UNIVERSITY of WASHINGTON

Have our tools gotten the better of us?

The unintended consequences of digital evidence in our legal system

Dr. Barbara Endicott-Popovsky
ACA@UBC

Fifth International Seminar and Symposium
We Shape our Tools and our Tools Shape Us

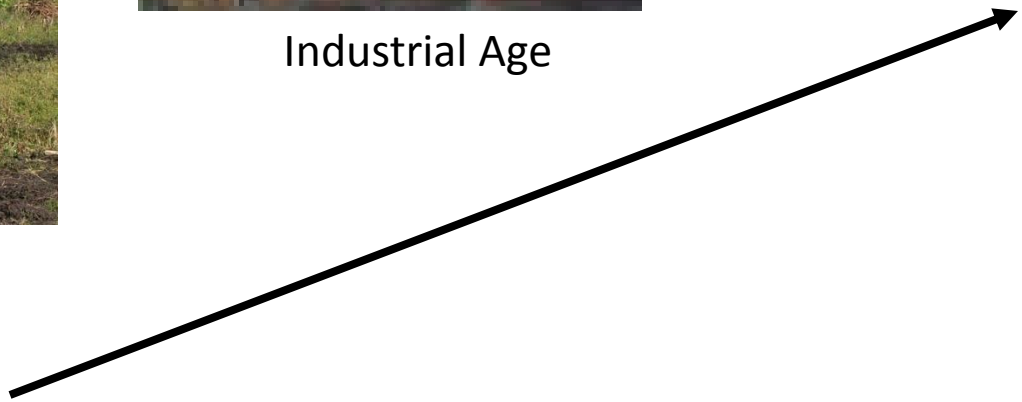
6 February 2013

Context Evolution

Agricultural Age

Industrial Age

Information Age



Attribute	Agricultural Age	Industrial Age	Information Age
Wealth	Land	Capital	Knowledge
Advancement	Conquest	Invention	Paradigm Shifts
Time	Sun/Seasons	Factory Whistle	Time Zones
Workplace	Farm	Capital equipment	Networks
Organization Structure	Family	Corporation	Collaborations
Tools	Plow	Machines	Computers
Problem-solving	Self	Delegation	Integration
Knowledge	Generalized	Specialized	Interdisciplinary
Learning	Self-taught	Classroom	Online

Adapted from S. Covey

Our Love Affair with the Internet

"Shoppers embrace the online model"

POSTED: 0727 GMT (1527 HKT), December 20, 2006

"Embracing Internet Technologies"

"Docs Embracing Internet"

"US Internet Users Embrace Digital Imaging"

"Baby Boomers Embracing Mobile Technology"

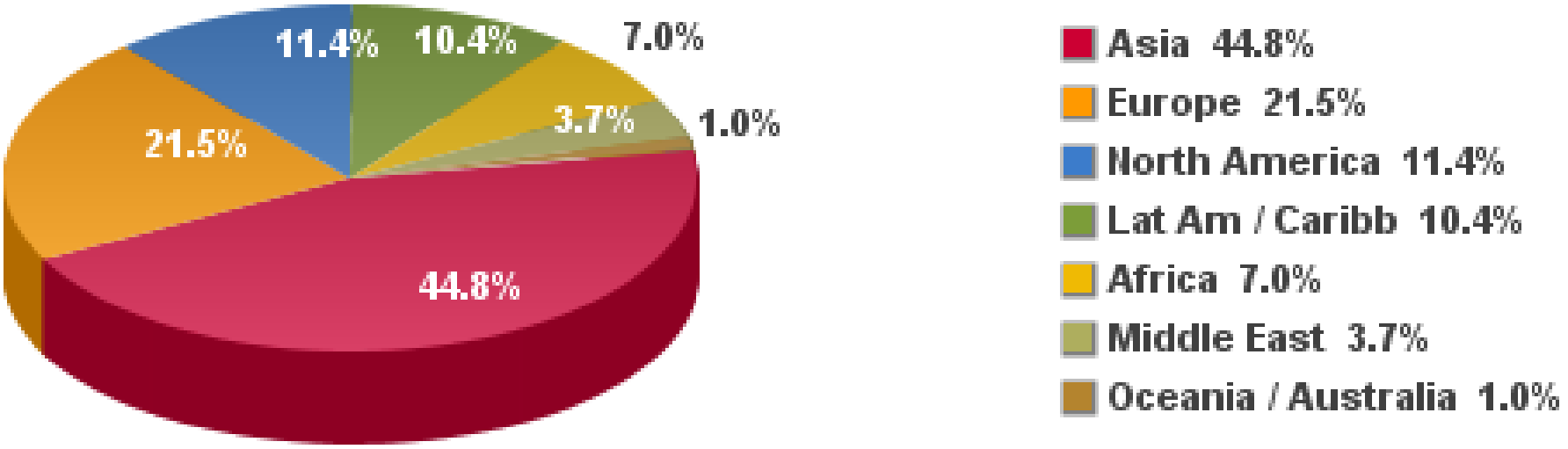
INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and Population Stats

WORLD INTERNET USAGE AND POPULATION STATISTICS
June 30, 2012

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7 %	7.0 %
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8 %
Europe	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5 %
Middle East	223,608,203	3,284,800	90,000,455	40.2 %	2,639.9 %	3.7 %
North America	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4 %
Latin America / Caribbean	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8 %	10.6 %
Oceania / Australia	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.0 %
WORLD TOTAL	7,017,846,922	360,985,492	2,405,518,376	34.3 %	566.4 %	100.0 %

