# Where are the hackers?

## preliminary analysis of the geographies of cybercrime


lartin Dodge
entre for Advanced Spatial Analysis, UCL
ttp://www.cybergeography.org

Muki Haklay
Dept. of Geomatic Engineering, UCL
http://www.casa.ucl.ac.uk/muki/

# Is geography relevant to cybercrime?

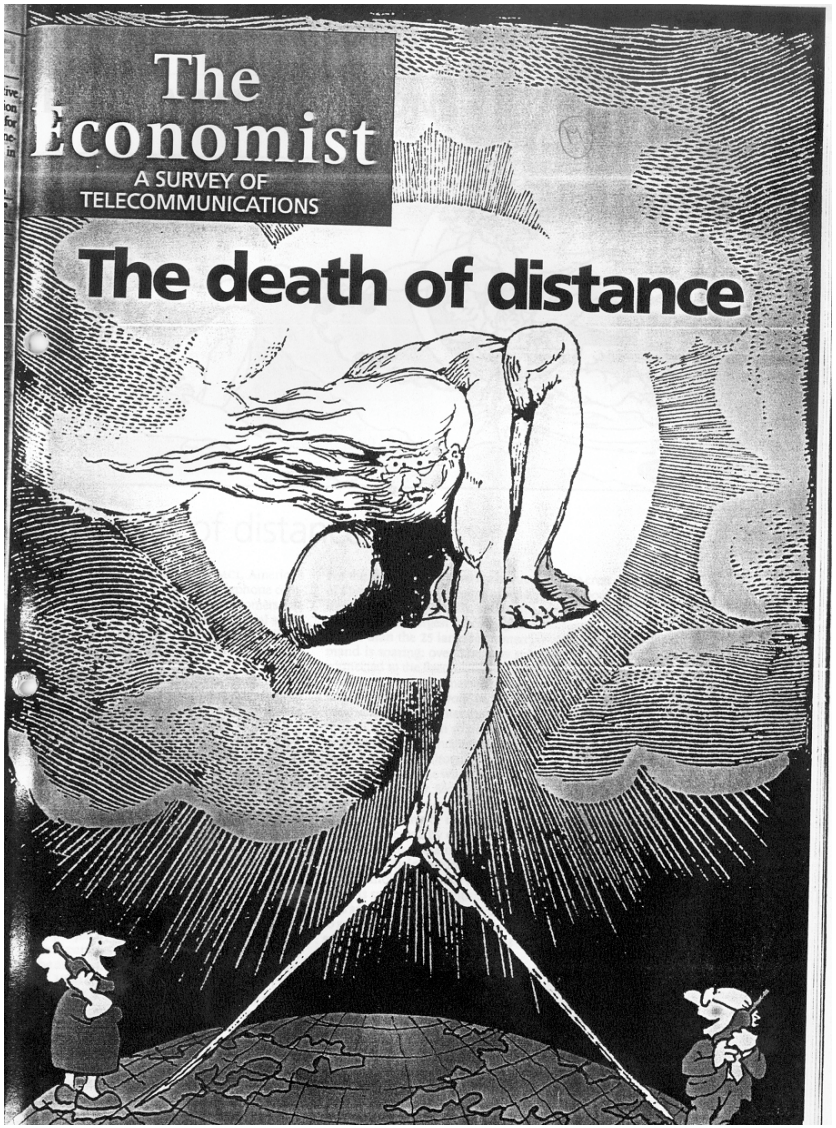
When it is as easy to hack a server 4,000 miles away as it is to hack the server next door?

Key questions:

- is location a determinant in risk and victimisation?
- is the location of the criminal important?
- can you find out where the cyber criminals are?

# Cyberspace - spaceless space, placeless place?

## death of distance / resurrection of geography




20th September 1995


11th August 2001

# Defining cybercrime

- cybercrime is crime that can only take place in cyberspace
- cybercrime is online crime and not simply crime online
- cybercrime is made possible by the space-adjustments and power adjustments afforded by global networks
- key types
  - scanning (‘looking for unlocked doors’)
  - intrusion (breaking-in and trespass)
  - vandalism and damage (defacement, deleting file, altering data)
  - denial of service (DOS)
  - viruses (malware, email viruses, worms, trojans)
  - [ spam?? ]
- different from ‘traditional’ crime
  - cybercrime is not same crime just using computers and networks
  - cybercrime is not theft of computer hardware, software piracy, copyright infringements, internet fraud

# Geography and crime

- traditionally most crime is local
- criminal, crime, victim are all co-present at same place
- many times victim and offender know each other
- journey to crime usually quite short
- evidence at the scene or nearby
- usually investigated by local LEA
- cross-border and truly international crimes require considerable effort and resources. relatively rare
- cybercrime
  - victim are usually geographically remote, possibly half a world away
  - importance of the sense of anonymity and spatial isolation from operating online. reducing the risks of getting caught

# Who are the cyber criminals?

- hackers or criminal crackers
- black hats, white hats, grey hats
- terrorists or a hacktivists
  - increasing criminalisation of action. what are the boundaries of legitimate protest and civil unrest and criminal and terrorist action?
- terrorists or cyber warriors
- foreign intelligence and state info warfare
- insiders - disgruntled employee
- script kiddie (no criminal intent?)
- stereotypes about their characteristics / demographics? typical nerd (male, intelligent, teens-to-thirties, educated, poor social-skills)

# Hacker motives?

- often difficult to determine from outward actions
- expressed motivation may not be genuine
- not all criminal intent,
- curiosity, exploring networks, challenge
- thrill of the forbidden, just trespassing
- mercenaries. cracking for money -> criminals
- shock tactics. attention seeking
- social and political motivations. highlight the cause,
- anti-corporate; anti-globalisation.
- challenging government regulation and draconian controls. expression of freedom
- expressing anger against the world

# Criminal motivations?

- black hats. Insiders, criminal groups, corporations, sub-state terrorist / freedom fighters, states cyber-warriors
- damage, corrupt data, steal information
- mercenaries. espionage to order
- revenge at the company
- attacking harder targets. not just going after opportune targets that are most insecure
- more sophisticated
- don’t want the publicity
- they know what they are doing is illegal. better understand the risks
- want to break-in undetected and leave without a trace
- more likely to exploit geography and space-adjusting power of cyberspace

# Hacking tactics

- alert to new vulnerabilities and exploits
- software and systems are increasingly complex. often not managed competently. holes are not patched everywhere
- social engineering
- there are *always* insecure targets
- mass scanning and automated tools
- use of third-party ‘zombie’ machines
- Internet monoculture makes for vulnerabilities. once one is broken, all are breakable
- importance of social networks of hackers on irc, web boards, etc for sharing tips and peer recognition

# Locating cybercrime?

- 4 ‘actors’ in cybercrime
  - location of the criminal(s)?
  - location of target(s)? does this matter?
  - location of victim (individual, company, organisation, government). multiple victims
  - location of law enforcement agencies (LEA). cooperation between agencies in different countries
- location - latitude/longitude; legal jurisdiction; network topology (which ISP)
- location to a street address and building or just the institutional geography
- location of all ‘actors’ can be different
- deliberately concealing location (spoofing); using third-party locations to launch crime.

