How to prevent a disaster in cyberspace ?

The need for an international approach to undermine the criminal cyber architecture

Open-ended intergovernmental expert meeting on cybercrime
UNODC Vienna, 19-01-2011

Presentation

- **Luc Beirens**
  Chief Superintendent
  Head of the Federal Computer Crime Unit
  Belgian Federal Judicial Police
  Direction Economical and financial crime

  Chairman of the EU Cybercrime task force
  representing the organization of heads of
  national hightech crime units of the EU

Topics - overview

- General trends today
- Cyber crimes and cyber criminals today
- What hinders the combat today ?
- A proposal for an integrated response
- Belgian experiences

General trends today

- Evolution towards **e-society**
  - replace persons by e-applications
  - Interconnecting all systems (admin, industrial, control)
- **IP** is **common platform** offered by **many ISPs** integrating telephony / data / VPN & all new apps =opportunities / Achilles tendon / scattered traces
- **Poor security** in **legacy** applications and protocols (userid+pw)=> identity fraud is easy
- **Enduser** is not yet educated to act properly

What do criminals want ?

- *Become **rich / powerfull** rapidly, easily, very big ROI in an illegal way if needed*

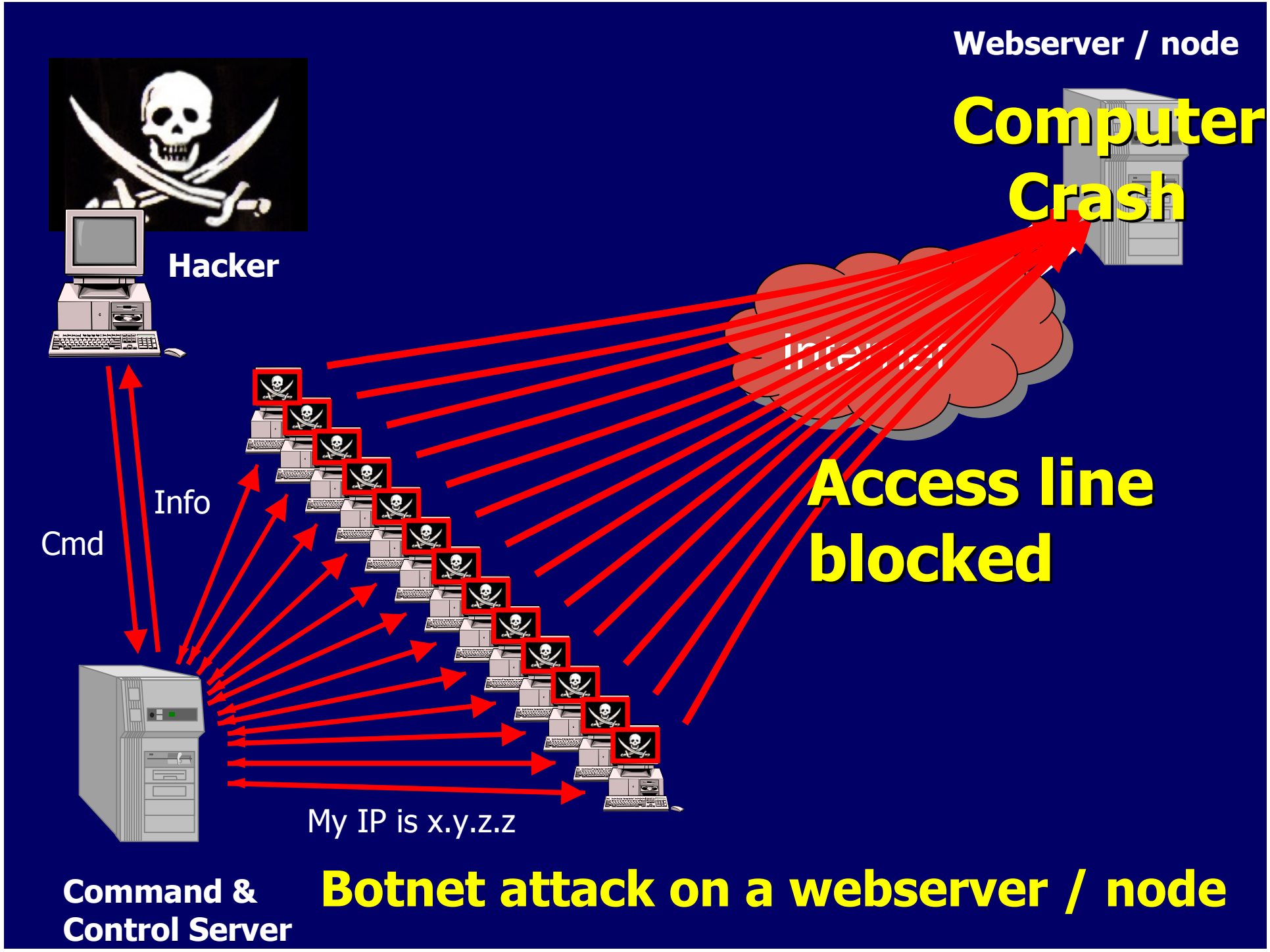
- ***Destabilaze (e-)society** by causing troubles*

