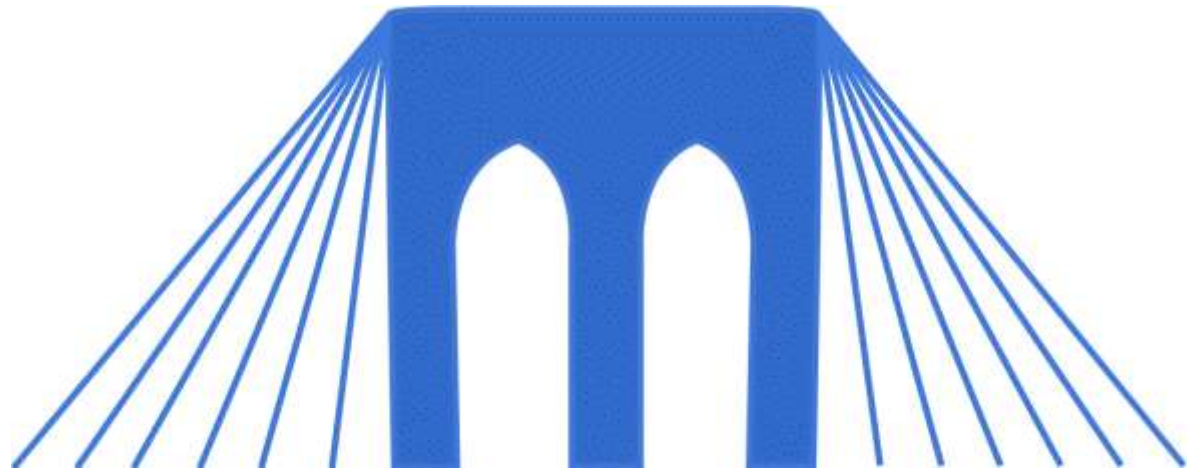
Bridges To Computing



General Information:

- This document was created for use in the "Bridges to Computing" project of Brooklyn College.
- You are invited and encouraged to use this presentation to promote computer science education in the U.S. and around the world.
- For more information about the Bridges Program, please visit our website at: http://bridges.brooklyn.cuny.edu/

Disclaimers:

- All images in this presentation were created by our Bridges to Computing staff or were found online through open access media sites and are used under the Creative Commons Attribution-Share Alike 3.0 License.
- If you believe an image in this presentation is in fact copyrighted material, never intended for creative commons use, please contact us at http://bridges.brooklyn.cuny.edu/ so that we can remove it from this presentation.
- This document may include links to sites and documents outside of the "Bridges to Computing" domain. The Bridges Program cannot be held responsible for the content of 3rd party sources and sites.

CYBERCRIME

M. Meyer
Bridges To Computing
2009

Content

1. What it is cybercrime?
2. The scale of the problem.
3. How to protect yourself.
4. Forensic computer science
5. Cyber-warfare!

What is Cybercrime?

- Cybercrime (also called computer crime, e-crime, hi-tech crime or electronic crime) is criminal activity where a computer or network is the:
  - source
  - tool
  - target
  - or place
- of a crime.

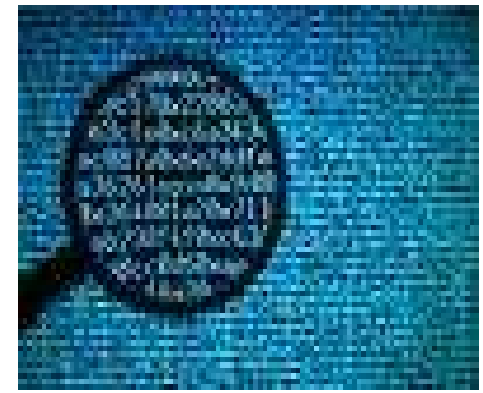
Types of Cybercrime (1):

Traditional Crimes:
(facilitated by computers)

- Fraud
- Theft
- Blackmail
- Forgery
- Embezzlement
- Harassment
- Trafficking

Digital Crimes:
(unique to the digital age)

- Spamming
- Copyright Crimes.
- D.O.S. (Denial of Service) attacks.
- Theft of Services.
- Cyber-Terrorism



Types of Cybercrime (2):

Computer Fraud:

- Identity Theft
- Embezzlement
- Market Manipulation
- "419" scams

Computer Crime:

- Theft of information.
- Theft of assets.
- Misuse of information.
- Misuse of assets.

Cybercrime is complex.

- Modern cybercrime is often a combination of crimes and not easily classified.
- Example: STORM WORM/BOTNET (2007-2009)
  - Storm-worm → "Trojan horse" spread by email.
  - Capable of disabling anti-virus software (misuse).
  - Could steal user information (identity theft).
  - Turned infected computes into "zombies" that could be controlled remotely (misuse of assets).
  - These “zombies” interacted (botnet) in coordinated operations: (SPAM, Phishing, cyber warfare).
  - Possibly created/controlled by Russian mafia.

Storm Botnet

- 2007-2008 controlled as many as 50 million computers. (Low estimate was still 1.5 million).
- Combined resources made it an extraordinarly powerful supercomputer.
- Stormnet's services were sold for use in SPAM/ Phishing attacks and scams.
- Stormnet was capable of cyber warfare...
  - October 2008, researches at UC-SD investigating the stormnet provoked a DOS attack by the botnet that crippled the University network.
  - Stormnet powerful enough to knock entire countries of the Internet (Ukraine, Estonia).

