NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

KIBERHADVISELÉS MAGYARORSZÁGON

Készítette: Kovács László
Budapest, 2015. március 24.

TARTALOM

- Kibertér és kiberfüggőség
- Az első kiberháború története
- Kritikus információs infrastruktúrák
- Kiberhadviselés alapjai
- Kibertámadók és eszközeik
- A kibertér védelme

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Kibertér

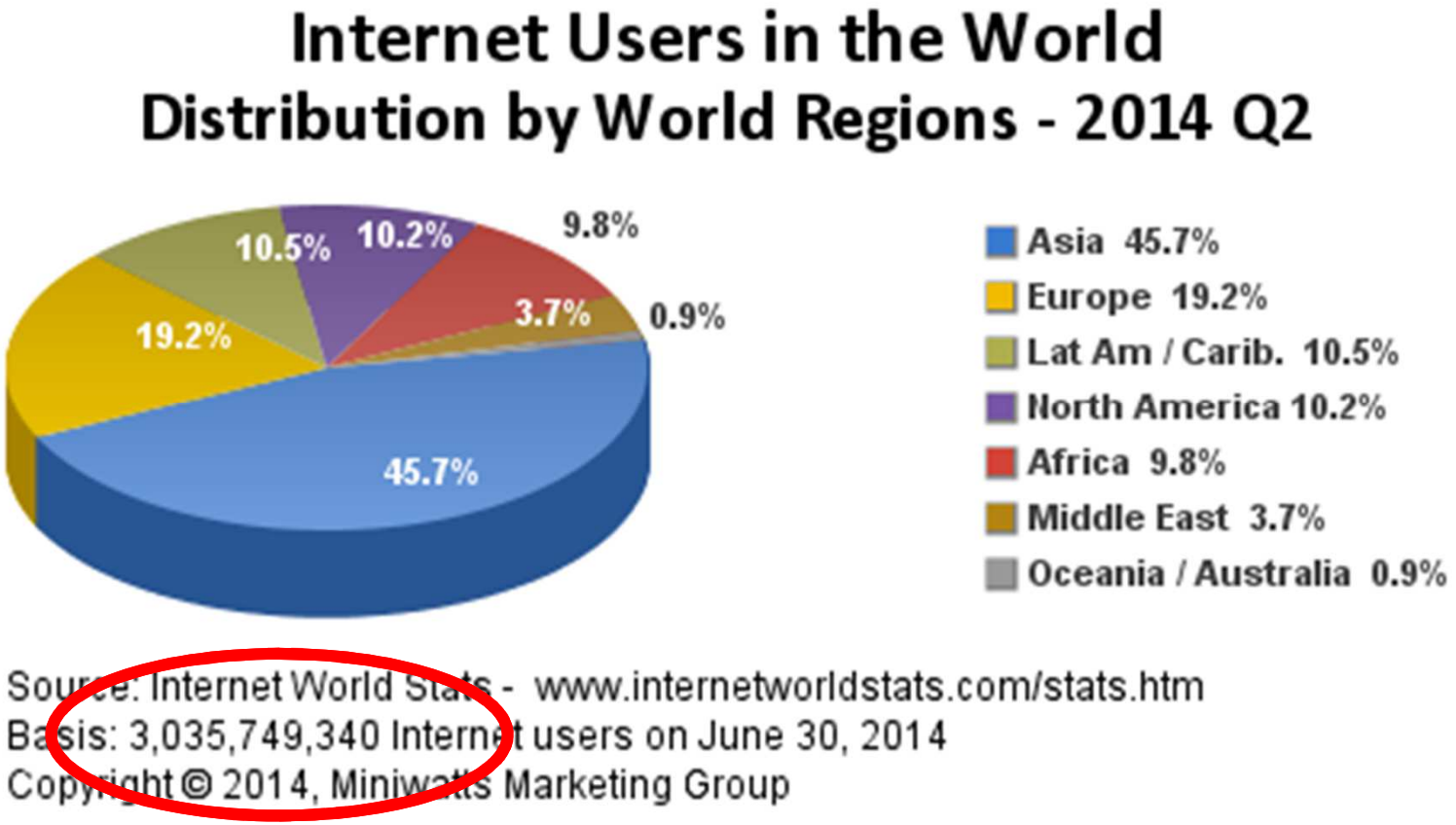
Kibertér = Internet

- vagy ennél azért több?

Kibertér

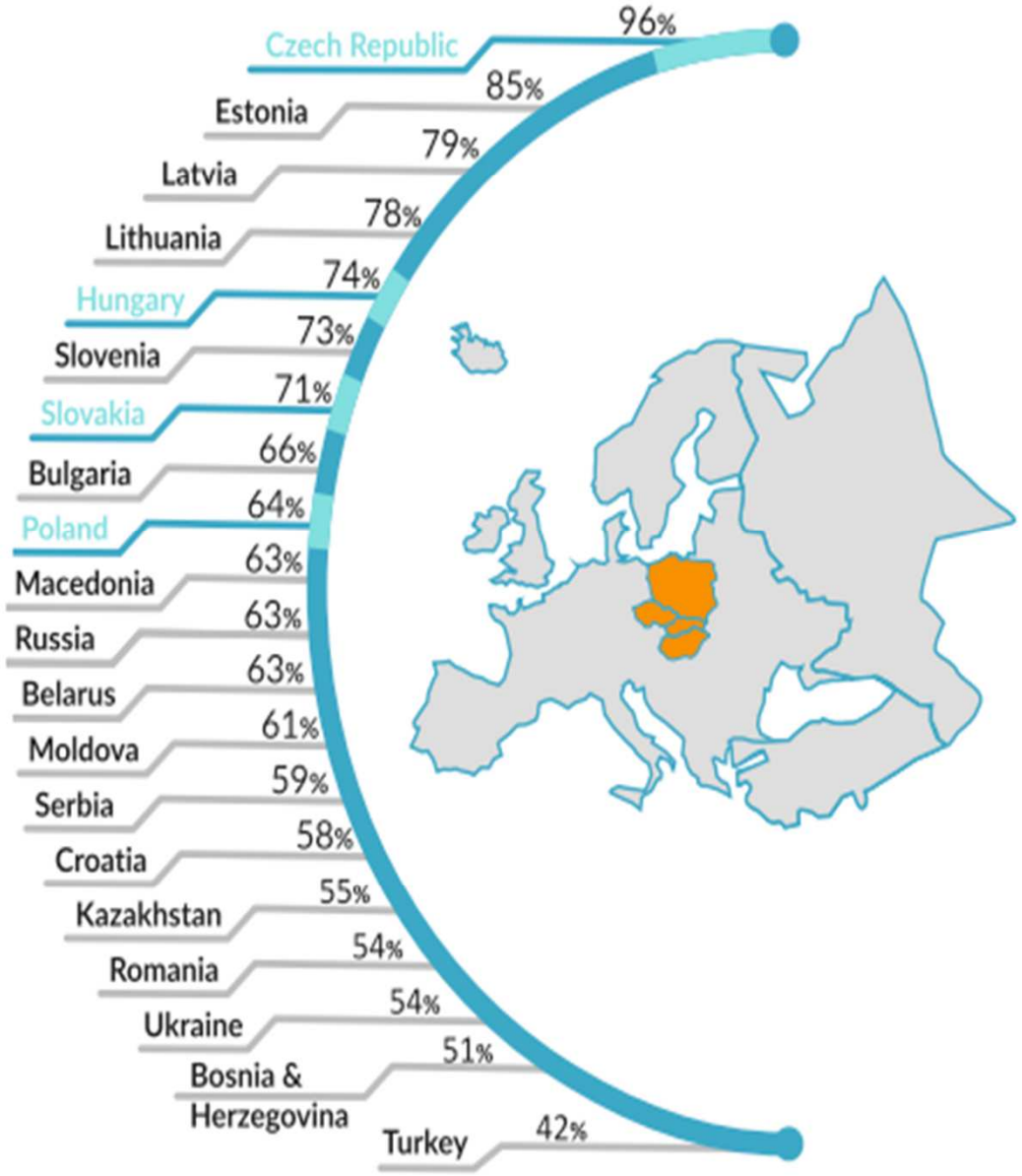
- Ez is a kibertér:
  - digitális gazdaság
  - e-kereskedelem
  - e-kormányzás
  - e-tervezés
  - logisztika
  - autógyártás
  - gyógyszergyártás

Kiberfüggőség



Készítette: Kovács László
Budapest, 2015. március 24.

Chart 1. Internet penetration in the CEE region (age:18-69)[1]



Source: BY: National Statistical Committee of the Republic of Belarus; BA: Valicon; BG: IPSOS, HR: CBS AXA; CZ: NetMonitor – SPIR – Gemius and Mediaresearch ; EE: TURU-UURINGUTE AS research; HU: Gemius/Ipsos; LV: SKDS; LT: RAIT; MK: TNS BRIMA Gallup Intl.; MD: CBS AXA; PL: Net Track Millward Brown SMG/KRC; RU: FOM; RO: Merkury 360; RS: IPSOS; SK: AIMmonitor – IAB Slovakia - Gemius and Mediaresearch; SI: Valicon; TR: Ipsos; UA: GFK, KZ: GFK, XII.2013

Az első kiberháború története

2007. április: Észtország fővárosában, a tallinni szovjet hősi emlékmű eltávolítása miatt tüntetések és zavargások.

