

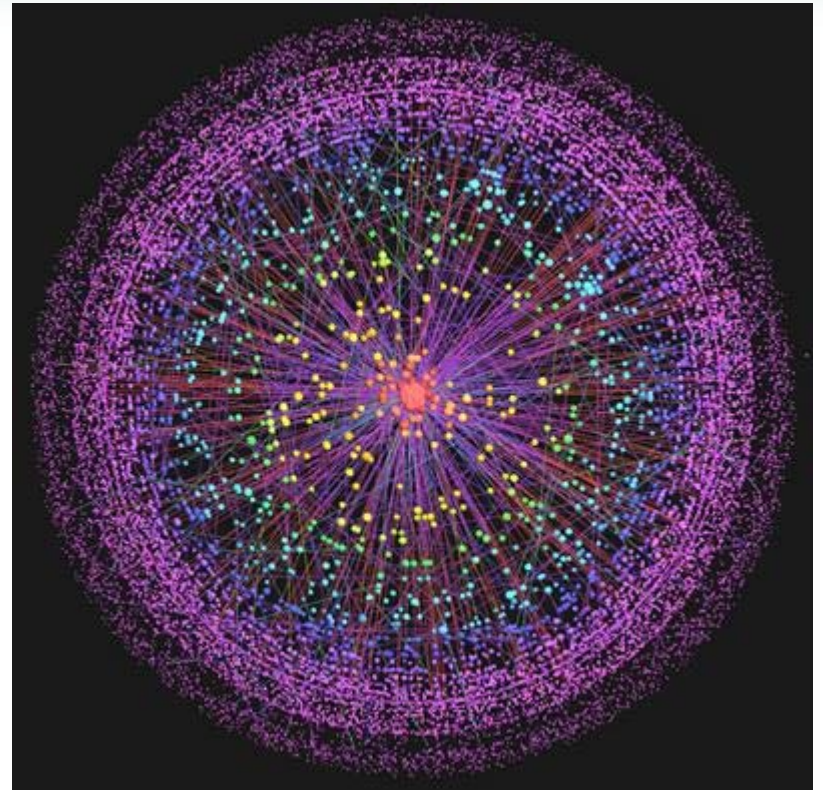
# CYBERCRIME, CYBER-WARFARE, NETWORKS AND RESILIENCE

