KOVÁCS LÁSZLÓ - KRASZNAY CSABA

DIGITÁLIS MOHÁCS

BEVEZETŐ

- **Az előadás célja:**
  felhívni a figyelmet, hogy az Európai Unió legtöbb országához hasonlóan hazánkban sem történt áttörés a Kritikus Infrastruktúrák és a Kritikus Információs Infrastruktúrák Védelme területén
- **Ugyanakkor a függőség percről percre nő ezen rendszerekkel szemben!**
- **Ezek a rendszerek pedig igen sérülékenyek, sőt mi több támadhatók!**
- **Fontos: nem minden esetben csak „tiszta” informatikai támadásokkal, hanem komplex – informatikai és fizikai – támadásokkal lehet igazi kárt okozni**

BEVEZETŐ

- Az előadásban csak nyílt forrásból származó információ került felhasználásra (Internet ->google)
- Nem tippadás, vagy ötletek gyártása a cél!
- A részleges vagy időleges működésképtelenségtől kezdve a teljes, az egész országot (régiót) érintő rendszerkiesések okozhatóak a vázolt helyek támadásával
- Következmények: BELÁTHATATLANOK!

MOHÁCS

- **MOHÁCS:**
  - **1526. augusztus 29.: 1,5 óra alatt gyakorlatilag Magyarország elesett**
  - **taktikai, stratégiai, információszerzési, és nem utolsó sorban talán belső (politikai) csatározások, helyezkedések miatt ->**

Ismerős történet?

KOMPLEX, INFORMÁCIÓS ÉS FIZIKAI TÁMADÁS-SOROZAT A MAGYAR KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK ELLEN

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK

Kritikus infrastruktúra:

„Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy **társadalmilag elvárt minimális** szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti **állapot fenntartásában**” *2080/2008. Korm. Hat.*

Kritikus információs infrastruktúra:

„**ICT systems** that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).” *EU Zöld Könyv*

Ágazat	Alágazat
I. Energia	1. kőolaj kitermelés, finomítás, tárolás és elosztás
	2. földgáztermelés, tárolás, szállítás és rendszerirányítás, elosztás
	3. villamosenergia-termelés, átvitel és rendszerirányítás, elosztás
II. Infokommunikációs technológiák	4. információs rendszerek és hálózatok
	5. eszköz-, automatikai és ellenőrzési rendszerek
	6. internet, infrastruktúra és hozzáférés
	7. vezetékes és mobil távközlési szolgáltatások
	8. rádiós távközlés és navigáció
	9. műholdas távközlés és navigáció
	10. műsorszórás
	11. postai szolgáltatások
	12. kormányzati informatikai, elektronikus hálózatok
II. Közlekedés	13. közúti közlekedés
	14. vasúti közlekedés
	15. légi közlekedés
	16. vízi közlekedés
	17. logisztikai központok
IV. Víz	18. ivóvíz szolgáltatás
	19. felszíni és felszín alatti vizek minőségének ellenőrzése
	20. szennyvízelvezetés és -tisztítás
	21. vízbázisok védelme
	22. árvízi védművek, gátak

V. Élelmiszer	23. élelmiszer előállítás
	24. élelmiszer-biztonság
VI. Egészségügy	25. kórházi ellátás
	26. mentésirányítás
	27. egészségügyi tartalékok és vérkészletek
	28. magas biztonsági szintű biológiai laboratóriumok
	29. egészségbiztosítás
VII. Pénzügy	30. fizetési, értékpapírklíring- és elszámolási infrastruktúrák és rendszerek
	31. bank és hitelintézeti biztonság
VIII. Ipar	32. vegyi anyagok előállítása, tárolása és feldolgozása
	33. veszélyes anyagok szállítása,
	34. veszélyes hulladékok kezelése és tárolása,
	35. nukleáris anyagok előállítása, tárolása, feldolgozása
	36. nukleáris kutatóberendezések
	37. hadiipari termelés
	38. oltóanyag és gyógyszergyártás
IX. Jogrend – Kormányzat	39. kormányzati létesítmények, eszközök
	40. közigazgatási szolgáltatások
	41. igazságszolgáltatás,
X. Közbiztonság – Védelem	42. honvédelmi létesítmények, eszközök, hálózatok
	43. rendvédelmi szervek infrastruktúrái

INFORMÁCIÓS HADVISELÉS:

Államok közötti információs tevékenység (hadviselés), inkább civil megfogalmazás

INFORMÁCIÓS MŰVELETEK:

Katonai tevékenység. Területei:

- PSYOP
- Elektronikai hadviselés
- Számítógép-hálózati műveletek
- Megtévesztés
- Műveleti biztonság

INCIDENSEK AZ ELMÚLT ÉVEKBEN

- Észtországot 2007. április 27-én érte külső támadás, ami elsősorban DDoS jellegű volt, de masszív spammelés és deface-ek is jellemezték.
- Célpontok:
  - Az észt Parlament
  - Bankok
  - Minisztériumok
  - Újságok és elektronikus hírközlők
- Az elkövetést egy orosz hazafias csoport vállalta magára 2009-ben.
- Egy ilyen támadás a sokkal informatizáltabb USA-ban lényegesen nagyobb károkat okozott volna!
- Részletesen ld. Muha Lajos 2007-es Hacktivity előadását!

INCIDENSEK AZ ELMÚLT ÉVEKBEN

- 2008 augusztusában, az Olimpia alatt kitör a grúz-orosz háború Dél-Oszétia miatt.
- A háború során mindkét fél intenzív információs csatát is vív, az internetet is felhasználva -> dacára a szegényes infrastruktúrának, az internetes tájékoztatás kiiktatását elsődleges fontosságúnak tartják
- A grúz kormány elérhetetlenné tette az orosz weboldalakat.
- A grúz, orosz, dél-oszét és azeri weboldalak folyamatos hacker célpontok voltak -> mindkét fél bevetette ezt az eszközt
- http://en.wikipedia.org/wiki/2008_South_Ossetia_war

INCIDENSEK AZ ELMÚLT ÉVEKBEN

- A gyaníthatóan a kínai kormány által indított támadások az USA szerverei ellen 2003-ban kezdődtek, melynek a Titan Rain fedőnevet adták
- 2009 áprilisában jelentek meg hírek arról, hogy a kínaiak hozzájutottak a szupertitkos Joint Strike Fighter bizonyos terveihez is
- A Kínában gyártott eszközökben időről időre „érdekes” kódokat találnak -> Green Dam egy Magyarországon forgalmazott IP kamerában
- Céljuk a behatolás, az információgyűjtés és egy esetleges konfliktus esetén a rombolás, NEM CSAK AZ USA-ban!!!

INCIDENSEK AZ ELMÚLT ÉVEKBEN

- 2009 júliusában dél-koreai magán és kormányzati oldalak ellen indult DDoS támadás
- Célpontok: hírportálok, online aukciós site, bankok, az elnök weblapja, a Koreában állomásozó amerikai csapatok honlapja, stb.
- A támadásba bevontak több amerikai weboldalt is, de ezeknek nem volt nagy hatása
- Feltételezések szerint vagy Észak-Korea vagy egy vele szimpatizáló kisebb hacker csoport áll a támadás mögött
- Tanulság: néhány ember, különösebb hadászati tudás nélkül is képes hatalmas károkat okozni, akár egy informatikailag fejletlen államból is!

MAGYAR ESEMÉNYEK

- Magyarországot szerencsére eddig nem érte különösebb külső támadás.
- Láttuk azonban, hogy egy kisebb csoport is képes kellemetlenséget okozni.
- Az elmúlt év magyar eseményei mutatják, hogy már a mi életünk is nagyban függ az informatikai szolgáltatásoktól.
- Címlapra került példák: Ügyfélkapu, OEP, ÁFSZ
- Pedig ezek csak emberi hibák voltak, senki nem akart rosszat!

EGY LEHETSÉGES FORGATÓKÖNYV

- 2002-ben a Gartner és a US Naval War College felkérte négy iparág (elektromos hálózat, telekommunikáció, pénzügyi szolgáltatások, internet) biztonsági szakembereit, hogy tervezzék meg a saját területük informatikai romba döntését.
- A keretek: terrorista támadást kellett szimulálni, a kor technológiáinak felhasználásával, a támadó csapatok 5 főből álltak, minimális fizikai támadásra volt lehetőség, a költség pedig nem lehetett több 50 millió dollárnál…
- Lépései: stratégiai tervezés, felkészülés és felderítés, támadás és ellentevékenység, felülvizsgálat

EGY LEHETSÉGES FORGATÓKÖNYV

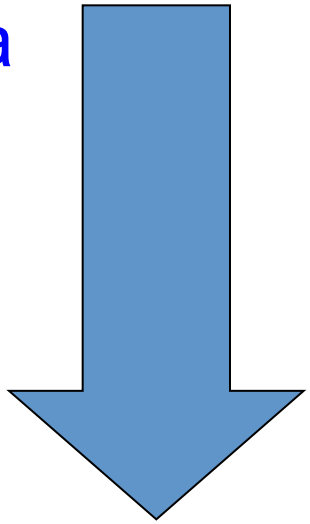
- Eredmények:
  - Elektromos hálózat: helyi kiesések okozhatók távoli támadásokkal, de teljes kimaradás nem. A fizikai (nagyfeszültségű vezetékek oszlopainak felrobbantása) vagy social engineering támadások viszont sikeresek lehetnek. A SCADA rendszerek védtelennek tűnnek. Ha nincs áram, nem működik a többi rendszer sem…
  - Pénzügyi szolgáltatások: A rengeteg szolgáltató miatt heterogén környezet alakult ki, ezért tömeges károkozás nem valószínű. Ha viszont sikerül, az USA gazdasága megbénulhat.