# Where are the bad guys then?

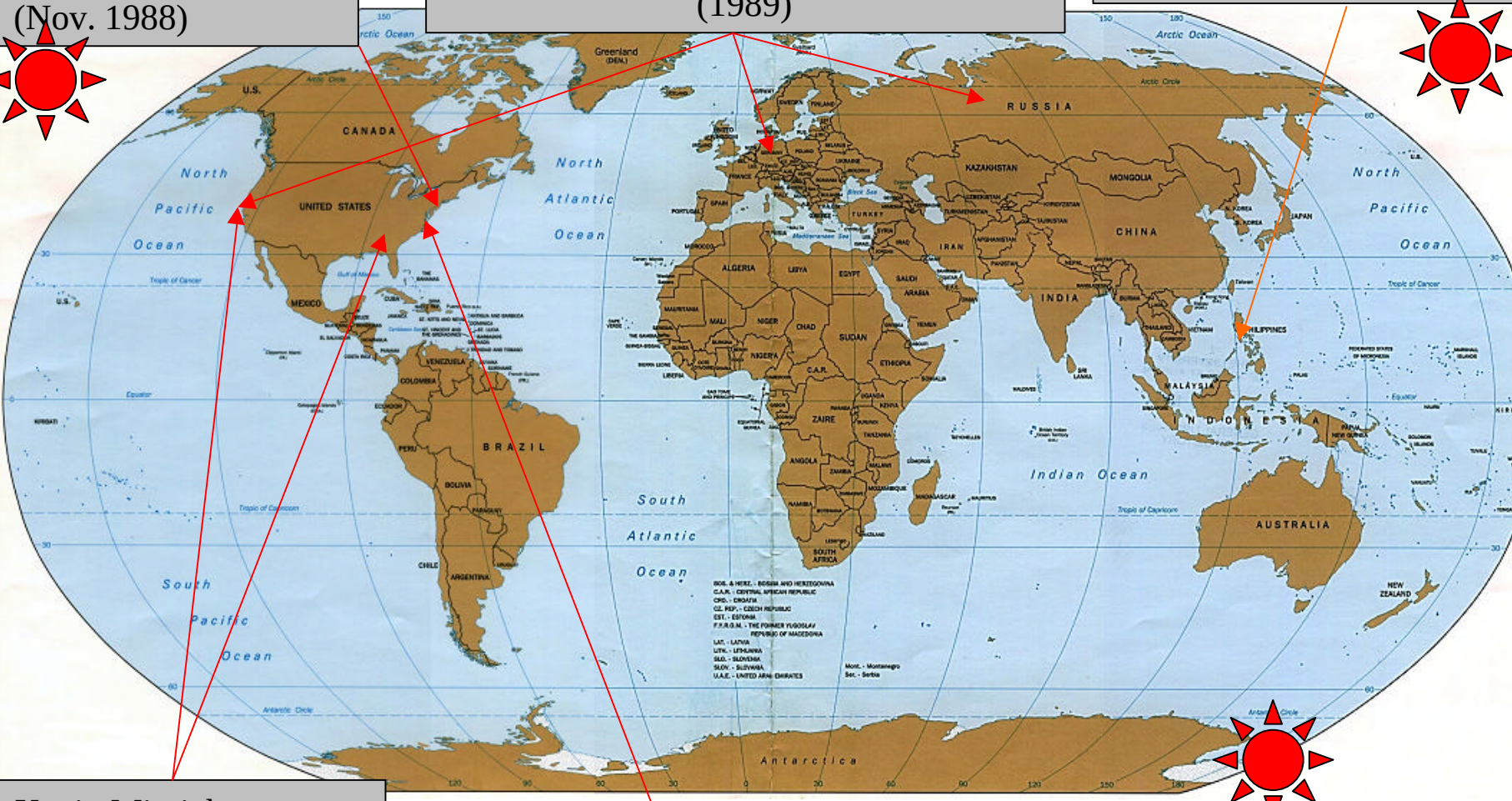
- popular coverage of cybercrime does not give a representative picture
- often presented as a new threat from the ‘others’, coming from ‘dangerous parts of the world’. overtones of racism
- geopolitical stereotyping of particular countries
  - Russia (home of global crackers - ‘toxic blend of organised crime and government corruption’)
  - Bulgaria (source of all those computer viruses)
  - South Korea (lots of ‘zombies’ and the source of spam)
  - Nigeria (those infamous spam letters)
  - China (major threat of info warfare)

# Cybercrime 'hype' - some high profile incidents

Morris Internet Worm, Cornell Univ. student (Nov. 1988)

'Cuckoo's Egg', Clifford Stoll (UCSB) West German 'cyberspies' -> Soviet KGB (1989)

LoveBug virus (May 2000), Philippines; world wide effe




Kevin Mitnick, arrested Raleigh, NC ( Feb, 1995); tried in LA

Melissa virus (March 1999), David Smith, New Jersey; impact is world wide

Code Red worm (July 2001), unknown origin, rapid world wide impact

# The MafiaBoy distributed denial of service attacks

DDOS attack used widely dispersed number of ‘zombie’ PCs, estimates of 75 different countries

Suburban Montreal

Computer crime squad of RCMP in Montreal


Amazon

FBI field office Portland

eBay, Yahoo!

Buy.com

E*Trade

DELL

CNN.com

FBI's National Computer Crime Squad, Washington DC

“This was a crisis that many experts had been warning about for years. Nothing less than the public’s confidence in the future of the Internet economy was at stake.”, Dan Verton, National Post, 25th May 2002

# The MafiaBoy case, spring 2000

- global scale denial of service attack, shows some of the potential of cybercrime to cause economic damage
- launched from bedroom in suburban Montreal; classic case of super-empowered individual (14 y.o. boy)
- multiple high-profile targets
- left clues, not very sophisticated. but difficult to track; much effort and several different ISPs used; several LEAs
- geography matters - you still need to find the right house
- required lengthy ‘wiretap’ of suspects house.
- needed to determine who was actually sitting at the PC during the attacks
- Sept. 2001 sentenced to 8 months juvenile detention

# Why geography matters?

## 1. Justice

- no handcuffs in cyberspace
- LEA needs to find the perpetrator in the ‘off-line’ world
- cyberspace is an a embodied space
- justice and punishment are centred on the physical body in fixed geography space
- “*The body is the locus of criminality and deviance, as well as punishment, justice and correction. It is identifiable, definable, and confinable*.” (Source: Douglas Thomas, *CyberCrime: Law, Security and Privacy in the Information Age*, Routledge, 1998, page 29)
- LEA and judicial systems based on fixed territorial units
- importance of legislative and institutional geographies which vary from country to country