Andrés Guadamuz, SCRIPT

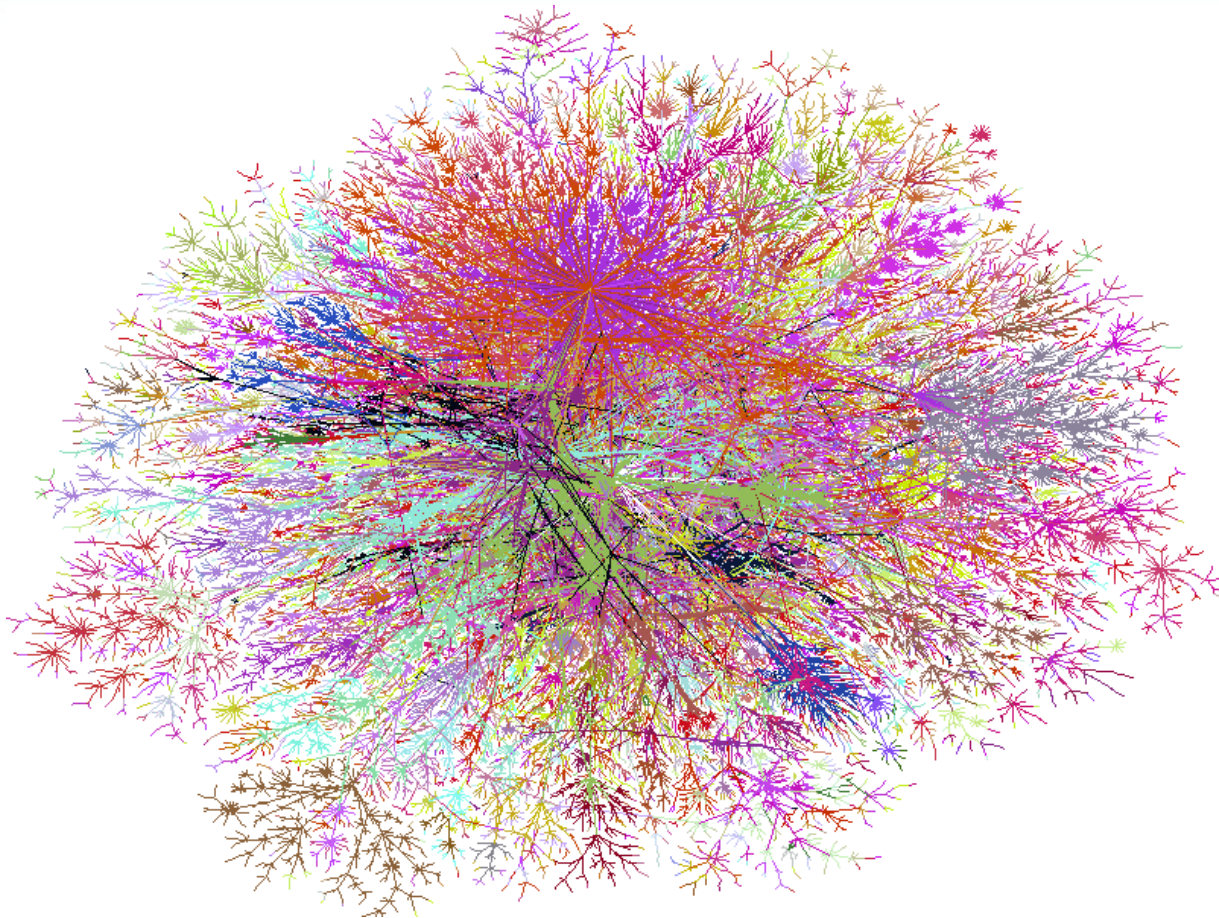
# IN THE BEGINNING...