EGY LEHETSÉGES FORGATÓKÖNYV

- Internet: Sikerült olyan megoldást találni, amivel az internet megbénítható. Ehhez a szakértők kártékony kódokat terveztek, amiket P2P hálózatokon keresztül kívántak terjeszteni. Hasonlóan a mai botnetek működéséhez…
- Távközlés: a részt vevő szakértők már a tervezés megkezdése előtt tudták, hogy a távközlési szolgáltatás megbénítható. Az iparág ugyanis sok egyéni megoldást használ, megfelelő biztonsági tervezés nélkül – szemben a közhiedelemmel.

DIGITÁLIS MOHÁCS FORGATÓKÖNYV

- **A forgatókönyv alapjai**:
  - Információgyűjtés
  - PSYOP
  - Infrastruktúrák **KOMPLEX** támadása
- **A támadás sorrendje**:
  - Média, műsorszórás és internetes média
  - Pénzügy
  - Közlekedés
  - Telekommunikáció és internet
  - Villamos-energia szolgáltatás



MŰSORSZÓRÁS

- **PSYOP**:

  A fizikai támadást megelőzően olyan hírek elterjesztése, amelyek a közelgő támadásokat harangozzák be -> a média ma (is) vevő a szenzációra!

- **Technikai támadás**:
  - Informatikai támadás a kereskedelmi és közszolgálati médiumok ellen – deface, majd rendszerleállítás;
  - Fizikai és/vagy elektronikai támadás (zavarás, EMP) a műsorsugárzó rendszer ellen (AH)

HACKTIVITY

MŰSORSZÓRÁS

Széchenyi-hegy, adótorony

By GRics
Misplaced?
Inappropriate
Comment it

Panoramio

Upload your photos »

INTERNETES MÉDIA

- A tömegtájékoztatás alapvető eleme, támadásának célja kettős:
  - Dezinformáció
  - Az információktól való elszigetelés
- A legnagyobbak: Origo, Index, Blikk, NOL, Hírszerző, stb.
- Talán a legsérülékenyebb célpontok -> Nyílt forrásból ismert az Index korábbi sebezhetősége
- Egy konfliktus esetén elsődleges célpontok lesznek!

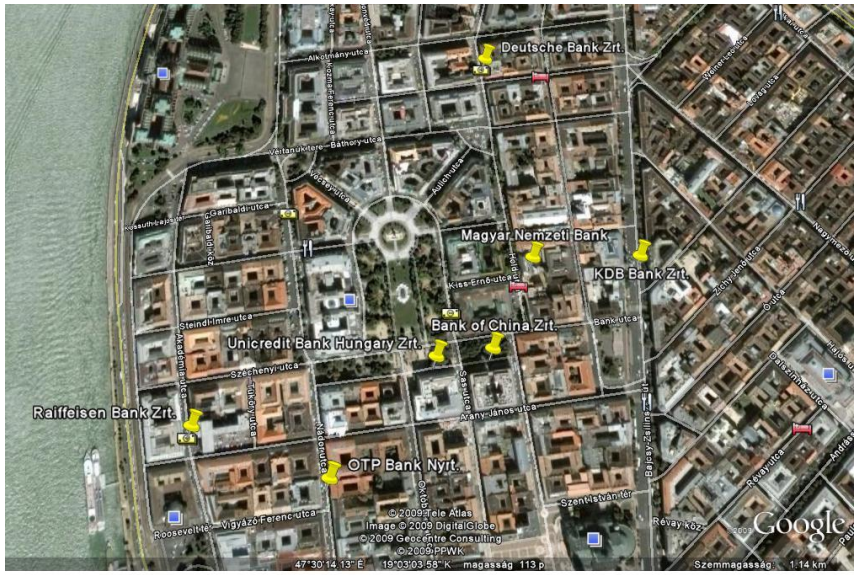
Célpont:

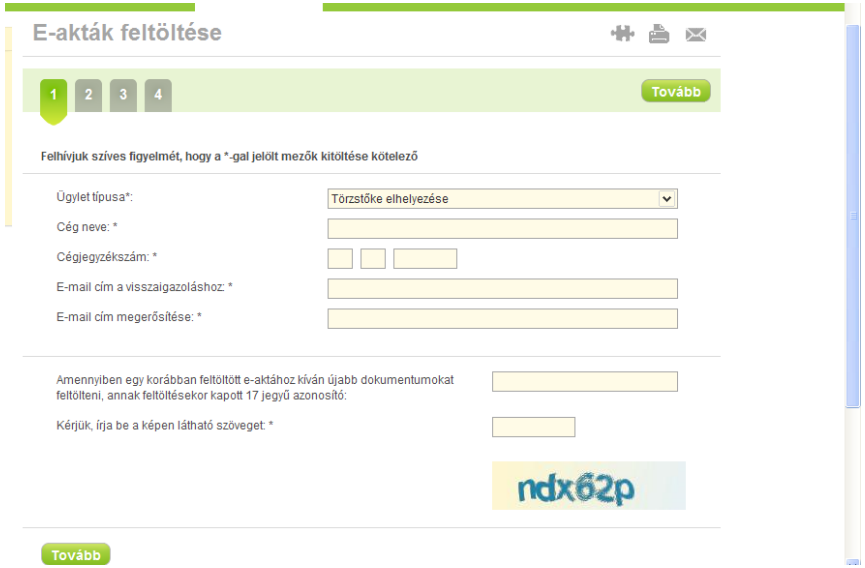
Magyar Államkincstár

- Nagyon jól védett mind fizikailag, mind informatikailag.
- Az egyik legfontosabb pénzügyi infrastruktúra
- De! (Hogyan):
  - Social Engineering,
  - Külső szakértők és vállalatok
  - Területi igazgatóságok
  - Önkormányzati informatikai kapcsolatok

BANK ÉS HITELINTÉZETEK

- Talán a legjobban védett infrastruktúrák (köszönjük, PSZÁF!)
- De tudjuk, hogy a központok csomókban helyezkednek el (köszönjük, PSZÁF!☺)
- A fizikai támadások ebben az esetben is sikeresek lehetnek
- De amíg ilyen barátságos feltöltőfelületet biztosítanak, az interneten is lehet próbálkozni!





BANK ÉS HITELINTÉZETEK

- **Példa a leállásra:**

  2008. január elején a CIB Bank és az Inter-Európa Bank egyesítette informatikai rendszerét.

  Eredmény:
  több hetes kiesések az internet banki szolgáltatásban.

Célpont:

Budapesti közúti közlekedés-irányítás és ezzel párhuzamosan a BKV forgalomirányítása

- **Hatás:**
  - országos logisztikai ellehetetlenülés,
  - alapvető regionális ellátási problémák,
  - egészségügyi ellátási problémák
  - …
  - …

Célpont:

Budapesti közúti közlekedés irányítás és ezzel párhuzamosan a BKV

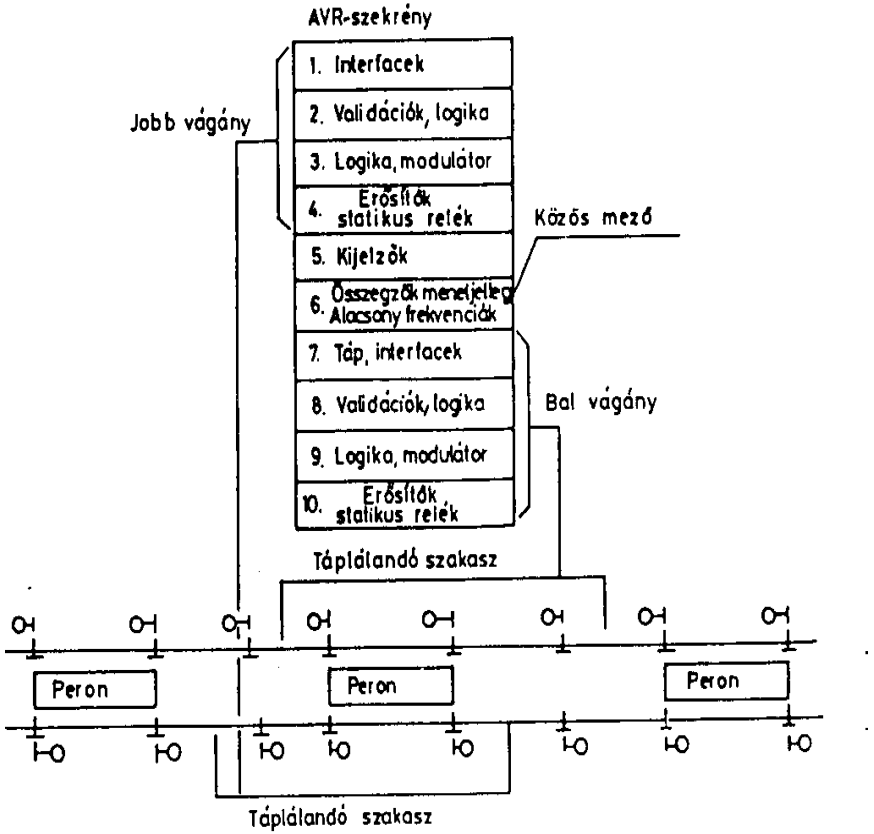
- **Hogyan:**
  - Open your mind!
  - Csak két példa ->

Példa 1:

METRÓ

A metró vasútbiztosító és automatikus vonatvezető rendszere

- A 3-as metróvonal max. kapacitása **26-27000** utas/óra irányonként!
- Két megálló között, mindkét irányban megáll egy-egy zsúfolt szerelvény … (LONDON)



Proximity kártyás azonosítás

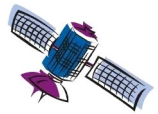
Gépjárművezető
Jegyellenőr

Kapcsolattartás az elektronikus jegyek és bérletek kezelésére alkalmas olvasóberendezéssel

Autóbuszok

Helyzet-meghatározás (GPS)
Kommunikáció (GPRS, WLAN)
Viszonylatjelzők vezérlése
Utastájékoztató táblák vezérlése
Hangos utastájékoztatás
A jármű paramétereinek figyelése
A FORDA kezelése
Menetlevél előkészítés
"Beléptető" rendszer
Késés, sietés kezelése
Kapcsolattartás a jelzőlámpákkal
stb...