How : cyber crimes today

- **e-fraud** => give money to the criminals
- **spam** => start for eFrauds
- **hacking** =>
  - change content of your website (defacing)
  - transfer money from the hacked system
  - espionnage => know your victim
  - use of hacked system =>
    storage / spam / proxy / DNS / CC / DDOS
- **DDOS** distributed denial of service attacks

How to combat cyber criminals ?

Analyse their methods and tools


Webserver / node
Computer Crash
Hacker
Internet
Access line blocked
Info
Cmd
My IP is x.y.z.z
Command & Control Server
Botnet attack on a webserver / node

Interesting DDOS

- 2004 UK : gambling website down (+ hoster + ISP)
- 2005 Netherlands : 2 botnets : millions of zombies
- 2005 Belgium : Commercial firm during social conflict
- 2006 Sweden : Gov websites after police raid on P2P
- 2007 Estonia : political inspired widespread DDOS attack
- 2008 Georgia : cyber war during military conflict
- 2010 Worldwide : Wikileaks cyberconflict

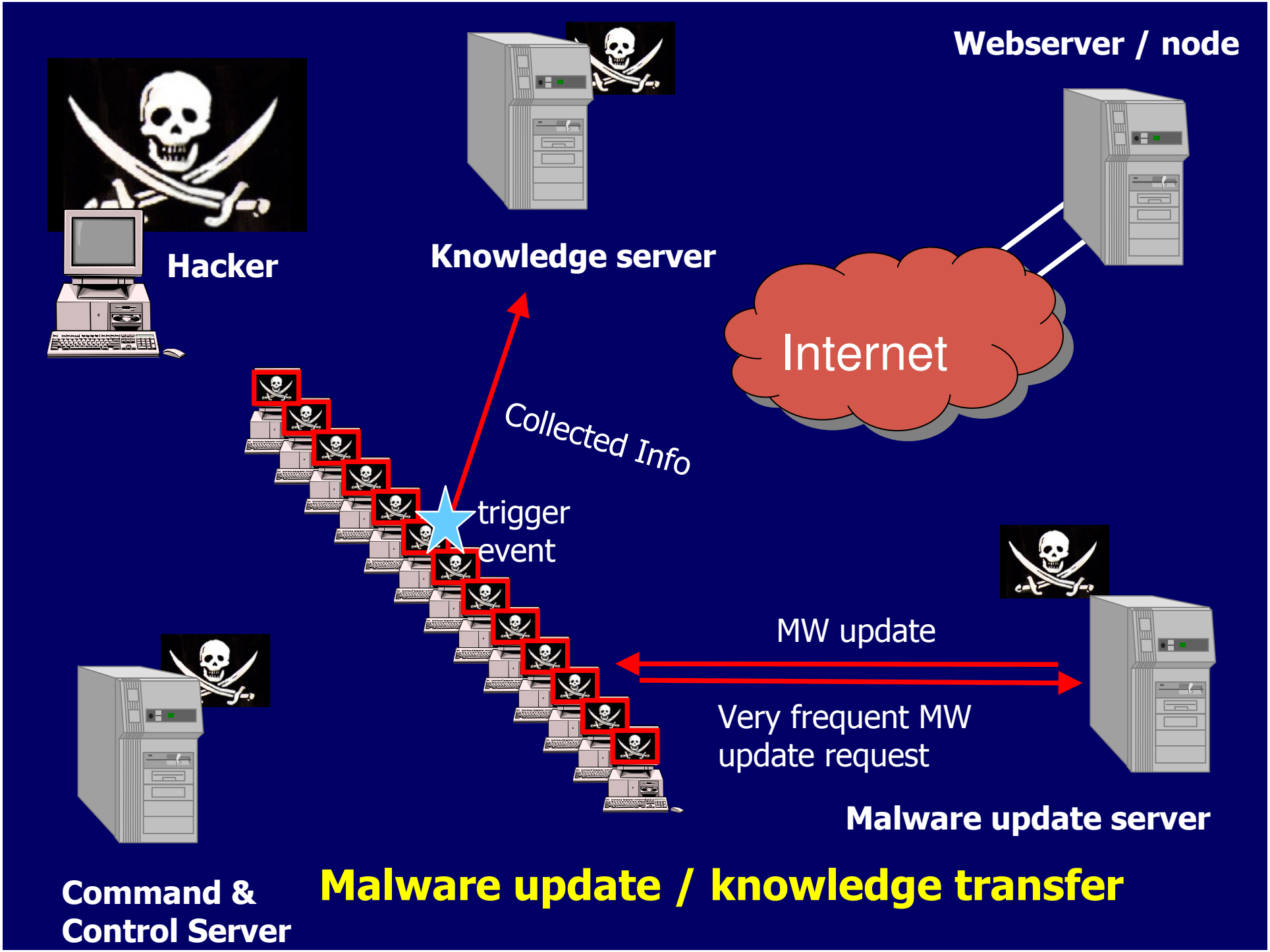
What are botnets used for ? Making money !