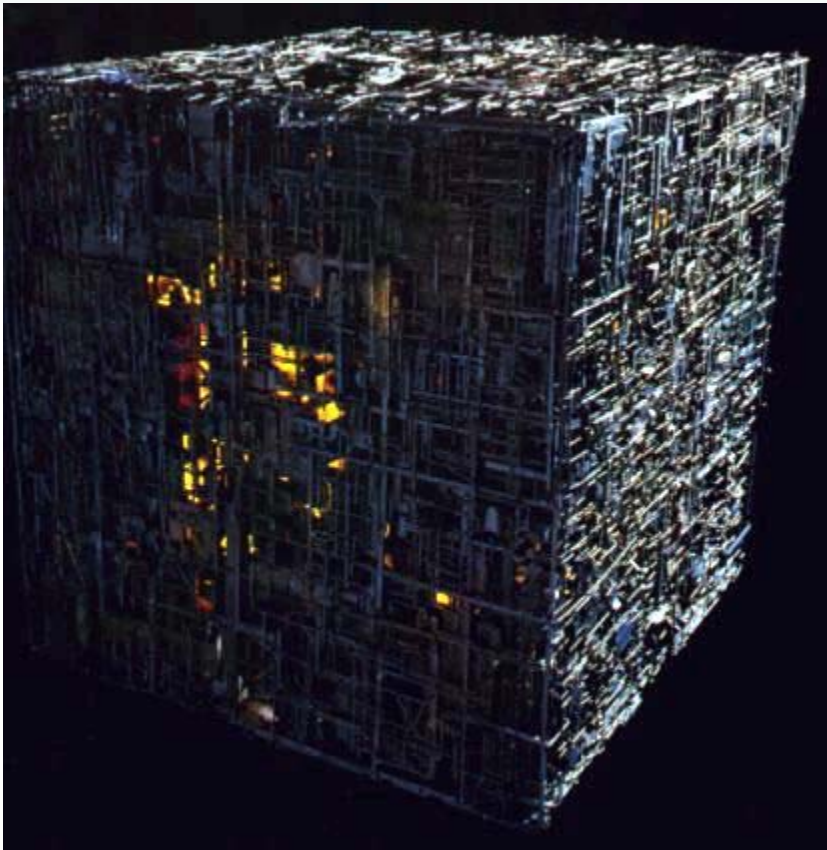
# THE WARGAMES INTERNET



# THE INTERNET AS INTENDED



# THE HIVE INTERNET

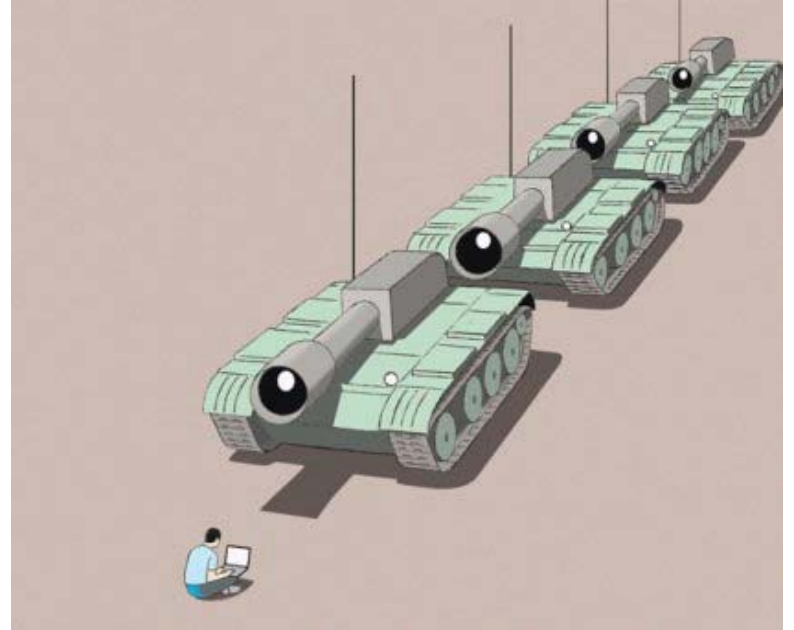




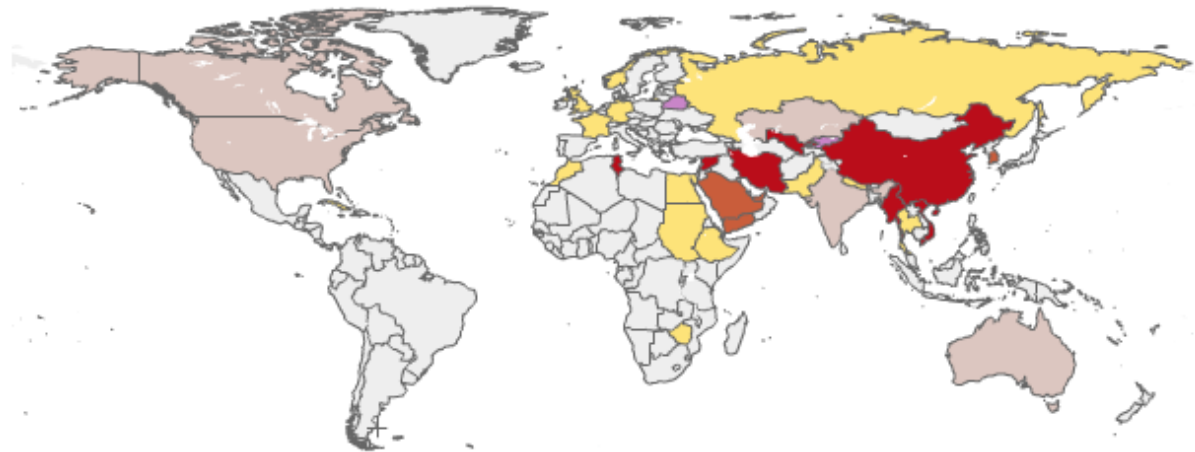
# CHARACTERISTICS OF THE HIVE INTERNET

- ⊙ Decentralised
- ⊙ Resilient
- ⊙ Fast replication of information
- ⊙ Damage to the system is rerouted
- ⊙ Difficult to regulate
- ⊙ Did I mention decentralised?