GPS
Műholdak



Kis hatótávolságú rádió

GSM GPRS

Forgalomirányító jelzőlámpák

"Zöld út kérés"

Megállói utastájékoztató táblák vezérlése

Mikor jön a következő járat ?

Kommunikáció a központtal

GPRS InterNet

WLAN

Kis hatótávolságú rádió

GSM GPRS

Pályaudvari utastájékoztatás

Kommunikáció a központtal

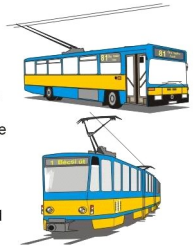
GSM GPRS

Mobilszolgáltató GATEWAY SERVER

GSM GPRS

Trolibuszok, Villamosok

Helyzet-meghatározás (GPS)
Kommunikáció (GPRS, WLAN)
Viszonylatjelzők vezérlése
Utastájékoztató táblák vezérlése
Hangos utastájékoztatás
A jármű paramétereinek figyelése
A FORDA kezelése
Menetlevél előkészítés
"Beléptető" rendszer
Késés, sietés kezelése
Kapcsolattartás a jelzőlámpákkal
stb...



Proximity kártyás azonosítás

Gépjárművezető
Jegyellenőr

Kapcsolattartás az elektronikus jegyek és bérletek kezelésére alkalmas olvasóberendezéssel

InterNet

Internet

Külső munkaállomások
Mobil terminálok
VPN

DSL Internet

Internetszolgáltató GATEVAY SERVER

Internet
FIX IP

TŰZFAL

Irányítási rendszer adatkapcsolati és adatbázis SERVER
telephely

Kapcsolattartás a járművekkel
Kapcsolattartás a megállótáblákkal
Adatok gyűjtése, archiválása
Adatbáziskezelés

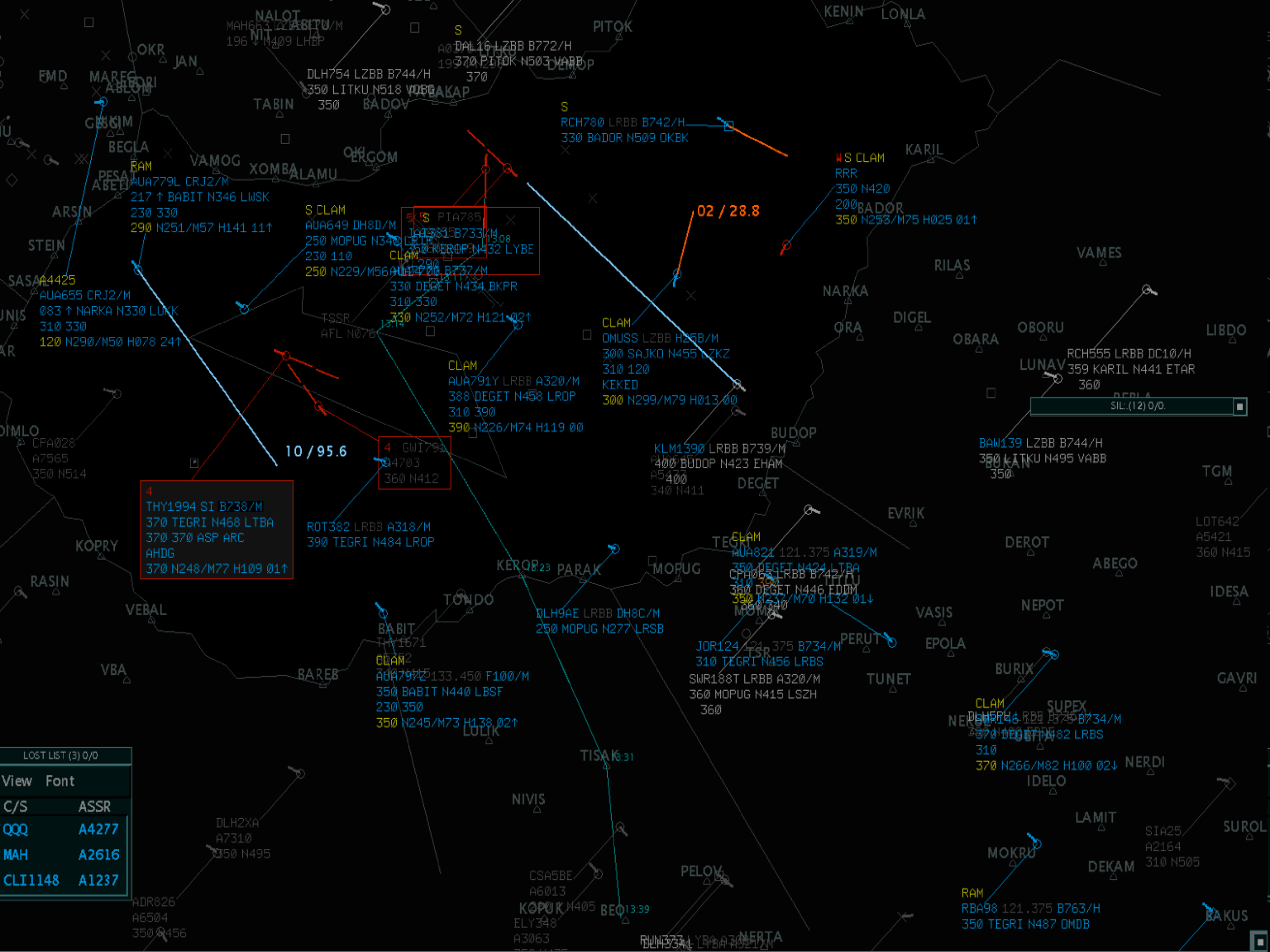
Belső IntraNet
telephely

IntraNet

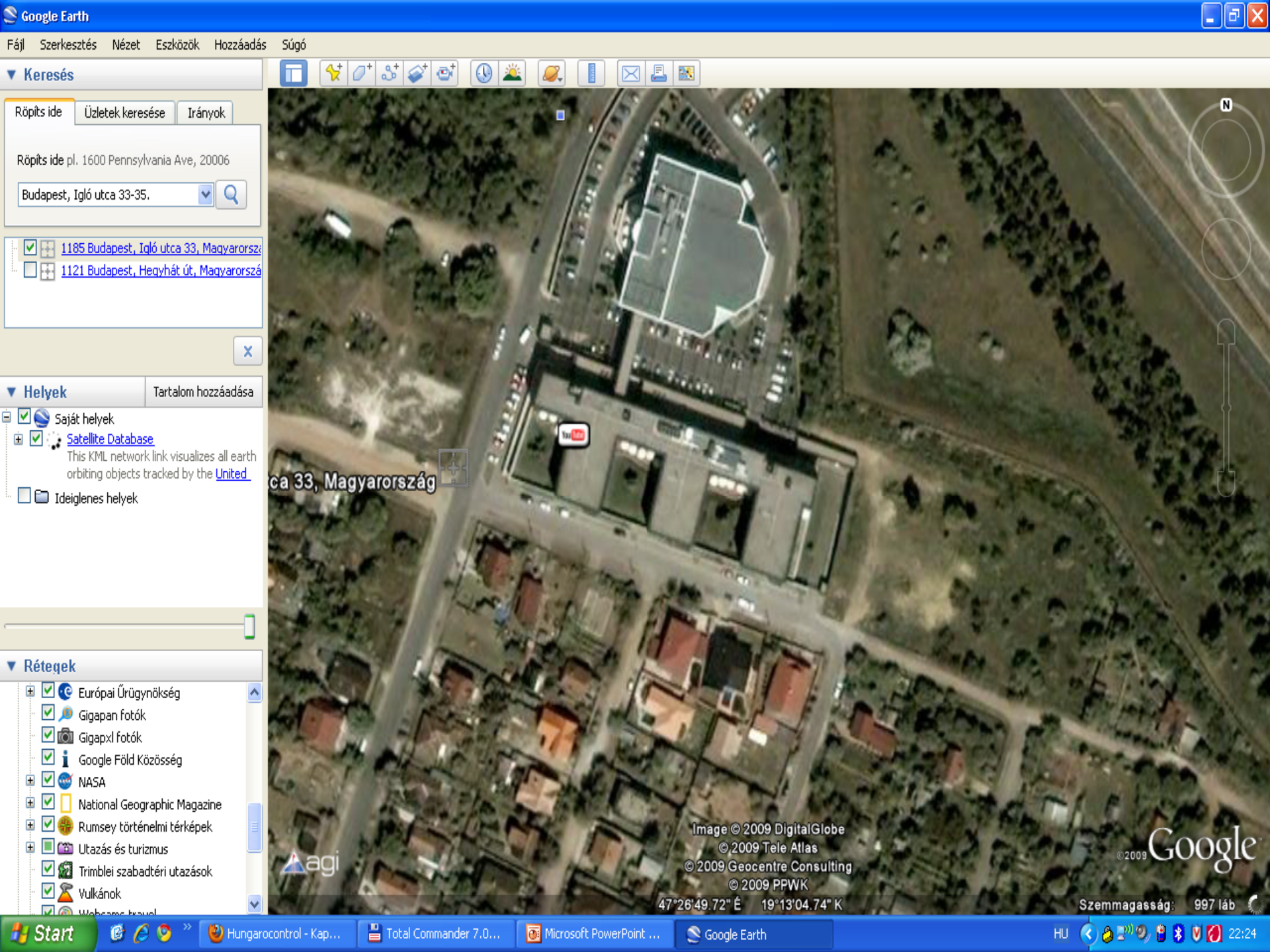
Célpont:

Légiirányítás

- MATIAS (Magyar Automated and Integrated Air Traffic System)
- Informatikailag jól védett
- Fizikailag? EMP ellen?