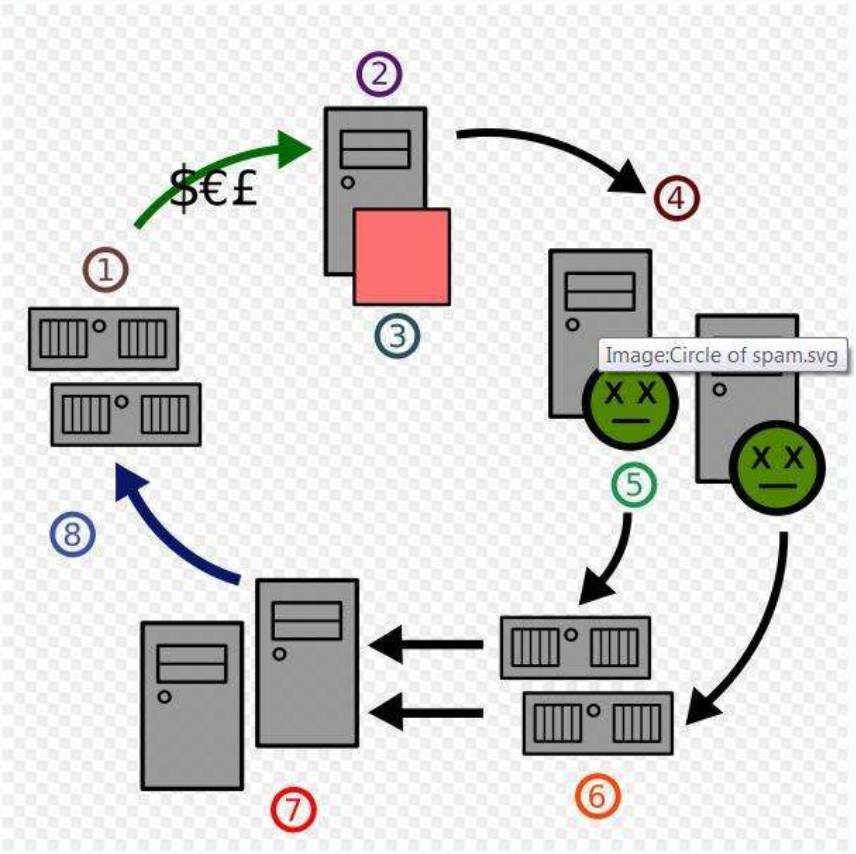
Current Botnet Threats

- Bevy of Botnets currently at large:
  - Cutwail, Rustock, Bobax, Srizbi, Kraken*, Conficker (10 million), Gumblar (currently No. 1), Sasfis, Bredolab, Zeus
- April 14th 2010, 88% of Fortune 500 company domains infected.
- Evidence botnets being used in corporate warfare.

*Principle threat to botnets... other botnets.