# HOWEVER...



# THE FREE INTERNET?

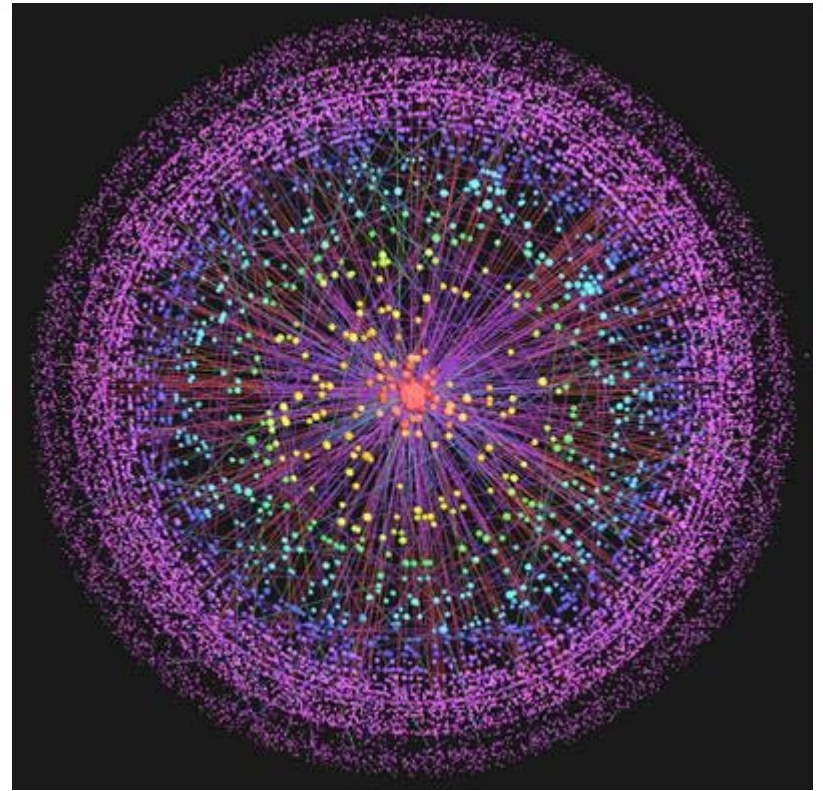


Filtering: ■ Pervasive ■ Substantial ■ Nominal ■ Indirect ■ Watchlist

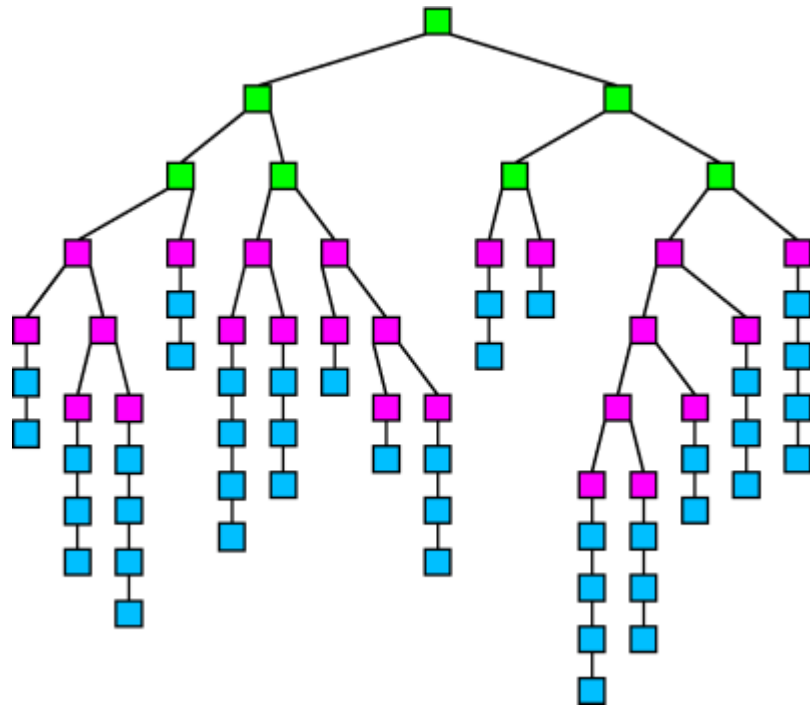
Level of cyber-censorship.