DAL16 LZBB B772/H
370 PITOK N503 VABB
DLH754 LZBB B744/H
350 LITKU N518 VOBG
350
RCH780 LRBB B742/H
330 BADOR N509 OKBK
RAM
AUA779L CRJ2/M
217 ↑ BABIT N346 LWSK
230 330
290 N251/M57 H141 11↑
S CLAM
AUA649 DH8D/M
250 MOPUG N348 LBWN
230 110
250 N229/M56 H127 01↑
A4425
AUA655 CRJ2/M
083 ↑ NARKA N330 LUKK
310 330
120 N290/M50 H078 24↑
02 / 28.8
W S CLAM
RRR
350 N420
200
350 N253/M75 H025 01↑
CLAM
OMUSS LZBB H25B/M
300 SAJKO N455 LZKZ
310 120
KEKED
300 N299/M79 H013 00
330 DEGET N434 BKPR
310 330
330 N252/M72 H121 02↑
CLAM
AUA791Y LRBB A320/M
388 DEGET N458 LROP
310 390
390 N226/M74 H119 00
10 / 95.6
4 GWI791
A4703
360 N412
4
THY1994 SI B738/M
370 TEGRI N468 LTBA
370 370 ASP ARC
AHDG
370 N248/M77 H109 01↑
ROT382 LRBB A318/M
390 TEGRI N484 LROP
RCH555 LRBB DC10/H
359 KARIL N441 ETAR
360
SIL:(12) 0/0.
BAW139 LZBB B744/H
350 LITKU N495 VABB
350
KLM1390 LRBB B739/M
400 BUDOP N423 EHAM
400
CLAM
AUA821 121.375 A319/M
350 DEGET N424 LTBA
CFH065 LRBB B742/H
360 DEGET N446 EDDM
DLH9AE LRBB DH8C/M
250 MOPUG N277 LRSB
JOR124 121.375 B734/M
310 TEGRI N456 LRBS
SWR188T LRBB A320/M
360 MOPUG N415 LSZH
360
CLAM
AUA797Z 133.450 F100/M
350 BABIT N440 LBSF
230 350
350 N245/M73 H138 02↑
CLAM
370 DEGET N482 LRBS
310
370 N266/M82 H100 02↓
RAM
RBA98 121.375 B763/H
350 TEGRI N487 OMDB
LOT642
A5421
360 N415
SIA25
A2164
310 N505
DLH2XA
A7310
350 N495
ADR826
A6504
350 N456
CSA5BE
A6013
CPA028
A7565
350 N514
LOST LIST (3) 0/0
View Font
C/S ASSR
QQQ A4277
MAH A2616
CLI1148 A1237
KENIN
LONLA
PITOK
NALOT
OKR
JAN
FMD
MAREG
TABIN
BADOV
BEGLA
VAMOG
XOMBA
ALAMU
ERGOM
KARIL
ARSIN
STEIN
BADOR
VAMES
RILAS
NARKA
DIGEL
ORA
OBORU
OBARA
LIBDO
LUNAV
BUDOP
DEGET
TGM
EVRIK
DEROT
ABEGO
IDESA
KOPRY
RASIN
VEBAL
TONDO
PARAK
MOPUG
VASIS
NEPOT
EPOLA
PERUT
TUNET
BURIX
GAVRI
VBA
BAREB
BABIT
LULIK
SUPEX
NERDI
IDELO
LAMIT
SUROL
TISAK
NIVIS
MOKRU
DEKAM
PELOV
KOPUK
BEO
NERTA
KAKUS


Google Earth
Fájl Szerkesztés Nézet Eszközök Hozzáadás Súgó
Keresés
Röpíts ide
Üzletek keresése
Irányok
Röpíts ide pl. 1600 Pennsylvania Ave, 20006
Budapest, Igló utca 33-35.
1185 Budapest, Igló utca 33, Magyarorsz
1121 Budapest, Hegyhát út, Magyarorszá
Helyek
Tartalom hozzáadása
Saját helyek
Satellite Database
This KML network link visualizes all earth orbiting objects tracked by the United
Ideiglenes helyek
Rétegek
Európai Űrügynökség
Gigapan fotók
Gigapxl fotók
Google Föld Közösség
NASA
National Geographic Magazine
Rumsey történelmi térképek
Utazás és turizmus
Trimblei szabadtéri utazások
Vulkánok
ca 33, Magyarország
N
Image © 2009 DigitalGlobe
© 2009 Tele Atlas
© 2009 Geocentre Consulting
© 2009 PPWK
47°26'49.72" É 19°13'04.74" K
Szemmagasság: 997 láb
agi
©2009 Google
Start
Hungarocontrol - Kap...
Total Commander 7.0...
Microsoft PowerPoint ...
Google Earth
HU
22:24

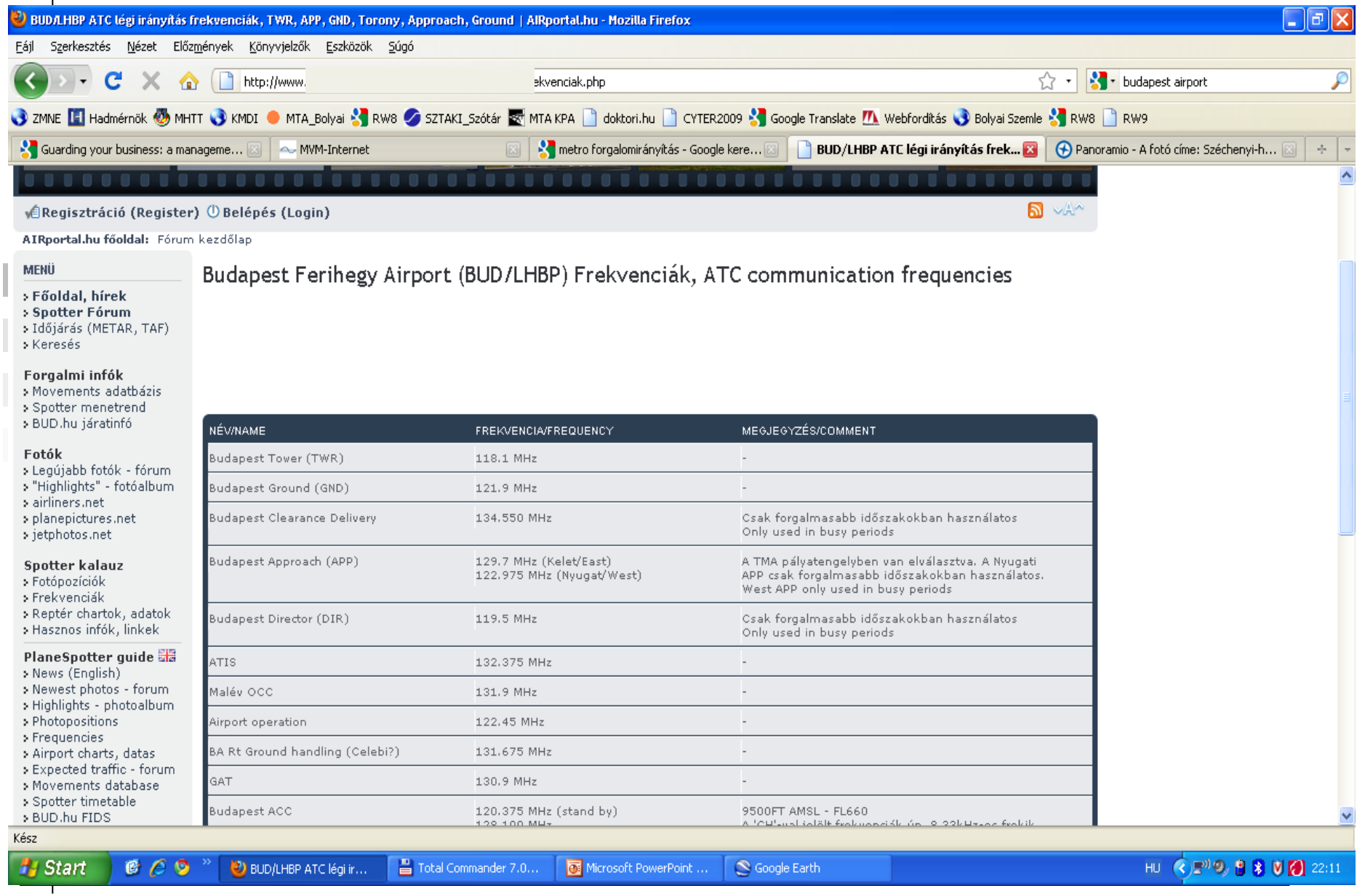
LÉGIKÖZLEKEDÉS

Célpont:

