HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám

GYURÁK GÁBOR

A kriptográfia és a hírszerzés hadtudományi gyökerei

Military roots of cryptography and intelligence

Absztrakt

Az információ nem csak napjaink társadalmában játszik fontos szerepet, hiszen már az idők kezdete óta az emberek és gyakorlatilag minden élőlény a rendelkezésére álló információk alapján hajtja végre cselekedeteit. Akár a magánéletben akár egy hadsereg vezetőjeként egy jó döntést csak úgy lehet meghozni, ha releváns információkkal rendelkezünk a döntést érintő körülményekről. Ebben a cikkben szeretném bemutatni, hogy a történelem (főként a hadtörténelem) jeles szereplői miként viszonyultak az információ megszerzésének és titokban tartásának művészetéhez, illetve tudományához. Bemutatásra kerülnek Szun-ce, Plübiosz, Julius Caesar, Clausewitz, Zrínyi Miklós gondolatai, de nem maradnak ki az újkor és napjaink elektronikus hírközlésének, hírszerzésének és rejtjelezésének meghatározó momentumai sem.

Abstract

Information plays an important role in nowdays society, but it was always important in history. Since the beginning of time every human and every living being base decisions on information. As a private person or even as a general we can make good decision only if we have enough and relevant information about the conditions affecting the decesion. In this paper I would like to present how scientists, especially military scientsts were thinking about information retrieval and cryptography during history. Ideas are presented from Sun-ce, Plübiosz, Julius Caesar, Clausewitz, Miklós Zrínyi and others. Challenges and solutions of cryptography and intelligence are also shown from the infocommunication based present age.

BEVEZETÉS

„*Scientia potentia est*”, azaz a tudás hatalom, hirdeti a latin mondás. A tudást viszont információkból tudjuk felépíteni. Akinek a birtokában van az információ, az előnyben van másokhoz képest, ezért mindenki arra törekszik, hogy minél gyorsabban, minél több információval rendelkezzen. Ez a folyamat az információ-szerzés, amelyet a társadalmi fejlődéssel párhuzamosan egyre tudatosabban használ az emberiség. Amikor megjelentek az

HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám

első államok, akkor a közösség biztonsága azt kívánta meg, hogy szemmel tartsák a szomszédokat, kifürkésszék azok ellenséges szándékait. Így az egyén információszerzése mellett a közösség érdekében végzett hírszerzés és kémkedés is kezdetét vette.

Az élet többszereplős játék, amelyben úgy is előnyre tehetünk szert, ha versenytársaink információ-szerző képességét korlátozzuk, esetleg hamis információkkal megtévesztjük. Az információért folytatott küzdelemben nagyon fontos szerepe van az információ eltitkolásnak. Mondhatnánk úgy is, hogy a titkolódzás egyidős az emberiséggel, de ezt a művészetet már az emberiség megjelenése előtt is sikerrel alkalmazta az élővilág. Az evolúció évmilliók óta dolgozik azon, hogy az élőlények rejtőzködési képességét tökéletesítse. A történelem során az ember egyre kifinomultabb technikákat alkalmazott az információk eltitkolására. Ennek egyik eszköze a rejtjelezés.

A hírszerzés és a rejtjelezés legfontosabb momentumai könnyebben átláthatók, ha a történelmet korszakokra bontjuk. A felbontáshoz a hírközlő eszközök fejlődésének korszakait vegyük alapul. 6.[2]

1. Az első korszak a *szóbeli közlések* korszaka, amikor közvetlen kommunikációval történt meg az információ átadása.
2. A második korszak az *írásbeli közlés* időszaka, amikor az írás információhordozóvá vált.[1] Így lehetővé vált az üzenetek többlépcsős továbbítása.
3. A harmadik korszak a *futárrendszer*, amelyet Kínában, Indiában és a görögöknél már az ókorban is alkalmaztak.
4. A negyedik korszak a *távírók* korszaka, amikor nagy távolságokra lehetett üzeneteket továbbítani különböző fizikai megoldásokkal (füst, fény…). Ennek gyökerei egészen az i.e. II. századig nyúlnak vissza.
5. A XIX. században kifejlesztett távíró alapozta az ötödik korszakot, az *elektronikus hírközlés* korszakát.
6. Végül napjaink hírközlési korszakának jellemzője a *globális kommunikáció*. Mobiltelefon és műholdas hálózatok, valamint a számítógép-hálózatokra épülő Internet jelenti a hírközlés alapvető eszközét.

