



Virginia Cyber Security Partnership



VIRGINIA CYBER SECURITY PARTNERSHIP

- The mission of the Virginia Cyber Security Partnership (VCSP) is to establish and maintain a **trusted community** of **public and private sector** cyber professionals. The Partnership leverages our collective experience and knowledge, promotes mutually beneficial information sharing and fosters professional development. This mission seeks to advance our nation's interests.



MISSION OBJECTIVES

- Skills Enhancement
- Risk Management Best Practices
- Threat Information Sharing
- Resource Development Pipeline
- Community Outreach



WHO ARE WE?



Dominion[®]
It all starts here.[®]

NORTHROP GRUMMAN

J. Sargeant Reynolds
Community College



Capital OneSM

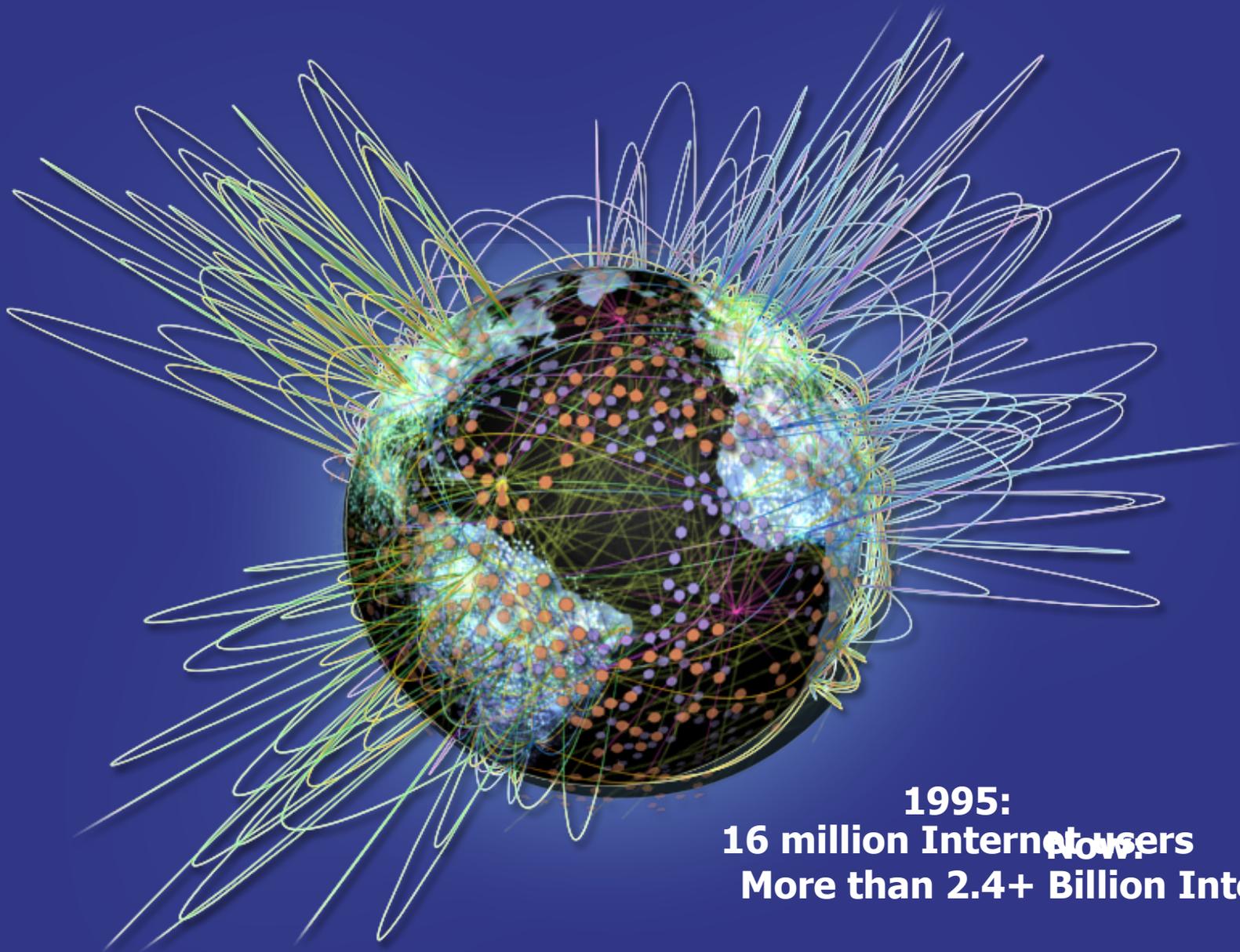


e⁺



Deloitte.





1995:
16 million Internet users
Now,
More than 2.4+ Billion Internet users



EXPLOITATION OF TRUST

- **Trusted Email**
 - Inbound e-mail trusted, exploited by “Spear Phishing”
- **Trusted Internet Websites**
 - Cross site scripting, remote code execution
- **Trusted Applications**
 - Un-patched program vulnerabilities, e.g. PDF, Word, Excel exploits
 - Unauthorized software, e.g. media player
- **Trusted Business Relationships**
 - Subcontractors and/or peer connections
 - Mergers, business partnerships, etc.
- **Trust of Internal Networks**
 - Authentication performed externally
 - “Internal” users assumed to be
- **Use of ‘Valid’ Credentials**





The Cyber Threatscape



Hacktivist	Criminal	Espionage	Terrorist	Warfare
Computer network exploitation or attack to advance a political or social cause	Financially-motivated criminal enterprises conducting computer intrusions	Nation-state actors conducting computer intrusions to illegally obtain information	Use of computer network attack by terrorist groups to harm the U.S. critical infrastructure	Nation-state actors using computer network operations to commit sabotage or disrupt critical systems
<i>Dismantled the LulzSec conspiracy Executed multiple phases of Operation Shattered Mask, 78 int'l arrests</i>	<i>Operation Card Shop takedown, multiple website shutdowns and 27 int'l arrests, June 2012 Operation Ghost Click, Jan. 2012</i>	Classified	Classified	Classified