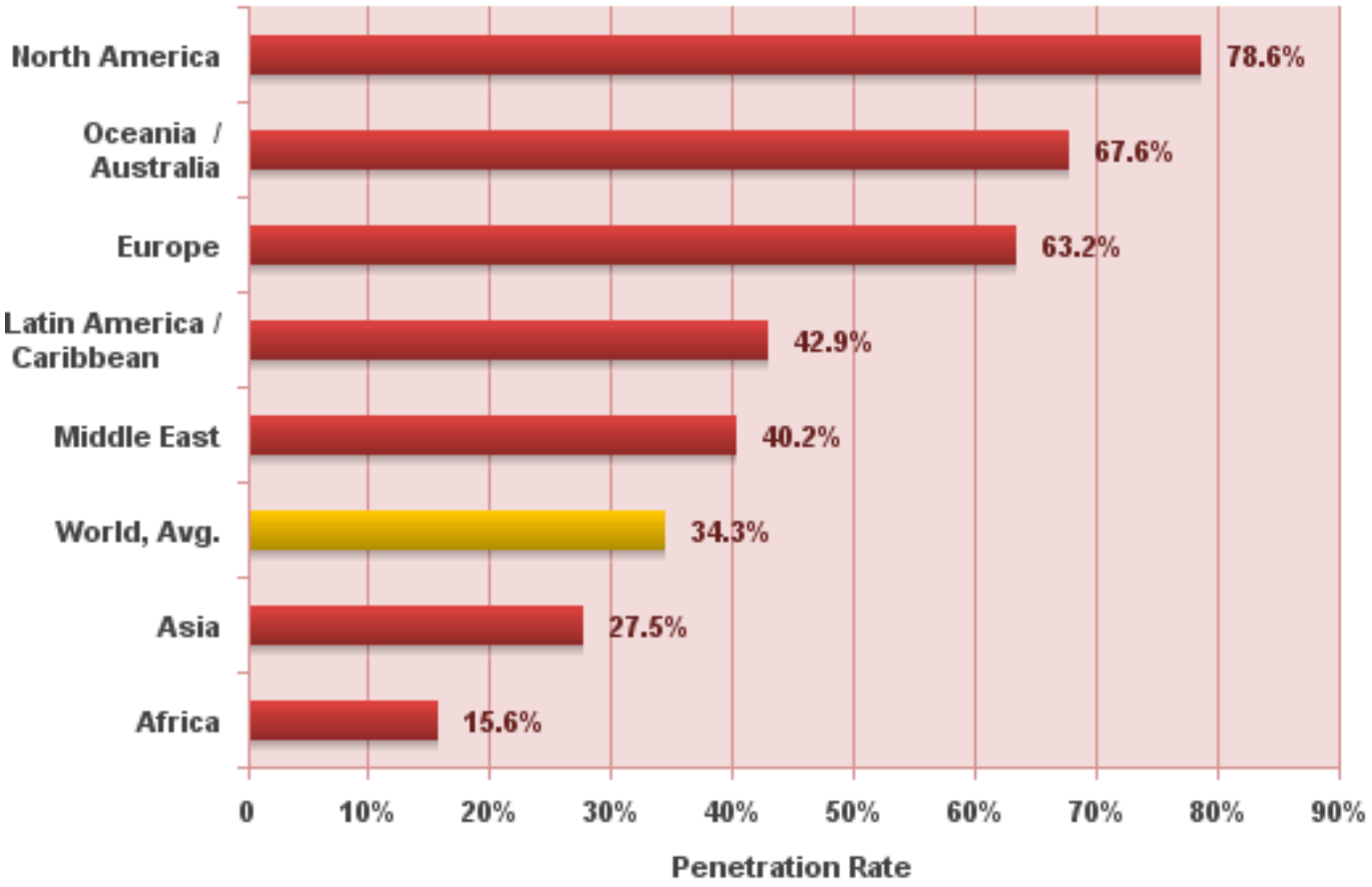
NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2012. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau and local census agencies. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local ICT Regulators and other reliable sources. (5) For definitions, disclaimers, navigation help and methodology, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com.