- Sometimes still for **fun** (scriptkiddies)

- **Spam** distribution via Zombie
- **Click generation** on banner publicity
- **Dialer** installation on zombie to make premium rate calls
- **Spyware / malware / ransomware** installation

- **Espionage** : **banking** details / passwords / keylogging
- **Transactions** via zombie PC

- Capacity for distributed denial of service attacks **DDOS** => disturb functioning of internet device (server/router)


Webserver / node
Hacker
Knowledge server
Internet
Collected Info
trigger
event
MW update
Very frequent MW
update request
Malware update server
Command &
Control Server
Malware update / knowledge transfer

Cyber criminal's toolbox

- **malware** => trojan horses
  - distribution via mail, p2p, social networks, websites
  - **auto-update** & **auto-propagation** in network
  - very high rate of new versions
- remote control of infected systems => **botnets**
- creation of **knowledge databases**
  - collected & keylogged info of infected pc
- keyservers in **safe haven** countries

But the criminal cyber architecture also includes ...

- **Underground fora** and chatrooms
  - Botnets for hire
  - Malware on demand / off the shelf packages
  - Trade stolen Credit cards / credentials
  - Money laundering services
- Organized Cyber criminals
  - take over / set up **ISP's**
  - infiltrate in **development firms**

And the victims ?

- Who ?
  - Communication networks and service providers
  - Companies especially transactional websites
  - Every internet user
- Reaction
  - **Unaware** of incidents going on => dark number
  - Victims try to solve it themselves
  - Nearly **no complaints** made => dark number
- Result ? The hackers go on developing botnets

Risks

- Economical disaster
  - Large scale : critical infrastructure
  - Small scale : enterprise
- Individual & corporate (secret) data
- **Loss of trust** in e-society

Combined threat

- What if abused by terrorists ? Cyber army ? ... simultaniously with a real world attack?
- How will you handle the crisis ?
  Your telephone system is not working !

Intermediate conclusions

- Society is very dependant of ICT
- eSociety is very vulnerable for attacks
- Urgent need to reduce risks on critical ICT
- Botnets as criminal cyber infrastructure is common platform for lots of cybercrimes

=> *undermine it and you reduce crime*

Traditional way of law enforcement to tackle cybercrime

- Reactive
  - Register complaint => judicial case
  - Hotlines (or cooperation with)
  - (Eventualy) undercover operations
- Proactive (?)
  - Who is doing what, where and how ?
  - Patrolling the net
- Effective (?) but not undermining cybercriminals

What hinders an effective combat of cyber crime ?