CYBER THREATS: HACKTIVISM





CYBER THREATS: ANONYMOUS



OpPayback

#OpBigBrother

#OpFerguson

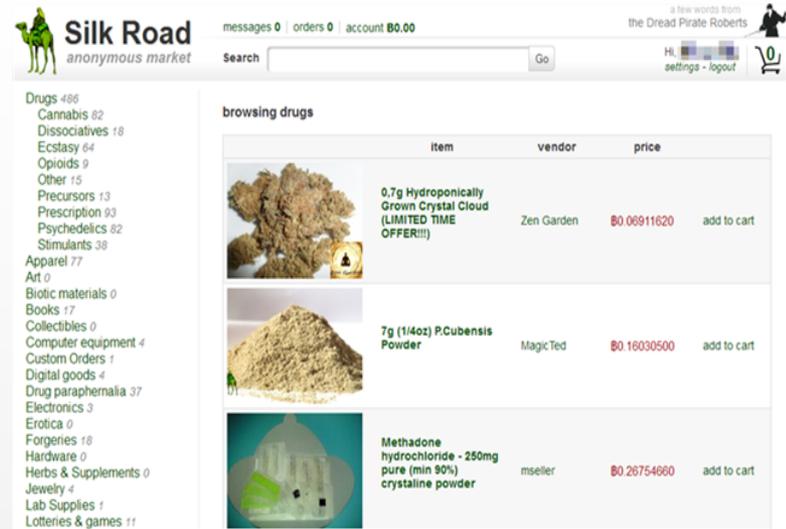
#OpDayofRage

#OpIcelSIS



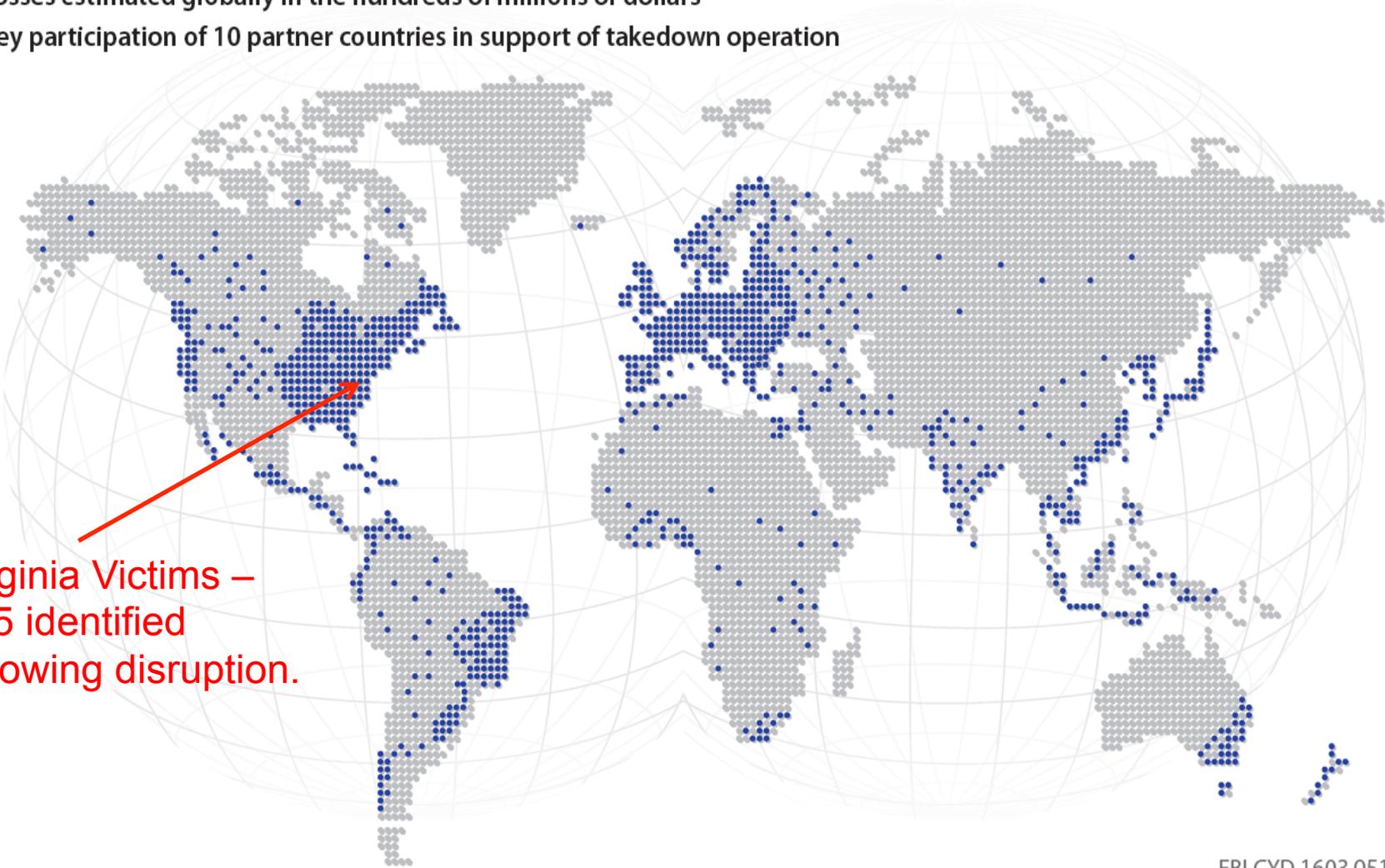
Silk Road – “Ebay of Vice”

- Bitcoin-based digital black market for drugs
- *Addiction* journal, nearly 20 percent of drug consumers in the U.S. used narcotics bought on Silk Road
- Also hacking tools, fake ID's, passports, drivers licenses, social security card, etc
- Ross Ulbricht aka Dread Pirate Roberts convicted and faces life in prison