Internet Users in the World
Distribution by World Regions - 2012 Q2

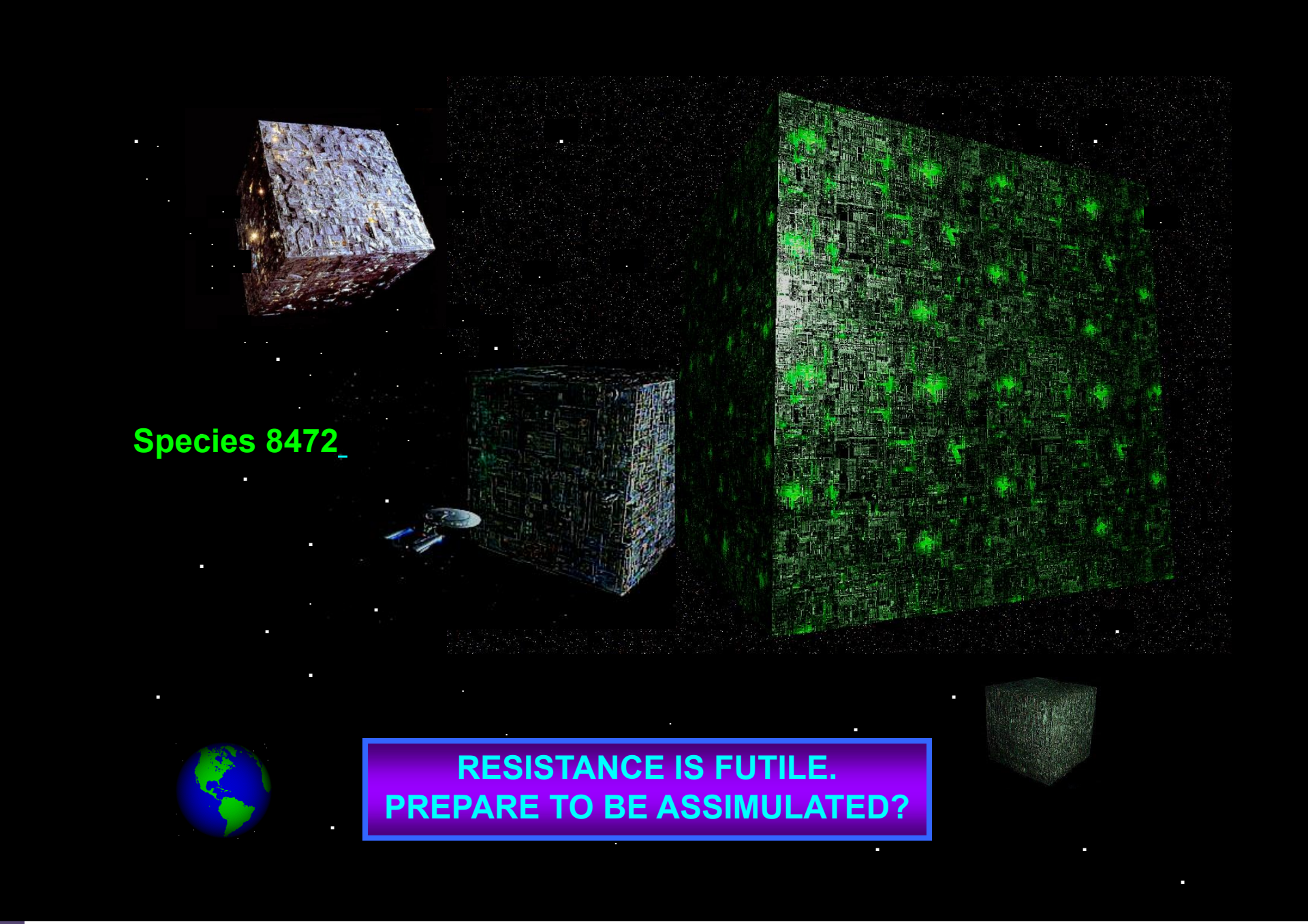


Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,405,518,376 Internet users on June 30, 2012

World Internet Penetration Rates
by Geographic Regions - 2012 Q2



Source: Internet World Stats - www.internetworldststs.com/stats.htm
Penetration Rates are based on a world population of 7,017,846,922 and 2,405,518,376 estimated Internet users on June 30, 2012.



Courtesy: K. Bailey/E. Hayden, CISOs

Smashing

Industrial Age

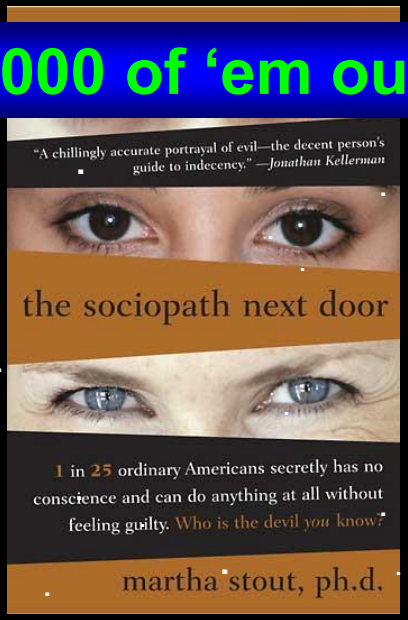
Infrastructure!


Surprise!!
KNXA

Unintended Consequences of Embracing the Internet…..

Troubling Realities

41,000,000 of 'em out there!

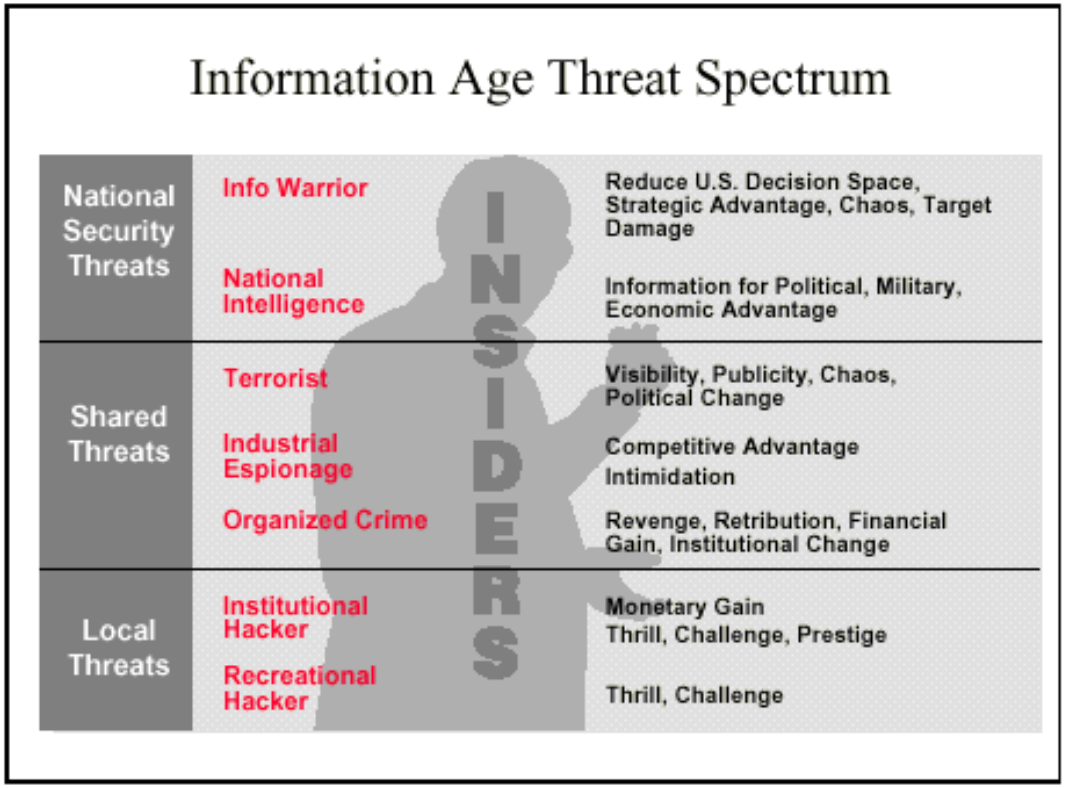


Dan Geer
Chief Scientist
Verdasys

"In the world of networked computers every sociopath is your neighbor."