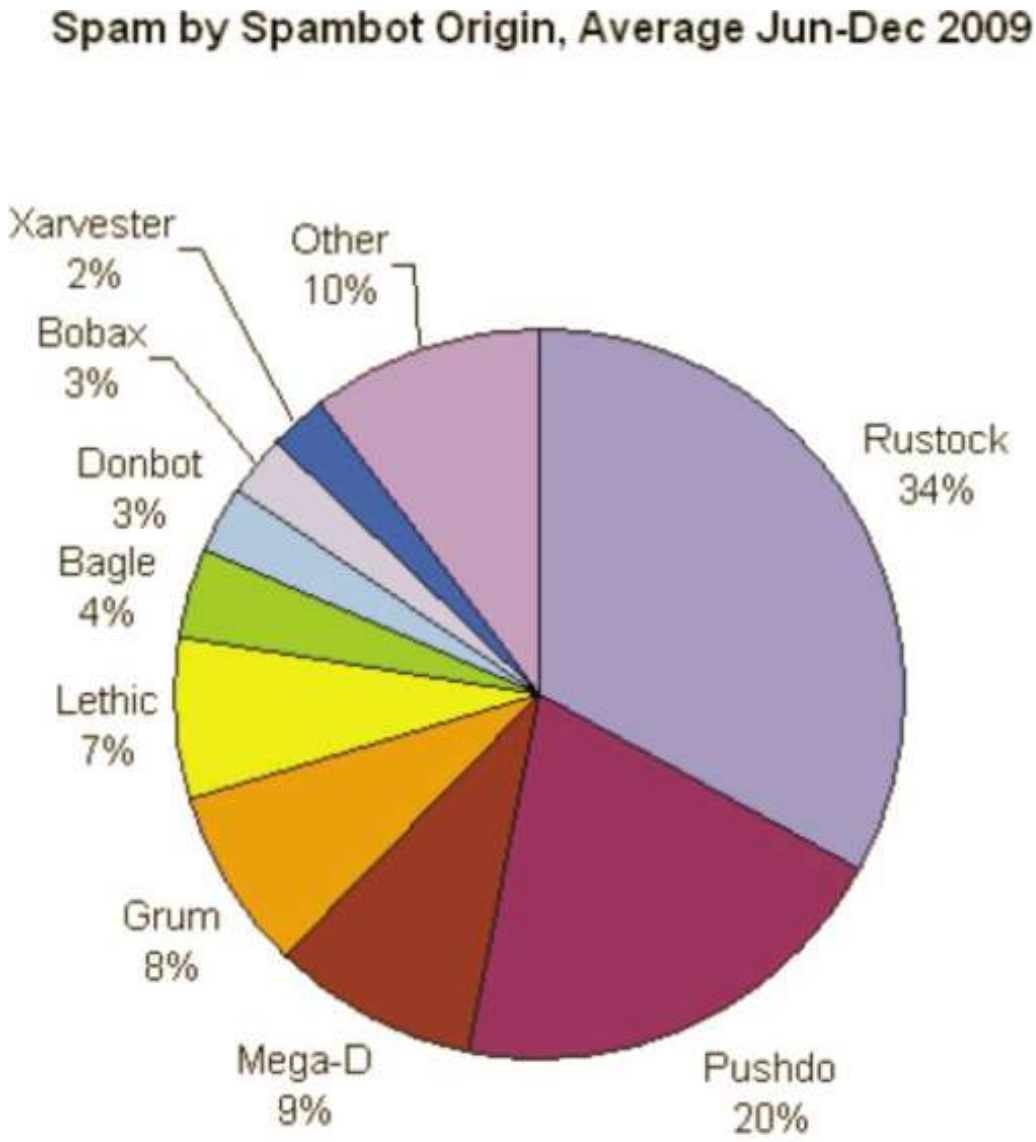
The Circle of Spam

(1): Spammer's site.
(2): Botnet Controller
(3): Botnet Software
(4): Infected computers
(5): Virus or trojan
(6): Mail servers
(7): Users Computers
(8): Web traffic **



** Many websites make money by charging advertisers for the number of visitors they get. Put payload could also be a stock market advertisement for a "pump and dump" scheme, or a link to a "phishing site" designed to trick users into giving out private information.

Spam, spam, spam, spam,



There were over 90 trillion emails sent out in 2009.

81% of those emails were Spam.

That's over 200 Billion spam emails every day of the year.

Spam by Botnet Origin, Average Jun-Dec 2009

The Scale of the Problem

- Reported 2009 cyber-crime losses $2-3 Trillion [see 90% comment below] (3).
  - 2009 – Worldwide businesses lost over $1 Trillion to Cyber-Crime (1).
  - 2009 - Global illegal drug trade 350-400 billion.
- Cyber-crime is considered cheap, easy and low risk.
  - Copy of Zeus botnet kit, $700.
  - In 2007 10.8 trillion spam message (10.5). (5)
  - Estimated 90% of all cyber-crime unreported. (2)
  - Penalties for cyber-crime are low.

(1) McAfee CEO David DeWalt. (2) Garlick, UK. (3) IDC (4) Rediff, IT. (5) IDC

Protecting Yourself

- The 5 most common types of cybercrimes perpetrated against individuals are:
  1. SPAM and other unsolicited email.
  2. Harassment / Cyber-stalking / Defamation.
  3. Unauthorized control/access of computer.
  4. Fraud.
  5. Identity Theft.

SPAM and unsolicited email.

- Don't give out email address unless required.
- Don't include your email address in documents you post on-line, and if you do then put it in a form that cannot be read by automated webcrawlers.
  - Example: meyer(dot)matt(at)gmail(dot)com
  - Better then above, use a picture.
- Use a program or web-service that can detect and block unwanted SPAM.
- NEVER respond to a SPAM email, even too "opt-out". You will just confirm that you got the email.

Harassment / Cyber-Stalking / Defamation.