2007. április 26-27: az első túlterheléses támadások. A parlament, az elnök és a miniszterelnök rendszereit és oldalait is érik támadások

2007. április 30.: számos napilap online kiadását éri támadás. További DDoS támadások bankok és telefontársaságok ellen. Deface támadások.

Készítette: Kovács László
Budapest, 2015. március 24.

Az első kiberháború története

2007. május 2.: ISP-k segítségével sikerül az elsősorban orosz szerverekről érkező támadásokat elhárítani IP cím blokkolással

2007. május 5.: az észt rendőrség őrizetbe vesz egy 19 éves észt fiatalt, akit a támadásokban való részvétellel gyanúsítanak. Észt hivatalos források Oroszországot teszik felelőssé a támadás miatt.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Az első kiberháború története

Adatok:

- 128 DDoS támadás
- 2-10 órás időtartamú egy-egy támadás
- 100 Mbps sávszélességet is elérte a legsúlyosabb támadás (óriási zombi hálózatot feltételez)
- a hálózati adatforgalom esetenként a normális ezerszerese volt
- parlament 4 napig internet nélkül volt
- 24 órát meghaladó ideig nem vagy csak részleges banki szolgáltatások
- média és telekommunikációs cégek részleges működésképtelensége …

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Az első kiberháború története

1. Kérdés: Észtország NATO tagállam.

NATO alapokmány 5. cikkely:

„A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett **fegyveres támadást** valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben, azonnal megteszi azokat az intézkedéseket - **ideértve a fegyveres erő alkalmazását** is , amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart.”

Az Észak-atlanti Szerződés Alapokmánya
Washington DC, 1949. április 4.

Az első kiberháború története

NATO Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról, 2010. Lisszabon:

4. a. Kollektív védelem.
„A NATO tagállamok mindig segítséget nyújtanak egymásnak egy esetleges **támadással** szemben, a Washingtoni Szerződés V. cikkelyével összhangban. Ez az elkötelezettség szilárd és kötelező erejű marad. A NATO elrettent és megvéd minden agresszióval való fenyegetéssel és felmerülő biztonsági kihívással szemben, amelyek az egyes szövetségesek vagy a Szövetség egészének alapvető biztonságát fenyegetik.”

12. A kibertámadások egyre gyakoribbá, szervezettebbé és a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okozóvá válnak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti. Külföldi haderők és titkosszolgálatok, szervezett bűnözők, terrorista és/vagy szélsőséges csoportok egyaránt lehetnek egy ilyen támadás végrehajtói.

Az első kiberháború története

2. Kérdés: Ki a támadó?

3. Kérdés: Mi a támadás módja?

4. Kérdés: Milyen bizonyítékok vannak a támadásra, valamint a támadókra (IT Forensic – digitális nyom)

5. kérdés: Milyen válaszakciók lehetségesek? (diplomáciai, katonai, nemzetközi jogi)

6. Kérdés: Lehetséges-e megelőző támadás? (doktrínális és nemzetközi jogi kérdések)

7. Kérdés: A fejlett IT infrastruktúra magában hordozza a sérülékenységet?

8. Kérdés: Milyen védelmi megoldások lehetnek az erős inter- és intradependenciában lévő információs infrastruktúrák esetében, amely regionális és esetenként globális kapcsolatokkal is rendelkeznek?

Az első kiberháború története

- **NATO Cooperative Cyber Defence Centre of Excellence** magalapítása Tallinban (Észtország, Németország, Olaszország, Litvánia, Lettország, Szlovákia és Spanyolország,
2010: Magyarország);
- **NATO Cyber Defence Concept** kialakítása:
  - ✓ Cyber Defence Management Authority (Board) felállítása
- **NATO Cyber Defence Programme** (2002 Prága):
  - ✓ NATO Computer Incident Response Capability (NCIRC) megalakítása kezdeti képességekkel
  - ✓ NCIRC teljes képességeinek kialakakítása
- **2008 Cyber Defense Policy**
- **2011. június: Új NATO Policy on Cyber Defence**
+ Action Plan


INFORMÁCIÓS TÁRSADALOM
FÜGGŐSÉG
INFORMÁCIÓS TECHNIKA ÉS TECHNOLÓGIA

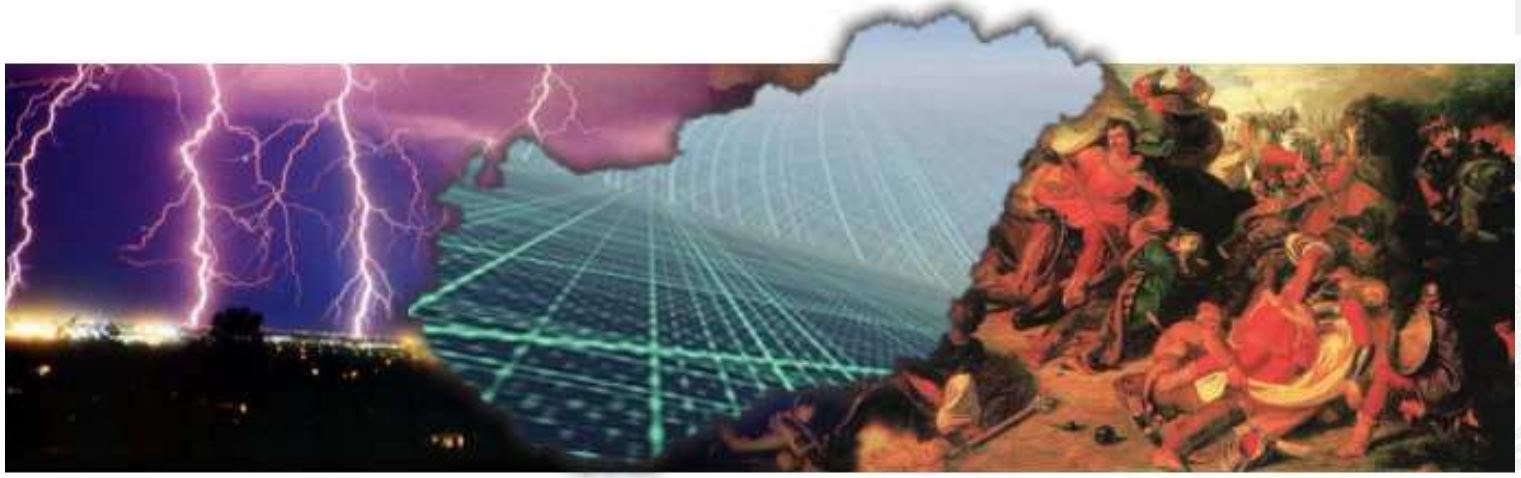
Kritikus információs infrastruktúrák

- **Energia előállító, tároló és szállító rendszerek (gáz, olaj, villamos energia)**
- **Közmű szolgálatok rendszerei (víz, csatorna)**
- **Távközlési rendszerek**
- **Banki- és pénzügyi hálózatok**
- **Vészhelyzeti szolgálatok (Tűzoltóság, rendőrség, katasztrófavédelem)**
- **Közlekedés**
- **Kormányzati rendszerek**

MŰKÖDÉSÜK ALAPVETŐ FONTOSSÁGÚ ÉS NÉLKÜLÖZHETETLEN A TÁRSADALOM MŰKÖDTETÉSÉHEZ!