ÓKORI MEGOLDÁSOK

Az előző fejezetben láttuk, hogy a hírszerzés, a kémkedés és a rejtjelezés egyidős az emberrel, de úgy gondolom elegendő, ha abba a korszakba megyünk vissza, amikor már tudatosan használták ezeket a technikákat.

[1] Az írás hordozójaként nem csak a papír szolgált. A görögök úgy küldtek titkos üzeneteket, hogy rabszolgáik leborotvált fejbőrére írták üzenetüket, majd csak azután küldték el a címzetthez, ha újra kinőtt a haja. *6.[1]*

HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám

SZUN-CE (I. E. V. SZÁZAD[2])

Szun mestert többféle néven említik a feljegyzések, de abban nagyjából egységes az álláspont, hogy fő műve *„A háború művészete”* hadművészeti alapmű. A könyv 13 fejezetben ismerteti a hadászati stratégiákat és leírja, hogy milyen a jó hadvezér. Olyan alapelveket fektet le, amelyek figyelmeztetik a hadvezéreket, hogy kerüljék a felesleges vérontást:

„A háború legfőbb művészete az ellenség legyőzése harc nélkül.”

„A legjobb csata az, amely harc nélkül zajlik.”

Ezt úgy lehet elérni, ha a hadvezér a lehető legtöbb információval rendelkezik az ellenségről. A mű egyértelműen a hírszerzés fontosságára hívja fel a figyelmet. Ennek alátámasztására külön fejezet[3] foglalkozik a kémkedéssel.

Az ellenség legyőzésének titkát (a siker titkát) az „*előretudásban*” látja, amelyhez kémeket kell alkalmazni. Pontosan ötféle kém alkalmazását javasolja:[4]

- *helybéli kém:* a helyi lakosok közül felfogadott kém;
- *belső kém:* az ellenség tisztviselői közül felfogadott kém;
- *átállt kém (kettős ügynök)*: az ellenség kémei közül felfogadott kém;
- *feláldozható kém:* saját kém, akit hamis információval látunk el annak érdekében, hogy félrevezesse az ellenséget miután az elfogta;
- *élő kém*: az ellenségtől hírekkel visszatérő kém.

A kémekre azért van szükség, hogy megismerjük az ellenfelet és mindenről előre tudjunk. A kémeket nagyvonalúan meg kell jutalmazni, és titokban kell tartani a tevékenységüket. Utolsó gondolatában, mintegy konklúzióként megállapítja, hogy *„a háborúban ez a legfontosabb; a hadsereg a kémekre támaszkodva tud helyesen cselekedni.”*

A kínai mester a kémekre, mint az információszerzés „eszközeire” tekint, de titkosítással és rejtjelezéssel kapcsolatos gondolatokat is olvashatunk műveiben. A háború művészetének taglalásakor követelményként szabja, hogy a csapatok *„úgy járjanak el, úgy cselekedjenek a hadvezér tervei és számításai szerint, hogy abba senki ne nyerhessen bepillantást*”. Ez azt jelenti, hogy titokban kell tartani a terveket, sőt, azt is leírja, hogy célszerű többször megváltoztatni a tervet és a szándékokat, hiszen az ellenfél előnyt kovácsolhat abból, ha a titoknak hitt információkat megszerzi. A katonai titok megőrzése elengedhetetlen feltétele a győzelemnek.

Szun-ce nem csak hadvezér és katonai teoretikus, hanem kiváló matematikus is volt és éppen a titkosítás, a rejtjelezés az, ami megmagyarázza a kapcsolatát mindkét tudománnyal. A modern kriptográfia[5] részét képezik a kongruenciarendszerek, amelyek megoldására a kínai maradéktétel használható. [5] A tétel onnan kapta a nevét, hogy egy kínai mate-

[2] Nem tudjuk pontosan mikor élt, csak becslések vannak rá.
[3] *6.[3]* 13. fejezet.
[4] Más fordításokban más elnevezésekkel találkozhatunk. Például a Terebess kiadásában megjelent, Tőkei Ferenc fordításban az öt kém sorrendben: megtelepedett kém, belső kém, visszatérő kém, halál kéme, élet kéme.
[5] Görög eredetű szó, jelentése titkosírás. Mára önálló, de erősen az informatikához kötődő tudományágnak tekinthető.

