökbe. Bár kevés információ található civil szereplők vonatkozásában, de ebbe a kategóriába tartozhat a felderítés vagy egy esetleges ellentámadás, a támadással azonosított szerver, rendszer, támadó-fél ellen is (Bratosin, 2014). Erre a mai jogszabályok nem adnak lehetőséget polgári szervezeteknek, ezért elvi lehetőség marad.

A bemutatott két típus a védekezés szempontjából meglátásom szerint:

- Proaktív, vagyis a felkészülési projektek.
- Reaktív, a reagálással kapcsolatos projektek.

Másik szemszögből vizsgálva, a megvalósítás folyamatára fókuszálva, szintén két kategóriát tudok azonosítani. Az egyik a projektvezetés folyamatával kapcsolatos tevékenység, vagyis a projekt kivitelezése közben történő védelem, mely a projektmenedzser hatáskörébe tartozik (Szemere et al., 2021). A jelenleg

2. ábra: Kibervédelmi tevékenység a projektekben



Forrás: saját szerkesztés

használt és elfogadott modellek kockázatként kezelik a projektekben a kibertámadást és folyamatos, reaktív védelem van ellene, részben a szervezeti policyt és eszközöket részben ideiglenes adhoc védelmi elemeket adaptálva. A másik kategória projektmenedzsment szemszögből egy sokkal proaktívabb tevékenység. Maga a használt projektmenedzsment modell tartalmazza a kiberbiztonságra vonatkozó előírásokat, standardokat. Ezáltal, azok validálásával és kiválasztásával nem szükséges foglalkozni, a kialakított környezet rendeltetésszerű használatára helyeződik a hangsúly.

A két kategóriával egy mátrix írható fel (2. ábra), mely teljeskörűen bemutatja a projektmenedzsment és kibervédelem kapcsolatát.

A mátrix kiolvasása a bemutatottak tükrében:

- Folyamat és proaktív: a projektvezetés szempontjából passzív védekezés, mert a védekezés a használt projektmenedzsment módszertanban kerül definiálásra, nincs lehetőség a standardokat felülírni projekt szinten. Előre meghatározott eszközöket és folyamatokat kell használni.
- Folyamat és reaktív: a projektek menedzselésének kibervédelmi aspektusa helyezkedik itt el. A projektvezető hatásköre és felelőssége a megfelelő védekezés, folyamatosan szükséges vele foglalkozni, reaktív módon, minden fenyegetésre, kockázat bekövetkezésre reagálni.
- Eredmény és reaktív: a projektek eredményén van a fókusz. Reakció a bekövetkezett biztonsági incidensekre, ellentevékenység semlegesítése, kárcsökkentés, kárhelyre állítás, tartozhat ide.
- Eredmény és passzív: a projekt eredményén van a fókusz. A kibervédelem megtervezése és kialakítása, valamint ehhez szükséges eszközök kifejlesztése a fő cél. A leszállított eredmények átadásáig tart a projekt, utána a támadás szempontjából egy passzív védelem, amit megpróbálnak áttörni vagy megkerülni.

Összegzés

Bemutatásra került az kiberhadviselés és az információs műveletek közti összefüggés, részletesen elemeztem a kiberteret, mint a környezetet, amelyben ezek a tevékenységek zajlanak. Rámutattam az IKT terület és kibertér elválaszthatatlan kapcsolatára, ezáltal az infokommunikációs szektor szereplőinek a szervezetek és szakemberek szerepének a fontosságára, mi több nélkülözhetetlenségére. Az ICT terület és a projektmenedzsment fejlődése egymásra kölcsönösen hatással van, erősítik egymást. A jelenleg elterjedt szervezeti struktúrák a projekt alapú működést és hatékony projektmenedzsmentet támogatva fejlődtek ki. Ebből következően az informatikai projektek, minden területen jelen vannak. A kibervédelemben jelenleg is jól kimutatható a fejlesztési, implementációs, rendszerintegrációs és tesztelési projekteket menedzselünk, valamint a kiberbiztonság területen reaktív projektek kivitelezése is zajlik. A projektmenedzsmentnek kétféle kibervédelmi aspektusa azonosítható, magára a módszertanra fókuszálva és egy aktívabb a projektvezetése közbeni tevékenység. Az általam kialakított mátrixnál, megemlítettem a felderítés és esetleges ellentevékenység elvi lehetőségét, ennek részletes vizsgálata azonban jelen publikációba nem fér bele.

Az összegzésem alapján jól láthatóan a gyakorló projektmenedzserek aktív szereplői lehetnek a kiberhadviselésnek, fontos kompetenciákat birtokolnak a reguláris erők számára. A további primer kutatás fókusza lehet, interjús és kérdőíves megkérdezése, az IKT szektor projektvezetői körében a meglévő együttműködések körbejárása, valamint a katonai és kormányzati szektor kiber erői körében egy igényfelmérés a további kapcsolati pontok azonosítása érdekében.

A kiberhadviselés teljes spektrumát lefedve és tovább erősítve a fenti elemzést jövőbeni kutatási és publikációs célnak azonosítom a projektmenedzsment kapcsolatát a kibertérben folyó felderítéssel és ellentevékenységgel.

Felhasznált irodalom

Agile Manifesto (2001): Manifesto for Agile Software Development. Link: https://agilemanifesto.org/ Letöltve:2020.06.20.

Bratosin, Bogdan Alexandru (2014): Cyber Defense Exercises and their Role in Cyber Warfare. *Journal of Mobile, Embedded and Distributed Systems*, 6(2), 70-76. Retrieved from http://jmeds.eu/index.php/jmeds/article/view/Cyber_Defense_Exercises_and_their_Role_in_Cyber_Warfare 2022.07.12.