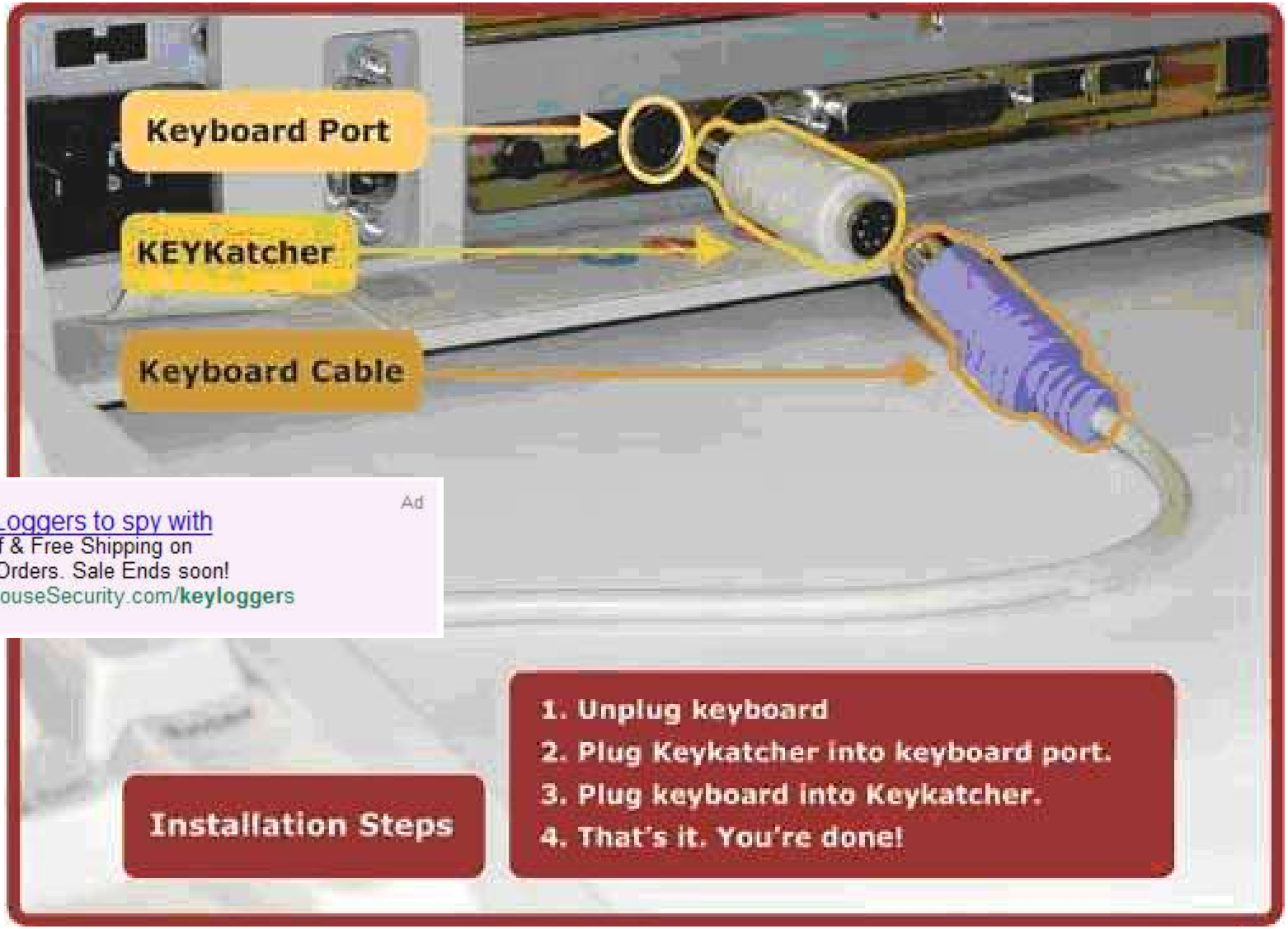
- You can protect yourself by:
  - Changing your web identity frequently.
  - Not posting personal details online.
    - REMEMBER: It is basically impossible to delete something from the Internet. Never post, email or text anything unless you are comfortable with everyone on earth seeing what you are about to send, from now, until the end of time.
- If you feel you have been a victim:
  - REPORT IT!
  - Keep records of the emails, chat messages, web postings (etc.) as proof of the harassment.

Unauthorized Computer Access/Control

- (This includes viruses and malware that infect and/ control your computer.)
- To protect yourself:
  - Don't share passwords, or write them down.
  - Use different passwords and change them frequently.
  - Use an antivirus/antispyware program.
  - Keep your antivirus programs updated.
  - Don't illegally download copyrighted materials.
  - Avoid "questionable" websites.
  - Be aware of hardware & software keyloggers!!!!

Key-loggers

Hardware (and software) key-loggers are cheap and easy ways for criminals to spy on people. Be careful when using computers in public spaces.



Fraud

- Confidence schemes, have been around for centuries, and the anonymity and scale of the Internet make them easier to attempt.
- To protect yourself remember:
  1. If it sounds too good to be true, THEN IT IS!
     - You have not won, or been selected.
  2. Be skeptical.
     - And iff you want to help, give to a charity.
  3. Never ever give out personal details about yourself online.

Identity Theft

Young people, even children are at risk for this type of crime, as they are less likely to check things like their credit score.

<u>To protect yourself:</u>

1. Never, ever give out personal details online.
   - This includes your BIRTHDAY!
   - If you must share your SSN, or CC# then look for https: and VeriSign on the site.
2. Check your credit scores!
   - You are entitled by law to see your credit score from all 3 providers, once a year, for free.
   - www.annualcreditreport.com

Forensic Computer Science

- Considering the scale of the problem of cybercrime it is not surprising that there has been a huge increase in the demand for individuals with "Forensic Computer Science" experience.
- Schools that offer degrees in F.C.S.
  - John Jay College Of Criminal Justice, CUNY
  - Argosy University - Orange County Campus
  - The University of Baltimore
  - University of Boston
  - University of Florida
  - George Washington University
  - Etc. etc.
- Most major universities are now offering "computer forensics" classes and majors/minors.

What is F.C.S.

- Two definitions:
  - In the business world, FCS is the application of computer investigation and analysis techniques in the interest of determining potential criminal wrongdoing (proactive security experts).
    - Network intrusion detection.
      - Hacking
    - Software & hardware tampering.
      - Cracking.
    - Secure communication techniques.
      - Encryption breaking.

What is F.C.S.

2. In the legal world, FCS is a process to answer questions about digital states and events, and requires the proper tools and knowledge to meet the Court's criteria (crime scene investigators).

Mostly, computer forensics experts investigate data storage devices like (USB Drives, External drives, Micro Drives etc.). Computer forensics experts:

- Identify sources digital evidence.
- Preserve the evidence.
- Analyze the evidence.
- Present the findings.