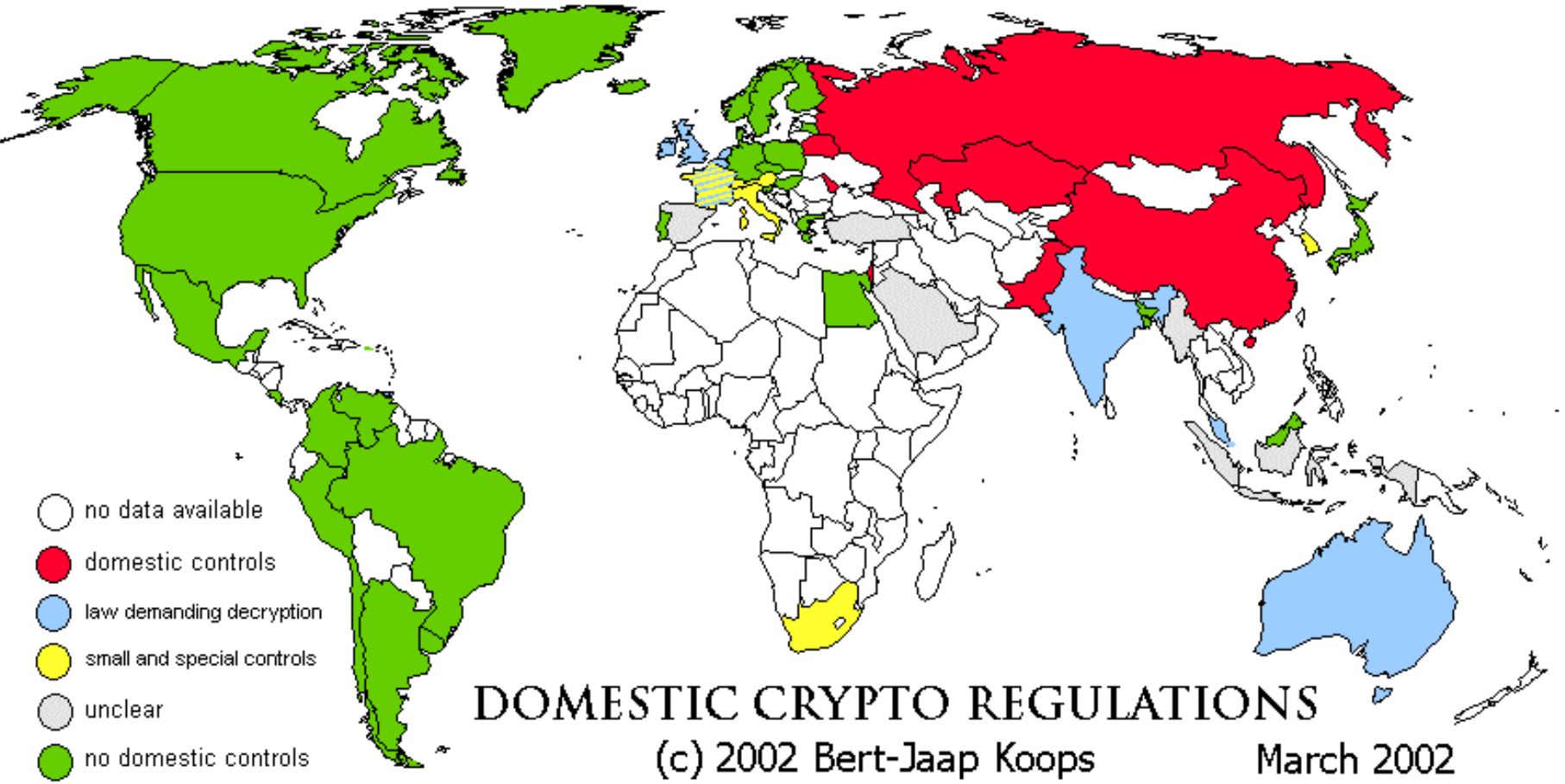
# Differences in cybercrime legislation, December 2000

| Figure 2: Countries with Updated Laws | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Country | Data Crimes | | | Network Crimes | | Access Crimes | | Related Crimes | | |
| | Data Interception | Data Modification | Data Theft | Network Interference | Network Sabotage | Unauthorized Access | Virus Dissemination | Aiding and Abetting Cyber Crimes | Computer-Related Forgery | Computer-Related Fraud |
| Australia | ✔ | ✔ | ✔ | ✔ | | ✔ | | | ✔ | ✔ |
| Brazil | | ✔ | | | ✔ | ✔ | | ✔ | | |
| Canada | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | | ✔ |
| Chile | ✔ | ✔ | ✔ | ✔ | ✔ | | | | | |
| China | | ✔ | | ✔ | | | ✔ | | | |
| Czech Republic | | ✔ | ✔ | | ✔ | ✔ | | | | ✔ |
| Denmark | | ✔ | | ✔ | | | | | | ✔ |
| Estonia | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ |
| India | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ |
| Japan | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ |
| Malaysia | | ✔ | | | | ✔ | | ✔ | | ✔ |
| Mauritius | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | |
| Peru | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | | | ✔ |
| Philippines | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Poland | | ✔ | ✔ | ✔ | | | | ✔ | | |
| Spain | ✔ | ✔ | ✔ | | | | | ✔ | | ✔ |
| Turkey | | ✔ | ✔ | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ |
| United Kingdom | | ✔ | | ✔ | ✔ | ✔ | | ✔ | | |
| United States | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | | ✔ |

(source: Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information,

# Summary of crypto controls by country

by Bert-Jaap Koops, March 2002



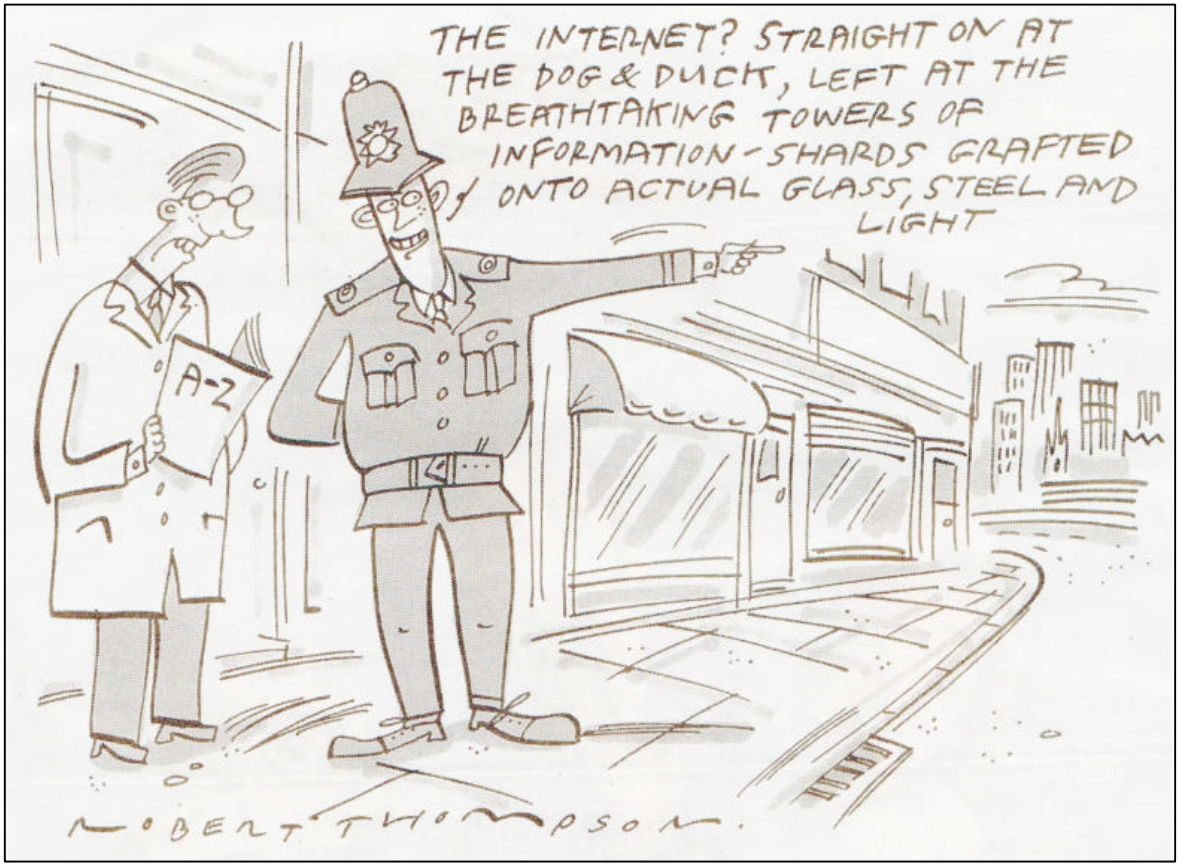

(Source: <http://rechten.kub.nl/koops/cryptolaw/cls-sum.htm>)

# Why geography matters?
## 2. technical and infrastructure

"*Nevertheless, the Net cannot float free of conventional geography. Not a single bit could pass through it without miles of copper wire and glass fiber, as well as tons of computing hardware – all of which is very much situated in the physical world. The cables and routing centers of the Internet have specific coordinates on the earth's surface, even if users of the network seldom give much thought to where their bits are going.*"

(Source: Brian Hayes, The infrastructure of the information infrastructure, *American Scientist*, May-June 1997, Vol. 85, No. 3, pages 214)

# Why geography matters?




• where are the wires? where are the servers? data is served from somewhere and delivered to to somewhere

