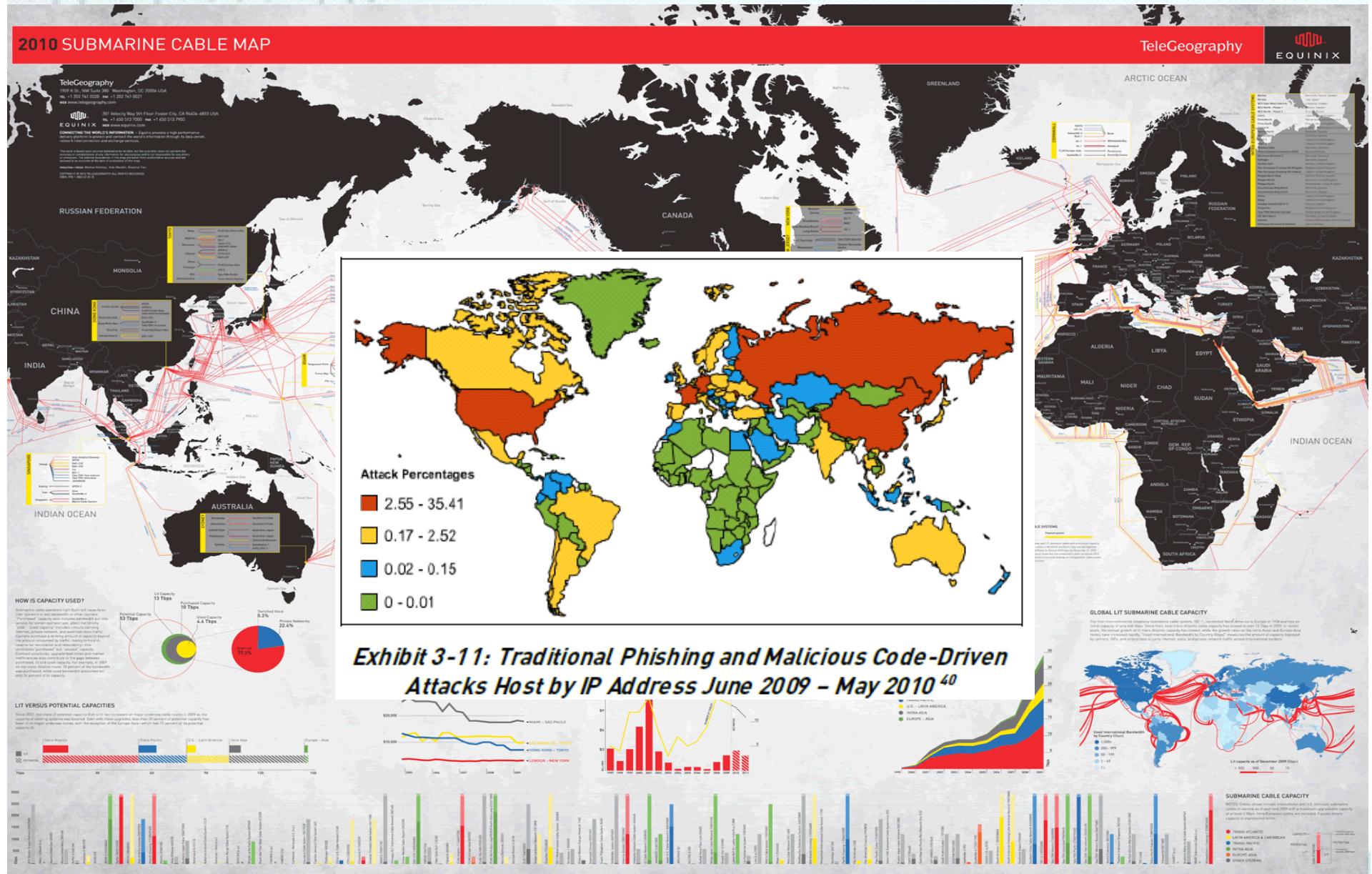


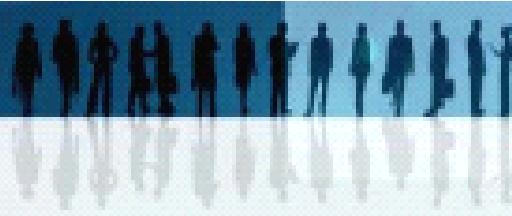


Eagle Wan @chinawill2012



About Chinese Hackers .. **You** need to ..