Major Obstacles for Forensic Computer Scientists

- Like any other piece of evidence, the information generated as the result of a computer forensics investigation must follow standards of admissible evidence. Special care must be taken when handling a suspects files; dangers to the evidence include:
  - viruses,
  - electromagnetic or mechanical damage,
  - and even booby traps.
- In other cases the volume of data to be analyzed (email) is the major obstacle.

Forensic Detective Tool-Kits

- Both criminals and investigators are benefiting from a boom in packaged security programs.
  - It is possible to buy a computer virus or worm online.
    - You then customize the payload.
    - Very basic programming experience needed.
  - Hacker CD's (BackTrack)
    - Several dozen security tools on a bootable CD.
    - Used by both criminals and investigators.
    - Can commit and investigate attacks.

BackTrack

Includes:

- Wireshark*
- Nmap*
- Metasploit
- RFMON
- Kismet
- Ettercap
- BeEF

Cyber-Warfare

- On March 28, 2009, "GhostNet" in China stole classified documents from government and private organizations in 103 countries, including the U.S. Both businesses and individuals were targeted.

- In July 2009, coordinated cyber attacks against major government, news media, and financial sites in South Korea and the United States. North Korea is the principle suspect.

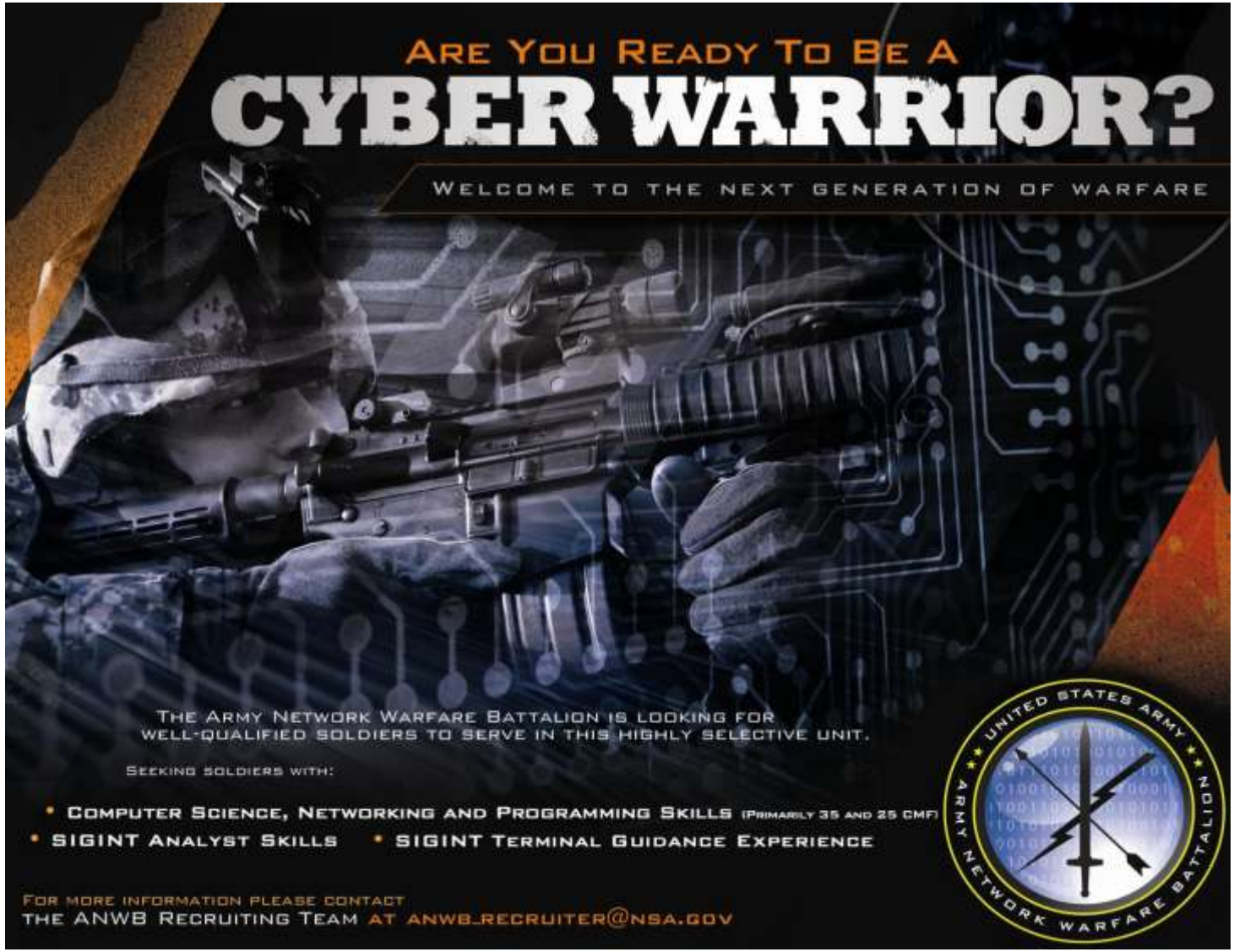
- Unconfirmed reports indicated that the Pentagon, The White House, The Office of U.S. Naval Intelligence, the CIA and the FBI have all been the victims of successful, foreign launched cyber attacks.