HADTUDOMÁNYI SZEMLE

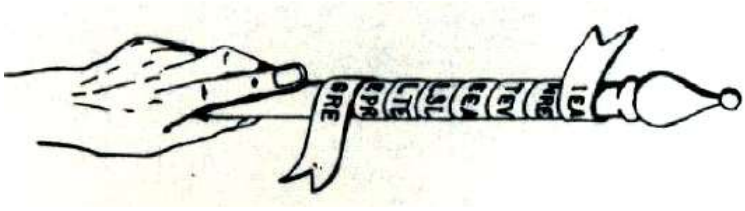
2014. VII. évfolyam 3. szám

matikus művében olvasható a legkorábbi megfogalmazása. A mű címe: *„Matematikai kánon”* és szerzője nem más, mint Szun-ce.[6] Valószínűleg a szerző nem volt tisztában azzal, hogy az általa megfogalmazott matematikai tétel lesz a 21. század rejtjelezésének egyik alapja, katonai művében mégis nagy jelentőséget tulajdonít a műveletek titokban tartásának.

GÖRÖGÖK (I. E. III. SZÁZAD)

Az ókori görögöknél a hírszerzés és titkosítás mindenféle megoldásával találkozhatunk, amelyek abban a korban nagyon hasznosnak bizonyultak. A hírek továbbításához számtalan fortélyt alkalmaztak annak érdekében, hogy az információ ne kerüljön jogosulatlanok birtokába. Voltak, akik fülbevaló helyett henger alakúra formált ólom lapocskákon rejtették el az üzeneteteket, és voltak olyanok is, akik sebeikre erősített falevelekre írták a titkokat.

Talán az egyik leghíresebb és a modern kriptográfiai könyvekben szinte kivétel nélkül megemlített titkosítási megoldás a *szkütálé* (1. ábra), amelyet a spártaiak vezettek be. Ez volt a világtörténelem első katonai rejtjelkulcsa. Egy lapos tekercs tartalmazta a titkos üzenetet, amely csak úgy vált olvashatóvá, ha a tekercset egy megfelelően vastag pálcára feltekerték. *Lüszandrosz*[7] is ezt használta a titkos üzenetekhez.



1. ábra Szkütálé [8] [9]

A megfejtés kulcsa a pálca vastagságának ismerete volt (ennek az információnak a címzett birtokában kellett lennie). [7] Látható, hogy már az ókorban is kulcsokat használtak a titkosított üzenet előállítására és visszafejtésére. *Aineiasz* i.e. 360 körül azt írja, hogy *„különböző módozatok léteznek, csak az szükséges, hogy azok küldője és kézhez kapója előbb egyeztessenek.*” [6] A kulcsok cseréjére különböző módszereket is javasol.

A szkütálé megfelel a modern szimmetrikus kulcsú titkosítási rendszerek ősének, amikor is ugyanazt a kulcsot alkalmazza a küldő és a fogadó is. Akkor is és ma is megoldást kell keresni a kulcsok biztonságos eljuttatására. A harmadik hírközlési korszakban ezt

[6] Szun-ce többféle néven is ismert: Sun Tzu, Sun Wu, Szun-cu, Sun Tzi
[7] Lüszandrosz spártai hadvezér, i.e. 395-ben halt meg.
[8] Az ACA (American Cryptogram Association) hivatalos szimbóluma.
[9] Az ábra Dr. Tóth Mihály – A Kriptorendszerek első generációja című főiskolai jegyzet címlapjáról való (BMF)

futárokkal oldották meg, manapság pedig bonyolult kulcscsere-protokollok[10] végzik ezt a feladatot. Az elvek ugyanazok, csak az eszközök változtak.