Maturing Threat Spectrum

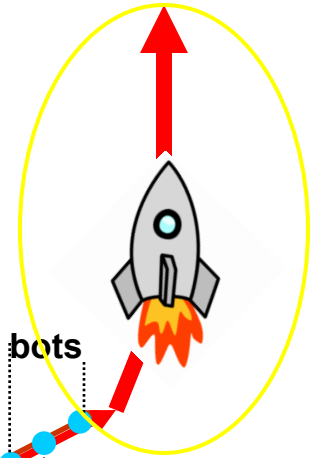
*"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."—**Foreign Government Newspaper***

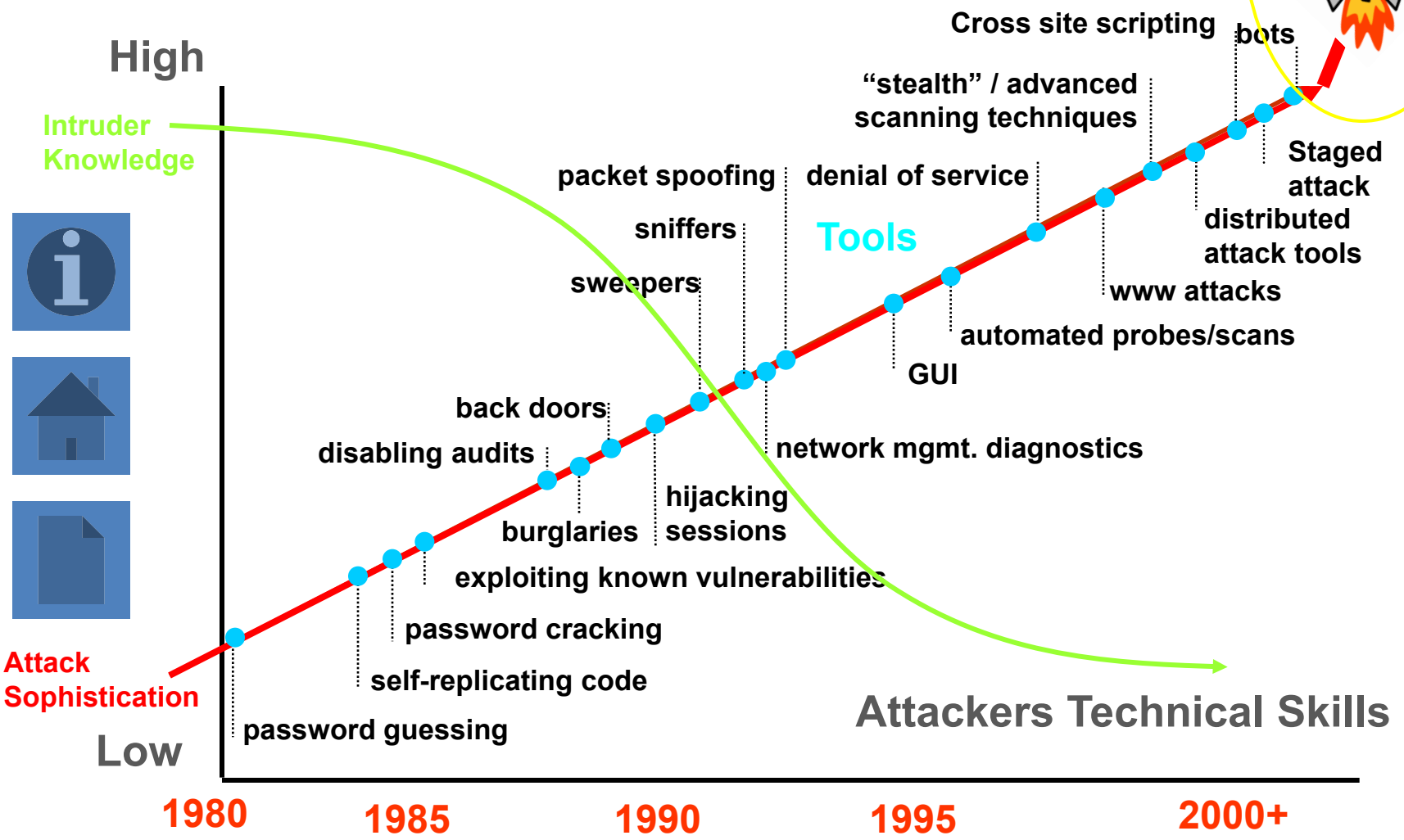


UNIVERSITY of WASHINGTON

Cyber Attack Sophistication Continues To Evolve

Source: CERT 2004





Cybercrime and Money…

- McAfee CEO: "Cybercrime has become a $100+B business that now surpasses the value of the illegal drug trade worldwide"

Symantec Internet Security Threat Report

- **Threat landscape is more dynamic than ever**
- **Attackers rapidly adapting new techniques and strategies to circumvent new security measures**
- **Today's Threat Landscape..**
  - Increased professionalism and commercialization of malicious activities
  - Threats tailored for specific regions
  - Increasing numbers of multi-staged attacks
  - Attackers targeting victims by first exploiting trusted entities
  - Convergence of attack methods

"If the Internet were a street, I wouldn't walk it in daytime…" K. Bailey, CISO UW

- 75% of traffic is malicious
- Unprotected computer infected in < 1 minute
- Organized crime makes more money on the Internet than through drugs
- The 'take' from the Internet doubles e-commerce