锣，鼓，电话延伸了耳朵

结绳，算盘，教筹，计算机延伸了大脑

望远镜，显微镜延伸了眼睛

棍棒延伸了双臂

石头，榔头延伸了拳头

汽车，火车延伸了双腿

公路，铁路，航运，飞机航线



电报机的发明

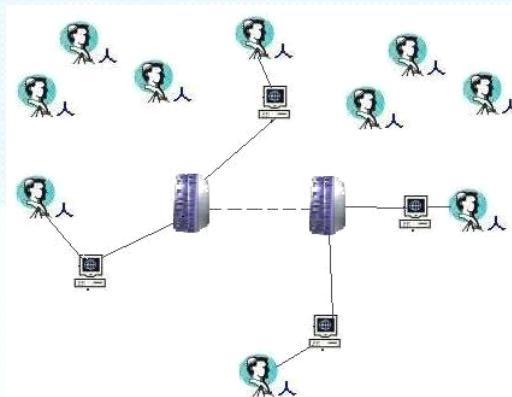
Morse码的发明

电话交换系统出现

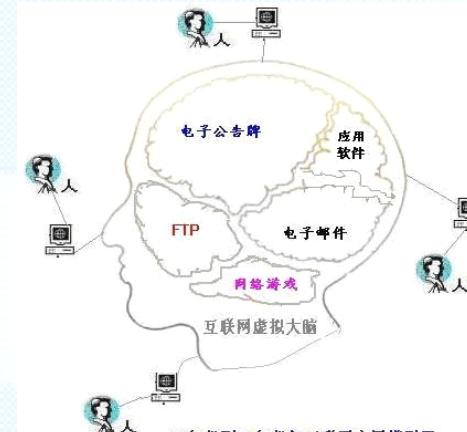
电脑的发明

数据通信技术出现

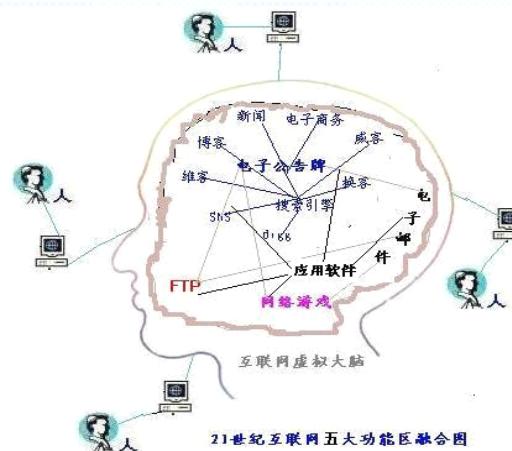
### 互联网诞生前的技术准备工作



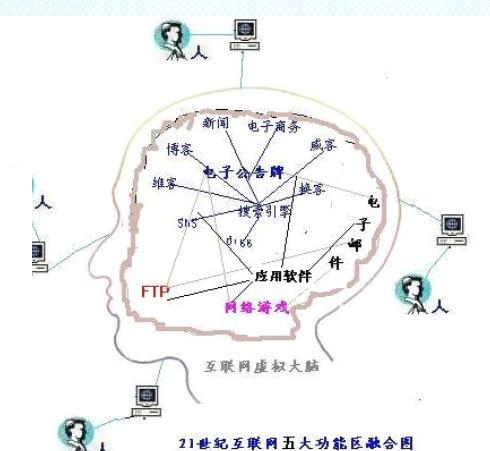
1969年互联网诞生物理结构图



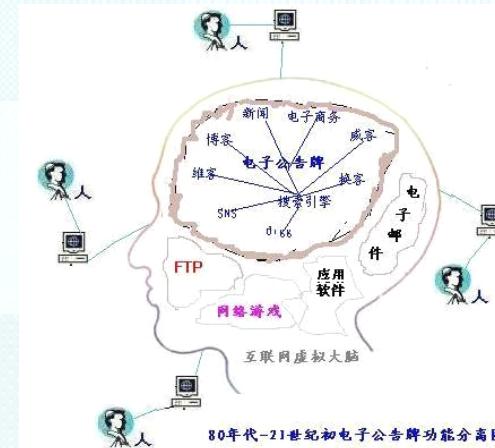
70年代到80年代初互联网应用模型图



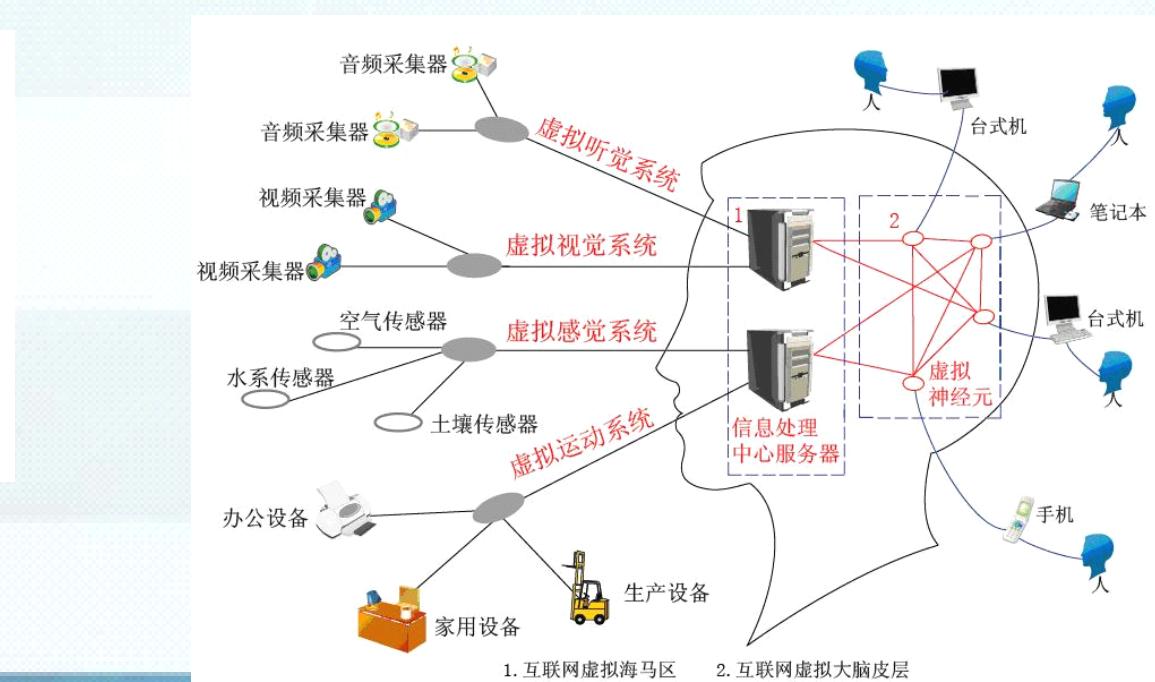
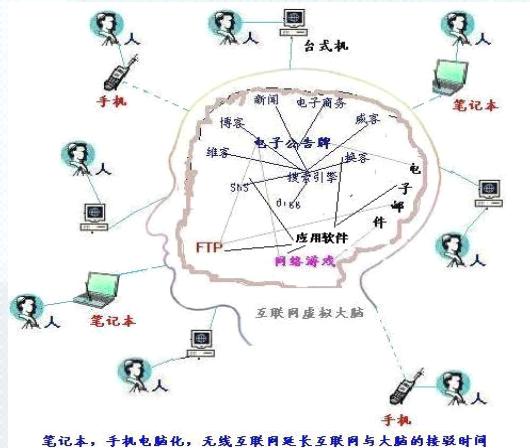
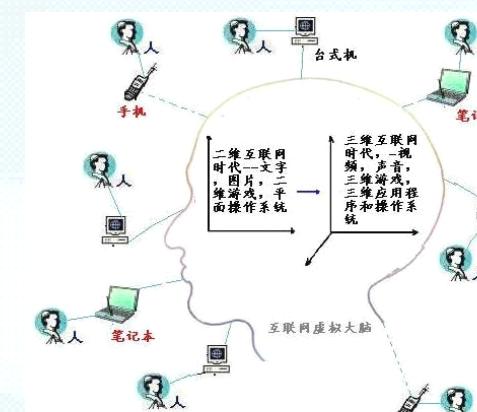
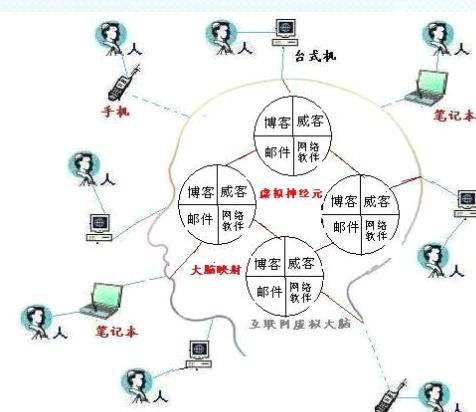
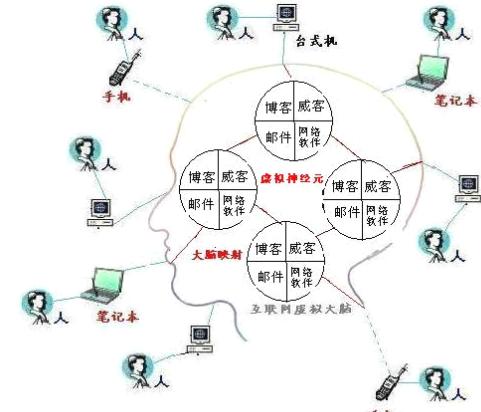
21世纪互联网五大功能区融合图



