

# A botnetek, mint a közeli jövő fegyverei

Gyányi Sándor  
Budapesti Műszaki Főiskola KVK HTI



# Veszélyforrások

Ha egy számítógépes hálózat nyilvános hálózatról elérhető, akkor könnyen megtámadható. Az okok:

- Feltűnési viszketegség, „dicsőség” iránti vágy.
- Anyagi előnyszerzés, számítógépes bűnözés.
- Politikai, vallási, ideológiai meggyőződés (terrorizmus).
- Katonai célok.

# DoS támadás meghatározása

- Denial of Service: szolgáltatás megtagadás. A támadó a célpont informatikai rendszerét próbálja olyan módon túlterhelni, hogy az képtelen legyen a normál, üzemszerű működésre és így az általa nyújtott szolgáltatás nyújtására.  
Leggyakoribb módszer: túlterhelés.

# DDoS

- Distributed Denial of Service: elosztott szolgáltatás megtagadásos támadási módszerek.
- A támadó egyidejűleg nagyszámú végpontot használva indítja meg a támadást.

# DDoS támadások

- A sikeres akciókhoz nagy mennyiségű támadó végpont szükséges.
- Bár hivatalosan nem ismerik el, szakértők szerint több ország hadereje is tart készenlétben támadási célokat szolgáló hálózatokat.

# DDoS támadások 2.

- 2008. júliusában a grúz erők megtámadták a szakadár dél-ozsét terület fővárosát, amire Oroszország válaszul katonai műveletekbe kezdett.
- Az orosz internetes alvilág fórumain megjelentek a DDoS támadásokat végrehajtani képes önkéntes botmaster toborzások.
- A grúz kormányzati weboldalak gyakorlatilag eltűntek az Internetről.

# Bot, zombi PC

- A legtöbb DDoS támadást botnetek követik el.
- Megsokasodtak az olyan rosszindulatú alkalmazások, amelyek segítségével az áldozat számítógépe távolról irányíthatóvá válik.
- Kedvelt elnevezésük a „robot” szó rövidítéséből adódó „bot”.
- Botnet: több „bot” hálózatba szervezésével alakul ki.

# Botnet részei

- Botmaster, vagy botherder: a botnet „tulajdonosa”. Ő adja ki a feladatokat.
- Command & Control (C2) csatorna: a botmaster és a botnet tagok közti kommunikációt biztosítja.
- Drop server: a botnet működése során keletkezett adatok tároló helye.
- A hálózat tagjai.

# Katonai botnetek

- Egyes hírek szerint több ország jelentős botnet kapacitással rendelkezik.
- Egyre többen úgy látják, hogy a hagyományos, „falak mögé” bújtatott védekezés nem elegendő ezen a téren.

## Carpet bombing in cyberspace

### Why America needs a military botnet

BY COL. CHARLES W. WILLIAMSON III

The world has abandoned a fortress mentality in the real world, and needs a network that can project power by building an af.mil ro amounts of traffic to target computers that they can no longer adversaries than hunks of metal and plastic. America needs the deterrent we lack.