Cyber-Warfare

Types of Attacks

1. Attacking critical infrastructure (power, water, traffic, trading systems)
2. Equipment disruption (satellites, servers)
3. Distributed Denial-of-Service Attacks
4. Theft of information
5. Propaganda
6. Web Vandalism
7. Cyber Espionage

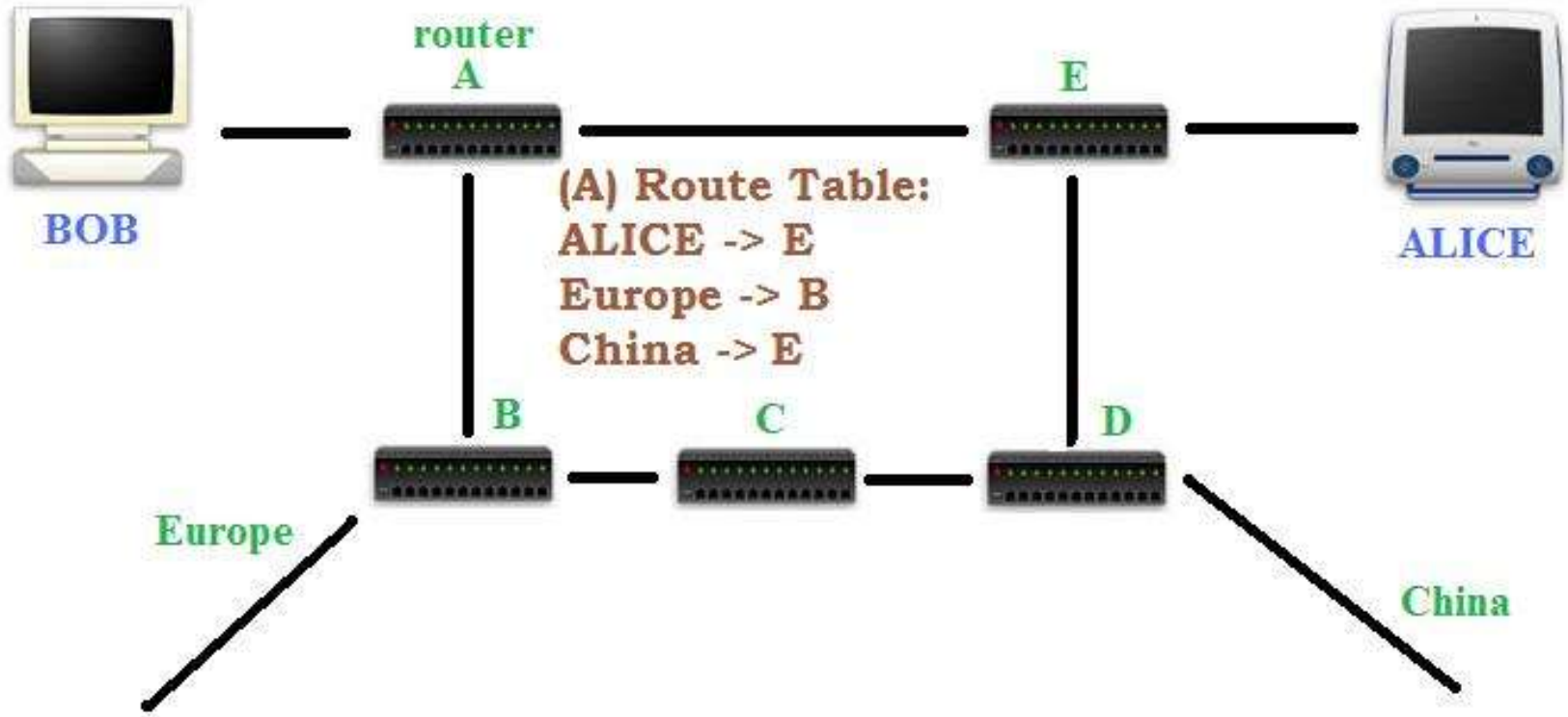
The next battlefield?