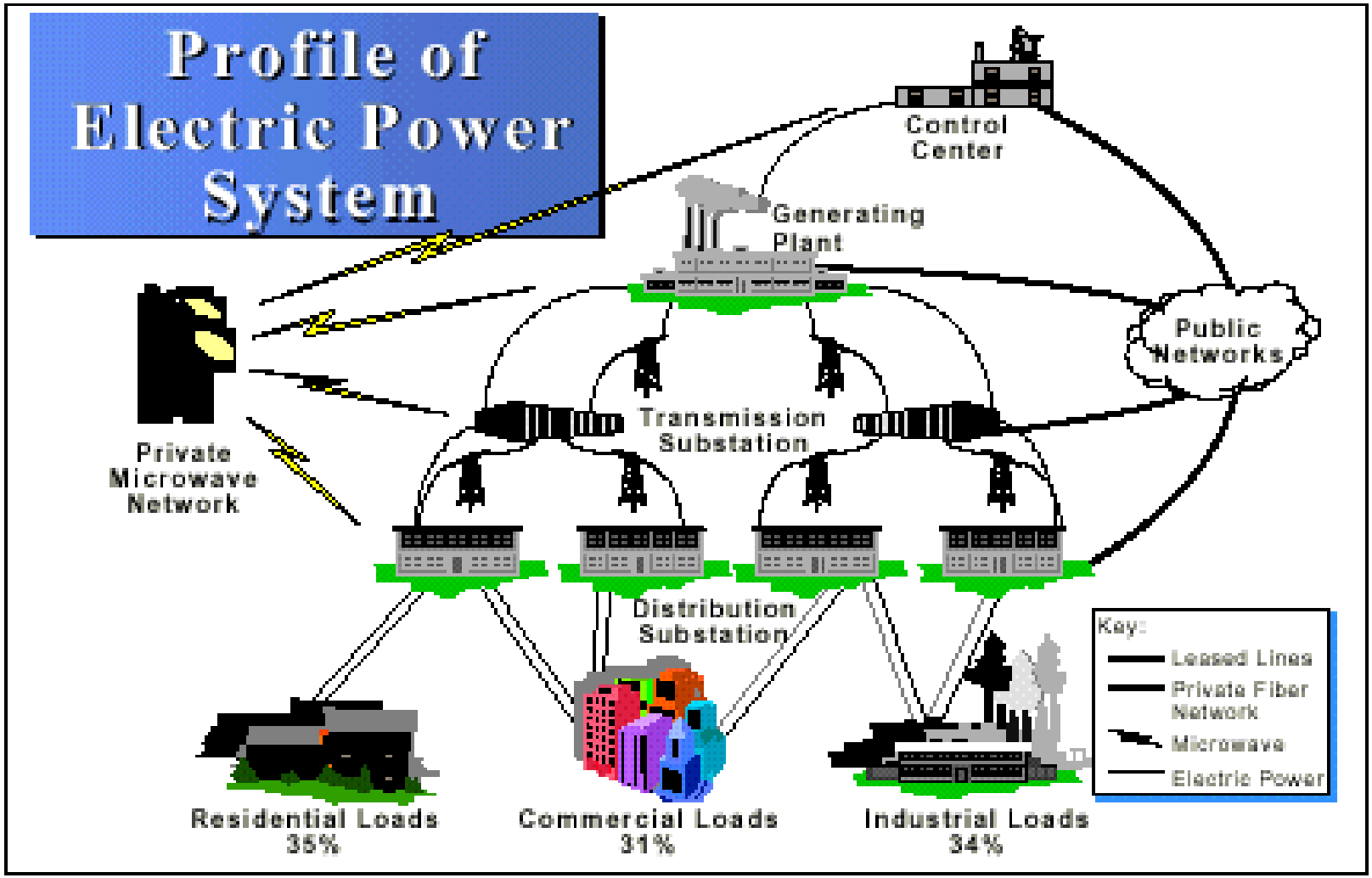
Courtesy: FBI, LE

What does all this mean to you?….

Mini-survey

- How many have received credit notifications?
  - Credit card ?
  - Banks ?
- How many have been victims of identity theft?
- How many have received phishing emails?
  - Nigerian scam ?
  - Phony bank notices ?
  - e-Bay/PayPal ?
- How many have known of someone solicited online?

Interdependence of Critical Infrastructure



Majority think outsourcing threatens network security

Angela Moscaritolo
September 29, 2009

A majority of IT security professionals believe that outsourcing technology jobs to offshore locations has a negative impact on network security, according to a survey released Tuesday.

In the survey of 350 IT managers and network administrators concerned with computer and network security at their organizations, 69 percent of respondents said they believe outsourcing negatively impacts network security, nine percent said it had a positive impact and 22 said it had no impact.

The survey, conducted this month by Amplitude Research and commissioned by VanDyke Software, a provider of secure file transfer solutions, found that 29 percent of respondents' employers outsource technology jobs to India, China and other locations.

Of those respondents whose companies outsource technology jobs, half said that they believe doing so has had a negative impact on network security.

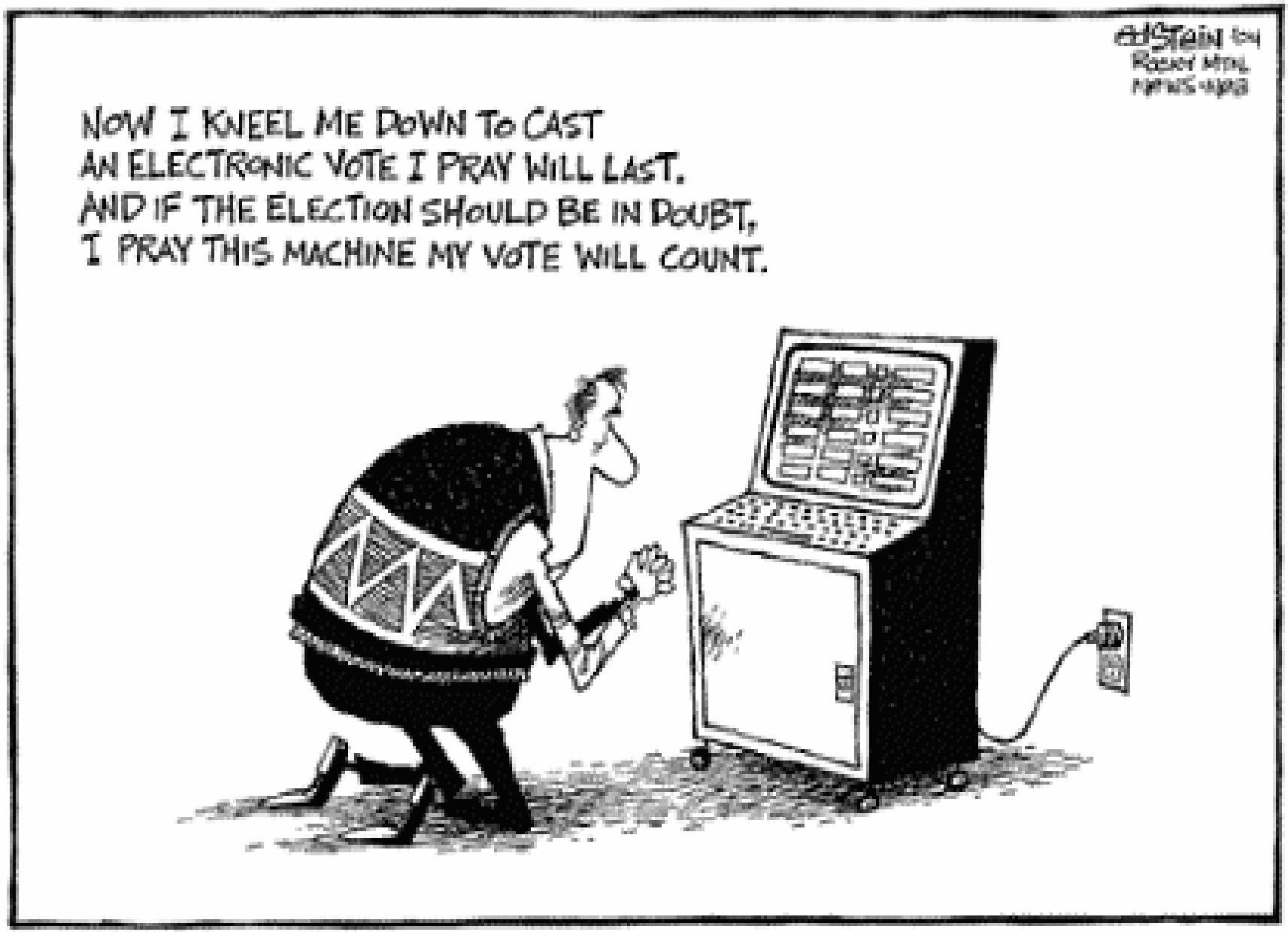
Sixty-one percent of respondents whose companies outsource technology jobs also said their organization experienced an unauthorized intrusion. In contrast, just 35 percent of those whose company does not outsource did. However, the survey noted that organizations that do outsource were “significantly” more likely than those that do not to report intrusions.