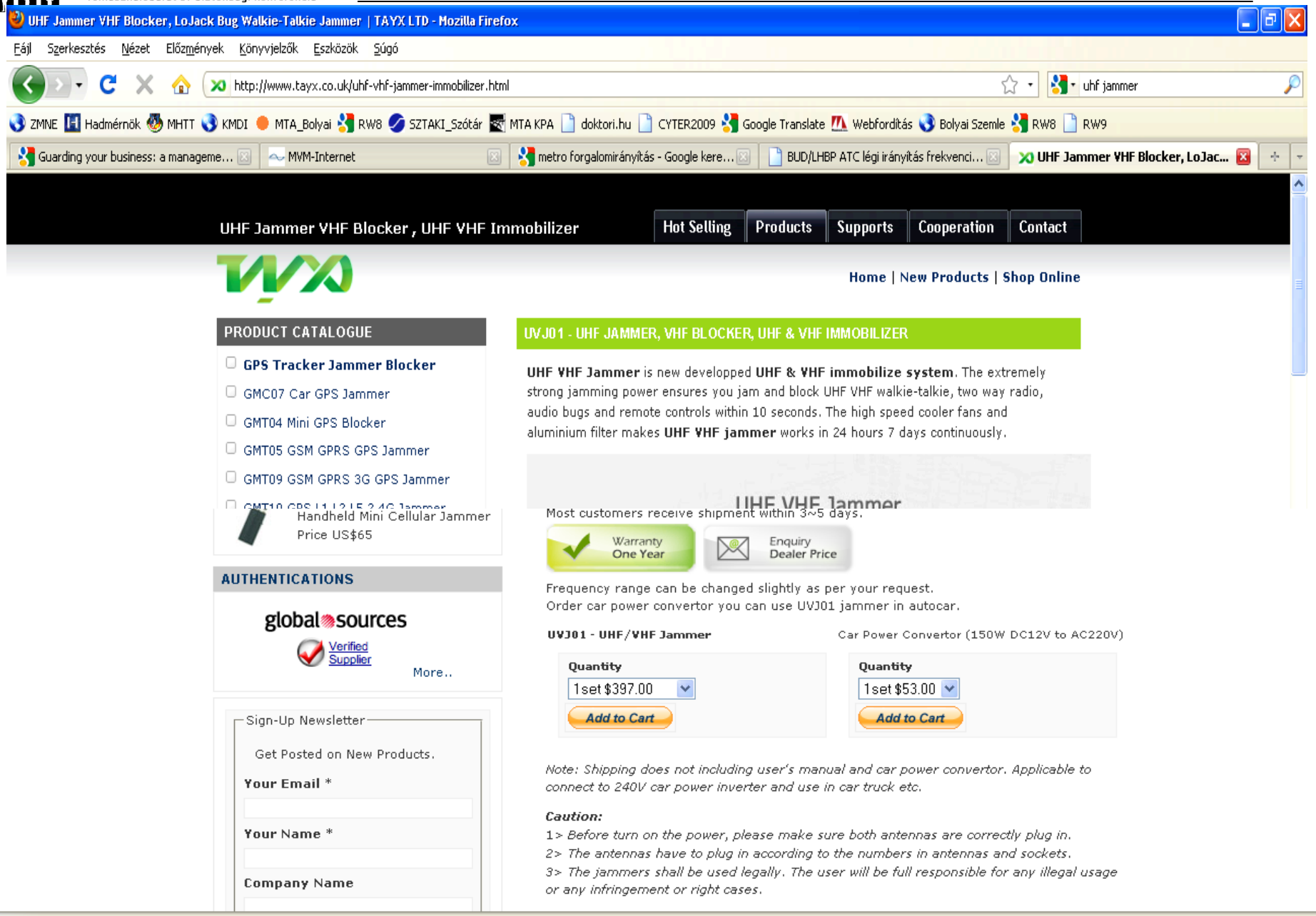
Repülőtér

- utas terminál tájékoztató informatikai rendszere
- chek-in informatikai rendszer (informatikai és social engineering),
- baggage rendszer

LÉGIKÖZLEKEDÉS



LÉGIKÖZLEKEDÉS



LÉGIKÖZLEKEDÉS

Célpont:

Légirányítás és Repülőtér

Hatás:

- Az európai légirányítás (EUROCONTROL) komoly terhelése
- Hazai légiközlekedés időszakos szünetelése

INTERNETES HÁLÓZATOK

- Ha nincs internet, nem működik a gazdaságunk.
- Az internet-szolgáltatók viszont elég jól felkészültek erre az eshetőségre.
- De zavart okozni attól még lehet! Mondjuk a forgalom lassításával! Erre kiváló célpont a BIX.
- 5 BIX csomópont, a központ a Victor Hugo utcában
- Elsősorban fizikai támadást lehet elképzelni

INTERNETES HÁLÓZATOK

- Példa: 2009. 01. 25. Autópálya-építők vágnak el egy gerincvezetéket, amitől túlterhelődött az Adatpark (-> éles helyzetben nem mindig működik a katasztrófaterv)
- A fél magyar internet órákra kiesett
- Az azért megnyugtató, hogy nem a teljes…
- Összehangolt, sorozatos támadásokkal ezek a zavarok napokig fenntarthatók lennének

KORMÁNYZATI INFORMATIKA

- Az internet-használat magyarországi elterjedésének egyik legfontosabb előremozdítója volt az elektronikus adóbevallás kötelezővé tétele
- Éppen ezért ha valamivel címlapra lehet kerülni, az az Ügyfélkapu elérhetetlensége adóbevallási időszakban
- Márpedig bevallási időszak minden hónapban többször is van.
- Az államba vetett bizalom (?) megingatásának egyik leghatékonyabb módja a kormányzati oldalak támadása -> láttuk, hogy békeidőben ez milyen eredménnyel járhat, gondoljuk el ezt egy puskaporos hangulatban!

KORMÁNYZATI INFORMATIKA

- Persze vannak további példák: OEP, ÁFSZ…
- Az EKG bevezetésével olyan centralizált közigazgatási hálózat jött/jön létre, mely akár a legkisebb faluból is hozzáférhető.
- Gyaníthatóan már most célpontnak tekintik ezt a hálózatot.
- Sikeres támadás esetén nem csak adót bevallani nem tudunk, de lényegében a teljes közigazgatás működése megbénulhat minden szinten!

EGÉSZSÉGBIZTOSÍTÁS, SZOCIÁLIS ELLÁTÁS

Célpont:

Egészségügyi informatikai rendszerek

- Sem fizikailag sem informatikailag nem megfelelően védettek

Hatás:

- TB jogosultság ellenőrzésének lehetetlenné válása
- Komoly időveszteség a gyógyszerszállításban
- …
- …

avagy a teljes káosz elérése

- Kell-e az atomerőműve(ke)t támadni?
- Nem! (Fizikailag jól védettek, informatikailag nem lehetséges a ‘komoly’ beavatkozás)

Célpont:

Villamosenergia-ipari rendszerirányítás

Hogyan:

- Informatika -> nehéz ügy, de: SCADA?
- Social engineering
- EMP
- Fizikai támadás

MAVIR Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR ZRt.) - Főoldal - Mozilla Firefox

Fájl Szerkesztés Nézet Előzmények Könyvjelzők Eszközök Súgó

http://portal.mavir.hu/portal/page/portal/Mavir

ZMNE Hadmérnök MHTT KMDI MTA_Bolyai RW8 SZTAKI_Szótár MTA KPA doktori.hu CYTER2009 Google Translate Webfordítás Bolyai Szemle

MAVIR Magyar Villamosenergia-ipari...

MAVIR

60 ÉVES A RENDSZERIRÁNYÍTÁS 1949 - 2009

keresés OK

Részletes keresés »

Magunkról | Hivatalos | Szakmai | Adatpublikáció | Hasznos | Sajtó | Karrier

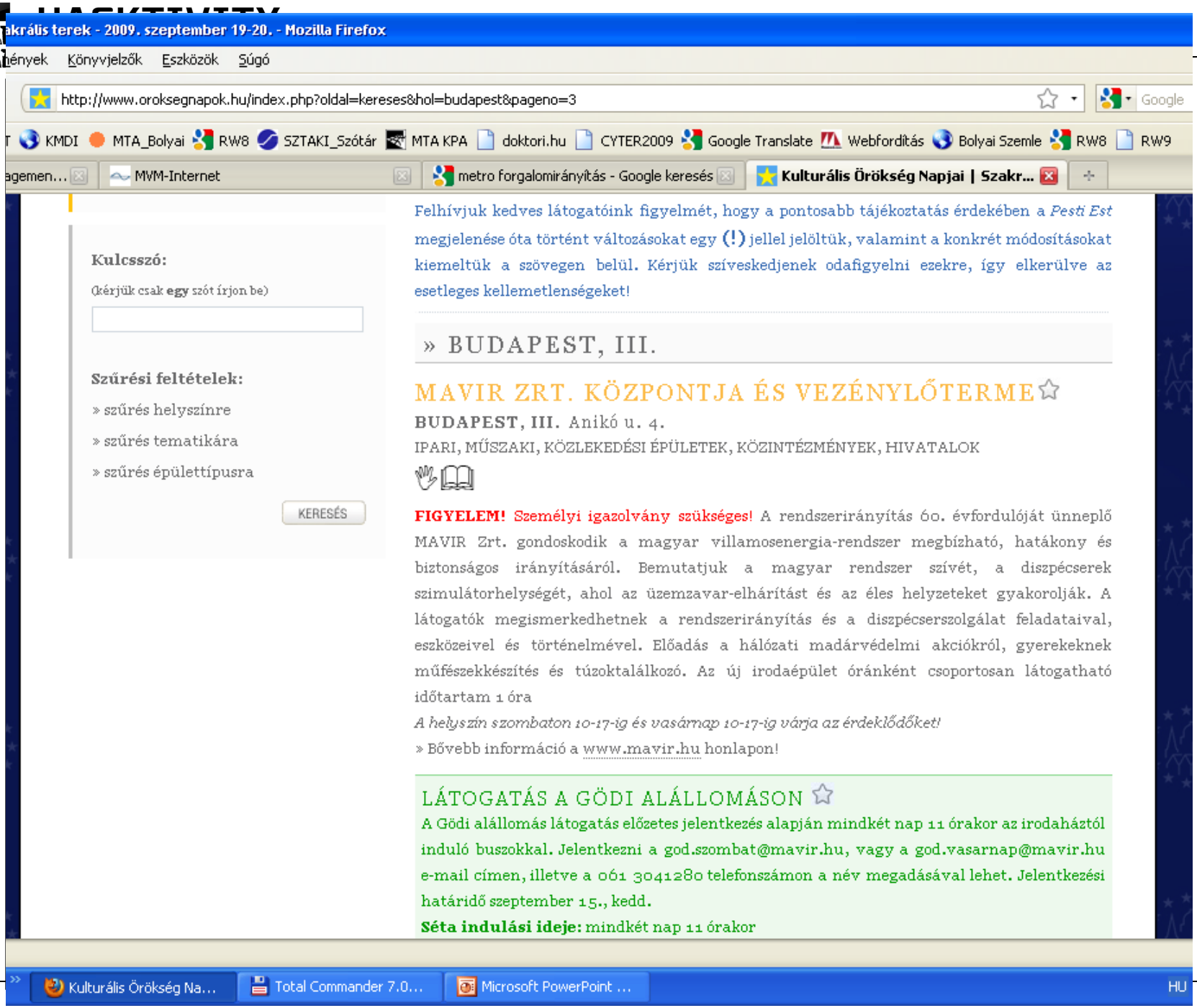
Kedves Látogató!