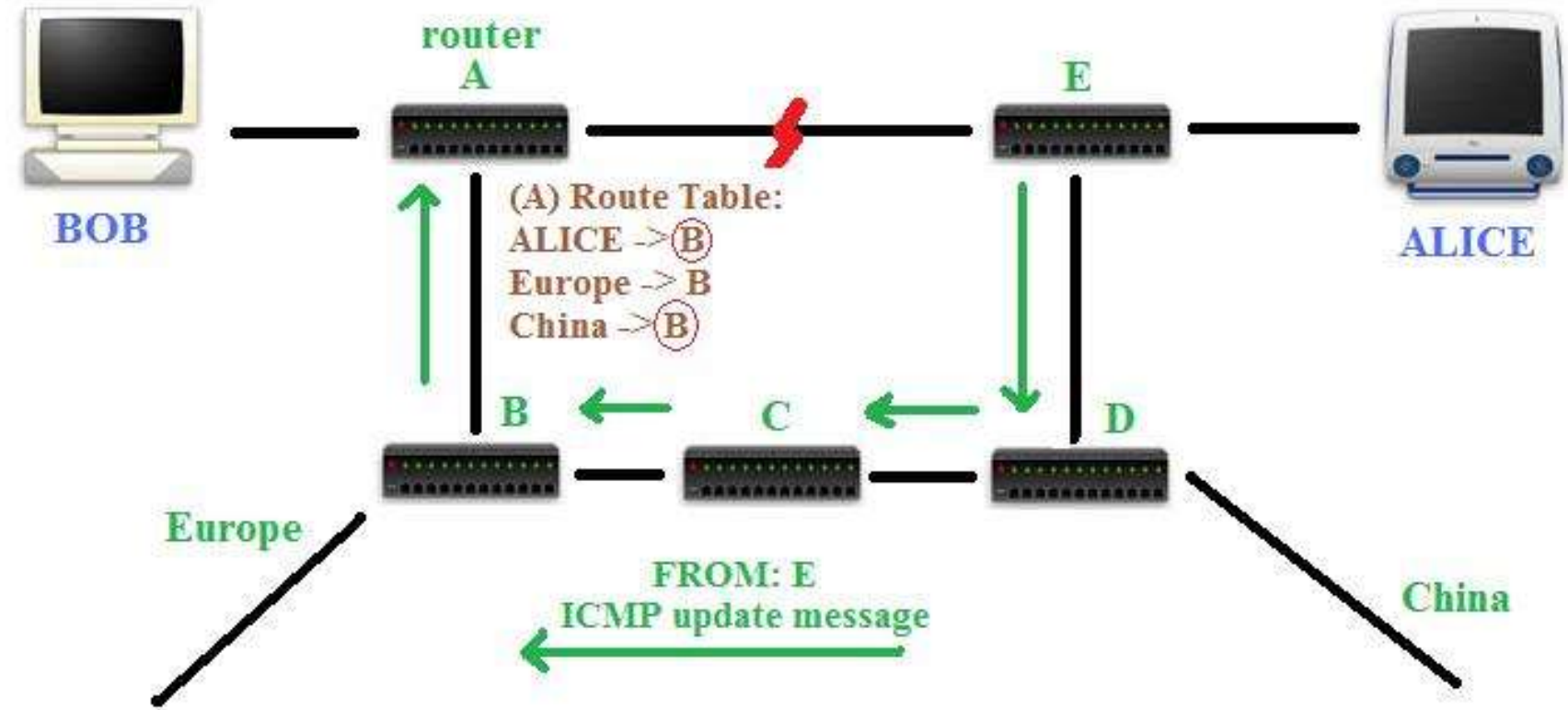
Examples of Cyber-Warfare

- Denial of Service Type Attacks:
  - Ping of Death.
  - SYN ACK attack.
  - The poisoned router cache attack (ARP).
    - Routers are network devices that help forward information to their destinations.
    - The keep "route tables" which detail the fastest way to get messages to their destination.
    - Routers communicate with each other to keep those tables updated (ICMP).
    - ICMP messages can be faked.