003/45/7844
ISAT GeoStar 45
23:15 EST 14 Aug. 2003

DIGITÁLIS MOHÁCS



NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

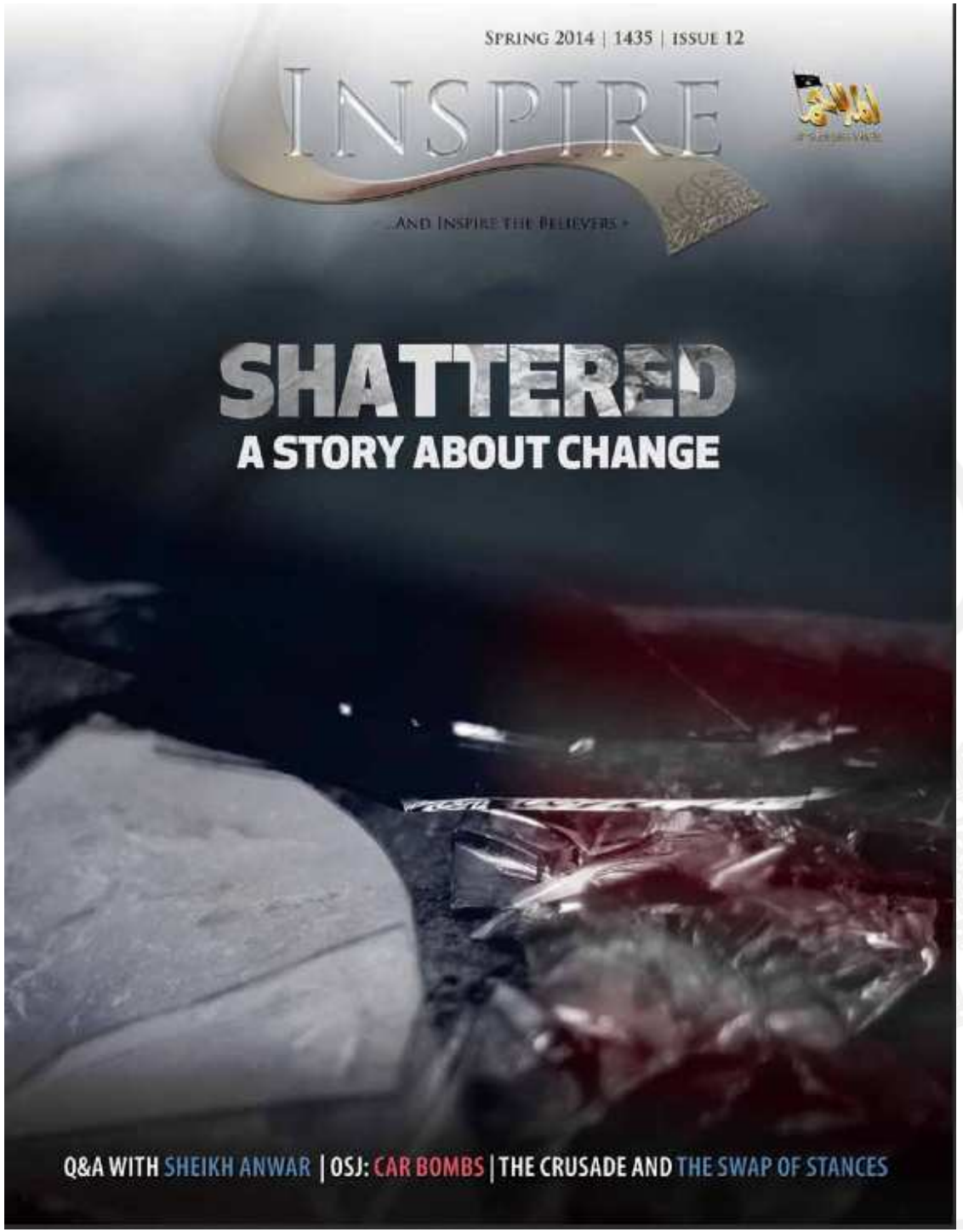
Készítette: Kovács László
Budapest, 2015. március 24.

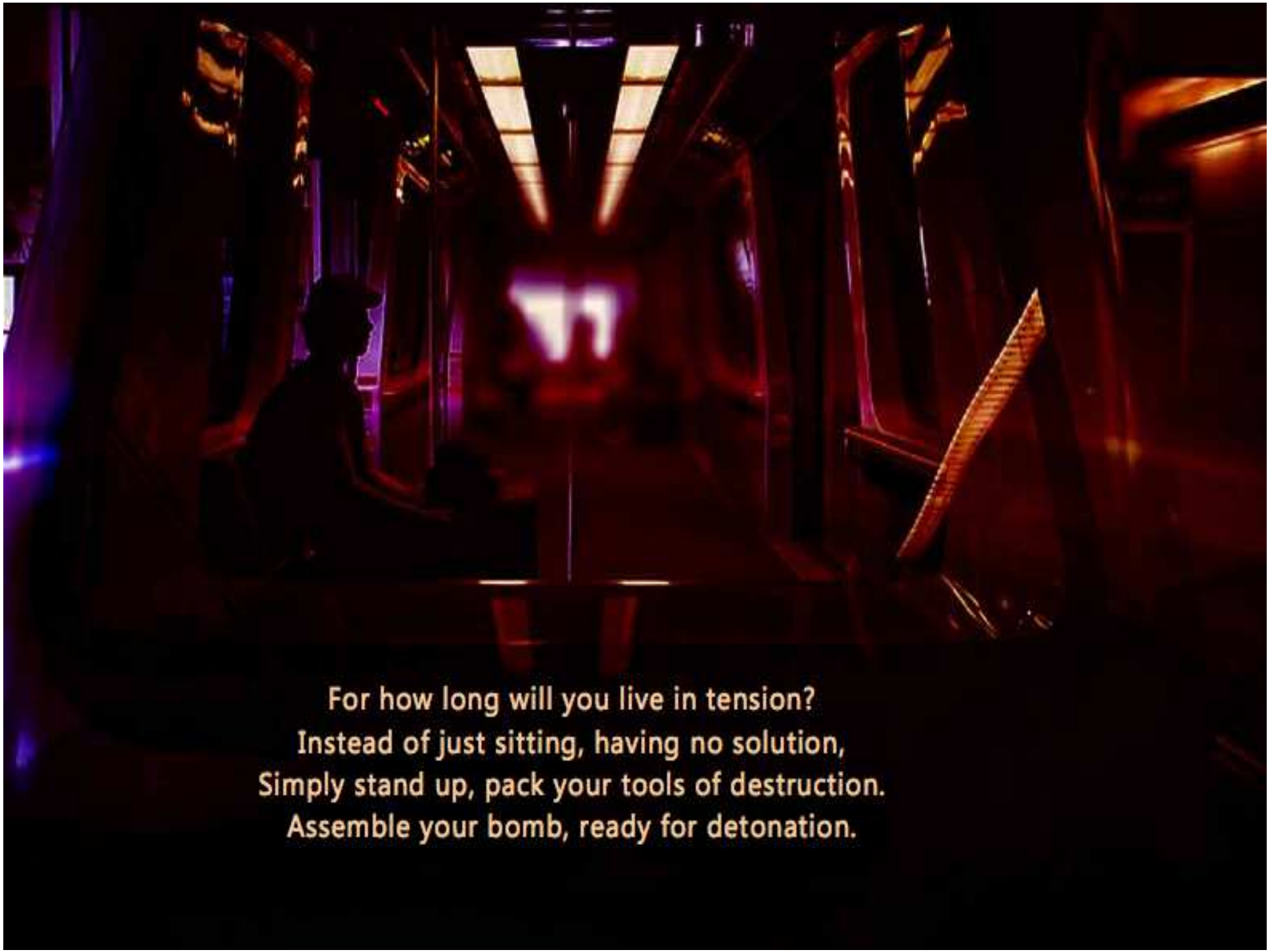
Terrorizmus és információtechnológia

- **Tervezés:**
  - ✓támadások megtervezése
  - ✓kommunikáció
  - ✓szinkronizáció (titkosított adatforgalom)
- **Toborzás:**
  - ✓weboldalak:
    http://www.hizbollah.org
    http://www.alqassam.info
    http://www.qudsway.com
    http://www.kataebaqsa1.com/
- **Adat- és információszerzés:**
  - ✓adatbázisok
  - ✓védelmi rendszerek
  - ✓fegyverek, robbanóanyagok, szerkezetek
- **Propaganda**:
  - ✓az „ügy” bemutatása
  - ✓akciók bemutatása
  - ✓vezetők és „hősök” bemutatása
- **Pénzügyi háttér biztosítása**

- 2001. szeptember 11 után több ezer dokumentum interneten keresztüli elérését szüntették meg a DoD-ban és egyéb helyeken (FAS)
- 2003. január: Rumsfeld Memo*

* http://www.fas.org/sgp/news/2003/01/dodweb.html


SPRING 2014 | 1435 | ISSUE 12
INSPIRE
...AND INSPIRE THE BELIEVERS
SHATTERED
A STORY ABOUT CHANGE
Q&A WITH SHEIKH ANWAR | OSJ: CAR BOMBS | THE CRUSADE AND THE SWAP OF STANCES


For how long will you live in tension?
Instead of just sitting, having no solution,
Simply stand up, pack your tools of destruction.
Assemble your bomb, ready for detonation.

OSJ BOMB SCHOOL

CAR BOMBS INSIDE AMERICA

w/ AQ Chef

Inspire Magazine's goal is to empower Muslim youth. And what is empowerment without being strong, powerful and intelligent? In this section, we give you strength, power and intelligence. Believe me, using car bombs gives you all that.

It is absolutely simple. And we will make it simpler for you, *biidhnillāh*, so that every Muslim, who loves Allāh and His Messenger, and wants to accelerate Islam's victory, becomes prepare to make, even if this is the first military material his eyes has set on.

This recipe gives you the ability to make a car bomb even in countries with tight security and surveillance. The reason is: primary materials easily available and they do not raise suspicion. These materials are not explosives in nature. But after you have assemble and prepare them, they become a bomb ready for destruction, *biidhnillāh*.

This type of car bomb is not usually used to destroy buildings, but is very effective in killing individuals.

The merit of this method is that you can prepare a car bomb in a few hours during the availability of the primary materials. So there is less worry about your personal security.

My Muslim brother, before you start reading the instructions, remember that this type of operation if prepared well and an appropiate target is chosen and Allah decrees success for you, history will never forget it. It will be recorded as a crushing defeat on the enemies of Islam.

REQUIRED COMPONENTS

- Cooking Gas Cylinders (6 or more)
- Oxygen Gas Cylinder (full)
- Barometer (suiting the Cooking Gas Cylinder)
- Connecting nut and pipe
- 6 Decoration lamps
- Match
- Epoxy
- Tissue
- Battery (12v or more)
- Wire


Epoxy


Decoration Lamp


Barometer


Connecting Nut

THE GENERAL IDEA:

We are going to mix two gases; one an oxidizer, another a fuel, in one sealed container that will change the normal combustion of the two materials into an explosive combustion. The explosion will start as soon as a flame emitted from a torch comes in contact with the gas that will burn rapidly under very high pressure.