- Unawareness and negligence **end user**
- Lack of overall view on risks / incidents by
  - Enterprise managers
  - Political decision makers
- Combating : **everyone on his own**
- Lack of specialized investigators
- Jurisdictions limited by **national** borders
- Subscriber **identity fraud**
- **Mobility** of the (criminal) services in cloud

What actions are needed ?

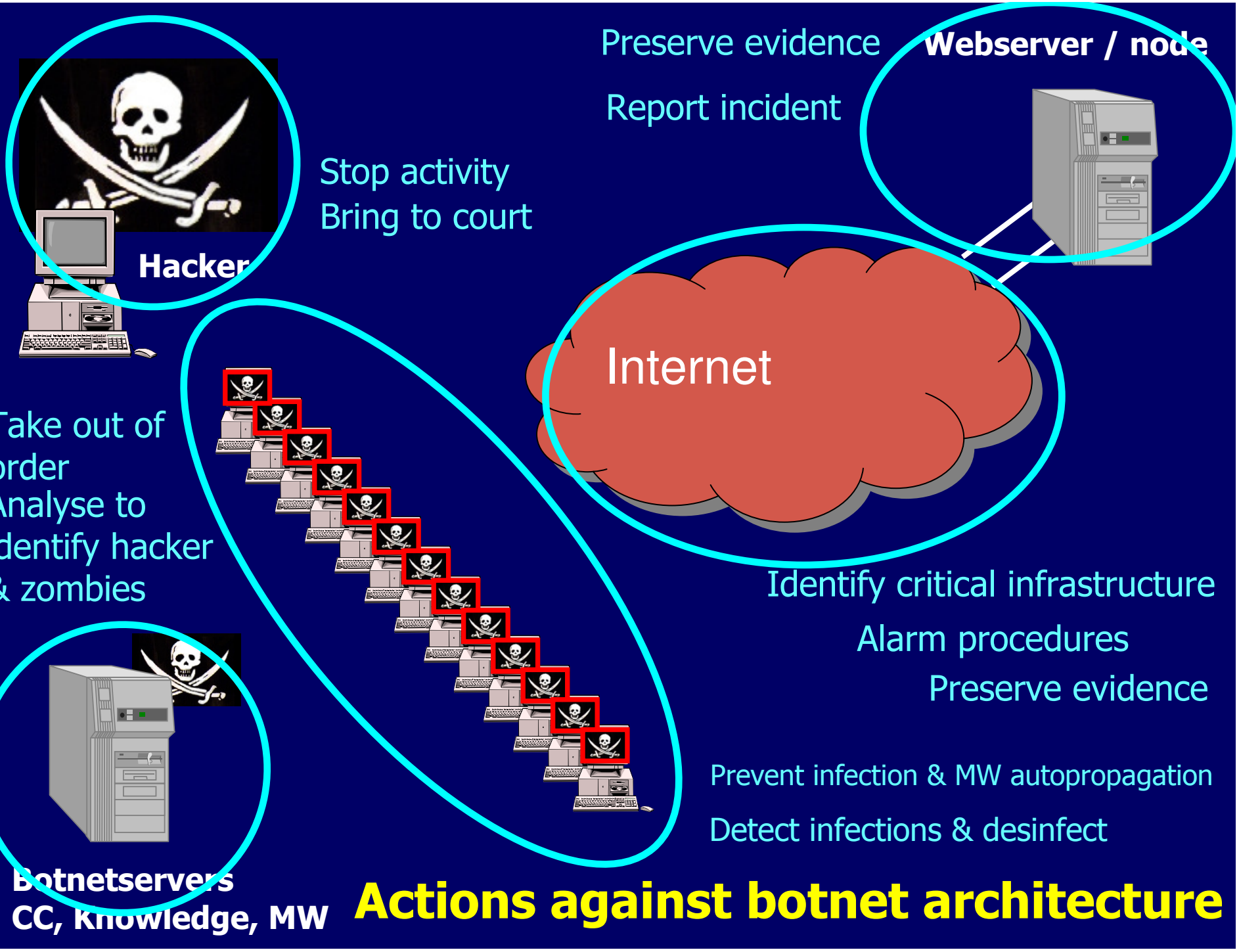
Everyone plays a role in e-security

We have to do it as **partners**

We have to do it in an **integrated way**

Goals for operational cybercrime action plan

- As "society" (= gov & private sector) improve **detection** and **get a view** and **act** on
  - criminal cyberinfrastructure especially botnets
  - incidents threatening eSociety
- Strengthen **robustness** of ICT eSociety
  - ISP's / Enterprises / End users
- **Weaken** and **dismantle** the criminal cyberinfrastructure
  - Each partner within his role & competence