Üdvözöljük a MAVIR megújult honlapján! Reméljük, hogy a korszerűbb és biztonságosabb felület megkönnyíti majd a közhasznú információk elérését és a mindennapi szakmai együttműködést egyaránt. Partnereink valamennyi szolgáltatásunkat hasonló szerkezetben, esetleg más cím alatt találják. Hogy az átmenet minél kevesebb fennakadást okozzon, 2009. október 15-éig a régi honlap elérhetőségét is biztosítjuk. A régi honlapot itt érheti el:
regi.mavir.hu

Az aktuális, legfrissebb információkat azonban már csak az új honlapon publikáljuk!
Kérdéseit, észrevételeit az alábbi felületen várjuk:
info@mavir.hu

Bízunk benne, hogy az új honlap is könnyen kezelhető oldalakkal támogatja partnereink munkáját és hasznos információkat nyújt az

Kész


akrális terek - 2009. szeptember 19-20. - Mozilla Firefox
ények Könyvjelzők Eszközök Súgó
http://www.oroksegnapok.hu/index.php?oldal=kereses&hol=budapest&pageno=3
Google
KMDI MTA_Bolyai RW8 SZTAKI_Szótár MTA KPA doktori.hu CYTER2009 Google Translate Webfordítás Bolyai Szemle RW8 RW9
agemen... MVM-Internet metro forgalomirányítás - Google keresés Kulturális Örökség Napjai | Szakr...
Kulcsszó:
(kérjük csak egy szót írjon be)
Szűrési feltételek:
» szűrés helyszínre
» szűrés tematikára
» szűrés épülettípusra
KERESÉS
Felhívjuk kedves látogatóink figyelmét, hogy a pontosabb tájékoztatás érdekében a Pesti Est megjelenése óta történt változásokat egy (!) jellel jelöltük, valamint a konkrét módosításokat kiemeltük a szövegen belül. Kérjük szíveskedjenek odafigyelni ezekre, így elkerülve az esetleges kellemetlenségeket!
» BUDAPEST, III.
MAVIR ZRT. KÖZPONTJA ÉS VEZÉNYLŐTERME
BUDAPEST, III. Anikó u. 4.
IPARI, MŰSZAKI, KÖZLEKEDÉSI ÉPÜLETEK, KÖZINTÉZMÉNYEK, HIVATALOK
FIGYELEM! Személyi igazolvány szükséges! A rendszerirányítás 60. évfordulóját ünneplő MAVIR Zrt. gondoskodik a magyar villamosenergia-rendszer megbízható, hatákony és biztonságos irányításáról. Bemutatjuk a magyar rendszer szívét, a diszpécserek szimulátorhelységét, ahol az üzemzavar-elhárítást és az éles helyzeteket gyakorolják. A látogatók megismerkedhetnek a rendszerirányítás és a diszpécserszolgálat feladataival, eszközeivel és történelmével. Előadás a hálózati madárvédelmi akciókról, gyerekeknek műfészekkészítés és túzoktalálkozó. Az új irodaépület óránként csoportosan látogatható időtartam 1 óra
A helyszín szombaton 10-17-ig és vasárnap 10-17-ig várja az érdeklődőket!
» Bővebb információ a www.mavir.hu honlapon!
LÁTOGATÁS A GÖDI ALÁLLOMÁSON
A Gödi alállomás látogatás előzetes jelentkezés alapján mindkét nap 11 órakor az irodaháztól induló buszokkal. Jelentkezni a god.szombat@mavir.hu, vagy a god.vasarnap@mavir.hu e-mail címen, illetve a 061 3041280 telefonszámon a név megadásával lehet. Jelentkezési határidő szeptember 15., kedd.
Séta indulási ideje: mindkét nap 11 órakor
Kulturális Örökség Na... Total Commander 7.0... Microsoft PowerPoint ...
HU

Súgó

2440 Százhalombatta, Erőmű út 2, Magyarország

Vasút utca

Kerékpárút

© 2009 PPWK
© 2009 Tele Atlas
© 2009 Cnes/Spot Image
Image © 2009 DigitalGlobe
47°19'25.35" É 18°55'19.23" K

Google

Szemmagasság: 3263 láb

Súgó

75%

Keresés

A MAVIR Rt. informatikai stratégiája

Minden vállalat alapvető érdeke, hogy rendelkezzen a vállalat távlati céljait kiszolgáló informatikai stratégiával. A MAVIR Rt. esetében a stratégia elkészítését az önálló vállalatként történő működés, és a piacnyitásból következő jelentős fejlesztési igények összehangolása indokolta. Az elkészítést nehezítette, hogy ma még a piaci szereplők hosszú távú működési modellje, stratégiája kidolgozás alatt van, a villamosenergia-törvénytől függően a jövőben jelentősen változhat. Ebből következően valószínű, hogy a MAVIR Rt. informatikai stratégiáját is több területen pontosítani, módosítani kell majd.

Az MVM Rt. 2001. január 1. dátummal létrehozta a Magyar Villamosenergia-ipari Rendszerirányító Rt.-t. Jelenlegi feladata alapjaiban megegyezik a korábban az MVM Rt. igazgatóságaként működő Országos Villamos Teherelosztó feladataival.

A magyar villamosenergia-rendszer operatív irányítását végzi és ellátja mindazon feladatokat, amelyek szorosan kapcsolódnak ehhez a tevékenységhez (üzem-előkészítés, nemzetközi villamosenergia-elszámolás stb.). Azonban rövid időn belül jelentős változások, bővülések várhatóak a MAVIR Rt. feladataiban. Bár még nem jelent meg az új energiatörvény, amely pontosan szabályozná a MAVIR Rt. feladatait, így az új

nan létesítendő részek munkáit a célok figyelembe vételével, azokkal összhangban kell végezni azért, hogy a változásoknak rugalmas keretet adó, az informatikai eszközök gyors fejlődéseinek eredményeit alkalmazó rendszert lehessen

dani. A megvalósításhoz egy szorosan összefüggő feltételrendszernek eleget téve kell tevékenykedni. Valamennyi feladat a MAVIR-nak a törvényben (VET) előírt kötelezettségeiből és hatásköreiből, valamint a működési környezet ezt követő szabályozásaiból származik.

Fontos hangsúlyozni, hogy bár a MAVIR önálló vállalatként történő megalapítását a villamosenergia-piac nyitásának előkészítése indokolta, a MAVIR feladatainak nagy részét bármilyen piacgazdasági modellben el kellene látnia.

A különbség az egyes funkciók terjedelmében és időbeliségében van. Más szavakkal: a MAVIR informatikai stratégi-

avagy a teljes káosz elérése

- Kell-e az atomerőműve(ke)t támadni?
- Nem! (Fizikailag jól védettek, informatikailag nem lehetséges a ‘komoly’ beavatkozás)

Célpont:

Villamosenergia-ipari rendszerirányítás

Hatás:

- *Klasszikus:* **Ha nincs villany semmi sincs!**
- **100-120 évvel korábbi állapotokra veti vissza – akár hetekre – a társadalom működését a kiesés!**
- **Komoly regionális, és európai ellátási kiesések!**

A FENYEGETÉS MÉRTÉKE

- Független csapatokok, hacktivisták esélye nagy (ld. szlovák-magyar viszony), de hatása kicsi. Erre lehet az észt-orosz a példa
- Államok közötti kémkedés, esélye nagy, hatása nagy (USA-Kína)
- Államok közötti csetepaté, esélye kicsi, hatása óriási (orosz-grúz)

A HACKER KÖZÖSSÉG SZEREPE

- Úgy tudjuk, hogy a hackerek véleményét sosem kérdezték meg a nemzeti kibervédelemről
- Pedig ez a közösség lehet a legfőbb humán erőforrás az állami és a magánszervezetek védelméhez
- Éppen ezért szerettük volna megtudni, mit gondoltok TI a nemzetvédelemről
- A kérdőívet a Hacktivity weboldalán publikáltuk és 600 e-mail címre küldtük ki hírlevélben
- A címzettek majdnem 20%-a válaszolt (187 válaszadó)!