Cooking Gas Cylinder


Oxygen Gas Cylinder

OPERATIONAL IDEA:

- Pure 'Oxygen' was used as the oxidizing gas, cooking gas 'Propane' as the fuel, and Cooking Gas Cylinder as the sealed container.
- An amount of gas was discharged from the Cooking Gas Cylinder.
- The highly pressurized Oxygen Cylinder was connected to the Cooking Gas Cylinder.
- When the safety valves of both the cylinders were opened, Oxygen Gas moved into the Cooking Gas Cylinder directly. This was caused by pressure difference.
- The pressure inside the Oxygen Cylinder was very high compared to that inside the Cooking Gas Cylinder. We know that gas moves from a high pressure region to a lower pressure region.

PRESSURE DIFFERENCE:

- While the tap is closed, the pressure in the yellow balloon is zero, while the pressure in the red balloon is one.


Closed Tap


Opened Tap

- But when we open the tap, gas moves from the high pressure region (red balloon) to the low pressure region (yellow balloon) in such the pressures in the two balloons become equal.

BAROMETERS:

Pressure measuring instruments are called 'barometers'.

There are different types of barometers, some measure up to 11 bars, others up to 280 bars, and others in between. Barometers used to measure tire pressure usually measure up to 11, 12 or 16 bars.

Barometers used for gas cylinders differ as per the type of the cylinder. For example, large Oxygen cylinders use barometers of 240 bars or 280 bars. Medium cooking gas cylinders use barometers of 34 or 36 bars. There are also many other types of barometers.

Barometers use different units, some use bars, others 'atm', pound per square inch (psi), Pascals (Pa) or milimeter of mercury (mmHg).

Here are some barometers:


Regulator

1. This barometer is sometimes called a 'regulator'. We will use it in these instructions. The meter on the right measures the pressure in the oxygen cylinder - its maximum measurement is 28,000 kiloPascals (kPa), equivalent to 280 bars. While the meter on the left measures the cooking gas cylinder - its maximum measurement is 1400 kPa, equivalent to 14 bars.

PRESSURE UNITS:

- The standard atmosphere that we live in is a unit of pressure.
- The standard atmosphere is almost equal to one bar (1 bar = 1 atm).
- In this procedure we are going to use 'bar' as the standard pressure unit for the gas cylinders.
- When you come across any other unit in your barometer e.g. Pascals, kiloPascals or psi, convert it into bar.
- Conversion is very simple, all you have to do is use a converter in your computer OS calculator.
- A Cooking Gas Cylinder can sustain up to 12 bars.
- An Oxygen Cylinder can sustain up to 135 bars.
- 'kg/cm²' is the same as atm (atmosphere).

Important

It is better to start preparing the car bomb few hours before the operation, because the security forces (if they come into your work place/house) cannot accuse you of preparing a bomb, especially if you distribute the ingredients in your house well.

Fig : 4.1

A Cooking Gas Cylinder Bomb. You have completed the preparation of one cylinder, now prepare the other cylinders in the same way (to make a total of not less than six).

Maximum Carnage

- It is better to use shrapnel (nuts, ball bearings, nails or any other) on the outer surface of the cylinders.
- The best way to arrange the shrapnel is in circles.
- In this car bomb you can use up to 100,000 pieces of shrapnel.
- A hand grenade usually contains 360 shrapnel only.

5 - Inserting the ignition lamp

- Insert the lamp into the connector, while the wires are out.
- Apply epoxy to seal the connector or the modified regulator.

Ignition lamp in connecting nut

Ignition lamp in modified regulator

- Fasten the connector to mixed gas cylinder.

4.1. Cooking Gas Cylinder Bomb

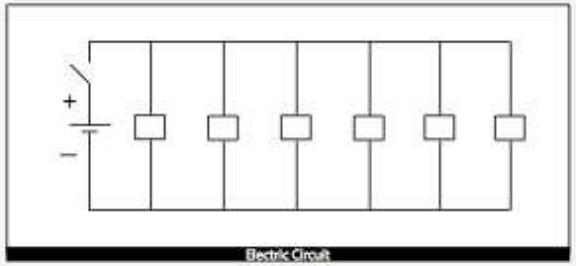
6 - Preparing the Car-Bomb:

- Prepare no less than six 25-litre cylinders.
- Place them closely to each other. Leave as little space between them as possible.
- Connect the ignition lamps.

Car Bomb without Electrical Circuit

7- Preparing the electric circuit: (connecting the cooking gas cylinders)

Every ignition lamp has two wires. Connect the wires on the right to the positive pole (+) of the battery (12v or more), and the wires on the left to the negative pole (-).



Electric Circuit

battery Cooking Gas Cylinder Bomb A Switch

- When these two wires are connected to the battery the car will explode.
- THAT IS WHY YOU SHOULD PUT A SWITCH ON THE POSITIVE SIDE SO THAT YOU CAN CONTROL WHEN TO DETONATE THE CAR BOMB, AND PROTECT THE CIRCUIT FROM UNINTENDED DETONATION.
- Note: It is recommended to test the electric circuit using another decoration lamp of the same type used for ignition.
- If you are a martyrdom bomber and you want to detonate the car bomb directly, use a manual switch that is operated by hand directly.
- If you want to make it a time bomb, use a time switch (you can refer to Inspire Magazine issue 1 and 9 for details).
- If you want a remote detonation, use a toy-car remote, alarm remote, garage remote or any other. You can test the remote with a lamp (or refer to issue 8 for details).

That's all there is to it

Remember

If you intend to hide your identity buy a car without any formal paperwork being exchanged.

Important

If it possible, carry out an experiment even if in a smaller scale in a safe place, because an experiment will give you lot of experience before the main operation.

OSJ SPECIALIST CONSULTANCY

CAR-BOMB: FIELD DATA

w/ AQ Chef

SPECIFIC TARGETS:

Areas and Restaurants with high profile personalities - Usually these people visit the restaurants during the weekend:

- Arlington
- Alexandria

- It is worth to mention a more specific target, Savoy Hotel located on the Strand in central London. At about 10 pm GMT, businessmen and high profile targets leave the hotel. This is a perfect place and time to detonate your car bomb.

SPECIFIC TARGETS IN FRANCE:

- With over 82 million foreign tourists per annum, France is ranked as the first tourist destination in the world, beaches and seaside resorts, ski resorts, and rural regions that many enjoy for their beauty and tranquility (green tourism).
- The Transport express régional (TER)'s stations. Rush hours will always do.
- The Dordogne valley, during summers. Hit two birds with one stone; both

region's main seaport. Virginia in general attracts a load of tourists.

- Chicago:

It is in the mid of the US, hence it is a major transportation hub. It is an important component in global distribution, as it is the third largest inter-modal port in the world. It is also an important worldwide center of commerce. The city has the second largest financial center in the United States. Among its most important financial structures:

1. Sears Tower, a 108-story skyscraper, it held the title tallest building in the world for about 25 years.

2. The Chicago Board of Trade Building.

- Los Angeles:

The most populous city in the state of California, and the second most populous in the United States. It is also the largest manufacturing center in the western United States. It is also the home base of Hollywood.

first tourist destination in the world, beaches and seaside resorts, ski resorts, and rural regions that many enjoy for their beauty and tranquility (green tourism).

- The Transport express régional (TER)'s stations. Rush hours will always do.
- The Dordogne valley, during summers. Hit two birds with one stone; both the English and the French.
- The Coupe de la Ligue; only open to professional clubs. Expect huge crowds of supporters outside the entrances.
- The Bastille Day Military Parade: the morning of 14th July each year in Paris.
- During special exhibition in the Musée du Louvre: the most visited art museum in the world and a historic monument.
- The French Riviera.

Give 'em War

US, UK and French police force are not used to a frontline-type war. They cannot withstand a bang of a grenade, let alone a full car bomb blast.

no secret. It does not even use pretexts to invade Muslims. What happens in Central African Republic is enough evidence. It invaded the country to help the Christian militia fight the regime Army for its relation to Islam

Logic

When targeting high profile places, go for the entrance; you cannot get a car into most of these targets. But what goes in, comes out; there should be an entrance.

Készítette: Kovács László
Budapest, 2015. március 24.

Bitcoin may be the next weapon in ISIS extremists' arsenal

By Patrick Howell O'Neill Follow on July 08, 2014

A blogger is teaching jihadi groups, and specifically members of the Islamic State of Iraq and Syria (ISIS), how to organize and finance terrorism through Bitcoin, Sky News reports. A recent blog post highlights how well the cryptocurrency can serve the needs of ISIS militants.

ISIS, which now calls itself the Islamic Caliphate, has captured a large swath of territory in northern Syria and Iraq in recent months, as it attempts to

"The jihadists are investing a lot in encryption technologies and they have developed their own software to protect their communications and when western agencies work out how to crack them they adapt quickly."