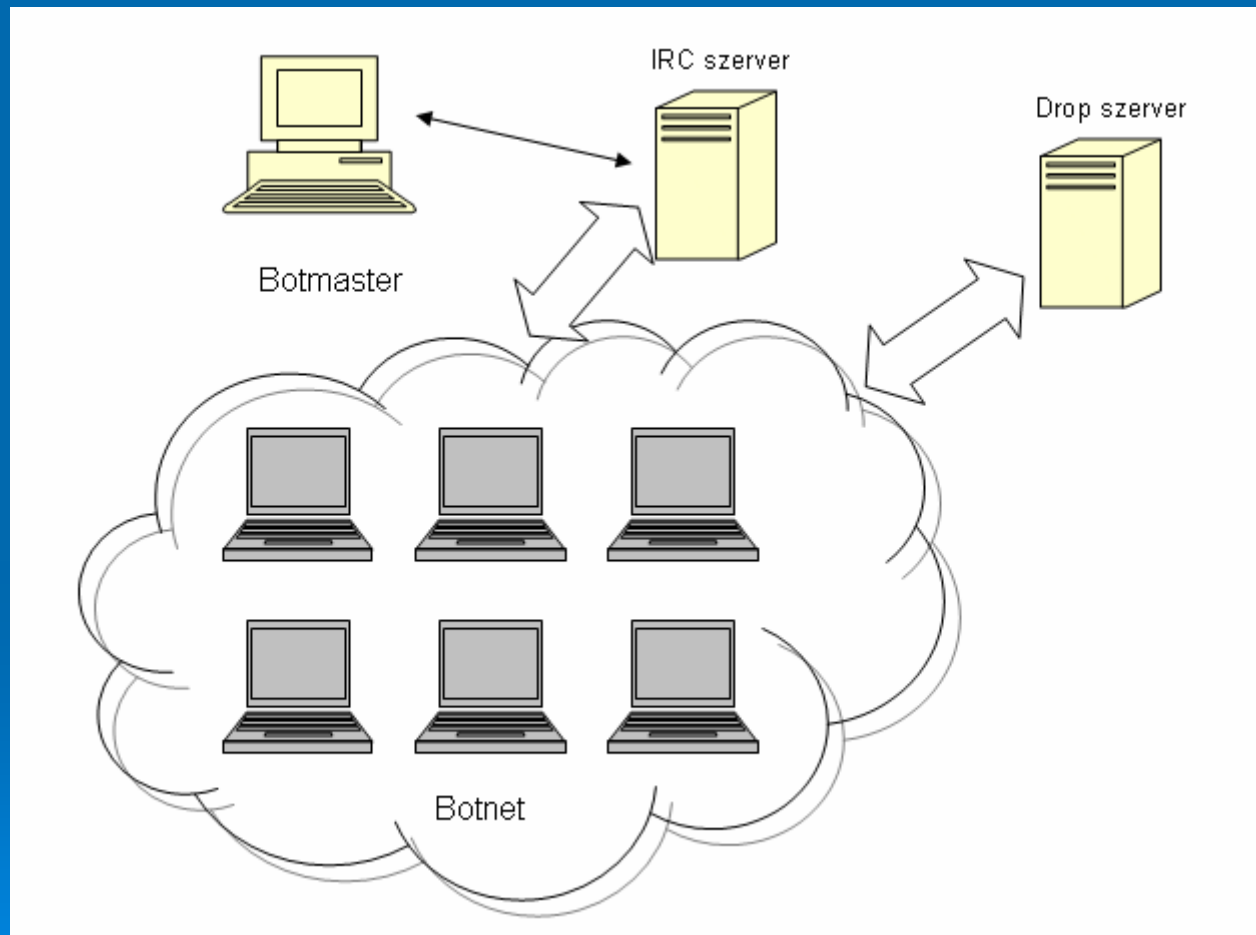
America faces increasingly sophisticated threats against its military has no credible deterrent, and our adversaries prove it every de concept is fundamentally flawed, and we have not learned the simpl

As much as some think the information age is revolutionary, local n the ancient model of roads and towns: Things are produced in one more value. The road-and-town model works well between cooperat do, they sometimes have to defend themselves from attack. In to firewalls, gateways, passwords, port blocking, intrusion detection the same strategy as the medieval castle with its walls, moat, draw worked more or less for hundreds of years, they are now abandon anemic attack.

# Botnet struktúrák

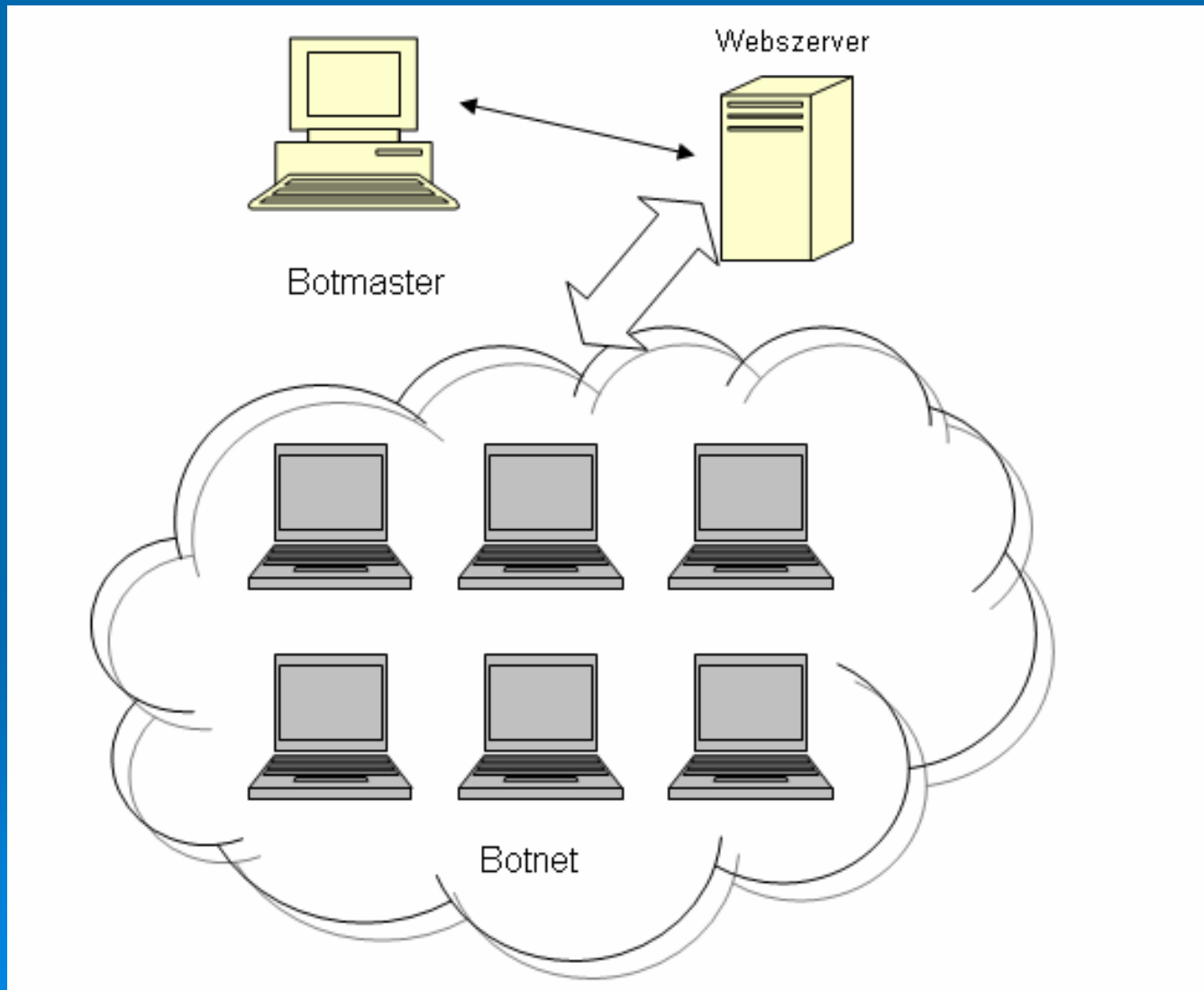
- IRC alapú Command & Control
- Web alapú Command & Control
- Peer-to-peer alapú Command & Control.