21世纪互联网五大功能区融合图



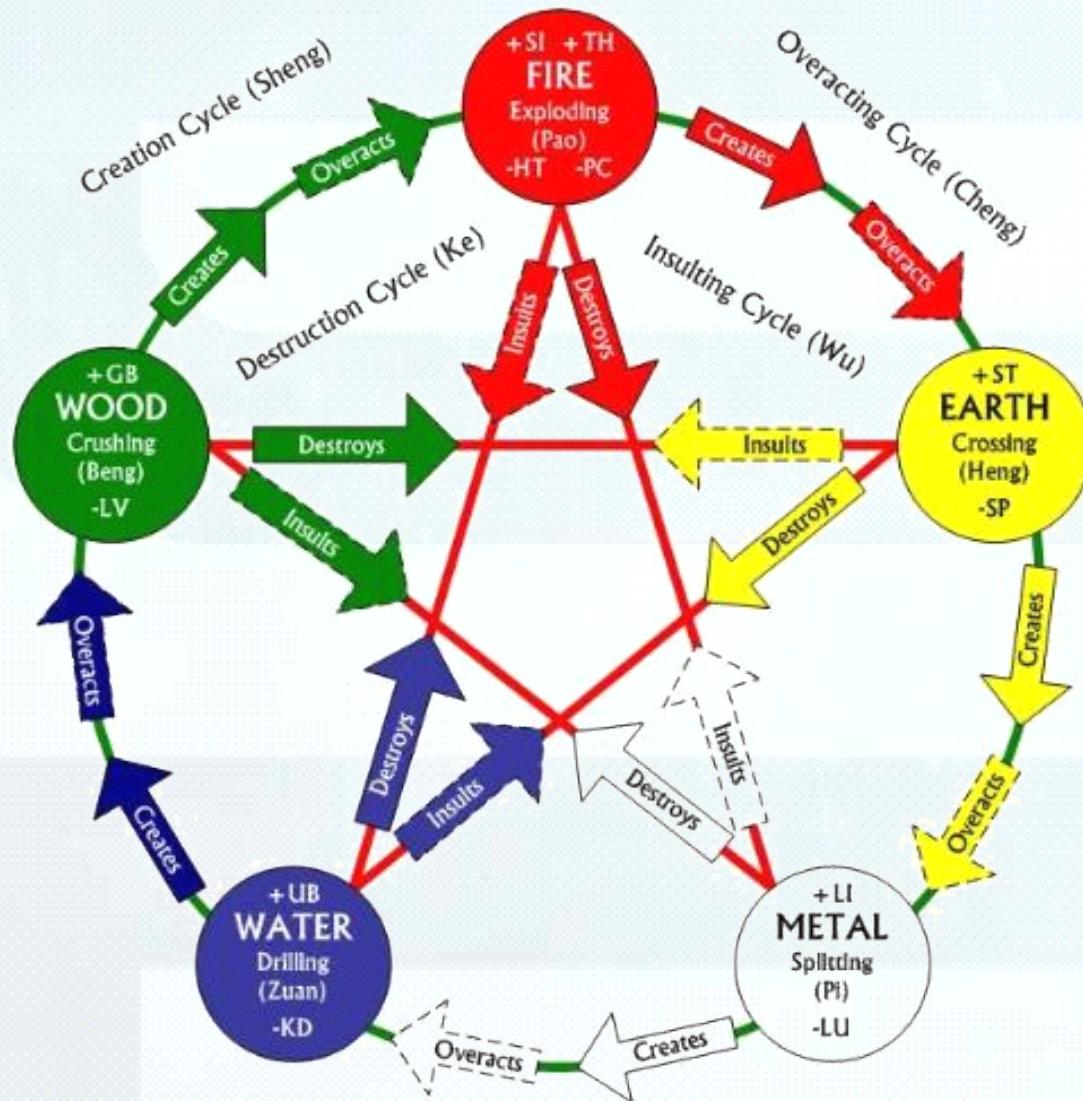
80年代-21世纪初电子公告牌功能分离图





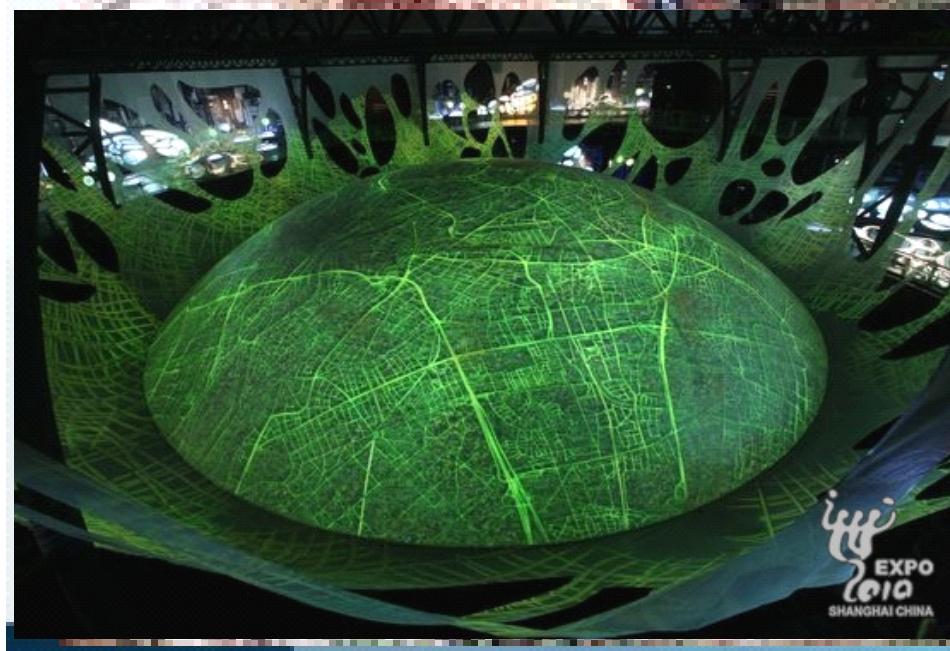
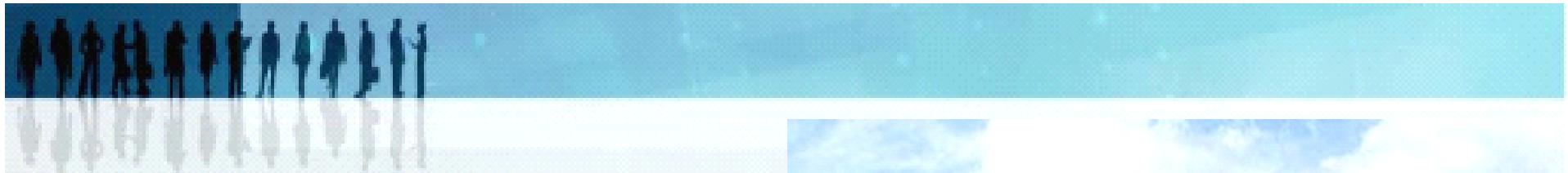
## FIVE ELEMENTS