Steve Stalinsky, executive director of the Middle East Media Research Institute

http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/

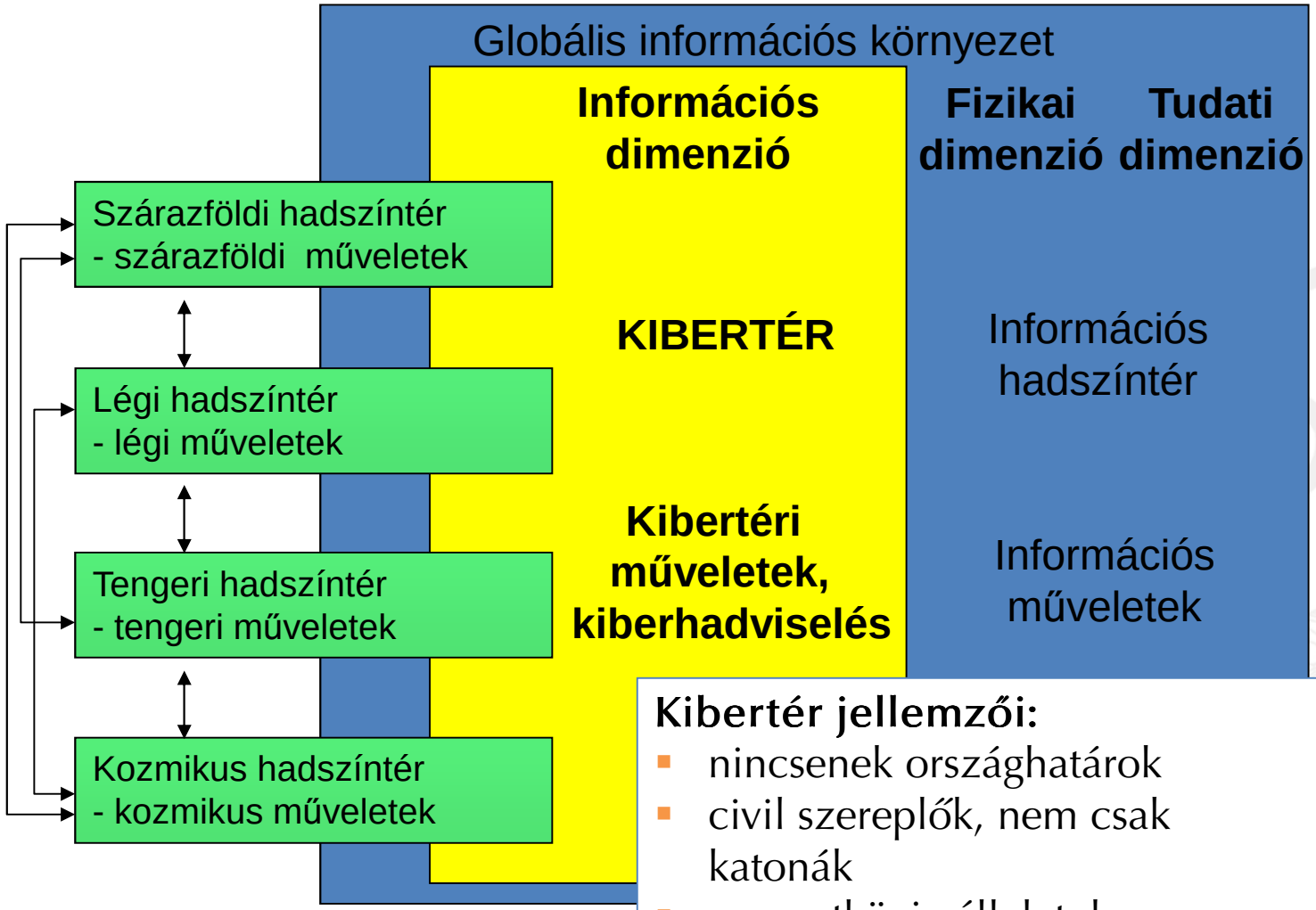
„De mi történik, ha egy kibertámadás mögé egy ország áll?"

- korlátlan humán;
- technikai;
- és gazdasági erőforrásaival?

KIBERHADVISELÉS

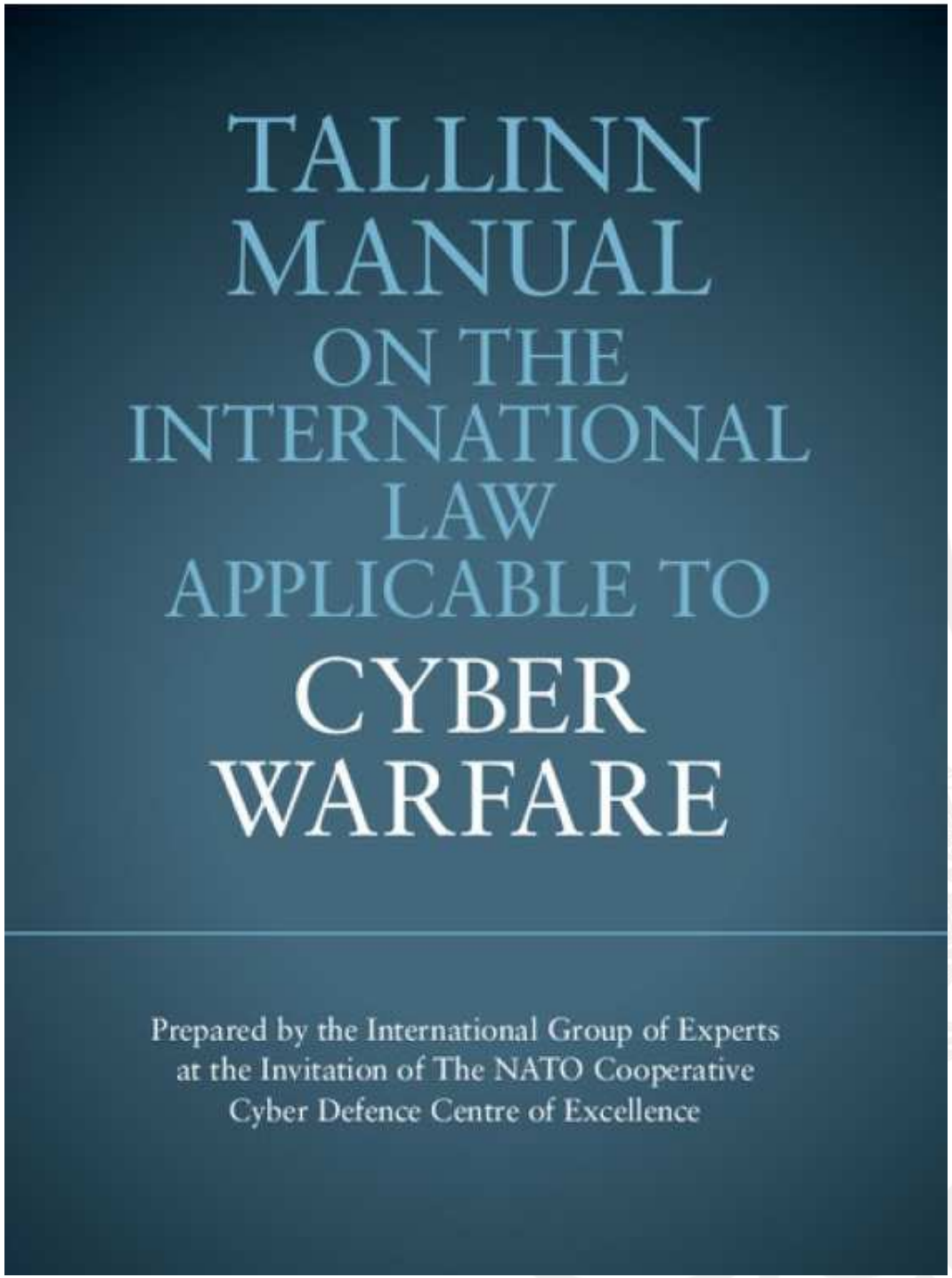
Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés



Kibertér jellemzői:

- nincsenek országhatárok
- civil szereplők, nem csak katonák
- nemzetközi vállalatok
- hazai és nemzetközi szolgáltatók
- globális szolgáltatások



Kiberhadviselés

- Számítógépek és hálózatok katonai célok érdekében történő felhasználása;
- Információszerzés;
- Párhuzamos műveletek a hagyományos katonai műveletekkel;
- Számítógép-hálózatok működésképtelenné tétele.

Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés összetevői

- Számítógép-hálózati műveletek
  Computer Network Operations:
  - ✓ Computer Network Exploitation
  - ✓ Computer Network Attack
  - ✓ Computer Network Defense
- Elektronikai hadviselés
  Electronic Warfare
- Elektronikai felderítés
  Signals Intelligence - SIGINT

Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés eszközei

- 0-day exploitok
- Botnetek
- (Célzott) malwarek
- DoS, DDoS
- APT-k
- Social engineering
- Kinetikus fegyverek
- Elektromágneses fegyverek

Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés célpontjai

- Szembenálló fél információs rendszerei
  (katonai -, nemzetbiztonsági -, közigazgatási rendszerek)

- Kritikus információs infrastruktúrák
  (energiaellátás, ipari irányítás, kommunikáció, közlekedés, pénzügyi rendszerek)