“We're not going to say we have any proven cause and effect,” Steve Birnkrant, CEO of Amplitude Research, told SCMagazineUS.com on Tuesday. “Correlation doesn't prove causation, but it's definitely intriguing that the companies that outsource jobs offshore are more likely to report unauthorized intrusions.”

In a separate survey released last December from Lumension Security and the Ponemon Institute, IT security professionals said that outsourcing would be the biggest cybersecurity threat of 2009.

In light if the recession, companies are outsourcing to reduce costs, but the practice opens organizations up to the threat of sensitive or confidential information not being properly protected, and unauthorized parties gaining access to private files, the survey concluded.

In contrast to their overall views about the impact that outsourcing has on network security, Amplitude/VanDyke Software survey respondents were largely positive about the impact of outside security audits. Seventy-two percent of respondents whose companies paid for outside audits said they were worthwhile investments and 54 percent said they resulted in the discovery of significant security problems.



FAITH-BASED VOTING

http://bwcentral.org/voting-fraud/

Connecticut drops felony charges against Julie Amero, four years after her arrest

By
Rick Green
on November 21, 2008 5:16 PM |

The unbelievable story of Julie Amero concluded quietly Friday afternoon at Superior Court in Norwich, with the state of Connecticut dropping four felony pornography charges.

Amero agreed to plead guilty to a single charge of disorderly conduct, a misdemeanor. Amero, who has been hospitalized and suffers from declining health, also surrendered her teaching license.

"Oh honey, it's over. I feel wonderful," Amero, 41, said a few minutes after accepting the deal where she also had to surrender her teaching license. "The Norwich police made a mistake. It was proven. That makes me feel like I'm on top of the world."

In June of 2007, Judge Hillary B. Strackbein tossed out Amero's conviction on charges that she intentionally caused a stream of "pop-up" pornography on the computer in her classroom and allowed students to view it. Confronted with evidence compiled by forensic computer experts, Strackbein ordered a new trial, saying the conviction was based on "erroneous" and "false information."

But since that dramatic reversal, local officials, police and state prosecutors were unwilling to admit that a mistake may have been made -- even after computer experts from around the country demonstrated that Amero's computer had been infected by "spyware."

New London County State's Attorney Michael Regan told me late Friday the state remained convinced Amero was guilty and was prepared to again go to trial.

"I have no regrets. Things took a course that was unplanned. Unfortunately the computer wasn't examined properly by the Norwich police," Regan said.