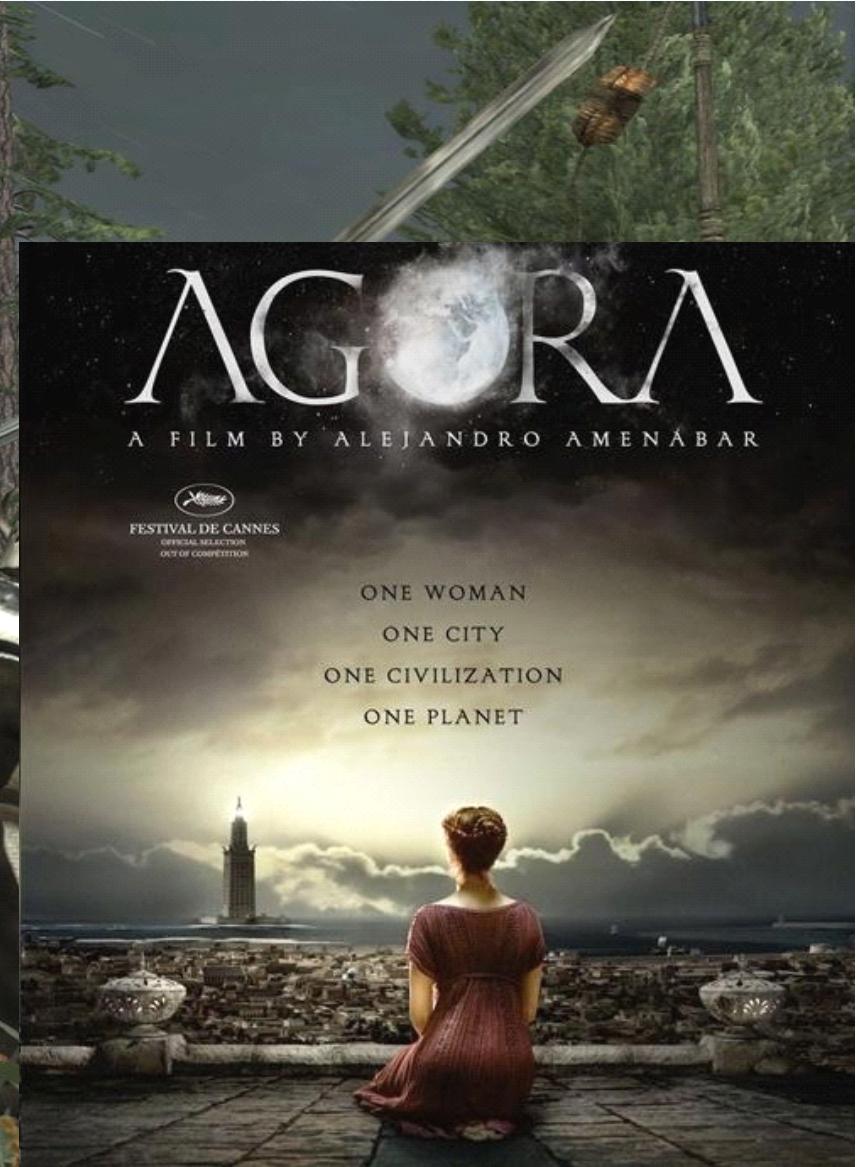
### CYCLES OF GENERATION AND CONTROL



### CYCLES OF IMBALANCE

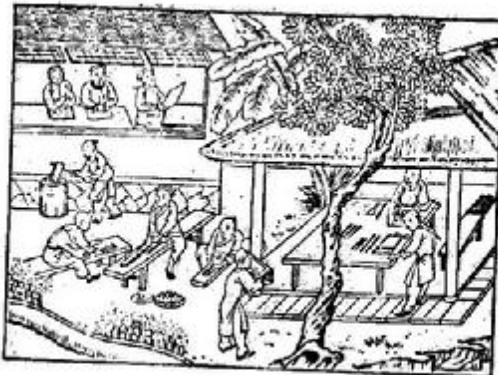
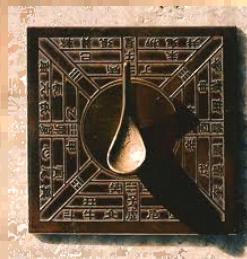