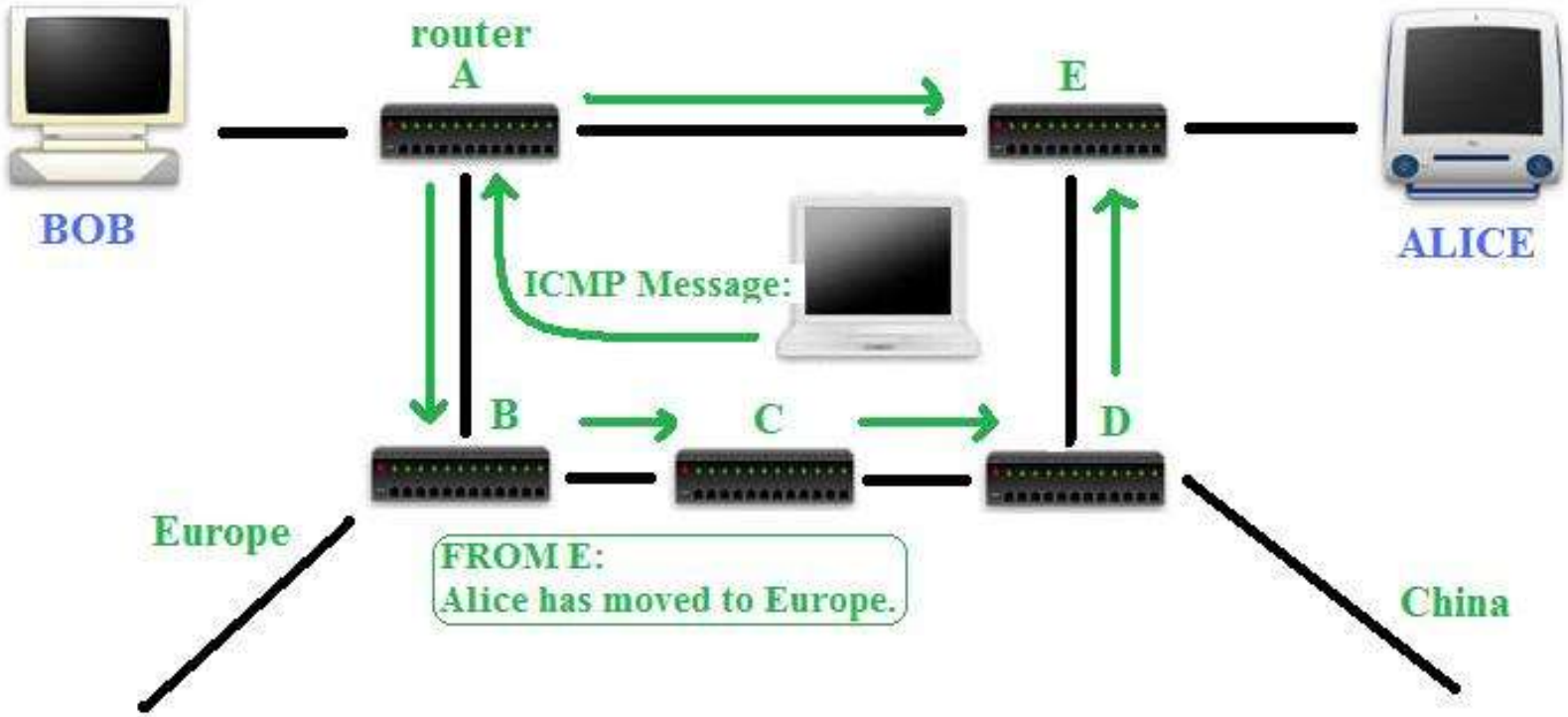
Basic Routing



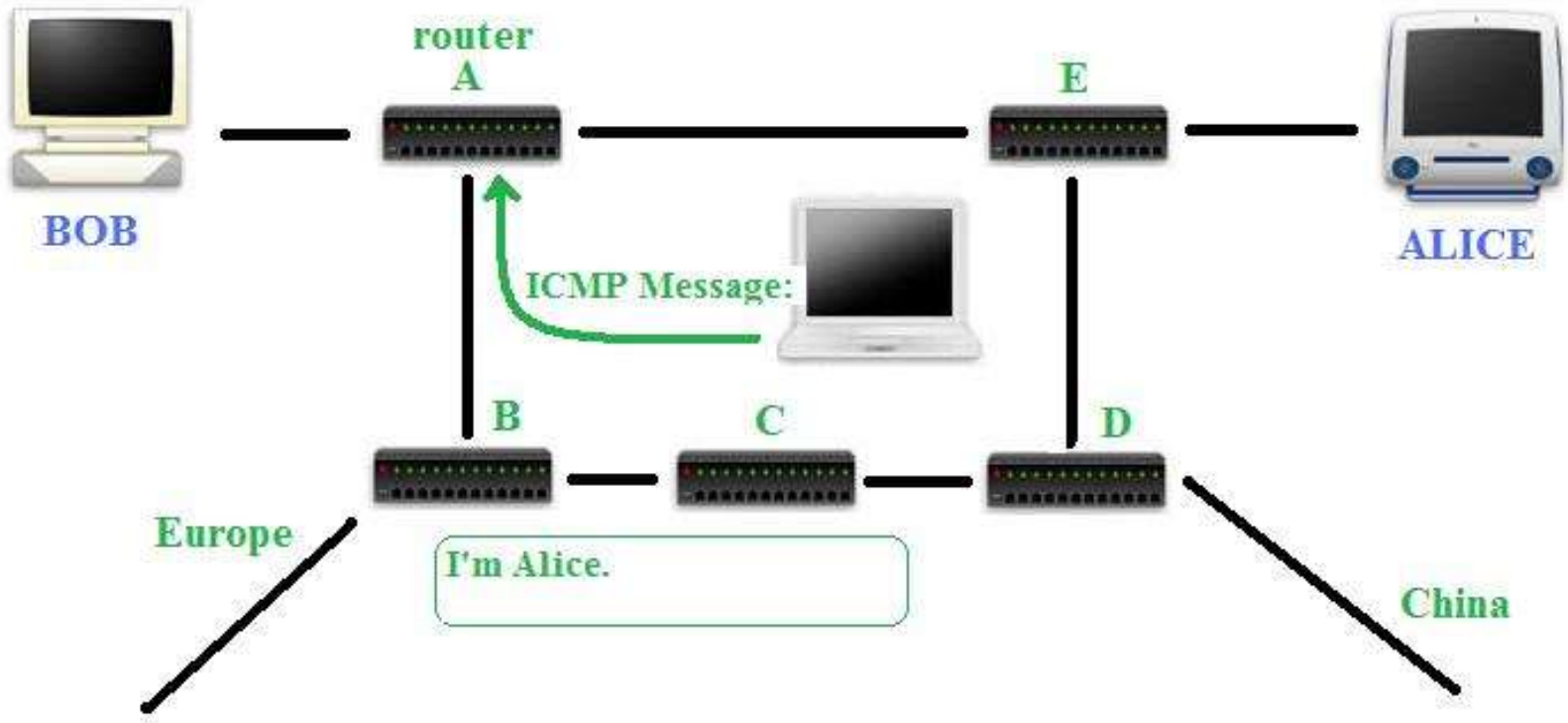
An ICMP from E.



ARP Cache Poisoning.



MAC address spoofing as part of a "Man in the Middle" attack.



2010 Updates

- In May 2010, In response to Indian Cyber Army defacing Pakistani websites, 1000+ Indian websites were defaced by PakHaxors, TeaMp0isoN, UrduHack & ZCompany Hacking Crew all Pakistan based.
- In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare. The U.S. and Israel were implicated by the Iranians in the attack.
- In October 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said Britain faces a "real and credible" threat from cyber attacks by hostile states and criminals, and that British government systems were targeted over1,000 times each month.
- On November 26 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge of the Mumbai terrorist attack which had confirmed the involvement of Pakistani terrorists.[69]
- On December 4 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry.

- More events will soon follow...

The End