• vital to understanding the geography of network infrastructure

# Why geography matters?

- invisibility of network infrastructure
- infrastructure is diverse - local, national, global, satellites, mobile/wireless; different technologies and protocols
- infrastructure has many owners and operators
- borderless geography. global networks. seamless data flows, cross multiple countries, timezones and jurisdictions
- where should the LEA place their wiretaps?
- cybercrime happens somewhere (x,y). the attacked server(s) have a geographical footprint
- the attack is launched from somewhere (x,y)
- data trails are left

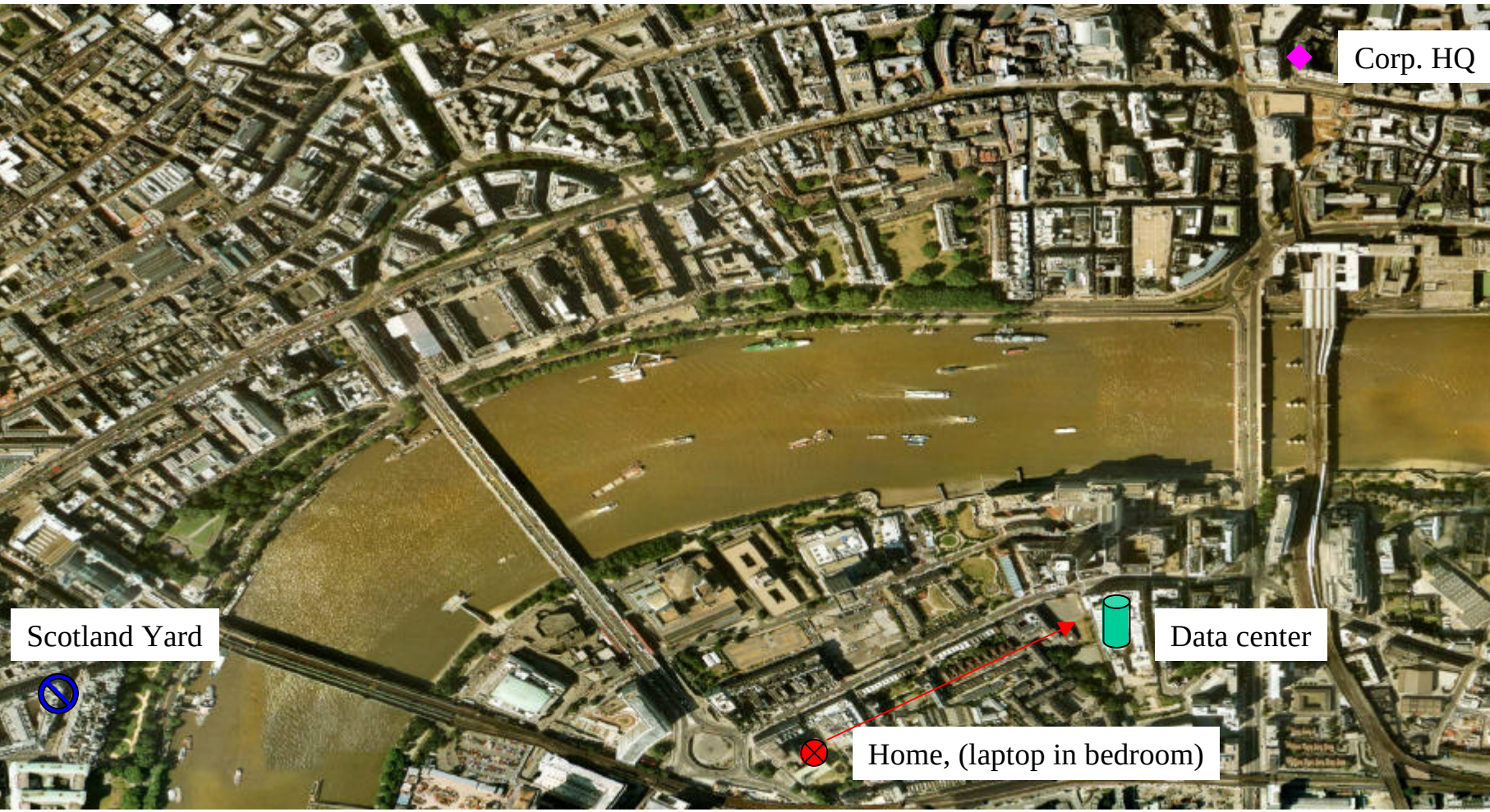
# Geographic scales of cybercrime

- conceptualisation as a hierarchy of five scales:

1. local (within the same organisation / building; within the same city)
2. national (within the same political / legal jurisdiction)
3. regional (cross border, but connected)
4. international (transcontinental)
5. global

# Local scale cybercrime

disgruntled employee breaks into their company's system. Criminal, target, victim, and LEA are all in the same city within a few miles of each other




= offender = target = L.E.A

= victim = crime vector


# National scale cybercrime

Hacktivist defaces government department website as a political protest.

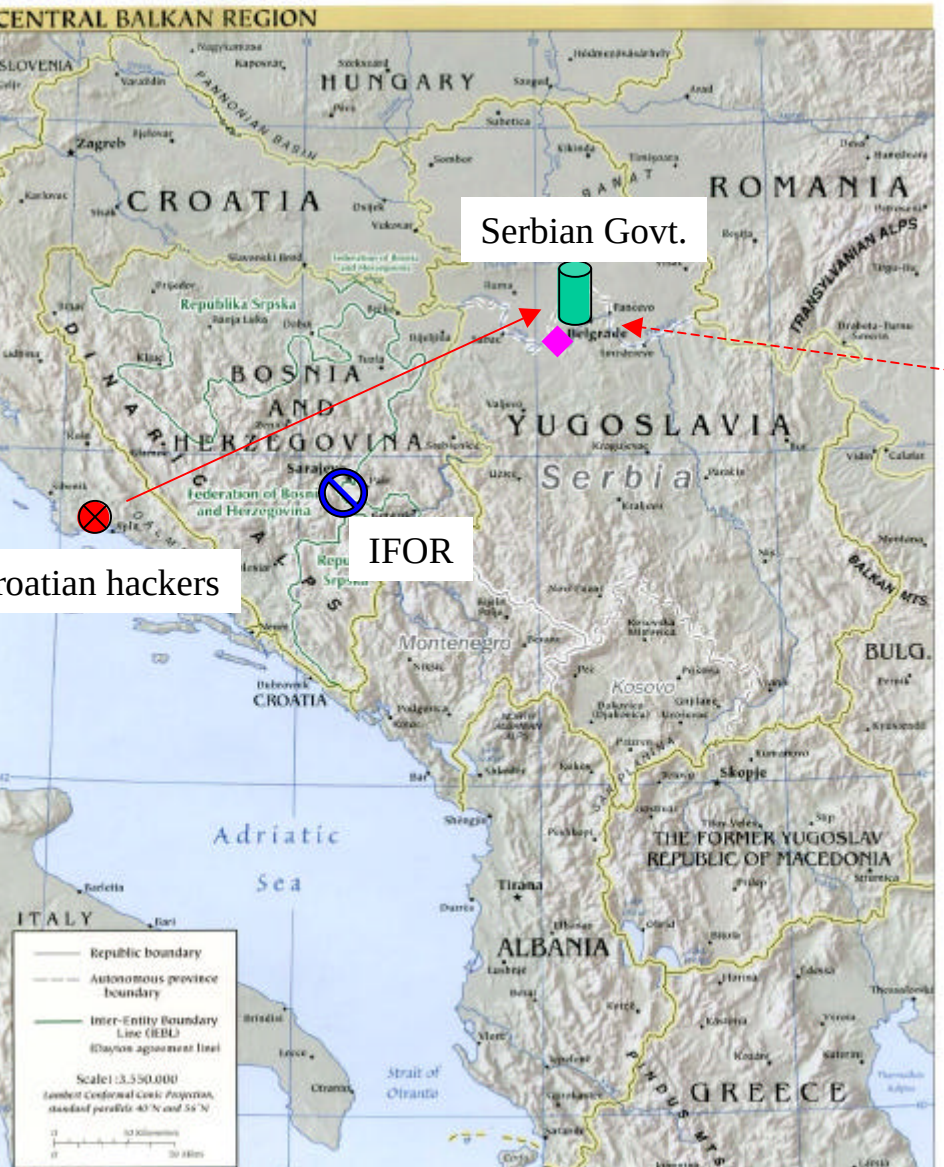
All actors are geographically distant, and not directly connected. Crucially, however, they are within one country and so are all in the same jurisdiction.