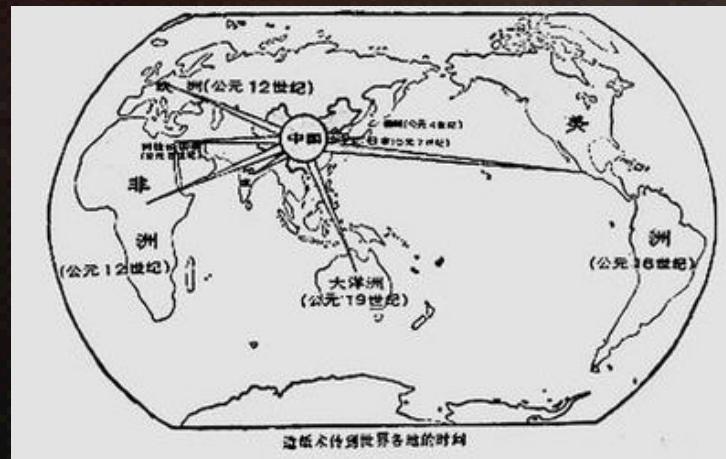




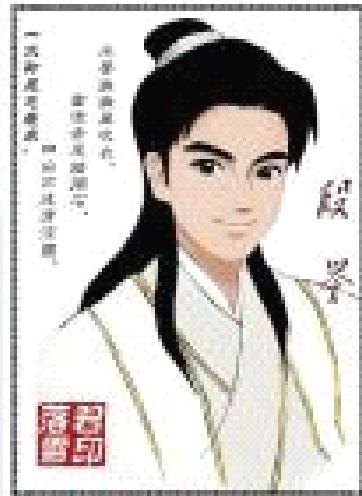




# Our History ..







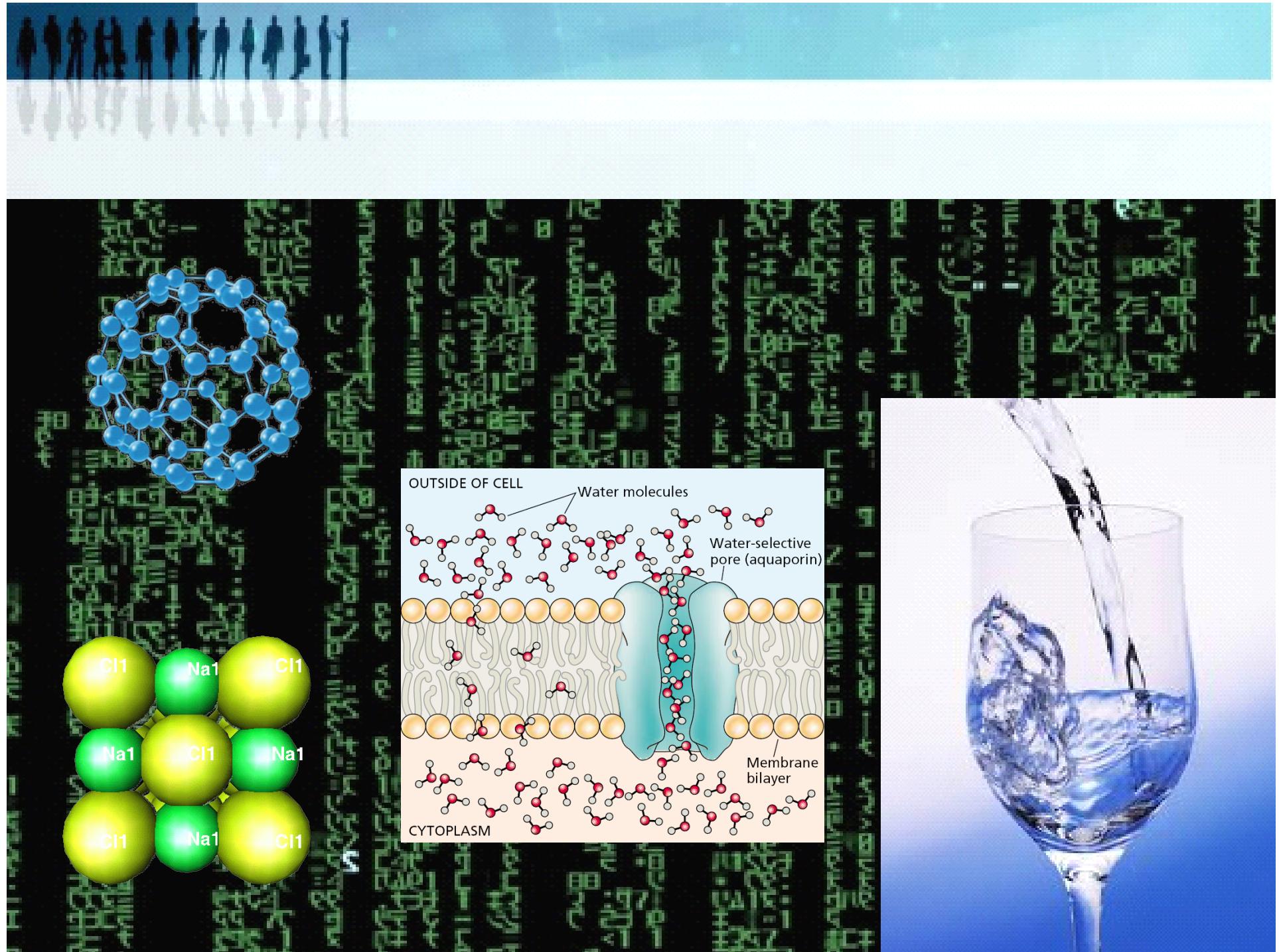


FREE SHARE EQUALITY COOPERATE..