Preserve evidence
Webserver / node
Report incident
Stop activity
Bring to court
Hacker
Internet
Take out of order
Analyse to identify hacker & zombies
Identify critical infrastructure
Alarm procedures
Preserve evidence
Prevent infection & MW autopropagation
Detect infections & desinfect
Botnetservers
CC, Knowledge, MW
Actions against botnet architecture

Role of governments & international organizations

- Working according **a strategy**
- Develop **international** plans & reaction schemes for **critical ICT infrastructure protection**
- Develop **legal framework**
  - Obligation to report cybercrime incidents
  - Obligation to secure your computersystem (?)
  - Possibility for ISP to cut off infected machines (?)
  - Obligation to respond to requests of Gov authority when serious incidents happen

Telecommunications sector

- Prevent / reduce SPAM
- Have to make there infrastructure **robust**
- **Report** serious incidents to CERT
- **Integrated reaction** with authorities

- Implement **strong authentication** in internet protocols and services
- Detect negligent **end users** & react/help/cut off

Enterprises

- E-Security = **business risk** => management responsibility
- Think about **how to survive** when e-systems are under attack

- Enforce **detection** of incidents – IDS ?
- **Report** incidents to CERT ? to police ?
- Integrate **strong authentication** in e-business applications

Developers

- Strong authentication
  - Use the strongest available but ...
  - Think as a hacker
    How can a transaction on an infected PC be intercepted ?
- Store **IP-addresses** and timestamps
  - of the end user ! not of the router !
  - Needed in case of an **incident** !

Responsibilization of end user

- **Awareness** raising => media
- **Training** on e-security & attitude
  - already at school
  - in the enterprises
- Obligation to **secure his PC properly ?**

Role of police and justice ?

- **Gather intelligence** about Botnets
- **Dismantle botnet servers** in your country
- **Analyse Botnet-servers** to find traces to criminals
- Focus on knowledge servers & CC servers

Belgian experience

- 1 national **FCCU** +25 Regional CCU=175 officers (computer forensics & cybercrime combat)
- 2 specialized Federal prosecutors
  minimum 1 ICT reference prosecutor / district
- FCCU analyses attacks on critical ICT infra

- **BelNIS** Gov Network information security
  - Develops and organizes ICT security strategy
  - Problem : no central authority
- Since 2009 : **Cert.be** for Gov and Critical infra

Belgian experience

- eBanking fraud => start of **Malware analysis**
  - Gain insight in how it's working
  - Leads to detection of botnet-servers / bogus ISP's
- Combined team **cybercrime & financial investigators**
- **Building trust** with law enforcement with other countries
- Collaboration with several partners and organizations => Information send to & analysed by **Cert.be**
- Effective in dismantling of Botnet-servers (50 since '09)
- Impact of 1 Malware distribution server ? Analysis shows
  - 2 months 1,5 million downloads, 300.000 unique IP's

Problems

- Botnet-servers often on **victim's servers**
  - But is it really a victim ?
- No knowledge-servers in BE
- Language problem during analysis CC-server
- Is it the role of the police / Cert ?
  - If Cert does it (eg Finland)
    - => fast but do we go after criminals afterwards ?
    - Which incidents are severe enough to report to police ?
  - If police does it
    - Which botnet-servers do we analyse ?
    - Malware analysis => help from AV-industry ?

Do we really have an impact ?

- Several hundreds of botnets
- 5.000 – 10.000 botnet servers world wide
- Millions of infected end users

=> need for action in every country

Contact information

Federal Judicial Police
Direction for Economical and Financial crime
Federal Computer Crime Unit
Notelaarstraat 211 - 1000 Brussels – Belgium

Tel office : +32 2 743 74 74
Fax : +32 2 743 74 19

E-mail : luc.beirens@fccu.be