POLÜBIOSZ (I. E. 203-120)

A hírközlés negyedik korszakát Polübiosztól számítjuk. Ő volt az, aki leírta az első katonai híradó rendszer, a *tűztávíró* alapjait. A rendszer részeit képezik a jelzőállomások, amelyeket jellemzően várfalakon álló emberek valósítottak meg. Az emberek a kezükben tartott fáklyák felemelésével tudtak információt közölni a távoli megfigyelőknek. A vevő a fényjeleket megismétli, így a feladó megbizonyosodhat arról, hogy az üzenetet megértették. Bár nagyon egyszerű dologról van szó, mégis megteremtette a ma is széles körben használt nyugtázás alapjait.[11] Az üzenetek továbbítása kódolt formában történt. A kódolást egy táblázat tartalmazta (ez volt a kulcs), amely meghatározta a fáklyák darabszámát és elhelyezkedését. Tehát ez a rendszer nem csak a hír (információ) nagy sebességgel, nagy távolságra történő eljuttatását tette lehetővé, hanem azt is, hogy mindezt biztonságosan, titkosítva lehetett megtenni.

JULIUS CAESAR (I. E. 100-44)

Caesar nevéről mindenkinek eszébe jut a kiváló hadvezér és halálának misztikus körülményei. Olyan emberről van szó, akinek a neve minden rejtjelezéssel foglalkozó könyv történeti áttekintésében megtalálható.

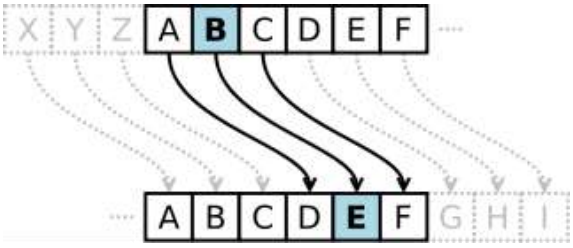
Julius Caesar a galliai háború során idegen területeken vezette seregeit, ezért információkat kellett gyűjtenie a sikeres döntések meghozatalához. Ezt a hírszerzés és a kémek szolgáltatták neki. Nem elhanyagolható az sem, hogy saját üzeneteit, parancsait rejtett formában juttatta el embereihez, így ha a futárokat el is fogta az ellenség, akkor sem juthatott értékes információk birtokába.

Caesar már megkülönböztette a kémeket a hírszerzőktől. A hírszerzők csoportosan dolgoztak, míg a kémek szigorúan titkosan, önállóan végezték feladatukat. A hivatásos hírszerző és kémszolgálat kiépítése mellett felismerte a titkos üzenetek célba juttatásának veszélyeit, gyengeségeit és kifejlesztett egy rejtjelezési megoldást, amely a mai napig az ő nevét viseli. Ez a *Caesar titkosítás* [5], amelyet a 2. ábra szemléltet.

[10] Például Diffie-Hellmann kulccsere protokoll *6.[5]*
[11] Hasonló elven működik a TCP (Transmission Control Protocol) protokoll, amely lehetővé teszi az megbízhatatlan szolgáltatást nyújtó IP (Internet Protocol) feletti megbízható adatátvitelt.

HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám



2. ábra Caesar titkosító[12]

Caesar *„ha titkos dolgot közölt, kulcsírást alkalmazott, vagyis úgy állította össze a betűk sorrendjét, hogy abból valóságos szó nem alakult. Ha valaki ezt az írást meg akarja fejteni, az ABC negyedik betűjét, tehát a D betűt helyezze az A helyére, hasonlóképpen kell a többi betűt is felcserélni.”*[13]

A mai kor színvonalán ez a rejtjelezés már nem jelent védelmet titkos üzeneteinknek, de kiindulási alapként felhasználható a komplexebb rejtjelezők összeállításához, illetve a kriptográfia oktatásának bevezető példájaként alkalmazható.[14]

ÚJKORI MEGOLDÁSOK

Az ókor után egyből az újkor megoldásaira térünk át. Ez nem azt jelenti, hogy a középkorban ne lettek volna fontos állomásai az információszerzésnek és titkosításnak. A középkorban élt Fibonacci (1170-1250), aki Szun-céhoz hasonlóan újra megfogalmazta a kínai maradéktételt és a róla elnevezett Fibonacci-sorozat alapját jelenti a mai véletlenszám generátoroknak.[15]

Az arab kriptográfia jeles képviselője, Ibn Khaldun (1332-1406) munkássága és Johannes Trithemius (1462-1516) nyomtatott kriptológia könyve[16] is a sötét középkorhoz köthető.