自由 共享

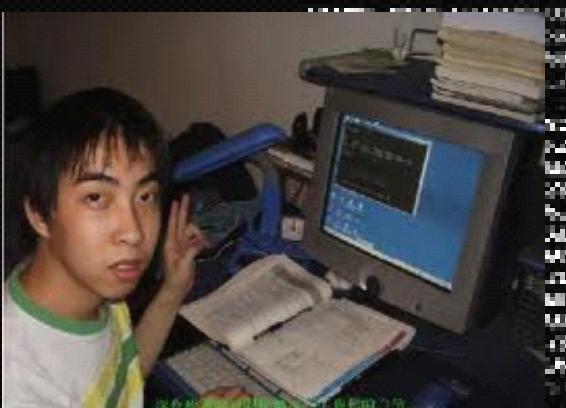
平等 互助





# Chinese Hacker

Yesterday



# Chinese Hacker

## 技术状况分析

### 编程代码类



P6

高端rootkit编写、漏洞挖掘、深度逆向

P5

漏洞挖掘，比如IE、Adobe、CDA、本地提权，可以根据公布的部分漏洞细节进行代码实现

P4

轻量型rootkit,可以绕过windows自带的工具，但是确无法回避类似xuetr, gmer等工具的扫描

P3

还原vmp,游戏外挂，游戏木马编写，以及修改网络公布的代码重新获得代码免疫性

P2

具有一定的编程能力，可以根据网上公布的代码细节进行分析，编写小病毒、自感染型，具备一定PE免杀，源码免杀，能对付常见的主动防御

P1

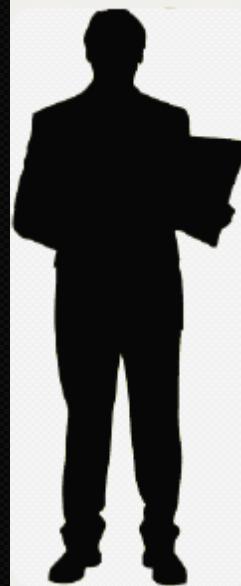
低端破解一般只会破解无壳软件，以及没有过多技术防护的软件

只会根据一些已知漏洞原理编写一些简单的漏洞利用工具

GETTING HIGHER

# Chinese Hacker

## 渗透入侵类



L6  
L5  
L4  
L3  
L2  
L1

手握各种0day，一般不轻易出手，各种国际出口流量，足以影响互联网，并且低调的可怕，高手在民间。

独立渗透各类网站  
各大公司进出自如从来不刷卡，加之庞大的社会关系学基础，这类人经验丰富，各种手法使用游刃有余。

脚本漏洞挖掘级别，具有一定的挖掘漏洞知识，对类似Web应用脚本的挖掘非常有经验，对跨站，注入等技巧灵活贯通思路新颖。

一般可以渗透指定防护级别不高，具有一定用户流量的网站，并且具有一定的经验，入侵使用的工具大部分来自网络免费或特定版本。

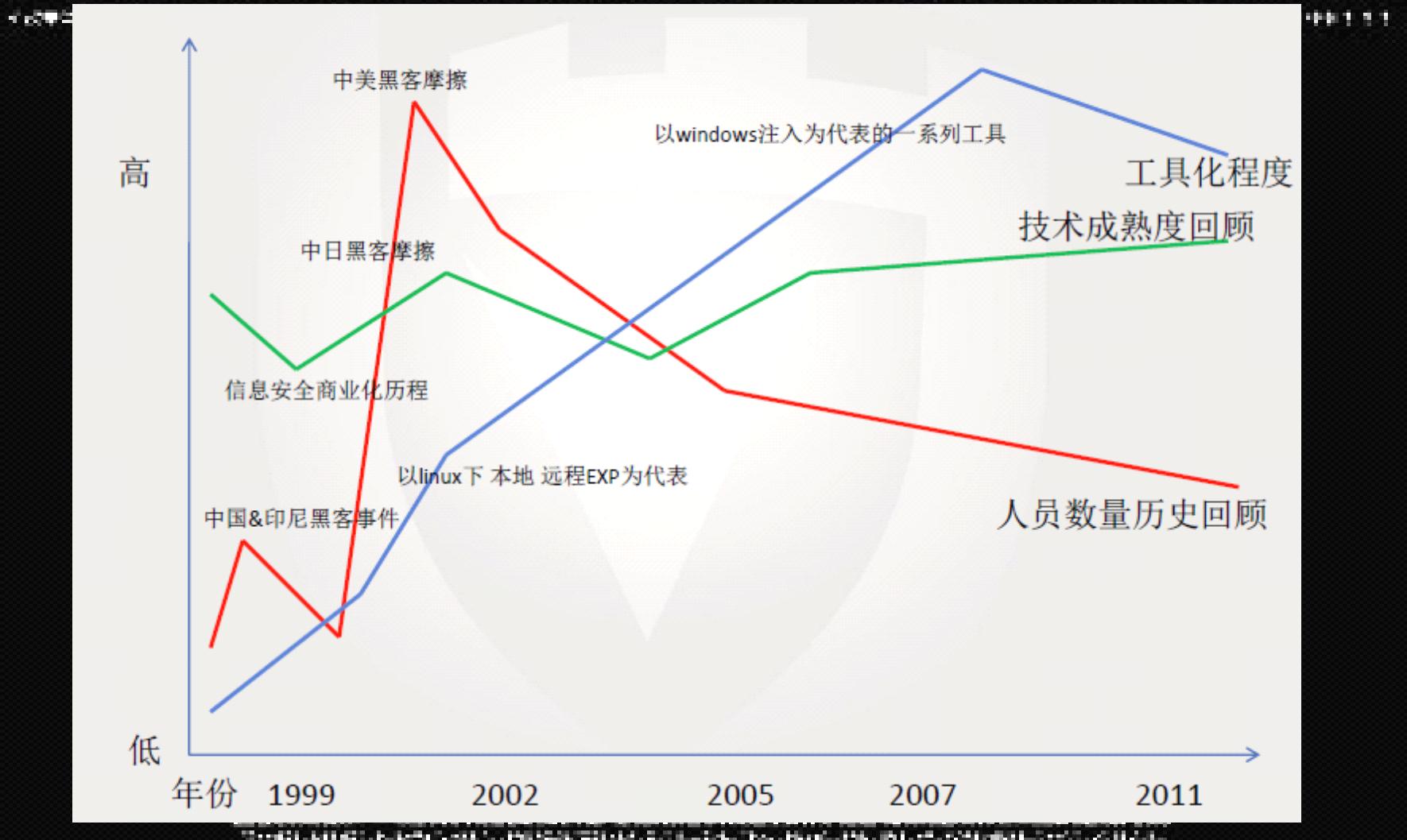
低端脚本入侵，只会按照教程使用工具，入侵手法也仅限于查找特定漏洞的站点，一招办式闯天下，柿子专挑软的捏。