Source: *Internet Justice*

# SO WE ARE BACK TO THE 80S



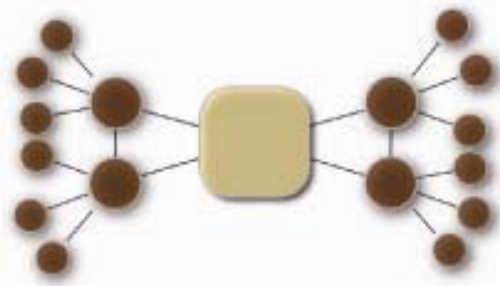
# CASCADING FAILURES





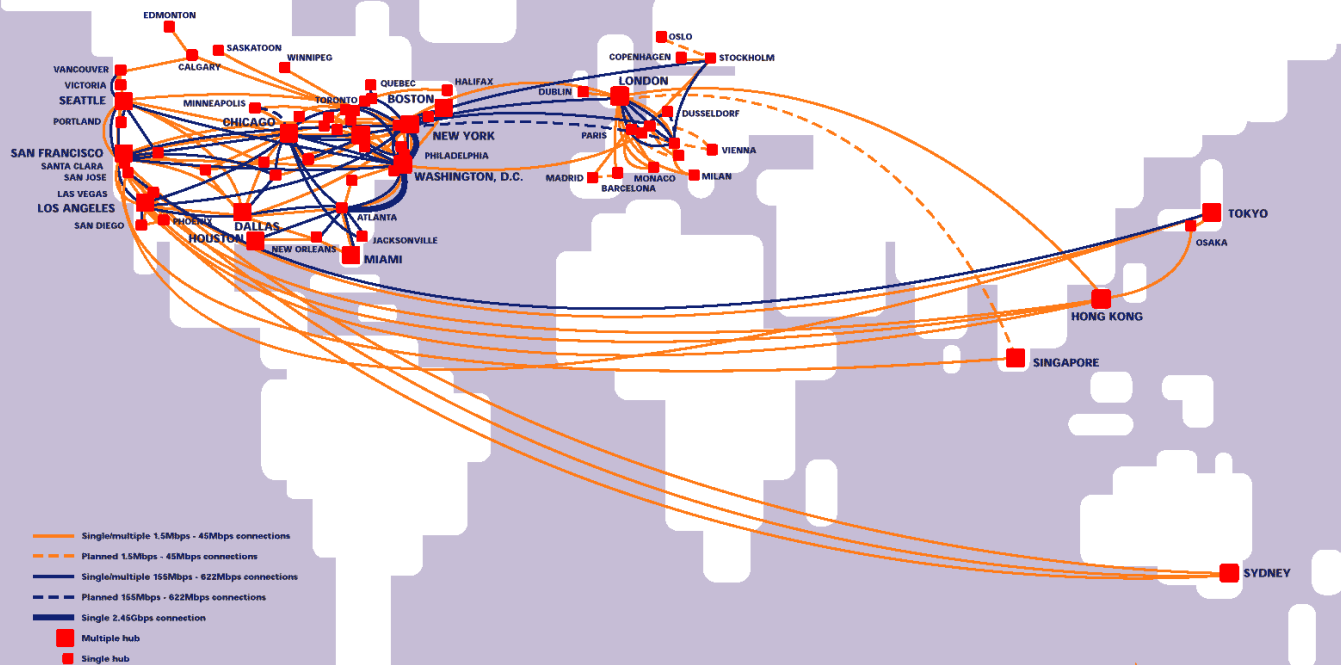
# WARNINGS OF A CENTRALISED INTERNET

- ① **The Central American Capsize:** (Dec 2007) A submarine fault eliminates all broadband speed for all Central America.
- ① **The Pakistani Panic:** (Feb 2008) Pakistani censorship instruction gets infected to the entire internet, blacking out YouTube for hours.
- ① **The Scorpion Scandal:** (Dec 2008) UK's Internet Watch Foundation blacklisted a Wikipedia page containing a morally dubious album cover from German band Scorpions. This affected normal service across several ISPs.