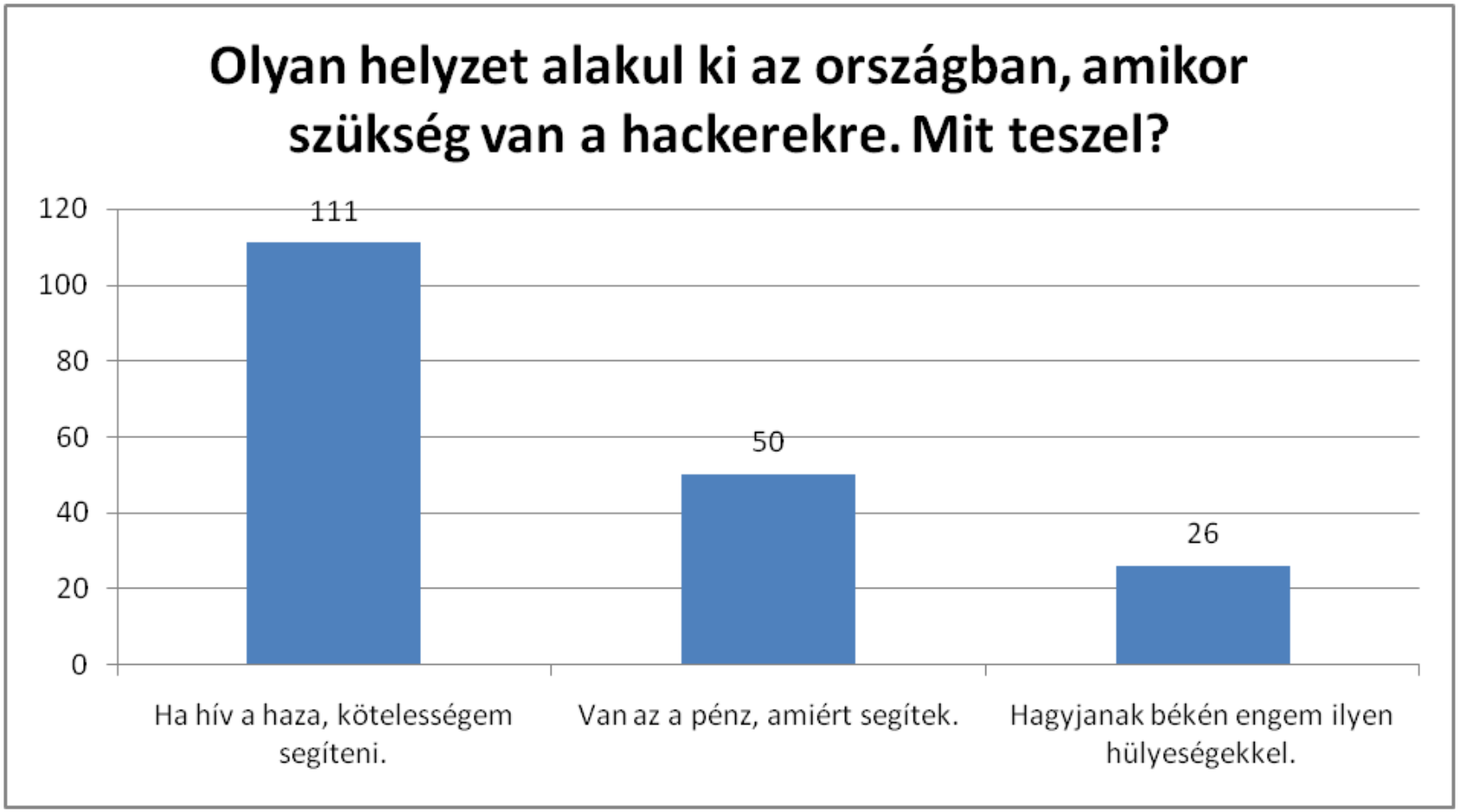
KÉRDŐÍV

- **4 kérdés:**
  - Olyan helyzet alakul ki az országban, amikor szükség van a hackerekre. Mit teszel?
  - Az IT biztonság melyik motivációját érzed leginkább magadénak?
  - Hova sorolnád be magadat?
  - Mi a véleményed a Magyar Honvédségről?
- **Mérni szerettük volna:**
  - A hazafiság mértékét
  - A hackerek szerepét a nemzetvédelemben
  - Helyüket a piacon
  - A Honvédségről alkotott őszinte véleményüket

A HAZAFISÁG FOKA

- **3 lehetséges válasz:**
  - Ha hív a haza, kötelességem segíteni.
  - Van az a pénz, amiért segítek.
  - Hagyjanak békén engem ilyen hülyeségekkel.
- **Előzetes feltételezés:**
  - A legtöbb válaszadó szereti az országát és ingyen segítene

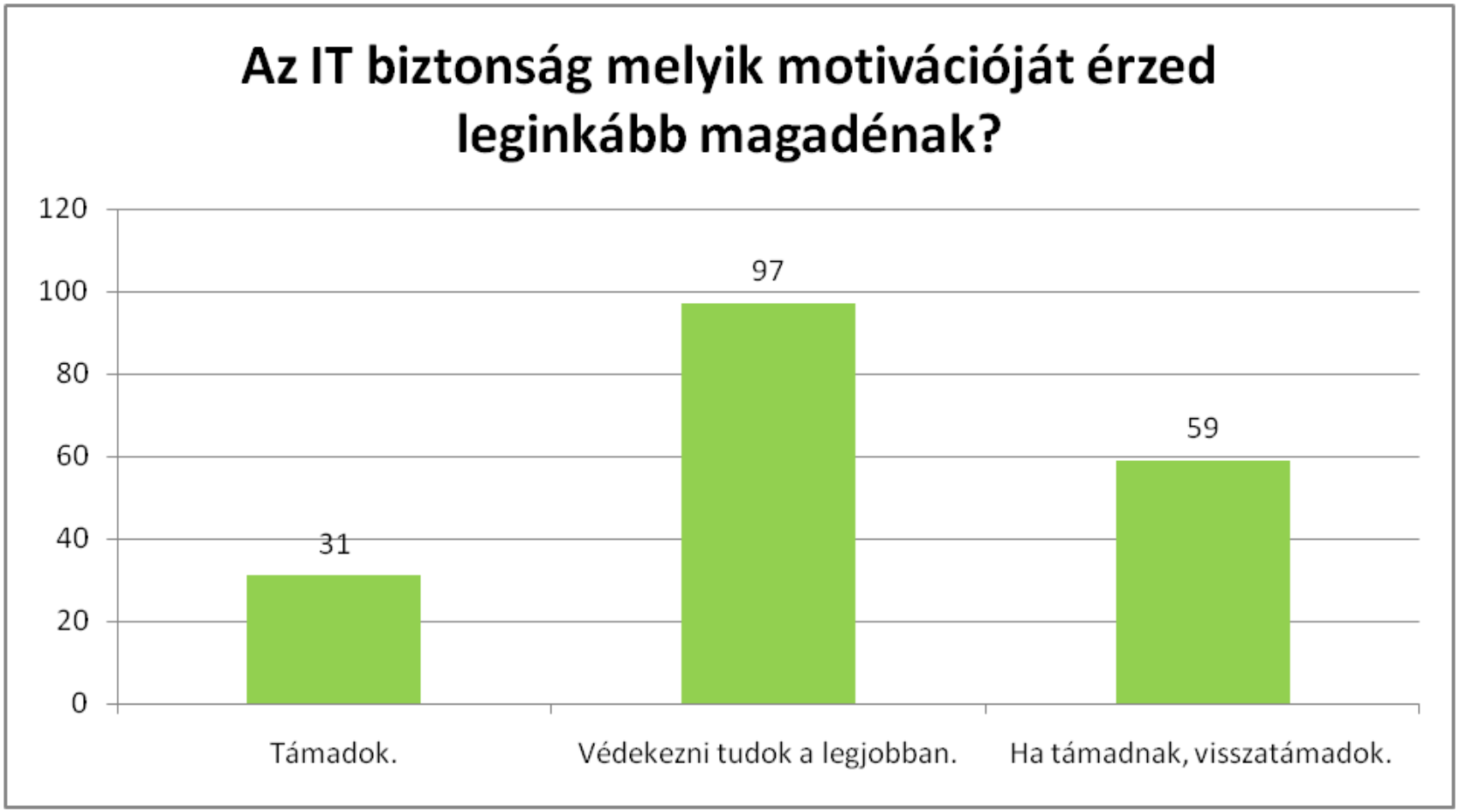
A HAZAFISÁG FOKA



TÁMADNI VAGY VÉDEKEZNI?

- A kibervédelem a megfelelő állami szervek feladata, nem a hackereké
- A hackerek viszont jól tudnak támadni vagy támadást szimulálni, esetleg külső támadás esetén visszavágni
- **3 lehetséges válasz:**
  - Támadok.
  - Védekezni tudok a legjobban.
  - Ha támadnak, visszatámadok.
- **Előzetes feltételezés:**
  - A válaszadók többsége támadni akar

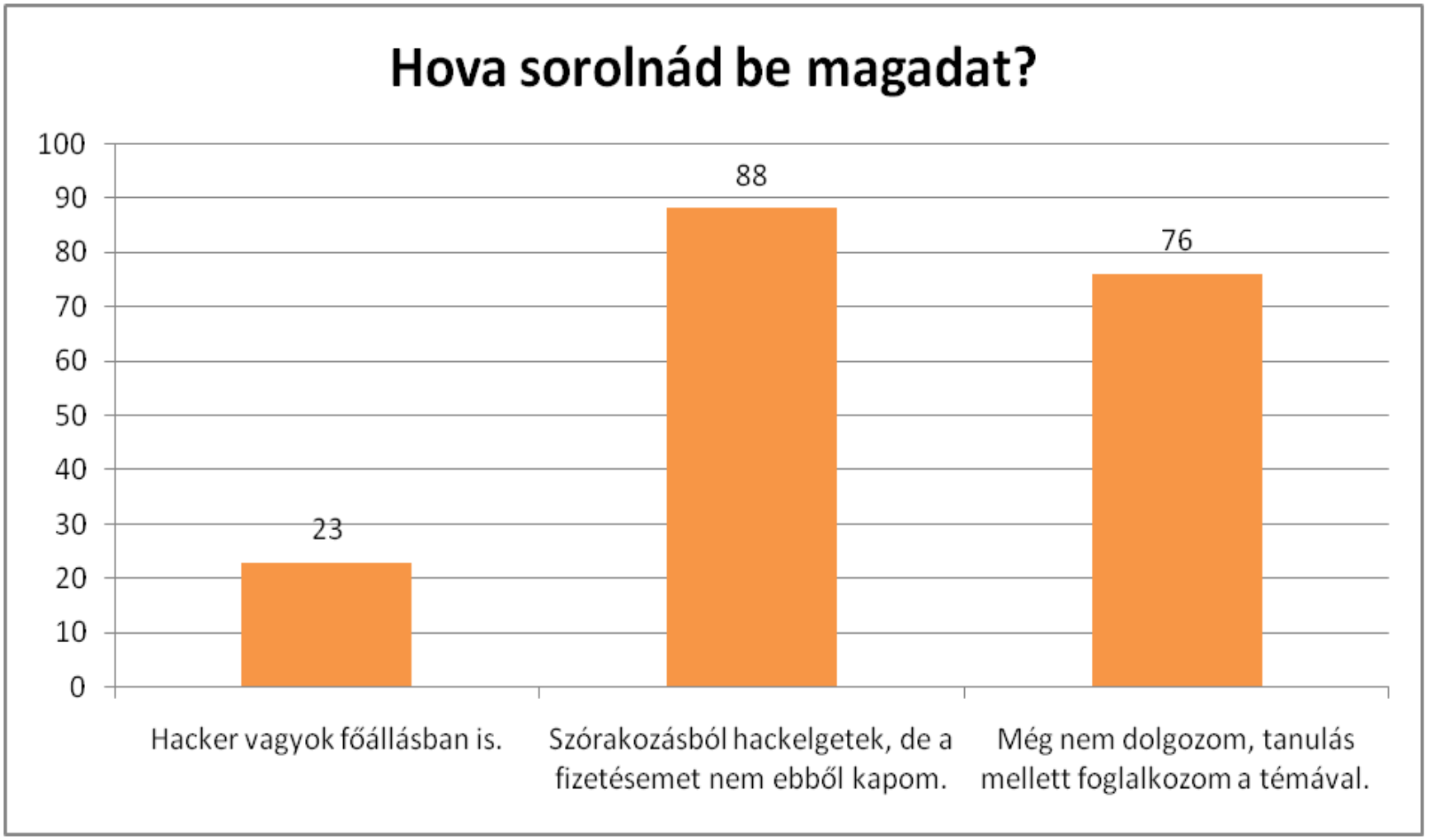
TÁMADNI VAGY VÉDEKEZNI?