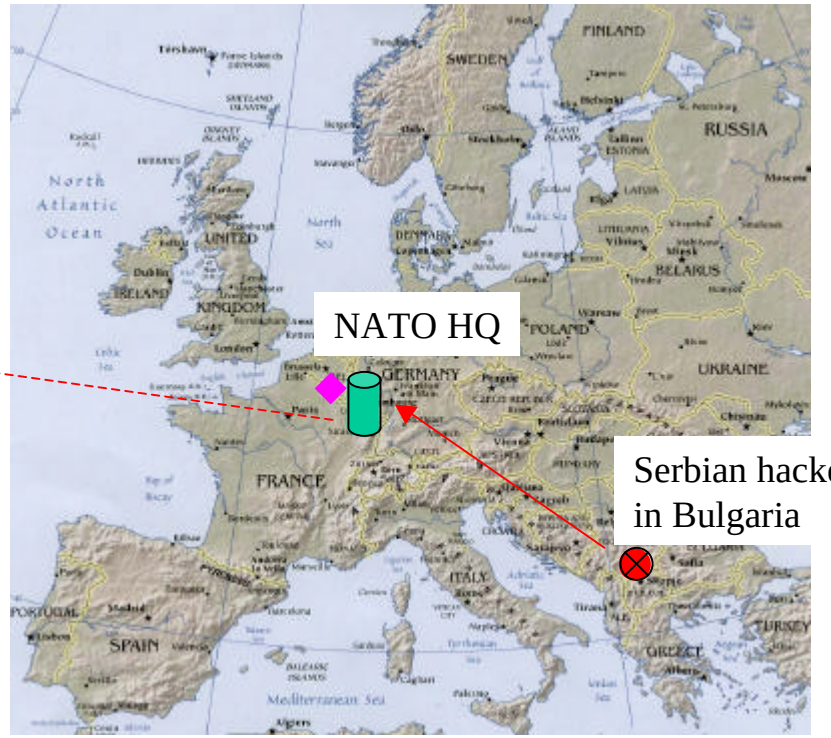
= offender = target = L.E.A

= victim = crime vector

# Regional scale cybercrime

## DOS and defacement attacks as part of the Balkans conflict




Serbian Govt.

NATO HQ

IFOR

roatian hackers

Serbian hacke
in Bulgaria

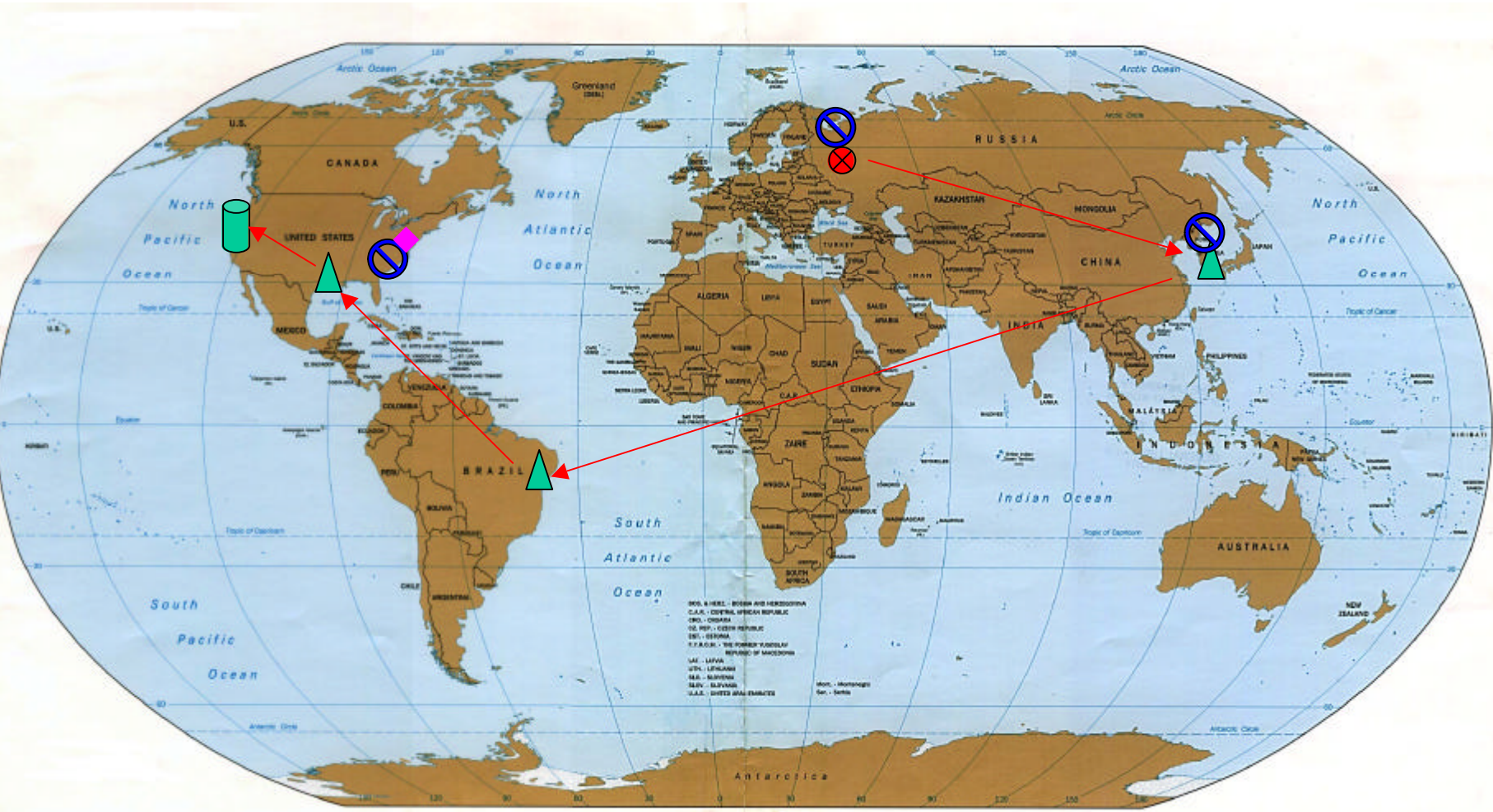
Multiple actors, in multiple countries and jurisdictions.
But with definite relationships.