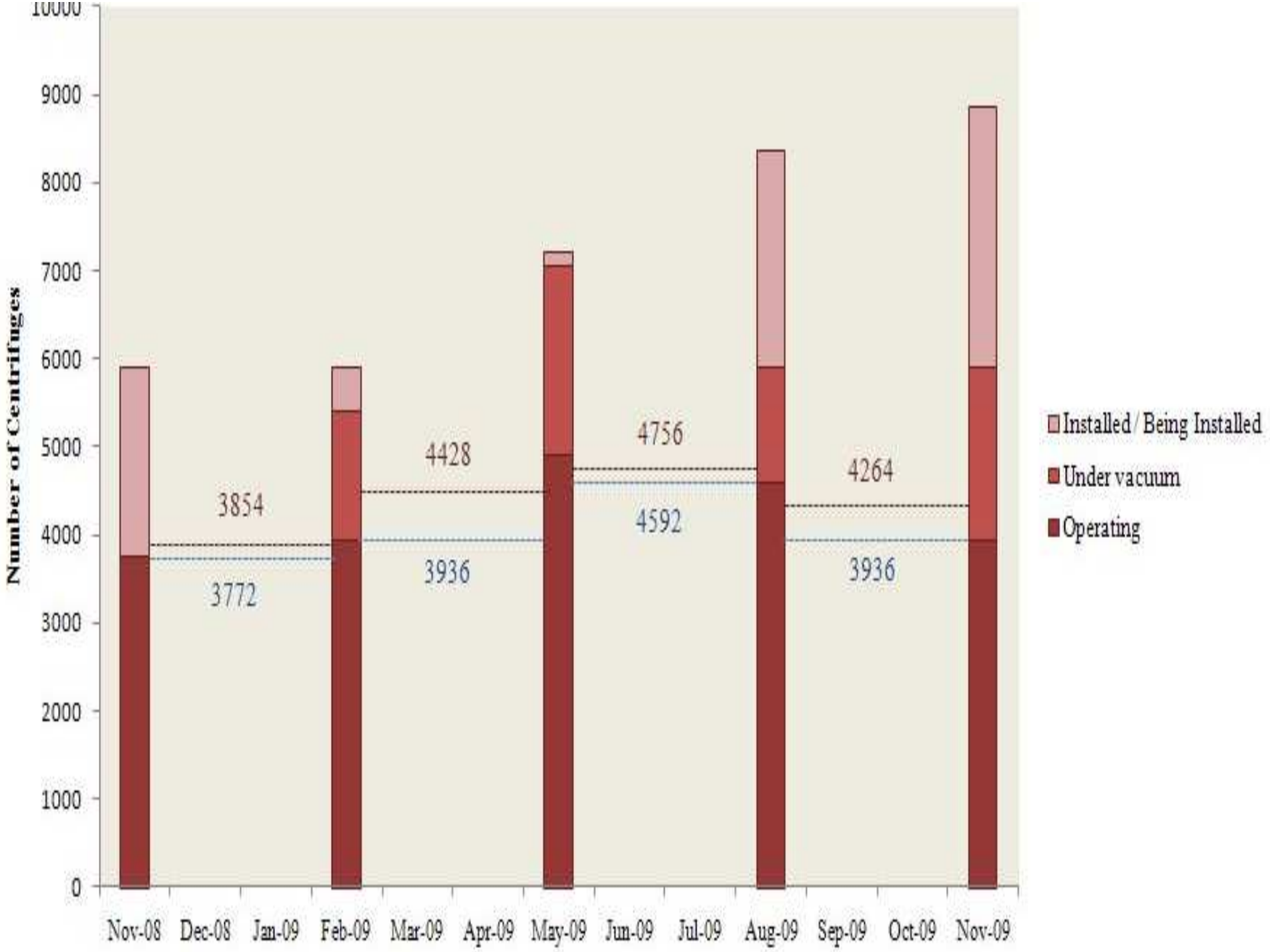
Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés célpontjai

NEMZETI
KÖZSZOLGÁLATI
EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Kiberhadviselés célpontjai


Number of Centrifuges
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
Nov-08
Dec-08
Jan-09
Feb-09
Mar-09
Apr-09
May-09
Jun-09
Jul-09
Aug-09
Sep-09
Oct-09
Nov-09
3854
3772
4428
3936
4756
4592
4264
3936
Installed / Being Installed
Under vacuum
Operating