只会DDOS，关键时刻甚至不惜牺牲自己作为流量带宽，基本无技术含量。

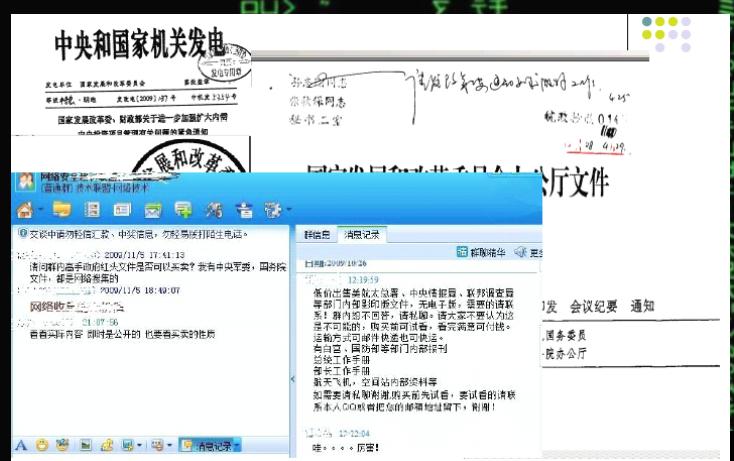
通过网上教程学习入门级渗透技巧，然后大面积撒网，瞎猫碰着死老鼠，有时候运气好还能逮个把兔子，一般各大黑客技术群里居多。

GETTING HIGHER

# Chinese Hacker



# “黑客經濟”成爲發展特點



日本网游单 <http://www.eonline.jp> <http://www.balesweaver.jp> <http://www.megaleonline.com>  
<http://www.benimushi.jp> <http://saka.hanbitstation.jp> 以上是一些单, 还有更多的.

所有都看万元以上我是中介，这是朋友告诉我的，他不是黑客，他希望有人帮他拿数据，他自己刷重

我希望每成功入侵拿到数据库一次，都能拿到 $\text{ex} \rightarrow \text{ex}$ 的提成。日后的利润分

中大上山的主校道，由狮子亭往左走，经过图书馆旁的台阶，就到中大著名的“十七棵榕树”了。

“我告诉你们后就快，咱顶上三九风寒，等不到你学习，这样孩子才学成才”。



- 攻擊產業化，威脅數量激增
  - 攻擊自動化，快速蔓延
  - 攻擊智能化，威脅技術多樣化

## 威脅數量激增

快速蔓延

## 威脅技術多樣化

齊二兄くの千子と・口ムロアニ・ト丈ム升ジ



ソルトヘッド＝アーヴィングの死

# 黑客發展史

# Chinese Hacker

名称 大小 修改时间

名称	大小	修改时间
7k7k2000万_2047.rar	194.21 MB	2012-01-10 16:05
178-b.rar	42.28 MB	2012-01-05 13:28
178.rar	103.51 MB	2012-01-10 16:05
766_16368.rar	101.33 MB	2012-01-10 16:05
766+开心.rar	109.23 MB	2012-01-10 16:32
1000W+IS2_16436.rar	157.77 MB	2012-01-10 16:05
17173_6208.rar	568.73 MB	2012-01-10 16:30
aipai_1156.zip	265.35 MB	2012-01-10 16:05
co188_87383.zip	30.40 MB	2012-01-10 16:05
CSDN-中文IT社	104.85 MB	2011-12-27 21:52

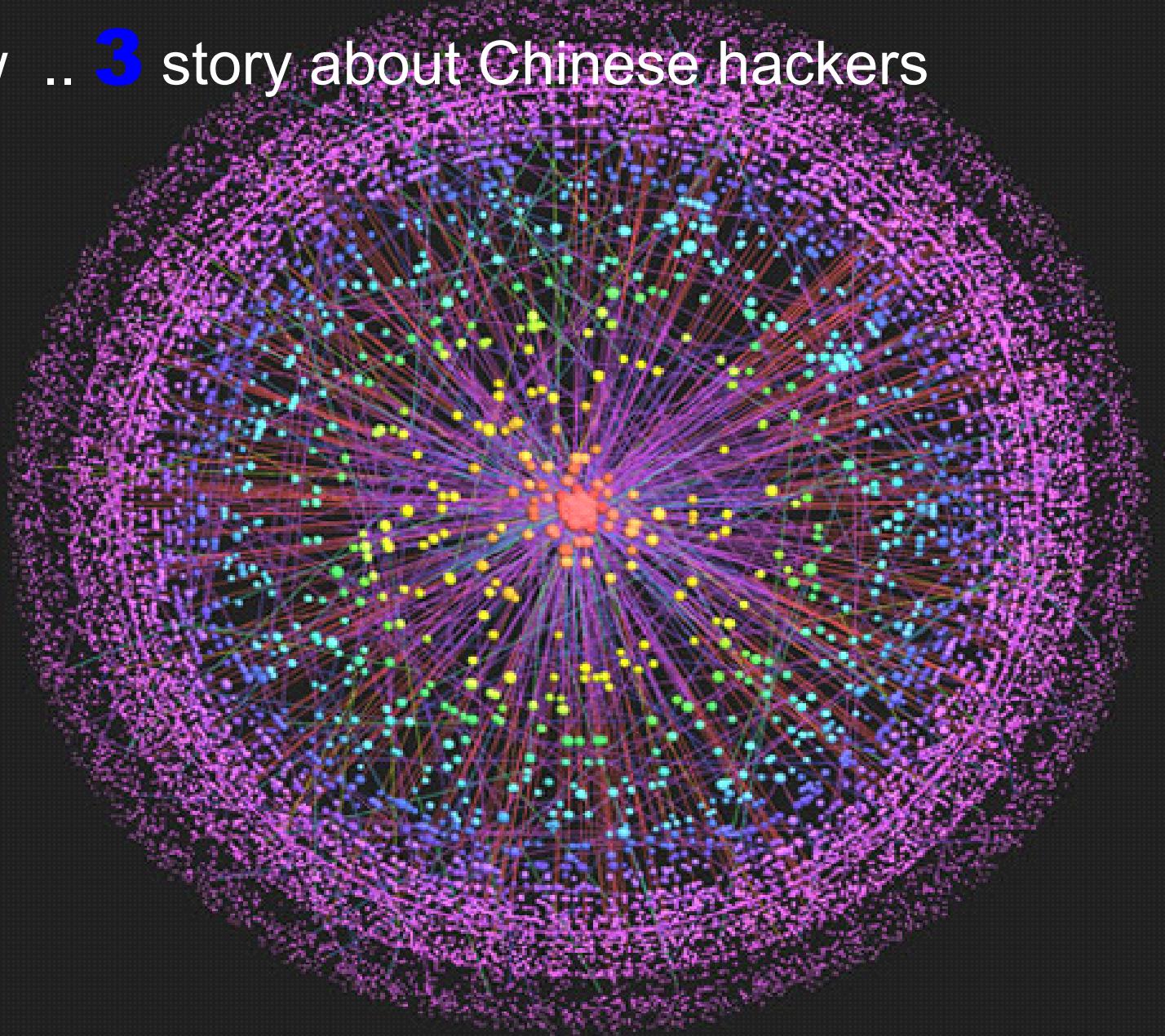
(3.28 GB)

```
L:白 CWD /IDF  
[右] 250 CWD command successful  
[右] PWD  
[右] 257 "/IDF"  
[右] PASV  
[右] 227 Entering Passive Mode (117,79,73,228,220,220)  
[右] 正在打开数据连接 IP: 117.79.73.228 端口: 56540  
[右] MLSL  
[右] 150 Opening ASCII mode data connection for MLSL  
[右] 226 Transfer complete  
[右] 列表完成: 3 KB 于 0.05 秒 (3.1 KB/秒)  
[右] TYPE I  
[右] 200 Type set to I  
[右] PASV  
[右] 227 Entering Passive Mode (117,79,73,228,217,197)  
[右] 正在打开数据连接 IP: 117.79.73.228 端口: 55749  
[右] RETR 7k7k2000万_2047.rar  
[右] 150 Opening BINARY mode data connection for 7k7k2000万_2047.rar
```