= offender = target = L.E.A

= victim = crime vector

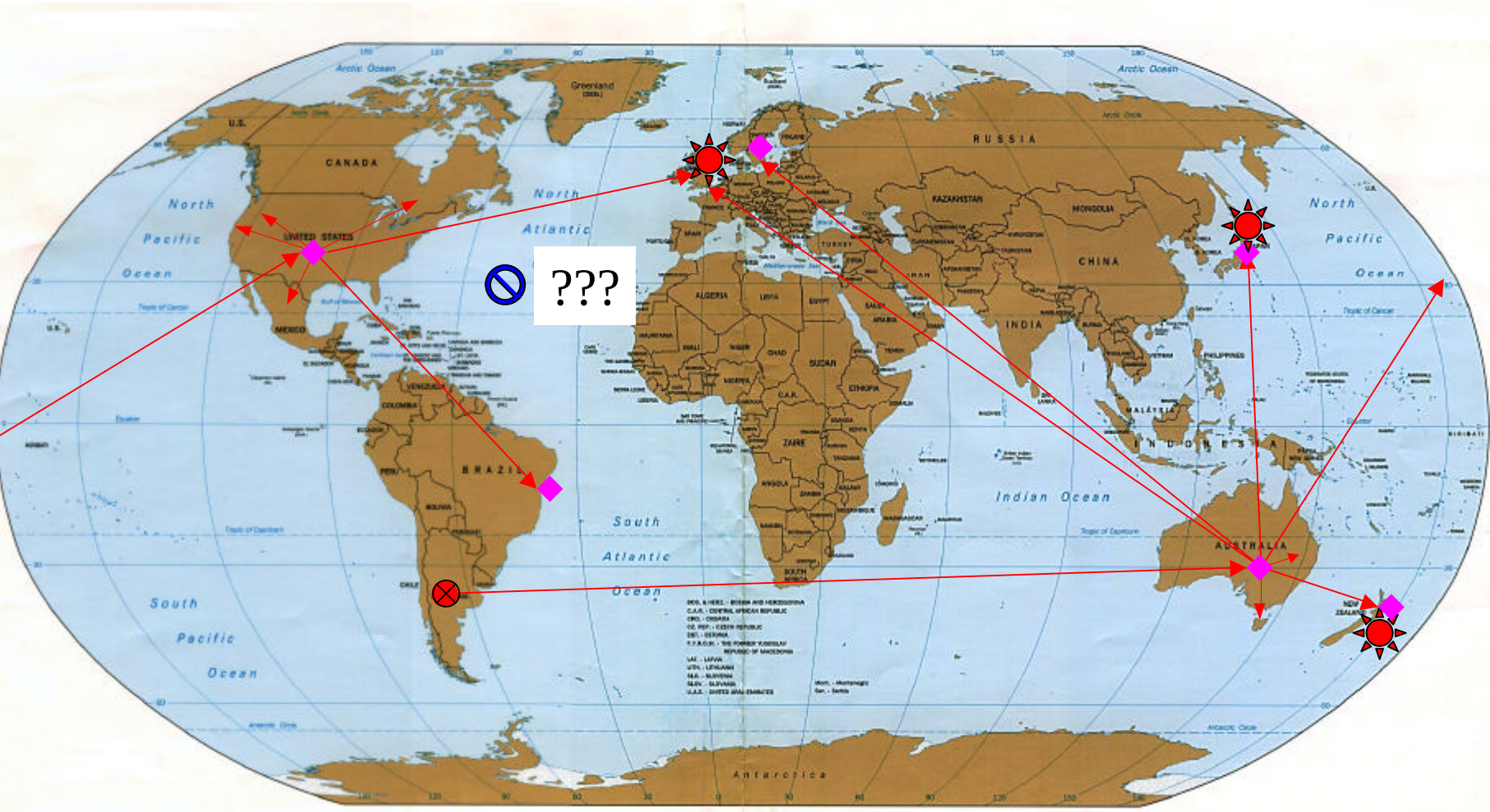
# International scale cybercrime

Russian mafia hire hackers to break security of a US bank. Hackers use multiple intermediate computer systems and networks to cover their tracks



# Global scale cybercrime

virus outbreak, offender is in Argentina but released the virus in Australia. It spreads across the globe within 24 hours. Many thousands of victims,



# Geography of website defacements

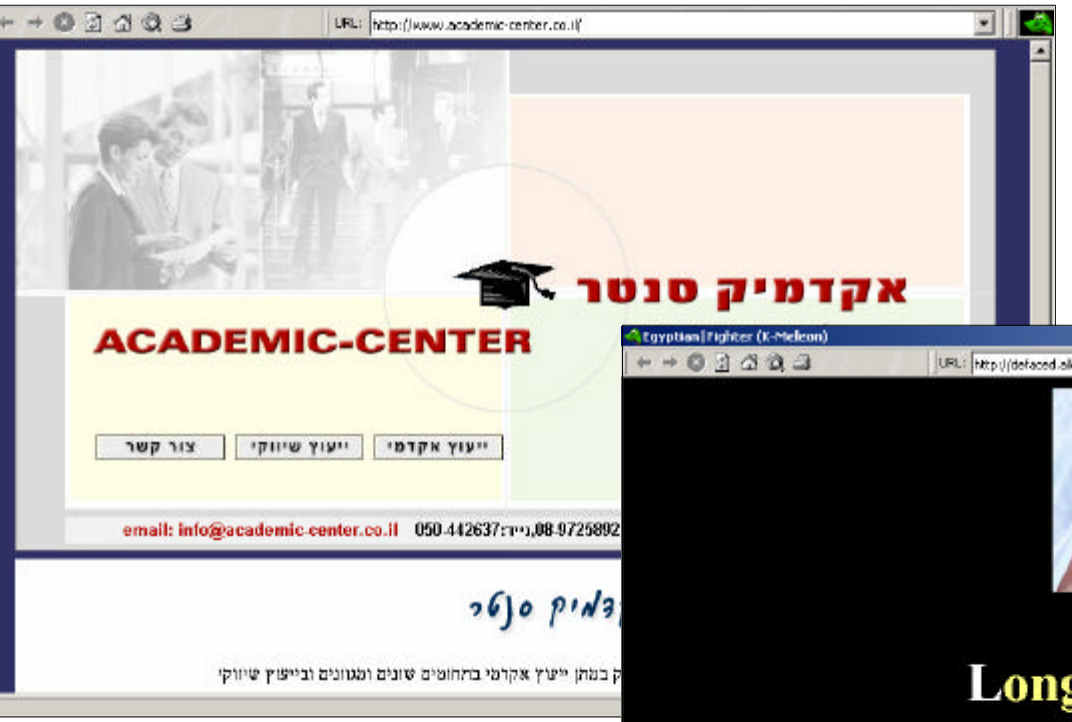
- defacement - unauthorised change to website, usually visible vandalism of the homepage
- minimal damage, but cost to reputation can be very high
- driven by available data source
- empirical case study, empirical analysis
- data source: Alldas Defacement Archive <http://defaced.alldas.org> (+ Netcraft, www.netcraft.com)
- total: 30,668 incidents (from Jan. 1998 - May 2002)
- countries: 151
- top five countries: US (10,795), Brazil (2,348), China (1,487), Taiwan (1,344), Korea (1,007)