Kiberhadviselési nagyhatalmak

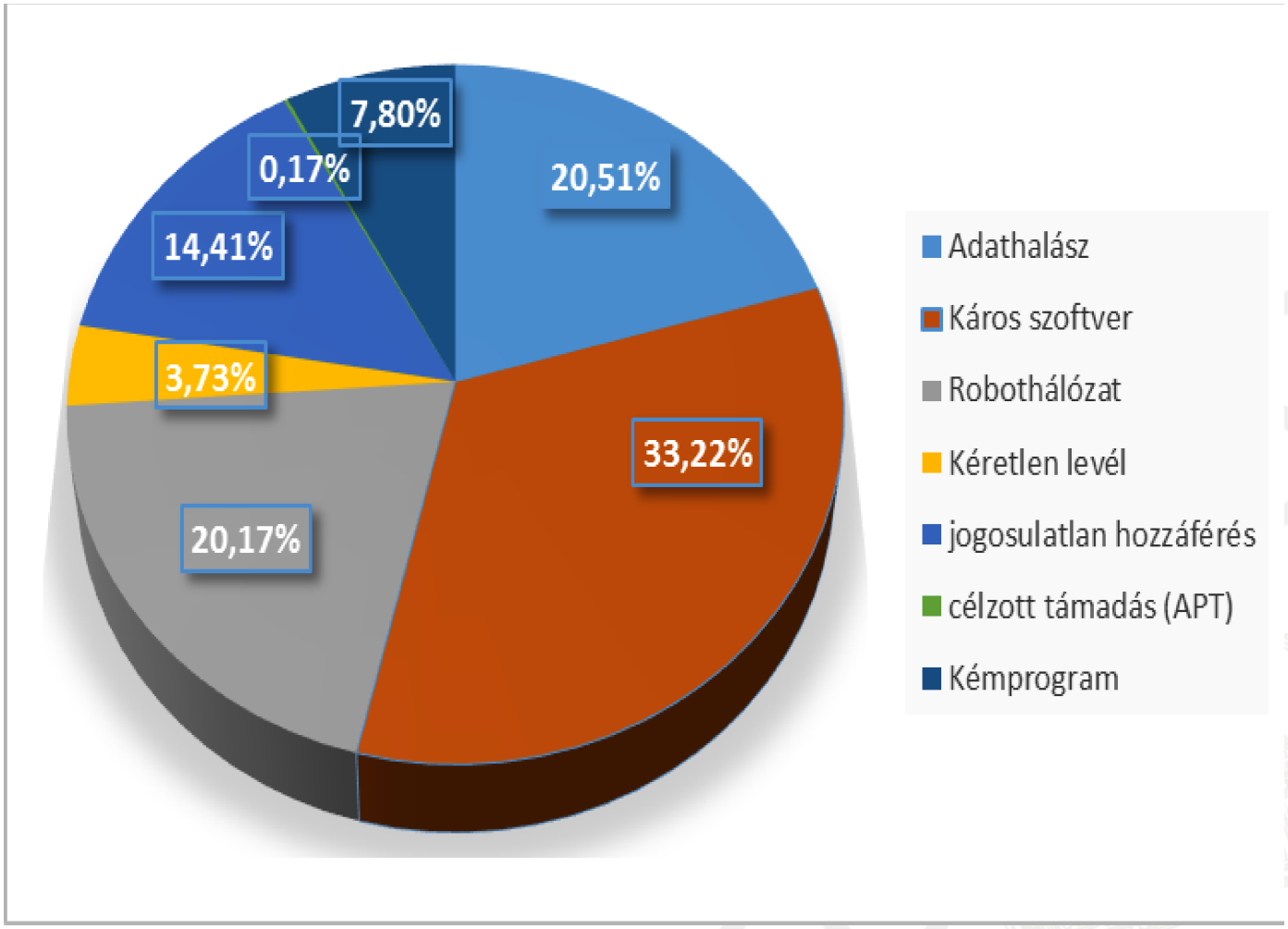
- USA 

- Kína 
- Németország
- Franciaország

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Magyarországi helyzetkép

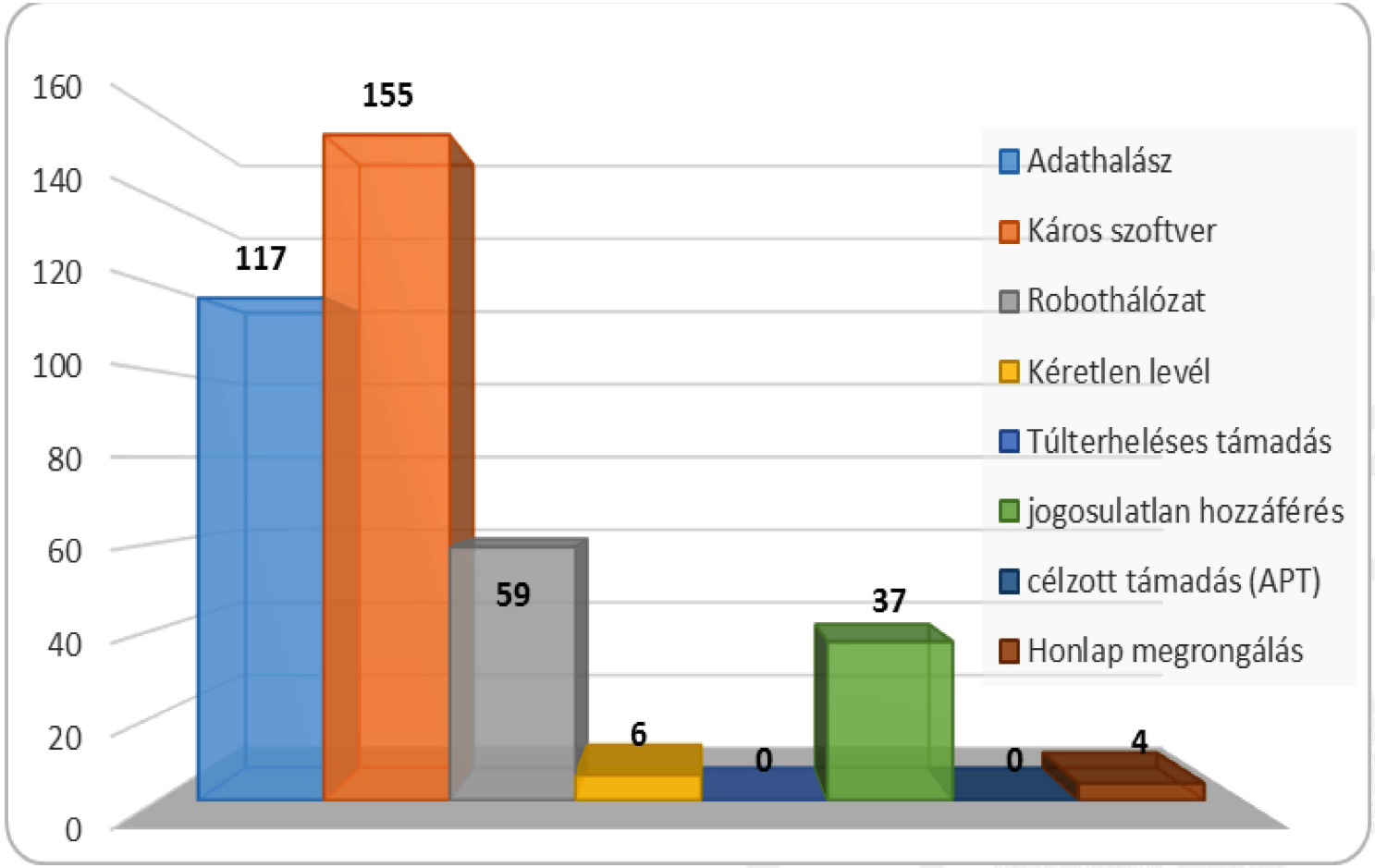


A 2014. 4. negyedév során bejelentett összes incidens típusonkénti megoszlása

Készítette: Kovács László
Budapest, 2015. március 24.

Forrás: Gov-CERT Hungary Kormányzati eseménykezelő Központ

Magyarországi helyzetkép



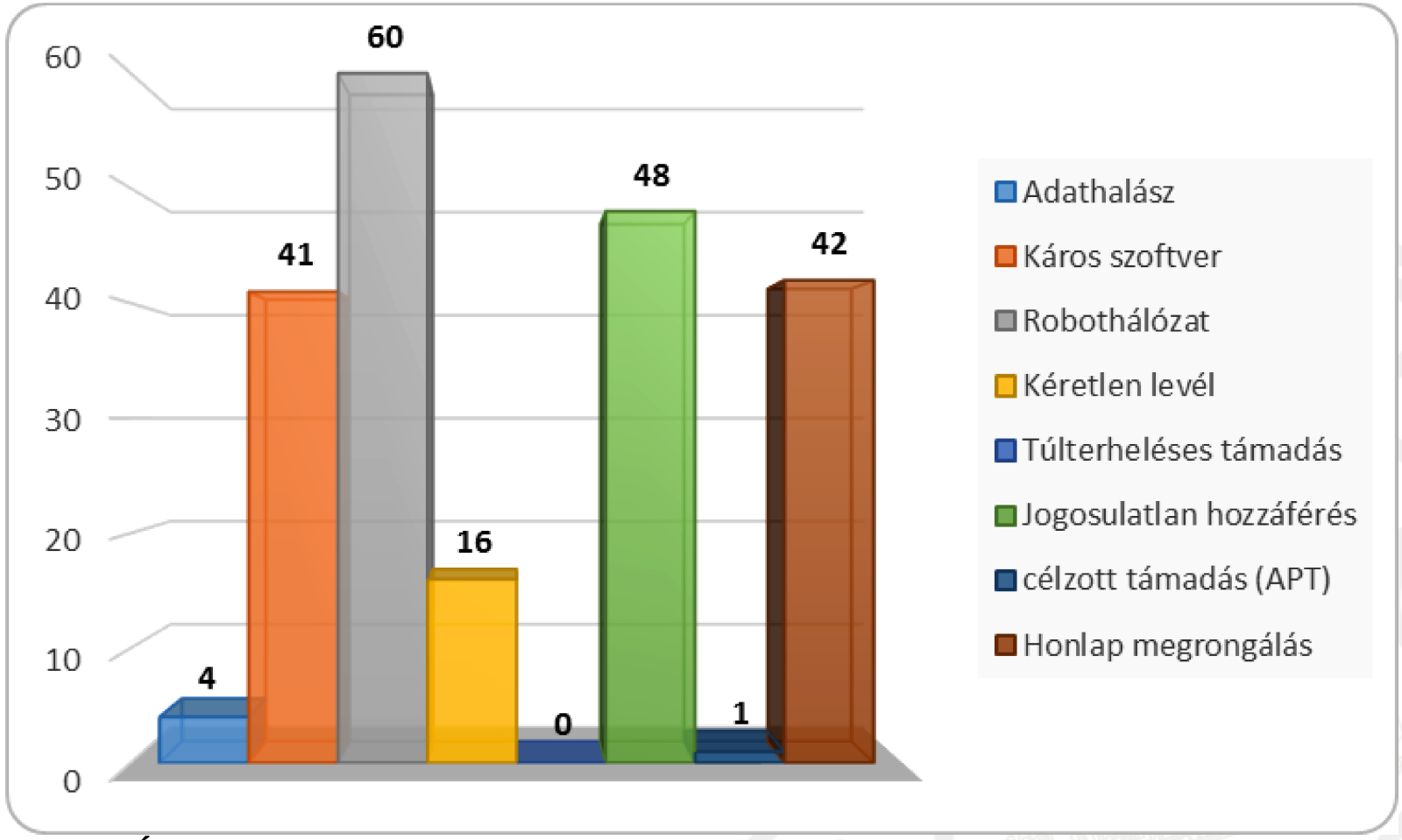
Nem állami- és önkormányzati szervet érintő incidensek 2014. 4. negyedév

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Forrás: Gov-CERT Hungary Kormányzati eseménykezelő Központ

Magyarországi helyzetkép



Állami- és önkormányzati szervet érintő incidensek 2014. 4. negyedév

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Forrás: Gov-CERT Hungary Kormányzati eseménykezelő Központ

A kibertér védelme Magyarországon

- Fejlett IT infrastruktúra;
- Kialakuló jogszabályi háttér;
- Kialakuló szervezeti háttér;
- Nemzetközi együttműködés aktív részesei vagyunk.

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

Nemzeti Biztonsági Stratégia

- A Kormány 1035/2012. (II.21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról
- *„31. Kiberbiztonság.* […] *A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia.”*

Nemzeti Katonai Stratégia

- A Kormány 1656/2012. (XII. 20.) Korm. határozata Magyarország Nemzeti Katonai stratégiájának elfogadásáról
- *„33.* […] *kiemelkedik a számítógépes hálózatok elleni támadások növekvő száma és károkozási potenciálja. A kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását.”*
- *„52.* […] *Ilyen fenyegetést jelent elsősorban a kiber hadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.”*
- *„82.* […] *erősíteni kell a Magyar Honvédség kibervédelmét…”*

Kritikus infrastruktúrák védelme

- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- Mindennapi élet fenntartásához szükséges
- BM OKF felügyeli és ellenőrzi
- Azonosítás és kijelölés (10 ágazat, 42 alágazat)
- Hatósági ellenőrzés – bírság
- Közszféra és magánszféra vegyesen birtokolja
- Digitális Mohács?

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

szerk.: Szengáli Gergely

Nemzeti Kiberbiztonsági Stratégia

- A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
- Kiberbiztonsági környezet meghatározása
- Célok és feladatok kijelölése
- Eszközrendszer megállapítása
- Létrehozza a Nemzeti Kiberbiztonsági Koordinációs Tanácsot

Elektronikus információbiztonsági törvény

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- „Ibv. törvény" – egységes keretrendszer
- A magyar kibervédelmi szervek 80%-ának ez a törvény a jogforrása
- Állami és önkormányzati rendszerek és szervezetek felmérése és biztonsági osztályba sorolása
- 2014. július elsejéig kellett elkészíteni a besorolást – utána 2-3 évente felülvizsgálatra van szükség

Nemzeti Kiberbiztonsági Koordinációs Tanács

- Miniszterelnökségnek alárendelve működik
- Elnök: Lázár János (politikai) + Szemerkényi Réka (kiberkoordinátor)
- Kormányzati koordináció
- Nemzeti Eseménykezelési Központ Munkacsoport:
  - CERT-ek
  - Havi ülésezés
  - Incidenskezelő protokoll kialakítása
- Nemzeti Kiberbiztonsági Koordinációs Fórum (magán- és akadémiai szféra, CEO szint)

Kormányzati szektor
Nemzeti Elektronikus Információbiztonsági Hatóság

- Nemzeti Fejlesztési Minisztériumnak alárendelve működik
- Ibtv. hatálya alá szervezetek biztonsági szintjének ellenőrzése és a végső döntés meghozatala
- A kormányzati incidenskezelő munkacsoport irányítása
- Éves jelentés a nemzeti kibervédelem állapotáról
- Biztonságtudatosság erősítése, továbbképzések lebonyolítása