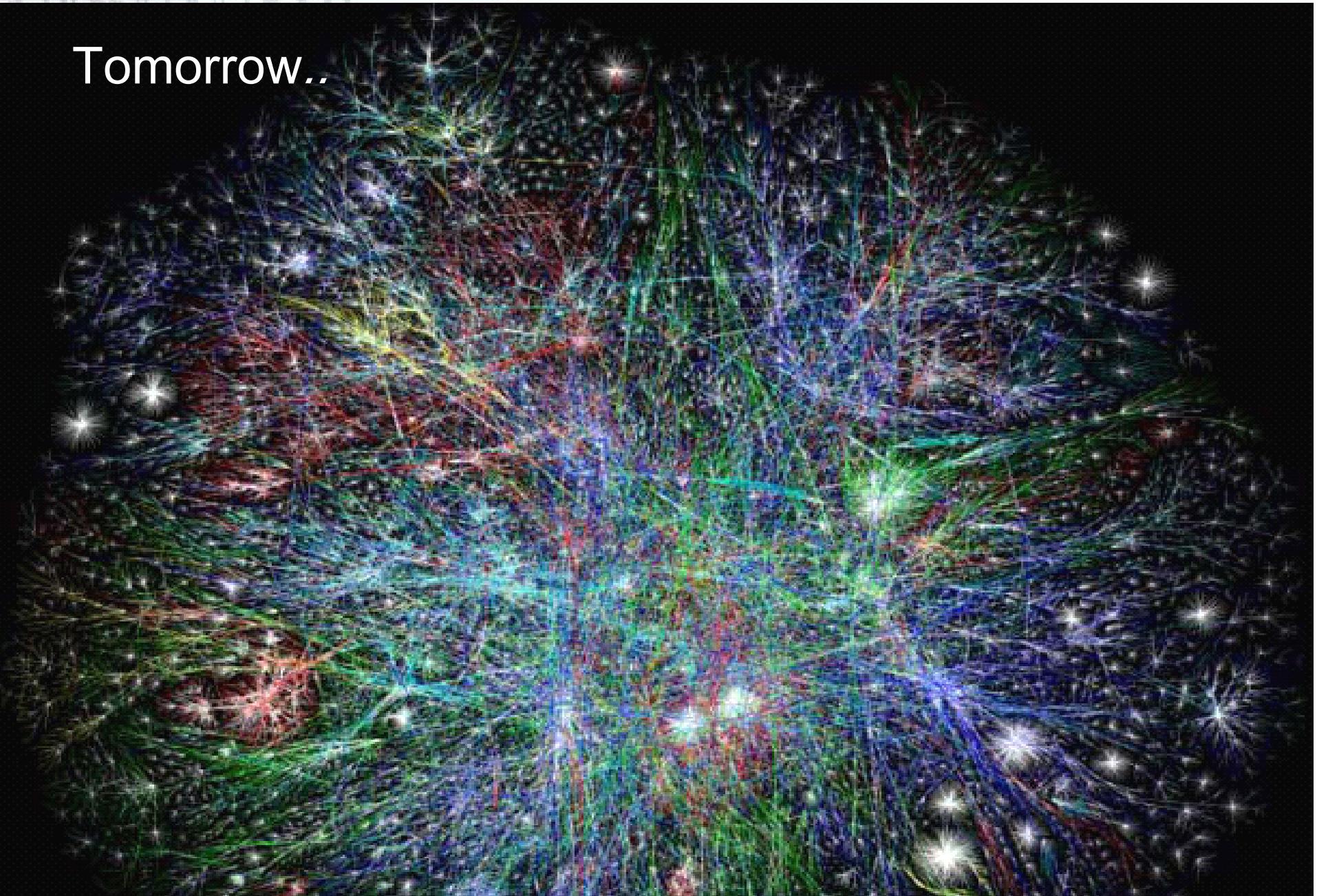


Now .. **3** story about Chinese hackers





Tomorrow..





*For the Future ..*



Thank  
You