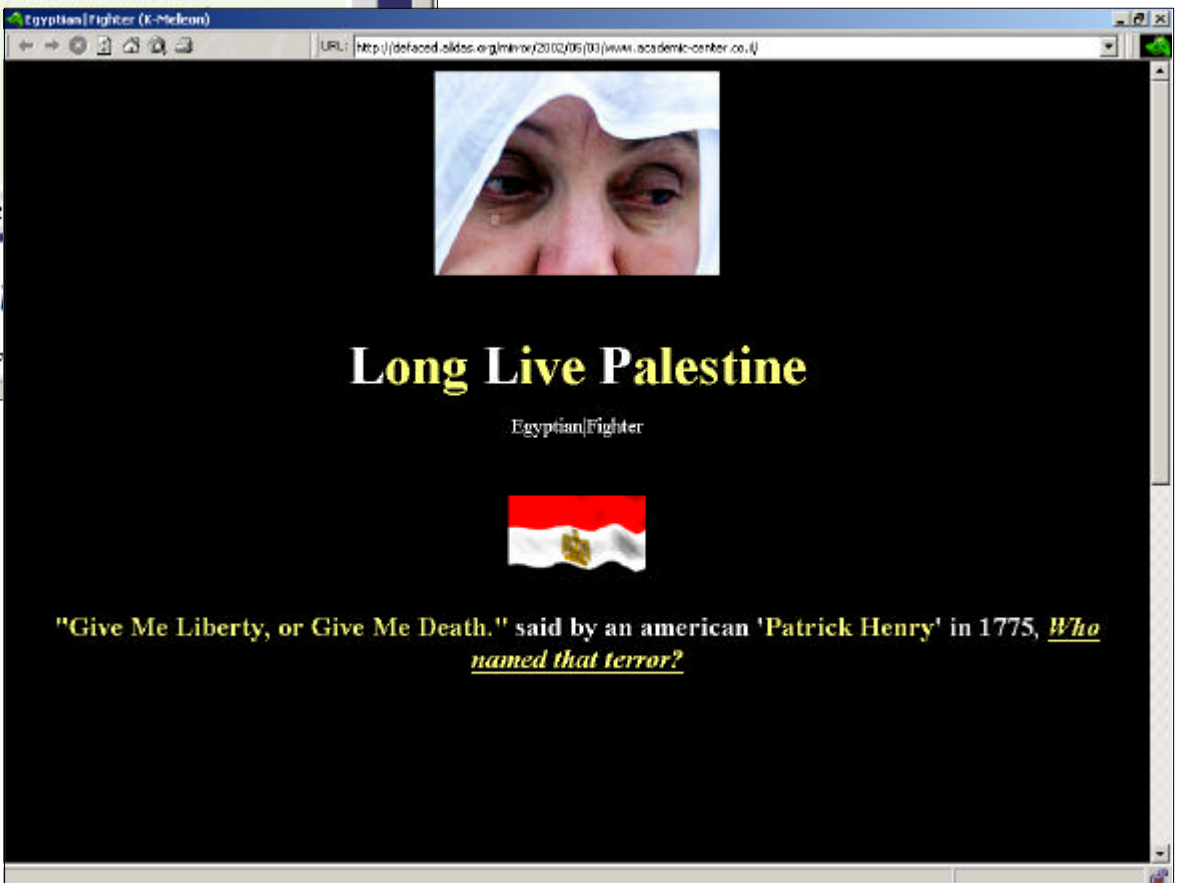
# Defacement is not new

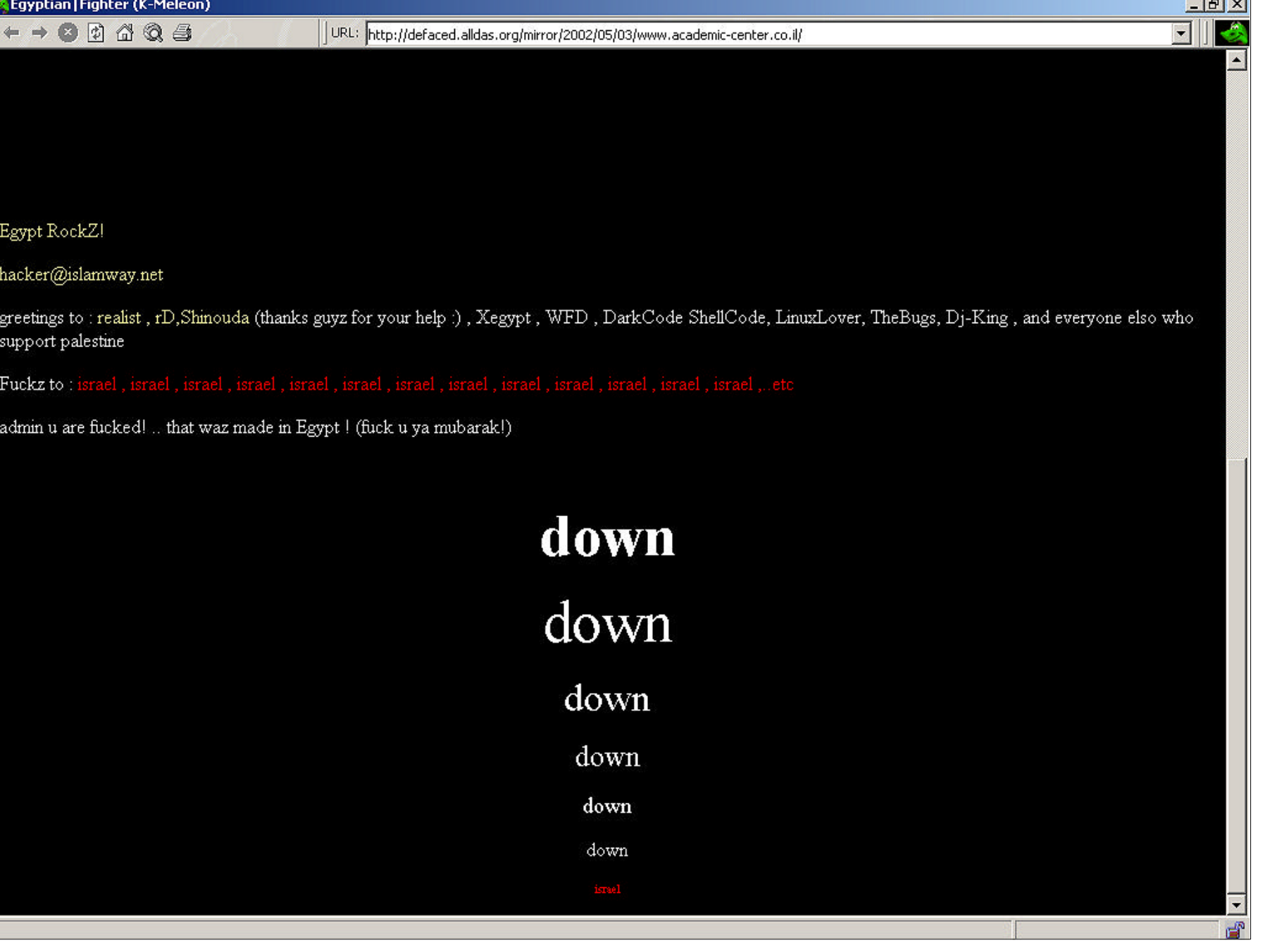

Vandalism or defacement of Winston Churchill's statue as part of May Day, Reclaim the streets protests, 2000


Culture jamming <http://www.adbusters.org>

# Defacing Israeli websites




Egyptian|Fighter (K-Meleon)
URL: http://defaced.alldas.org/mirror/2002/05/03/www.academic-center.co.il/
Egypt RockZ!
hacker@islamway.net
greetings to : realist , rD,Shinouda (thanks guyz for your help :) , Xegypt , WFD , DarkCode ShellCode, LinuxLover, TheBugs, Dj-King , and everyone elso who support palestine
Fuckz to : israel , israel , israel , israel , israel , israel , israel , israel , israel , israel , israel , israel , israel ,..etc
admin u are fucked! .. that waz made in Egypt ! (fuck u ya mubarak!)
down
down
down
down
down
down
israel

# Four typical website defacements from 5th May 2002

Perfect.Br (K-Meleon)

URL: aced.alldas.org/mirror/2002/05/01/www.iitr.ernet.in/

File Edit View Go Bookmarks Favorites Help

URL: ed.alldas.org/mirror/2002/05/01/www.fatjames.com/

File Edit View Go Bookmarks Favorites Help

FUCK TO ADMIN...


we are [ [
[ D1G_D1G ]