[12] Forrás: http://people.inf.elte.hu/pibuaai/ (Látogatva: 2014.06.11.)
[13] Gaius Suetonius Tranquillus – A császárok élete, Magyar Helikon, 1975.
[14] Például a Pécsi Tudományegyetem Pollack Mihály Műszaki és Informatikai Karán az „Informatika biztonság alapjai” című tantárgy egyik gyakorlatán a hallgatók Caesar rejtjelezőt készítenek Java programozási nyelven.
[15] Pontosabban az álvéletlen számok generálására használható a Fibonacci-sorozat, amely az algoritmizált kriptográfiához elengedhetetlen.
[16] Ez volt az első a világtörténelemben.

HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám

ZRÍNYI MIKLÓS (1620-1664)

Kiváló költőnk és hadvezérünk, akit a „magyar Szun mesterként" is említenek, műveiben többször kiemeli a kémkedés és a titoktartás jelentőségét.

A *Vitéz hadnagy* [8] Aphorismák[17] fejezetének *Explorator*[18] szakaszában ezt írja: „*… valamennyi vitéz cselekedet volt ez világon, mind jobbára kémek által ment végbe.*" A végvári harcokban (is) nagy szerepe volt annak, hogy megismerjék az ellenség haderejének mennyiségét és minőségét, a velük hadban álló fél szándékát. Akkoriban még nem a mai fogalmaink szerinti hírszerzés történt. Általában kereskedők kémkedtek, hiszen ők áruikkal bejárták nem csupán a magyar várakat, hanem a török által megszállt területeket, sőt Konstantinápolyt is. Általában elmondható, hogy Zrínyi idejében a hírszerzés és a kémkedés egyéni tevékenység volt, amelyhez olyan egyéni módszerek társultak, amelyek általában a kémek és megbízóik titkai maradtak.

Az Aphorismák *Secretum*[19] szakaszában kifejti a titok megőrzésének jelentőségét. Véleménye szerint titok nélkül egy kapitány nem lehet sikeres. Fontos, hogy az alárendeltjei zúgolódása, elégedetlenkedése ellenére se tárja fel nekik valós szándékait, mert „a titok a kulcsa a ládának, ahol a te szerencséd fekszik." Az ember természetéből eredendően nehezen tud titkot tartani, de egy kapitánynak rendelkeznie kell ezzel a képességgel. A titok megőrzéséhez viszont ismernie kell azt is, hogy milyen módon lehet elveszíteni azt. Ennek négy lehetőségét tárja fel: (1) részegség, (2) bosszúság, (3) nyereség és (4) félelem. Figyelmeztet arra az örök igazságra is, hogy az asszonyok nem tudnak titkot tartani. A szakasz utolsó gondolata sokak által idézett mondata Zrínyinek: „*Nem titok az, akit sok ember tud.*"

A hadvezér nem csak elméletben beszél a titok fontosságáról, de levelezései során alkalmazza is a titkosítást. Eddig 204 levelét találták meg és hozták nyilvánosságra. A levelek tanúsága szerint a titkosírást II. Rákóczi Györggyel történt levelezéseiben kezdte használni. [9]

CARL VON CLAUSEWITZ (1780-1831)

Clausewitz korának egyik legjelentősebb katonai teoretikusa volt. A hadtudomány egyik alapművének számító „*A háborúról"* című könyvének sorai között[20] is találhatunk olyan gondolatokat, amelyek ezen cikk témájához kapcsolódnak.