# IRC alapú C2



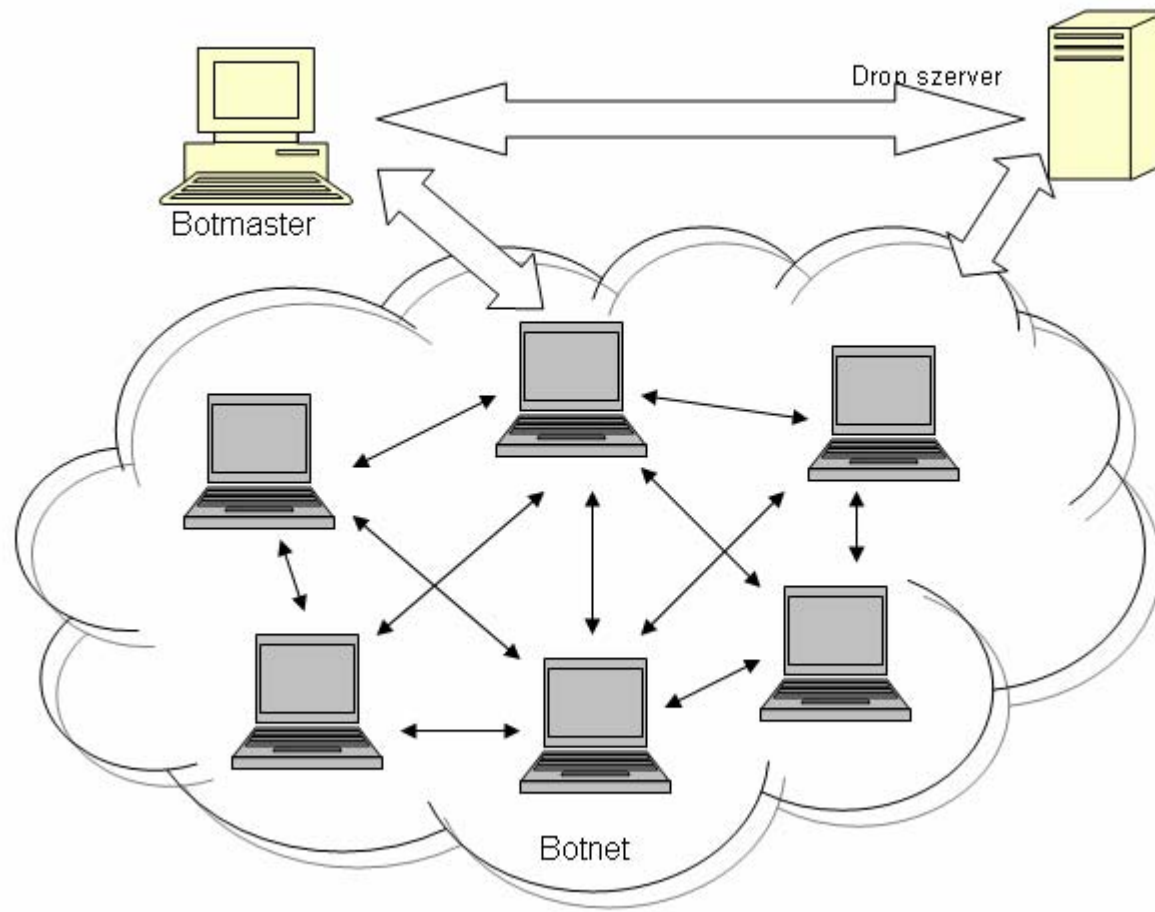
- Az ilyen botnetek tagjai egy közös IRC szerverre csatlakoznak, és innen kapják a feladatokat.
- A tagok úgy viselkednek a csatornában (szobában) mint a passzív emberi kliensek, azonban a megfelelő parancsokat beírva aktivizálhatók.
- Ma már könnyen detektálhatók.