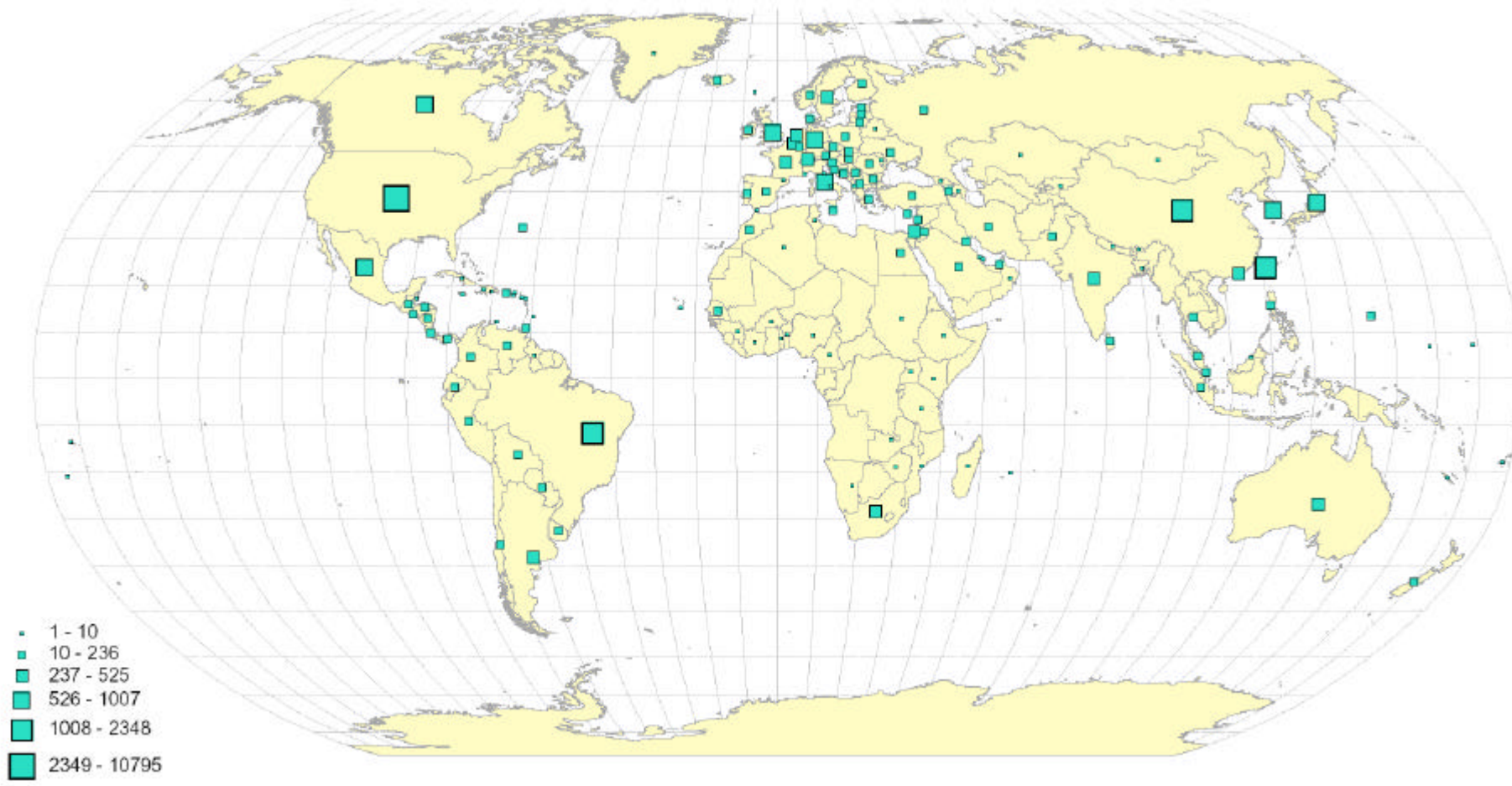
] contact [
[ d1g_d1g@hackermail.com ]

] irc [
[ irc.brasnet.org - #virtualhell ]

] greetz [
[ [ Interactive, phRoZen, TriaX, BHS, Attacked SOul, cr1m3 Org4n1z4d0

# Total number of website defacements

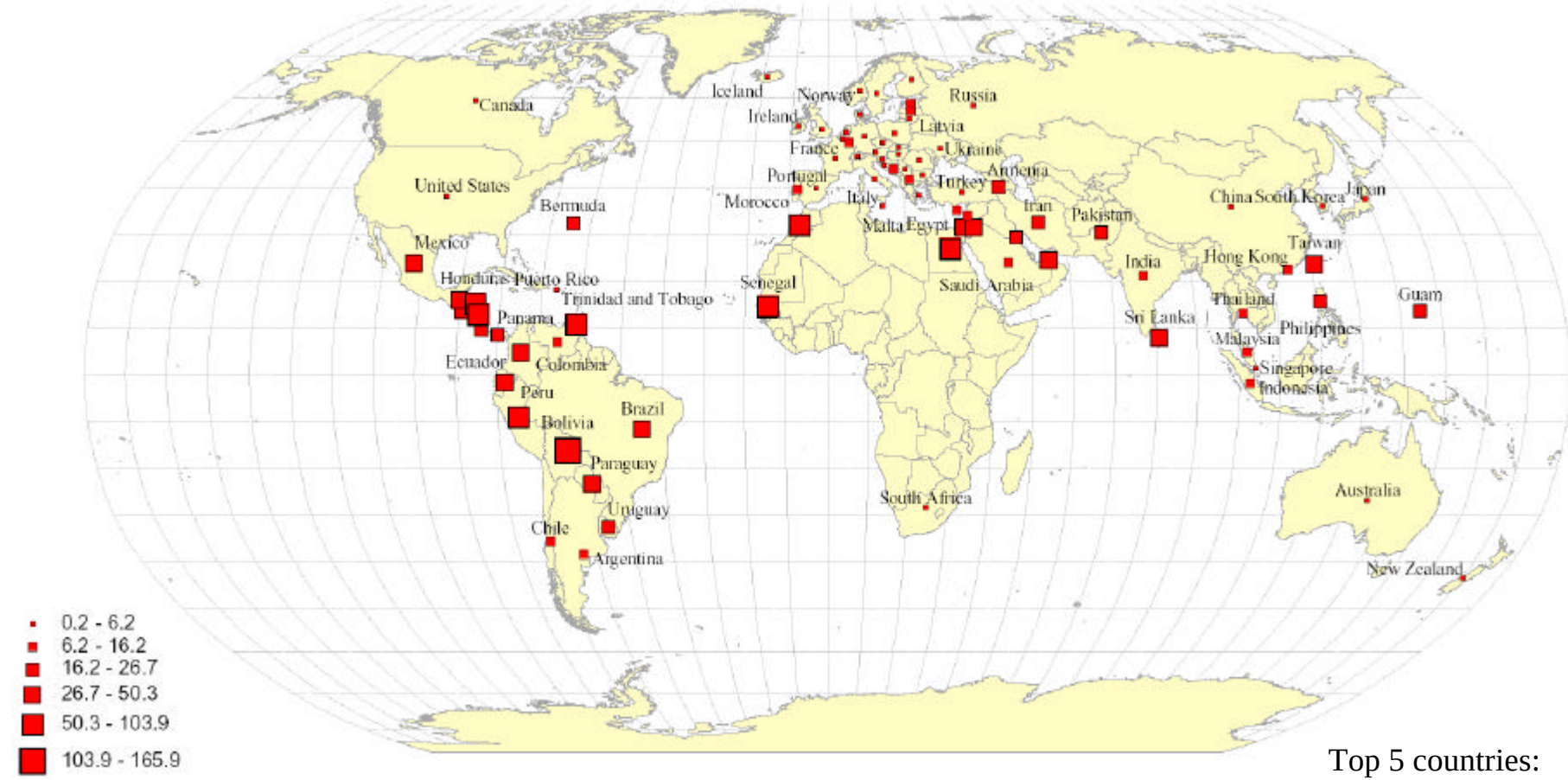
(Jan. 1998-May 2002)




(Data source: http://alldas.de/ - http://www.zone-h.org/)

# Number of website defacements per 1,000 active websites

[Excluding countries with < 10 defacements]




Total: 87 countries

Top 5 countries:
1. Bolivia (166)
2. Honduras (104)
3. Morocco (89)
4. Peru (81)

# Difficulties in analysing geography of cybercrime

- role of geography is still debatable?
- can you actually determine location?
- paranoia, hype and misinformation
- can you get representative data? no one gathers comparable data
- many (most) incidents not detected or not reported
- most reports produced by companies / agencies with a particular agenda (to boost the threat of cybercrime!)
- much more research to be done