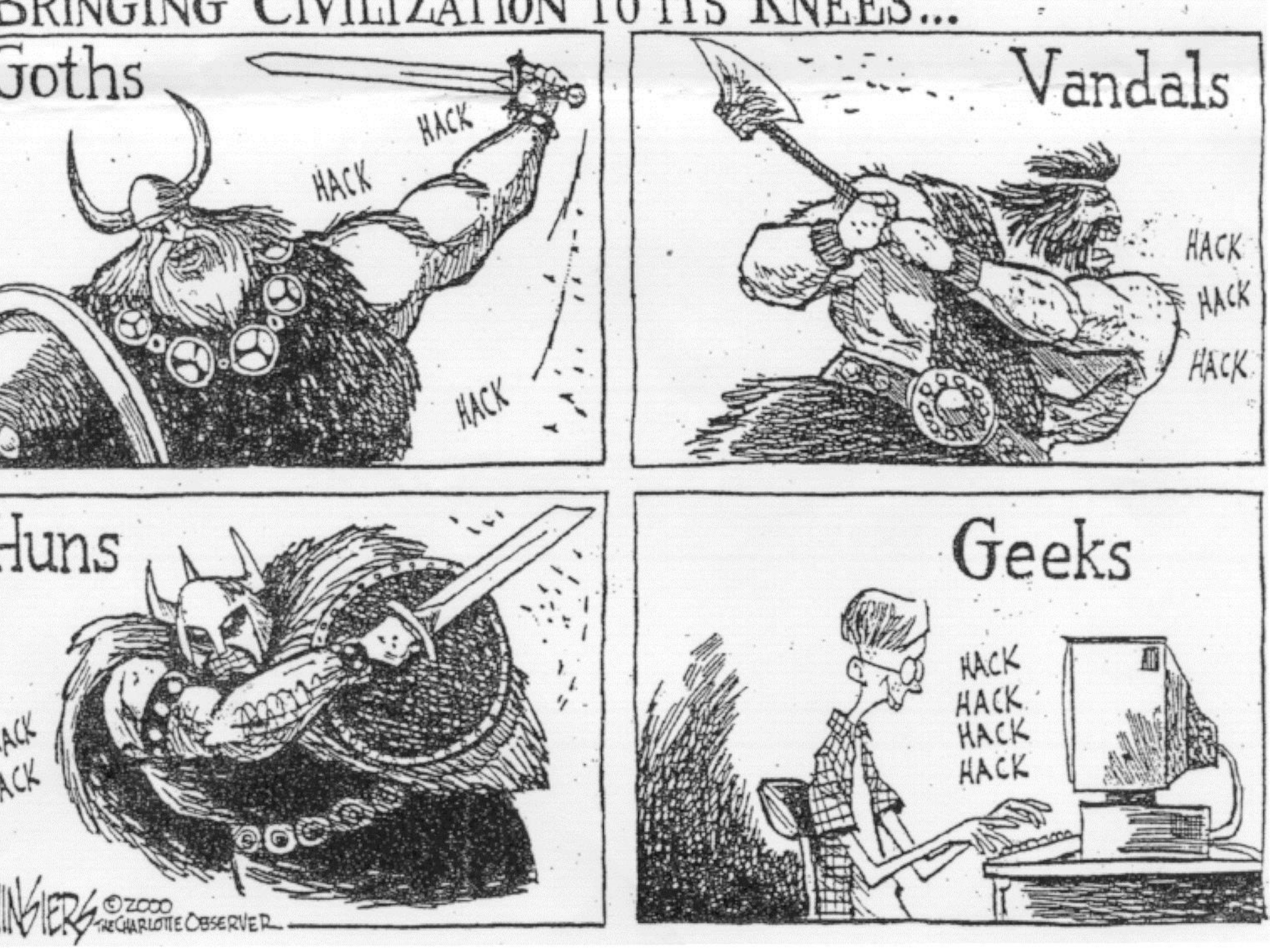
"For some reason this case caught the media's attention," Regan said.

The case also caught the attention of computer security experts from California to Florida, who read about Amero's conviction on Internet news sites. Recognizing the classic signs of a computer infected by malicious adware, volunteers examined computer records and the hard drive and determined that Amero was not responsible for the pornographic stream on her computer.

The state never conducted a forensic examination of the hard drive and instead relied on the expertise of a Norwich detective, with limited computer experience. Experts working for Amero ridiculed the state's evidence, saying it was a classic case of spyware seizing control of the computer. Other experts also said that Amero's response -- she failed to turn off the computer -- was not unusual in cases like this.

Among other things, the security experts found that the Norwich school system had failed to properly update software that would have blocked the pornography in the first place.

http://blogs.courant.com/rick_green/2008/11/connecticut-drops-felony-charg.html


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
ACK
ACK
Geeks
HACK
HACK
HACK
HACK
INSIERS ©2000 THE CHARLOTTE OBSERVER

A Metaphor…..


The Unintended
Consequences

Implications for the Legal System

Crossroads

Motivation for our Work

J**udges & lawyers** need to know about **digital evidence** in order to make effective, educated decisions.

They are woefully ignorant!

Why is this Important?

- Avoid miscarriages of Justice
- Prevent disruption to legal system

Two Cases

- Derive digital evidence literacy requirements from:
  - *State of Connecticut v. Julie Amero*
  - *Lorraine v. Markel American Insurance Co.*

Case Analysis Framework

- Digital evidence admitted
- Evaluation of digital evidence by Judge and Attorneys
- Expert Witness testimony
- Legal court precedence
- Laws and regulations identified
- Legal Result

Connecticut drops felony charges against Julie Amero, four years after her arrest

By
Rick Green
on November 21, 2008 5:16 PM |

The unbelievable story of Julie Amero concluded quietly Friday afternoon at Superior Court in Norwich, with the state of Connecticut dropping four felony pornography charges.

Amero agreed to plead guilty to a single charge of disorderly conduct, a misdemeanor. Amero, who has been hospitalized and suffers from declining health, also surrendered her teaching license.

"Oh honey, it's over. I feel wonderful," Amero, 41, said a few minutes after accepting the deal where she also had to surrender her teaching license. "The Norwich police made a mistake. It was proven. That makes me feel like I'm on top of the world."

In June of 2007, Judge Hillary B. Strackbein tossed out Amero's conviction on charges that she intentionally caused a stream of "pop-up" pornography on the computer in her classroom and allowed students to view it. Confronted with evidence compiled by forensic computer experts, Strackbein ordered a new trial, saying the conviction was based on "erroneous" and "false information."

But since that dramatic reversal, local officials, police and state prosecutors were unwilling to admit that a mistake may have been made -- even after computer experts from around the country demonstrated that Amero's computer had been infected by "spyware."

New London County State's Attorney Michael Regan told me late Friday the state remained convinced Amero was guilty and was prepared to again go to trial.

"I have no regrets. Things took a course that was unplanned. Unfortunately the computer wasn't examined properly by the Norwich police," Regan said.

"For some reason this case caught the media's attention," Regan said.

The case also caught the attention of computer security experts from California to Florida, who read about Amero's conviction on Internet news sites. Recognizing the classic signs of a computer infected by malicious adware, volunteers examined computer records and the hard drive and determined that Amero was not responsible for the pornographic stream on her computer.

The state never conducted a forensic examination of the hard drive and instead relied on the expertise of a Norwich detective, with limited computer experience. Experts working for Amero ridiculed the state's evidence, saying it was a classic case of spyware seizing control of the computer. Other experts also said that Amero's response -- she failed to turn off the computer -- was not unusual in cases like this.