# Web alapú C2



- Az IRC-vel ellentétben egy webserverre a kliensek nem állandó kapcsolattal csatlakoznak.
- A weboldalak lekérésére szolgáló http protokoll szerint a kliens a kívánt oldal letöltéséhez felcsatlakozik a szerverre, majd a tranzakció befejezése után bontja a kapcsolatot.
- A botnet tagjai rendszeres időközönként csatlakoznak a szerverhez és lekérik az aktuális feladatot, egyúttal elküldik a saját adataikat.

# P2P alapú C2



- A botmaster a botnet bármelyik tagjára képes távolról, az Interneten keresztül rácsatlakozni és a szükséges feladatokat elindítani.
- Ennél a struktúrájánál nincs központosított C2 szerver, így a küzdelem meglehetősen nehéz.
- A nagyobb elterjedtségnek örvendő bot alkalmazások normál fájlcsere-protokollokat használnak, tehát a hálózati forgalom elvegyül a többi, nem botnet által generált forgalomban.

# Ellentevékenység

- A botneteket a tevékenységük figyelésével fel lehet deríteni.
- A felderített botnetek semlegesíthetők, azonban néhány nemzetközi jogi probléma felmerül, különösen abban az esetben, ha az érintett felek között állami szervek is vannak.

# Háború a virtuális térben

- Mi történne, ha egy állam egy másik állam kritikus információs infrastruktúrája ellen támadást intézne a virtuális térben?
- A cyber támadásokról külön rendelkezések még nincsenek, a hagyományos, fegyveres konfliktusokra vonatkozóak pedig nem minden esetben illeszkednek.
- Az ENSZ alapokmányának VII. fejezete rendelkezik a hagyományos konfliktusokról.

# Az ENSZ alapokmányának VII. fejezete

*"A Biztonsági Tanács határozza meg, hogy milyen fegyveres erők felhasználásával nem járó rendszabályokat kíván fogatosítani abból a célból, hogy határozatainak érvényt szerezzen és felhívhatja az Egyesült Nemzetek tagjait arra, hogy ilyen rendszabályokat alkalmazzanak. Ilyeneknek tekintendők a gazdasági kapcsolatok, a vasúti, tengeri, légi, postai, távírói, rádió és **egyéb forgalom** teljes vagy részleges felfüggesztése, valamint a diplomáciai kapcsolatok megszakítása.,,*

<http://www.menszt.hu/layout/set/print/content/view/full/186>

# Kommunikáció korlátozása

- Az „egyéb forgalom” eredetileg „other means of communication”, vagyis a kommunikáció egyéb formái (így az internetes forgalom is) korlátozhatók.
- Megítélés kérdése, hogy egy virtuális térben kivitelezett támadás mekkora okozott kártól (anyagi vagy emberélet) számít fegyveres konfliktusnak.

# Ellencsapások

- 1998-ban az Electronic Disturbance Theater (EDT) nevű radikális politikai szervezet megtámadta a Pentagon webservert.
- Ahogy a támadás ténye kiderült, a Pentagon szakemberei azonnal ellentámadásba lendültek.
- A támadó kliensekre töltöttek egy Java appletet (hostileapplet), amely a böngésző képernyőjén kávéscsészéket - a Java logója - és az "ACK" üzenetet jelenítette meg akkora mennyiségben, hogy a böngésző erőforrásai elfogytak, ami a támadó számítógép lefagyását idézte elő.
- Az EDT fontolóra vette a Pentagon perbe fogását a „Posse Comitatus”, egy 1878-as törvény alapján, amely tiltja a katonaság bevetését a belföldi törvények betartatása során.

# Ellencsapások 2.

- Az Internet nem ismer határokat, jellegéből adódóan egy ellencsapás adatforgalma áthalad más – semleges - országok hálózatain.
- A tényleges támadó nem ugyanaz, mint ahonnan a támadás indul, a célpont meghatározása gyakran lehet téves.
- Téves ellencsapás támadásnak minősül.

**Köszönöm a figyelmet!**