GOZ/CryptoLocker Scope

- More than 1 million GOZ infections globally
- Roughly 25% of infected computers are located in the United States
- Losses estimated globally in the hundreds of millions of dollars
- Key participation of 10 partner countries in support of takedown operation

A world map composed of a grid of small dots. Most dots are grey, representing uninfected computers. Blue dots represent infected computers. The blue dots are most densely clustered in North America, particularly in the United States, and are also scattered across Europe, Asia, and South America. A red arrow points from the text below to a specific area in the eastern United States.

Virginia Victims –
385 identified
following disruption.



Cyber Threats: Spies to Hackers

WANTED BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

SUN KAILIANG



Aliases: Sun Kai Liang, Jack Sun

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, including Sun Kai Liang, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual expertise to an alleged conspiracy to penetrate the computer networks of six American companies while those companies were engaged in negotiations or joint ventures or were pursuing legal action with, or against, state-owned enterprises in China. They then used their illegal access to allegedly steal proprietary information including, for instance, e-mail exchanges among company employees and trade secrets related to technical specifications for nuclear plant designs. Sun, who held the rank of captain during the early stages of the investigation, was observed both sending malicious e-mails and controlling victim computers.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.



CAREERS IN CYBER SECURITY





HOW DO CYBER JOBS COMPARE?

- Ninth Highest Paying Job in the US
 - Computer and Information Systems Manager
 - Avg. Starting Salary: \$59,221
 - Avg. Annual Salary: \$126,190
 - Median Personal Income with Bachelor's Degree: \$43,143
- Among Top 10 Jobs
 - Computer Programmer - #9
 - Computer Systems Analyst - #7
 - Web Developer - #6
 - Database Administrator - #5
 - Software Developer - #2

Source: cnbc.com/id/47984925/page/9

Source: money.usnews.com/money/careers/slideshows/the-10-best-jobs/11



20 Coolest Careers in Info Security

- #1 Information Security Crime Investigator/Forensics Expert
- #2 System, Network, and/or Web Penetration Tester
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager

Source: www.sans.org/20coolestcarrers/



CYBER SECURITY CAREERS

- Key Character Traits
 - Integrity, Leadership, Strong Work Ethic, Results Oriented
 - Teamwork and Collaboration
- Essential Skills
 - Critical Thinking, Time Management, Organization, Communication (Oral and Written), Analytical / Troubleshooting
- Career Paths
 - Risk Management
 - Policy, Strategy, Regulatory Compliance, Security Investigations
 - Threat and Incident Management
 - Security Operations
 - Perimeter Protection, Malware Protection, Technical Policy Enforcement
 - Cyber Security Operations Center Monitoring and Analysis



OPPORTUNITIES NOW

- AF National High School Cyber Defense Competition
 - www.uscyberpatriot.org
- DHS Scholarships, Fellowships, Internships and Training
 - <http://www.dhs.gov/student-opportunities-0>
- CSAW High School Cyber Forensics Challenge
 - www.poly.edu/csaw2012
- US Cyber Challenge – The Governors Cyber Challenge
 - www.technology.virginia.gov/CyberChallenge
- Maryland Cyber Challenge
 - www.fbcinc.com/e/cybermdconference/challenge
- Cyber Security Partnership Capture the Flag
 - Coming Soon!!



STAY CURRENT!!!!

- Dark Reading - <http://www.darkreading.com/>
- The Register - <http://www.theregister.co.uk/>
- Slash Dot - <http://slashdot.org/>
- CSO Online - <http://www.csoonline.com/>
- Wired - <http://www.wired.com/>
- Search Security - <http://searchsecurity.techtarget.com/>



WHAT CAN THE CSP DO FOR YOU

- Mentorship
- Training
- Letters of Recommendations
- Internship opportunities
- Job's after college
- Information on new technology