Clausewitz megfogalmazásában a hírek az ellenségről és az országról szerzett értesülések összességét jelentik, ezek képezik elgondolásaink és cselekedeteink alapját. A háborúban szerzett hírek azonban többnyire bizonytalanok, nagyobb részük valótlan, ellentmondó. Szerinte megnehezíti a hírek objektív értékelését az is, hogy a rosszat hamarabb

[17] Az Aphorismák a könyv egyik fejezete a Discursusok és a Centuriák mellett.
[18] 5. szakasz, jelentése: hírszerző, kém.
[19] 53. szakasz, jelentése: titoktartás
[20] Hatodik fejezet: A hírek

hisszük el, mint a jót. Az ember hajlamos arra, hogy a rosszat felnagyítsa, különösen háborús helyzetben nehéz a tisztánlátás. A tapasztalatlan hadvezérek ezért a helyszínen többnyire tanácstalanná válnak, mivel azt hiszik, hogy a körülmények eltérnek attól, ahogy elképzelték őket. [10]

ARTHUR SCHERBIUS (1878-1929)

Az I. világháború végén már az 5. generációs – elektronikus – hírközlő rendszerek világát értjük, amikor Arthur Scherbius német mérnök kifejleszti Enigma névre keresztelt rejtjelező gépét. Az írógép nagyságú berendezés működési elvének alapját a francia Bazaries őrnagy által felfedezett rejtjelező tárcsák adták. A titkosítást úgy oldották meg, hogy a billentyűzet egy gombjának lenyomása a tárcsasoron egy olyan áramkört zárt, amelynek árama meggyújtott egy jelzőlámpát, ami a rejtjelbetűt jelezte. A gépi úton rejtjelezett szöveg továbbítása rádión valósult meg. A vevő oldalon a titkosított szöveg dekódolása szintén Enigmával történt. Scherbius találmányát a német hadsereg átvette és a II. világháborúban is alkalmazták. Az Enigmát feltörhetetlennek tartották.

3. ábra Enigma H [21]

A gép működési elvének megfejtésével angol és francia tudósok próbálkoztak, de végül egy lengyel kódfejtőkből álló csapatnak sikerült megfejteni. A siker kulcsa az volt, hogy az angoloknak sikerült megszerezni a németektől két készüléket, amelyet részletesen tudtak tanulmányozni. Ezek után 1942-től az angolok már tömegesen fejtették meg a német táviratokat.

A kriptográfusok által elért eredmény jelentőségét mutatja, hogy Winston Churchill kijelentése: „*Nos, hála a minden fronton használt titkos fegyvernek, megnyertük a háborút…*”

[21] Forrás: Crypto museum (www.cryptomuseum.com, utolsó látogatás: 2014.06.15.)

HADTUDOMÁNYI SZEMLE

2014. VII. évfolyam 3. szám

RON RIVERST, ADI SHARIM, LEONARD ADLEMAN (1977)

1977-et írunk, amikor a három tudós az elődök által lefektetett ismereteket felhasználva kifejleszti a nyílt kulcsú titkosítást megalapozó RSA algoritmust. Működése a nagy prímszámok és azok összeszorzásával létrejövő még nagyobb számok prímtényezőkre bontásának nehézségén alapul. Ez az algoritmus, amely napjaink biztonságos kommunikációját lehetővé teszi. A titkosított böngészéstől a digitális aláírásig mindenhol találkozunk vele (és a belőle kifejlesztett alkalmazásokkal). Keresve sem találhatnánk jobb példát arra, hogyan ér össze a múlt és a jelen. Az RSA-hoz szükség volt Szun-ce kínai maradéktételére, Vigénere ötleteire, Fermat tételeire és a többi elődök elszántságára, amellyel a tudományt gazdagították.

NAPJAINKBAN

Néhány évtizede már, hogy a globális kommunikáció korszakába léptünk. Az elektronika és a számítástechnika olyan léptékű technikai fejlődést eredményezett az információszerzés és rejtjelezés világában, hogy alapjaiban megváltoztatta világunkat. A mindennapi életünk részévé váltak az információs technológiák. Az információszerzés és rejtjelezés mindenki által ismert és alkalmazott fogalmak.