Kormányzati szektor
Kormányzati Eseménykezelő Központ

- GovCERT-Hungary
- Belügyminisztériumnak alrendelve a Nemzetbiztonsági Szakszolgálat üzemelteti
- Ibtv.-ben meghatározott rendszerek és hálózatok védelme
- Kapcsolattartás a nemzetközi CERT közösséggel
- Negyedéves biztonsági jelentés készítése a Nemzeti Kiberbiztonsági Koordinációs Tanács részére
- Ágazati CERT-ek támogatása, nyilvántartása

Kormányzati szektor
Nemzeti Biztonsági Felügyelet

- Belügyminisztériumnak (korábban a Közigazgatási és Igazságügyi Minisztériumnak) alárendelve működik
- Fő feladata a hazai és nemzetközi (NATO, EU) minősített adatok védelme és felügyelete – ezek átalakítás alatt vannak
- Cyber Defence Maganagement Authority
  - Kérésre sérülékenységvizsgálatot végez
  - Biztonsági események műszaki adatainak vizsgálata
  - Kiberbiztonsági gyakorlatokon képviseli az országot

Kormányzati szektor
Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja

- BM Országos Katasztrófavédelmi Főigazgatóságnak alárendelve működik
- Feladata a kritikus infrastruktúrák informatikai rendszereinek felügyelete és védelme
- Ágazati eseménykezelő központokat felszólíthatja feltárt kritikus sérülékenységek határidőre történő kijavítására
- Oktatási és tájékoztatási feladatokat is ellát

Készítette: Kovács László
Budapest, 2015. március 24.

szerk.: Szengáli Gergely

Közszféra
Nemzetbiztonsági szektor

- **Alkotmányvédelmi Hivatal**
  - Műveleti IT Osztály
  - Célzott (APT) és nem célzott („non-targeted”) elektronikus támadások – új hírszerző technikák, állami támogatással
- **Nemzetbiztonsági Szakszolgálat**
  - GovCERT-Hungary üzemeltetése
  - Műveleti technikai támogatás
  - Azonosítás (pl. DDoS esetén) és FORENSIC tevékenység
- **Katonai Nemzetbiztonsági Szolgálat**
  - HM és HVK információvédelmi támogatása
  - Rendszerfelügyeleti (figyelő-jelentő) és készenléti (beavatkozó) szolgálat
  - Katonai CERT

Közszféra
Rendészeti szektor

- Nemzeti Nyomozó Iroda
  - Csúcstechnológiai Bűnözés Elleni Osztály
  - Kiberbűnözés elleni szerv
- Terrorelhárítási Központ
  - E-Osztály
  - Terrorizmus és Számítógépes Bűnözés Elleni Monitoring Egység

Közszféra

Katonai szektor

Magyar Honvédség

- Nemzeti Katonai Stratégiából eredő célok és feladatok
- MH Kibervédelmi Szakmai Koncepció
- MH Kormányzati Célú Elkülönült Hírközlő Hálózat és katonai rendszerek védelme
- Ibtv. a honvédségre is vonatkozik
- KNBSZ, mint rendszerfelügyelő szerv
- Támadóképességek?

Készítette: Kovács László
Budapest, 2015. március 24.

szerk.: Szengáli Gergely

Közszféra

Készítette: Kovács László
Budapest, 2015. március 24.

Szerk.: Szentgáli Gergely

Akadémiai szektor
Nemzeti Közszolgálati Egyetem

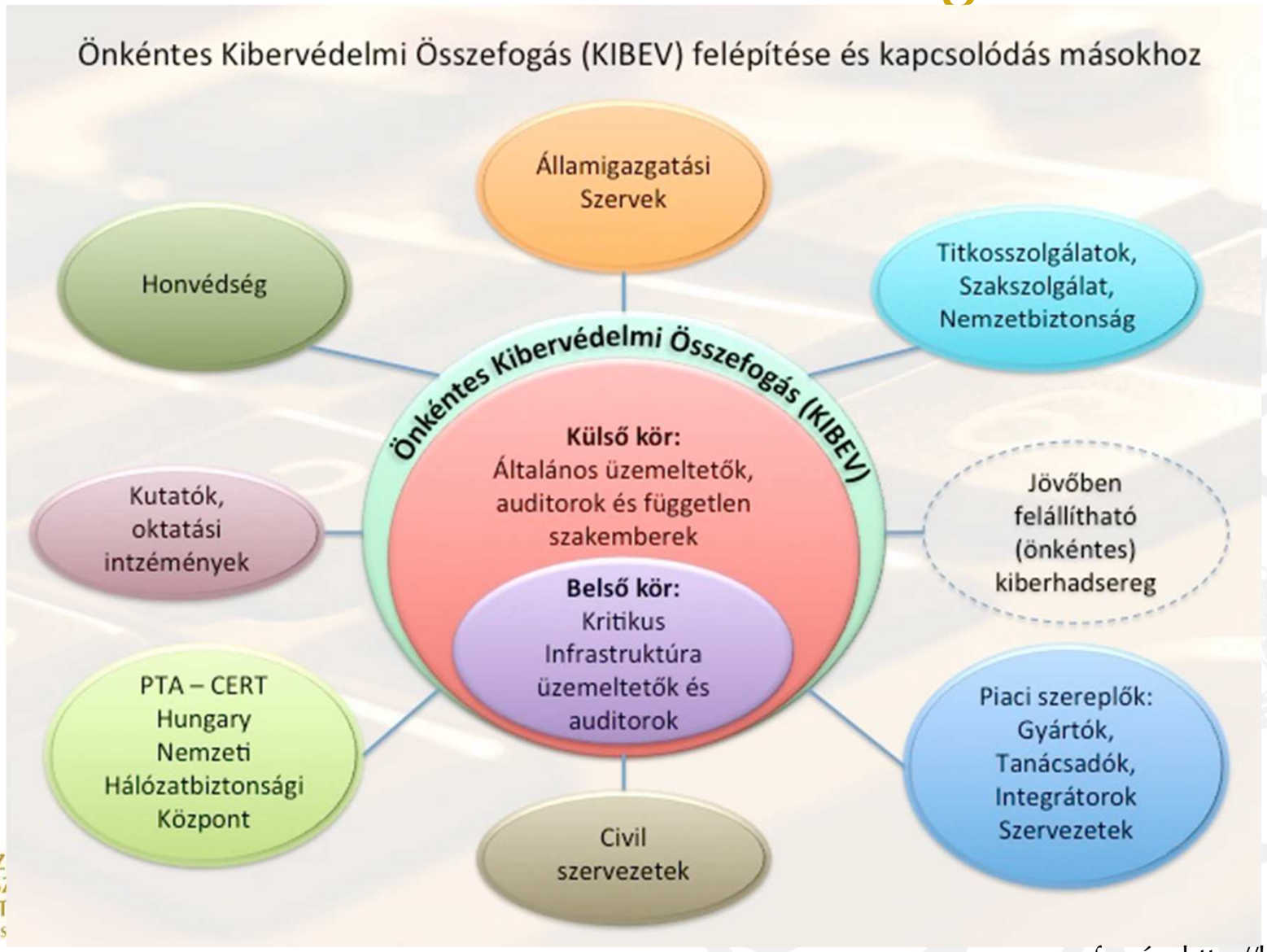
- Ibtv. is nevesíti, mint oktatási-képző és kutatási-fejlesztési szervezetet
- NKE-KTK
  - E-közszolgálat Fejlesztési Intézet
- NKE-HHK Informatikai és Elektronikai Hadviselés Tanszék, illetve Híradó Tanszék
  - Védelmi vezetéstechnikai rendszertervező MSc – információbiztonsági szakirány
- NKE-NETK Biztonság- és védelempolitika BSc és MSc

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN

Készítette: Kovács László
Budapest, 2015. március 24.

szerk.: Szengáli Gergely

KIBEV
Önkéntes Kibervédelmi Összefogás



forrás: http://kibev.hu

A kibertér védelme Magyarországon

- Fejlett IT infrastruktúra;
- Kialakuló jogszabályi háttér;
- Kialakuló szervezeti háttér;
- Nemzetközi együttműködés aktív részesei vagyunk;

- Lemaradás az oktatásban;
- Elmaradás a biztonságtudatosságban;
- Nincs támadó képesség.

Készítette: Kovács László
Budapest, 2015. március 24.

Összefoglalás

- A kiberhadviselés napjaink komoly kihívása;
- Rendszereink sebezhetőek;
- Veszély a kiberterrorizmus;
- Állami támogatású kibertámadások prognosztizálhatóak;
- Magyarország jó úton jár a védekezésben, de van még mit tenni ...

Irodalom

- 1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról http://www.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf
- 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról http://www.kormany.hu/download/d/05/c0000/2012_1220_NKS.PDF
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről http://www.complex.hu/kzldat/t1200166.htm/t1200166.htm
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról http://www.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
- Defending the networks The NATO Policy on Cyber Defence http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, Brussels, 7.2.2013 JOIN(2013) 1 final http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

Köszönöm a figyelmet!

Kovács László

kovacs.laszlo@uni-nke.hu

NEMZETI KÖZSZOLGÁLATI EGYETEM
A HAZA SZOLGÁLATÁBAN