# CONNECTEDNESS

## UUNET's Global Internet Backbone



For more information visit [www.uu.net](http://www.uu.net)

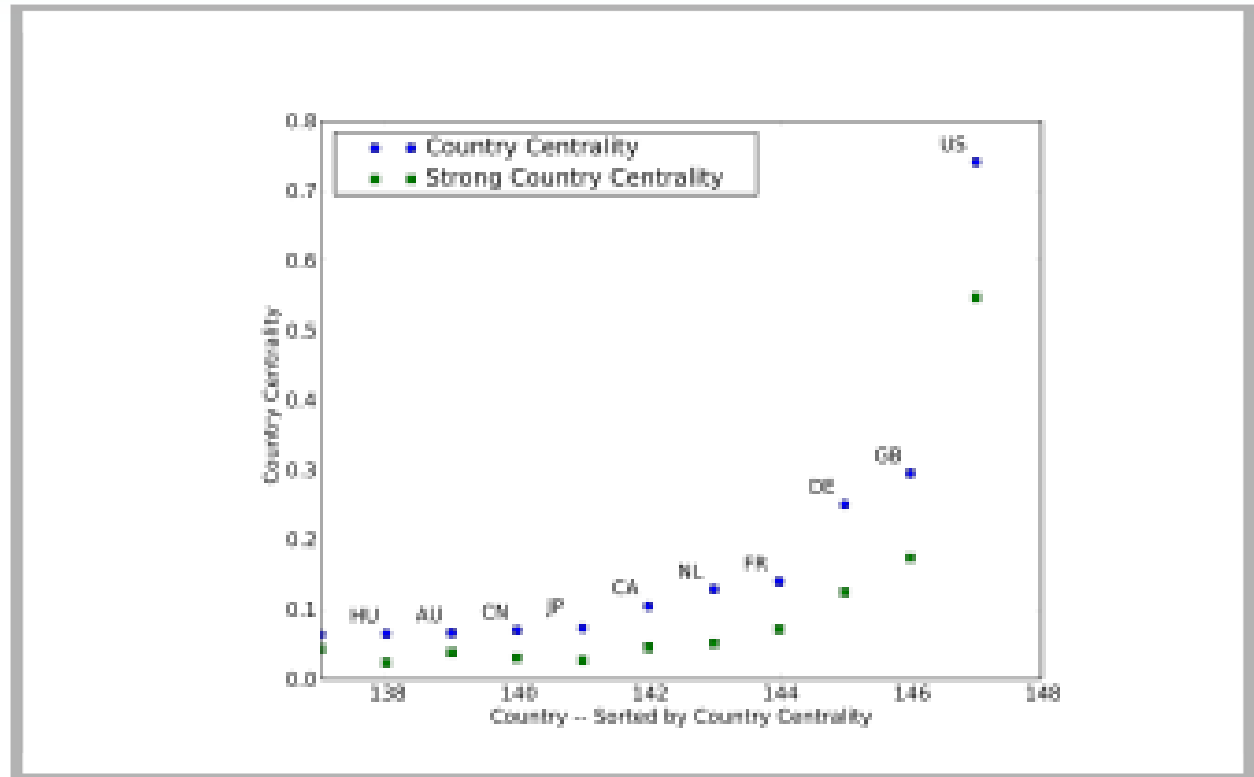
NB: With the exception of North America, Spain & Germany, all major 'in-country' links have been excluded from this map. 'In-state' links within the USA have also been excluded.