JELENLEGI POZÍCIÓ

- Az országban van néhány hivatásos etikus hacker, akik alapját képezhetik egy „kiberszázadnak”.
- Van rengeteg diákunk, akik egyszer talán hivatásos etikus hackerek lehetnek
- És van sok olyan informatikusunk, akiknek ez az egész hobbi, a kenyerüket mással keresik
- 3 lehetséges válasz:
  - Hacker vagyok főállásban is.
  - Szórakozásból hackelgetek, de a fizetésemet nem ebből kapom.
  - Még nem dolgozom, tanulás mellett foglalkozom a témával.
- Előzetes feltételezés:
  - Nincsen sok etikus hackerünk, de nagyon erős az egyetemi háttér

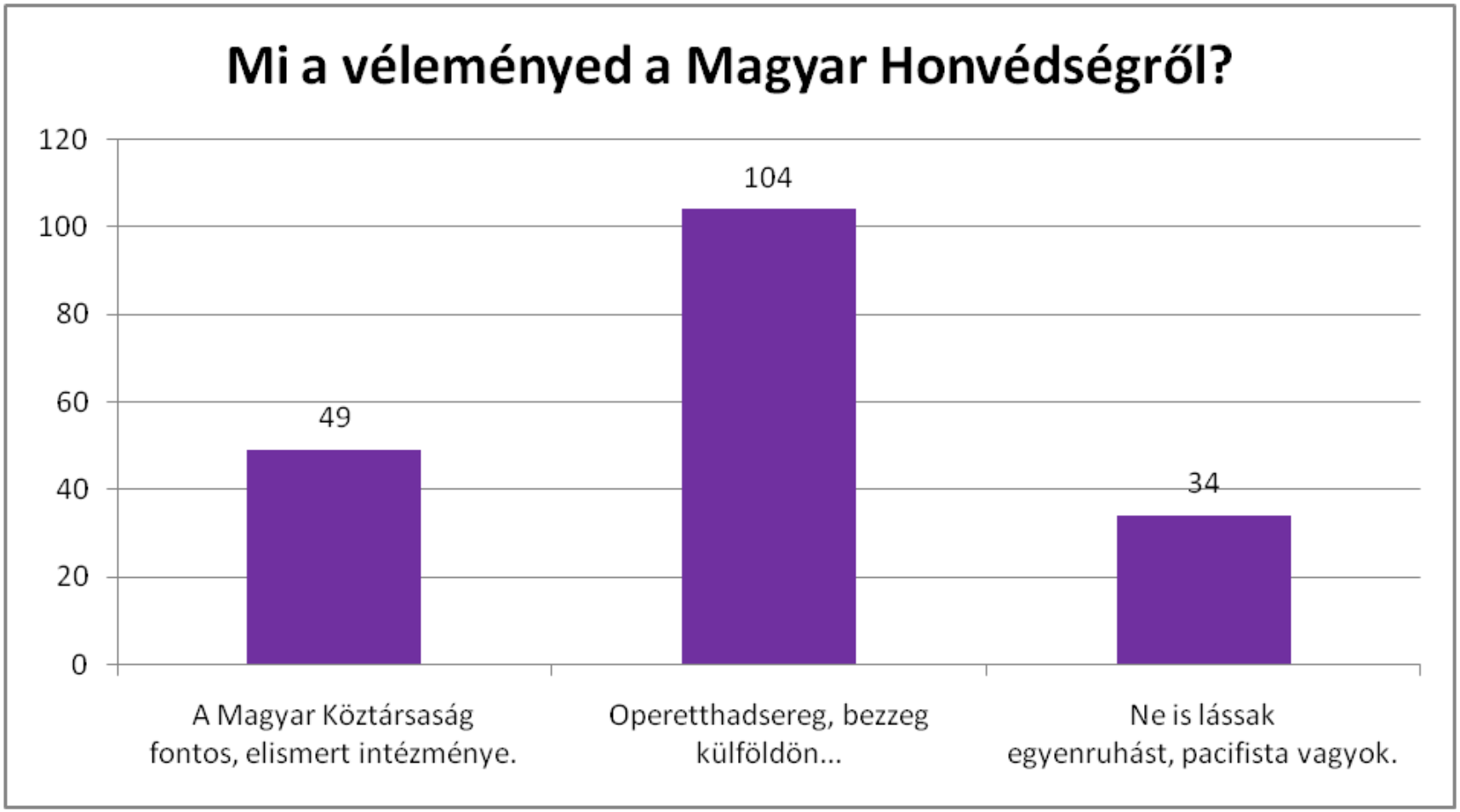
JELENLEGI POZÍCIÓ



VÉLEMÉNY A HONVÉDSÉGRŐL

- Amennyiben a Honvédség (vagy más szerv) együtt szeretne működni a hacker közösséggel, pozitív képet kell kiépítenie
- 3 lehetséges válasz:
  - A Magyar Köztársaság fontos, elismert intézménye.
  - Operetthadsereg, bezzeg külföldön...
  - Ne is lássak egyenruhást, pacifista vagyok.
- Előzetes feltételezés:
  - A válaszadók többsége nem pacifista, de meglehetősen negatív képe van a Magyar Honvédségről

VÉLEMÉNY A HONVÉDSÉGRŐL



MEGÁLLAPÍTÁSOK

- A hacker közösség szereti az országot és kész megvédeni a maga eszközeivel
- A válaszadók fele kész támadni vagy visszatámadni
- Magyarországon van néhány hivatásos hacker, és hatalmas utánpótlás az egyetemeken
- A Magyar Honvédségnek sokkal pozitívabb képet kell kialakítania, ha ezen a területen elfogadják a javaslatainkat

ÉRDEKES ÖSSZEFÜGGÉSEK

- A hivatásos hackerek fele pénzért, másik felük ingyen segítene
- Az etikus hackereknek nincs jó véleményük a Magyar Honvédségről
- A hobbihackereknek van a legjobb benyomásuk a Honvédségről
- A hazafiak nem pacifisták
- A hobbihackerek készen állnak támadni és visszatámadni
- A diákok hazafiak és nem pacifisták

ZÁRÓ GONDOLATOK

- Ha mi lennénk az illetékes hivatalnokok:
  - Aktívan részt vennék a hacker konferenciákon
  - Pozitív képet építenénk a Honvédségről
  - Támogatást szereznénk egy kiber-hadgyakorlathoz
  - Ebbe bevonnánk a hazafias hackereket is
  - Megijednénk az eredményétől, és azonnal elkezdenénk a szükséges jogalkotást és koordinációt

VÉDELMI LEHETŐSÉGEK

- **USA:**
  - Obama's New Cybersecurity policy: rövid és középtávú – a veszélyek és a fenyegetések alapján összeállított reális – védelmi tervek
  - Cybersecurity Czar is WANTED!: olyan aki hatékonyan tud koordinálni, és van is jogköre…
  - Cybercommand -> NSA (CIIP)
  - Cybercommand -> DoD (megelőző cybercsapás is!)

- **Németország:**
  Bundeswehr Kommando Strategische Aufklärung (KdoStratAufkl)

- **NATO:**
  NATO Cyber Defence Centre of Excellence (Tallin)

MAGYAR LÉPÉSEK

- Merre tovább Magyarország?
- Nem vagyunk lemaradva! **De!**
- **Probléma:** sok bába között elvész a gyerek: NGFM, IRM, OKF, CERT? Ki a valódi koordinátor? Kell-e egy esetleges csúcsszerv?
- **Eddigi lépések:**
  - 2080/2008. Korm. határozat
  - CERT-ek
  - MTA és egyetemi kutatások, doktori értekezések
  - Informatikai biztonság oktatása, tudatos internet használat
  - KII védelmi törekvések, konferenciák -> Hacktivity 2009

KÖSZÖNJÜK A FIGYELMET!

Dr. KOVÁCS LÁSZLÓ
Zrínyi Miklós Nemzetvédelmi Egyetem
egyetemi docens
kovacs.laszlo@zmne.hu

KRASZNAY CSABA
Zrínyi Miklós Nemzetvédelmi Egyetem
doktorandusz hallgató
csaba@krasznay.hu