George Arthur Orwell 1949-ben megjelent „1984” című híres regényében előrevetítette a jövőt. „*Az embernek abban a tudatban kellett élnie – s abban a tudatban is élt, ösztönné vált megszokásból –, hogy minden hangját hallják, s kivéve, ha sötét van, minden mozdulatát megfigyelik*” [22]

Orwell fantáziája valósággá vált. 2000-ben világszenzációként robbant be a köztudatba az ECHELON nevű műholdas lehallgató rendszer, amely a legkülönbözőbb kommunikációs eszközök (telefon, fax, Internet…) lehallgatására alkalmas. Öt ország (USA, Kanada, Ausztrália, Nagy-Britannia és Új-Zéland) együttműködésével épült ki az egész emberiség kommunikációs hálózatának forgalmát figyelő, szigorúan titkos műholdak, földi megfigyelő bázisok, kémhajók és tengeralattjárók integrált rendszere. [11] Az ECHELON a legkorszerűbb hang- és optikai karakterfelismerő rendszereket tartalmazza és olyan kódszavas, illetve kifejezés szótárakon alapuló szövegfelismerőt, amely a kulcsszavak alapján kiválogatott üzenetekre hívja fel a figyelmet. A rendszer célja a terrorizmus megelőzése és elhárítása, egyféle információpajzsként veszi körbe Földünk minden lakosát. A 2001. szeptember 11-es események mégis azt bizonyítják, hogy ez a pajzs áttörhető. [2]

Mindamellett, hogy jobbnál jobb titkosítási algoritmusok léteznek, a Földön olyan elképzelhetetlenül nagy számítási kapacitás is rendelkezésre áll, amellyel szemben a legjobb titkosítással sem lehet védekezni. Az Orwell által megálmodott „Big Brother” világnak „va-

[22] George Arthur Orwell: 1984

lószínűleg" szereplői a titkosszolgálatok,[23] az Internetes közösségi oldalak,[24] a világméretű információs szolgáltatók,[25] a kormányok… végső soron mindenki.

ÖSSZEFOGLALÁS

A fentiekben áttekintettük az információszerzés és titkosítás történelmi mérföldköveit és megoldásait egészen az ókortól napjainkig. Megállapítható, hogy mindkét fogalom a kezdetek óta jelen van és foglalkoztatja az embert. Ugyanazok a problémák újra és újra előjönnek, a különbség az, hogy fejlettebb technikával és az elődök tudásának ismeretében egyre jobb és jobb megoldások születnek.

Kulcsszavak: hírszerzés, kémkedés, rejtjelezés, rejtjelfejtés,

Keywords: intelligence, spying, encryption, decryption

FELHASZNÁLT IRODALOM

[1] Gonda János: A rejtjelezés néhány kérdése, ELTE, Budapest, 2010.

[2] Dénes Tamás: TitokTan Trilógia, Bagolyvár Kiadó, Budapest, 2004.

[3] Szun-ce: A háború művészete (ford.: Tokaji Zsolt és Szántai Zsolt)

[4] Szun-ce: A hadviselés törvényei (ford.: Tőkei Ferenc) WEB forrás: http://terebess.hu/keletkultinfo/hadviseles.html (látogatva: 2014.07.07.)

[5] Buttyán Levente, Vajda István: Kriptográfia és alkalmazásai, Typotex, Budapest, 2013.

[6] Háhn István: A hadművészet ókori klasszikusai, Zrínyi Kiadó, 1963. (elektronikus változat)

[7] Simon Sight: Kódkönyv, Park Könyvkiadó, 2007.

[8] Zrínyi Miklós: Vitéz Hadnagy, Zrínyi Miklós hadtudományi munkái, Zrínyi Kiadó, Budapest, 1976.

[9] Révay Zoltán: Titkosírások, Kossuth Nyomda, Szeged, 2001.

[10] Carl von Clausewitz: A háborúról (Fordította: Réczey Ferenc), Budapest, 1961.

[11] Janusz Piekalkiewicz: A kémkedés világtörténete, Zrínyi kiadó, Budapest, 1997.

[23] A cikk írásakor a híradások rendszeresen beszámolnak az NSA (National Security Agency) lehallgatási botrányáról.
[24] A cikk írásakor legnépszerűbb ilyen szolgáltatás a Facebook (facebook.com)
[25] A cikk írásakor a legnagyobb információs mamutvállalatot (Google Inc.) rengeteg támadás éri az általa alkalmazott adatvédelmi szabályzata miatt.