This does not constitute a solicitation of any former MCI customer whose dedicated Internet access service was transferred to Cable & Wireless unless the customer was also a WorldCom company Internet services customer as of the MCI/WorldCom merger.



# COUNTRY CENTRALITY

Source: *Nation  
State Routing,  
Censorship  
Wiretapping and  
BGP* (Karlin et al)





# CYBER-WARFARE

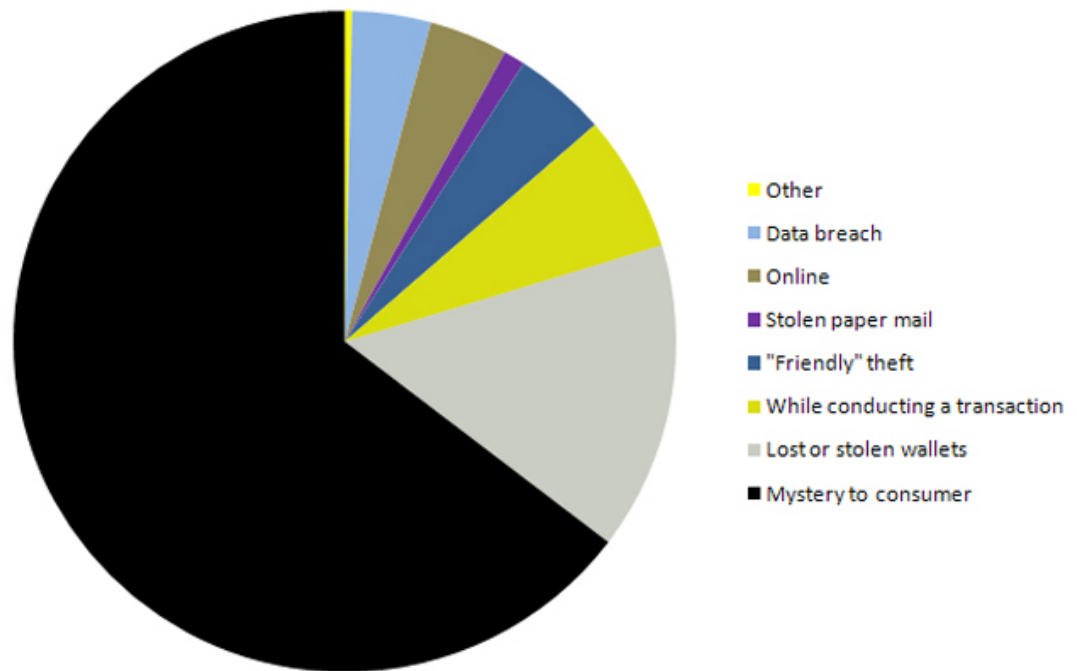
- ◎ **May 2007:** Estonia hit by cyber-attacks that bring down much of the e-government infrastructure.
- ◎ **August 7, 2008:** Russian intelligence accused of releasing instructions to the Russian hacker community ahead of attack on Georgia.
- ◎ **August 8, 2008:** Georgian banks, telecommunication networks, government websites, and news agencies hit by hacker attacks.
- ◎ **August 8-9 2008:** Russian planes bomb Georgia, Russian navy imposes blockade.

# BEFORE SENDING IN THE TROOPS, DEPLOY THE GEEKS



# CYBERCRIME

Figure 2: What Are the Most Common Methods of Access?



# CYBERCRIME 4.0



## World of Warcraft Map Overlay of Washington, DC Photo



**WAR\_MONGER**> Come in **South East of The Zoram Strand**. Clear out all the mobs. Then we attack the **Keep** itself and use the **Spell**. The Oracle says there are **110 Gold and 234 Silver** inside. That's the real target!

**TALON238**> **110 234** Got it.

**WAR\_MONGER**> Remember, eliminate all castle guards patrolling the road to the **Keep**, and kill all other players in the area... then get clear. The **Dragon Fire** spell will be coming through the **south gates of the Keep!**

**WAR\_MONGER**> No one will dance there for **a hundred years** after this spell is cast.

# CONCLUDING...



A.GUADAMUZ@ED.AC.UK