Cisco (2019): *Visual Networking Index: Forecast and Trends*, 2017-2022, White Paper, Cisco Public https://twiki.cern.ch/twiki/pub/HEPIX/TechwatchNetwork/HtwNetworkDocuments/white-paper-c11-741490.pdf Letöltve: 2021.05.12.

Cisco (2020): *Annual Internet Report* (2018–2023) White Paper, Cisco Public https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html Letöltve: 2021.09.15.

Clark, Wallace – Polakov, Walter – Trabold Frank (1922): *The Gantt Chart: A Working Tool of Management.* NY: Ronald Press Company, New York

Csutak Zsolt (2018): Új idők új hadviselése – Kognitív biztonság az információs és a kiberhadviselés korában. *Honvédségi Szemle* – Hungarian Defence Review, A Magyar Honvédség Központi Folyóirata, 146(5), 33–45. Elérés forrás https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/345

Dely Péter (2017): Polgári válságkezelő műveletek információs támogatása: *Magyar Rendészet* 17. évf., 2. sz. (2017) p. 113-128

Gaál Zoltán – Szabó Lajos (2003): *Segédlet a projektmenedzsmenthez II*, Veszprémi Egyetemi Kiadó.

Gartner (2019): *5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies,* Kasey Panetta https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/ Letöltve: 2020.06.20.

Gémes Csaba (2018): A kibertér szereplői, *Hadmérnök* XIII. Évfolyam 3. szám – 2018. szeptember

Haig Zsolt (2018): *Információs Műveletek A Kibertérben*, Dialóg Campus Kiadó. Budapest, 2018. 110 o. URL: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf;jsessionid=97D3B77EE69E4C11F4B0AE1A46544334?sequence=1 Letöltve:2020.06.20.

IBM Cloud Education (2021): https://www.ibm.com/cloud/learn/iaas-paas-saas Letöltve: 2021.10.20.

IPMA (2015): 50 years anniversary of IPMA – The early period of IPMA https://www.ipma.world/about-us/ipma-international/history-of-ipma/

Kelemen Roland (2020): A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle* – Hungarian Defence Review, 148(4), 65–81. https://doi.org/10.35926/HSZ.2020.4.5

Klimburg, Alexander (2012): *National cyber security framework manual, Tallinn, Estonia*: NATO Cooperative Cyber Defence Centre of Excellence Publication. Tallin,

Kovács László (2018): *A kibertér védelme*, Dialóg Campus Kiadó. Budapest, 2018. 110 o. URL: http://hdl.handle.net/20.500.12944/12603

Kurzweil, Ray (2013): *A szingularitás küszöbén*. Ad-Astra Kiadó, Budapest, 2013

Laith, Farhan – Rupak, Kharel – Omprakash, Kaiwartya – Marcela Quiroz-Castellanos, Ali Alissa – Mohamed Abdulsalam (2018): *A Concise Review on Internet of Things (IoT) -Problems, Challenges and Opportunities*," 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2018, pp. 1-6, doi: 10.1109

Malcolm, Donald G – Roseboom, John H. – Clark, Charles E. (1959): Application of a Technique for Research and Development Program Evaluation, *Operations Research* Vol. 7, No. 5, September–October, pp. 646–669 https://doi.org/10.1287/opre.7.5.646

Pather, Shaun – Remenyi, Brendan – Remenyi, Dan (2022): *MANAGING RISKS OF ICT PROJECTS.* Published by Academic Publishing LtdCurtis Farm, Kidmore End, Nr Reading, RG4 9AY, UK https://www.researchgate.net/publication/267684648_MANAGING_RISKS_OF_ICT_PROJECTS Letöltve: 2022.07.12.

PMI (2011): PMI Founders, pmi.org https://www.pmi.org/about/learn-about-pmi/founders Letöltve: 2020.06.20.

PMI (2018): Pulse of the Profession: Success in Disruptive Times, https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf Letöltve: 2020.06.20.

Prince2 (2017): The History of Prince2, www.prince2.com Letöltve: 2020.06.20. https://www.prince2.com/eur/blog/the-history-of-prince2

PWC (2007): Insights and Trends: Current Programme and Project Management Practices, PricewaterhouseCoopers https://www.pwc.com/cl/es/publicaciones/assets/insighttrends.pdf Letöltve: 2020.06.20.

Rózsa Tibor (2021): Az információs műveletek elmélete, gyakorlata és tendenciái. *Honvédségi Szemle* – Hungarian Defence Review, 147(5), 73–87. Elérés forrás https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/225 Letöltve: 2022.07.12.

Saáry Réka – Csiszárik-Kocsir Ágnes – Varga János (2021): Examination of the Consumers' Expectations Regarding Company's Contribution to Ontological Security, *Sustainability* 2021,13,9987. https://doi.org/ 10.3390/su13179987 13: 17 p. 9987, 19 p.

Sridhar, Varadharajan (2019): Why Regulate the ICT Sector? In: *Emerging ICT Policies and Regulations*. Springer, Singapore. Online https://doi.org/10.1007/978-981-32-9022-8_1

Szemere Tibor Pál – Garai-Fodor Mónika – Csiszárik-Kocsir Ágnes (2021): Risk Approach - Risk Hierarchy or Construction Investment Risks in the Light of Interim Empiric Primary Research Conclusions, *Risks* 2021, 9(5), 84; https://doi.org/10.3390/risks9050084

Taylor, Frederick Winslow (1911): *The Principles of Scientific Management internet archive Norton* https://web.archive.org/web/20050828013043/http://melbecon.unimelb.edu.au/het/taylor/sciman.htm Letöltve: 2020.06.20.