Among other things, the security experts found that the Norwich school system had failed to properly update software that would have blocked the pornography in the first place.

http://blogs.courant.com/rick_green/2008/11/connecticut-drops-felony-charg.html

State of Connecticut v. Julie Amero

- Overview:
  - Middle-school substitute Julie Amero
    - Told not to turn off computer
  - Continuous loop of pornographic pop-ups were viewed on computer by class
  - Anti-Virus expired five months earlier
  - Amero attempted to shield the screen but did not shut off the computer or monitor

State v. Amero

- **Digital Evidence Admitted**
  - Hard drive
    - Fuzzy chain of evidence
    - Unclear if properly duplicated
    - Timestamp discrepancy of “10 to 12 mins.”
    - No examination for viruses

State v. Amero

- **Evaluation of digital evidence by Judges & Attorneys**
  - No clear and full objection of admissibility
  - Lawyers did not question discrepancies
  - Lawyers had low computer literacy
  - No objection to displaying full-size pictures in courtroom when actual was pop-up size
  - Judge did not allow defense expert witness

State v. Amero

- **Expert & Witness Testimony**
  - Testimony often inaccurate:
    - Anti-Virus was properly updated – *false*
    - Not possible to have pornographic loop – *false*
    - Temp. File links in red = intentional site visit – *false*

State v. Amero

Q: … anything different about that link as opposed to other links?
A: The color, it's red.

Q: And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?
A: That indicates that the link was actively clicked on and you were sent to that page.

Q: Okay. So a person would actually have to click on the… link to go to another page, correct?
A: Yes

State v. Amero

- **Legal court precedence**
  - None referenced

- **Laws and regulations identified**
  - None referenced

State v. Amero

- **Legal Result**
  - Julie Amero was convicted
  - Faced up to a 40 year sentence
  - After years of appeal, trial results set aside and retrial called for later
  - Amero pled to a misdemeanor to end it
    - Paid $100
    - Gave up teaching license

UNIVERSITY of WASHINGTON

Admissibility Process

Case II

Lorraine v. Markel American Insurance Co.

- Overview:
  - Judge Paul W. Grimm
  - Insurance dispute for boat struck by lightning
  - Plaintiff claims damage to hull found several months later was caused by lightning strike & should be covered under insurance
- The ***opinion*** is what matters in this case—sets precedence

Lorraine v. Markel

Digital evidence admitted:

Admissibility starts with: **Judge determination**

"The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible."

Fed R. Evid. 104(a)

BUT…

Depends largely on objections by opposing counsel

Referred to Fed Rules of Evidence

- Relevance
- Authentication
- Hearsay rules
- Original writing and best evidence

Lorraine v. Markel

Relevance

Evidence is relevant if it has *"… any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."*

Fed. R. Evid. 401

Lorraine v. Markel

Authentication

"To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."

Fed. R. Evid. 901(a)

Lorraine v. Markel

Hearsay

Generally, not applicable for digital evidence

Original Writing Rule & Best Evidence

Duplicates can be admitted in place of originals unless authenticity of original is in question

Rules of Evidence identified/applied in *Lorraine v. Markel*

Legal Guidance	*Subject*
Federal Rules of Evidence 104(a) Federal Rules of Evidence 104(b)	Preliminary Questions; relationship between judge and jury
Federal Rules of Evidence 401 Federal Rules of Evidence 402	Relevance
Federal Rules of Evidence 901	Authenticity; including examples of how to authenticate
Federal Rules of Evidence 902	Self-Authentication; including examples
Federal Rules of Evidence 801 Federal Rules of Evidence 803 Federal Rules of Evidence 804 Federal Rules of Evidence 807	Hearsay; including exceptions to the hearsay
Federal Rules of Evidence 1001 through 1008	Original Writing Rule; also known as the "Best Evidence Rule." Includes use of accurate duplicates.
Federal Rules of Evidence 403	Balance of Probative Value with Unfair Prejudice

UNIVERSITY of WASHINGTON

Applying *Lorraine v. Markel* & the Federal Rules of Evidence to *State v. Amero*

Digital evidence admitted

State v. Amero

- Hard drive

Lorraine v. Markel

- Defined admissibility & authentication procedures

Evaluation of digital evidence by Judge & Attorneys

State v. Amero

- Defense lawyers did not question authenticity of expert testimony
- No clear and full objection of admissibility

Lorraine v. Markel

- While admissibility decision is by judge,
- It depends largely on objections by opposing counsel

Expert & Witness Testimony

State v. Amero

- Many State expert witnesses, though sometimes inaccurate
- No challenges

- Defense expert witness not allowed to testify

Lorraine v. Markel

- Establishes expert witnesses must be used (both sides) to authenticate digital evidence

  (referencing Fed. R. Evid. 901)

Legal court precedence

State v. Amero

- None referenced

Lorraine v. Markel

- *Acknowledges lack of precedence, but attempts to establish same*

"Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial"

Laws and regulations identified

State v. Amero

- None referenced

Lorraine v. Markel

- Federal Rules of Evidence

Likely Amero Outcomes had Lorraine v. Merkel Applied

- Dismissal of Amero case
- Sanctioning of prosecutor
- Life reclaimed
  - Years of legal agony
  - Marriage intact
  - Career intact
  - Health intact

Recommendations

For digital evidence education requirements for lawyers & judges

Recommendation 1:

Basic Computer Literacy

- Provide basic knowledge of how computer systems work
- Basis for proper line of questioning

Recommendation 2:

Understanding of digital forensics process

- Provide basic understanding of proper chain of custody procedures, proper handling of digital evidence

Recommendation 3:

Knowledge of Federal Rules Evidence & how they apply to digital evidence

- Provide examples of how those rules integral to admissibility apply to authenticate digital evidence

Recommendation 4:

Survey of case law

- To further understand how the process of admissibility has been decided
- To inform our understanding of other admissibility tests, also:
  - *Daubert* test
  - *Frye* test

Future Work

- Expand research to include more cases
- Use findings to inform development of digital evidence curriculum at law schools
  - Current collaboration with UW School of Law
  - Expecting to expand to others in the State

Questions?

Dr. Barbara Endicott-Popovsky

endicott@uw.edu

Center for Information Assurance & Cybersecurity
University of Washington